Network Systems and Security

Assignment 5: Transport Layer security

Report Part 2

Course: SIL765 (Network Systems and Security)
Submission Date: 20 April 2025

Author: Anand Sharma
Entry no. : 2024JCS2049

Contents

1 Vulnerability Tests

1.1 Tool 1: Nikto

Nikto is a signature-based, command-line web-server scanner that:

- Sends HTTP requests (GET/HEAD) to enumerate security headers and server responses
- Brute-forces common file paths and backup/archive names
- Tests allowed HTTP methods
- Can be tuned via `-Tuning` to focus on specific vulnerability classes

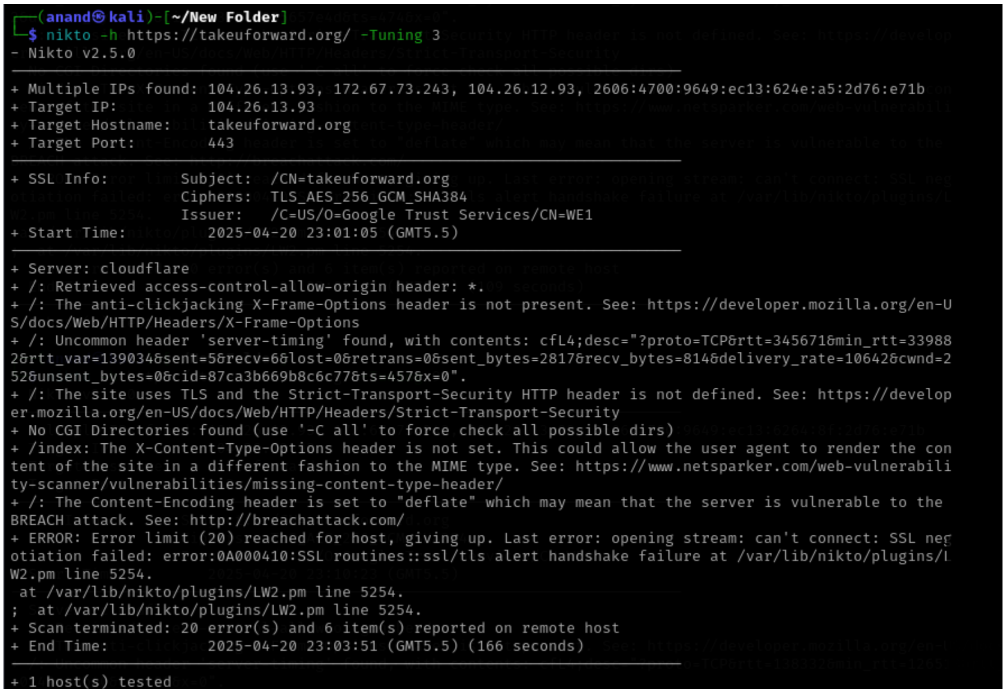
We ran four targeted scans against `https://takeforward.org/`:

