Lab Pentest Report

Performed By
Priyanshu Patel

Start Date: 30 Aug 2023
End Date: 30 Aug 2023

Contact:
priyanshupatel2301@gmail.com

Scope: https://portswigger.net/web-security/sql-injection/lab-sql-injection-with-filter-bypass-via-xml-encoding
access the lab and that's our scope of testing.

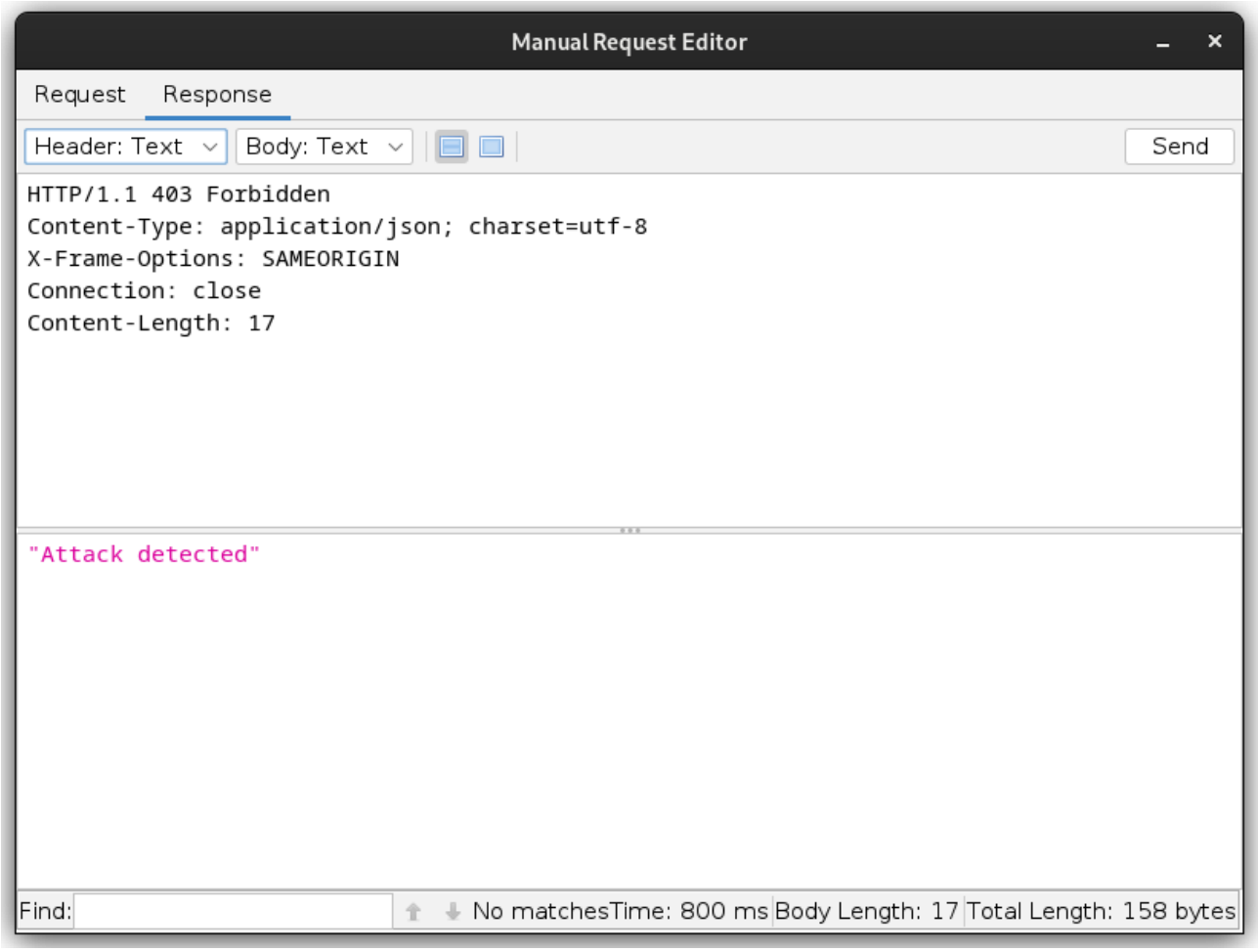
Goal Assesment:
what do we know?
1. vulnerable parameter is: stock check feature
2. query is returned on application's response
3. there's a users table which contains username and password
4. site has a web application firewall which will detect the obvious signs of SQLi
5. XML parameter of get request is where we put our payload

