Future Interns Cyber Security Internship

Task 1: Web Application Security Testing

Name: Vivek Yadav
Track Code: CS
Task Number: 1
Internship Provider: Future Interns
Start Date: [30-07-2025] **End date:** [31-07-2025]

---

1. Introduction

This report outlines the process and findings of a web application penetration test conducted as part of Task 1 in the Cyber Security Internship with Future Interns. The main objective of this task was to identify common vulnerabilities like SQL Injection (SQLi), Cross-Site Scripting (XSS), and authentication flaws using industry-standard tools on a purposely vulnerable application.

---

2. Target Application

- **Application Used:** DVWA (Damn Vulnerable Web Application)
- **Environment:** XAMPP (Apache + MySQL + PHP)
- **Access:** Localhost on Kali Linux

---

3. Tools Used

Tool	Purpose
OWASP ZAP	Vulnerability scanning, XSS detection
Burp Suite	Proxy, manual testing, authentication flaws
SQLMap	SQL Injection testing
XAMPP	Localhost setup for DVWA

---

4. Vulnerabilities Found

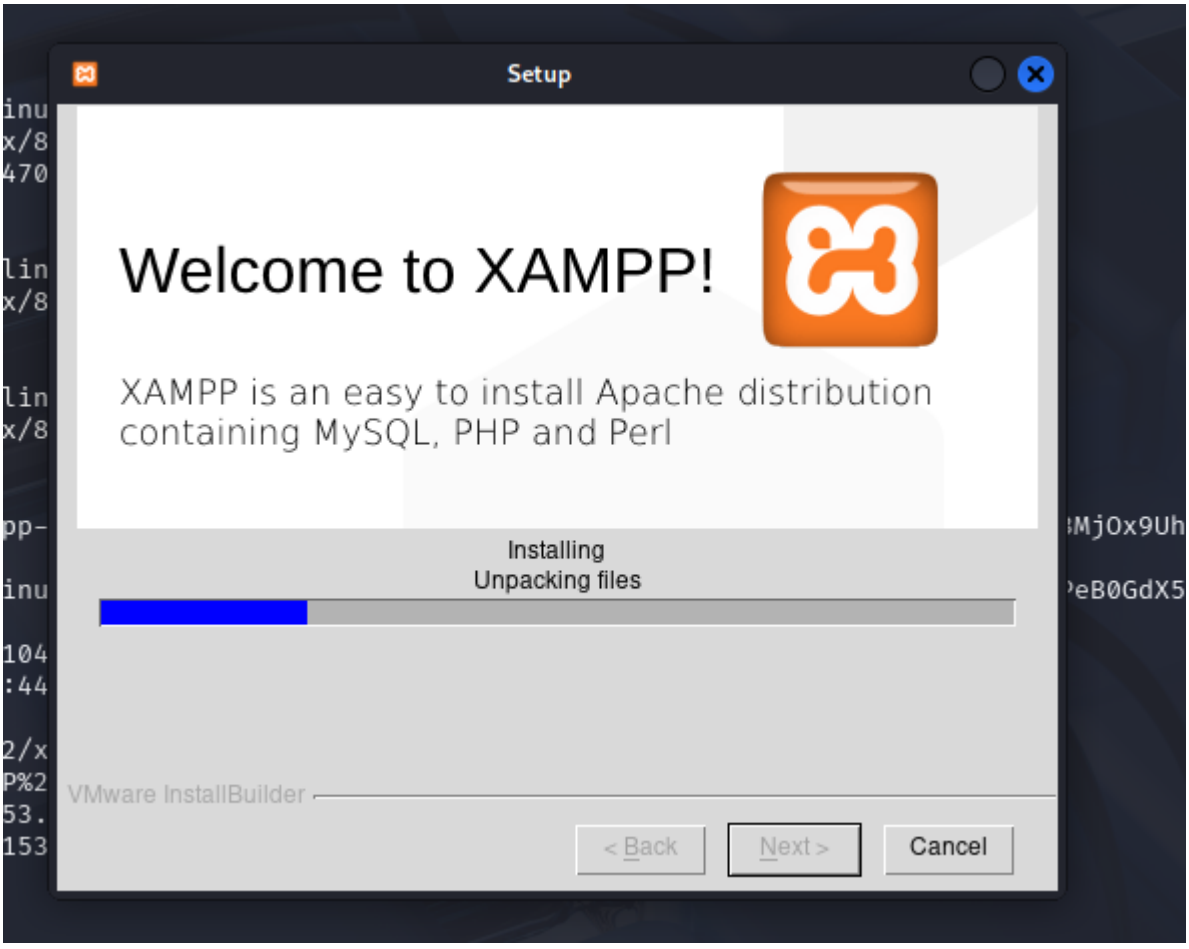
4.1 SQL Injection

- **Location:** Vulnerable page in DVWA
- **Tool Used:** SQLMap
- **Description:** SQL Injection vulnerability allowed retrieval of database schema.
- **Screenshot:**

```
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/digininja/DVWA.git
Cloning into 'DVWA'...
remote: Enumerating objects: 5373, done.
remote: Total 5373 (delta 0), reused 0 (delta 0), pack-reused 5373 (from 1)
Receiving objects: 100% (5373/5373), 2.57 MiB | 2.59 MiB/s, done.
Resolving deltas: 100% (2673/2673), done.
```

```
┌──(kali㉿kali)-[~]
└─$ wget https://sourceforge.net/projects/xampp/files/XAMPP%20Linux/8.2.12/xampp-linux-x64-8.2.12-0-insta
--2025-07-30 12:09:31--  https://sourceforge.net/projects/xampp/files/XAMPP%20Linux/8.2.12/xampp-linux-x6
Resolving sourceforge.net (sourceforge.net)... 104.18.13.149, 104.18.12.149, 2606:4700::6812:c95, ...
Connecting to sourceforge.net (sourceforge.net)|104.18.13.149|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://sourceforge.net/projects/xampp/files/XAMPP%20Linux/8.2.12/xampp-linux-x64-8.2.12-0-insta
--2025-07-30 12:09:32--  https://sourceforge.net/projects/xampp/files/XAMPP%20Linux/8.2.12/xampp-linux-x6
Reusing existing connection to sourceforge.net:443.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://sourceforge.net/projects/xampp/files/XAMPP%20Linux/8.2.12/xampp-linux-x64-8.2.12-0-insta
