

LAB: 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:

Usernames

Passwords

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

Solution

I did the same thing as in the previous lab. Brute-forcing the username and password but it didn't work out as they've fixed the response-error for wrong username from the previous lab. Which means, if we try to brute-force usernames directly without any changes, It won't get us anywhere because of the same response "Wrong username or password".

I also was cautious about the response time, but no lucks so far!

I noticed something strange that the response length is different after a set of usernames. However, there's no pattern to why response length for a set of username differ to other.

Which makes me curious as to what is causing the length to change?

Username enumeration via subtly different responses

```
</title>
</head>
<body>
<script>
  fetch('/analytics?id=64414049')
</script>
<script src="/resources/labheader/js/labHeader.js">
</script>
<div id="academyLabHeader">
  <section class='academyLabBanner'>
    <div class=container>
      <div class=logo>
```

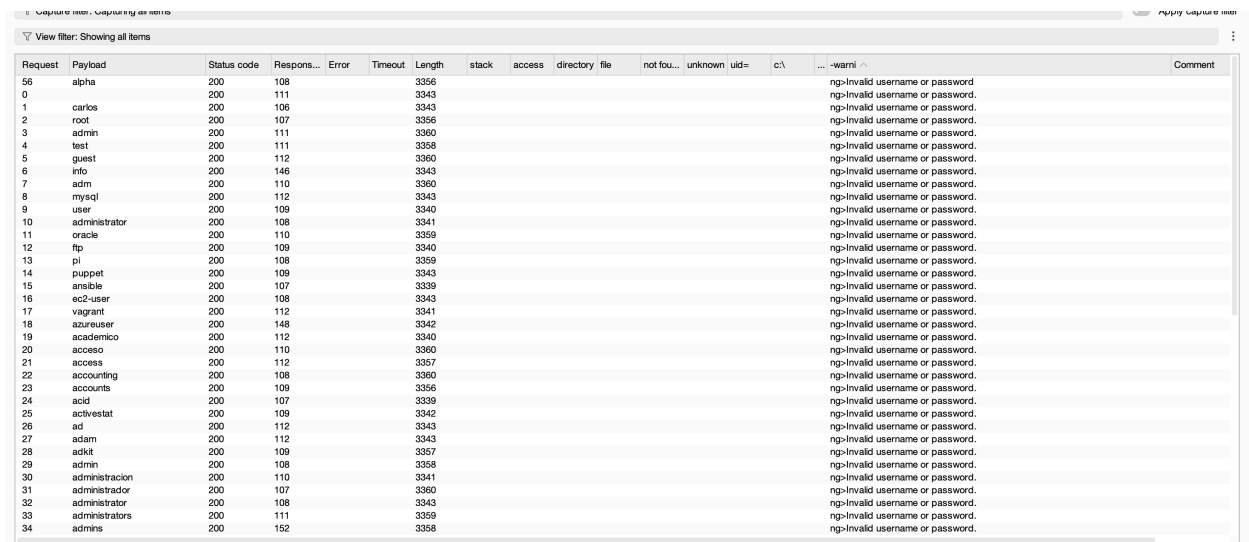
The IDs here but i now suspect that the response for the "right" username might be different.

So i made changes before triggering my next attack in the "Settings" option at the intruder page.

The screenshot shows the 'Define extract grep item' dialog box in Burp Suite. The 'Define start and end' section is active, with 'Start after expression' set to '-warni' and 'End at delimiter' set to '/p>\n'. The 'Extract from regex group' section is also visible, with a regex pattern '\-warni(?:.*)?/p>\n' and 'Case sensitive' checked. Below the dialog, a snippet of HTML is visible, showing a warning message and a login form. The 'Grep - Payloads' settings are also shown, with 'Search responses for payload strings' checked. The status bar at the bottom indicates 'Memory: 299.9MB' and 'Disabled'.

selecting that response element to see if it's exactly the same for each response.

Et le voila!



Request	Payload	Status code	Response	Error	Timeout	Length	stack	access	directory	file	not fou...	unknown	uid=	c:\	... -warni ^	Comment
56	alpha	200	108			3356										ng>Invalid username or password
0		200	111			3343										ng>Invalid username or password.
1	carlos	200	106			3343										ng>Invalid username or password.
2	root	200	107			3356										ng>Invalid username or password.
3	admin	200	111			3360										ng>Invalid username or password.
4	test	200	111			3358										ng>Invalid username or password.
5	guest	200	112			3360										ng>Invalid username or password.
6	info	200	146			3343										ng>Invalid username or password.
7	adm	200	110			3360										ng>Invalid username or password.
8	mysql	200	112			3343										ng>Invalid username or password.
9	user	200	109			3340										ng>Invalid username or password.
10	administrator	200	108			3341										ng>Invalid username or password.
11	oracle	200	110			3359										ng>Invalid username or password.
12	ftp	200	109			3340										ng>Invalid username or password.
13	pi	200	108			3359										ng>Invalid username or password.
14	puppet	200	109			3343										ng>Invalid username or password.
15	ansible	200	107			3339										ng>Invalid username or password.
16	ec2-user	200	108			3343										ng>Invalid username or password.
17	vagrant	200	112			3341										ng>Invalid username or password.
18	azureuser	200	148			3342										ng>Invalid username or password.
19	academico	200	112			3340										ng>Invalid username or password.
20	acceso	200	110			3360										ng>Invalid username or password.
21	access	200	112			3357										ng>Invalid username or password.
22	accounting	200	108			3360										ng>Invalid username or password.
23	accounts	200	109			3356										ng>Invalid username or password.
24	acid	200	107			3339										ng>Invalid username or password.
25	activestat	200	109			3342										ng>Invalid username or password.
26	ad	200	112			3343										ng>Invalid username or password.
27	adam	200	112			3343										ng>Invalid username or password.
28	adkit	200	109			3357										ng>Invalid username or password.
29	admin	200	108			3358										ng>Invalid username or password.
30	administracion	200	110			3341										ng>Invalid username or password.
31	administrador	200	107			3360										ng>Invalid username or password.
32	administrator	200	108			3343										ng>Invalid username or password.
33	administrators	200	111			3359										ng>Invalid username or password.
34	admins	200	152			3358										ng>Invalid username or password.

The 53rd Request has a different response. The "Subtle" response.

53rd Req : invalid username or password

Others : invalid username or password.

missing .

Now, brute forcing the passwords with alpha username:



28	TTTTTT	200	109			3340										ng>Invalid username or password
29	121212	200	109			3341										ng>Invalid username or password
30	000000	200	109			3340										ng>Invalid username or password
31	qazwsx	200	110			3341										ng>Invalid username or password
32	123qwe	200	110			187										
33	killer	200	110			3447										ng>Invalid username or password
34	trustno1	200	110			3447										ng>Invalid username or password
35	invtan	200	110			3430										ng>Invalid username or password

Final details

username: alpha

password: 123qwe

Congratulations, you solved the lab!

Share your skills!



[Continue learning >>](#)

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

My Account

Your username is: alpha

Your email is: alpha@normal-user.net

Email

Update email