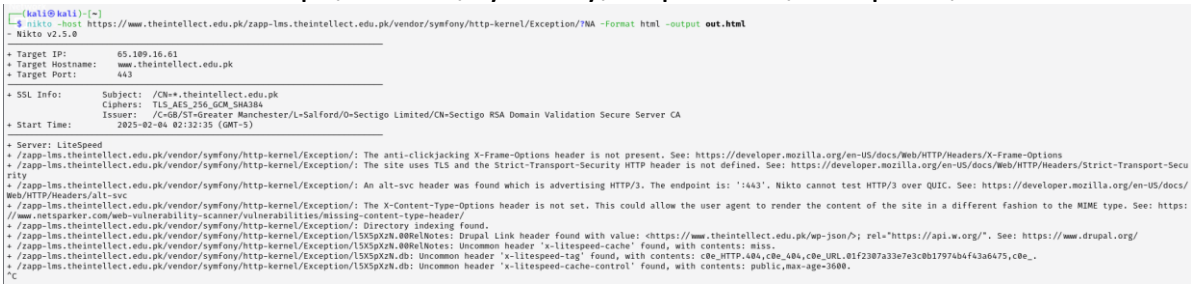
Date: 04/ 02 /2025

Lab Practical #08:
Perform Network Vulnerability scan using Nikto

1) **Host:**https://www.theintellect.edu.pk/zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/?NA



```
┌──(kali㉿kali)-[~]
└─$ nikto -host https://www.theintellect.edu.pk/zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/?NA -Format html -output out.html
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          65.109.16.61
+ Target Hostname:    www.theintellect.edu.pk
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=*.theintellect.edu.pk
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=GB/ST=Greater Manchester/L=Salford/O=Sectigo Limited/CN=Sectigo RSA Domain Validation Secure Server CA
+ Start Time:         2025-02-04 02:32:35 (GMT-5)
---------------------------------------------------------------------------
+ Server: LiteSpeed
+ /zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc
+ /zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/: Directory indexing found.
+ /zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/lSX5pXzN.0@RelNotes: Drupal Link header found with value: <https://www.theintellect.edu.pk/wp-json/>; rel="https://api.w.org/". See: https://www.drupal.org/
+ /zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/lSX5pXzN.0@RelNotes: Uncommon header 'x-litespeed-cache' found, with contents: miss.
+ /zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/lSX5pXzN.db: Uncommon header 'x-litespeed-tag' found, with contents: c0e_HTTP.404,c0e_404,c0e_URL.01f2307a33e7e3c0b17974b4f43a6475,c0e_.
+ /zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/lSX5pXzN.db: Uncommon header 'x-litespeed-cache-control' found, with contents: public,max-age=3600.
^C
```

Vulnerability

URI	/zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/
HTTP Method	GET
Description	/zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/: Directory indexing found.
Test Links	https://www.theintellect.edu.pk:443/zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/ https://65.109.16.61:443/zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/
References	
URI	/zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/RzEkGYe5.show_query_columns
HTTP Method	GET
Description	/zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/RzEkGYe5.show_query_columns: Drupal Link header found with value: <https://www.theintellect.edu.pk/wp-json/>; rel="https://api.w.org/".
Test Links	https://www.theintellect.edu.pk:443/zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/RzEkGYe5.show_query_columns https://65.109.16.61:443/zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/RzEkGYe5.show_query_columns
References	https://www.drupal.org/
URI	/zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/RzEkGYe5.show_query_columns
HTTP Method	GET
Description	/zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/RzEkGYe5.show_query_columns: Uncommon header 'x-litespeed-cache-control' found, with contents: public,max-age=3600.
Test Links	https://www.theintellect.edu.pk:443/zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/RzEkGYe5.show_query_columns https://65.109.16.61:443/zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/RzEkGYe5.show_query_columns
References	
URI	/zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/RzEkGYe5.show_query_columns
HTTP Method	GET
Description	/zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/RzEkGYe5.show_query_columns: Uncommon header 'x-litespeed-cache' found, with contents: miss.
Test Links	https://www.theintellect.edu.pk:443/zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/RzEkGYe5.show_query_columns https://65.109.16.61:443/zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/RzEkGYe5.show_query_columns
References	
URI	/zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/RzEkGYe5.show_query_columns
HTTP Method	GET
Description	/zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/RzEkGYe5.show_query_columns: Uncommon header 'x-litespeed-tag' found, with contents: c0e_HTTP.404,c0e_404,c0e_URL.aa7eecdd4793b4ea0c68aae0f86ea0c7,c0e_.
Test Links	https://www.theintellect.edu.pk:443/zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/RzEkGYe5.show_query_columns https://65.109.16.61:443/zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/RzEkGYe5.show_query_columns
References	
URI	/zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/index.php?
HTTP Method	GET
Description	/zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/index.php?: Uncommon header 'x-redirect-by' found, with contents: WordPress.
Test Links	https://www.theintellect.edu.pk:443/zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/index.php? https://65.109.16.61:443/zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/index.php?
References	
URI	/zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/
HTTP Method	GET
Description	/zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/: The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the BREACH attack.
Test Links	https://www.theintellect.edu.pk:443/zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/ https://65.109.16.61:443/zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/
References	http://breachattack.com/
URI	/zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/
HTTP Method	GET
Description	Server is using a wildcard certificate: *.theintellect.edu.pk.
Test Links	https://www.theintellect.edu.pk:443/zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/ https://65.109.16.61:443/zapp-lms.theintellect.edu.pk/vendor/symfony/http-kernel/Exception/
References	https://en.wikipedia.org/wiki/Wildcard_certificate