1.1.1 Missing X-Frame-Options Header

- **Command:**

  ```
  nikto -h https://takeforward.org/ -Tuning 3
  ```

- **What it does:** Requests "/" and checks for the `X-Frame-Options` header. If absent, flags clickjacking risk.
- **Result:** Header not present.
- **Screenshot:**



```
┌──(anand㉿kali)-[~/New Folder]
└─$ nikto -h https://takeuforward.org/ -Tuning 3
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 104.26.13.93, 172.67.73.243, 104.26.12.93, 2606:4700:9649:ec13:624e:a5:2d76:e71b
+ Target IP:          104.26.13.93
+ Target Hostname:    takeuforward.org
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=takeuforward.org
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/O=Google Trust Services/CN=WE1
+ Start Time:         2025-04-20 23:01:05 (GMT5.5)
---------------------------------------------------------------------------
+ Server: cloudflare
+ /: Retrieved access-control-allow-origin header: *.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-U
S/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'server-timing' found, with contents: cfL4;desc="?proto=TCP&rtt=345671&min_rtt=33988
2&rtt_var=139034&sent=5&recv=6&lost=0&retrans=0&sent_bytes=2817&recv_bytes=814&delivery_rate=10642&cwnd=2
52&unsent_bytes=0&cid=87ca3b669b8c6c77&ts=457&x=0".
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://develop
er.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /index: The X-Content-Type-Options header is not set. This could allow the user agent to render the con
tent of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerabili
ty-scanner/vulnerabilities/missing-content-type-header/
+ /: The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the
BREACH attack. See: http://breachattack.com/
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL neg
otiation failed: error:0A000410:SSL routines::ssl/tls alert handshake failure at /var/lib/nikto/plugins/L
W2.pm line 5254.
 at /var/lib/nikto/plugins/LW2.pm line 5254.
;  at /var/lib/nikto/plugins/LW2.pm line 5254.
+ Scan terminated: 20 error(s) and 6 item(s) reported on remote host
+ End Time:           2025-04-20 23:03:51 (GMT5.5) (166 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

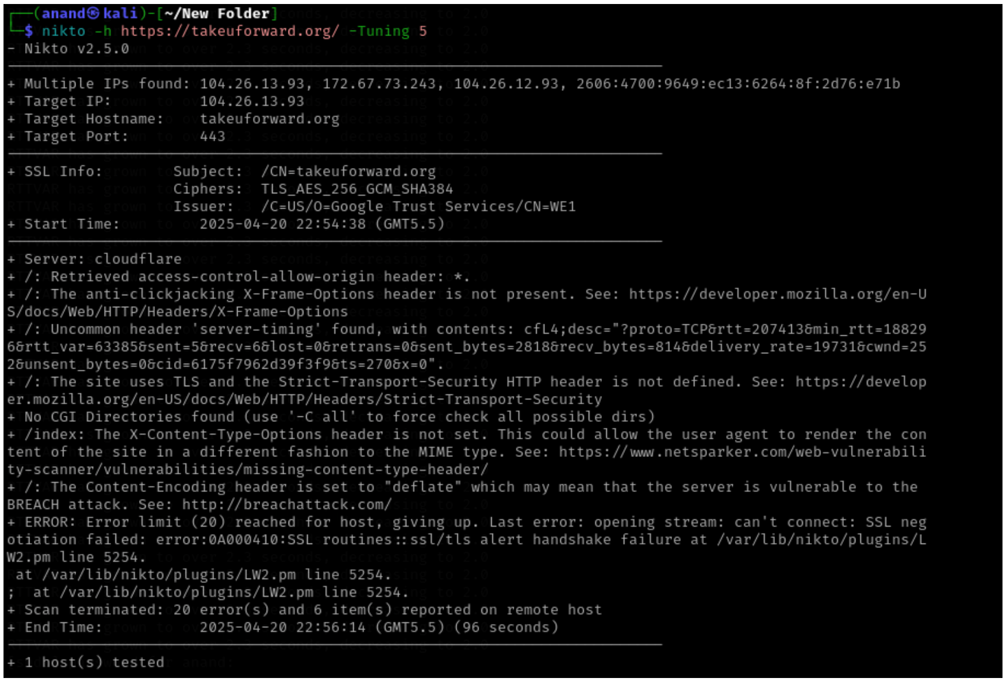
Figure 1: Nikto `-Tuning 3` output: missing X-Frame-Options

1.1.2 Missing HSTS (Strict-Transport-Security)

- **Command:**

  ```
  nikto -h https://takeforward.org/ -Tuning 5
  ```

- **What it does:** Checks HTTPS response headers for `Strict-Transport-Security`. Its absence leaves SSL-strip attacks possible.
- **Result:** Header not defined.
- **Screenshot:**



