Vulnerability Assessment Report
Liquidweb Parent

Audited on Fri Feb 20 2026 08:17:17

CONFIDENTIAL

Part 1: Scan Information	
Organization Scanned:	Liquidweb Parent
Scan Completion Date:	Fri Feb 20 2026 13:50:30
Scan Profile(s):	Full Vulnerability Scanning
Scan Profile Description:	**Full Vulnerability Scanning** (Based of Full and fast) Most NVT's; optimized by using previously collected information.
Result Summary:	There were a total of **110** vulnerabilities found during this scan. No High level vulnerabilities were detected. **2** vulnerabilities were found to have a medium risk. Medium level vulnerabilities are a bit more difficult to exploit and may only partially affect the system. **108** low risk vulnerabilities were found. These vulnerabilities may provide information that can assist in subsequent exploitation attempts against your environment.

Part 2. Live Host Summary

IP Address	Asset Name	High	Medium	Low	Risk Score
209.59.154.193	host.bayclub.in	0	2	108	Medium (500)

Part 3. Vulnerability Details for each IP Address

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	443/tcp	The script attempts to identify files containing sensitive data at the remote web server.	medium	NOCVE	5.0
	Vulnerability Detection Result: The following files containing sensitive information were identified (URL:Description): https://209.59.154.193/web.config:Microsoft IIS / ASP.NET Core Module web.config file accessible. This could contain sensitive information about the structure of the application / web server and shouldn't be accessible. **Impact:** Based on the information provided in these files an attacker might be able to gather additional info and/or sensitive data like usernames and passwords. **Solution** **Solution type:** MitigationThe sensitive files shouldn't be accessible via a web server. Restrict access to it or remove it completely. **Detection Reliability:** Remote checks that do some analysis but which are not always fully reliable. **Vulnerability Insight:** Currently the script is checking for files like e.g.: - Software (Blog, CMS) configuration or log files - Web / application server configuration / password files (.htaccess, .htpasswd, web.config, web.xml, ...) - Cloud (e.g. AWS) configuration files - Files containing API keys for services / providers - Database backup files - SSH or SSL/TLS Private Keys			**Vulnerability Detection Method:** Enumerate the remote web server and check if sensitive files are accessible. **Details:** Sensitive File Disclosure (HTTP) (NVT: 1.3.6.1.4.1.25623.1.0.107305) **Version used:** 2023-09-26T05:05:30+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:P/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF	
209.59.154.193 host.bayclub.in	522/tcp	The remote SSH server is configured to allow / support weak encryption algorithm(s).	medium	NOCVE	4.3
	Vulnerability Detection Result: The following weak client-to-server encryption algorithms are supported by the remote service: aes128-cbc aes256-cbc The following weak server-to-client encryption algorithms are supported by the remote service: aes128-cbc aes256-cbc **Solution** **Solution type:** MitigationDisable the reported weak encryption algorithm(s). **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so. **Vulnerability Insight:** - The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore. - The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it. - A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.			**Vulnerability Detection Method:** Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server. Currently weak encryption algorithms are defined as the following: - Arcfour (RC4) cipher based algorithms - 'none' algorithm - CBC mode cipher based algorithms **Details:** Weak Encryption Algorithm(s) Supported (SSH) (NVT: 1.3.6.1.4.1.25623.1.0.105611) **Version used:** 2023-09-28T05:05:04+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:M/Au:N/C:P/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://www.rfc-editor.org/rfc/rfc8758, URL:https://www.kb.cert.org/vuls/id/958563, URL:https://www.rfc-editor.org/rfc/rfc4253#section-6.3	

