Cybersecurity 701

Session Replay Lab

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Session Replay Materials

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

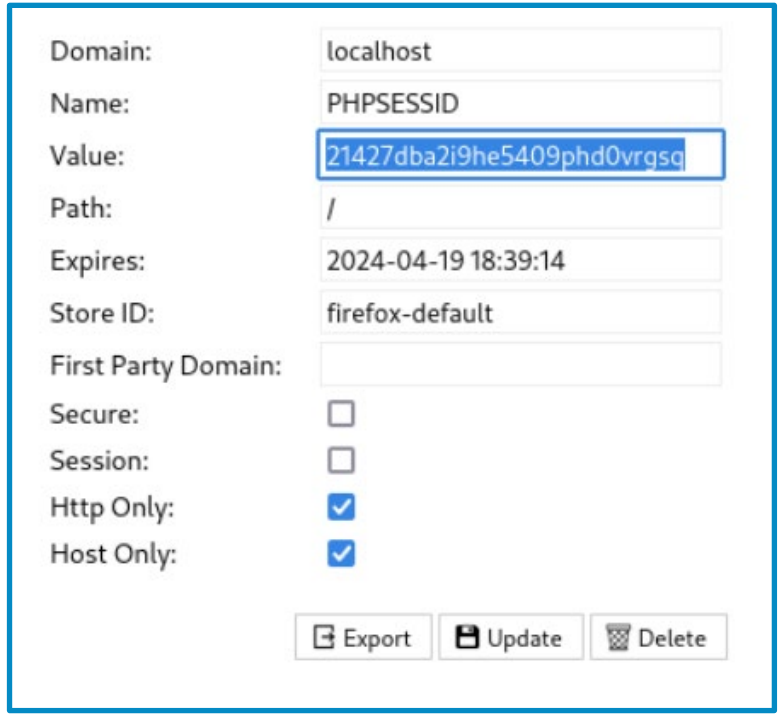
- Software tool used
  - DVWA (Web/Application)

Objectives Covered

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

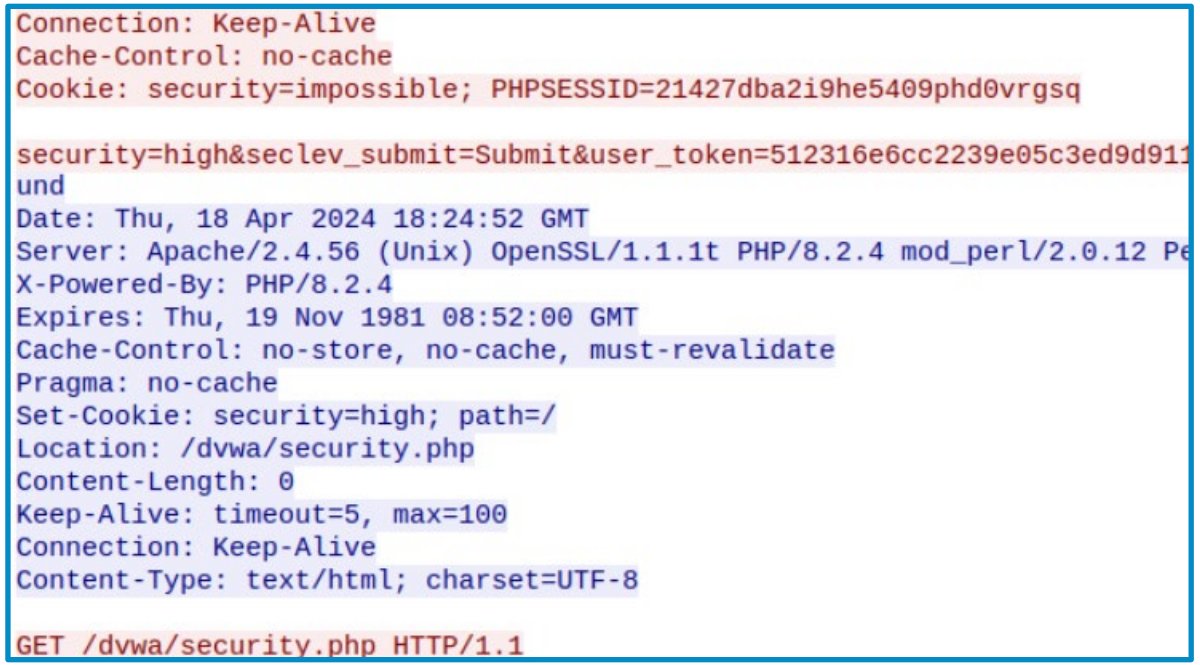
What is a session replay attack?