Attack Perspective:
we know the above stuff and other then that we are operating as blackbox perspective

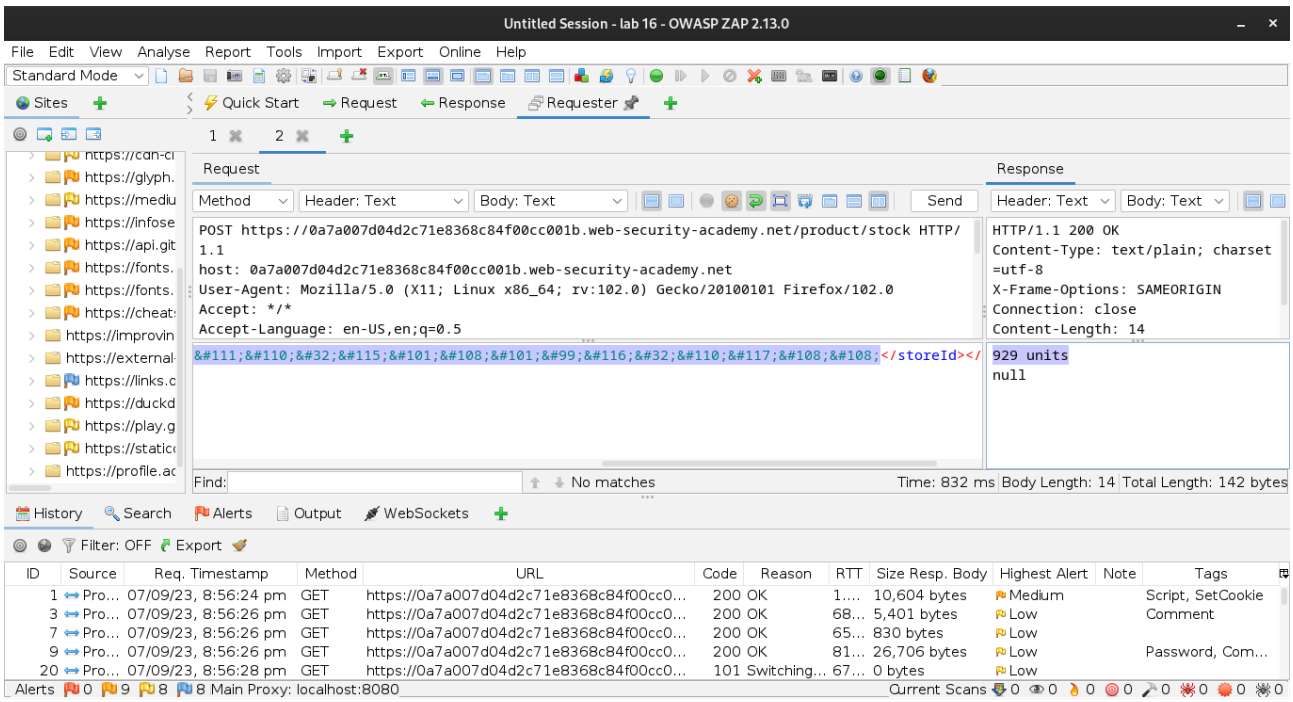
Tools used:
1. owasp-zap
2. firefox
3. foxy proxy (extension)
4. libreoffice writer (report writing)

Attacking The Lab Environment (Attack Steps):