--2025-07-30 12:09:32--  https://sourceforge.net/projects/xampp/files/XAMPP%20Linux/8.2.12/xampp-linux-x6
Reusing existing connection to sourceforge.net:443.
HTTP request sent, awaiting response... 302 Found
Location: https://downloads.sourceforge.net/project/xampp/XAMPP%20Linux/8.2.12/xampp-linux-x64-8.2.12-0-i
=excellmedia&r= [following]
--2025-07-30 12:09:32--  https://downloads.sourceforge.net/project/xampp/XAMPP%20Linux/8.2.12/xampp-linux-
D%3D&use_mirror=excellmedia&r=
Resolving downloads.sourceforge.net (downloads.sourceforge.net)... 104.18.12.149, 104.18.13.149, 2606:470
Connecting to downloads.sourceforge.net (downloads.sourceforge.net)|104.18.12.149|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://excellmedia.dl.sourceforge.net/project/xampp/XAMPP%20Linux/8.2.12/xampp-linux-x64-8.2.1
--2025-07-30 12:09:33--  https://excellmedia.dl.sourceforge.net/project/xampp/XAMPP%20Linux/8.2.12/xampp-
Resolving excellmedia.dl.sourceforge.net (excellmedia.dl.sourceforge.net)... 202.153.32.19, 2401:fb00:0:1
Connecting to excellmedia.dl.sourceforge.net (excellmedia.dl.sourceforge.net)|202.153.32.19|:443... conne
HTTP request sent, awaiting response... 200 OK
Length: 160483784 (153M) [application/x-makeself]
Saving to: 'xampp-linux-x64-8.2.12-0-installer.run'

xampp-linux-x64-8.2.12-0-installer.run                    100%[===================================

2025-07-30 12:20:56 (229 KB/s) - 'xampp-linux-x64-8.2.12-0-installer.run' saved [160483784/160483784]
```

```
┌──(kali㉿kali)-[~]
└─$ wget https://sourceforge.net/projects/xampp/files/XAMPP%20Linux/8.2.12/xampp-linux-x64-8.2.12-0-installer.run
--2025-07-30 12:09:31--  https://sourceforge.net/projects/xampp/files/XAMPP%20Linux/8.2.12/xampp-linux-x64-8.2.12-
Resolving sourceforge.net (sourceforge.net)... 104.18.13.149, 104.18.12.149, 2606:4700::6812:c95, ...
Connecting to sourceforge.net (sourceforge.net)|104.18.13.149|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://sourceforge.net/projects/xampp/files/XAMPP%20Linux/8.2.12/xampp-linux-x64-8.2.12-0-installer.run
--2025-07-30 12:09:32--  https://sourceforge.net/projects/xampp/files/XAMPP%20Linux/8.2.12/xampp-linux-x64-8.2.12-
Reusing existing connection to sourceforge.net:443.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://sourceforge.net/projects/xampp/files/XAMPP%20Linux/8.2.12/xampp-linux-x64-8.2.12-0-installer.run