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	general/tcp	The remote host implements TCP timestamps and therefore allows to compute the uptime.	low	NOCVE	2.6
	Vulnerability Detection Result: It was detected that the host implements RFC1323/RFC7323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 3863558710 Packet 2: 3863559818 **Impact:** A side effect of this feature is that the uptime of the remote host can sometimes be computed. **Solution** **Solution type:** MitigationTo disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information. **Affected Software/OS:** TCP implementations that implement RFC1323/RFC7323. **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so. **Vulnerability Insight:** The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.			**Vulnerability Detection Method:** Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. **Details:** TCP Timestamps Information Disclosure (NVT: 1.3.6.1.4.1.25623.1.0.80091) **Version used:** 2023-08-01T13:29:10+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:H/Au:N/C:P/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://datatracker.ietf.org/doc/html/rfc1323, URL:https://datatracker.ietf.org/doc/html/rfc7323, URL:https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152		
209.59.154.193 host.bayclub.in	general/tcp	This plugin runs nmap to find open ports.	low	NOCVE	0.0
	Vulnerability Detection Result: There are no UDP ports exposed. **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** Nmap (NASL wrapper) (NVT: 1.3.6.1.4.1.25623.1.0.14259) **Version used:** 2023-08-01T13:29:10+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://nmap.org/, URL:https://nmap.org/book/performance-timing-templates.html, URL:https://nmap.org/book/man-performance.html		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	general/tcp	This plugin runs nmap to find open ports.	low	NOCVE	0.0
	Vulnerability Detection Result: The following ports were discovered with open state allowing TCP connections: 21/tcp open ftp 25/tcp open smtp 53/tcp open domain 80/tcp open http 110/tcp open pop3 143/tcp open imap 443/tcp open https 465/tcp open smtps 522/tcp open ulp 587/tcp open submission 993/tcp open imaps 995/tcp open pop3s **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** Nmap (NASL wrapper) (NVT: 1.3.6.1.4.1.25623.1.0.14259) **Version used:** 2023-08-01T13:29:10+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://nmap.org/, URL:https://nmap.org/book/performance-timing-templates.html, URL:https://nmap.org/book/man-performance.html		
209.59.154.193 host.bayclub.in	465/tcp	This plugin performs service detection.	low	NOCVE	0.0
	Vulnerability Detection Result: A TLScustom server answered on this port **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so. **Vulnerability Insight:** This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.		**Details:** Services (NVT: 1.3.6.1.4.1.25623.1.0.10330) **Version used:** 2023-06-14T05:05:19+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	993/tcp	This plugin performs service detection.	low	NOCVE	0.0
	Vulnerability Detection Result: An IMAP server is running on this port through SSL **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so. **Vulnerability Insight:** This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.		**Details:** Services (NVT: 1.3.6.1.4.1.25623.1.0.10330) **Version used:** 2023-06-14T05:05:19+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	143/tcp	This plugin performs service detection.	low	NOCVE	0.0
	Vulnerability Detection Result: An IMAP server is running on this port **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so. **Vulnerability Insight:** This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.		**Details:** Services (NVT: 1.3.6.1.4.1.25623.1.0.10330) **Version used:** 2023-06-14T05:05:19+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	443/tcp	This plugin performs service detection.	low	NOCVE	0.0
	Vulnerability Detection Result: A TLScustom server answered on this port **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so. **Vulnerability Insight:** This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.		**Details:** Services (NVT: 1.3.6.1.4.1.25623.1.0.10330) **Version used:** 2023-06-14T05:05:19+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	993/tcp	This plugin performs service detection.	low	NOCVE	0.0
	Vulnerability Detection Result: A TLScustom server answered on this port **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so. **Vulnerability Insight:** This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.		**Details:** Services (NVT: 1.3.6.1.4.1.25623.1.0.10330) **Version used:** 2023-06-14T05:05:19+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	443/tcp	This plugin performs service detection.	low	NOCVE	0.0
	Vulnerability Detection Result: A web server is running on this port through SSL **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so. **Vulnerability Insight:** This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.		**Details:** Services (NVT: 1.3.6.1.4.1.25623.1.0.10330) **Version used:** 2023-06-14T05:05:19+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	80/tcp	This plugin performs service detection.	low	NOCVE	0.0
	Vulnerability Detection Result: A web server is running on this port **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so. **Vulnerability Insight:** This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.		**Details:** Services (NVT: 1.3.6.1.4.1.25623.1.0.10330) **Version used:** 2023-06-14T05:05:19+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	995/tcp	This plugin performs service detection.	low	NOCVE	0.0
	Vulnerability Detection Result: A TLScustom server answered on this port **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so. **Vulnerability Insight:** This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.		**Details:** Services (NVT: 1.3.6.1.4.1.25623.1.0.10330) **Version used:** 2023-06-14T05:05:19+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	522/tcp	This plugin performs service detection.	low	NOCVE	0.0
	Vulnerability Detection Result: An ssh server is running on this port **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so. **Vulnerability Insight:** This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.		**Details:** Services (NVT: 1.3.6.1.4.1.25623.1.0.10330) **Version used:** 2023-06-14T05:05:19+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	110/tcp	This plugin performs service detection.	low	NOCVE	0.0
	Vulnerability Detection Result: A pop3 server is running on this port **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so. **Vulnerability Insight:** This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.		**Details:** Services (NVT: 1.3.6.1.4.1.25623.1.0.10330) **Version used:** 2023-06-14T05:05:19+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	995/tcp	This plugin performs service detection.	low	NOCVE	0.0
	Vulnerability Detection Result: A pop3 server is running on this port **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so. **Vulnerability Insight:** This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.		**Details:** Services (NVT: 1.3.6.1.4.1.25623.1.0.10330) **Version used:** 2023-06-14T05:05:19+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	21/tcp	This plugin performs service detection.	low	NOCVE	0.0
	Vulnerability Detection Result: An FTP server is running on this port. Here is its banner : 220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so. **Vulnerability Insight:** This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.		**Details:** Services (NVT: 1.3.6.1.4.1.25623.1.0.10330) **Version used:** 2023-06-14T05:05:19+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	25/tcp	This plugin performs service detection.	low	NOCVE	0.0
	Vulnerability Detection Result: An SMTP server is running on this port Here is its banner : 220-host.bayclub.in ESMTP Exim 4.99.1 #2 Fri, 20 Feb 2026 18:58:31 +0530 **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so. **Vulnerability Insight:** This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.		**Details:** Services (NVT: 1.3.6.1.4.1.25623.1.0.10330) **Version used:** 2023-06-14T05:05:19+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	465/tcp	This plugin performs service detection.	low	NOCVE	0.0
	Vulnerability Detection Result: An SMTP server is running on this port through SSL Here is its banner : 220-host.bayclub.in ESMTP Exim 4.99.1 #2 Fri, 20 Feb 2026 18:58:31 +0530 **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so. **Vulnerability Insight:** This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.		**Details:** Services (NVT: 1.3.6.1.4.1.25623.1.0.10330) **Version used:** 2023-06-14T05:05:19+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	587/tcp	This plugin performs service detection.	low	NOCVE	0.0
	Vulnerability Detection Result: An SMTP server is running on this port Here is its banner : 220-host.bayclub.in ESMTP Exim 4.99.1 #2 Fri, 20 Feb 2026 18:58:33 +0530 **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so. **Vulnerability Insight:** This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.		**Details:** Services (NVT: 1.3.6.1.4.1.25623.1.0.10330) **Version used:** 2023-06-14T05:05:19+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	21/tcp	This Plugin detects and reports a FTP Server Banner.	low	NOCVE	0.0
	Vulnerability Detection Result: Remote FTP server banner: 220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220-You are user number 2 of 50 allowed. 220-Local time is now 18:58. Server port: 21. 220-This is a private system - No anonymous login 220-IPv6 connections are also welcome on this server. 220 You will be disconnected after 15 minutes of inactivity. This is probably (a): - Pure-FTPd - Various FTP servers (e.g. Zyxel Access Points) Server operating system information collected via "SYST" command: 215 UNIX Type: L8 **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** FTP Banner Detection (NVT: 1.3.6.1.4.1.25623.1.0.10092) **Version used:** 2023-08-25T05:06:04+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	995/tcp	This detects the POP3 Server's type and version by connecting to the server and processing the received banner.	low	NOCVE	0.0
	Vulnerability Detection Result: Remote POP3 server banner: +OK Dovecot ready. This is probably: - Dovecot The remote POP3 server is announcing the following available CAPABILITIES via an encrypted connection: AUTH-RESP-CODE, CAPA, PIPELINING, RESP-CODES, SASL PLAIN LOGIN, TOP, UIDL, USER **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** POP3 Server type and version (NVT: 1.3.6.1.4.1.25623.1.0.10185) **Version used:** 2023-08-01T13:29:10+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	21/tcp	Checks if the remote FTP server supports SSL/TLS (FTPS) with the 'AUTH TLS' command.	low	NOCVE	0.0
	Vulnerability Detection Result: The remote FTP server supports TLS (FTPS) with the 'AUTH TLS' command. **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** SSL/TLS: FTP 'AUTH TLS' Command Detection (NVT: 1.3.6.1.4.1.25623.1.0.105009) **Version used:** 2023-07-26T05:05:09+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://tools.ietf.org/html/rfc4217		
209.59.154.193 host.bayclub.in	110/tcp	This detects the POP3 Server's type and version by connecting to the server and processing the received banner.	low	NOCVE	0.0
	Vulnerability Detection Result: Remote POP3 server banner: +OK Dovecot ready. This is probably: - Dovecot The remote POP3 server is announcing the following available CAPABILITIES via an unencrypted connection: AUTH-RESP-CODE, CAPA, PIPELINING, RESP-CODES, SASL, STLS, TOP, UIDL **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** POP3 Server type and version (NVT: 1.3.6.1.4.1.25623.1.0.10185) **Version used:** 2023-08-01T13:29:10+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	522/tcp	This detects the SSH Server's type and version by connecting to the server and processing the buffer received.	low	NOCVE	0.0
	Vulnerability Detection Result: Remote SSH server banner: SSH-2.0-OpenSSH_8.0 Remote SSH supported authentication: password,publickey Remote SSH text/login banner: (not available) This is probably: - OpenSSH Concluded from remote connection attempt with credentials: Login: OpenVASVT Password: OpenVASVT **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so. **Vulnerability Insight:** This information gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.		**Details:** SSH Server type and version (NVT: 1.3.6.1.4.1.25623.1.0.10267) **Version used:** 2023-09-27T05:05:31+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	993/tcp	This detects the IMAP Server's type and version by connecting to the server and processing the received banner.	low	NOCVE	0.0
	Vulnerability Detection Result: Remote IMAP server banner: * OK [CAPABILITY IMAP4rev1 LOGIN-REFERRALS ID ENABLE IDLE SASL-IR LITERAL+ AUTH=PLAIN AUTH=LOGIN] Dovecot ready. * ID ("name" "Dovecot") This is probably: - Dovecot The remote IMAP server is announcing the following available CAPABILITIES via an encrypted connection: AUTH=LOGIN, AUTH=PLAIN, ENABLE, ID, IDLE, LITERAL+, LOGIN-REFERRALS, SASL-IR **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** IMAP Server type and version (NVT: 1.3.6.1.4.1.25623.1.0.11414) **Version used:** 2023-08-01T13:29:10+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	143/tcp	This detects the IMAP Server's type and version by connecting to the server and processing the received banner.	low	NOCVE	0.0
	Vulnerability Detection Result: Remote IMAP server banner: * OK [CAPABILITY IMAP4rev1 LOGIN-REFERRALS ID ENABLE IDLE SASL-IR LITERAL+ STARTTLS LOGINDISABLED] Dovecot ready. * ID ("name" "Dovecot") This is probably: - Dovecot The remote IMAP server is announcing the following available CAPABILITIES via an unencrypted connection: ENABLE, ID, IDLE, LITERAL+, LOGIN-REFERRALS, LOGINDISABLED, SASL-IR, STARTTLS **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** IMAP Server type and version (NVT: 1.3.6.1.4.1.25623.1.0.11414) **Version used:** 2023-08-01T13:29:10+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	110/tcp	Checks if the remote POP3 server supports SSL/TLS with the 'STLS' command.	low	NOCVE	0.0
	Vulnerability Detection Result: The remote POP3 server supports SSL/TLS with the 'STLS' command. The remote POP3 server is announcing the following CAPABILITIES before sending the 'STLS' command: AUTH-RESP-CODE, CAPA, PIPELINING, RESP-CODES, SASL, STLS, TOP, UIDL The remote POP3 server is announcing the following CAPABILITIES after sending the 'STLS' command: AUTH-RESP-CODE, CAPA, PIPELINING, RESP-CODES, SASL PLAIN LOGIN, TOP, UIDL, USER **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** SSL/TLS: POP3 'STLS' Command Detection (NVT: 1.3.6.1.4.1.25623.1.0.105008) **Version used:** 2021-11-12T09:42:39+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://tools.ietf.org/html/rfc2595		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	143/tcp	Checks if the remote IMAP server supports SSL/TLS with the 'STARTTLS' command.	low	NOCVE	0.0
	Vulnerability Detection Result: The remote IMAP server supports SSL/TLS with the 'STARTTLS' command. The remote IMAP server is announcing the following CAPABILITIES before sending the 'STARTTLS' command: ENABLE, ID, IDLE, LITERAL+, LOGIN-REFERRALS, LOGINDISABLED, SASL-IR, STARTTLS The remote IMAP server is announcing the following CAPABILITIES after sending the 'STARTTLS' command: AUTH=LOGIN, AUTH=PLAIN, ENABLE, ID, IDLE, LITERAL+, LOGIN-REFERRALS, SASL-IR **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** SSL/TLS: IMAP 'STARTTLS' Command Detection (NVT: 1.3.6.1.4.1.25623.1.0.105007) **Version used:** 2021-11-12T09:42:39+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://tools.ietf.org/html/rfc2595		
209.59.154.193 host.bayclub.in	587/tcp	This detects the SMTP Server's type and version by connecting to the server and processing the buffer received.	low	NOCVE	0.0
	Vulnerability Detection Result: Remote SMTP server banner: 220-host.bayclub.in ESMTP Exim 4.99.1 #2 Fri, 20 Feb 2026 18:59:01 +0530 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail. The remote SMTP server is announcing the following available ESMTP commands (EHLO response) via an unencrypted connection: 8BITMIME, HELP, LIMITS MAILMAX=1000 RCPTMAX=50000, PIPECONNECT, PIPELINING, SIZE 52428800, STARTTLS **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** SMTP Server type and version (NVT: 1.3.6.1.4.1.25623.1.0.10263) **Version used:** 2023-08-01T13:29:10+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	53/tcp	TCP based detection of a DNS server.	low	NOCVE	0.0
	Vulnerability Detection Result: The remote DNS server banner is: 9.11.36-RedHat-9.11.36-16.el8_10.6 **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** DNS Server Detection (TCP) (NVT: 1.3.6.1.4.1.25623.1.0.108018) **Version used:** 2021-11-30T08:05:58+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	465/tcp	This detects the SMTP Server's type and version by connecting to the server and processing the buffer received.	low	NOCVE	0.0
	Vulnerability Detection Result: Remote SMTP server banner: 220-host.bayclub.in ESMTP Exim 4.99.1 #2 Fri, 20 Feb 2026 18:59:51 +0530 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail. The remote SMTP server is announcing the following available ESMTP commands (EHLO response) via an encrypted connection: 8BITMIME, AUTH PLAIN LOGIN, HELP, LIMITS MAILMAX=1000 RCPTMAX=50000, PIPECONNECT, PIPELINING, SIZE 52428800 **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** SMTP Server type and version (NVT: 1.3.6.1.4.1.25623.1.0.10263) **Version used:** 2023-08-01T13:29:10+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	25/tcp	This detects the SMTP Server's type and version by connecting to the server and processing the buffer received.	low	NOCVE	0.0
	Vulnerability Detection Result: Remote SMTP server banner: 220-host.bayclub.in ESMTP Exim 4.99.1 #2 Fri, 20 Feb 2026 19:00:41 +0530 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail. The remote SMTP server is announcing the following available ESMTP commands (EHLO response) via an unencrypted connection: 8BITMIME, HELP, LIMITS MAILMAX=1000 RCPTMAX=50000, PIPECONNECT, PIPELINING, SIZE 52428800, STARTTLS **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** SMTP Server type and version (NVT: 1.3.6.1.4.1.25623.1.0.10263) **Version used:** 2023-08-01T13:29:10+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	587/tcp	Checks if the remote SMTP server supports SSL/TLS with the 'STARTTLS' command.	low	NOCVE	0.0
	Vulnerability Detection Result: The remote SMTP server supports SSL/TLS with the 'STARTTLS' command. The remote SMTP server is announcing the following available ESMTP commands (EHLO response) before sending the 'STARTTLS' command: 8BITMIME, HELP, LIMITS MAILMAX=1000 RCPTMAX=50000, PIPECONNECT, PIPELINING, SIZE 52428800, STARTTLS The remote SMTP server is announcing the following available ESMTP commands (EHLO response) after sending the 'STARTTLS' command: 8BITMIME, AUTH PLAIN LOGIN, HELP, LIMITS MAILMAX=1000 RCPTMAX=50000, PIPECONNECT, PIPELINING, SIZE 52428800 **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** SSL/TLS: SMTP 'STARTTLS' Command Detection (NVT: 1.3.6.1.4.1.25623.1.0.103118) **Version used:** 2023-07-12T05:05:04+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://tools.ietf.org/html/rfc3207		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	25/tcp	Checks if the remote SMTP server supports SSL/TLS with the 'STARTTLS' command.	low	NOCVE	0.0
	Vulnerability Detection Result: The remote SMTP server supports SSL/TLS with the 'STARTTLS' command. The remote SMTP server is announcing the following available ESMTP commands (EHLO response) before sending the 'STARTTLS' command: 8BITMIME, HELP, LIMITS MAILMAX=1000 RCPTMAX=50000, PIPECONNECT, PIPELINING, SIZE 52428800, STARTTLS The remote SMTP server is announcing the following available ESMTP commands (EHLO response) after sending the 'STARTTLS' command: 8BITMIME, AUTH PLAIN LOGIN, HELP, LIMITS MAILMAX=1000 RCPTMAX=50000, PIPECONNECT, PIPELINING, SIZE 52428800 **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** SSL/TLS: SMTP 'STARTTLS' Command Detection (NVT: 1.3.6.1.4.1.25623.1.0.103118) **Version used:** 2023-07-12T05:05:04+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://tools.ietf.org/html/rfc3207		
209.59.154.193 host.bayclub.in	general/tcp	Consolidation of Dovecot detections.	low	NOCVE	0.0
	Vulnerability Detection Result: *1 (Click here to access the vulnerability details) **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** Dovecot Detection Consolidation (NVT: 1.3.6.1.4.1.25623.1.0.113212) **Version used:** 2022-01-18T12:57:07+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://www.dovecot.org/		
209.59.154.193 host.bayclub.in	587/tcp	The script sends a connection request to the server and attempts to extract the version number from the reply.	low	NOCVE	0.0
	Vulnerability Detection Result: Detected Exim Version: 4.99.1 Location: 587/tcp CPE: cpe:/a:exim:exim:4.99.1 Concluded from version/product identification result: 220-host.bayclub.in ESMTP Exim 4.99.1 #2 Fri, 20 Feb 2026 18:59:01 +0530 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail. **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** Exim Detection (NVT: 1.3.6.1.4.1.25623.1.0.105189) **Version used:** 2023-07-26T05:05:09+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	465/tcp	The script sends a connection request to the server and attempts to extract the version number from the reply.	low	NOCVE	0.0
	Vulnerability Detection Result: Detected Exim Version: 4.99.1 Location: 465/tcp CPE: cpe:/a:exim:exim:4.99.1 Concluded from version/product identification result: 220-host.bayclub.in ESMTP Exim 4.99.1 #2 Fri, 20 Feb 2026 18:59:51 +0530 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail. **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** Exim Detection (NVT: 1.3.6.1.4.1.25623.1.0.105189) **Version used:** 2023-07-26T05:05:09+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	25/tcp	The script sends a connection request to the server and attempts to extract the version number from the reply.	low	NOCVE	0.0
	Vulnerability Detection Result: Detected Exim Version: 4.99.1 Location: 25/tcp CPE: cpe:/a:exim:exim:4.99.1 Concluded from version/product identification result: 220-host.bayclub.in ESMTP Exim 4.99.1 #2 Fri, 20 Feb 2026 19:00:41 +0530 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail. **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** Exim Detection (NVT: 1.3.6.1.4.1.25623.1.0.105189) **Version used:** 2023-07-26T05:05:09+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	general/tcp	Consolidation of OpenSSH detections.	low	NOCVE	0.0
	Vulnerability Detection Result: Detected OpenSSH Server Version: 8.0 Location: 522/tcp CPE: cpe:/a:openbsd:openssh:8.0 Concluded from version/product identification result: SSH-2.0-OpenSSH_8.0 **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** OpenSSH Detection Consolidation (NVT: 1.3.6.1.4.1.25623.1.0.108577) **Version used:** 2022-03-28T10:48:38+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://www.openssh.com/		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	522/tcp	This script detects which algorithms are supported by the remote SSH Service.	low	NOCVE	0.0
	Vulnerability Detection Result: The following options are supported by the remote ssh service: kex_algorithms: curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,kex-strict-s-v00@openssh.com server_host_key_algorithms: rsa-sha2-512,rsa-sha2-256,ssh-rsa,ecdsa-sha2-nistp256,ssh-ed25519 encryption_algorithms_client_to_server: aes256-gcm@openssh.com,chacha20-poly1305@openssh.com,aes256-ctr,aes256-cbc,aes128-gcm@openssh.com,aes128-ctr,aes128-cbc encryption_algorithms_server_to_client: aes256-gcm@openssh.com,chacha20-poly1305@openssh.com,aes256-ctr,aes256-cbc,aes128-gcm@openssh.com,aes128-ctr,aes128-cbc mac_algorithms_client_to_server: hmac-sha2-256-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha1,umac-128@openssh.com,hmac-sha2-512 mac_algorithms_server_to_client: hmac-sha2-256-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha1,umac-128@openssh.com,hmac-sha2-512 compression_algorithms_client_to_server: none,zlib@openssh.com compression_algorithms_server_to_client: none,zlib@openssh.com **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.			**Details:** SSH Protocol Algorithms Supported (NVT: 1.3.6.1.4.1.25623.1.0.105565) **Version used:** 2023-09-27T05:05:31+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF	
209.59.154.193 host.bayclub.in	522/tcp	Identification of SSH protocol versions supported by the remote SSH Server. Also reads the corresponding fingerprints from the service.	low	NOCVE	0.0
	Vulnerability Detection Result: The remote SSH Server supports the following SSH Protocol Versions: 1.99 2.0 SSHv2 Fingerprint(s): ecdsa-sha2-nistp256: 8a:8a:0c:9f:f0:18:63:77:b1:d7:fc:0c:a5:d8:b6:a6 ssh-rsa: 77:4b:8f:45:33:3a:c4:80:53:3d:65:8a:4e:ac:38:fa **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response shows the likely presence of the vulnerable application or of the vulnerability. "Likely" means that only rare circumstances are possible where the detection would be wrong.			**Vulnerability Detection Method:** The following versions are tried: 1.33, 1.5, 1.99 and 2.0. **Details:** SSH Protocol Versions Supported (NVT: 1.3.6.1.4.1.25623.1.0.100259) **Version used:** 2023-09-27T05:05:31+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF	