Solution

1. **Directory Indexing Found:**
   Disable directory listing by modifying the server configuration:
   - Apache: Add Options -Indexes in the .htaccess or httpd.conf
   - Nginx: Add autoindex off; in the configuration file.
2. **Drupal Link Header Found:**
   - Disable this header in Drupal settings.
   - Use security modules like Security Kit to mask such information.

Date: 04/ 02 /2025

3. **Content-Encoding Header Set to "Deflate" (Potential BREACH Attack):**
   - Disable HTTP compression for sensitive data:
     Apache: Disable mod_deflate for sensitive pages.
     Nginx: Set gzip off; for authentication pages.
   - Use CSRF tokens and rate limiting to mitigate attacks.
4. **Wildcard Certificate Detected:**
   - Use strict certificate pinning.
   - Ensure proper subdomain isolation to prevent misuse.
5. **X-Redirect-By Header Found (WordPress):**
   - Use a security plugin (e.g., Hide My WP) to remove this header.

2) Host : Darshan.ac.in

```
┌──(kali㉿kali)-[~]
└─$ nikto -host darshan.ac.in -ssl -Format html -o darshan.html
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          103.13.112.180
+ Target Hostname:    darshan.ac.in
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=darshan.ac.in
                   Ciphers:  ECDHE-RSA-AES256-GCM-SHA384
                   Issuer:   /C=US/O=Let's Encrypt/CN=R11
+ Start Time:         2025-02-04 09:05:57 (GMT-5)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/10.0
+ /: Retrieved x-aspnet-version header: 4.0.30319.
+ /: Retrieved x-powered-by header: ASP.NET.
+ /: Uncommon header 'x-powered-by-plesk' found, with contents: PleskWin.
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Str
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME
/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /: Cookie __RequestVerificationToken created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
```

Vulnerability

URI	/
HTTP Method	GET
Description	/: Uncommon header 'x-powered-by-plesk' found, with contents: PleskWin.
Test Links	https://darshan.ac.in:443/ https://103.13.112.180:443/
References	

URI	/
HTTP Method	GET
Description	/: The site uses TLS and the Strict-Transport-Security HTTP header is not defined.
Test Links	https://darshan.ac.in:443/ https://103.13.112.180:443/
References	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security

URI	/
HTTP Method	GET
Description	/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.
Test Links	https://darshan.ac.in:443/ https://103.13.112.180:443/
References	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/

URI	/
HTTP Method	GET
Description	/: Cookie __RequestVerificationToken created without the secure flag.
Test Links	https://darshan.ac.in:443/ https://103.13.112.180:443/
References	https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies

URI	/
HTTP Method	GET
Description	/: The web server may reveal its internal or real IP in the Location header via a request to with HTTP/1.0. The value is "127.0.0.1".
Test Links	https://darshan.ac.in:443/ https://103.13.112.180:443/
References	CVE-2000-0649

URI	/
HTTP Method	GET
Description	/: The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the BREACH attack.
Test Links	https://darshan.ac.in:443/ https://103.13.112.180:443/
References	http://breachattack.com/

Date: 04/ 02 /2025

Solution

1. **Uncommon Header X-Powered-By: PleskWin Found**
   - Remove the X-Powered-By header in Plesk:
     Apache: Add Header unset X-Powered-By to .htaccess or httpd.conf.
     Nginx: Add server_tokens off; to the config file.
   - Keep Plesk updated to avoid known exploits.