--2025-07-30 12:09:32--  https://sourceforge.net/projects/xampp/files/XAMPP%20Linux/8.2.12/xampp-linux-x64-8.2.12-
Reusing existing connection to sourceforge.net:443.
HTTP request sent, awaiting response... 302 Found
Location: https://downloads.sourceforge.net/project/xampp/XAMPP%20Linux/8.2.12/xampp-linux-x64-8.2.12-0-installer.
=excellmedia&r= [following]
--2025-07-30 12:09:32--  https://downloads.sourceforge.net/project/xampp/XAMPP%20Linux/8.2.12/xampp-linux-x64-8.2.
D%3D&use_mirror=excellmedia&r=
Resolving downloads.sourceforge.net (downloads.sourceforge.net)... 104.18.12.149, 104.18.13.149, 2606:4700::6812:d
Connecting to downloads.sourceforge.net (downloads.sourceforge.net)|104.18.12.149|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://excellmedia.dl.sourceforge.net/project/xampp/XAMPP%20Linux/8.2.12/xampp-linux-x64-8.2.12-0-insta
--2025-07-30 12:09:33--  https://excellmedia.dl.sourceforge.net/project/xampp/XAMPP%20Linux/8.2.12/xampp-linux-x64
Resolving excellmedia.dl.sourceforge.net (excellmedia.dl.sourceforge.net)... 202.153.32.19, 2401:fb00:0:1fe:8000::
Connecting to excellmedia.dl.sourceforge.net (excellmedia.dl.sourceforge.net)|202.153.32.19|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 160483784 (153M) [application/x-makeself]
Saving to: 'xampp-linux-x64-8.2.12-0-installer.run'

xampp-linux-x64-8.2.12-0-installer.run                    100%[===================================================

2025-07-30 12:20:56 (229 KB/s) - 'xampp-linux-x64-8.2.12-0-installer.run' saved [160483784/160483784]
```



```
┌──(kali㉿kali)-[~]
└─$ sudo cp /opt/lampp/htdocs/DVWA/config/config.inc.php.dist /opt/lampp/htdocs/DVWA/config/config.inc.php

┌──(kali㉿kali)-[~]
└─$ sudo chmod -R 755 /opt/lampp/htdocs/DVWA

┌──(kali㉿kali)-[~]
└─$ sudo /opt/lampp/lampp restart
Restarting XAMPP for Linux 8.2.12-0 ...
XAMPP: Stopping Apache ... ok.
XAMPP: Stopping MySQL ... ok.
XAMPP: Stopping ProFTPD ... ok.
XAMPP: Starting Apache ... ok.
XAMPP: Starting MySQL ... ok.
XAMPP: Starting ProFTPD ... ok.
```

```
┌──(kali㉿kali)-[~]
└─$ chmod +x xampp-linux-x64-8.2.12-0-installer.run

┌──(kali㉿kali)-[~]
└─$ sudo ./xampp-linux-x64-8.2.12-0-installer.run
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ sudo mv ~/DVWA /opt/lampp/htdocs/
```