- 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



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



Set up Environments

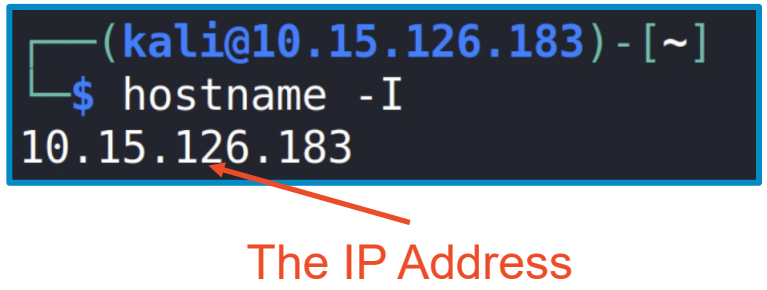
- Log into your range
- Open the Kali Linux and Windows 7 environments
  - You should be on your Kali Linux Desktop
  - You should also be on your Windows7 Desktop

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



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)-[~]
└─$
```

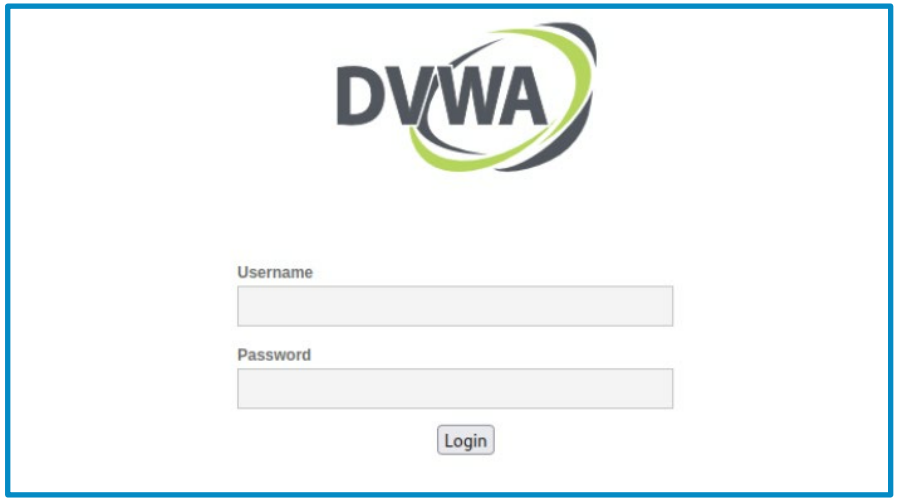
- Start up the web servers (on the Kali machine)

  `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`**



Capture the Session ID

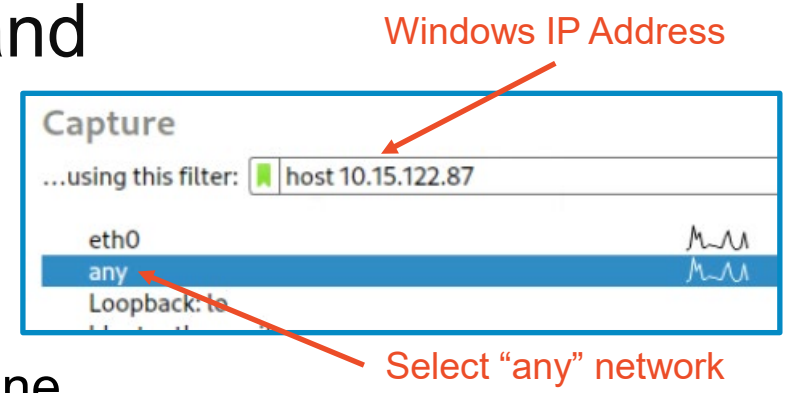
- In Kali, open a Terminal
- Open Wireshark with the following command

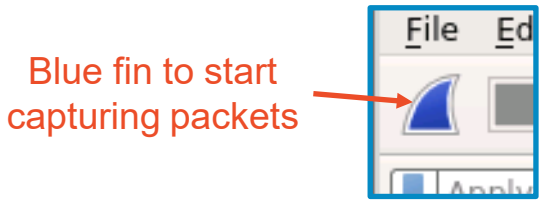
