



Cybersecurity 701

Session Replay Lab



Session Replay Materials

- Materials needed
 - Kali Linux Virtual Machine
 - Windows 7 Virtual Machine
- Software tool used
 - DVWA (Web/Application)



Objectives Covered

- Security + Objectives (SY0-701)
 - Objective 2.4 – Given a scenario, analyze indicators of malicious activity.
 - On-path
 - Credential replay
 - Malicious code



What is a session replay attack?

- Session replay is when an attacker gains access to a legitimate session
 - Gains access by using the same cookies (especially the session ID cookie)
 - This is sometimes called cookie hijacking
 - A hacker authenticates via the same cookies as the normal user

Domain:	localhost
Name:	PHPSESSID
Value:	21427dba2i9he5409phd0vrqsg
Path:	/
Expires:	2024-04-19 18:39:14
Store ID:	firefox-default
First Party Domain:	
Secure:	<input type="checkbox"/>
Session:	<input type="checkbox"/>
Http Only:	<input checked="" type="checkbox"/>
Host Only:	<input checked="" type="checkbox"/>

[Export](#) [Update](#) [Delete](#)

Session Replay Lab Overview

1. Set up Environments
2. Find Kali's IP Address
3. Log into DVWA
4. Capture the session ID
5. Use the Session ID
6. Replay the Session

```
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: security=impossible; PHPSESSID=21427dba2i9he5409phd0vrgsq

security=high&seclev_submit=Submit&user_token=512316e6cc2239e05c3ed9d911
und
Date: Thu, 18 Apr 2024 18:24:52 GMT
Server: Apache/2.4.56 (Unix) OpenSSL/1.1.1t PHP/8.2.4 mod_perl/2.0.12 Pe
X-Powered-By: PHP/8.2.4
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: security=high; path=/
Location: /dvwa/security.php
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

GET /dvwa/security.php HTTP/1.1
```



Set up Environments

- Log into your range
- Open the Kali Linux and Windows 7 environments
 - You should be on your Kali Linux Desktop
 - You should also be on your Windows7 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@10.15.126.183) - [~]  
$ hostname -I  
10.15.126.183
```

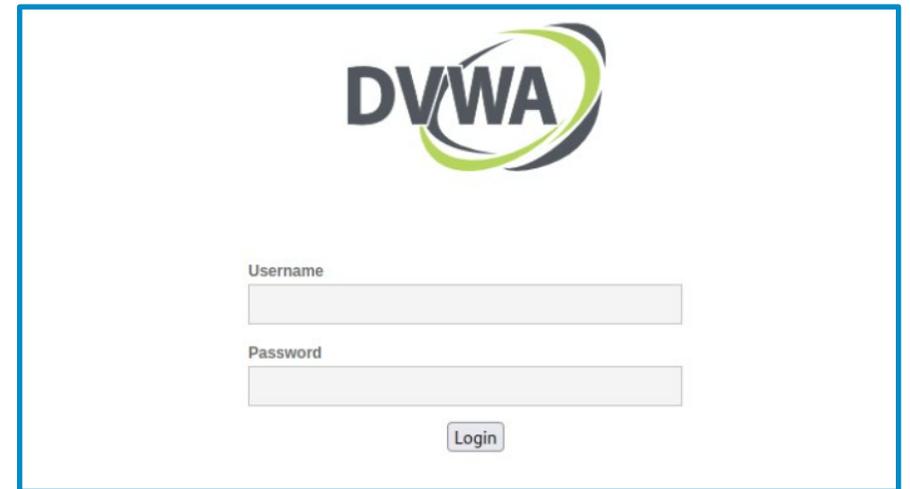
The IP Address



Log into DVWA