Setup DVWA

Instructions

About

Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: **/opt/lampp/htdocs/DVWA/config/config.inc.php**

If the database already exists, **it will be cleared and the data will be reset**.
You can also use this to reset the administrator credentials ("**admin** // **password**") at any stage.

Setup Check

General
Operating system: ***nix**

DVWA version:

- Git reference: **c6e3d05c503cc6c02feccfe78cab5b4b747ba83d**
- Author: Robin Wood

reCAPTCHA key: **Missing**

Writable folder /opt/lampp/htdocs/DVWA/hackable/uploads/: **No**
Writable folder /opt/lampp/htdocs/DVWA/config: **No**

Apache
Web Server SERVER_NAME: **localhost**

mod_rewrite: **Not Enabled**
mod_rewrite is required for the AP labs.

PHP
PHP version: **8.2.12**
PHP function display_errors: **Disabled**
PHP function display_startup_errors: **Enabled**
PHP function allow_url_include: **Disabled**
PHP function allow_url_fopen: **Enabled**
PHP module gd: **Installed**
PHP module mysql: **Installed**
PHP module pdo_mysql: **Installed**

Database
Backend database: **MySQL/MariaDB**
Database username: **dvwa**
Database password: ******
Database database: **dvwa**
Database host: **127.0.0.1**
Database port: **3306**

API
This section is only important if you want to use the API module.
Vendor files installed: **Not Installed**

For information on how to install these, see the **README**.

***Status in red**, indicate there will be an issue when trying to complete some modules.*

If you see disabled on either *allow_url_fopen* or *allow_url_include*, set the following in your php.ini file and restart Apache.

```
allow_url_fopen = On
allow_url_include = On
```

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

Create / Reset Database

localhost/DVWA/login.php

ocs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

DVWA

Username

Password

Login

DVWA

Home
Instructions
Setup / Reset DB

Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
Cryptography
API

DVWA Security
PHP Info
About

Logout

Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerabilities**, with **various levels of difficultly**, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerabilities** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

WARNING!

Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any Internet facing servers**, as they will be compromised. It is recommend using a virtual machine (such as VirtualBox or VMware), which is set to NAT networking mode. Inside a guest machine, you can download and install XAMPP for the web server and database.

Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

More Training Resources

DVWA aims to cover the most commonly seen vulnerabilities found in today's web applications. However there are plenty of other issues with web applications. Should you wish to explore any additional attack vectors, or want more difficult challenges, you may wish to look into the following other projects:

- Mutillidae
- OWASP Vulnerable Web Applications Directory

DVWA Security

Security Level

Security level is currently: **impossible**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
   Prior to DVWA v1.9, this level was known as 'high'.

Impossible Submit

DVWA

- Home
- Instructions
- Setup / Reset DB

- Brute Force
- Command Injection
- CSRF
- File Inclusion
- File Upload
- Insecure CAPTCHA
- SQL Injection
- SQL Injection (Blind)
- Weak Session IDs
- XSS (DOM)
- XSS (Reflected)
- XSS (Stored)
- CSP Bypass
- JavaScript
- Authorisation Bypass
- Open HTTP Redirect
- Cryptography
- API