  `sudo wireshark`

- In the "…using this filter:" option, type

  `host <Windows-IP-Address>`

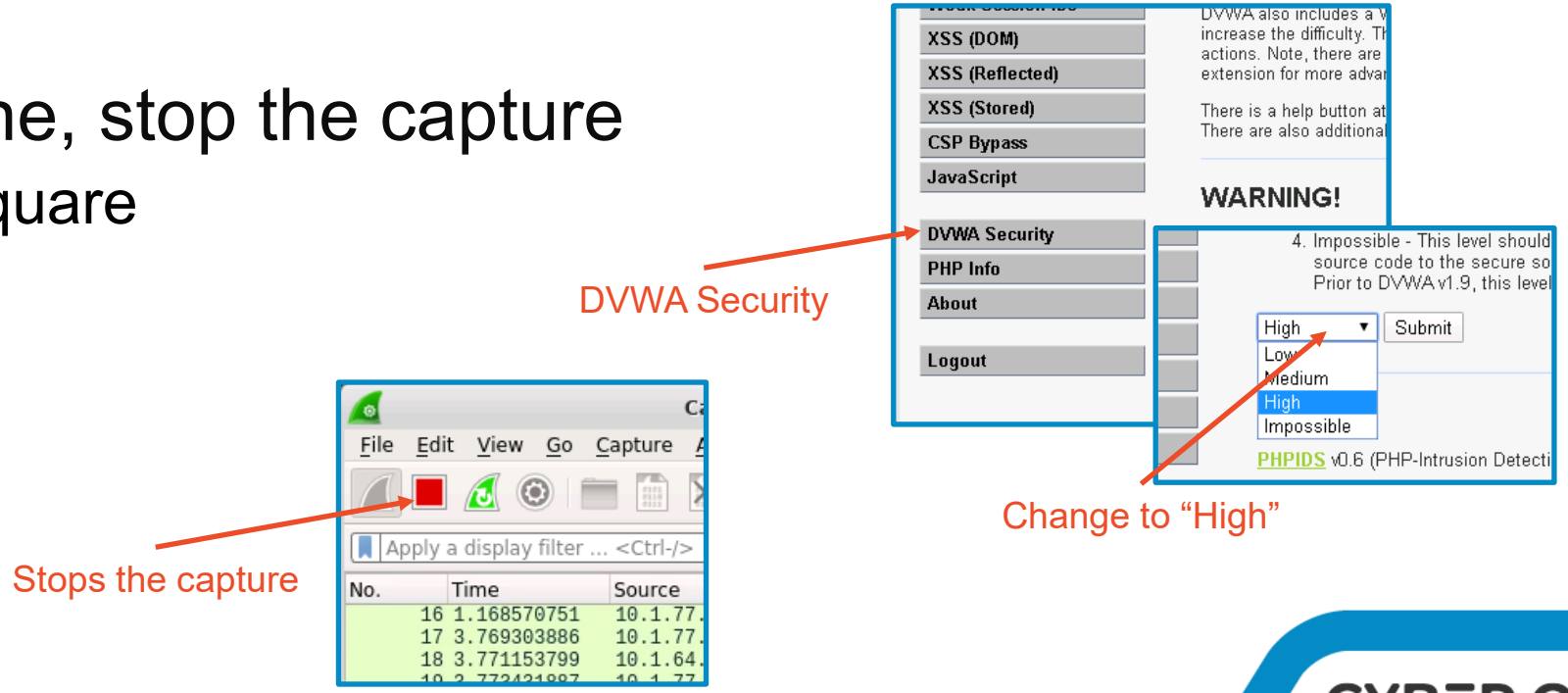
  - This will only find packets from the Windows machine
  - Select the "any" network below
- Click on the blue fin to start capturing packets





Capture the Session ID

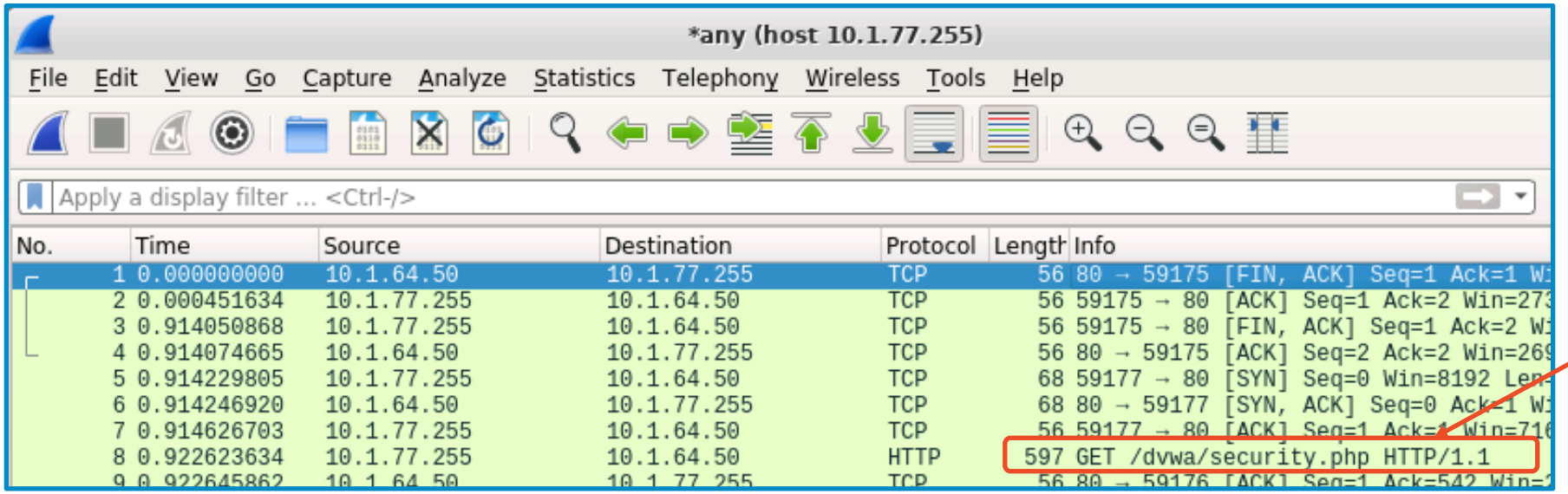
- On the Windows 7 machine, change the security to “High”