```
(kali@10.15.35.46)-[~]
└─$ DVWA_start
Starting XAMPP for Linux 8.2.4-0...
XAMPP: Starting Apache...ok.
XAMPP: Starting MySQL...ok.
XAMPP: Starting ProFTPD...ok.
(kali@10.15.35.46)-[~]
└─$
```

- Start up the web servers (on the Kali machine)
`DVWA_start`
- On the Windows Machine, go to the DVWA webpage
`http://Kali-IP-Address/dvwa`
- Login using the following credentials
 - Username: `admin`
 - Password: `password`

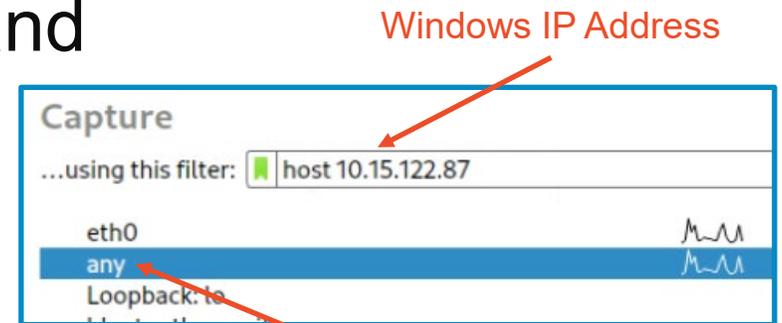


The screenshot shows the DVWA login page. At the top center is the DVWA logo, which consists of the letters 'DVWA' in a bold, sans-serif font, with a green and grey swoosh graphic behind the letters. Below the logo are two input fields: the first is labeled 'Username' and the second is labeled 'Password'. Both fields are empty. Below the password field is a 'Login' button.

Capture the Session ID

- In Kali, open a Terminal
- Open Wireshark with the following command
`sudo wireshark`
- In the “...using this filter:” option, type
`host <Windows-IP-Address>`
 - This will only find packets from the Windows machine
 - Select the “any” network below
- Click on the blue fin to start capturing packets

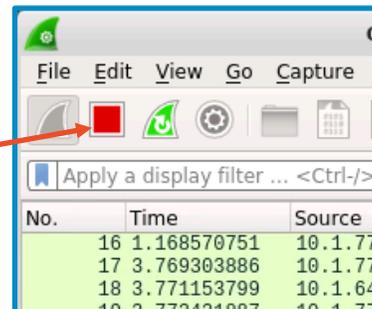
```
(kali@10.15.126.183) - [~]  
$ sudo wireshark
```



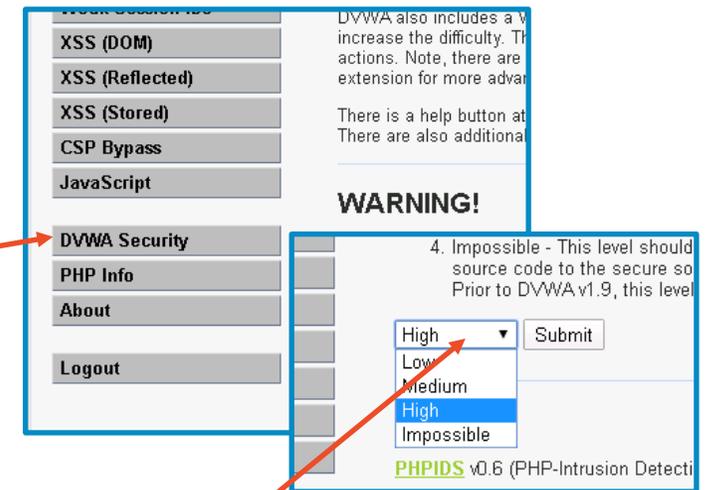
Capture the Session ID

- On the Windows 7 machine, change the security to “High”
 - Click on the DVWA Security tab