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	53/tcp	DNS based detection of ISC BIND.	low	NOCVE	0.0
	Vulnerability Detection Result: Detected ISC BIND Version: 9.11.36 Location: 53/tcp CPE: cpe:/a:isc:bind:9.11.36 Concluded from version/product identification result: 9.11.36-RedHat-9.11.36-16.el8_10.6 **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** ISC BIND Detection (DNS) (NVT: 1.3.6.1.4.1.25623.1.0.10028) **Version used:** 2023-08-01T13:29:10+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	443/tcp	This routine identifies services supporting the following extensions to TLS: - Application-Layer Protocol Negotiation (ALPN) - Next Protocol Negotiation (NPN). Based on the availability of this extensions the supported Network Protocols by this service are gathered and reported.	low	NOCVE	0.0
	Vulnerability Detection Result: The remote service advertises support for the following Network Protocol(s) via the ALPN extension: SSL/TLS Protocol:Network Protocol TLSv1.2:HTTP/1.1 **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** SSL/TLS: NPN / ALPN Extension and Protocol Support Detection (NVT: 1.3.6.1.4.1.25623.1.0.108099) **Version used:** 2023-04-18T10:19:20+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://tools.ietf.org/html/rfc7301, URL:https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04		
209.59.154.193 host.bayclub.in	25/tcp	This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).	low	NOCVE	0.0
	Vulnerability Detection Result: Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.105018) **Version used:** 2021-12-09T13:40:52+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	995/tcp	This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).	low	NOCVE	0.0
	Vulnerability Detection Result: Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.105018) **Version used:** 2021-12-09T13:40:52+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	993/tcp	This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).	low	NOCVE	0.0
	Vulnerability Detection Result: Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.105018) **Version used:** 2021-12-09T13:40:52+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	587/tcp	This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).	low	NOCVE	0.0
	Vulnerability Detection Result: Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.105018) **Version used:** 2021-12-09T13:40:52+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	465/tcp	This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).	low	NOCVE	0.0
	Vulnerability Detection Result: Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.105018) **Version used:** 2021-12-09T13:40:52+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	443/tcp	This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).	low	NOCVE	0.0
	Vulnerability Detection Result: Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.105018) **Version used:** 2021-12-09T13:40:52+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	143/tcp	This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).	low	NOCVE	0.0
	Vulnerability Detection Result: Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.105018) **Version used:** 2021-12-09T13:40:52+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	110/tcp	This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).	low	NOCVE	0.0
	Vulnerability Detection Result: Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.105018) **Version used:** 2021-12-09T13:40:52+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	21/tcp	This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).	low	NOCVE	0.0
	Vulnerability Detection Result: *2 (Click here to access the vulnerability details) **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.105018) **Version used:** 2021-12-09T13:40:52+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	587/tcp	This script collects and reports the details of all SSL/TLS certificates. This data will be used by other tests to verify server certificates.	low	NOCVE	0.0
	Vulnerability Detection Result: The following certificate details of the remote service were collected. Certificate details: subject ...: CN=host.bayclub.in subject alternative names (SAN): host.bayclub.in issued by .: CN=R12,O=Let's Encrypt,C=US serial ....: 056C01720238D39BA470335A92AAB41BE703 valid from : 2026-02-11 04:53:24 UTC valid until: 2026-05-12 04:53:23 UTC fingerprint (SHA-1): AF2DA2B75CEE7EB8D27288E0C6260C648B54F867 fingerprint (SHA-256): 7CC24FC8E845D1DF663DB59780735C56057F431F33C2B2DA8EFFE4E4B07A7080 **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Collect and Report Certificate Details (NVT: 1.3.6.1.4.1.25623.1.0.103692) **Version used:** 2021-04-16T08:08:22+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	443/tcp	This script collects and reports the details of all SSL/TLS certificates. This data will be used by other tests to verify server certificates.	low	NOCVE	0.0
	Vulnerability Detection Result: The following certificate details of the remote service were collected. Certificate details: subject ...: CN=host.bayclub.in subject alternative names (SAN): host.bayclub.in issued by .: CN=R12,O=Let's Encrypt,C=US serial ....: 056C01720238D39BA470335A92AAB41BE703 valid from : 2026-02-11 04:53:24 UTC valid until: 2026-05-12 04:53:23 UTC fingerprint (SHA-1): AF2DA2B75CEE7EB8D27288E0C6260C648B54F867 fingerprint (SHA-256): 7CC24FC8E845D1DF663DB59780735C56057F431F33C2B2DA8EFFE4E4B07A7080 **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Collect and Report Certificate Details (NVT: 1.3.6.1.4.1.25623.1.0.103692) **Version used:** 2021-04-16T08:08:22+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	465/tcp	This script collects and reports the details of all SSL/TLS certificates. This data will be used by other tests to verify server certificates.	low	NOCVE	0.0
	Vulnerability Detection Result: The following certificate details of the remote service were collected. Certificate details: subject ...: CN=host.bayclub.in subject alternative names (SAN): host.bayclub.in issued by .: CN=R12,O=Let's Encrypt,C=US serial ....: 056C01720238D39BA470335A92AAB41BE703 valid from : 2026-02-11 04:53:24 UTC valid until: 2026-05-12 04:53:23 UTC fingerprint (SHA-1): AF2DA2B75CEE7EB8D27288E0C6260C648B54F867 fingerprint (SHA-256): 7CC24FC8E845D1DF663DB59780735C56057F431F33C2B2DA8EFFE4E4B07A7080 **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Collect and Report Certificate Details (NVT: 1.3.6.1.4.1.25623.1.0.103692) **Version used:** 2021-04-16T08:08:22+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	110/tcp	This script collects and reports the details of all SSL/TLS certificates. This data will be used by other tests to verify server certificates.	low	NOCVE	0.0
	Vulnerability Detection Result: The following certificate details of the remote service were collected. Certificate details: subject ...: CN=host.bayclub.in subject alternative names (SAN): host.bayclub.in issued by .: CN=R12,O=Let's Encrypt,C=US serial ....: 056C01720238D39BA470335A92AAB41BE703 valid from : 2026-02-11 04:53:24 UTC valid until: 2026-05-12 04:53:23 UTC fingerprint (SHA-1): AF2DA2B75CEE7EB8D27288E0C6260C648B54F867 fingerprint (SHA-256): 7CC24FC8E845D1DF663DB59780735C56057F431F33C2B2DA8EFFE4E4B07A7080 **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Collect and Report Certificate Details (NVT: 1.3.6.1.4.1.25623.1.0.103692) **Version used:** 2021-04-16T08:08:22+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	993/tcp	This script collects and reports the details of all SSL/TLS certificates. This data will be used by other tests to verify server certificates.	low	NOCVE	0.0
	Vulnerability Detection Result: The following certificate details of the remote service were collected. Certificate details: subject ...: CN=host.bayclub.in subject alternative names (SAN): host.bayclub.in issued by .: CN=R12,O=Let's Encrypt,C=US serial ....: 056C01720238D39BA470335A92AAB41BE703 valid from : 2026-02-11 04:53:24 UTC valid until: 2026-05-12 04:53:23 UTC fingerprint (SHA-1): AF2DA2B75CEE7EB8D27288E0C6260C648B54F867 fingerprint (SHA-256): 7CC24FC8E845D1DF663DB59780735C56057F431F33C2B2DA8EFFE4E4B07A7080 **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Collect and Report Certificate Details (NVT: 1.3.6.1.4.1.25623.1.0.103692) **Version used:** 2021-04-16T08:08:22+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	443/tcp	The remote server's SSL/TLS certificate will soon expire.	low	NOCVE	0.0
	Vulnerability Detection Result: The certificate of the remote service will expire within the next 60 days on 2026-04-15 23:55:37. Certificate details: subject ...: CN=applicationuat.bayclub.in subject alternative names (SAN): applicationuat.bayclub.in issued by .: CN=R13,O=Let's Encrypt,C=US serial ....: 064B5174DABCE990E135A1624868D983B761 valid from : 2026-01-15 23:55:38 UTC valid until: 2026-04-15 23:55:37 UTC fingerprint (SHA-1): 5994DDF03ECEE41D03C1516F8A9AEE94B689F1C2 fingerprint (SHA-256): A6644FB30F8312BE1145B41209CFAF68AF8019EE229B94CCA501C80581C59F60 **Solution** **Solution type:** MitigationPrepare to replace the SSL/TLS certificate by a new one. **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerability. **Vulnerability Insight:** This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any will expire during then next 28 days for the Let's Encrypt Certificate Authority or 60 days for any other Certificate Authority.		**Details:** SSL/TLS: Certificate Will Soon Expire (NVT: 1.3.6.1.4.1.25623.1.0.103957) **Version used:** 2021-11-22T15:32:39+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://letsencrypt.org/2015/11/09/why-90-days.html		
209.59.154.193 host.bayclub.in	21/tcp	This script collects and reports the details of all SSL/TLS certificates. This data will be used by other tests to verify server certificates.	low	NOCVE	0.0
	Vulnerability Detection Result: The following certificate details of the remote service were collected. Certificate details: subject ...: CN=host.bayclub.in subject alternative names (SAN): host.bayclub.in issued by .: CN=R12,O=Let's Encrypt,C=US serial ....: 056C01720238D39BA470335A92AAB41BE703 valid from : 2026-02-11 04:53:24 UTC valid until: 2026-05-12 04:53:23 UTC fingerprint (SHA-1): AF2DA2B75CEE7EB8D27288E0C6260C648B54F867 fingerprint (SHA-256): 7CC24FC8E845D1DF663DB59780735C56057F431F33C2B2DA8EFFE4E4B07A7080 **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Collect and Report Certificate Details (NVT: 1.3.6.1.4.1.25623.1.0.103692) **Version used:** 2021-04-16T08:08:22+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	995/tcp	This routine reports all SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0
	Vulnerability Detection Result: 'Strong' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 'Medium' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 No 'Weak' cipher suites accepted by this service via the TLSv1.2 protocol. No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol. No 'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol. **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** Notes: - As the VT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this VT instead. - SSLv2 ciphers are not getting reported as the protocol itself is deprecated, needs to be considered as weak and is reported separately as deprecated.		**Details:** SSL/TLS: Report Supported Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.802067) **Version used:** 2022-08-25T10:12:37+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF	
209.59.154.193 host.bayclub.in	995/tcp	This script collects and reports the details of all SSL/TLS certificates. This data will be used by other tests to verify server certificates.	low	NOCVE	0.0
	Vulnerability Detection Result: The following certificate details of the remote service were collected. Certificate details: subject ...: CN=host.bayclub.in subject alternative names (SAN): host.bayclub.in issued by .: CN=R12,O=Let's Encrypt,C=US serial ....: 056C01720238D39BA470335A92AAB41BE703 valid from : 2026-02-11 04:53:24 UTC valid until: 2026-05-12 04:53:23 UTC fingerprint (SHA-1): AF2DA2B75CEE7EB8D27288E0C6260C648B54F867 fingerprint (SHA-256): 7CC24FC8E845D1DF663DB59780735C56057F431F33C2B2DA8EFFE4E4B07A7080 **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Collect and Report Certificate Details (NVT: 1.3.6.1.4.1.25623.1.0.103692) **Version used:** 2021-04-16T08:08:22+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF	