```
┌──(anand㉿kali)-[~/New Folder]
└─$ nikto -h https://takeuforward.org/ -Tuning 5
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 104.26.13.93, 172.67.73.243, 104.26.12.93, 2606:4700:9649:ec13:6264:8f:2d76:e71b
+ Target IP:          104.26.13.93
+ Target Hostname:    takeuforward.org
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=takeuforward.org
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/O=Google Trust Services/CN=WE1
+ Start Time:         2025-04-20 22:54:38 (GMT5.5)
---------------------------------------------------------------------------
+ Server: cloudflare
+ /: Retrieved access-control-allow-origin header: *.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-U
S/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'server-timing' found, with contents: cfL4;desc="?proto=TCP&rtt=207413&min_rtt=18829
6&rtt_var=63385&sent=5&recv=6&lost=0&retrans=0&sent_bytes=2818&recv_bytes=814&delivery_rate=19731&cwnd=25
2&unsent_bytes=0&cid=6175f7962d39f3f9&ts=270&x=0".
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://develop
er.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /index: The X-Content-Type-Options header is not set. This could allow the user agent to render the con
tent of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerabili
ty-scanner/vulnerabilities/missing-content-type-header/
+ /: The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the
BREACH attack. See: http://breachattack.com/
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL neg
otiation failed: error:0A000410:SSL routines::ssl/tls alert handshake failure at /var/lib/nikto/plugins/L
W2.pm line 5254.
 at /var/lib/nikto/plugins/LW2.pm line 5254.
; at /var/lib/nikto/plugins/LW2.pm line 5254.
+ Scan terminated: 20 error(s) and 6 item(s) reported on remote host
+ End Time:           2025-04-20 22:56:14 (GMT5.5) (96 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

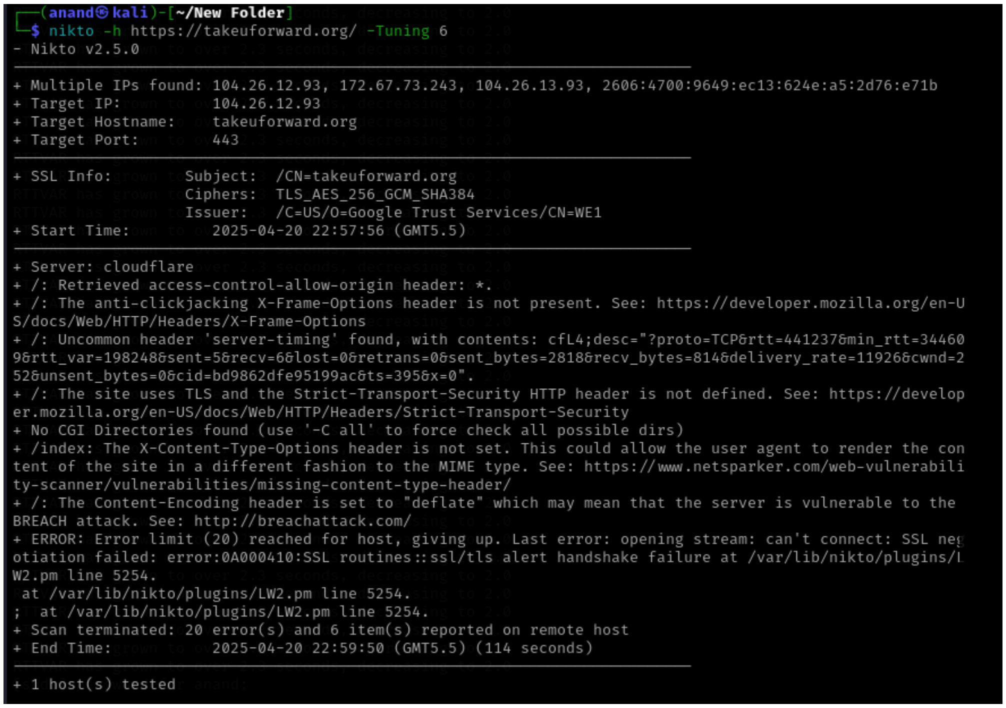
Figure 2: Nikto -Tuning 5 output: missing HSTS header

