

Домашнее задание:

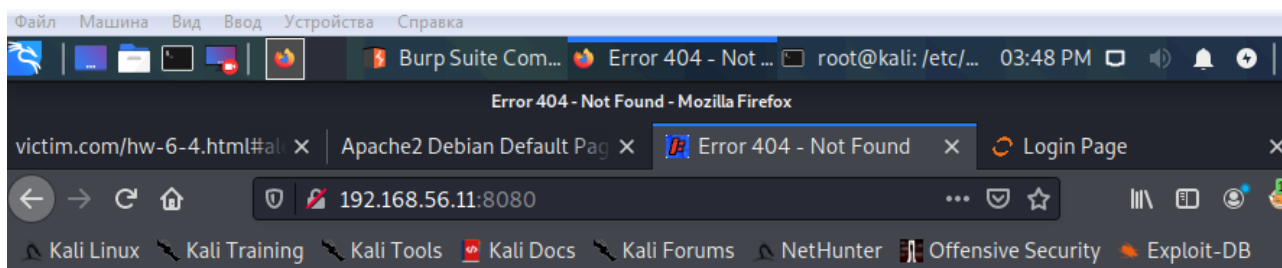
1. Найдите в ВМ Metasploitable 3 (Linux) адрес страницы Login Page проекта Continuum, который запущен на одном из кастомных портов (предварительно отключите межсетевой экран командой `iptables -F`, затем перезапустите `continuum` командой `service continuum restart`). В ответе укажите адрес страницы.
2. Какой сервис запущен на порту 6697 в ВМ Metasploitable 3 (Linux)?
3. Какой пароль пользователя `tim` из проекта `mutillidae`? В каком файле он содержится?

Домашнее задание (повышенная сложность):

1. \* В каком файле можно найти информацию о том, какой любимый фильм у юзера с именем `selene` (не является УЗ в `bwapp`)?
2. \* Составьте правило (или набор правил) для `mod_rewrite`, при помощи которого можно заблокировать доступ утилиты `curl` на веб сервер ВМ.

1.