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	143/tcp	This script collects and reports the details of all SSL/TLS certificates. This data will be used by other tests to verify server certificates.	low	NOCVE	0.0
	Vulnerability Detection Result: The following certificate details of the remote service were collected. Certificate details: subject ...: CN=host.bayclub.in subject alternative names (SAN): host.bayclub.in issued by .: CN=R12,O=Let's Encrypt,C=US serial ....: 056C01720238D39BA470335A92AAB41BE703 valid from : 2026-02-11 04:53:24 UTC valid until: 2026-05-12 04:53:23 UTC fingerprint (SHA-1): AF2DA2B75CEE7EB8D27288E0C6260C648B54F867 fingerprint (SHA-256): 7CC24FC8E845D1DF663DB59780735C56057F431F33C2B2DA8EFFE4E4B07A7080 **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Collect and Report Certificate Details (NVT: 1.3.6.1.4.1.25623.1.0.103692) **Version used:** 2021-04-16T08:08:22+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF	
209.59.154.193 host.bayclub.in	993/tcp	This routine reports all SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0
	Vulnerability Detection Result: 'Strong' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 'Medium' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 No 'Weak' cipher suites accepted by this service via the TLSv1.2 protocol. No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol. No 'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol. **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** Notes: - As the VT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this VT instead. - SSLv2 ciphers are not getting reported as the protocol itself is deprecated, needs to be considered as weak and is reported separately as deprecated.		**Details:** SSL/TLS: Report Supported Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.802067) **Version used:** 2022-08-25T10:12:37+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF	