- DVWA Security
- PHP Info
- About

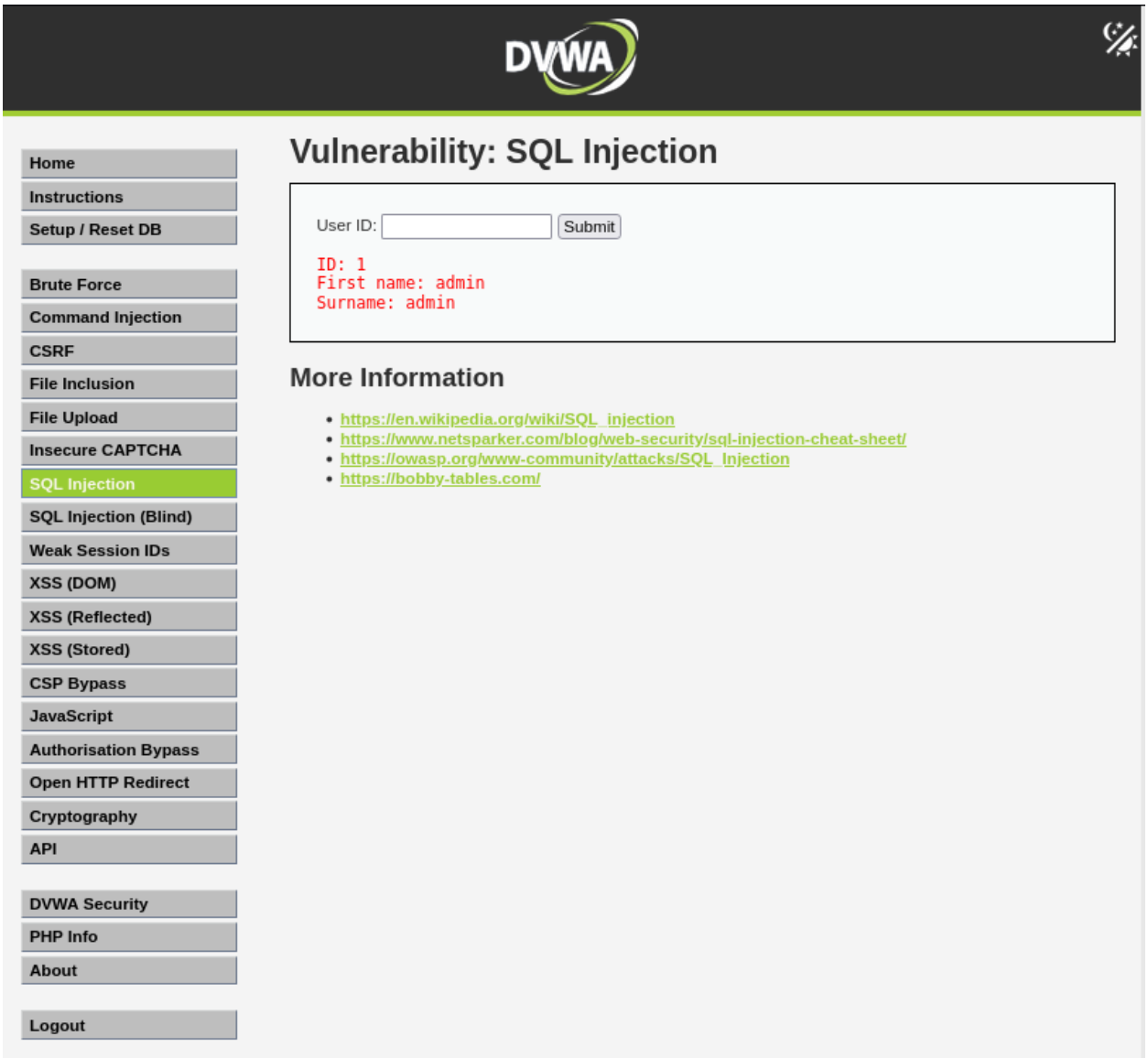
- Logout

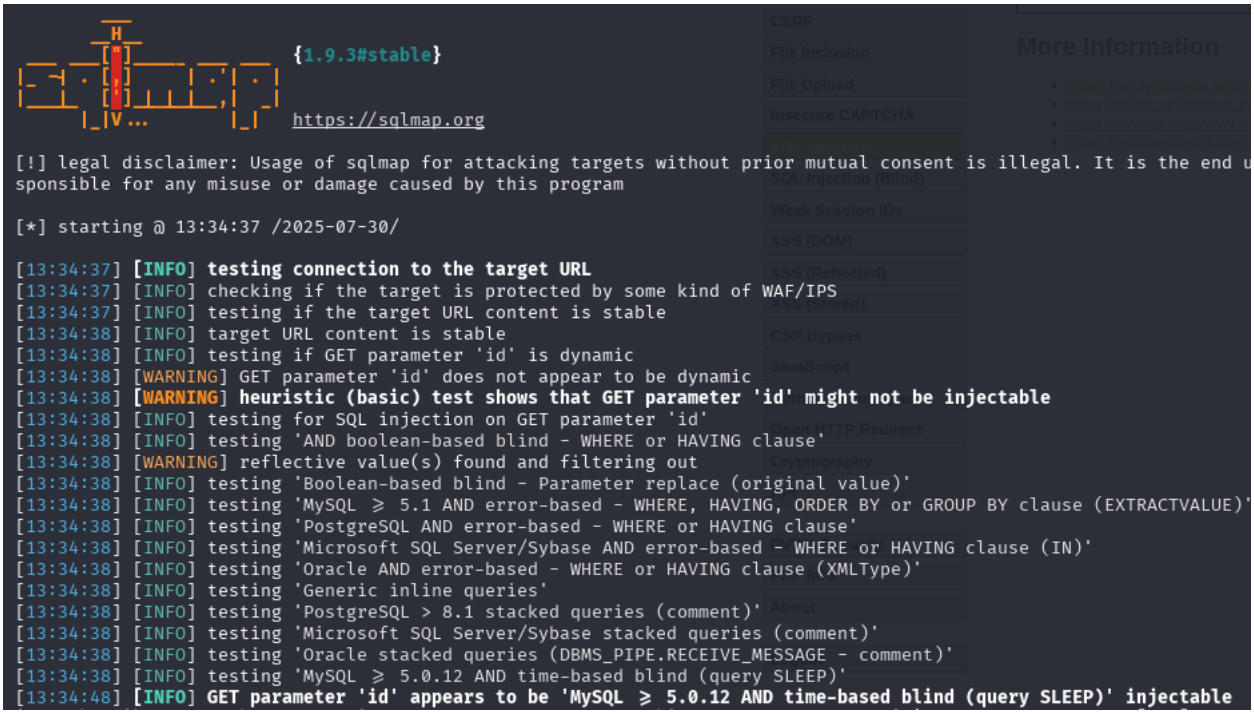
Vulnerability: SQL Injection

User ID: [ ] Submit

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
- https://owasp.org/www-community/attacks/SQL_Injection
- https://bobby-tables.com/