  - Click on the DVWA Security tab
  - On the dropdown menu, change “Impossible” to “High”
  - Click Submit
- On the Kali machine, stop the capture
  - Click on the red square



Capture the Session ID

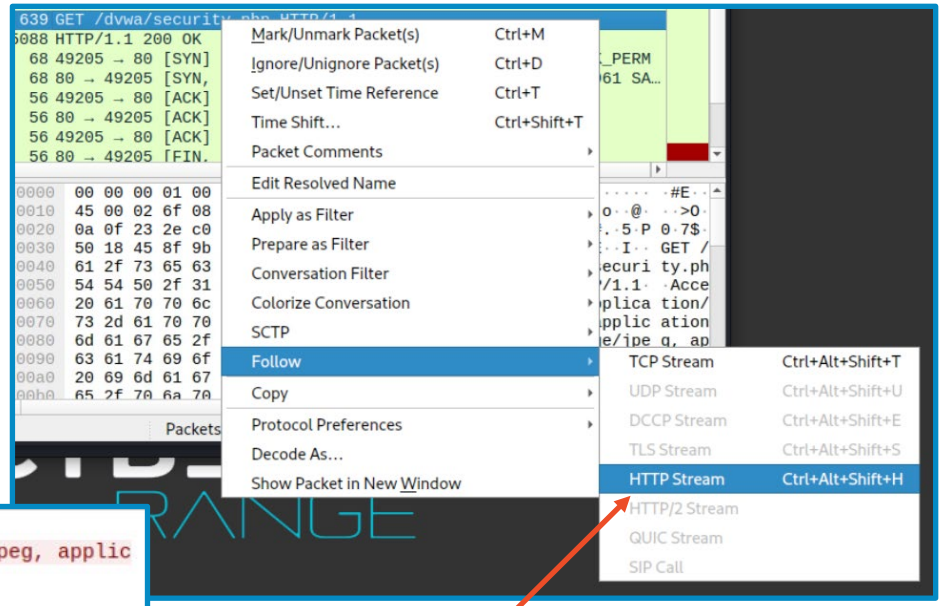
- In the packet capture, look for the following HTTP request in Info:

  `GET /dvwa/security.php`



Capture the Session ID