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	587/tcp	This routine reports all SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0
	Vulnerability Detection Result: 'Strong' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 'Medium' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 No 'Weak' cipher suites accepted by this service via the TLSv1.2 protocol. No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol. No 'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol. **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** Notes: - As the VT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this VT instead. - SSLv2 ciphers are not getting reported as the protocol itself is deprecated, needs to be considered as weak and is reported separately as deprecated.				**Details:** SSL/TLS: Report Supported Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.802067) **Version used:** 2022-08-25T10:12:37+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF
209.59.154.193 host.bayclub.in	465/tcp	This routine reports all SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0
	Vulnerability Detection Result: 'Strong' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 'Medium' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 No 'Weak' cipher suites accepted by this service via the TLSv1.2 protocol. No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol. No 'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol. **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** Notes: - As the VT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this VT instead. - SSLv2 ciphers are not getting reported as the protocol itself is deprecated, needs to be considered as weak and is reported separately as deprecated.				**Details:** SSL/TLS: Report Supported Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.802067) **Version used:** 2022-08-25T10:12:37+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	443/tcp	This routine reports all SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0
	Vulnerability Detection Result: 'Strong' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 'Medium' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 No 'Weak' cipher suites accepted by this service via the TLSv1.2 protocol. No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol. No 'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol. **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** Notes: - As the VT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this VT instead. - SSLv2 ciphers are not getting reported as the protocol itself is deprecated, needs to be considered as weak and is reported separately as deprecated.		**Details:** SSL/TLS: Report Supported Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.802067) **Version used:** 2022-08-25T10:12:37+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF	
209.59.154.193 host.bayclub.in	143/tcp	This routine reports all SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0
	Vulnerability Detection Result: 'Strong' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 'Medium' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 No 'Weak' cipher suites accepted by this service via the TLSv1.2 protocol. No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol. No 'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol. **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** Notes: - As the VT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this VT instead. - SSLv2 ciphers are not getting reported as the protocol itself is deprecated, needs to be considered as weak and is reported separately as deprecated.		**Details:** SSL/TLS: Report Supported Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.802067) **Version used:** 2022-08-25T10:12:37+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF	

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	110/tcp	This routine reports all SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0
	Vulnerability Detection Result: 'Strong' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 'Medium' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 No 'Weak' cipher suites accepted by this service via the TLSv1.2 protocol. No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol. No 'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol. **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** Notes: - As the VT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this VT instead. - SSLv2 ciphers are not getting reported as the protocol itself is deprecated, needs to be considered as weak and is reported separately as deprecated.				**Details:** SSL/TLS: Report Supported Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.802067) **Version used:** 2022-08-25T10:12:37+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF	
209.59.154.193 host.bayclub.in	25/tcp	This routine reports all SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0
	Vulnerability Detection Result: 'Strong' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 'Medium' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 No 'Weak' cipher suites accepted by this service via the TLSv1.2 protocol. No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol. No 'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol. **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** Notes: - As the VT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this VT instead. - SSLv2 ciphers are not getting reported as the protocol itself is deprecated, needs to be considered as weak and is reported separately as deprecated.				**Details:** SSL/TLS: Report Supported Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.802067) **Version used:** 2022-08-25T10:12:37+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF	