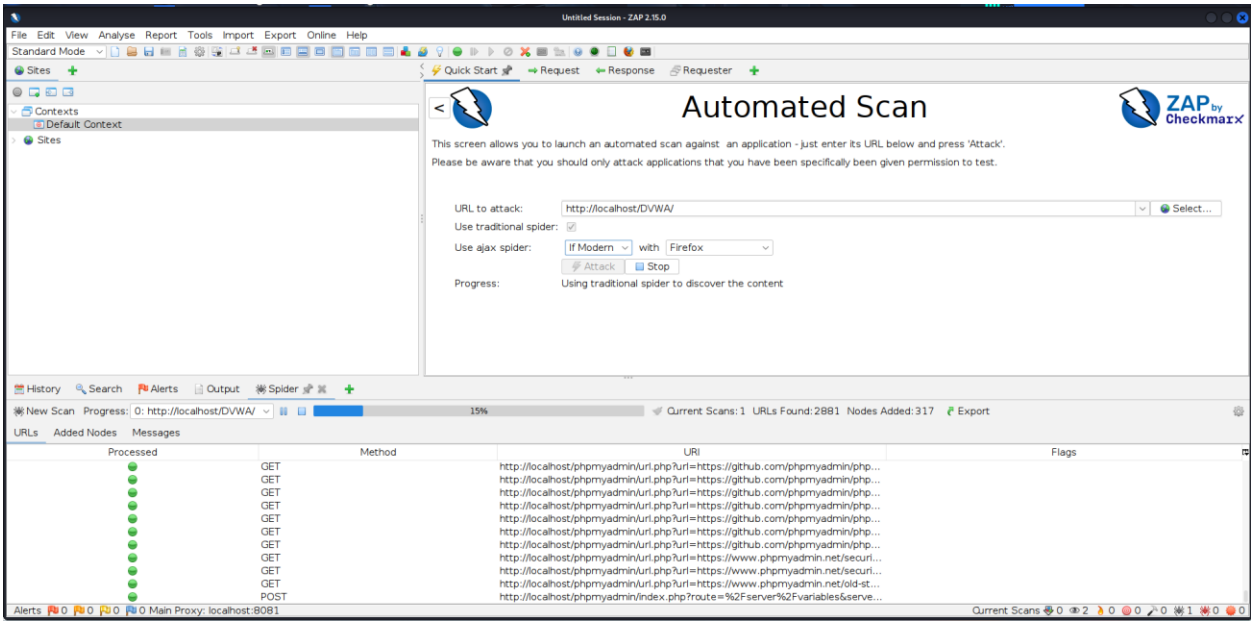

DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
Cryptography
API
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
ID: 1
First name: admin
Surname: admin
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/