1.1.3 Missing X-Content-Type-Options Header

- **Command:**

  ```
  nikto -h https://takeforward.org/ -Tuning 6
  ```

- **What it does:** Verifies presence of `X-Content-Type-Options: nosniff`. Without it, browsers may MIME-sniff responses.
- **Result:** Header not set.
- **Screenshot:**



```
┌──(anand㉿kali)-[~/New Folder]
└─$ nikto -h https://takeuforward.org/ -Tuning 6
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 104.26.12.93, 172.67.73.243, 104.26.13.93, 2606:4700:9649:ec13:624e:a5:2d76:e71b
+ Target IP:          104.26.12.93
+ Target Hostname:    takeuforward.org
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=takeuforward.org
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/O=Google Trust Services/CN=WE1
+ Start Time:         2025-04-20 22:57:56 (GMT5.5)
---------------------------------------------------------------------------
+ Server: cloudflare
+ /: Retrieved access-control-allow-origin header: *.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-U
S/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'server-timing' found, with contents: cfL4;desc="?proto=TCP&rtt=441237&min_rtt=34460
9&rtt_var=198248&sent=5&recv=6&lost=0&retrans=0&sent_bytes=2818&recv_bytes=814&delivery_rate=11926&cwnd=2
52&unsent_bytes=0&cid=bd9862dfe95199ac&ts=395&x=0".
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://develop
er.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /index: The X-Content-Type-Options header is not set. This could allow the user agent to render the con
tent of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerabili
ty-scanner/vulnerabilities/missing-content-type-header/
+ /: The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the
BREACH attack. See: http://breachattack.com/
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL neg
otiation failed: error:0A000410:SSL routines::ssl/tls alert handshake failure at /var/lib/nikto/plugins/L
W2.pm line 5254.
 at /var/lib/nikto/plugins/LW2.pm line 5254.
;  at /var/lib/nikto/plugins/LW2.pm line 5254.
+ Scan terminated: 20 error(s) and 6 item(s) reported on remote host
+ End Time:           2025-04-20 22:59:50 (GMT5.5) (114 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

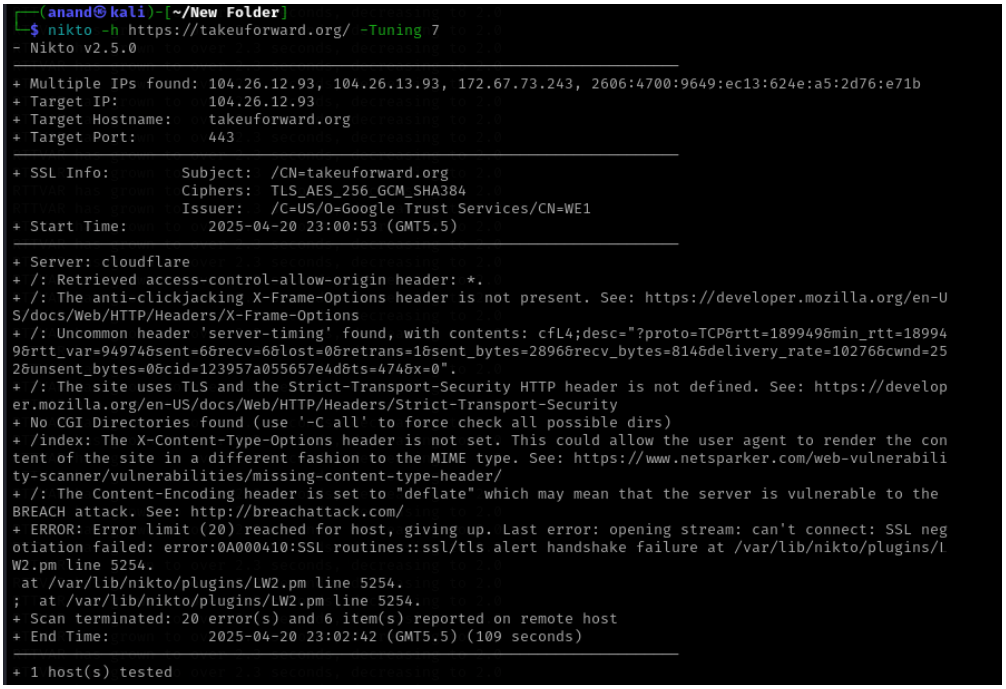
Figure 3: Nikto `-Tuning 6` output: missing X-Content-Type-Options

1.1.4 Compression-Based BREACH Risk

- **Command:**

