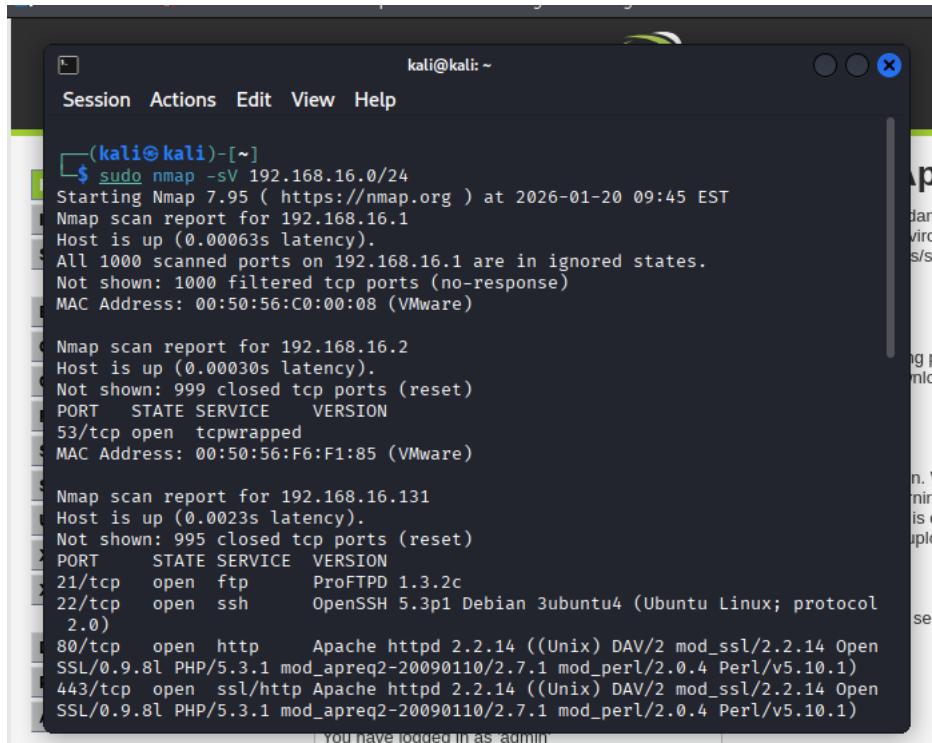


Prepared by: Otonye Iyalla

Assuming the attacker is sitting on the same network:

Other endpoints can be discovered by the attacker using nmap:



The screenshot shows a terminal window titled "kali@kali:~" running on Kali Linux. The user has run the command `sudo nmap -sV 192.168.16.0/24`. The output of the scan is displayed in three sections:

- Host 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)
- Host 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)
- Host 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)

The terminal window has a dark theme and includes a vertical sidebar on the right side.

The DVMA ip is discovered and logged in:

192.168.16.131/index.php

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

DVWA

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 DVWA 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:

The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The top navigation bar has the DVWA logo. On the left is a sidebar with links: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security (which is highlighted in green), PHP Info, About, and Logout. The main content area is titled "DVWA Security" with a padlock icon. It says "Script Security". Below that, it states "Security Level is currently **high**". A note says "You can set the security level to low, medium or high." Another note says "The security level changes the vulnerability level of DVWA." A dropdown menu for "Security Level" is open, showing "high" (selected), "low" (highlighted in blue), "medium", and "high". A note about PHPIDS says "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." It also says "PHPIDS is currently **disabled**. [[enable PHPIDS](#)]". At the bottom of the content area, there are links "[Simulate attack]" and "[View IDS log]". At the very bottom of the page, it displays "Username: admin", "Security Level: high", and "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:

More info

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

DVWA Security

PHP Info

About

Logout

Username: admin
 Security Level: low
 PHPIDS: disabled

[View Source](#) [View Help](#)

3. File Injection:

Using a simple php shell

The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The URL in the address bar is 192.168.16.131/vulnerabilities/upload/#. The top navigation bar includes links to Docs, Kali Forums, Kali NetHunter, Exploit-DB, and Google Hacking DB. The main title is "Vulnerability: File Upload". On the left, a sidebar menu lists various security modules: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload (which is highlighted in green), XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. Below the sidebar, user information is displayed: Username: admin, Security Level: low, PHPIDS: disabled. At the bottom right are "View Source" and "View Help" buttons. The main content area shows a form for uploading files, with a message indicating that ".../.../hackable/uploads/shell.php successfully uploaded!"

We can now run commands through the link

The screenshot shows a browser window with the URL 192.168.16.131/hackable/uploads/shell.php?cmd=ls. The browser's address bar also shows the full URL 192.168.16.131/hackable/uploads/shell.php. The top navigation bar is identical to the DVWA interface. The page content displays the output of the command ls, which includes "dwva_email.png group7.php shell.php".

