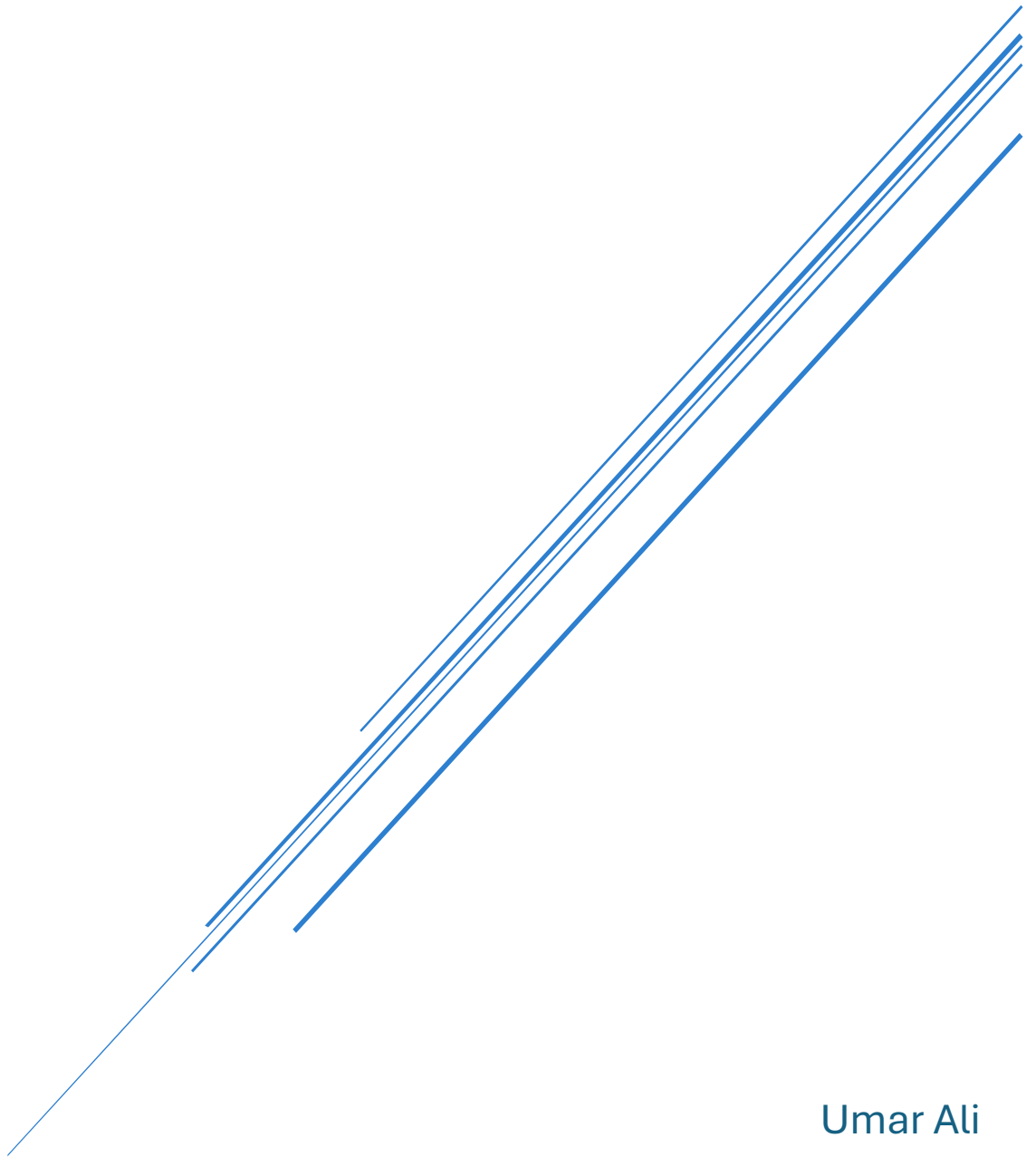


WEB ENGINEERING

ASSIGNMENT 3



Umar Ali

B22F0088SE094

SE-F22 Red

Mr. Syed Adil Ibrar

Tools Needed

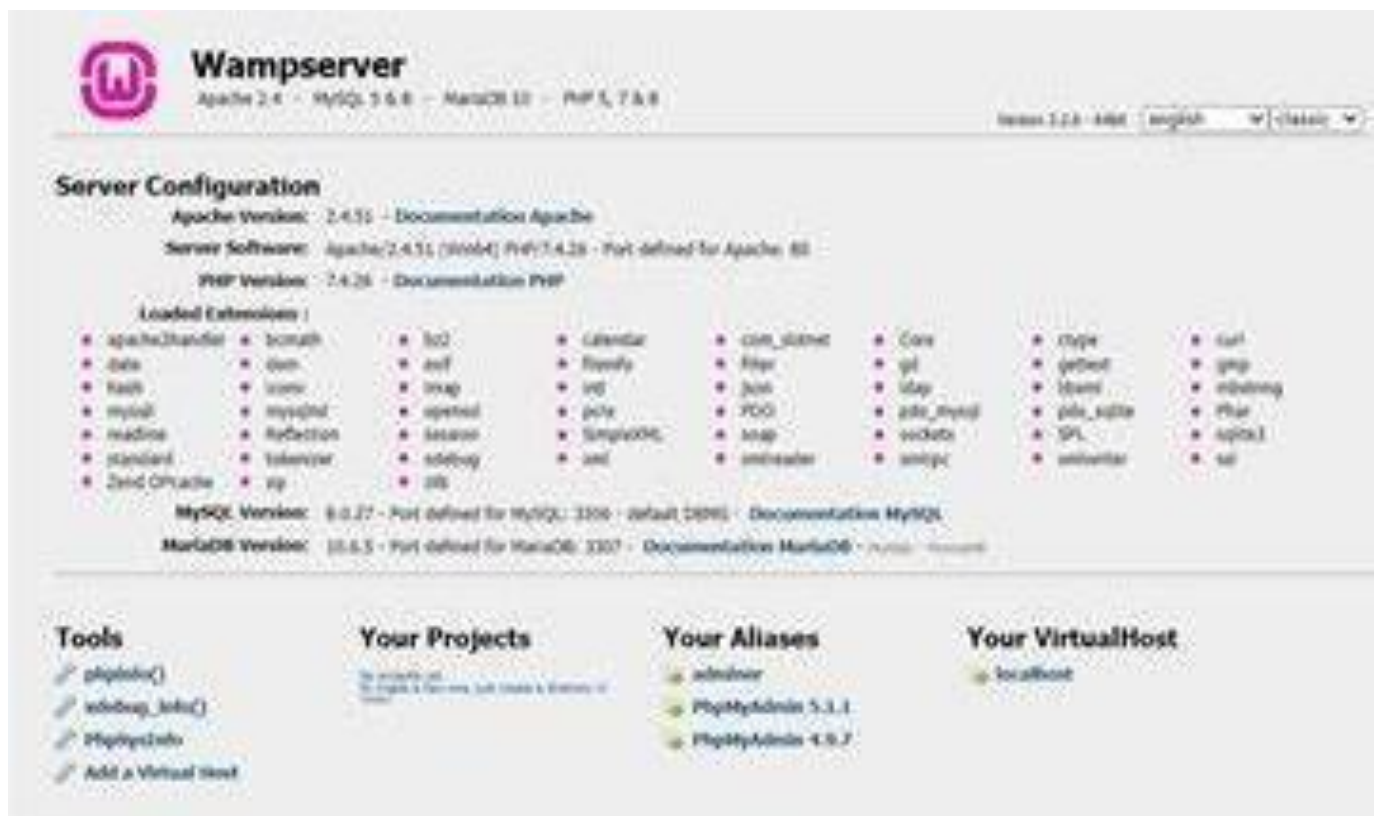
- WAMP Server (64-bit)
- OpenSSL (usually bundled with WAMP or can be installed)
- DVWA (Damn Vulnerable Web App)
- Text Editor (Notepad++, VSCode)
- Web Browser (for testing HTTPS, headers, etc.)