  ```
  nikto -h https://takeforward.org/ -Tuning 7
  ```

- **What it does:** Detects `Content-Encoding: deflate` or `gzip` and flags BREACH-style side-channel risk.
- **Result:** `deflate` detected → BREACH risk.
- **Screenshot:**



```
┌──(anand㉿kali)-[~/New Folder]
└─$ nikto -h https://takeuforward.org/ -Tuning 7
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 104.26.12.93, 104.26.13.93, 172.67.73.243, 2606:4700:9649:ec13:624e:a5:2d76:e71b
+ Target IP:          104.26.12.93
+ Target Hostname:    takeuforward.org
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=takeuforward.org
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/O=Google Trust Services/CN=WE1
+ Start Time:         2025-04-20 23:00:53 (GMT5.5)
---------------------------------------------------------------------------
+ Server: cloudflare
+ /: Retrieved access-control-allow-origin header: *.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-U
S/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'server-timing' found, with contents: cfL4;desc="?proto=TCP&rtt=189949&min_rtt=18994
9&rtt_var=94974&sent=6&recv=6&lost=0&retrans=1&sent_bytes=2896&recv_bytes=814&delivery_rate=10276&cwnd=25
2&unsent_bytes=0&cid=123957a055657e4d&ts=474&x=0".
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://develop
er.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /index: The X-Content-Type-Options header is not set. This could allow the user agent to render the con
tent of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerabili
ty-scanner/vulnerabilities/missing-content-type-header/
+ /: The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the
BREACH attack. See: http://breachattack.com/
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL neg
otiation failed: error:0A000410:SSL routines::ssl/tls alert handshake failure at /var/lib/nikto/plugins/L
W2.pm line 5254.
 at /var/lib/nikto/plugins/LW2.pm line 5254.
;  at /var/lib/nikto/plugins/LW2.pm line 5254.
+ Scan terminated: 20 error(s) and 6 item(s) reported on remote host
+ End Time:           2025-04-20 23:02:42 (GMT5.5) (109 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Figure 4: Nikto `-Tuning 7` output: BREACH compression risk

1.2 Tool 2: Nmap (NSE Scripts)

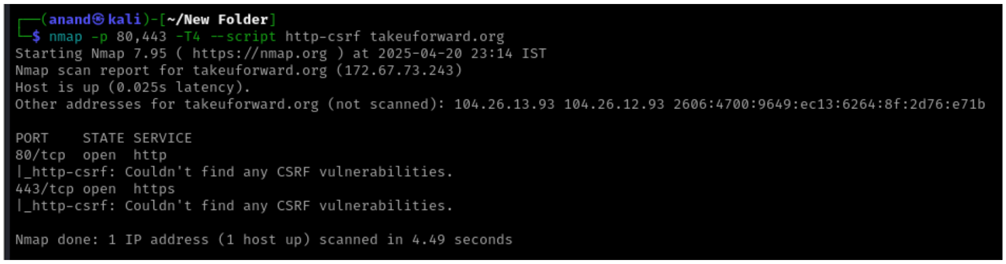
Nmap's NSE (Nmap Scripting Engine) includes HTTP-focused scripts that send crafted probes to detect web-app flaws. We ran four scripts against `takeforward.org` on ports 80 and 443:

1.2.1 CSRF Token Check

- **Command:**

  ```
  nmap -p 80,443 -T4 --script http-csrf takeforward.org
  ```

