

# **Cyber Security Task 1**

## **Web Application Security Testing**

**Prepared By**

Aditya Sutar

### **Manual Security Testing Findings**

Important screenshots demonstrating SQL Injection, XSS, Command Injection, Burp Suite, and ZAP scanning.

# Screenshot\_2025-11-28\_11\_44\_17.png



## Service Unavailable

The server is temporarily unable to service your request due to maintenance downtime or capacity problems. Please try again later.

---

Apache/2.4.65 (Debian) Server at localhost Port 80

# Screenshot\_2025-11-28\_11\_44\_57.png

```

Session Actions Edit View Help
Built by Debian
Zend Engine v4.4.11, Copyright (c) Zend Technologies
with Zend OPcache v8.4.11, Copyright (c), by Zend Technologies

(jerry@jerry)-[~]
└─$ apache2ctl -M | grep -i php || true

AH00558: apache2: Could not reliably determine the server's fully qualified d
omain name, using 127.0.1.1. Set the 'ServerName' directive globally to supp
ress this message
PHP module (shared)

(jerry@jerry)-[~]
└─$ curl -sI http://localhost/info.php

HTTP/1.1 404 Not Found
Date: Fri, 28 Nov 2025 06:12:48 GMT
Server: Apache/2.4.65 (Debian)
Content-Type: text/html; charset=iso-8859-1

(jerry@jerry)-[~]
└─$ sudo a2enmod php
sudo systemctl restart apache2
apache2ctl -M | grep -i php || true
curl -sI http://localhost/info.php

Considering dependency mpm_prefork for php8.4:
Considering conflict mpm_event for mpm_prefork:
Considering conflict mpm_worker for mpm_prefork:
Module mpm_prefork already enabled
Considering conflict php5 for php8.4:
Module php8.4 already enabled
AH00558: apache2: Could not reliably determine the server's fully qualified d
omain name, using 127.0.1.1. Set the 'ServerName' directive globally to supp
ress this message
PHP module (shared)
HTTP/1.1 404 Not Found
Date: Fri, 28 Nov 2025 06:13:00 GMT
Server: Apache/2.4.65 (Debian)
Content-Type: text/html; charset=iso-8859-1

(jerry@jerry)-[~]
└─$ sudo apt install -y php-fpm
sudo a2enmod proxy_fcgi setenvif
sudo a2enconf php-fpm || true
sudo systemctl restart apache2
curl -sI http://localhost/info.php

Installing:
php-fpm

Installing dependencies:
php8.4-fpm

Suggested packages:
php-pear

Summary:
Upgrading: 0, Installing: 2, Removing: 0, Not Upgrading: 1224
```

This screenshot shows a key exploitation step during DVWA testing.

# Screenshot\_2025-11-28\_11\_50\_56.png

```
Session Actions Edit View Help
jerry@jerry:~$ sudo systemctl start php8.4-fpm
jerry@jerry:~$ sudo systemctl enable php8.4-fpm
jerry@jerry:~$ sudo systemctl status php8.4-fpm --no-pager -n 30

Synchronizing state of php8.4-fpm.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable php8.4-fpm
● php8.4-fpm.service - The PHP 8.4 FastCGI Process Manager
   Loaded: loaded (/usr/lib/systemd/system/php8.4-fpm.service; enabled; preset: disabled)
   Active: active (running) since Fri 2025-11-28 11:45:37 IST; 4min 8s ago
     Invocation: 1b466ed0d904722e1da37226c0ca27
       Docs: man:php-fpm8.4(8)
     Main PID: 19185 (php-fpm8.4)
    Status: "Processes active: 0, idle: 2, Requests: 4, slow: 0, Traffic: 0.00req/sec"
      Tasks: 3 (limit: 5073)
     Memory: 14.1M (peak: 14.7M)
        CPU: 110ms
     CGroup: /system.slice/php8.4-fpm.service
             └─19186 "php-fpm: master process (/etc/php/8.4/fpm/php-fpm.conf)"
               └─19186 "php-fpm: pool www"
                 └─19187 "php-fpm: pool www"

Nov 28 11:45:36 Jerry systemd[1]: Starting php8.4-fpm.service - The PHP 8.4 FastCGI Process Manager...
Nov 28 11:45:37 Jerry systemd[1]: Started php8.4-fpm.service - The PHP 8.4 FastCGI Process Manager.

jerry@jerry:~$ sudo systemctl status php8.4-fpm
jerry@jerry:~$ sudo systemctl restart apache2
jerry@jerry:~$ sudo systemctl status apache2 --no-pager -n 20

Conf php8.4-fpm already enabled
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: active (running) since Fri 2025-11-28 11:49:58 IST; 28ms ago
     Invocation: 67b05fc007a54ba5ee025514b269f6d
       Docs: https://httpd.apache.org/docs/2.4/
     Process: 21967 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
    Main PID: 21970 (apache2)
      Tasks: 1 (limit: 5073)
     Memory: 12.4M (peak: 12.4M)
        CPU: 57ms
     CGroup: /system.slice/apache2.service
             └─21970 /usr/sbin/apache2 -k start
               └─21977 /usr/sbin/apache2 -k start
                 └─21978 /usr/sbin/apache2 -k start

Nov 28 11:49:58 Jerry systemd[1]: Starting apache2.service - The Apache HTTP Server...
Nov 28 11:49:58 Jerry apachectl[21969]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.0.1. Set the 'ServerName' directive globally to suppress this message
Nov 28 11:49:58 Jerry systemd[1]: Started apache2.service - The Apache HTTP Server.

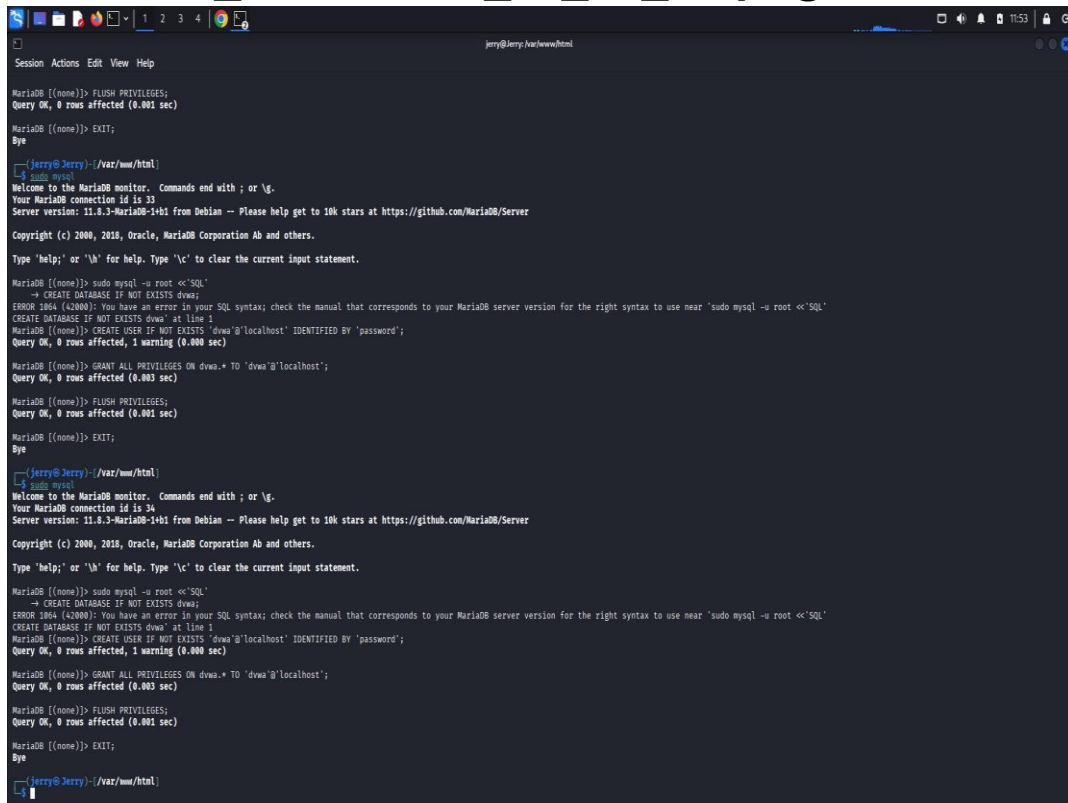
jerry@jerry:~$ echo $(php phpinfo()); >> | sudo tee /var/www/html/info.php > /dev/null
curl -i http://localhost/info.php

HTTP/1.1 200 OK
Date: Fri, 28 Nov 2025 06:28:08 GMT
Server: Apache/2.4.65 (Debian)
Content-Type: text/html; charset=UTF-8

jerry@jerry:~$
```

This screenshot shows a key exploitation step during DVWA testing.