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	21/tcp	This routine reports all SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0
	Vulnerability Detection Result: *3 (Click here to access the vulnerability details) **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** Notes: - As the VT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this VT instead. - SSLv2 ciphers are not getting reported as the protocol itself is deprecated, needs to be considered as weak and is reported separately as deprecated.		**Details:** SSL/TLS: Report Supported Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.802067) **Version used:** 2022-08-25T10:12:37+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	general/tcp	It was possible to discover an additional hostname of this server from its certificate Common or Subject Alt Name.	low	NOCVE	0.0
	Vulnerability Detection Result: The following additional and resolvable hostnames were detected: applicationuat.bayclub.in host.bayclub.in **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Hostname discovery from server certificate (NVT: 1.3.6.1.4.1.25623.1.0.111010) **Version used:** 2021-11-22T15:32:39+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	80/tcp	HTTP based detection of the Apache HTTP Server.	low	NOCVE	0.0
	Vulnerability Detection Result: Detected Apache HTTP/Web Server Version: unknown Location: 80/tcp CPE: cpe:/a:apache:http_server **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** Apache HTTP Server Detection (HTTP) (NVT: 1.3.6.1.4.1.25623.1.0.900498) **Version used:** 2021-09-01T14:04:04+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	443/tcp	This script detects and reports the HTTP Server's banner which might provide the type and version of it.	low	NOCVE	0.0
	Vulnerability Detection Result: The remote HTTP Server banner is: Server: Apache **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** HTTP Server type and version (NVT: 1.3.6.1.4.1.25623.1.0.10107) **Version used:** 2023-08-01T13:29:10+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	443/tcp	HTTP based detection of the Apache HTTP Server.	low	NOCVE	0.0
	Vulnerability Detection Result: Detected Apache HTTP/Web Server Version: unknown Location: 443/tcp CPE: cpe:/a:apache:http_server **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** Apache HTTP Server Detection (HTTP) (NVT: 1.3.6.1.4.1.25623.1.0.900498) **Version used:** 2021-09-01T14:04:04+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	80/tcp	This script detects and reports the HTTP Server's banner which might provide the type and version of it.	low	NOCVE	0.0
	Vulnerability Detection Result: The remote HTTP Server banner is: Server: Apache **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** HTTP Server type and version (NVT: 1.3.6.1.4.1.25623.1.0.10107) **Version used:** 2023-08-01T13:29:10+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	443/tcp	Web Servers can use a file called /robot(s).txt to ask search engines to ignore certain files and directories. By nature this file can not be used to protect private files from public read access.	low	NOCVE	0.0
	Vulnerability Detection Result: The file 'https://209.59.154.193/robots.txt' contains the following: User-agent: * Disallow: **Solution** **Solution type:** MitigationReview the content of the /robot(s).txt file and consider removing the files from the server or protect them in other ways in case you actually intended non-public availability. **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so. **Vulnerability Insight:** Any serious web search engine will honor the /robot(s).txt file and not scan the files and directories listed there. Any entries listed in this file are not even hidden anymore.		**Details:** robot(s).txt exists on the Web Server (NVT: 1.3.6.1.4.1.25623.1.0.10302) **Version used:** 2023-08-01T13:29:10+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://www.robotstxt.org/, URL:https://www.robotstxt.org/norobots-rfc.txt		
209.59.154.193 host.bayclub.in	443/tcp	HTTP based detection of Mailman.	low	NOCVE	0.0
	Vulnerability Detection Result: Detected Mailman Version: 2.2.0 Location: /mailman CPE: cpe:/a:gnu:mailman:2.2.0 Concluded from version/product identification result: alt="Delivered by Mailman" border=0> version 2.2.0 Concluded from version/product identification location: https://209.59.154.193/mailman/listinfo **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** Mailman Detection (HTTP) (NVT: 1.3.6.1.4.1.25623.1.0.16338) **Version used:** 2023-07-12T05:05:05+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:http://www.list.org/		
209.59.154.193 host.bayclub.in	80/tcp	HTTP based detection of Mailman.	low	NOCVE	0.0
	Vulnerability Detection Result: Detected Mailman Version: 2.2.0 Location: /mailman CPE: cpe:/a:gnu:mailman:2.2.0 Concluded from version/product identification result: alt="Delivered by Mailman" border=0> version 2.2.0 Concluded from version/product identification location: http://209.59.154.193/mailman/listinfo **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** Mailman Detection (HTTP) (NVT: 1.3.6.1.4.1.25623.1.0.16338) **Version used:** 2023-07-12T05:05:05+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:http://www.list.org/		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	general/tcp	This script consolidates the OS information detected by several VTs and tries to find the best matching OS. Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional information which might help to improve the OS detection. If any of this information is wrong or could be improved please consider to report these to the referenced community forum.	low	NOCVE	0.0
	Vulnerability Detection Result: *4 (Click here to access the vulnerability details) **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** OS Detection Consolidation and Reporting (NVT: 1.3.6.1.4.1.25623.1.0.105937) **Version used:** 2023-10-06T16:09:51+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://forum.greenbone.net/c/vulnerability-tests/7		
209.59.154.193 host.bayclub.in	general/icmp	The remote host responded to an ICMP timestamp request.	low	CVE-1999-0524	0.0
	Impact: This information could theoretically be used to exploit weak time-based random number generators in other services. **Solution** **Solution type:** MitigationVarious mitigations are possible: - Disable the support for ICMP timestamp on the remote host completely - Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks) **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so. **Vulnerability Insight:** The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.		**Vulnerability Detection Method:** Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received. **Details:** ICMP Timestamp Reply Information Disclosure (NVT: 1.3.6.1.4.1.25623.1.0.103190) **Version used:** 2023-05-11T09:09:33+0000 **References:** **CVSS v2 Vector:** (AV:L/AC:L/Au:N/C:P/I:N/A:N) **CVE:** CVE-1999-0524 **BID:** NOBID **CERT:** **XREF:** URL:https://datatracker.ietf.org/doc/html/rfc792, URL:https://datatracker.ietf.org/doc/html/rfc2780		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	443/tcp	The remote web server is not enforcing HPKP. Note: Most major browsers have dropped / deprecated support for this header in 2020.	low	NOCVE	0.0
	Vulnerability Detection Result: The remote web server is not enforcing HPKP. HTTP-Banner: HTTP/1.1 302 Found Date: ***replaced*** Server: Apache Cache-Control: no-cache, private Set-Cookie: ***replaced***%3D; expires=***replaced*** Set-Cookie: ***replaced***_bay_club_session=eyJpdiI6IlFVUGQ2aGk3UWdMNGpZTW9YT245bGc9PSIsInZhbHVlIjoiYXphVXFRdDd6cEQ3N0h0a2crWXBQYTl0TmtFbFgvbHlsUERwQ3NibDdYUGl5UWdmLy83d1J0WU9mQ2lEY2JIa1pNNTBsbXRDV1g4OUlVbHhveDlMZzE5VkhKUzJXTVMvdGVJUkplUGxJeXViVEgzM3VSQjBvZEVZaDFBMTZxMlQiLCJtYWMiOiJlOTU5ZWI5YWM3MjQyYjUxN2Y0ODdjMmNkZDNlOGUwM2Q5MmZkYTdiYjQ5ZjY3NjdjYThhOGY2MGRjMjI4ZjRiIiwidGFnIjoiIn0%3D; expires=***replaced*** Location: https://209.59.154.193/admin/login Cache-Control: max-age=600 Expires: ***replaced*** Vary: Accept-Encoding,User-Agent Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 **Solution** **Solution type:** WorkaroundEnable HPKP or add / configure the required directives correctly following the guides linked in the references. Note: Some web servers are not sending headers on specific status codes by default. Please review your web server or application configuration to always send these headers on every response independently from the status code. - Apache: Use 'Header always set' instead of 'Header set'. - nginx: Append the 'always' keyword to each 'add_header' directive. For different applications or web severs please refer to the related documentation for a similar configuration possibility. **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** SSL/TLS: HTTP Public Key Pinning (HPKP) Missing (NVT: 1.3.6.1.4.1.25623.1.0.108247) **Version used:** 2023-07-25T05:05:58+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://owasp.org/www-project-secure-headers/, URL:https://owasp.org/www-project-secure-headers/#public-key-pinning-extension-for-http-hpkp, URL:https://tools.ietf.org/html/rfc7469, URL:https://securityheaders.io/, URL:https://httpd.apache.org/docs/current/mod/mod_headers.html#header		
209.59.154.193 host.bayclub.in	443/tcp	All known security headers are being checked on the remote web server. On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.	low	NOCVE	0.0
	Vulnerability Detection Result: *5 (Click here to access the vulnerability details) **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** HTTP Security Headers Detection (NVT: 1.3.6.1.4.1.25623.1.0.112081) **Version used:** 2021-07-14T06:19:43+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://owasp.org/www-project-secure-headers/, URL:https://owasp.org/www-project-secure-headers/#div-headers, URL:https://securityheaders.com/		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	80/tcp	All known security headers are being checked on the remote web server. On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.	low	NOCVE	0.0
	Vulnerability Detection Result: Missing Headers | More Information ---------- Content-Security-Policy | https://owasp.org/www-project-secure-headers/#content-security-policy Document-Policy | https://w3c.github.io/webappsec-feature-policy/document-policy#document-policy-http-header Feature-Policy | https://owasp.org/www-project-secure-headers/#feature-policy, Note: The Feature Policy header has been renamed to Permissions Policy Permissions-Policy | https://w3c.github.io/webappsec-feature-policy/#permissions-policy-http-header-field Referrer-Policy | https://owasp.org/www-project-secure-headers/#referrer-policy X-Content-Type-Options | https://owasp.org/www-project-secure-headers/#x-content-type-options X-Frame-Options | https://owasp.org/www-project-secure-headers/#x-frame-options X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers/#x-permitted-cross-domain-policies X-XSS-Protection | https://owasp.org/www-project-secure-headers/#x-xss-protection, Note: Most major browsers have dropped / deprecated support for this header in 2020. **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** HTTP Security Headers Detection (NVT: 1.3.6.1.4.1.25623.1.0.112081) **Version used:** 2021-07-14T06:19:43+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://owasp.org/www-project-secure-headers/, URL:https://owasp.org/www-project-secure-headers/#div-headers, URL:https://securityheaders.com/		
209.59.154.193 host.bayclub.in	443/tcp	The script consolidates various information for CGI scanning. This information is based on the following scripts / settings: - HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034) - No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386) - Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662) - Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032) - The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use - The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use If you think any of this information is wrong please report it to the referenced community portal.	low	NOCVE	0.0
	Vulnerability Detection Result: *6 (Click here to access the vulnerability details) **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** CGI Scanning Consolidation (NVT: 1.3.6.1.4.1.25623.1.0.111038) **Version used:** 2022-03-24T09:16:49+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://community.greenbone.net/c/vulnerability-tests		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	80/tcp	The script consolidates various information for CGI scanning. This information is based on the following scripts / settings: - HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034) - No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386) - Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662) - Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032) - The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use - The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use If you think any of this information is wrong please report it to the referenced community portal.	low	NOCVE	0.0
	Vulnerability Detection Result: *7 (Click here to access the vulnerability details) **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** CGI Scanning Consolidation (NVT: 1.3.6.1.4.1.25623.1.0.111038) **Version used:** 2022-03-24T09:16:49+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://community.greenbone.net/c/vulnerability-tests		
209.59.154.193 host.bayclub.in	443/tcp	This script tries to detect / enumerate different HTTP server banner (e.g. from a frontend, backend or proxy server) by sending various different HTTP requests (valid and invalid ones).	low	NOCVE	0.0
	Vulnerability Detection Result: It was possible to enumerate the following HTTP server banner(s): Server banner | Enumeration technique --- Server: Apache | Valid HTTP 0.9 GET request to '/index.html' **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** HTTP Server Banner Enumeration (NVT: 1.3.6.1.4.1.25623.1.0.108708) **Version used:** 2022-06-28T10:11:01+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	80/tcp	This script tries to detect / enumerate different HTTP server banner (e.g. from a frontend, backend or proxy server) by sending various different HTTP requests (valid and invalid ones).	low	NOCVE	0.0
	Vulnerability Detection Result: It was possible to enumerate the following HTTP server banner(s): Server banner | Enumeration technique --- Server: Apache | Valid HTTP 0.9 GET request to '/index.html' **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** HTTP Server Banner Enumeration (NVT: 1.3.6.1.4.1.25623.1.0.108708) **Version used:** 2022-06-28T10:11:01+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	443/tcp	The remote web server is not enforcing HSTS.	low	NOCVE	0.0
	Vulnerability Detection Result: The remote web server is not enforcing HSTS. HTTP-Banner: HTTP/1.1 302 Found Date: ***replaced*** Server: Apache Cache-Control: no-cache, private Set-Cookie: ***replaced***%3D; expires=***replaced*** Set-Cookie: ***replaced***_bay_club_session=eyJpdiI6IlFVUGQ2aGk3UWdMNGpZTW9YT245bGc9PSIsInZhbHVlIjoiYXphVXFRdDd6cEQ3N0h0a2crWXBQYTl0TmtFbFgvbHlsUERwQ3NibDdYUGl5UWdmLy83d1J0WU9mQ2lEY2JIa1pNNTBsbXRDV1g4OUlVbHhveDlMZzE5VkhKUzJXTVMvdGVJUkpIUGxJeXViVEgzM3VSQjBvZEVZaDFBMTZxMlQiLCJtYWMiOiJlOTU5ZWI5YWM3MjQyYjUxN2Y0ODdjMmNkZDNlOGUwM2Q5MmZkYTdiYjQ5ZjY3NjdjYThhOGY2MGRjMjI4ZjRiIiwidGFnIjoiIn0%3D; expires=***replaced*** Location: https://209.59.154.193/admin/login Cache-Control: max-age=600 Expires: ***replaced*** Vary: Accept-Encoding,User-Agent Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 **Solution** **Solution type:** WorkaroundEnable HSTS or add / configure the required directives correctly following the guides linked in the references. Note: Some web servers are not sending headers on specific status codes by default. Please review your web server or application configuration to always send these headers on every response independently from the status code. - Apache: Use 'Header always set' instead of 'Header set'. - nginx: Append the 'always' keyword to each 'add_header' directive. For different applications or web severs please refer to the related documentation for a similar configuration possibility. **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** SSL/TLS: HTTP Strict Transport Security (HSTS) Missing (NVT: 1.3.6.1.4.1.25623.1.0.105879) **Version used:** 2023-07-20T05:05:17+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://owasp.org/www-project-secure-headers/, URL:https://owasp.org/www-project-cheat-sheets/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html, URL:https://owasp.org/www-project-secure-headers/#http-strict-transport-security-hsts, URL:https://tools.ietf.org/html/rfc6797, URL:https://securityheaders.io/		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	443/tcp	This routine reports all Medium SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0
	Vulnerability Detection Result: 'Medium' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** Any cipher suite considered to be secure for only the next 10 years is considered as medium.		**Details:** SSL/TLS: Report Medium Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.902816) **Version used:** 2021-12-01T13:10:37+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	995/tcp	This routine reports all Medium SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0
	Vulnerability Detection Result: 'Medium' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** Any cipher suite considered to be secure for only the next 10 years is considered as medium.		**Details:** SSL/TLS: Report Medium Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.902816) **Version used:** 2021-12-01T13:10:37+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	993/tcp	This routine reports all Medium SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0
	Vulnerability Detection Result: 'Medium' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** Any cipher suite considered to be secure for only the next 10 years is considered as medium.		**Details:** SSL/TLS: Report Medium Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.902816) **Version used:** 2021-12-01T13:10:37+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	587/tcp	This routine reports all Medium SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0
	Vulnerability Detection Result: 'Medium' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** Any cipher suite considered to be secure for only the next 10 years is considered as medium.		**Details:** SSL/TLS: Report Medium Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.902816) **Version used:** 2021-12-01T13:10:37+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	143/tcp	This routine reports all Medium SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0
	Vulnerability Detection Result: 'Medium' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** Any cipher suite considered to be secure for only the next 10 years is considered as medium.		**Details:** SSL/TLS: Report Medium Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.902816) **Version used:** 2021-12-01T13:10:37+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	465/tcp	This routine reports all Medium SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0
	Vulnerability Detection Result: 'Medium' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** Any cipher suite considered to be secure for only the next 10 years is considered as medium.		**Details:** SSL/TLS: Report Medium Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.902816) **Version used:** 2021-12-01T13:10:37+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	21/tcp	This routine reports all Medium SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0
	Vulnerability Detection Result: *8 (Click here to access the vulnerability details) **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** Any cipher suite considered to be secure for only the next 10 years is considered as medium.		**Details:** SSL/TLS: Report Medium Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.902816) **Version used:** 2021-12-01T13:10:37+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	25/tcp	This routine reports all Medium SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0
	Vulnerability Detection Result: 'Medium' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** Any cipher suite considered to be secure for only the next 10 years is considered as medium.		**Details:** SSL/TLS: Report Medium Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.902816) **Version used:** 2021-12-01T13:10:37+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	110/tcp	This routine reports all Medium SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0
	Vulnerability Detection Result: 'Medium' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application. **Vulnerability Insight:** Any cipher suite considered to be secure for only the next 10 years is considered as medium.		**Details:** SSL/TLS: Report Medium Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.902816) **Version used:** 2021-12-01T13:10:37+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	general/tcp	Collect information about the network route and network distance between the scanner host and the target host.	low	NOCVE	0.0
	Vulnerability Detection Result: Here is the route from 209.59.188.91 to 209.59.154.193: 209.59.188.91 69.167.128.76 69.167.128.145 209.59.154.193 **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so. **Vulnerability Insight:** For internal networks, the distances are usually small, often less than 4 hosts between scanner and target. For public targets the distance is greater and might be 10 hosts or more.		**Vulnerability Detection Method:** A combination of the protocols ICMP and TCP is used to determine the route. This method is applicable for IPv4 only and it is also known as 'traceroute'. **Details:** Traceroute (NVT: 1.3.6.1.4.1.25623.1.0.51662) **Version used:** 2022-10-17T11:13:19+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	21/tcp	The script is grabbing the banner of a FTP server and sends a 'HELP' command to identify a Pure-FTPd FTP Server from the reply.	low	NOCVE	0.0
	Vulnerability Detection Result: Detected Pure-FTPd Version: unknown Location: 21/tcp CPE: cpe:/a:pureftpd:pure-ftpd Concluded from version/product identification result: 220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220-You are user number 2 of 50 allowed. 220-Local time is now 18:58. Server port: 21. 220-This is a private system - No anonymous login 220-IPv6 connections are also welcome on this server. 220 You will be disconnected after 15 minutes of inactivity. **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** Pure-FTPd FTP Server Detection (NVT: 1.3.6.1.4.1.25623.1.0.111110) **Version used:** 2023-07-26T05:05:09+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://www.pureftpd.org		
209.59.154.193 host.bayclub.in	25/tcp	This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0
	Vulnerability Detection Result: 'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Report Non Weak Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.103441) **Version used:** 2021-12-01T09:24:41+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	995/tcp	This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0
	Vulnerability Detection Result: 'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Report Non Weak Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.103441) **Version used:** 2021-12-01T09:24:41+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	993/tcp	This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0
	Vulnerability Detection Result: 'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Report Non Weak Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.103441) **Version used:** 2021-12-01T09:24:41+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	587/tcp	This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0
	Vulnerability Detection Result: 'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Report Non Weak Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.103441) **Version used:** 2021-12-01T09:24:41+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	465/tcp	This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0
	Vulnerability Detection Result: 'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Report Non Weak Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.103441) **Version used:** 2021-12-01T09:24:41+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	443/tcp	This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0
	Vulnerability Detection Result: 'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Report Non Weak Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.103441) **Version used:** 2021-12-01T09:24:41+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	143/tcp	This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0
	Vulnerability Detection Result: 'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Report Non Weak Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.103441) **Version used:** 2021-12-01T09:24:41+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		