2. **Missing Strict-Transport-Security (HSTS) Header:**
   - **Issue:** Without HSTS, users can be subjected to man-in-the-middle attacks (e.g., SSL stripping)
   - **Solution:** Add the following header in your web server configuration
     - Strict-Transport-Security:max-age=31536000;includeSubDomains; preload

3. **Missing X-Content-Type-Options Header**
   - Add this header to prevent content sniffing
     "X-Content-Type-Options: nosniff"

4. **__RequestVerificationToken Cookie Missing Secure Flag**
   - Ensure all sensitive cookies have these flags
     "Secure; HttpOnly; SameSite=Strict"

5. **Internal IP Address Leak (127.0.0.1 in Location Header)**
   - **Issue**: The server reveals its internal or real IP address, which attackers can use to target internal systems.
   - **Solution**: Remove internal IPs from HTTP responses.

6. **Content-Encoding Set to "Deflate" (Potential BREACH Attack)**
   - **Issue:** The server allows HTTP compression, which can be exploited to recover sensitive information (e.g., CSRF tokens).
   - **Solution:** Disable compression for sensitive data

Date: 04/ 02 /2025

3) Host : https://tifonline.pk:443/mod/page/view.php/

```
┌──(kali㉿kali)-[~]
└─$ nikto -host https://tifonline.pk/mod/page/view.php?id=448 -Format html -o unk.html
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          198.54.121.83
+ Target Hostname:    tifonline.pk
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=tifonline.pk
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/O=Let's Encrypt/CN=R10
+ Start Time:         2025-02-04 09:35:28 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache
+ /mod/page/view.php/: Uncommon header 'content-style-type' found, with contents: text/css.
+ /mod/page/view.php/: Uncommon header 'content-script-type' found, with contents: text/javascript.
+ /mod/page/view.php/: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Header
ty
+ /mod/page/view.php/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the
www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /mod/page/view.php/: Cookie MoodleSession created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /mod/page/view.php/: Cookie MoodleSession created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
```

Vulnerability

URI	/mod/page/view.php/
HTTP Method	GET
Description	/mod/page/view.php/: Uncommon header 'content-style-type' found, with contents: text/css.
Test Links	https://tifonline.pk:443/mod/page/view.php/ https://198.54.121.83:443/mod/page/view.php/
References	
URI	/mod/page/view.php/
HTTP Method	GET
Description	/mod/page/view.php/: Uncommon header 'content-script-type' found, with contents: text/javascript.
Test Links	https://tifonline.pk:443/mod/page/view.php/ https://198.54.121.83:443/mod/page/view.php/
References	
URI	/mod/page/view.php/
HTTP Method	GET
Description	/mod/page/view.php/: The site uses TLS and the Strict-Transport-Security HTTP header is not defined.
Test Links	https://tifonline.pk:443/mod/page/view.php/ https://198.54.121.83:443/mod/page/view.php/
References	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
URI	/mod/page/view.php/
HTTP Method	GET
Description	/mod/page/view.php/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.
Test Links	https://tifonline.pk:443/mod/page/view.php/ https://198.54.121.83:443/mod/page/view.php/
References	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
URI	/mod/page/view.php/
HTTP Method	GET
Description	/mod/page/view.php/: Cookie MoodleSession created without the secure flag.
Test Links	https://tifonline.pk:443/mod/page/view.php/ https://198.54.121.83:443/mod/page/view.php/
References	https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
URI	/mod/page/view.php/
HTTP Method	GET
Description	/mod/page/view.php/: Cookie MoodleSession created without the httponly flag.
Test Links	https://tifonline.pk:443/mod/page/view.php/ https://198.54.121.83:443/mod/page/view.php/
References	https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies

Solution:

1. **Uncommon Header Content-Script-Type: text/javascript**
   - Remove uncommon and not necessary header.
2. **Missing Strict-Transport-Security (HSTS) Header**
   - The absence of HSTS means the site is vulnerable to SSL stripping attacks.
   - **For apache** : Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains; preload"
3. **Missing X-Content-Type-Options: nosniff Header**
   - Without this header, browsers may try to "guess" the MIME type, which can lead to security risks.
   - **Enable in Apache**: Header always set X-Content-Type-Options "nosniff"
   - **Enable in Nginx**: add_header X-Content-Type-Options "nosniff";

Date: 04/ 02 /2025

4. **MoodleSession Cookie Missing Secure Flag**
    - This cookie is not marked as Secure, meaning it can be transmitted over HTTP, leading to potential session hijacking.
    - Ensure it is only sent over HTTPS by setting the Secure flag
5. **MoodleSession Cookie Missing HttpOnly Flag**
    - The absence of HttpOnly means JavaScript can access this cookie, making it vulnerable to XSS attacks.
    - Add the HttpOnly flag
    - **For PHP**: session_set_cookie_params(['httponly' => true]);
    - **In Apache:** Header edit Set-Cookie ^(.*)$ $1; HttpOnly