# Screenshot\_2025-11-28\_11\_53\_43.png



```
Session Actions Edit View Help

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> EXIT;
Bye

--(jerry@jerry)-:/var/www/html
--$ sudo mysql
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 33
Server version: 11.6.3-MariaDB-1xb1 from Debian -- Please help get to 10k stars at https://github.com/MariaDB/Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> sudo mysql -u root <<'SQL'
=> CREATE DATABASE IF NOT EXISTS dwa;
ERROR 1064 (42000): 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 'sudo mysql -u root <<'SQL'
CREATE DATABASE IF NOT EXISTS dwa' at line 1
MariaDB [(none)]> CREATE USER IF NOT EXISTS 'dwa'@'localhost' IDENTIFIED BY 'password';
Query OK, 0 rows affected, 1 warning (0.000 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON dwa.* TO 'dwa'@'localhost';
Query OK, 0 rows affected (0.003 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> EXIT;
Bye

--(jerry@jerry)-:/var/www/html
--$ sudo mysql
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 34
Server version: 11.6.3-MariaDB-1xb1 from Debian -- Please help get to 10k stars at https://github.com/MariaDB/Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> sudo mysql -u root <<'SQL'
=> CREATE DATABASE IF NOT EXISTS dwa;
ERROR 1064 (42000): 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 'sudo mysql -u root <<'SQL'
CREATE DATABASE IF NOT EXISTS dwa' at line 1
MariaDB [(none)]> CREATE USER IF NOT EXISTS 'dwa'@'localhost' IDENTIFIED BY 'password';
Query OK, 0 rows affected, 1 warning (0.000 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON dwa.* TO 'dwa'@'localhost';
Query OK, 0 rows affected (0.003 sec)

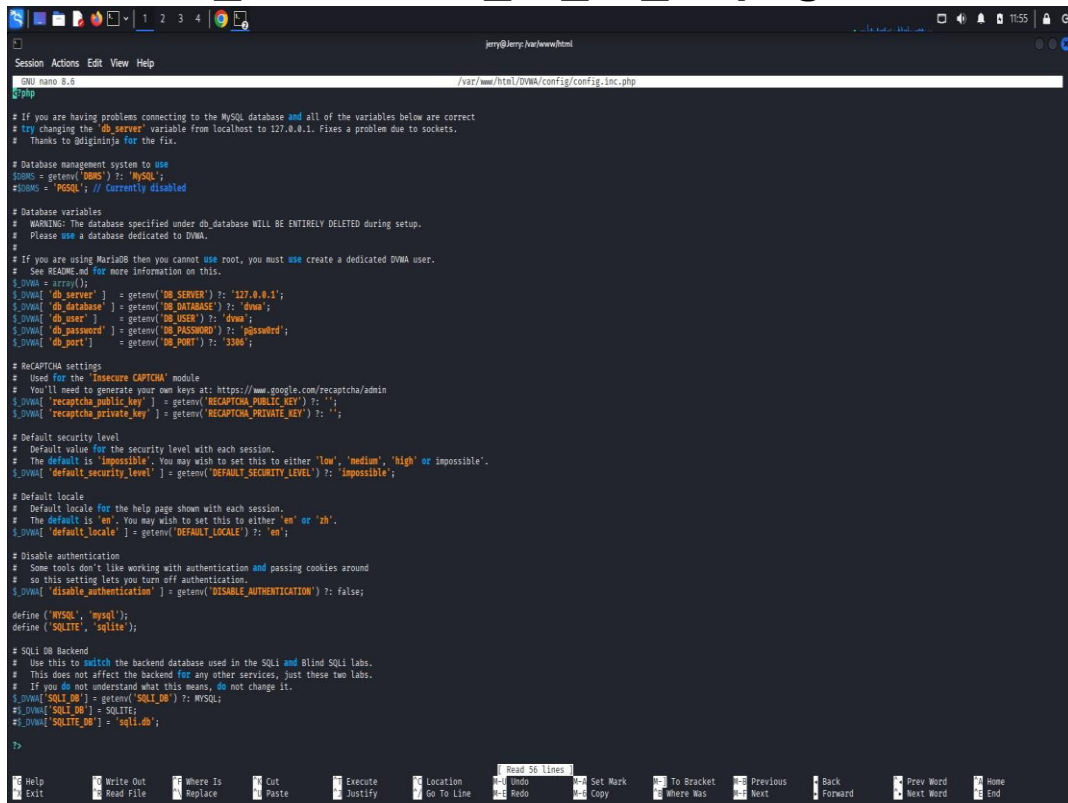
MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> EXIT;
Bye

--(jerry@jerry)-:/var/www/html
--$
```

This screenshot shows a key exploitation step during DVWA testing.

# Screenshot\_2025-11-28\_11\_55\_37.png



```
GNU nano 2.9.6 /var/www/html/DVWA/config/config.inc.php

<?php

# If you are having problems connecting to the MySQL database and all of the variables below are correct
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
# Thanks to @digininja for the fix.

# Database management system to use
$DBMS = getenv('DBMS') ? 'MySQL' :
$DBMS = 'MySQL'; // Currently disabled

# Database variables
# WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
# Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
# See README.md for more information on this.
$_DVWA = array();
$_DVWA['db_server'] = getenv('DB_SERVER') ? '127.0.0.1';
$_DVWA['db_database'] = getenv('DB_DATABASE') ? 'dvwa';
$_DVWA['db_user'] = getenv('DB_USER') ? 'dvwa';
$_DVWA['db_password'] = getenv('DB_PASSWORD') ? 'password';
$_DVWA['db_port'] = getenv('DB_PORT') ? '3306';

# ReCAPTCHA settings
# Used for the 'Insecure CAPTCHA' module
# You'll need to generate your own keys at: https://www.google.com/recaptcha/admin
$_DVWA['recaptcha_public_key'] = getenv('RECAPTCHA_PUBLIC_KEY') ? '';
$_DVWA['recaptcha_private_key'] = getenv('RECAPTCHA_PRIVATE_KEY') ? '';

# Default security level
# Default value for the security level with each session.
# The default is 'impossible'. You may wish to set this to either 'low', 'medium', 'high' or 'impossible'.
$_DVWA['default_security_level'] = getenv('DEFAULT_SECURITY_LEVEL') ? 'impossible';

# Default locale
# Default locale for the help page shown with each session.
# The default is 'en'. You may wish to set this to either 'en' or 'zh'.
$_DVWA['default_locale'] = getenv('DEFAULT_LOCALE') ? 'en';

# Disable authentication
# Some tools don't like working with authentication and passing cookies around
# so this setting lets you turn off authentication.
$_DVWA['disable_authentication'] = getenv('DISABLE_AUTHENTICATION') ? false;

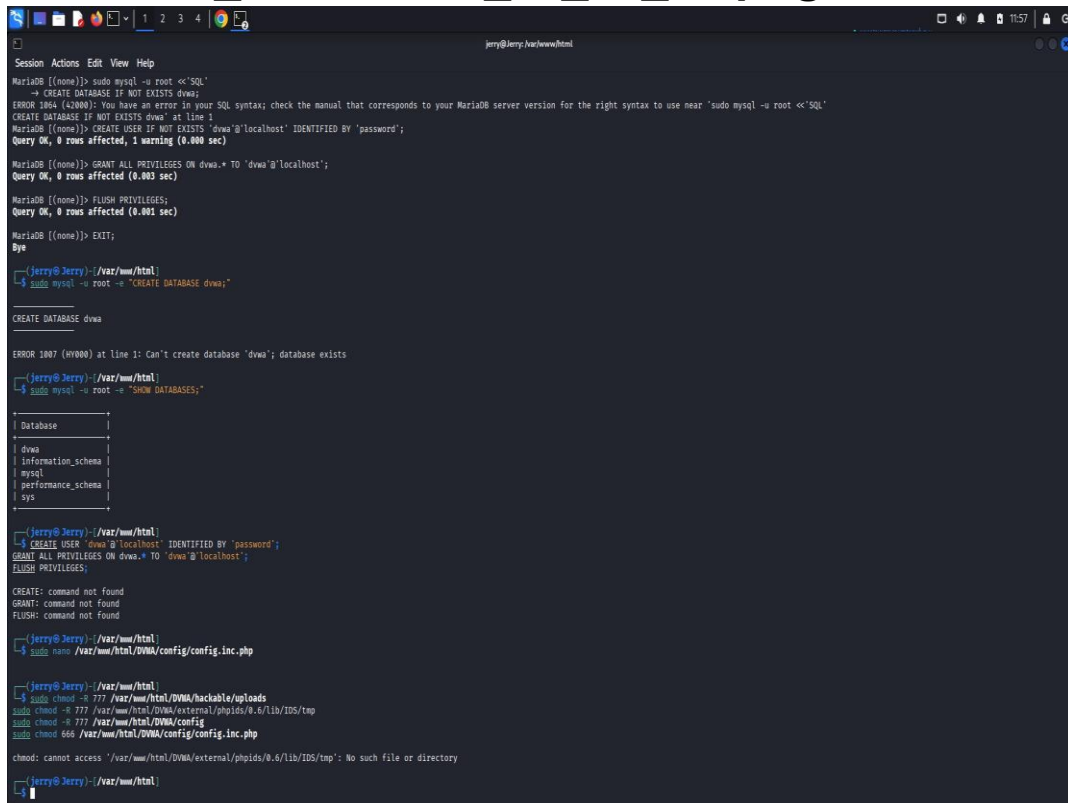
define('MYSQL', 'mysql');
define('SQLITE', 'sqlite');

# SQLi DB Backend
# Use this to switch the backend database used in the SQLi and Blind SQLi labs.
# This does not affect the backend for any other services, just these two labs.
# If you do not understand what this means, do not change it.
$_DVWA['SQLI_DB'] = getenv('SQLI_DB') ? MYSQL;
$_DVWA['SQLI_DB'] = SQLITE;
$_DVWA['SQLITE_DB'] = 'sqlite.db';

?>
```

This screenshot shows a key exploitation step during DVWA testing.