4. SQL Injection:

Using simple SQL injection commands

DVWA

Vulnerability: SQL Injection

User ID:

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>

Menu:

- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection**
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored

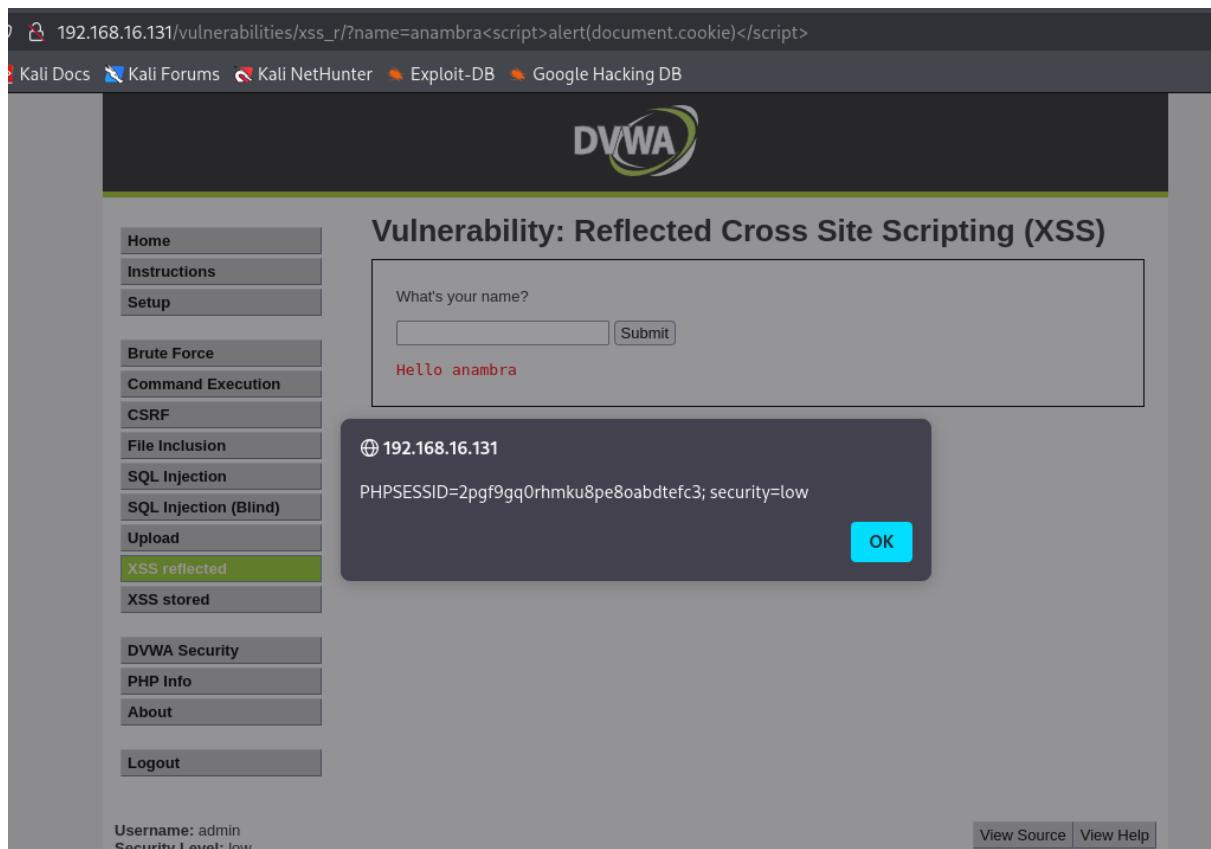
Information:

- DVWA Security
- PHP Info
- About

[Logout](#)