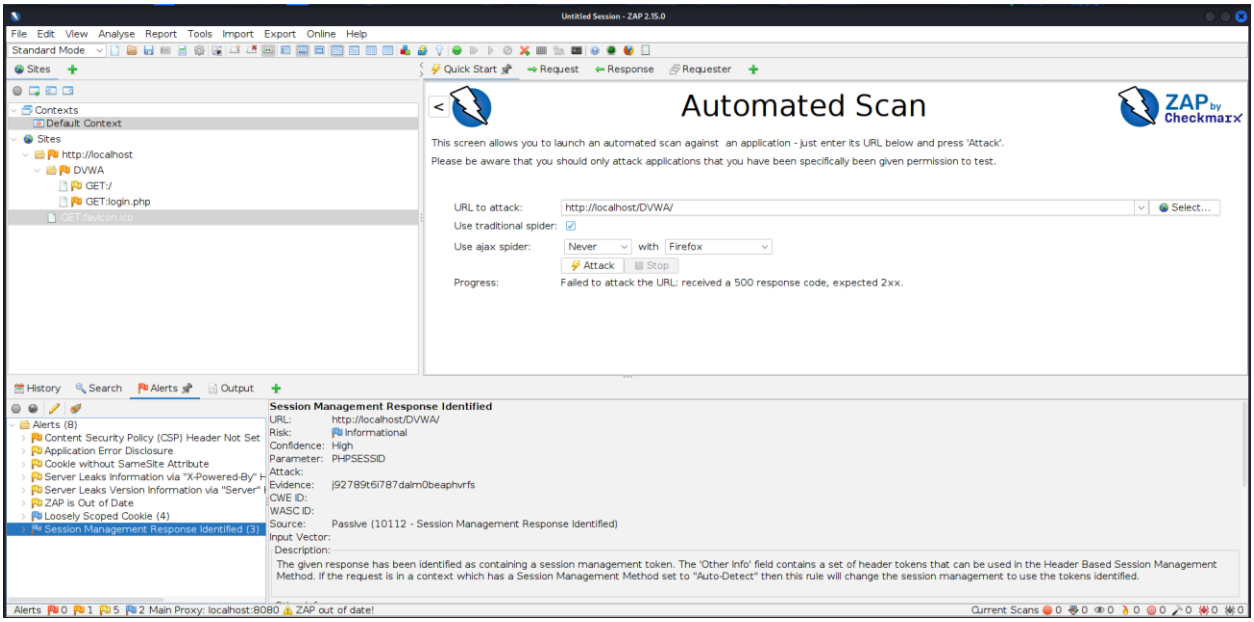


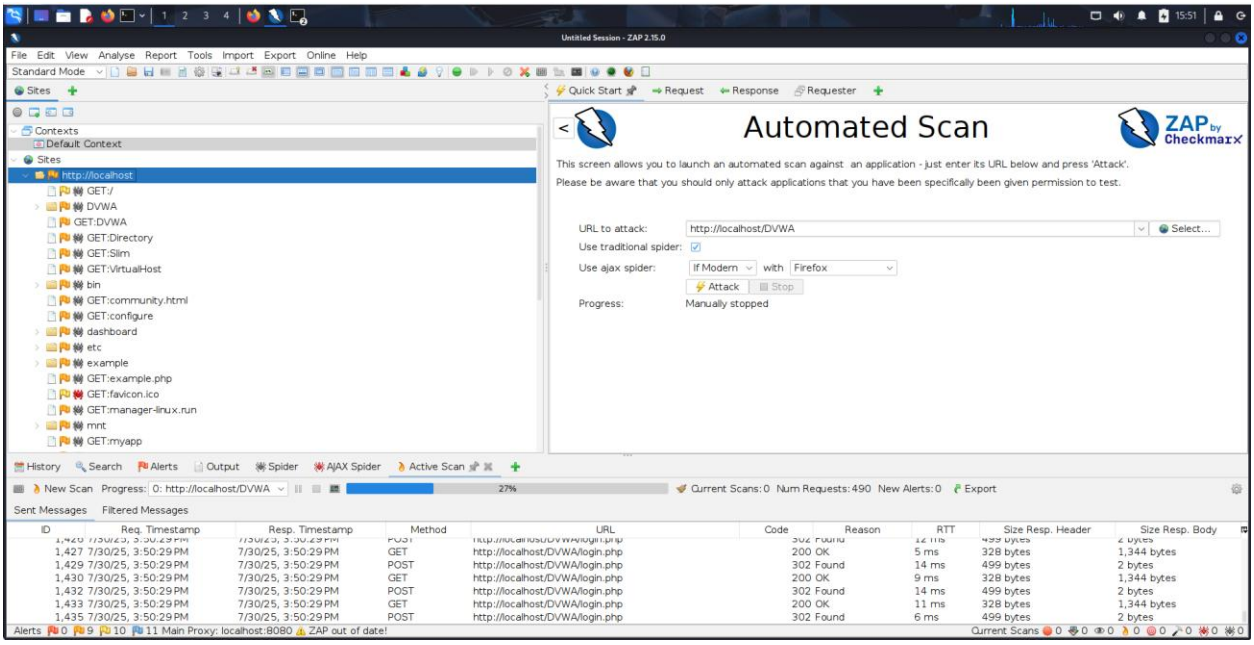
- **Remediation:** Use parameterized queries and input validation.

4.2 Cross-Site Scripting (XSS)

- **Location:** Comment input field in DVWA
- **Tool Used:** OWASP ZAP
- **Description:** Injected script alert was executed in the browser.
- **Screenshot:**