# Screenshot\_2025-11-28\_11\_57\_33.png



```
jerry@jerry:~/var/www/html

Session Actions Edit View Help

MariaDB [(none)]> sudo mysql -u root << 'SQL'
-> CREATE DATABASE IF NOT EXISTS dwa;
ERROR 1007 (HY000): 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 'sudo mysql -u root << 'SQL'
CREATE DATABASE IF NOT EXISTS dwa' at line 1
MariaDB [(none)]> CREATE USER IF NOT EXISTS 'dwa'@'localhost' IDENTIFIED BY 'password';
Query OK, 0 rows affected, 1 warning (0.000 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON dwa.* TO 'dwa'@'localhost';
Query OK, 0 rows affected (0.003 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> EXIT;
Bye

jerry@jerry:~/var/www/html
$ sudo mysql -u root -e "CREATE DATABASE dwa;"

CREATE DATABASE dwa

ERROR 1007 (HY000) at line 1: Can't create database 'dwa'; database exists

jerry@jerry:~/var/www/html
$ sudo mysql -u root -e "SHOW DATABASES;"

+-----+
| Database |
+-----+
| dwa      |
| information_schema |
| mysql    |
| performance_schema |
| sys      |
+-----+

jerry@jerry:~/var/www/html
$ sudo mysql -u root -e "CREATE USER 'dwa'@'localhost' IDENTIFIED BY 'password'; GRANT ALL PRIVILEGES ON dwa.* TO 'dwa'@'localhost'; FLUSH PRIVILEGES;"

CREATE: command not found
GRANTS: command not found
FLUSH: command not found

jerry@jerry:~/var/www/html
$ sudo nano /var/www/html/DVWA/config/config.inc.php

jerry@jerry:~/var/www/html
$ sudo chmod -R 777 /var/www/html/DVWA/hackable/uploads
$ sudo chmod -R 777 /var/www/html/DVWA/external/phpids/0.6/lib/IDS/tmp
$ sudo chmod -R 777 /var/www/html/DVWA/config
$ sudo chmod 666 /var/www/html/DVWA/config/config.inc.php

chmod: cannot access '/var/www/html/DVWA/external/phpids/0.6/lib/IDS/tmp': No such file or directory

jerry@jerry:~/var/www/html
$
```

This screenshot shows a key exploitation step during DVWA testing.

# Screenshot\_2025-11-28\_11\_59\_29.png

```

jerry@jerry:~/www/html
Session Actions Edit View Help

MariaDB [(none)]> GRANT ALL PRIVILEGES ON dvwa.* TO 'dvwa'@'localhost';
Query OK, 0 rows affected (0.003 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> EXIT;
Bye

jerry@jerry:~/www/html
$ sudo mysql -u root -e "CREATE DATABASE dvwa;"

CREATE DATABASE dvwa

ERROR 1007 (HY000) at line 1: Can't create database 'dvwa'; database exists

jerry@jerry:~/www/html
$ sudo mysql -u root -e "SHOW DATABASES;"

+-----+
| Database |
+-----+
| dvwa     |
| information_schema |
| mysql    |
| performance_schema |
| sys      |
+-----+

jerry@jerry:~/www/html
$ CREATE USER 'dvwa'@'localhost' IDENTIFIED BY 'password';
GRANT ALL PRIVILEGES ON dvwa.* TO 'dvwa'@'localhost';
FLUSH PRIVILEGES;

CREATE: command not found
GRANT: command not found
FLUSH: command not found

jerry@jerry:~/www/html
$ sudo nano /var/www/html/DVWA/config/config.inc.php

jerry@jerry:~/www/html
$ sudo chmod -R 777 /var/www/html/DVWA/hackable/uploads
$ sudo chmod -R 777 /var/www/html/DVWA/external/phpids/0.6/lib/IDS/tmp
$ sudo chmod -R 777 /var/www/html/DVWA/config
$ sudo chmod 666 /var/www/html/DVWA/config/config.inc.php

chmod: cannot access '/var/www/html/DVWA/external/phpids/0.6/lib/IDS/tmp': No such file or directory

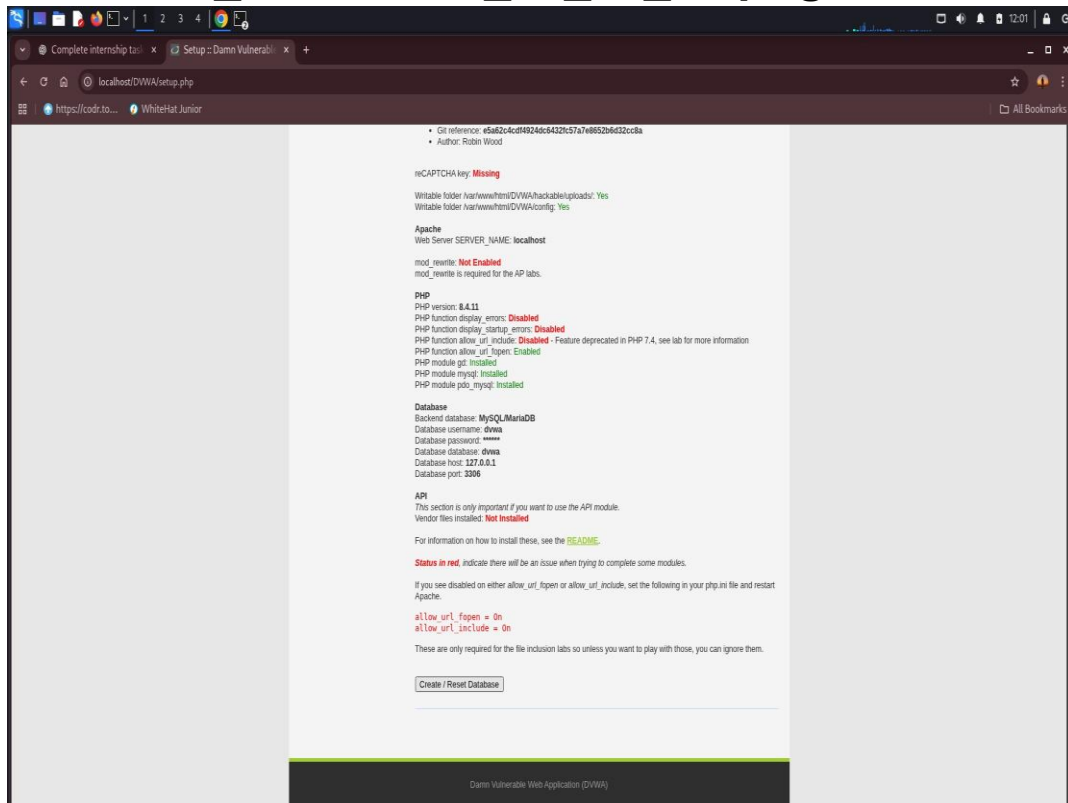
jerry@jerry:~/www/html
$ ls -l /var/www/html/DVWA/external

/var/www/html/DVWA/external:
recaptcha:
recaptchalib.php
```

This screenshot shows a key exploitation step during DVWA testing.

