OWASP Romania
InfoSec Conf - Bucharest 2013

The OWASP Foundation
http://www.owasp.org

Scanning Romania with Nessus (web part)

Adrian Furtună, PhD, OSCP, CEH
adif2k8@gmail.com

Introduction

What is this all about?

- ❑ The results of a passive vulnerability scan against ALL Romanian public IP addresses.
- ❑ Vulnerability scan:
  - Use an automated tool to detect vulnerabilities on a target system
  - Send probe ➔ Receive response ➔ Match against a signature database
  - Obtain a list of vulnerabilities that are not validated by exploitation
- ❑ Passive vulnerability scan:
  - Search for vulnerabilities on a target system without actually touching the system
  - The input data is provided by other systems

Introduction

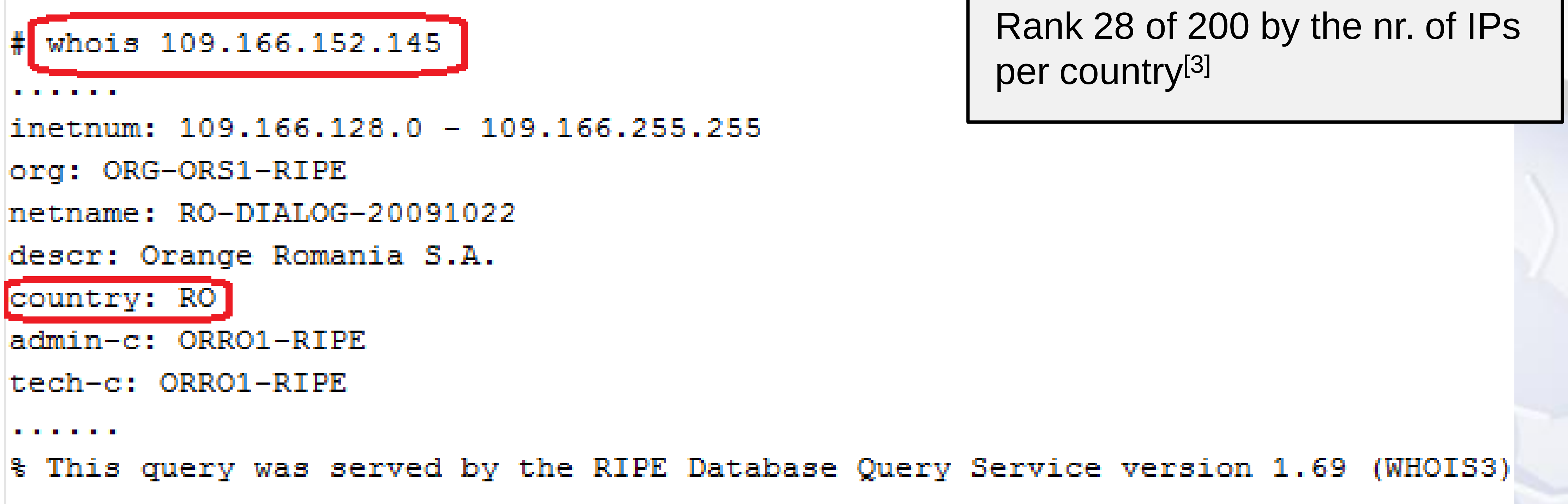
Objectives of this research

- Perform a quantitative analysis of the security state of Romania’s Internet
- Answer a few questions such as:
  - How many vulnerable systems are directly reachable?
  - Which are the vulnerable systems? What is their role?
  - What types of vulnerabilities affect Romania’s Internet?
  - How easily are they exploitable and what is the risk?

Introduction

Scope of this research (1)

- ALL Romanian public IP addresses
  - Source: RIPE[1] and MaxMind[2]



```
# whois 109.166.152.145
......
inetnum: 109.166.128.0 - 109.166.255.255
org: ORG-ORS1-RIPE
netname: RO-DIALOG-20091022
descr: Orange Romania S.A.
country: RO
admin-c: ORRO1-RIPE
tech-c: ORRO1-RIPE
......
% This query was served by the RIPE Database Query Service version 1.69 (WHOIS3)
```

  - Total: 1170 network ranges
  - Total: **13,847,000** IP addresses belonging to Romania

RO = 0.32% of Total IPv4 address space

Rank 28 of 200 by the nr. of IPs per country[3]