Task-by-Task Breakdown

Task 1: Setting Up a Secure WAMP Stack (10 Marks)

1. **Install WAMP Server o Download from** wampserver.com
2. **Install to** C:\wamp64
3. **Verify by opening** <http://localhost>

Deliverable: Screenshot of working <http://localhost>



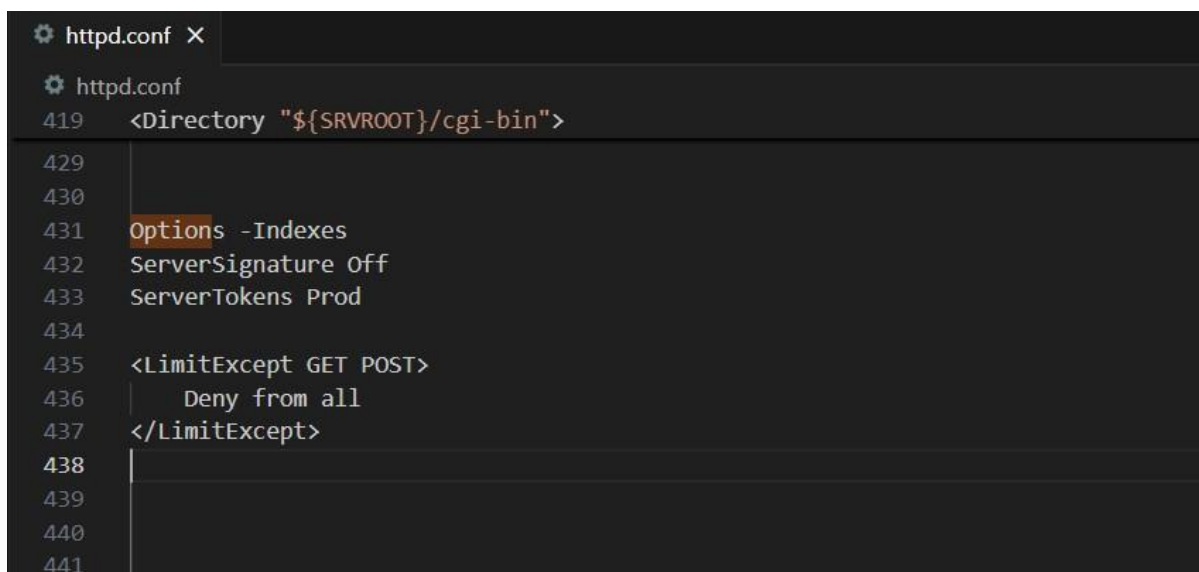
4. Secure Apache Configuration

5. **Open:** C:\wamp64\bin\apache\apache2.4.x\conf\httpd.conf o

Add this Code:

```
Options -Indexes  
  
ServerSignature Off  
  
ServerTokens Prod  
  
<LimitExcept GET POST HEAD>  
  
    Deny from all  
  
</LimitExcept>  
  
Timeout 60  
  
KeepAlive On  
  
MaxKeepAliveRequests 100  
  
KeepAliveTimeout 5  
  
# Additional security measures  
  
TraceEnable Off
```

Deliverable:



```
httpd.conf X  
httpd.conf  
419 <Directory "${SRVROOT}/cgi-bin">  
429  
430  
431 Options -Indexes  
432 ServerSignature Off  
433 ServerTokens Prod  
434  
435 <LimitExcept GET POST>  
436 |     Deny from all  
437 </LimitExcept>  
438  
439  
440  
441
```

Secure MySQL:

Open MySQL console:

```
sql
```

```
ALTER USER 'root'@'localhost' IDENTIFIED BY 'NewStrongPassword123!';
```

```
DELETE FROM mysql.user WHERE User="";
```

```
FLUSH PRIVILEGES;
```

Task 2:

Implementing Basic Web Security (15 Marks)

- **PHP Hardening Edit:**

C:\wamp64\bin\php\php8.x.x\php.ini

Set:

```
ini
```

```
disable_functions = exec,passthru,shell_exec,system expose_php = Off
```

```
allow_url_fopen = Off session.cookie_httponly = 1 session.cookie_secure = 1
```