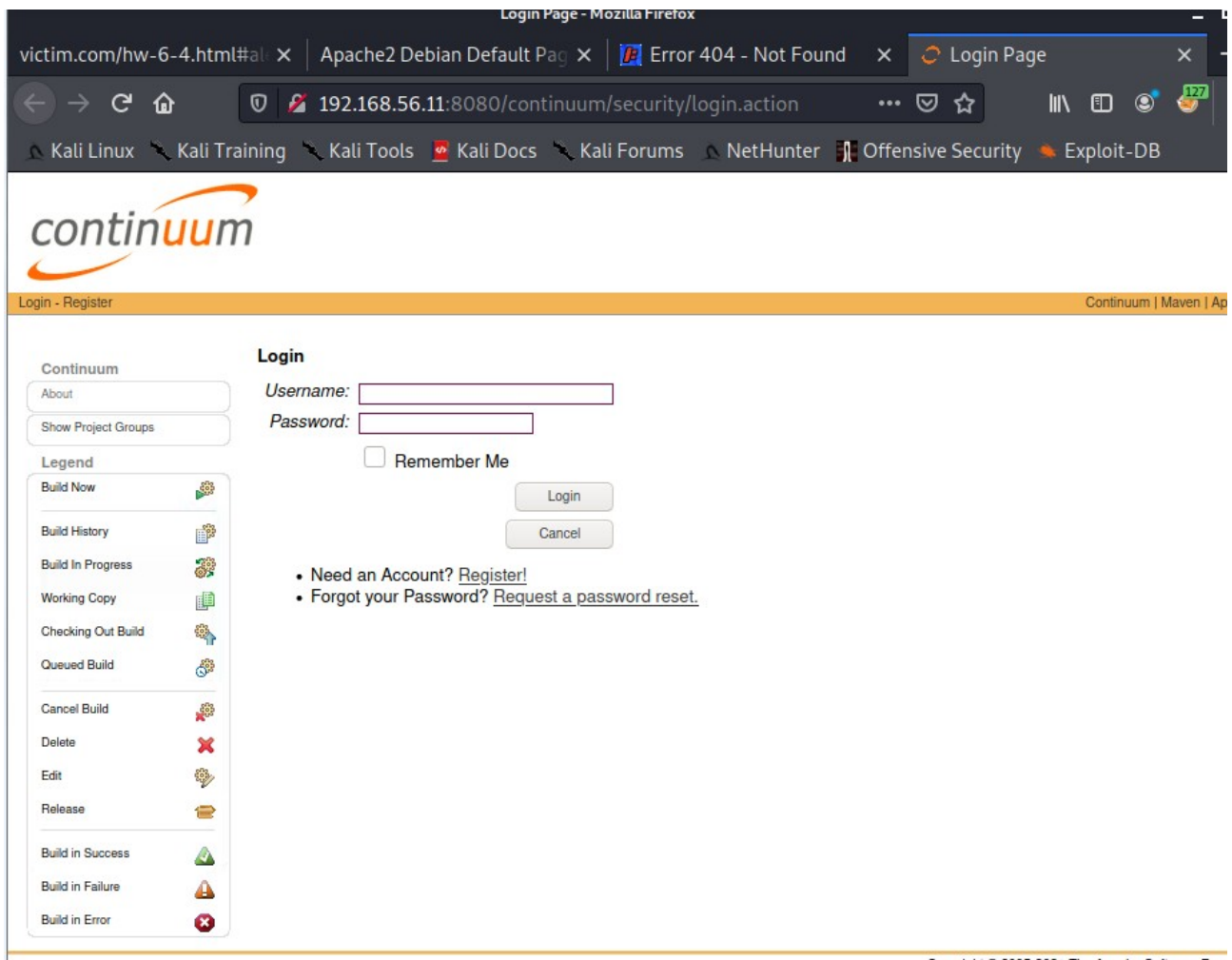
```
(root@kali)-[/etc/nginx/sites-available]
# nmap 192.168.56.11 -p21-10000
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-09 15:39 EDT
Nmap scan report for 192.168.56.11
Host is up (0.00021s latency).
Not shown: 9966 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
631/tcp   open  ipp
3306/tcp  open  mysql
6666/tcp  open  irc
6667/tcp  open  irc
6697/tcp  open  ircs-u
8067/tcp  open  infi-async
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
MAC Address: 08:00:27:48:80:0B (Oracle VirtualBox virtual NIC)
```



## Error 404 - Not Found.

No context on this server matched or handled this request.  
Contexts known to this server are:

- [/continuum ---> o.e.j.w.WebAppContext{/continuum,file:/opt/apache\\_continuum/apache-continuum-1.4.2/apps/continuum/},./apps/continuum](#)



2.

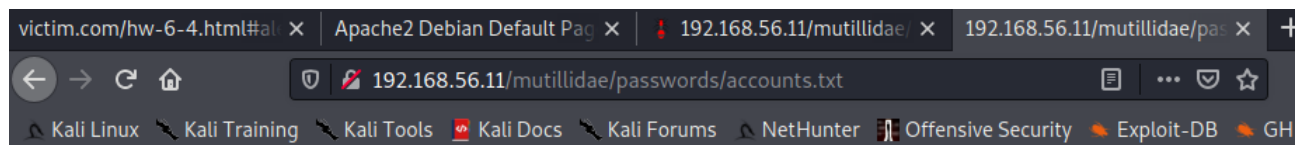
```
(root@kali)-[/etc/nginx/sites-available]
# nmap -sV 192.168.56.11 -p21-10000
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-09 16:04 EDT
Nmap scan report for 192.168.56.11
Host is up (0.00062s latency).
Not shown: 9966 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.5
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.11 (Ubuntu
80/tcp    open  http         Apache httpd
111/tcp   open  rpcbind      2-4 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp   open  ipp          CUPS 1.7
3306/tcp  open  mysql        MySQL (unauthorized)
6666/tcp  open  ftp          vsftpd 3.0.2
6667/tcp  open  irc          UnrealIRCd
6697/tcp  open  irc          UnrealIRCd
8067/tcp  open  irc          UnrealIRCd
```

3.