 - On the dropdown menu, change “Impossible” to “High”
 - Click Submit
- On the Kali machine, stop the capture
 - Click on the red square

Stops the capture



DVWA Security

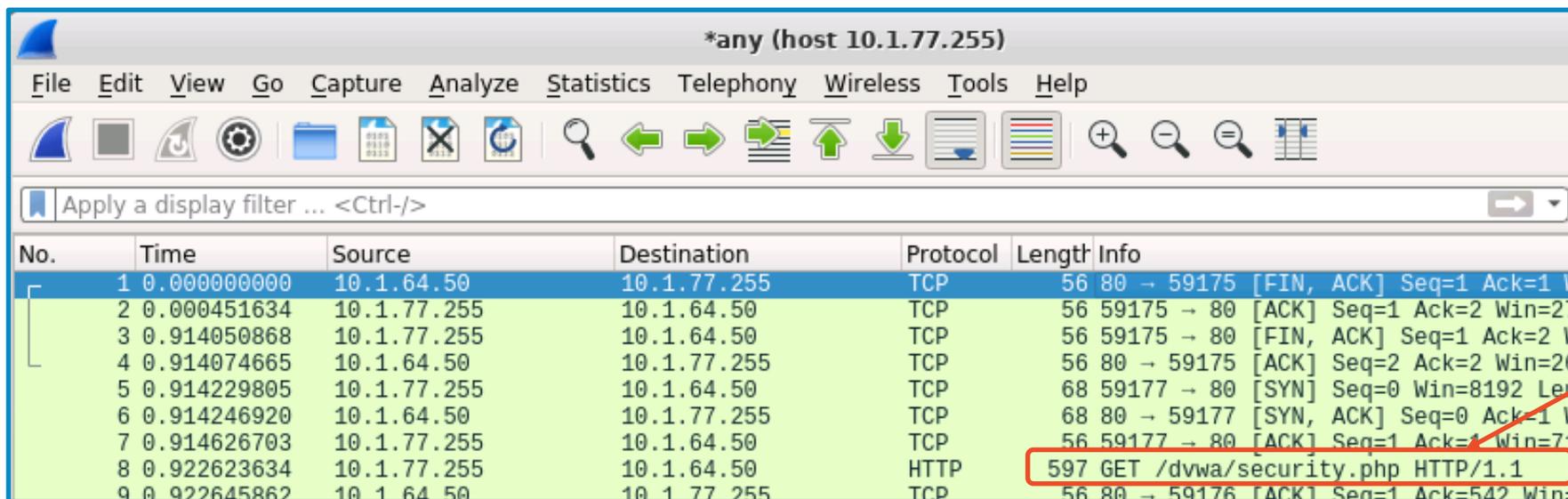


Change to “High”

Capture the Session ID

- In the packet capture, look for the following HTTP request in Info:

`GET /dvwa/security.php`



*any (host 10.1.77.255)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

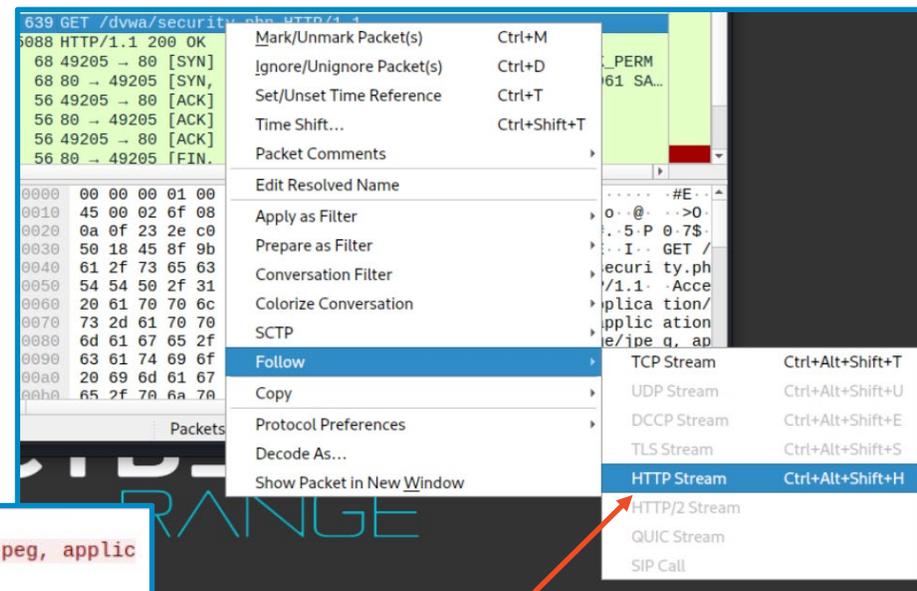
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.1.64.50	10.1.77.255	TCP	56	80 → 59175 [FIN, ACK] Seq=1 Ack=1 Win=0 Len=0
2	0.000451634	10.1.77.255	10.1.64.50	TCP	56	59175 → 80 [ACK] Seq=1 Ack=2 Win=272 Len=0
3	0.914050868	10.1.77.255	10.1.64.50	TCP	56	59175 → 80 [FIN, ACK] Seq=1 Ack=2 Win=0 Len=0
4	0.914074665	10.1.64.50	10.1.77.255	TCP	56	80 → 59175 [ACK] Seq=2 Ack=2 Win=260 Len=0
5	0.914229805	10.1.77.255	10.1.64.50	TCP	68	59177 → 80 [SYN] Seq=0 Win=8192 Len=0
6	0.914246920	10.1.64.50	10.1.77.255	TCP	68	80 → 59177 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0
7	0.914626703	10.1.77.255	10.1.64.50	TCP	56	59177 → 80 [ACK] Seq=1 Ack=1 Win=716 Len=0
8	0.922623634	10.1.77.255	10.1.64.50	HTTP		597 GET /dvwa/security.php HTTP/1.1
9	0.922645862	10.1.64.50	10.1.77.255	TCP	56	80 → 59176 [ACK] Seq=1 Ack=542 Win=0 Len=0

Look for this packet

Capture the Session ID

- Right-click on the packet
- Select the “Follow” option
- Select “HTTP Stream”
- This will open this HTTP exchange