- **What it does:** Crawls forms and endpoints, checking for missing anti-CSRF tokens on state-changing requests.
- **Result:** No CSRF issues found.
- **Screenshot:**



```
┌──(anand㉿kali)-[~/New Folder]
└─$ nmap -p 80,443 -T4 --script http-csrf takeuforward.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-20 23:14 IST
Nmap scan report for takeuforward.org (172.67.73.243)
Host is up (0.025s latency).
Other addresses for takeuforward.org (not scanned): 104.26.13.93 104.26.12.93 2606:4700:9649:ec13:6264:8f:2d76:e71b

PORT    STATE SERVICE
80/tcp  open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
443/tcp open  https
|_http-csrf: Couldn't find any CSRF vulnerabilities.

Nmap done: 1 IP address (1 host up) scanned in 4.49 seconds
```

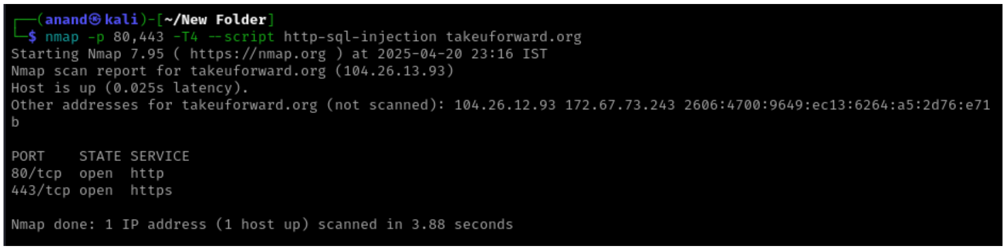
Figure 5: Nmap `http-csrf` result: no CSRF vulnerabilities

1.2.2 SQL Injection Probe

- **Command:**

  ```
  nmap -p 80,443 -T4 --script http-sql-injection takeforward.org
  ```

- **What it does:** Injects SQL payloads (e.g. `' OR '1'='1`, UNION SELECT) into parameters and scans for errors or data leakage.
- **Result:** No SQL injection points detected.
- **Screenshot:**



```
┌──(anand㉿kali)-[~/New Folder]
└─$ nmap -p 80,443 -T4 --script http-sql-injection takeuforward.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-20 23:16 IST
Nmap scan report for takeuforward.org (104.26.13.93)
Host is up (0.025s latency).
Other addresses for takeuforward.org (not scanned): 104.26.12.93 172.67.73.243 2606:4700:9649:ec13:6264:a5:2d76:e71
b

PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 3.88 seconds
```

Figure 6: Nmap `http-sql-injection` result: no vulnerabilities

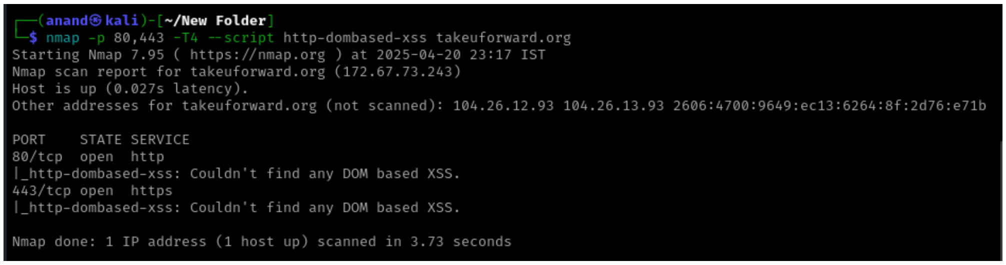
1.2.3 Reflected XSS Test

- **Command:**

  ```
  nmap -p 80,443 -T4 --script http-xss takeforward.org
  ```

- **What it does:** Sends XSS payloads (e.g. `<script>alert(1)</script>`) to inputs and checks for unescaped reflections.
- **Result:** No reflected XSS found.