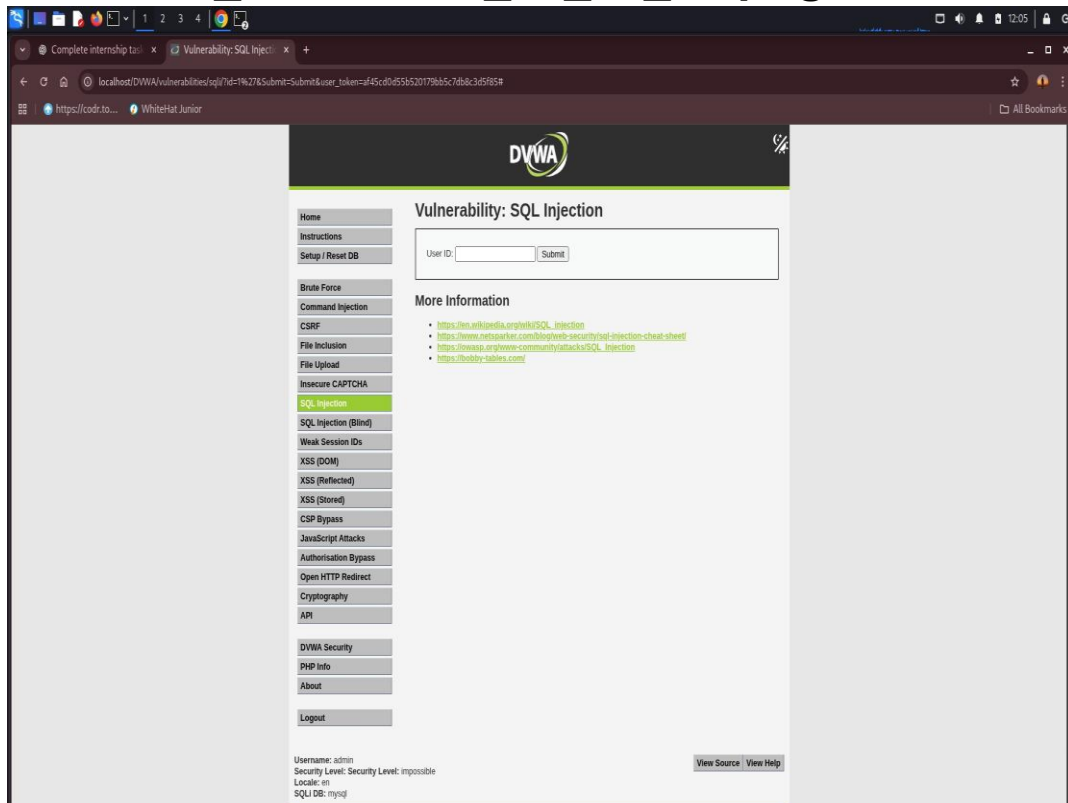


# Screenshot\_2025-11-28\_12\_01\_27.png



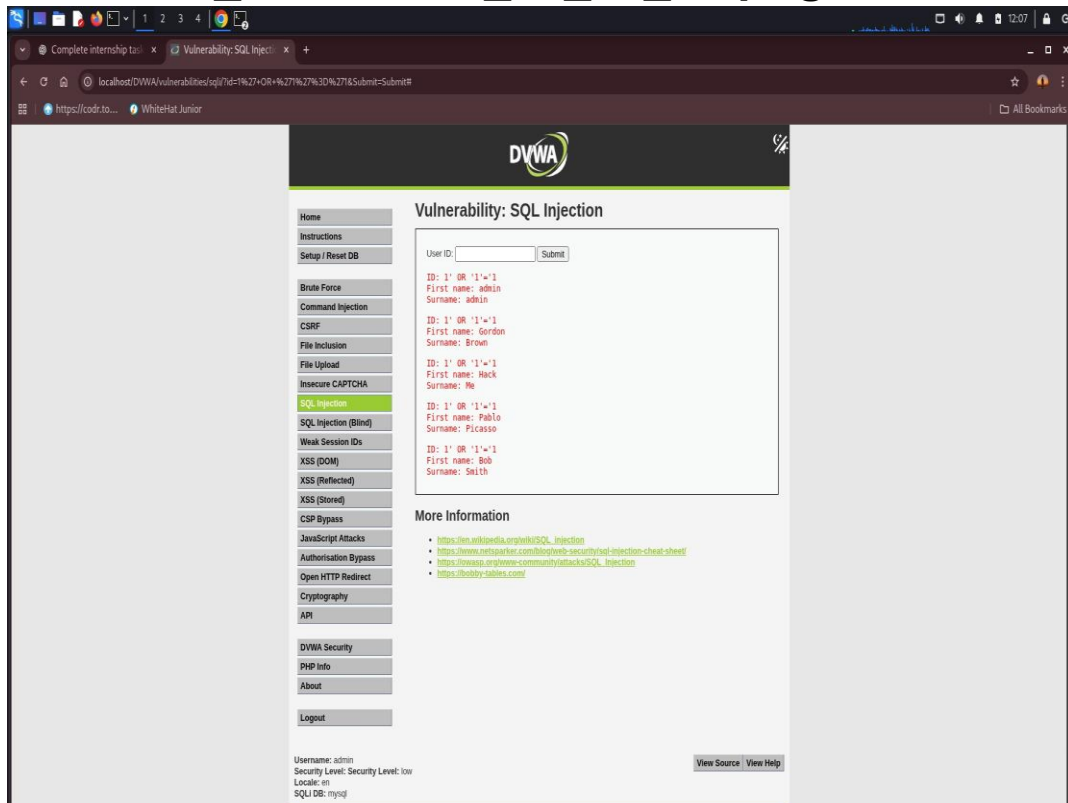
This screenshot shows a key exploitation step during DVWA testing.

# Screenshot\_2025-11-28\_12\_05\_34.png



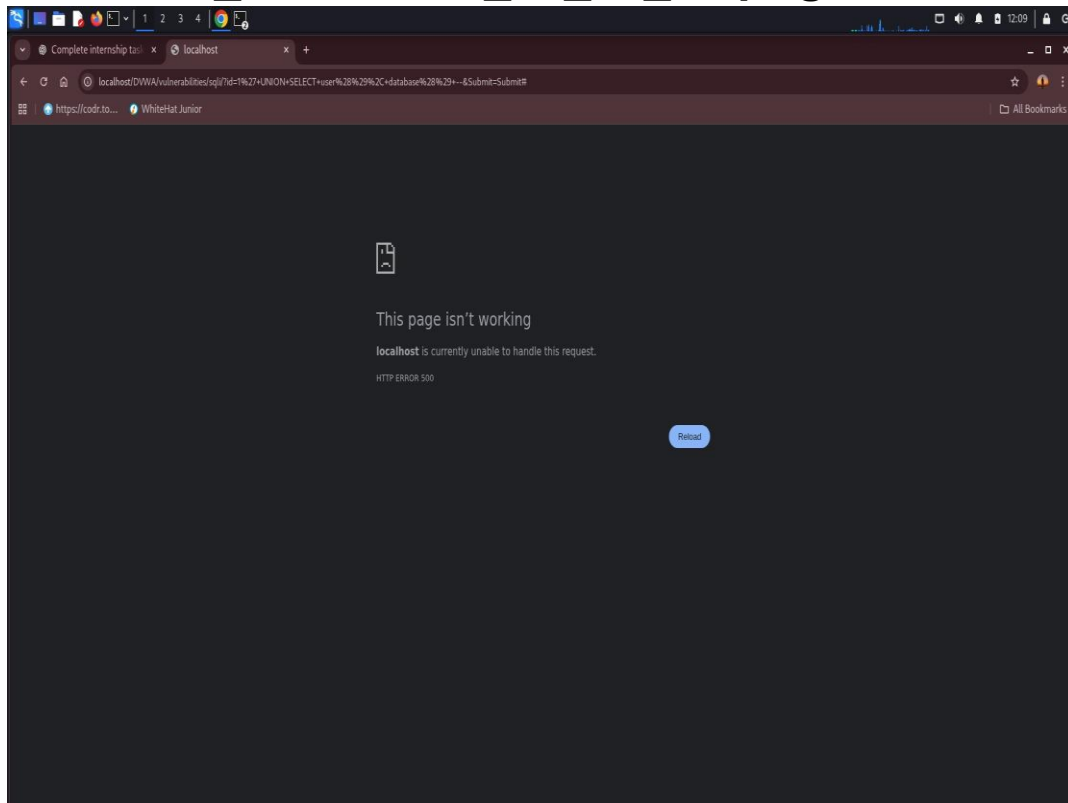
This screenshot shows a key exploitation step during DVWA testing.

# Screenshot\_2025-11-28\_12\_07\_27.png



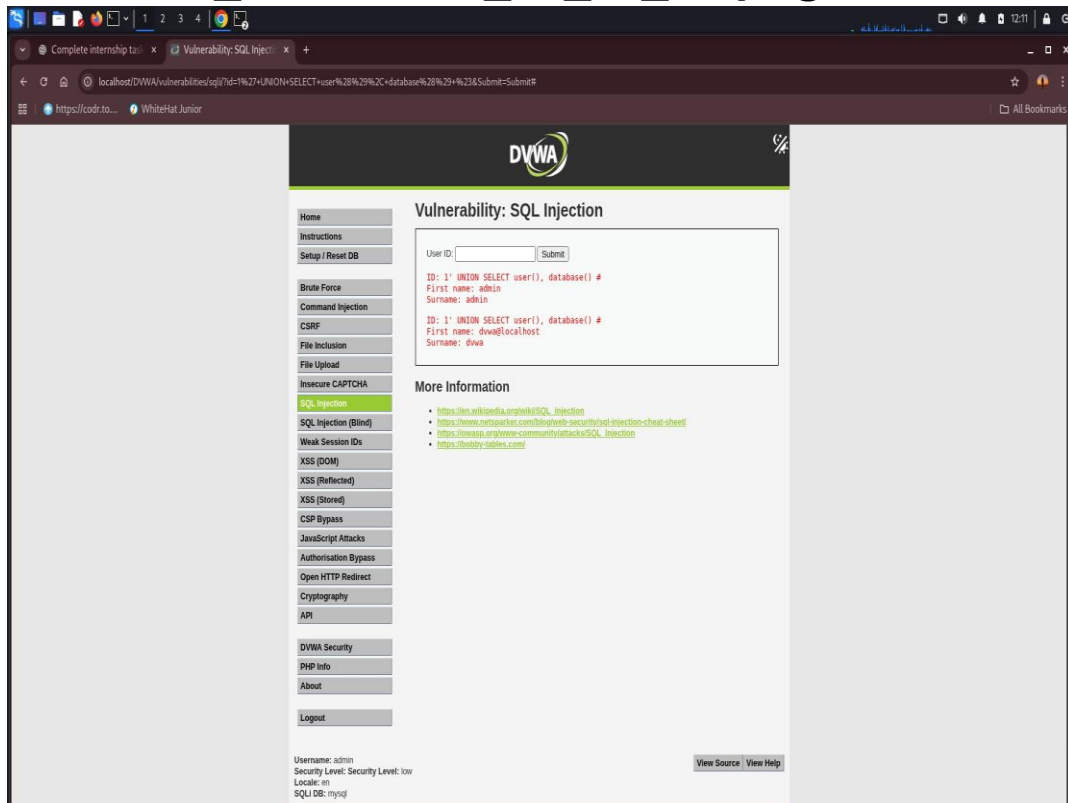
This screenshot shows a key exploitation step during DVWA testing.