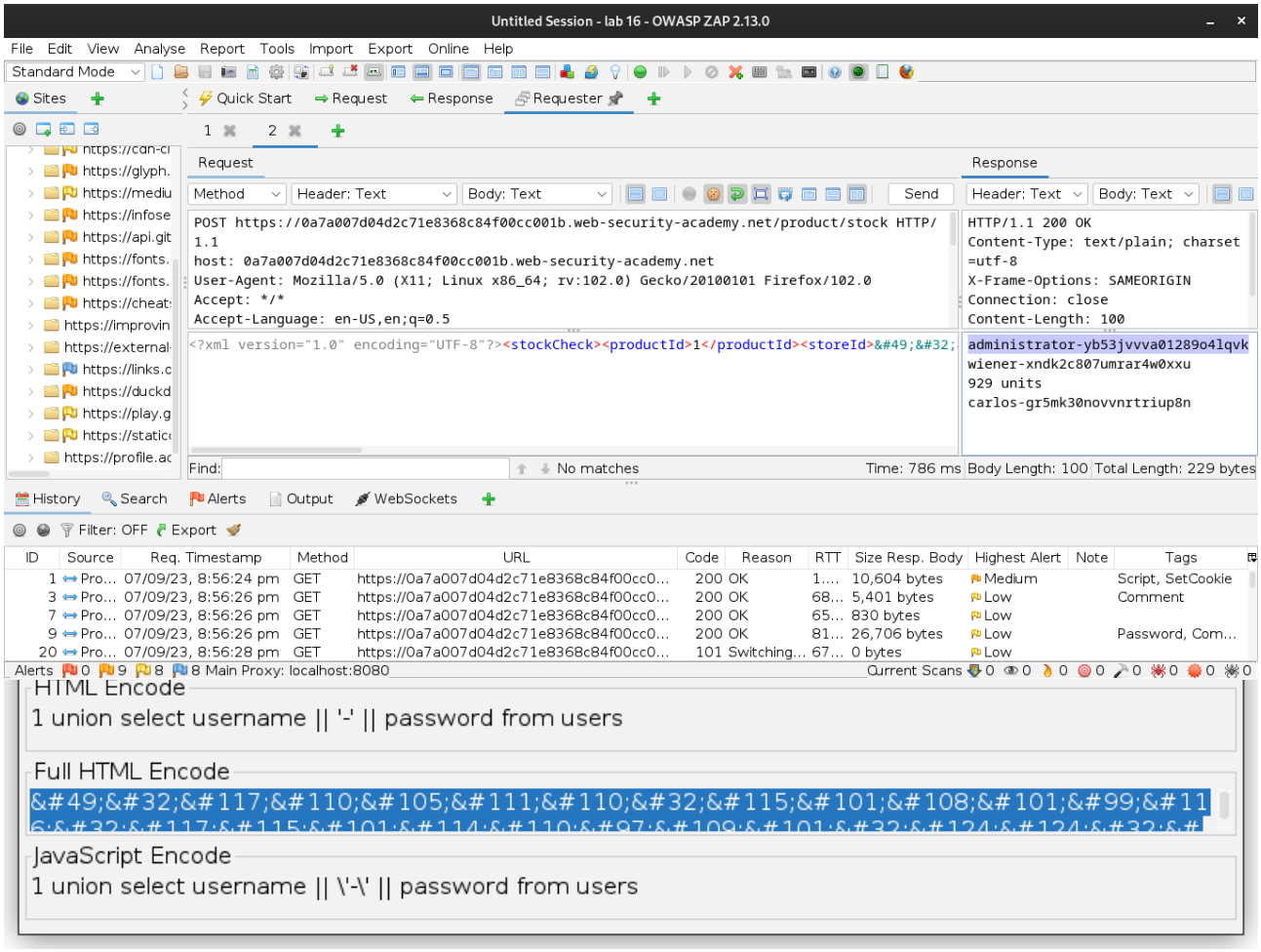
step 1:
tesing the first union select payload
and WAF detecting our payload with waring on site that "attack detected"



