



## 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:**

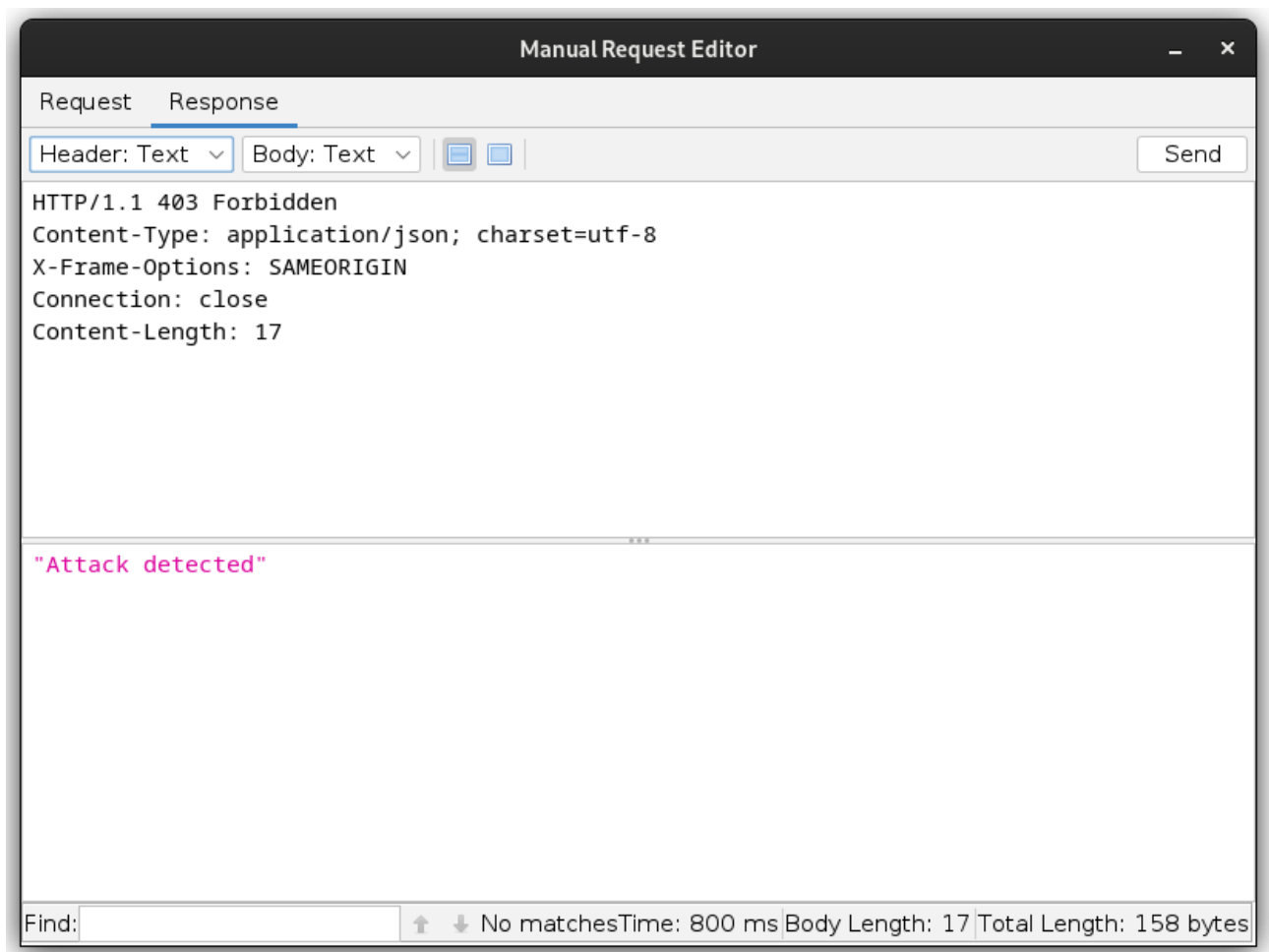
1. owasp-zap
2. firefox
3. foxy proxy (extension)
4. libreoffice writer (report writing)

### **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

Untitled Session - lab 16 - OWASP ZAP 2.13.0

File Edit View Analyse Report Tools Import Export Online Help

Standard Mode

Sites + Quick Start Request Response Requester +

1 2 +

Request

Method: POST URL: https://0a7a007d04d2c71e8368c84f00cc001b.web-security-academy.net/product/stock HTTP/1.1

Header: Text

Body: Text

Send

Response

Header: Text

Body: Text

HTTP/1.1 200 OK

Content-Type: text/plain; charset=utf-8

X-Frame-Options: SAMEORIGIN

Connection: close

Content-Length: 14

929 units

null

Find: No matches Time: 832 ms Body Length: 14 Total Length: 142 bytes

History Search Alerts Output WebSockets +

Filter: OFF Export

ID	Source	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
1	Pro...	07/09/23, 8:56:24 pm	GET	https://0a7a007d04d2c71e8368c84f00cc001b.web-security-academy.net/	200	OK	1...	10,604 bytes	Medium		Script, SetCookie
3	Pro...	07/09/23, 8:56:26 pm	GET	https://0a7a007d04d2c71e8368c84f00cc001b.web-security-academy.net/	200	OK	68...	5,401 bytes	Low		Comment
7	Pro...	07/09/23, 8:56:26 pm	GET	https://0a7a007d04d2c71e8368c84f00cc001b.web-security-academy.net/	200	OK	65...	830 bytes	Low		
9	Pro...	07/09/23, 8:56:26 pm	GET	https://0a7a007d04d2c71e8368c84f00cc001b.web-security-academy.net/	200	OK	81...	26,706 bytes	Low		Password, Com...
20	Pro...	07/09/23, 8:56:28 pm	GET	https://0a7a007d04d2c71e8368c84f00cc001b.web-security-academy.net/	101	Switching...	67...	0 bytes	Low		

Alerts 0 9 8 8 Main Proxy: localhost:8080 Current Scans 0 0 0 0 0 0 0 0 0 0

### 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.