```
GET /dvwa/security.php HTTP/1.1
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg, application/x-ms-xbap, */*
Referer: http://10.15.112.34/dvwa/index.php
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Accept-Encoding: gzip, deflate
Host: 10.15.112.34
Connection: Keep-Alive
Cookie: security=impossible; PHPSESSID=098lgbih3c1e0dm60el82a19lc

HTTP/1.1 200 OK
Date: Fri, 19 Apr 2024 13:10:04 GMT
Server: Apache/2.4.56 (Unix) OpenSSL/1.1.1t PHP/8.2.4 mod_perl/2.0.12 Perl/v5.34.1
X-Powered-By: PHP/8.2.4
Expires: Tue, 22 Jun 2009 12:00:00 GMT
```

The HTTP Stream

Capture the Session ID

- You should see the session ID
 - Will be in red
- You should also see the **security=impossible**
- Scroll down to see when the security changed to high
- Copy that session ID

Security set to
"impossible"

```
</html>GET /dvwa/dvwa/images/lock.png HTTP/1.1
Accept: /*
Referer: http://10.15.112.34/dvwa/security.php
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0;
.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET
Accept-Encoding: gzip, deflate
Host: 10.15.112.34
Connection: Keep-Alive
Cookie: security=impossible; PHPSESSID=098lgbih3c1e0dm60el82a19lc

HTTP/1.1 200 OK
Date: Fri, 19 Apr 2024 13:10:04 GMT
Server: Apache/2.4.56 (Unix) OpenSSL/1.1.1t PHP/8.2.4 mod_perl/2.0.12 Perl/v5.34.1
Last-Modified: Thu, 17 Aug 2023 16:09:15 GMT
```

```
GET /dvwa/security.php HTTP/1.1
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, i
ation/x-ms-xbap, /*
Referer: http://10.15.112.34/dvwa/security.php
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; S
.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4
Accept-Encoding: gzip, deflate
Host: 10.15.112.34
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: security=high; PHPSESSID=098lgbih3c1e0dm60el82a19lc