Component	Detected Open Ports, Services/ Protocols	Vulnerability	Severity Level	CVE Number	CVSS Score
209.59.154.193 host.bayclub.in	110/tcp	This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0
	Vulnerability Detection Result: 'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Report Non Weak Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.103441) **Version used:** 2021-12-01T09:24:41+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	21/tcp	This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.	low	NOCVE	0.0
	Vulnerability Detection Result: *9 (Click here to access the vulnerability details) **Detection Reliability:** Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.		**Details:** SSL/TLS: Report Non Weak Cipher Suites (NVT: 1.3.6.1.4.1.25623.1.0.103441) **Version used:** 2021-12-01T09:24:41+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** NOXREF		
209.59.154.193 host.bayclub.in	general/CPE-T	This routine uses information collected by other routines about CPE identities of operating systems, services and applications detected during the scan. Note: Some CPEs for specific products might show up twice or more in the output. Background: After a product got renamed or a specific vendor was acquired by another one it might happen that a product gets a new CPE within the NVD CPE Dictionary but older entries are kept with the older CPE.	low	NOCVE	0.0
	Vulnerability Detection Result: 209.59.154.193|cpe:/a:apache:http_server 209.59.154.193|cpe:/a:dovecot:dovecot 209.59.154.193|cpe:/a:exim:exim:4.99.1 209.59.154.193|cpe:/a:gnu:mailman:2.2.0 209.59.154.193|cpe:/a:isc:bind:9.11.36 209.59.154.193|cpe:/a:openbsd:openssh:8.0 209.59.154.193|cpe:/a:pureftpd:pure-ftpd 209.59.154.193|cpe:/o:redhat:linux:8 **Detection Reliability:** Remote banner check of applications that offer patch level in version. Many proprietary products do so.		**Details:** CPE Inventory (NVT: 1.3.6.1.4.1.25623.1.0.810002) **Version used:** 2022-07-27T10:11:28+0000 **References:** **CVSS v2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:N) **CVE:** NOCVE **BID:** NOBID **CERT:** **XREF:** URL:https://nvd.nist.gov/products/cpe		

*1 Vulnerability Detection Result for Host 209.59.154.193 (host.bayclub.in) - general/tcp

Detected Dovecot
Version: unknown
Location: 143/tcp
CPE: cpe:/a:dovecot:dovecot
Concluded from version/product identification result:
* OK [CAPABILITY IMAP4rev1 LOGIN-REFERRALS ID ENABLE IDLE SASL-IR LITERAL+
STARTTLS LOGINDISABLED] Dovecot ready.
* ID ("name" "Dovecot")
Detection Method: IMAP Banner
Detected Dovecot
Version: unknown
Location: 993/tcp
CPE: cpe:/a:dovecot:dovecot
Concluded from version/product identification result:
* OK [CAPABILITY IMAP4rev1 LOGIN-REFERRALS ID ENABLE IDLE SASL-IR LITERAL+
AUTH=PLAIN AUTH=LOGIN] Dovecot ready.
* ID ("name" "Dovecot")
Detection Method: IMAP Banner
Detected Dovecot
Version: unknown
Location: 110/tcp
CPE: cpe:/a:dovecot:dovecot
Concluded from version/product identification result:
+OK Dovecot ready.
Detection Method: POP3 Banner
Detected Dovecot
Version: unknown
Location: 995/tcp
CPE: cpe:/a:dovecot:dovecot
Concluded from version/product identification result:
+OK Dovecot ready.
Detection Method: POP3 Banner