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



Follow the HTTP Stream

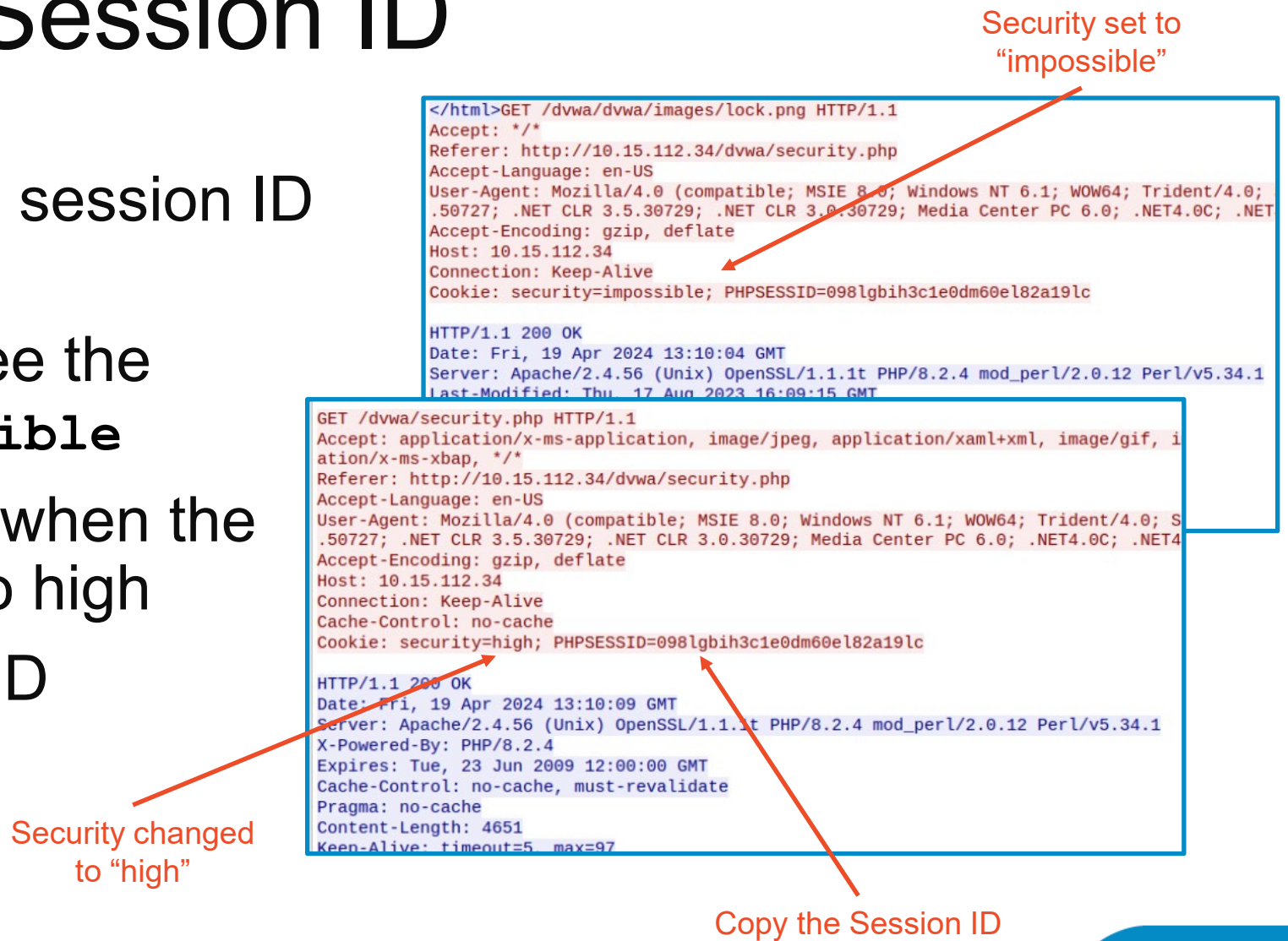
```
GET /dvwa/security.php HTTP/1.1
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg, applic
ation/x-ms-xbap, */*
Referer: http://10.15.112.34/dvwa/index.php
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; 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, 23 Jun 2009 12:00:00 GMT