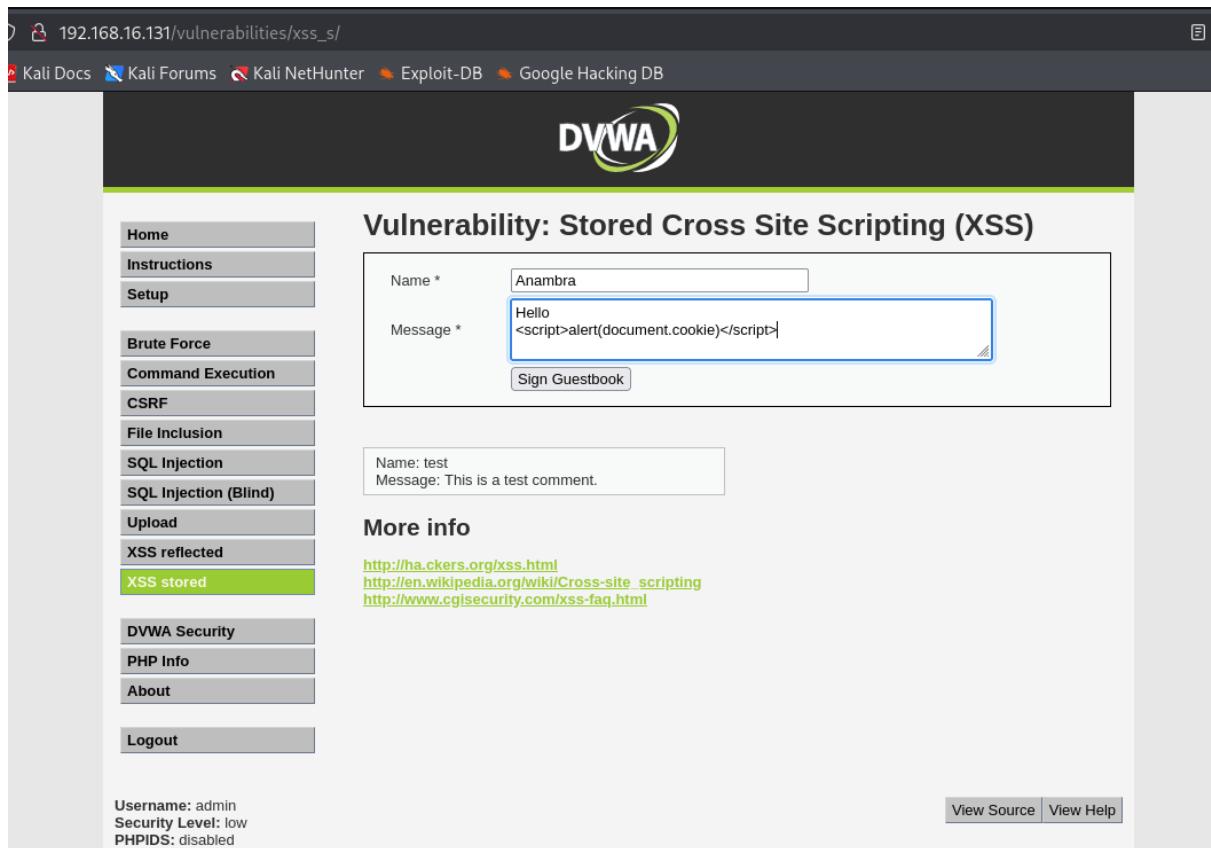
5. XSS

Reflected XSS to obtain the session cookie



The screenshot shows the DVWA application interface. On the left, a sidebar menu lists various security vulnerabilities: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected (highlighted in green), and XSS stored. Below this is a navigation bar with links to Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, and Google Hacking DB. The main content area has a title "Vulnerability: Reflected Cross Site Scripting (XSS)". It contains a form field labeled "What's your name?" with a red placeholder "Hello anambra". Below the form is a modal dialog box with the IP address "192.168.16.131" and the session ID "PHPSESSID=2pgf9gq0rhmkku8pe8oabdtefc3; security=low". A blue "OK" button is at the bottom right of the dialog. At the bottom of the page, it says "Username: admin" and "Security Level: low".

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



The screenshot shows the DVWA application interface. The sidebar menu is identical to the previous one, with "XSS reflected" highlighted in green. The main content area has a title "Vulnerability: Stored Cross Site Scripting (XSS)". It contains a form for a guestbook entry. The "Name *" field is filled with "Anambra". The "Message *" field contains the XSS payload "Hello <script>alert(document.cookie)</script>". Below the form is a preview section showing a guestbook entry from "Name: test" with the message "Message: This is a test comment.". A "Sign Guestbook" button is visible. At the bottom of the page, it says "Username: admin", "Security Level: low", and "PHPIDS: disabled".

The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. On the left, a sidebar lists various attack types: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, and XSS stored (which is highlighted). Below this are links to DVWA Security, PHP Info, About, and Logout. At the bottom of the sidebar, it says "Username: admin", "Security Level: low", and "PHPIDS: disabled". The main content area has a title "Vulnerability: Stored Cross Site Scripting (XSS)". It contains a form with fields for "Name *" (set to "Anambra") and "Message *" (containing "<Hello><script>alert(document.cookie)</script>"). A "Sign Guestbook" button is present. A modal dialog box is displayed with the IP address "192.168.16.131" and the message "PHPSESSID=2pgf9gg0rhmu8pe8oabdtefc3; security=low". Below the message are three links: <http://ha.ckers.org/xss.html>, http://en.wikipedia.org/wiki/Cross-site_scripting, and <http://www.cgisecurity.com/xss-faq.html>. An "OK" button is at the bottom right of the modal. At the very bottom right of the main content area are "View Source" and "View Help" buttons.

This screenshot shows the same DVWA XSS stored page as above, but with two messages visible in the list. The first message is from "Name: test" with the message "Message: This is a test comment.". The second message is from "Name: Anambra" with the message "Message: Hello". Below the messages, there is a section titled "More info" containing the same three links as the previous screenshot: <http://ha.ckers.org/xss.html>, http://en.wikipedia.org/wiki/Cross-site_scripting, and <http://www.cgisecurity.com/xss-faq.html>.

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