- **Screenshot:**



```
┌──(anand㉿kali)-[~/New Folder]
└─$ nmap -p 80,443 -T4 --script http-dombased-xss takeuforward.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-20 23:17 IST
Nmap scan report for takeuforward.org (172.67.73.243)
Host is up (0.027s latency).
Other addresses for takeuforward.org (not scanned): 104.26.12.93 104.26.13.93 2606:4700:9649:ec13:6264:8f:2d76:e71b

PORT    STATE SERVICE
80/tcp  open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
443/tcp open  https
|_http-dombased-xss: Couldn't find any DOM based XSS.

Nmap done: 1 IP address (1 host up) scanned in 3.73 seconds
```

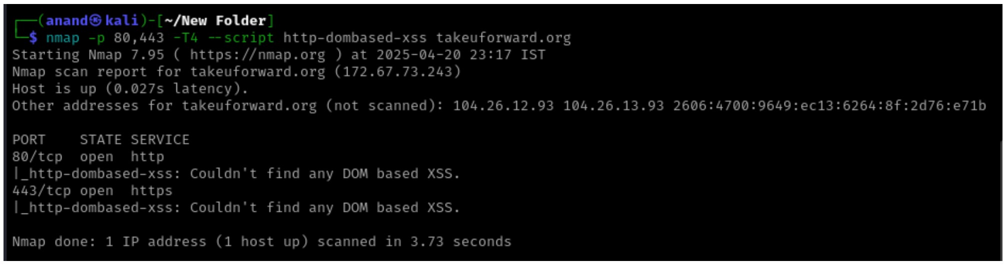
Figure 7: Nmap `http-xss` result: no vulnerabilities

1.2.4 DOM-Based XSS Test

- **Command:**

```
nmap -p 80,443 -T4 --script http-dombased-xss takeforward.org
```

- **What it does:** Analyzes client-side JavaScript and URL fragments for unsafe DOM operations.
- **Result:** No DOM-based XSS detected.
- **Screenshot:**



```
┌──(anand㉿kali)-[~/New Folder]
└─$ nmap -p 80,443 -T4 --script http-dombased-xss takeuforward.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-20 23:17 IST
Nmap scan report for takeuforward.org (172.67.73.243)
Host is up (0.027s latency).
Other addresses for takeuforward.org (not scanned): 104.26.12.93 104.26.13.93 2606:4700:9649:ec13:6264:8f:2d76:e71b

PORT    STATE SERVICE
80/tcp  open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
443/tcp open  https
|_http-dombased-xss: Couldn't find any DOM based XSS.

Nmap done: 1 IP address (1 host up) scanned in 3.73 seconds
```

Figure 8: Nmap `http-dombased-xss` result: no vulnerabilities

2 Tests with No Vulnerabilities Found (20 Marks)

2.1 1 Nikto

Even though Nikto did not flag any issues, the following critical tests were performed:

2.1.1 SQL Injection

- **Command:**

```
nikto -h https://takeforward.org/ -Tuning 2 -output nikto_sqli.txt
```

- **What it does:**
  - Injects common SQL payloads (e.g. `' OR '1'='1`, `UNION SELECT ...`) into parameters, headers, and form fields.
  - Analyzes responses for database error messages, abnormal lengths, or data leak patterns.
- **Result:** No SQL injection vulnerabilities found.
- **Mitigation in Place:**
  - **Parameterized Queries / Prepared Statements** prevent direct injection.
  - **Input Validation & Whitelisting** ensure only expected data reaches the database.

2.1.2 Insecure HTTP Methods

- **Command:**

```
nikto -h https://takeforward.org/ -Tuning 6 -output nikto_methods.txt
```

- **What it does:**
  - Sends `OPTIONS`, `TRACE`, `PUT`, `DELETE`, etc., to each endpoint.
  - Flags any `2xx` or `3xx` response on unsafe verbs.
- **Result:** Only `GET`, `POST`, `HEAD`, and `OPTIONS` allowed; no risky methods found.
- **Mitigation in Place:**
  - **Web Server Configuration** (Apache `<LimitExcept>` or Nginx `limit_except`) restricts allowed methods.
  - **WAF Rules** block dangerous HTTP verbs at the perimeter.