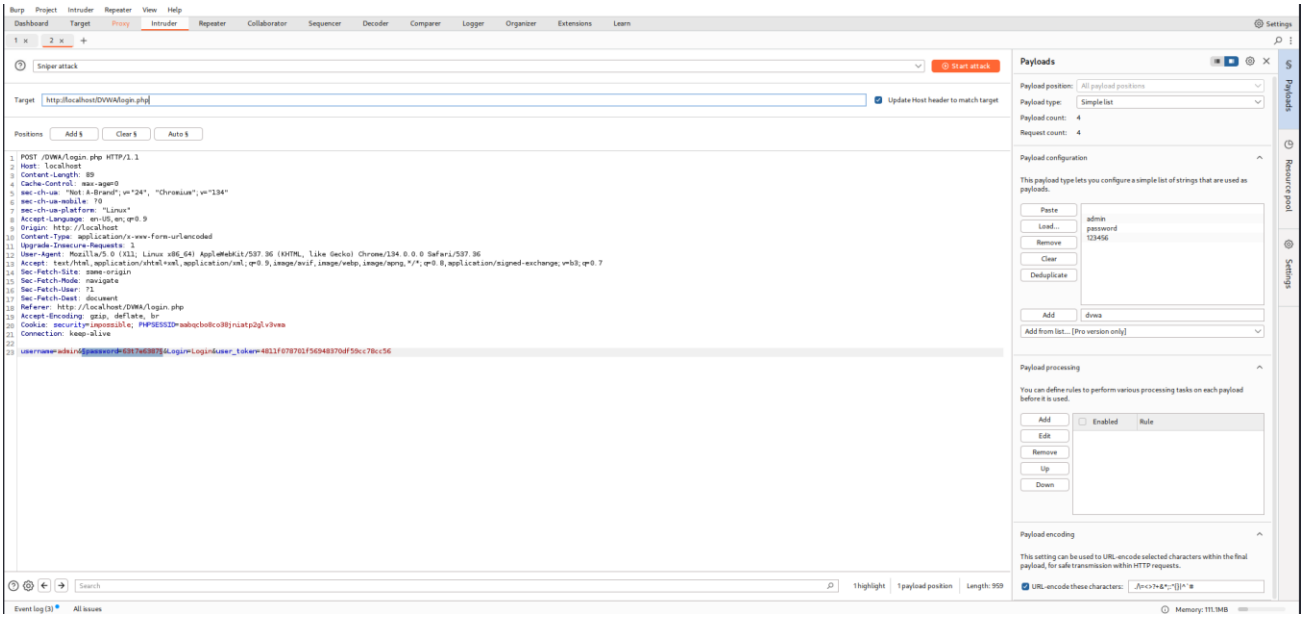
2025-07-30-ZAP-Report-.html

(As not able to see that original format in firefox but see clearly all reports and the alerts)

- **Remediation:** Encode output, use Content Security Policy (CSP).

4.3 Weak Authentication

- **Location:** Login Page
- **Tool Used:** Burp Suite (Intruder)
- **Description:** Brute-force attack revealed weak password.
- **Screenshot:**



3. Intruder attack of http://localhost/DVWA/login.php

Attack Save

3. Intruder attack of http://localhost/DVWA/login.php

Attack Save

Results Positions

Capture filter: Capturing all items

Apply capture filter

View filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0		302	27			557	
1		302	4			556	
2	admin	302	17			557	
3	password	302	3			556	
4	123456	302	35			557	

Payloads

Resource pool

Settings

Request Response

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Match and replace Proxy settings

Intercept on Forward Drop

Time	Type	Direction	Method	URL
14:03:55 30 Jul 2025	HTTP	→ Request	POST	http://localhost/DVWA/login.php
14:04:13 30 Jul 2025	HTTP	→ Request	POST	http://localhost/DVWA/login.php

Request

Pretty Raw Hex

```
POST /DVWA/login.php HTTP/1.1
Host: localhost
Content-Length: 86
Cache-Control: max-age=0
sec-ch-ua: "Not:A-Brand";v="24", "Chromium";v="134"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: en-US,en;q=0.9
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/DVWA/login.php
Accept-Encoding: gzip, deflate, br
Cookie: security=impossible; PHPSESSID=aabqcbo8co38jniatp2glv3vma
Connection: keep-alive
```

Search

Event log (3) All issues

- **Remediation:** Implement rate limiting and account lockout.

---

5. Learnings and Skills Gained

- Gained hands-on experience with real-world web vulnerabilities.
- Understood the use of tools like ZAP, Burp Suite, and SQLMap.
- Practiced writing a professional vulnerability report.
- Strengthened knowledge of OWASP Top 10 vulnerabilities.

---

6. Conclusion

This task helped reinforce core concepts in web application security. Using a controlled environment, I was able to identify and document serious vulnerabilities that often exist in poorly coded applications. The tools and techniques used here form the foundation of practical ethical hacking and penetration testing.

---

7. References

- DVWA GitHub
- OWASP ZAP
- Burp Suite
- SQLMap