[1] http://www.ripe.net

[2] http://www.maxmind.com

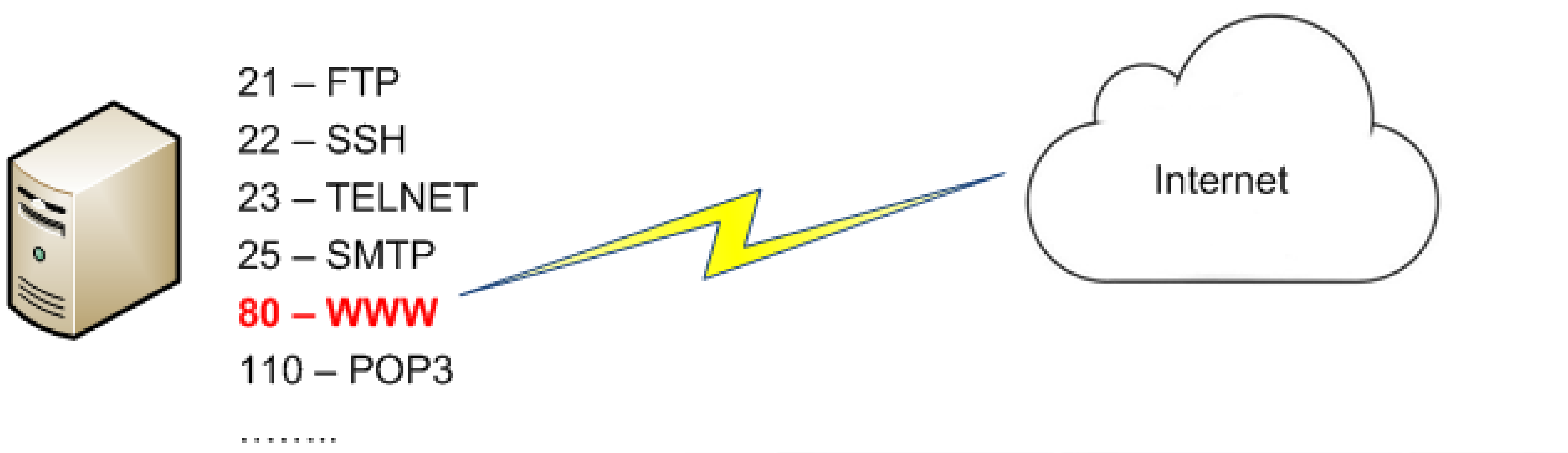
[3] http://en.wikipedia.org/wiki/List_of_countries_by_IPv4_address_allocation

Introduction
Scope of this research (2)

~2,500,000 web servers

= 18% of total RO IPs

- Only port 80 for now
- Vulnerabilities obtained from the HTTP response headers
  - Server type (e.g. Apache, IIS, nginx, lighttpd)
  - Server version (e.g. Apache 2.2.3, IIS 5.0)
  - Powered by: (e.g. PHP 5.1.3)