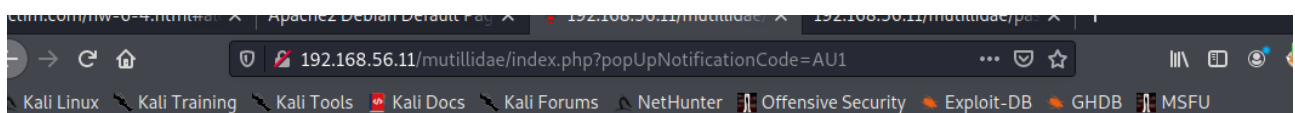
```
(root@kali)-[/etc/nginx/sites-available]
# nikto -host http://192.168.56.11/mutillidae
- Nikto v2.1.6 [word,zombie,films,rock!,admin]


+ Target IP: 192.168.56.11
+ Target Hostname: 192.168.56.11
+ Target Port: 80
+ Start Time: 2021-04-09 16:10:25 (GMT-4)

+ Server: Apache
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.26
+ The anti-clickjacking X-Frame-Options header is not present.
+ X-XSS-Protection header has been set to disable XSS Protection. There is unlikely to be a good reason for this.
+ Uncommon header 'logged-in-user' found, with contents:
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in
erent fashion to the MIME type
+ Cookie PHPSESSID created without the httponly flag
+ Cookie showhints created without the httponly flag
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ "robots.txt" contains 8 entries which should be manually viewed.
+ IP address found in the 'location' header. The IP is "127.0.1.1".
+ OSVDB-630: The web server may reveal its internal or real IP in the Location header via a request to /images over
0. The value is "127.0.1.1".
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.0
px for details.
+ /mutillidae/index.php?page=../../../../../../../../../../../../etc/passwd: The PHP-Nuke Rocket add-in is vulnerable to
versal, allowing an attacker to view any file on the host. (probably Rocket, but could be any index.php)
+ /mutillidae/phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-12184: /mutillidae/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information
tain HTTP requests that contain specific QUERY strings.
+ OSVDB-3268: /mutillidae/data/: Directory indexing found.
+ OSVDB-3092: /mutillidae/data/: This might be interesting...
+ OSVDB-3268: /mutillidae/includes/: Directory indexing found.
+ OSVDB-3092: /mutillidae/includes/: This might be interesting...
+ OSVDB-3268: /mutillidae/passwords/: Directory indexing found.
+ OSVDB-3092: /mutillidae/passwords/: This might be interesting...
```



```
1,admin,adminpass,g0t r00t?,Admin
2,adrian,somepassword,Zombie Films Rock!,Admin
3,john,monkey,I like the smell of confunk,Admin
4,jeremy,password,d1373 1337 speak,Admin
5,bryce,password,I Love SANS,Admin
6,samurai,samurai,Carving fools,Admin
7,jim,password,Rome is burning,Admin
8,bobby,password,Hank is my dad,Admin
9,simba,password,I am a super-cat,Admin
10,dreveil,password,Preparation H,Admin
11,scotty,password,Scotty do,Admin
12,cal,password,C-A-T-S Cats Cats Cats,Admin
13,john,password,Do the Duggie!,Admin
14,kevin,42,Doug Adams rocks,Admin
15,dave,set,Bet on S.E.T. FTW,Admin
16,patches,tortoise,meow,Admin
17,rocky,stripes,treats?,Admin
18,tim,lanmaster53,Because reconnaissance is hard to spell,Admin
19,Abdoo,66666666,Muffin tops only,Admin
```






## OWASP Mutillidae II: Keep Calm and Pwn On


**Version: 2.6.62**   **Security Level: 0 (Hosed)**   **Hints: Enabled (1 - Try easier)**   **Logged In User: tim (Because reconnaissance is hard to spell)**

[Home](#) | [Logout](#) | [Toggle Hints](#) | [Show Popup Hints](#) | [Toggle Security](#) | [Enforce SSL](#) | [Reset DB](#) | [View Log](#) | [View Captured Data](#)

OWASP 2017

OWASP 2013

 **Hints and Videos**

 **TIP: Click Hint and Videos**