```

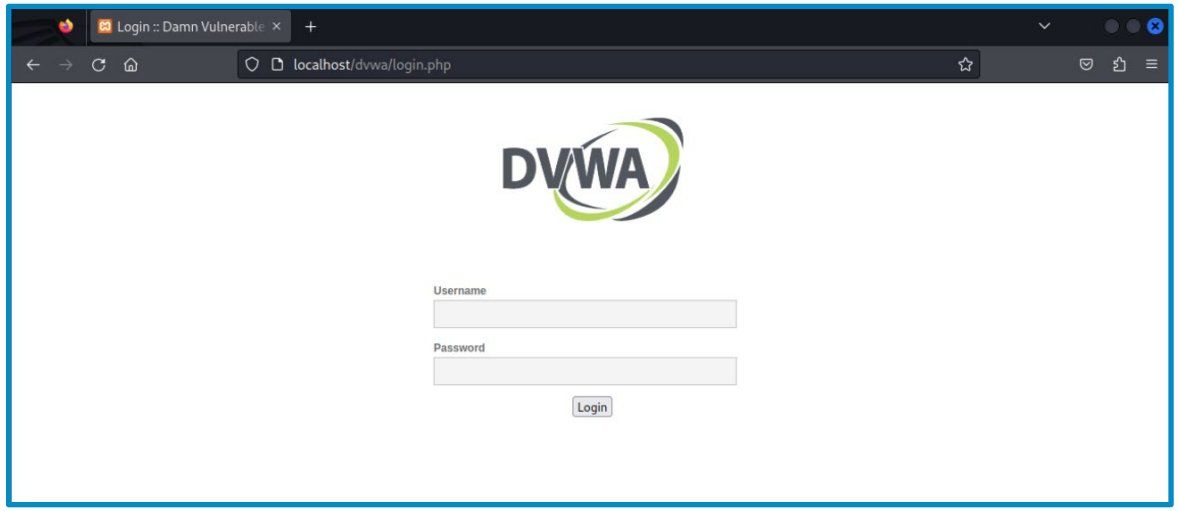
The HTTP Stream

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



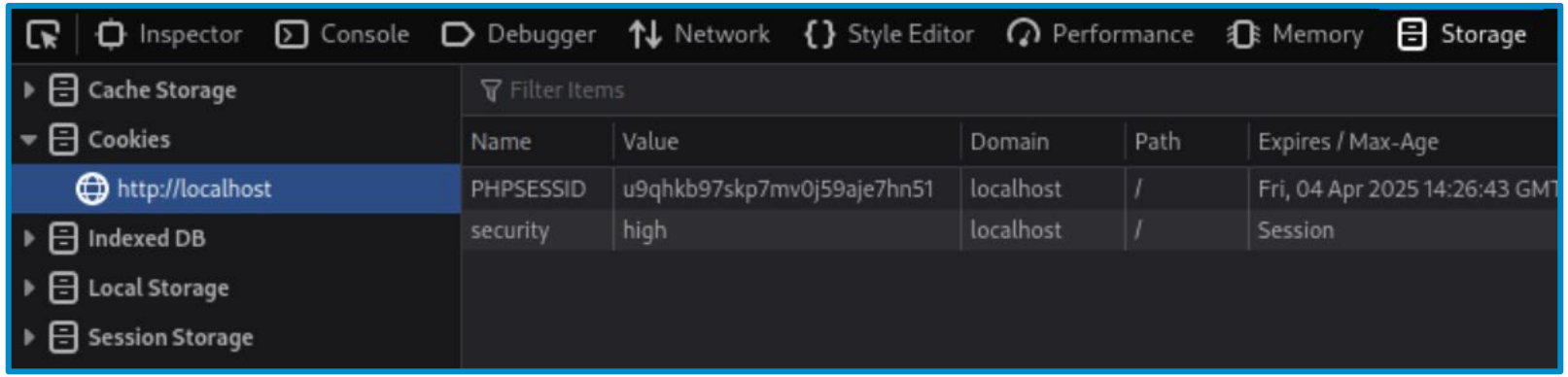
Using the Session ID



- 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

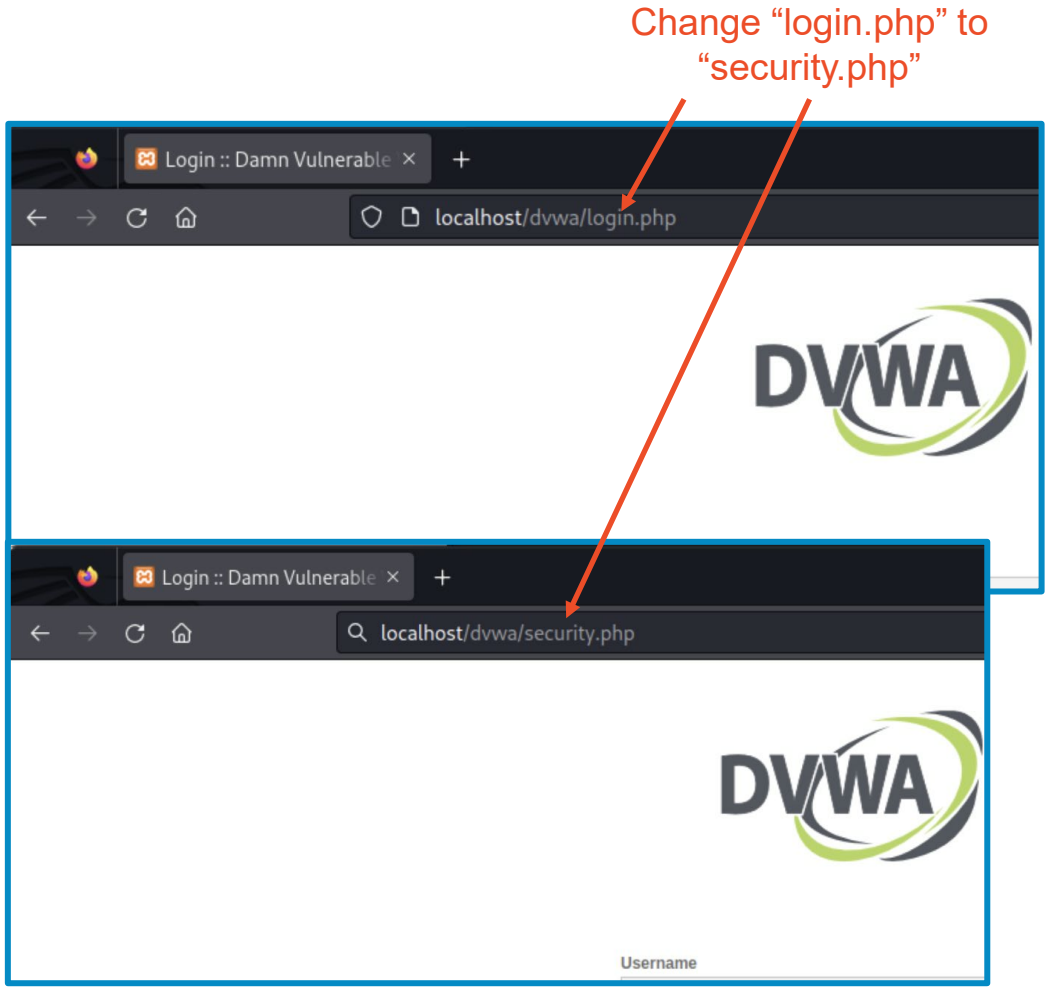
Open Web Developers Tools

- 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?