*2 Vulnerability Detection Result for Host 209.59.154.193 (host.bayclub.in) - 21/tcp

Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the
TLSv1.2 protocol:
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CCM
TLS_DHE_RSA_WITH_AES_128_CCM_8
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CCM
TLS_DHE_RSA_WITH_AES_256_CCM_8
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256
TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256

*3 Vulnerability Detection Result for Host 209.59.154.193 (host.bayclub.in) - 21/tcp

'Strong' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CCM
TLS_DHE_RSA_WITH_AES_128_CCM_8
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CCM
TLS_DHE_RSA_WITH_AES_256_CCM_8
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256
TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_CCM
TLS_RSA_WITH_AES_128_CCM_8
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_CCM
TLS_RSA_WITH_AES_256_CCM_8
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_ARIA_128_GCM_SHA256
TLS_RSA_WITH_ARIA_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
No 'Weak' cipher suites accepted by this service via the TLSv1.2 protocol.
No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol.

*4 Vulnerability Detection Result for Host 209.59.154.193 (host.bayclub.in) - general/tcp

Best matching OS:
OS: Redhat Linux 8
Version: 8
CPE: cpe:/o:redhat:linux:8
Found by NVT: 1.3.6.1.4.1.25623.1.0.108014 (DNS Server OS Identification)
Concluded from DNS server banner on port 53/tcp: 9.11.36-RedHat-9.11.36-16.el8_10.6
Setting key "Host/runs_unixoide" based on this information
Other OS detections (in order of reliability):
OS: Linux/Unix
CPE: cpe:/o:linux:kernel
Found by NVT: 1.3.6.1.4.1.25623.1.0.105355 (FTP OS Identification)
Concluded from FTP banner on port 21/tcp: 220---------- Welcome to Pure-FTPd [privsep]
[TLS] ----------
220-You are user number 2 of 50 allowed.
220-Local time is now 18:58. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
OS: Linux/Unix
CPE: cpe:/o:linux:kernel
Found by NVT: 1.3.6.1.4.1.25623.1.0.111068 (SMTP/POP3/IMAP Server OS Identification)
Concluded from IMAP banner on port 143/tcp: * OK [CAPABILITY IMAP4rev1 LOGIN-
REFERRALS ID ENABLE IDLE SASL-IR LITERAL+ STARTTLS LOGINDISABLED] Dovecot
ready.
* ID ("name" "Dovecot")
OS: Linux/Unix
CPE: cpe:/o:linux:kernel
Found by NVT: 1.3.6.1.4.1.25623.1.0.111068 (SMTP/POP3/IMAP Server OS Identification)
Concluded from POP3 banner on port 995/tcp: +OK Dovecot ready.
OS: Linux/Unix
CPE: cpe:/o:linux:kernel
Found by NVT: 1.3.6.1.4.1.25623.1.0.111068 (SMTP/POP3/IMAP Server OS Identification)
Concluded from IMAP banner on port 993/tcp: * OK [CAPABILITY IMAP4rev1 LOGIN-
REFERRALS ID ENABLE IDLE SASL-IR LITERAL+ AUTH=PLAIN AUTH=LOGIN] Dovecot
ready.
* ID ("name" "Dovecot")
OS: Linux/Unix
CPE: cpe:/o:linux:kernel
Found by NVT: 1.3.6.1.4.1.25623.1.0.111068 (SMTP/POP3/IMAP Server OS Identification)
Concluded from POP3 banner on port 110/tcp: +OK Dovecot ready.

*5 Vulnerability Detection Result for Host 209.59.154.193 (host.bayclub.in) - 443/tcp

Missing Headers | More Information

Content-Security-Policy | https://owasp.org/www-project-secure-headers/#content-security-policy

Document-Policy | https://w3c.github.io/webappsec-feature-policy/document-policy#document-policy-http-header

Expect-CT | https://owasp.org/www-project-secure-headers/#expect-ct

Feature-Policy | https://owasp.org/www-project-secure-headers/#feature-policy, Note: The Feature Policy header has been renamed to Permissions Policy

Permissions-Policy | https://w3c.github.io/webappsec-feature-policy/#permissions-policy-http-header-field

Public-Key-Pins | Please check the output of the VTs including 'SSL/TLS:' and 'HPKP' in their name for more information and configuration help. Note: Most major browsers have dropped / deprecated support for this header in 2020.

Referrer-Policy | https://owasp.org/www-project-secure-headers/#referrer-policy

Strict-Transport-Security | Please check the output of the VTs including 'SSL/TLS:' and 'HSTS' in their name for more information and configuration help.

X-Content-Type-Options | https://owasp.org/www-project-secure-headers/#x-content-type-options

X-Frame-Options | https://owasp.org/www-project-secure-headers/#x-frame-options

X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers/#x-permitted-cross-domain-policies

X-XSS-Protection | https://owasp.org/www-project-secure-headers/#x-xss-protection, Note: Most major browsers have dropped / deprecated support for this header in 2020.

*6 Vulnerability Detection Result for Host 209.59.154.193 (host.bayclub.in) - 443/tcp

The Hostname/IP "209.59.154.193" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable generic web application scanning" option within the "Global variable settings" of the scan config in use.
Requests to this service are done via HTTP/1.1.
This service seems to be able to host PHP scripts.
This service seems to be NOT able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 9.0.3)" was used to access the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI scanning. You can enable this again with the "Add historic /scripts and /cgi-bin to directories for CGI scanning" option within the "Global variable settings" of the scan config in use.
The following directories were used for CGI scanning:
https://209.59.154.193/
https://209.59.154.193/admin
https://209.59.154.193/admin/js
https://209.59.154.193/controlpanel
https://209.59.154.193/public/admin
https://209.59.154.193/public/admin/js
https://209.59.154.193/webmail
While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards
The following directories were excluded from CGI scanning because the "Regex pattern to exclude directories from CGI scanning" setting of the NVT "Global variable settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was:
"/(images|image|img|css|js/|javascript|style|styles|theme|themes|icons|jquery)"
https://209.59.154.193/admin/css
https://209.59.154.193/admin/images
https://209.59.154.193/admin/js/modernizr/js
The following CGIs were discovered:
Syntax : cginame (arguments [default value])
https://209.59.154.193/admin/authenticate (_token [P23fYqFShr7AAALEXP4PF55jcmLrQxzQAfrZVCHp] email [] password [] file_path [] g_captcha_response [])

*7 Vulnerability Detection Result for Host 209.59.154.193 (host.bayclub.in) - 80/tcp

The Hostname/IP "209.59.154.193" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable generic web application scanning" option within the "Global variable settings" of the scan config in use.
Requests to this service are done via HTTP/1.1.
This service seems to be able to host PHP scripts.
This service seems to be NOT able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 9.0.3)" was used to access the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI scanning. You can enable this again with the "Add historic /scripts and /cgi-bin to directories for CGI scanning" option within the "Global variable settings" of the scan config in use.
The following directories were used for CGI scanning:
http://209.59.154.193/
http://209.59.154.193/.well-known
http://209.59.154.193/.well-known/acme-challenge
http://209.59.154.193/.well-known/pki-validation
http://209.59.154.193/cgi-sys
http://209.59.154.193/mailman
While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards
The following directories were excluded from CGI scanning because the "Regex pattern to exclude directories from CGI scanning" setting of the NVT "Global variable settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was:
"/(images|image|img|css|js/|javascript|style|styles|theme|themes|icons|jquery)"
http://209.59.154.193/img-sys
Directory index found at:
http://209.59.154.193/.well-known/
http://209.59.154.193/.well-known/acme-challenge/
http://209.59.154.193/.well-known/pki-validation/
The following CGIs were discovered:
Syntax : cginame (arguments [default value])
http://209.59.154.193/.well-known/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://209.59.154.193/.well-known/acme-challenge/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://209.59.154.193/.well-known/pki-validation/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])

*8 Vulnerability Detection Result for Host 209.59.154.193 (host.bayclub.in) - 21/tcp

'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CCM
TLS_DHE_RSA_WITH_AES_128_CCM_8
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CCM
TLS_DHE_RSA_WITH_AES_256_CCM_8
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256
TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_CCM
TLS_RSA_WITH_AES_128_CCM_8
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_CCM
TLS_RSA_WITH_AES_256_CCM_8
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_ARIA_128_GCM_SHA256
TLS_RSA_WITH_ARIA_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256

*9 Vulnerability Detection Result for Host 209.59.154.193 (host.bayclub.in) - 21/tcp

'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CCM
TLS_DHE_RSA_WITH_AES_128_CCM_8
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CCM
TLS_DHE_RSA_WITH_AES_256_CCM_8
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256
TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_CCM
TLS_RSA_WITH_AES_128_CCM_8
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_CCM
TLS_RSA_WITH_AES_256_CCM_8
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_ARIA_128_GCM_SHA256
TLS_RSA_WITH_ARIA_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256