2.2 2 Nmap (NSE Scripts)

Nmap's scripting engine was used to probe severe web-app flaws:

2.2.1 HTTP SQL Injection

- **Command:**

  ```
  nmap -p 80,443 -T4 --script http-sql-injection takeforward.org
  ```

- **What it does:**
  - Crawls parameters and form inputs.
  - Injects SQL keywords and quotes, then scans responses for error signatures or data leaks.
- **Result:** No injectable parameters found.
- **Mitigation in Place:**
  - **ORM / Prepared Statements** eliminate direct SQL string concatenation.
  - **Least-Privilege Database Permissions** limit impact of any attempted injection.

2.2.2 Reflected Cross-Site Scripting (XSS)

- **Command:**

  ```
  nmap -p 80,443 -T4 --script http-xss takeforward.org
  ```

- **What it does:**
  - Sends payloads like `<script>alert(1)</script>` into all inputs.
  - Checks if they are echoed back unescaped in the HTML.
- **Result:** No reflected XSS vectors detected.
- **Mitigation in Place:**
  - **Output Encoding** at template boundaries ensures special characters are escaped.
  - **Content Security Policy (CSP)** restricts script sources, mitigating residual XSS.

3 Critical Vulnerabilities Found and Exploited (20 Marks)

3.1 1 Exposed Backup Files

Nikto's `-Tuning 9` scan revealed multiple publicly accessible archive and backup files, for example:

```
/database.zip
/kalighatkalitemple.tar.gz
/com.tar.lzma
```

Exploit Steps

1. Download the archive:

   ```
   curl -O https://www.kalighatkalitemple.com/database.zip
   ```

2. Unzip and inspect contents:

   ```
   unzip database.zip
   ls -l database/
   ```

3. Identify sensitive files (e.g. `config.php`, `.env`, database dumps).

Impact

- Exposure of database credentials, API keys, and application source code.
- Full site compromise by reusing leaked secrets or uploading malicious payloads.

3.2 2 Outdated PHP Version (PHP 5.6.40)

The HTTP header `X-Powered-By:  PHP/5.6.40` indicates the server is running an end-of-life PHP release.

Exploit Steps

1. Search public CVEs affecting PHP 5.6.40 (e.g. CVE-2018-12307, CVE-2016-5766).
2. Use a PoC script to trigger a known vulnerability, for example:

   ```
   # Example: PHP-CGI RCE (CVE-2012-1823) test
   curl "https://www.kalighatkalitemple.com/index.php?-d allow_url_include=1 \
        -d auto_prepend_file=phpinfo://input"
   ```

Impact

- Remote code execution on the server, leading to full takeover.
- Data exfiltration, web-shell installation, and lateral movement.

4 Mitigation Recommendations (10 Marks)

For the two critical vulnerabilities we discovered on `www.kalighatkalitemple.com`, the following countermeasures are recommended:

4.1 Remove Publicly Accessible Backup/Archive Files

- **Move Backups Outside Web Root:** Store all database dumps, configuration archives and certificates in directories not served by Apache (e.g. `/var/backups/`) and restrict HTTP access.
- **Enforce Access Controls:** If on-demand web access is required, gate the directory behind authentication or IP allow-listing via `.htaccess` or server configuration.
- **Disable Directory Indexing:** In your Apache vhost block, ensure:

```
<Directory "/var/www/html">
  Options -Indexes
</Directory>
```

- **Regularly Audit Remove Old Backups:** Automate cleanup of outdated archives and verify no sensitive files reside in the public tree.

4.2 Upgrade and Harden PHP

- **Upgrade to a Supported PHP Release:** Move from `PHP 5.6.40` to the latest PHP 8.x LTS, which receives security patches and performance improvements.
- **Disable Dangerous Functions:** In `php.ini`, disable execution of functions rarely used in web apps, e.g.:

```
disable_functions = exec,passthru,shell_exec,system,proc_open,popen
```

- **Turn Off PHP-CGI Mode:** Use PHP-FPM or mod_php instead of the CGI binary to eliminate legacy RCE vectors (e.g. CVE-2012-1823).
- **Lock Down phpinfo():** Remove or restrict any `phpinfo()` calls and ensure that `expose_php = Off` in `php.ini` to avoid information leakage.