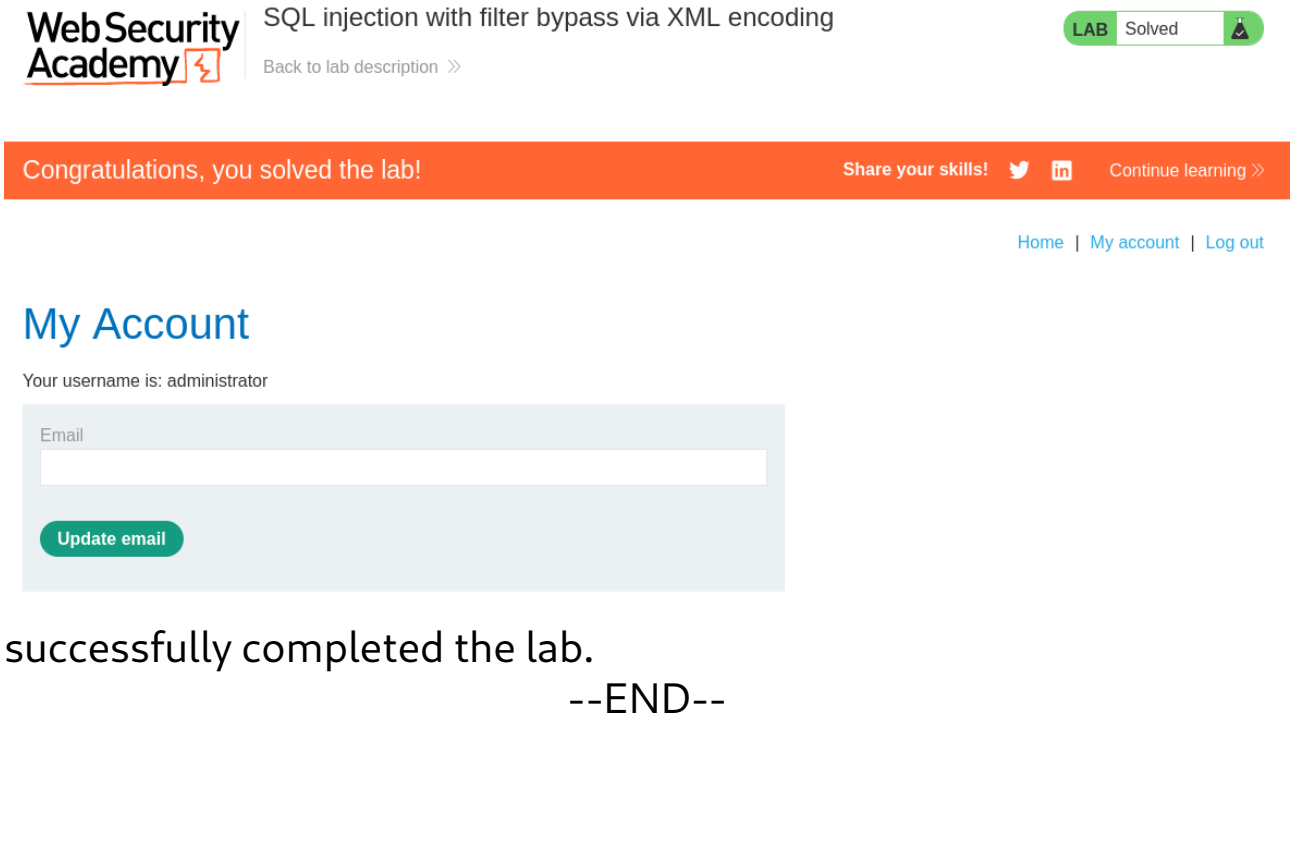
step 2:
encode our with full html payload that WAF no longer detects our payload. And shows number of units



Step 3:
get the username and password with union payload
payload: union select username || '-' || password from users
encode this payload to full html and then send
we get our username and passwords now just log in and we are done.



Okay as you can see above we have retrieved our password with our payload. Now we log in



successfully completed the lab.

--END--