Deliverable: Snippet of modified php.ini

```

session.auto_start = 0
; Lifetime in seconds of stored session (if session was created by the
; https://php.net/session.cookie-lifetime
session.cookie_lifetime = 0

; The path for which the cookie is valid.
; https://php.net/session.cookie-path
session.cookie_path = /

; The domain for which the cookie is valid.
; https://php.net/session.cookie-domain
session.cookie_domain =

; Whether or not to add the httpOnly flag to the cookie, which makes it
; inaccessible to browser scripting languages such as JavaScript.
; https://php.net/session.cookie-httponly
session.cookie_httponly = 1

; Add SameSite attribute to cookie to help mitigate Cross-Site Request Forgery (CSRF/XSRF)
; Current valid values are "Strict", "Lax" or "None". When using "None",
; make sure to include the quotes, as 'none' is interpreted like 'false' in ini files.
; https://tools.ietf.org/html/draft-west-first-party-cookies-07
session.cookie_samesite =

; Handler used to serialize data. php is the standard serializer of PHP.
; https://php.net/session.serialize-handler

```

```

File Edit View
serialize_precision = -1
; open_basedir, if set, limits the file operations the script can perform
; and below. This directive makes most sense if used in a per-directory
; or per-virtualhost web server configuration file.
; Note: disables the realpath cache
; https://php.net/open-basedir
open_basedir =

; This directive allows you to disable certain functions.
; It receives a comma-delimited list of function names.
; https://php.net/disable-functions
disable_functions = exec,passthru,shell_exec,system

; This directive allows you to disable certain classes.
; It receives a comma-delimited list of class names.
; https://php.net/disable-classes
disable_classes =

; Colors for Syntax Highlighting mode. Anything that's acceptable in
; <span style="color: ???????"> would work.
; https://php.net/syntax-highlighting
;highlight.string = #000000
;highlight.comment = #FF9900
;highlight.keyword = #007700
;highlight.default = #000000
;highlight.html = #000000

```

```

package main
php.ini
time.now.

File Edit View
file_uploads = On

; Temporary directory for temporary files (if specified).
; https://php.net/upload-tmp-dir
upload_tmp_dir = "c:/wamp64/tmp"

; Maximum allowed size for uploaded files.
; https://php.net/upload-max-filesize
upload_max_filesize = 2M

; Maximum number of files that can be uploaded via a single request
max_file_uploads = 20

; Fopen wrappers ;

; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; https://php.net/allow-url-fopen
allow_url_fopen = Off

; Whether to allow include/require to open URLs (like https:// or ftp://) as files.
; https://php.net/allow-url-include
allow_url_include = Off

; Define the anonymous ftp password (your email address). PHP's default setting

; This has no effect when zend.exception_ignore_args is enabled.
; Default Value: 15
; Development Value: 15
; Production Value: 0
zend.exception_string_param_max_len = 15

; Miscellaneous ;

; Decides whether PHP may expose the fact that it is installed on the server
; (e.g. by adding its signature to the Web server header). It is no security
; threat in any way, but it makes it possible to determine whether you use PHP
; on your server or not.
; https://php.net/expose-php
expose_php = Off

; Resource Limits ;

; Maximum execution time of each script, in seconds
; https://php.net/max-execution-time
; Note: This directive is hardcoded to 0 for the CLI SAPI
max_execution_time = 120

; https://php.net/session.cookie-secure
; session.cookie_secure = 1

; This option forces PHP to fetch and use a cookie for storing and maintaining
; the session id. We encourage this operation as it's very helpful in combating
; session hijacking when not specifying and managing your own session id. It is
; not the be-all and end-all of session hijacking defense, but it's a good start.
; https://php.net/session.use-only-cookies
session.use_only_cookies = 1

; Name of the session (used as cookie name).
; https://php.net/session.name
session.name = PHPSESSID

; Initialize session on request startup.
; https://php.net/session.auto-start
session.auto_start = 0

; Lifetime in seconds of cookie or, if 0, until browser is restarted.