# Screenshot\_2025-11-28\_12\_09\_43.png



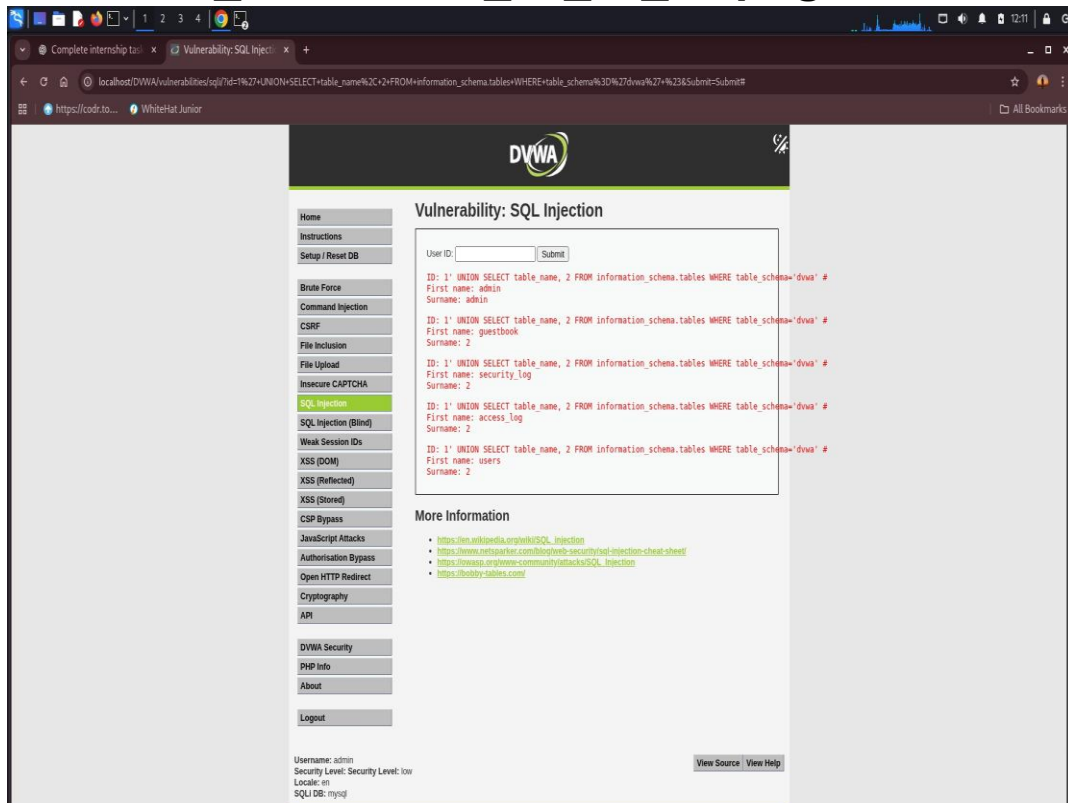
This screenshot shows a key exploitation step during DVWA testing.

# Screenshot\_2025-11-28\_12\_11\_17.png



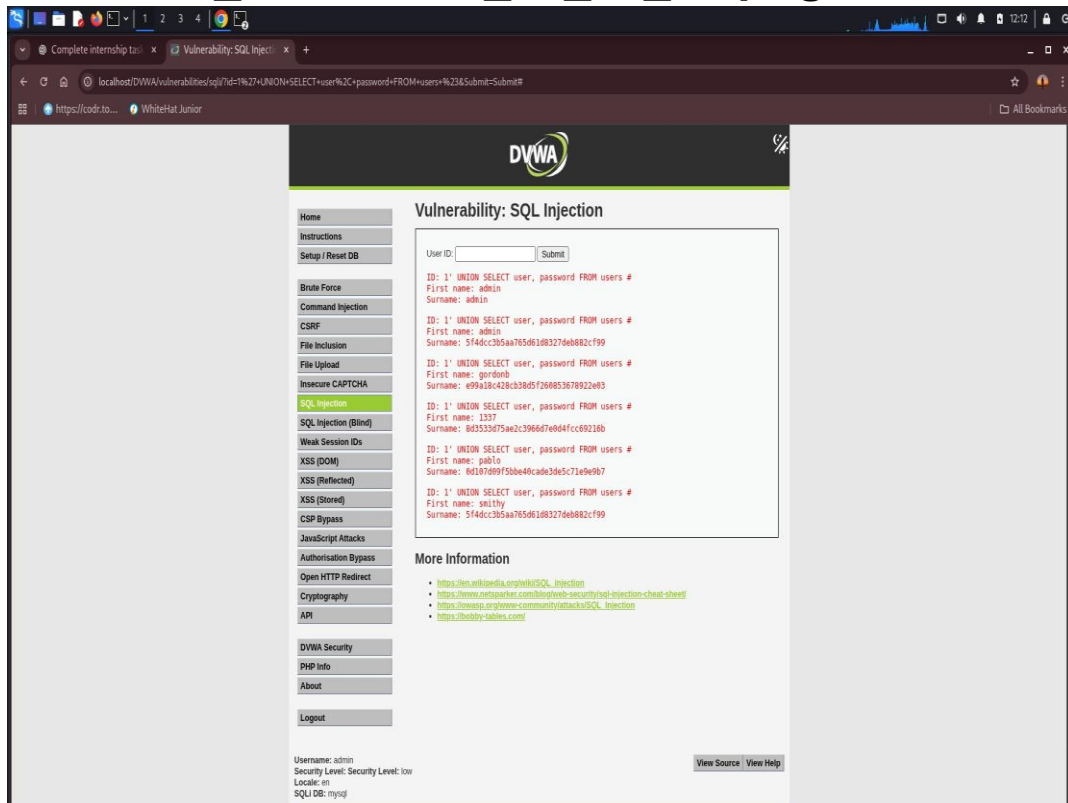
This screenshot shows a key exploitation step during DVWA testing.

# Screenshot\_2025-11-28\_12\_11\_57.png



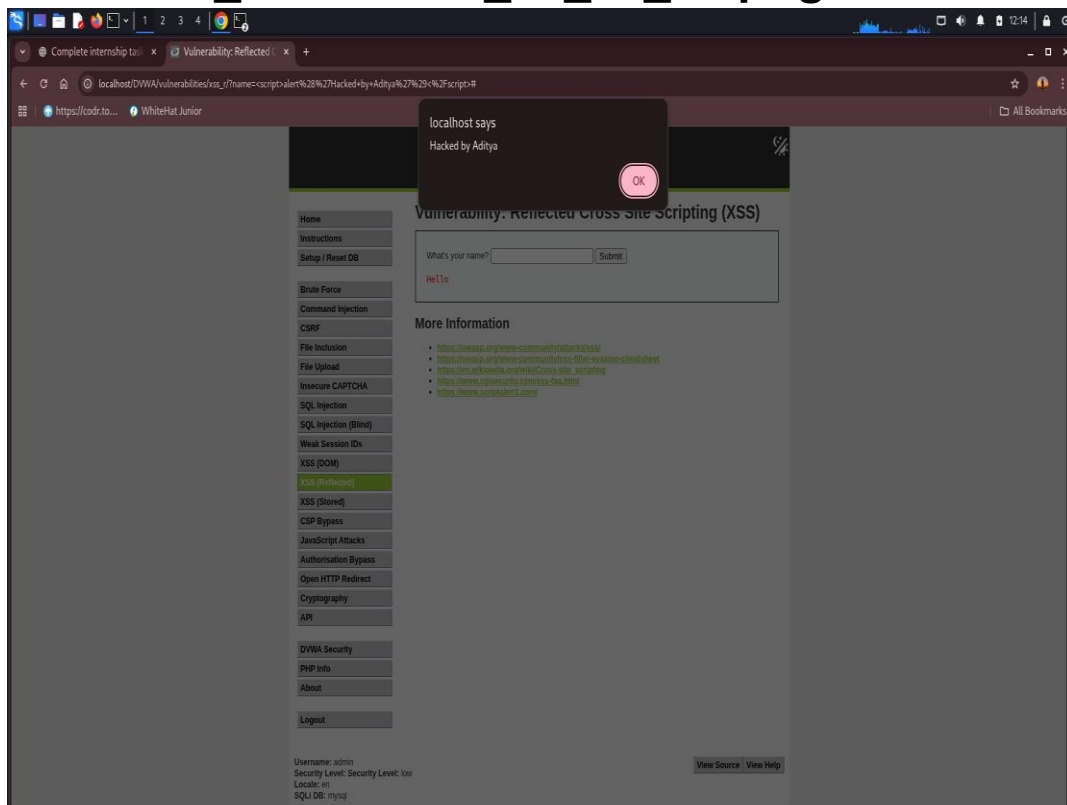
This screenshot shows a key exploitation step during DVWA testing.

# Screenshot\_2025-11-28\_12\_12\_51.png



This screenshot shows a key exploitation step during DVWA testing.