HTTP/1.1 200 OK
Date: Fri, 19 Apr 2024 13:10:09 GMT
Server: Apache/2.4.56 (Unix) OpenSSL/1.1.1t PHP/8.2.4 mod_perl/2.0.12 Perl/v5.34.1
X-Powered-By: PHP/8.2.4
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Content-Length: 4651
Keep-Alive: timeout=5, max=97
```

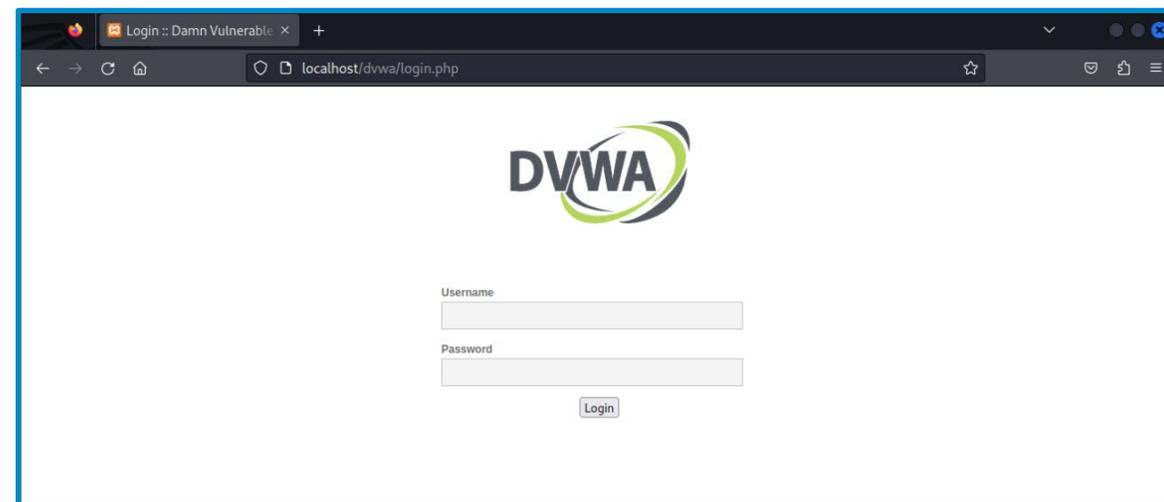
Security changed
to "high"

Copy the Session ID



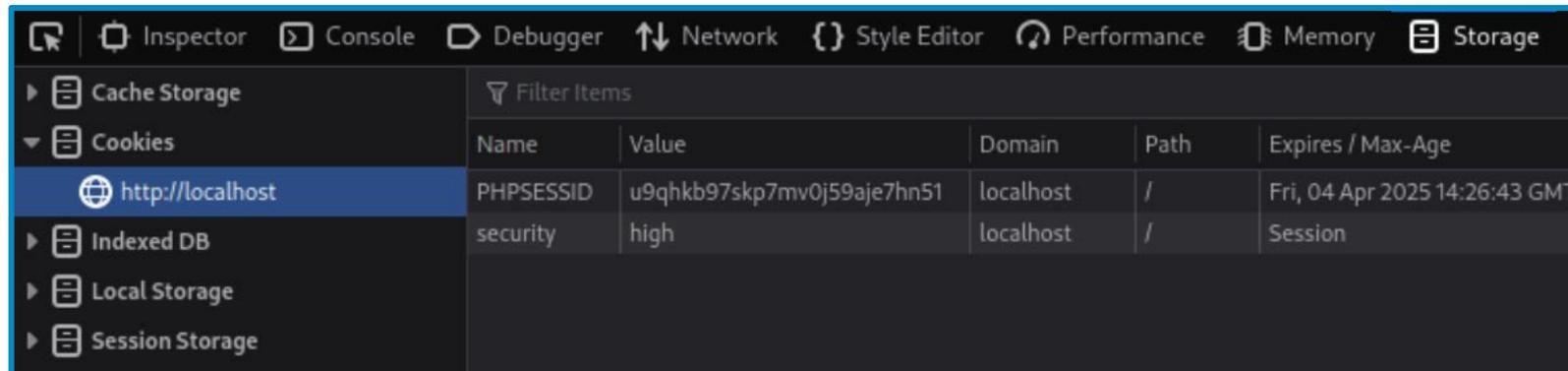
Using the Session ID

- In Kali, open Firefox
- Go to `localhost/dvwa`
 - This is the DVWA website
 - Notice you still have to log-in
- We will use the captured session ID to login on the next slide
 - This will skip the log-in step



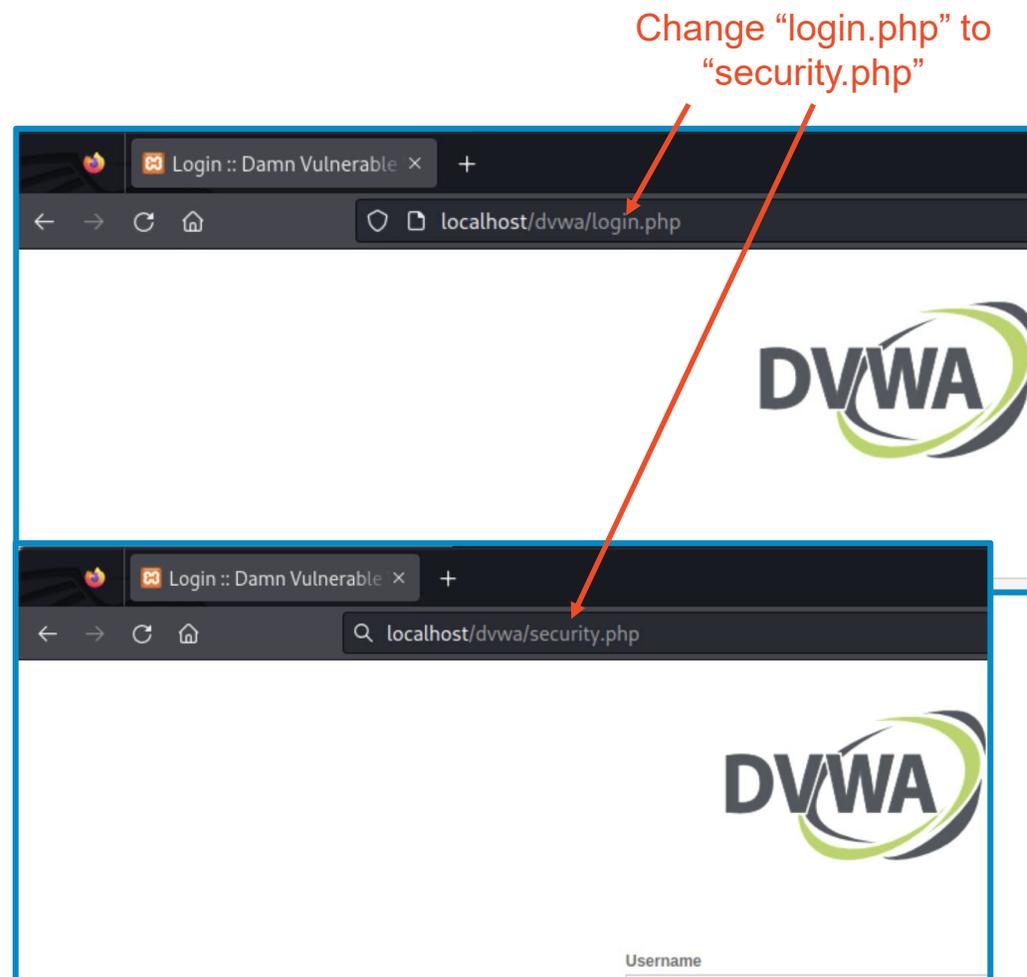
Open Web Developers Tools

- Type Ctrl+Shift+I
- Select the Storage Tab
- Double click the Value beside PHPSESSID and replace with the copied ID from Wireshark
- Double click the Value beside security to change impossible to high



Replay the Session

- Click on the DVWA tab in Firefox
- Change the URL
 - Change the login.php to security.php
- Load the webpage
- Notice you are now logged into DVWA
 - This is the same session as the Windows session!
- You have hijacked the Windows user's session and never had to enter their password or log into DVWA!



Defend Against Session Replay Attacks

- Avoid GET when possible
- Do not leave session opened
 - This attack would not have happened if the user was not logged into the DVWA website application on the other tab
- Timestamp cookies/sessions
- Use SameSite Cookies
 - Don't allow cookies to be used on external websites
- What are some other ways of defending against a session hijacking?