```

Ln 1410, Col 23 13 of 74,573 characters 100% Windows (CRLF) UTF-8

[illegible]

```
openssl.cnf X
openssl.cnf
388 # Certificate revocation
389 cmd = rr
390 oldcert = $insta::certout # insta.cert.pem
391
392
393 SSLEngine on
394 SSLCertificateFile "C:/wamp64/bin/apache/apache2.4.62.1/conf/localhost.crt"
395 SSLCertificateKeyFile "C:/wamp64/bin/apache/apache2.4.62.1/conf/localhost.key"
396
```

Security Headers:

Add to Apache config:

apache

Header always set X-Frame-Options "DENY"

Header always set X-Content-Type-Options "nosniff"

Header always set Content-Security-Policy "default-src 'self'"

```
httpd.conf X openssl.cnf
httpd.conf
597
598
599 Header always set X-Frame-Options "DENY"
600 Header always set X-Content-Type-Options "nosniff"
601 Header always set Content-Security-Policy "default-src 'self'"
602 Header always set X-XSS-Protection "1; mode=block"
```

Task 3:

Vulnerability Testing & Mitigation (15 Marks)

Install DVWA:

Download & extract to :

C:\wamp64\www\dvwa

Edit config/config.inc.php:

php

```
$_DVWA['db_password'] = 'NewStrongPassword123!';
```


Structure

SQL

Search

Query

Export

Import

Operations

Privileges

Routines

Events

Triggers

Designer

Filters

Containing the word:

Table	Action	Rows	Type	Collation	Size	Overhead
<input type="checkbox"/> guestbook	<div><div>★</div><div><div><div><div>Browse</div></div><div><div>Structure</div></div><div><div>Search</div></div><div><div>Insert</div></div><div><div>Empty</div></div><div><div>Drop</div></div></div></div></div>	1	MyISAM	utf8mb4_0900_ai_ci	2.0 KiB	-
<input type="checkbox"/> users	<div><div>★</div><div><div><div><div>Browse</div></div><div><div>Structure</div></div><div><div>Search</div></div><div><div>Insert</div></div><div><div>Empty</div></div><div><div>Drop</div></div></div></div></div>	5	MyISAM	utf8mb4_0900_ai_ci	2.4 KiB	-
2 tables	Sum	6	MyISAM	utf8mb4_0900_ai_ci	4.4 KiB	0 B

```
$_DVWA = array();
$_DVWA[ 'db_server' ] = getenv('DB_SERVER') ?: '127.0.0.1';
$_DVWA[ 'db_database' ] = getenv('DB_DATABASE') ?: 'dvwa';
$_DVWA[ 'db_user' ] = getenv('DB_USER') ?: 'dvwa';
$_DVWA[ 'db_password' ] = 'NewStrongPassword123!';
$_DVWA[ 'db_port' ] = getenv('DB_PORT') ?: '3306';
```

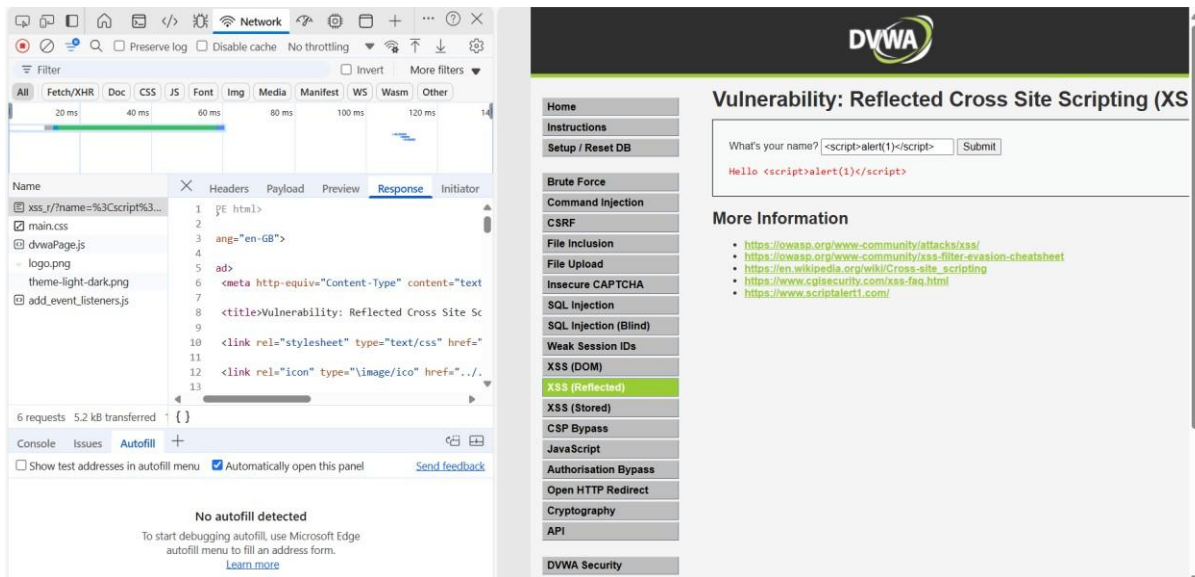
Test Vulnerabilities o Attempt:

SQL Injection: ' OR '1'='1

XSS: <script>alert(1)</script>

Check headers via browser dev tools.

The screenshot shows a web browser displaying the DVWA application. The browser's developer tools are open, showing the Network tab. The first request, 'sql/?id=%27+OR+%271%27%3D%271&Submit=Submit&user_token=a8b14cd02c377279a7f12c37cc404941#', is selected, and the 'Response' tab is active. The response is an HTML document with a title 'Vulnerability: SQL Injection :: Damn' and a link to the 'SQL Injection' page. The browser's address bar shows the URL: localhost/dvwa/vulnerabilities/sql/?id=%27+OR+%271%27%3D%271&Submit=Submit&user_token=a8b14cd02c377279a7f12c37cc404941#.



Mitigate SQLi:

php

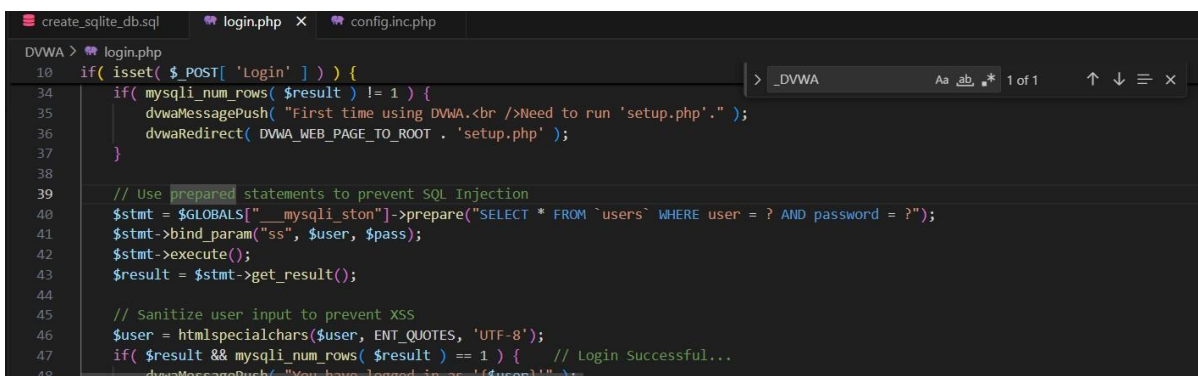
```
$stmt = $pdo->prepare("SELECT * FROM users WHERE user = ? AND password = ?");
```

```
$stmt->execute([$user, $pass]);
```

- **XSS: php CopyEdit echo htmlspecialchars(\$user_input, ENT_QUOTES, 'UTF-8');**

Deliverables:

- **Screenshots of blocked attempts**



Secure PHP snippets

Task 4: Advanced Security (10 Marks)

Web Application Firewall:

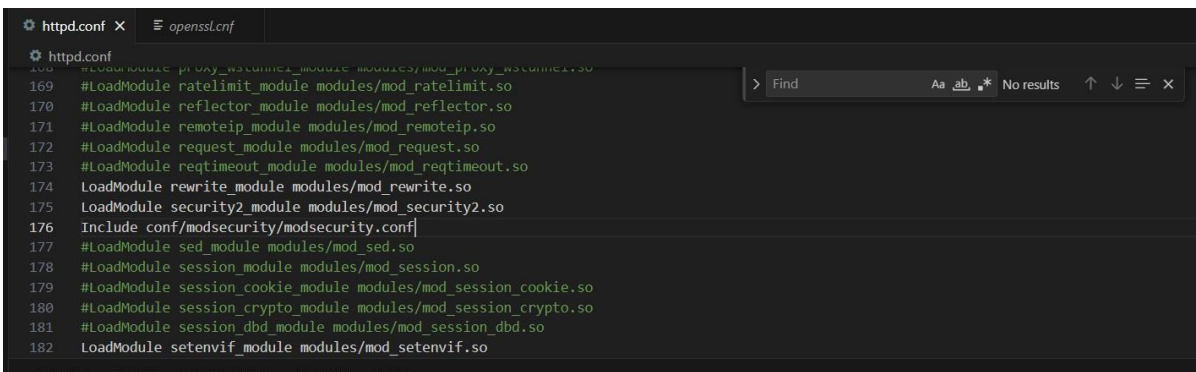
Download ModSecurity from [Apache Lounge](#)

Edit httpd.conf:

apache

LoadModule security2_module modules/mod_security2.so

Include conf/modsecurity/modsecurity.conf



```
168 #LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
169 #LoadModule ratelimit_module modules/mod_ratelimit.so
170 #LoadModule reflector_module modules/mod_reflector.so
171 #LoadModule remoteip_module modules/mod_remoteip.so
172 #LoadModule request_module modules/mod_request.so
173 #LoadModule reqtimeout_module modules/mod_reqtimeout.so
174 LoadModule rewrite_module modules/mod_rewrite.so
175 LoadModule security2_module modules/mod_security2.so
176 Include conf/modsecurity/modsecurity.conf
177 #LoadModule sed_module modules/mod_sed.so
178 #LoadModule session_module modules/mod_session.so
179 #LoadModule session_cookie_module modules/mod_session_cookie.so
180 #LoadModule session_crypto_module modules/mod_session_crypto.so
181 #LoadModule session_dbd_module modules/mod_session_dbd.so
182 LoadModule setenvif_module modules/mod_setenvif.so
```

Logging & Monitoring

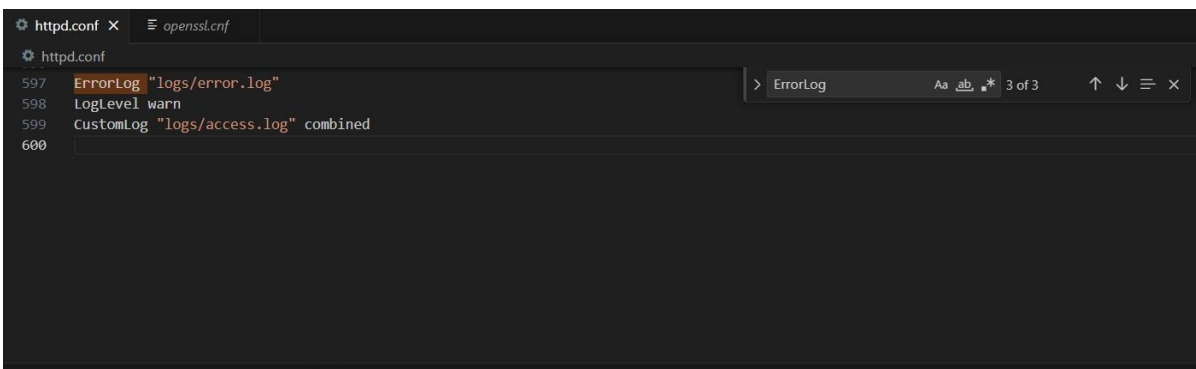
Add in Apache config:

apache

ErrorLog "logs/error.log"

LogLevel warn

CustomLog "logs/access.log" combined



```
597 ErrorLog "logs/error.log"
598 LogLevel warn
599 CustomLog "logs/access.log" combined
600
```

Deliverables:

Screenshot of ModSecurity blocking an attack

Sample entries from error.log or access.log