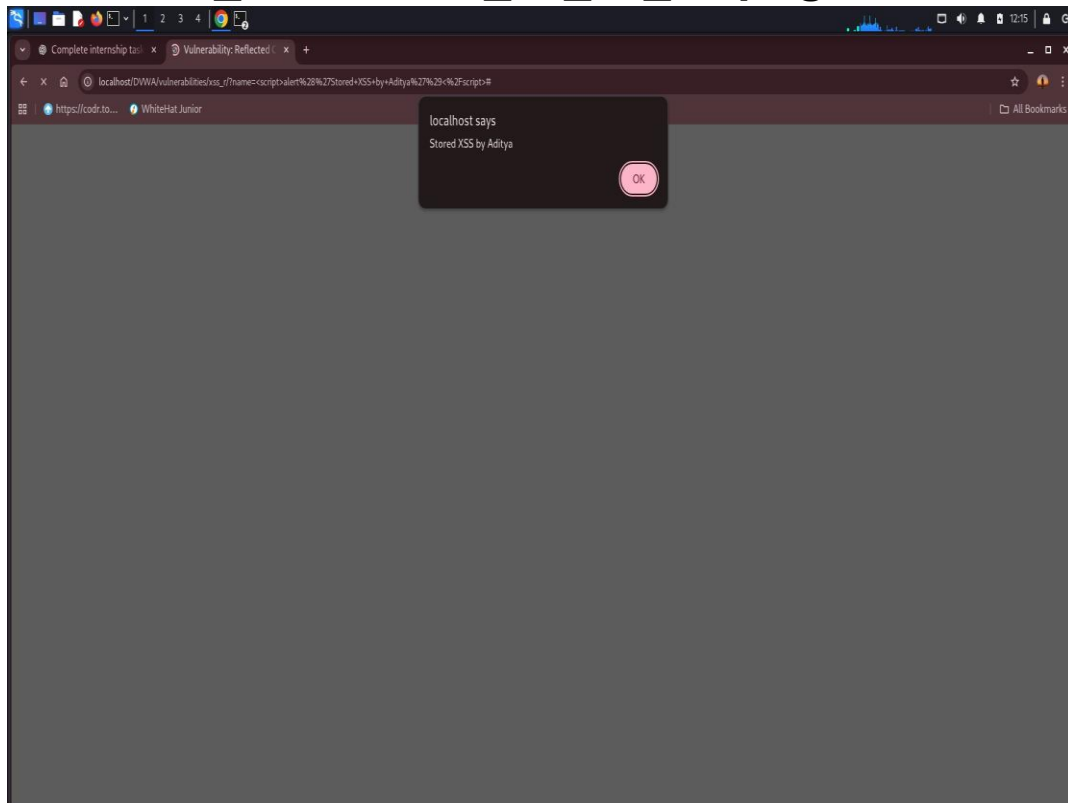
# Screenshot\_2025-11-28\_12\_14\_04.png



This screenshot shows a key exploitation step during DVWA testing.

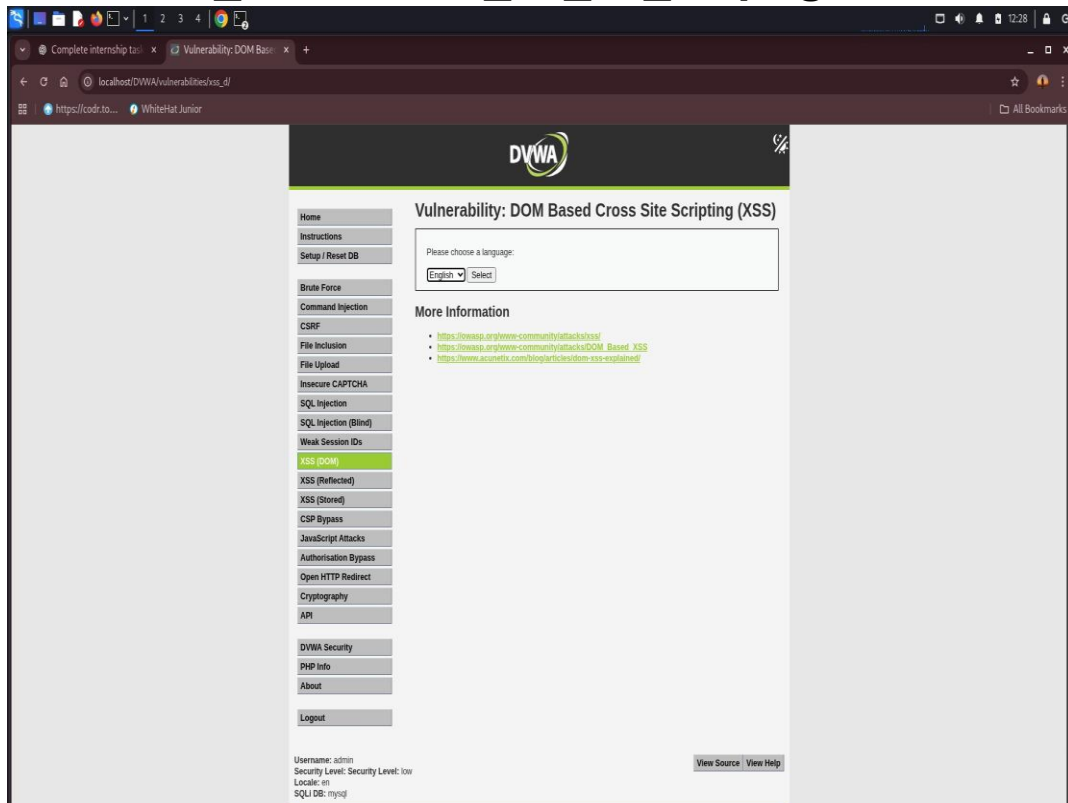


## Screenshot\_2025-11-28\_12\_15\_01.png



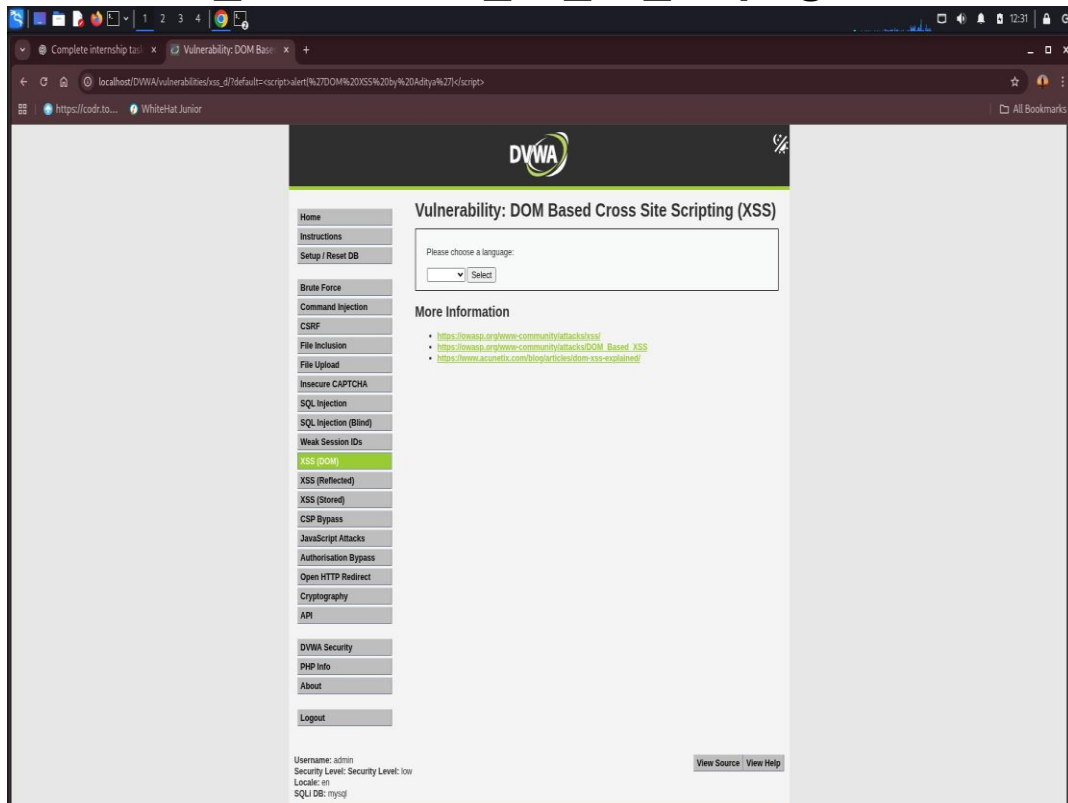
This screenshot shows a key exploitation step during DVWA testing.

# Screenshot\_2025-11-28\_12\_28\_23.png



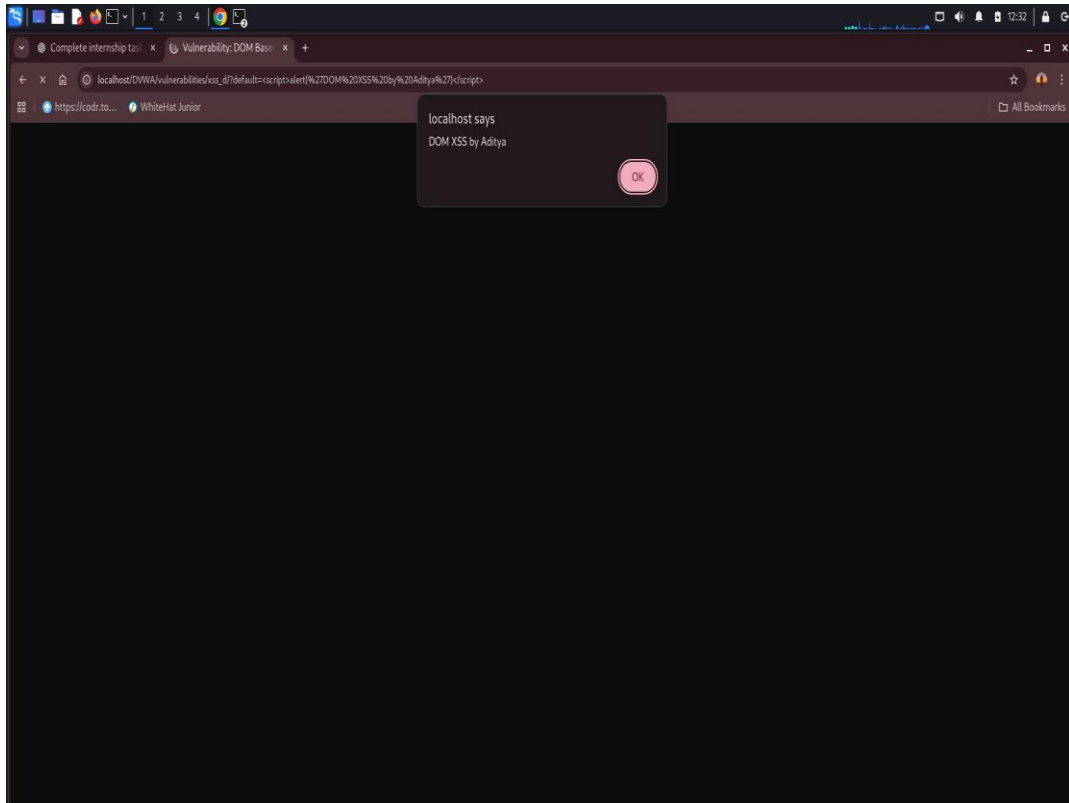
This screenshot shows a key exploitation step during DVWA testing.

# Screenshot\_2025-11-28\_12\_31\_19.png



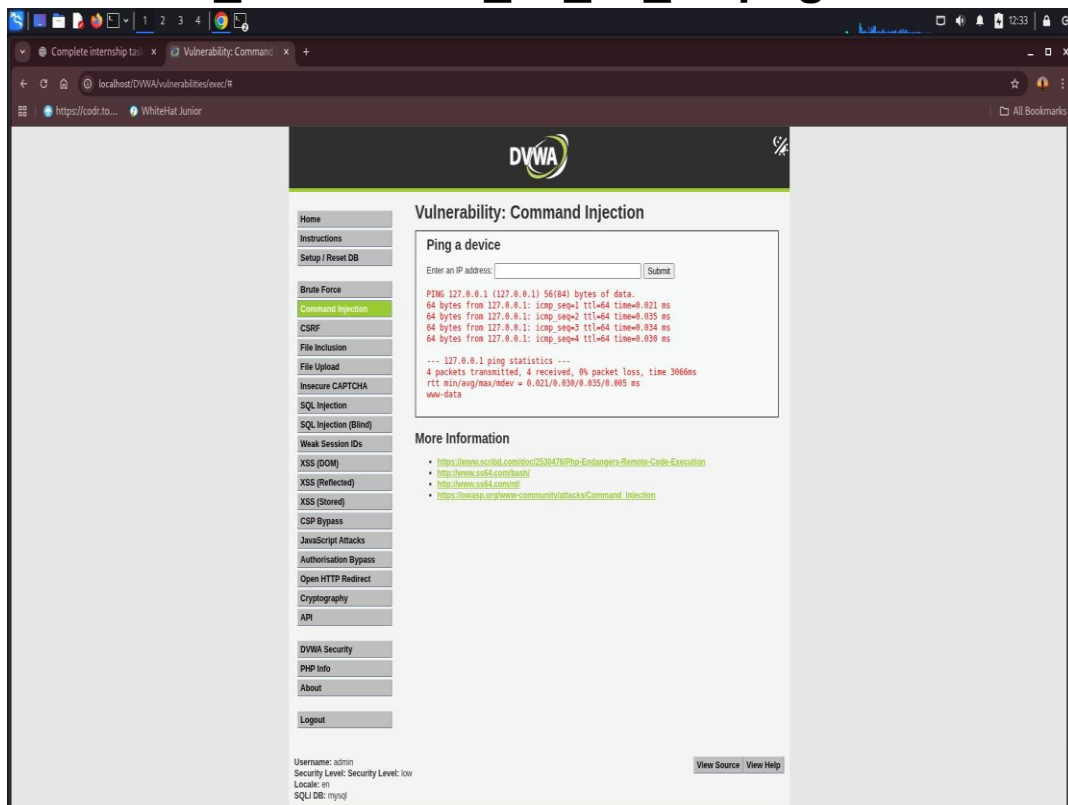
This screenshot shows a key exploitation step during DVWA testing.

**Screenshot\_2025-11-28\_12\_32\_38.png**



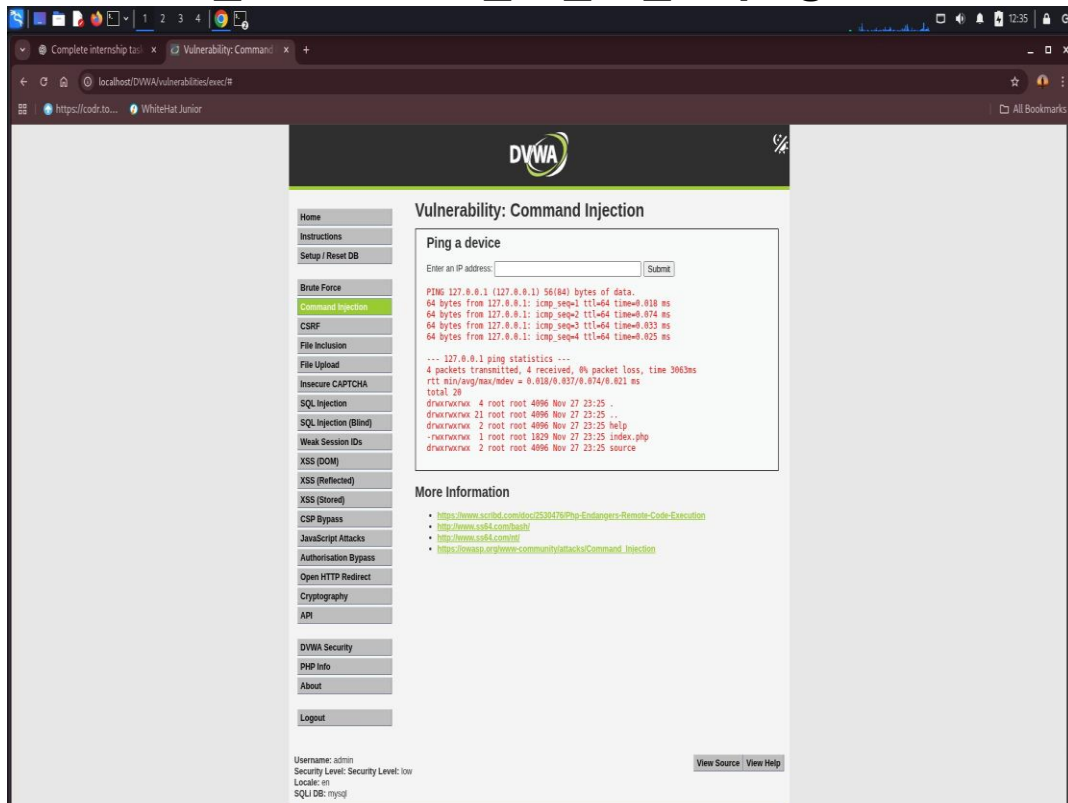
This screenshot shows a key exploitation step during DVWA testing.

# Screenshot\_2025-11-28\_12\_33\_58.png



This screenshot shows a key exploitation step during DVWA testing.

# Screenshot\_2025-11-28\_12\_35\_59.png



This screenshot shows a key exploitation step during DVWA testing.

# Screenshot\_2025-11-28\_12\_39\_09.png

```
Session Actions Edit View Help
| sys |
+-----+

--(jerry@jerry)-:/var/www/html
--4 CREATE USER 'dwva'@'localhost' IDENTIFIED BY 'password';
GRANT ALL PRIVILEGES ON dwva.* TO 'dwva'@'localhost';
FLUSH PRIVILEGES;

CREATE: command not found
GRANT: command not found
FLUSH: command not found

--(jerry@jerry)-:/var/www/html
--4 sudo nano /var/www/html/DVWA/config/config.inc.php

--(jerry@jerry)-:/var/www/html
--4 sudo chmod -R 777 /var/www/html/DVWA/hackable/uploads
sudo chmod -R 777 /var/www/html/DVWA/external/phpids/0.6/lib/IDS/tmp
sudo chmod -R 777 /var/www/html/DVWA/config
sudo chmod 666 /var/www/html/DVWA/config/config.inc.php

chmod: cannot access '/var/www/html/DVWA/external/phpids/0.6/lib/IDS/tmp': No such file or directory

--(jerry@jerry)-:/var/www/html
--4 ls -l /var/www/html/DVWA/external
/var/www/html/DVWA/external:
total 0
-rw-r--r-- 1 root root 0 Nov 28 12:39
recaptcha:
recaptchalib.php

--(jerry@jerry)-:/var/www/html
--4 sudo chmod -R 777 /var/www/html/DVWA/external/phpids/IDS/tmp
sudo chmod -R 777 /var/www/html/DVWA/external/IDS/tmp
sudo chmod -R 777 /var/www/html/DVWA/external/phpids

chmod: cannot access '/var/www/html/DVWA/external/phpids/IDS/tmp': No such file or directory
chmod: cannot access '/var/www/html/DVWA/external/IDS/tmp': No such file or directory
chmod: cannot access '/var/www/html/DVWA/external/phpids': No such file or directory

--(jerry@jerry)-:/var/www/html
--4 sudo chmod -R 777 /var/www/html/DVWA/hackable/uploads
sudo chmod -R 777 /var/www/html/DVWA/config
sudo chmod 666 /var/www/html/DVWA/config/config.inc.php

--(jerry@jerry)-:/var/www/html
--4 sudo systemctl restart apache2
sudo systemctl restart php8.4-fpm
sudo systemctl restart mariadb

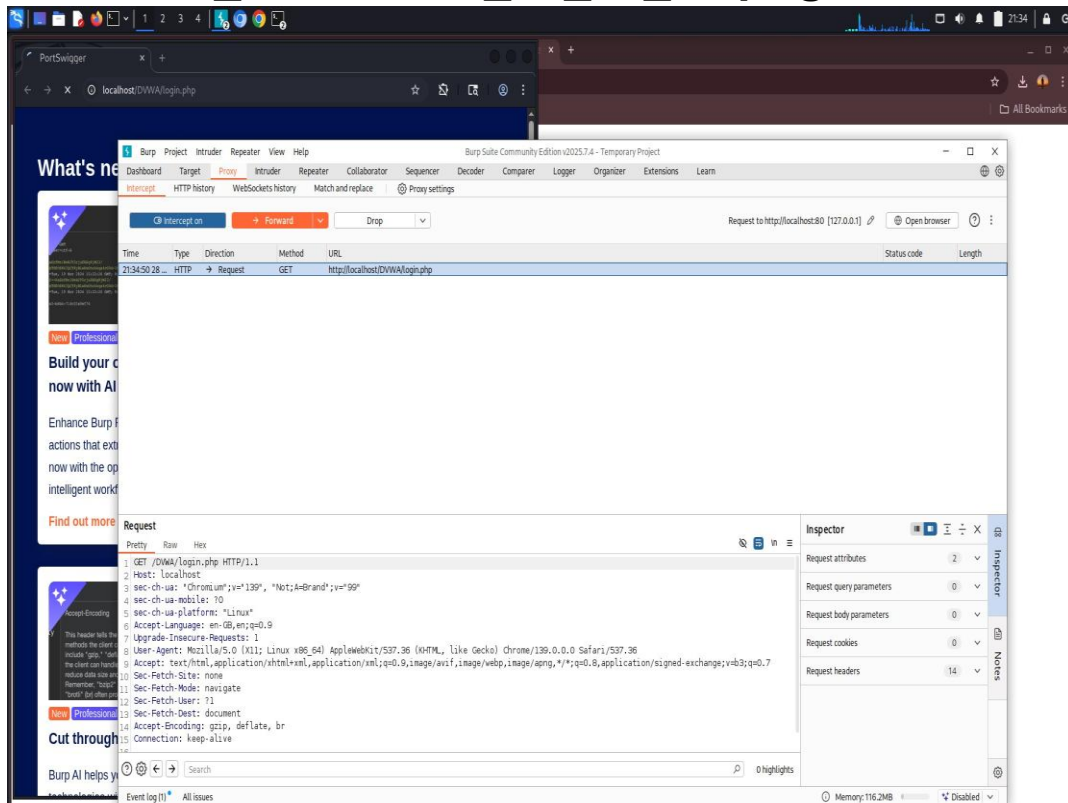
--(jerry@jerry)-:/var/www/html
--4 echo "<?php system($_GET['cmd']); ?>" > shell.php

zsh: permission denied: shell.php

--(jerry@jerry)-:/var/www/html
--4
```

This screenshot shows a key exploitation step during DVWA testing.

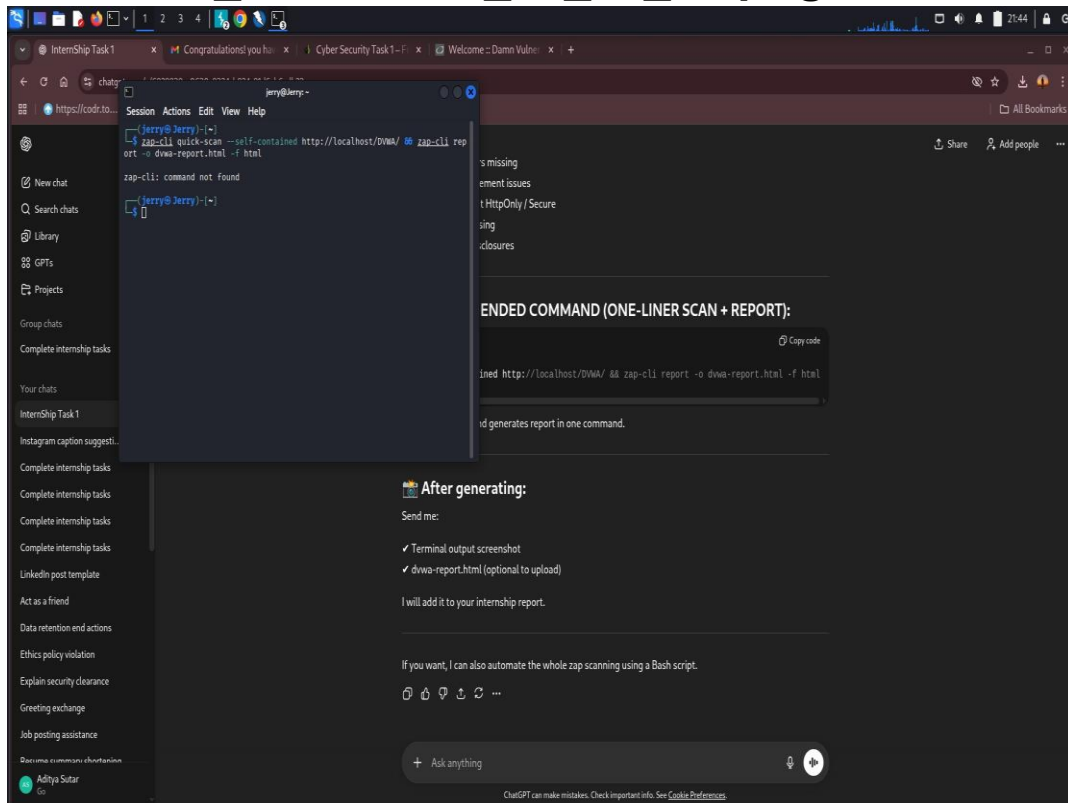
# Screenshot\_2025-11-28\_21\_34\_58.png



This screenshot shows a key exploitation step during DVWA testing.

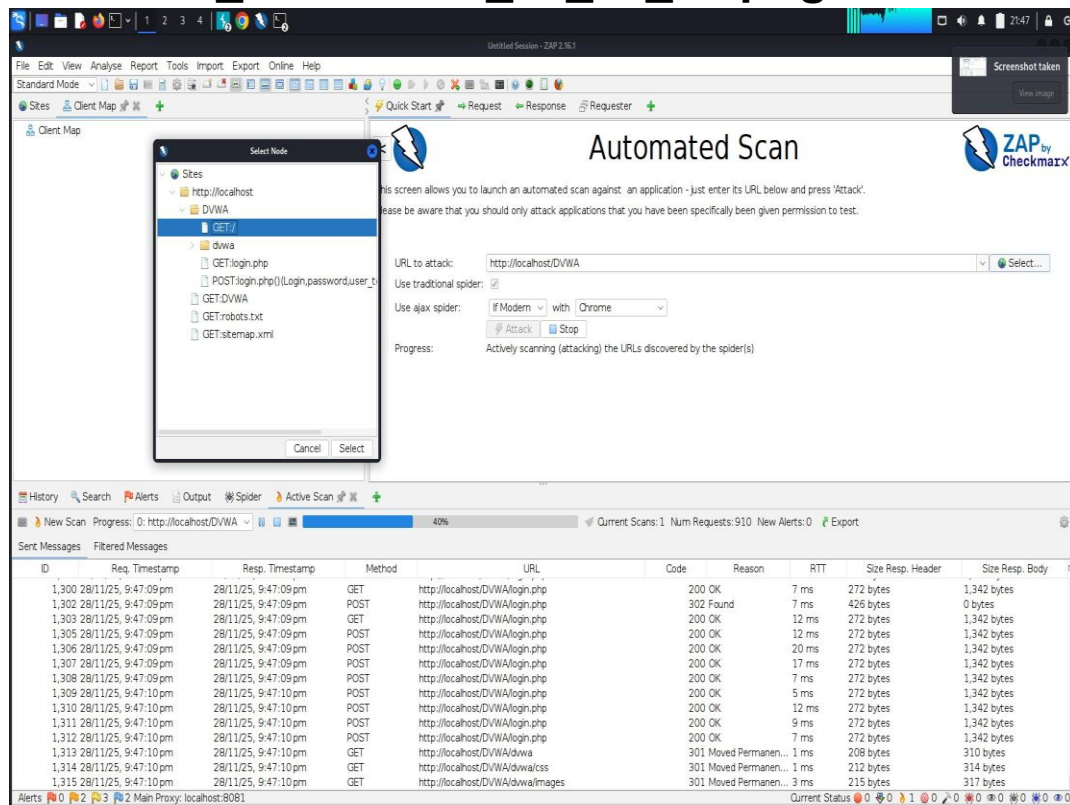


# Screenshot\_2025-11-28\_21\_44\_32.png



This screenshot shows a key exploitation step during DVWA testing.

# Screenshot\_2025-11-28\_21\_47\_31.png



This screenshot shows a key exploitation step during DVWA testing.

## Conclusion

The DVWA assessment successfully demonstrated SQL Injection, XSS, Command Injection, and automated scanning using ZAP.