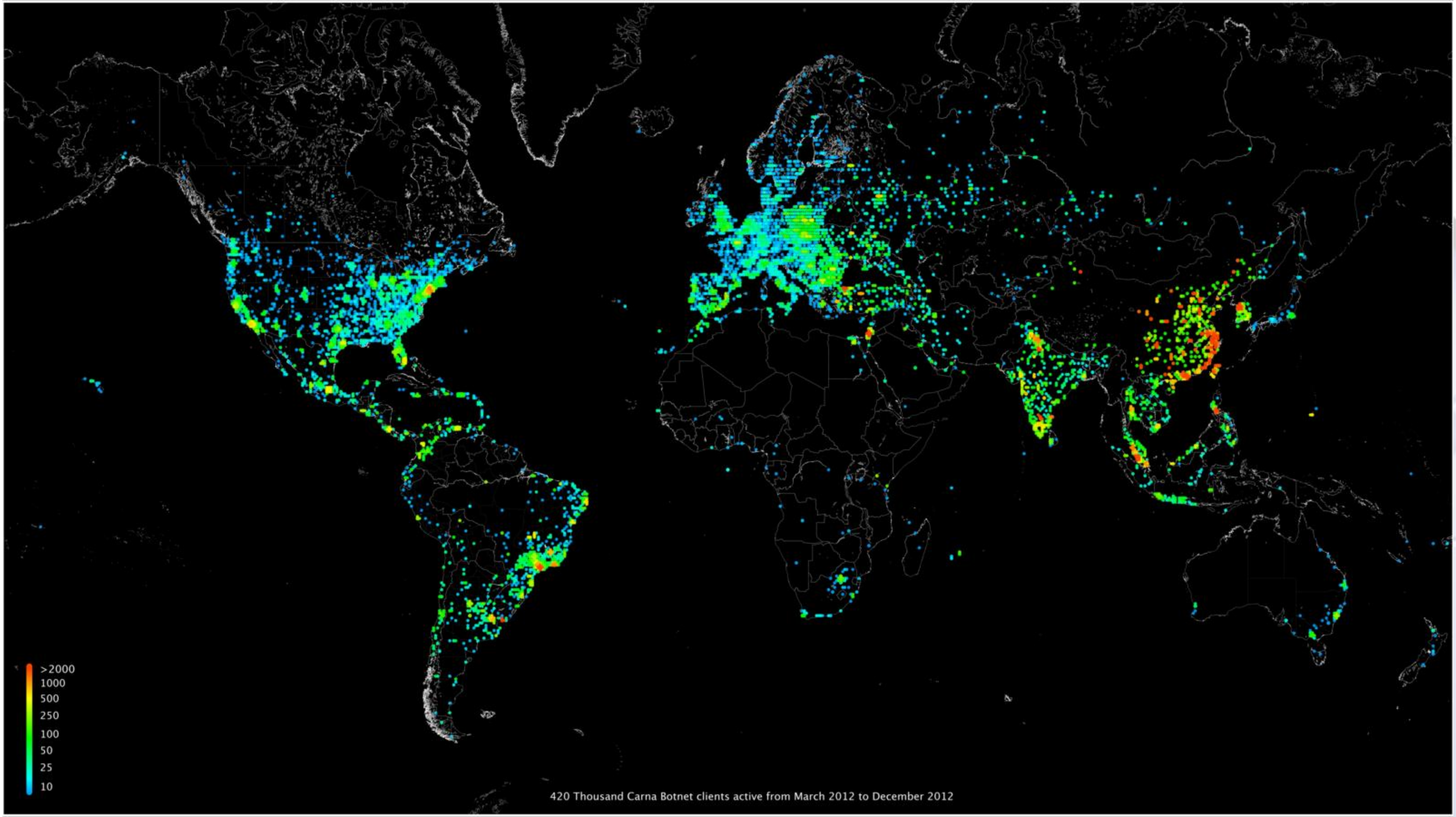
Source data

- CARNA Botnet – Internet Census 2012[1]
- Distributed scanner that used ~420K insecure devices to scan ALL internet (/0)
  - For each IP address:
    - ICMP ping
    - Reverse DNS
    - Scan 632 TCP ports + service probes
    - Scan 110 UDP ports + service probes
- Results are publicly available: 568 GB of compressed data ~= 9TB decompressed [2]

[1] http://internetcensus2012.bitbucket.org/

[2] http://internetcensus2012.bitbucket.org/download.html

CARNA Botnet - clients map

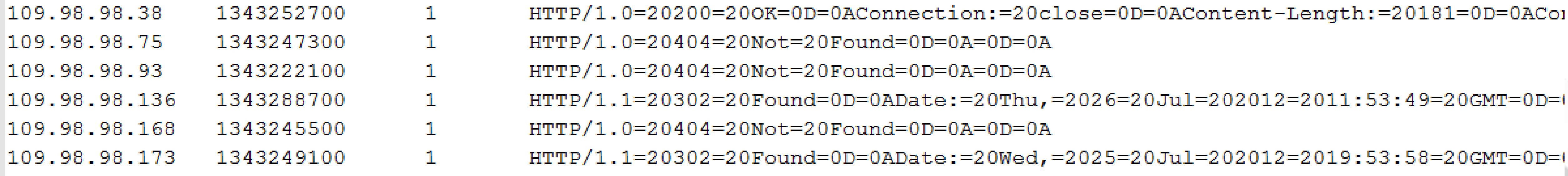


420 Thousand Carna Botnet clients active from March 2012 to December 2012

http://internetcensus2012.bitbucket.org/images/

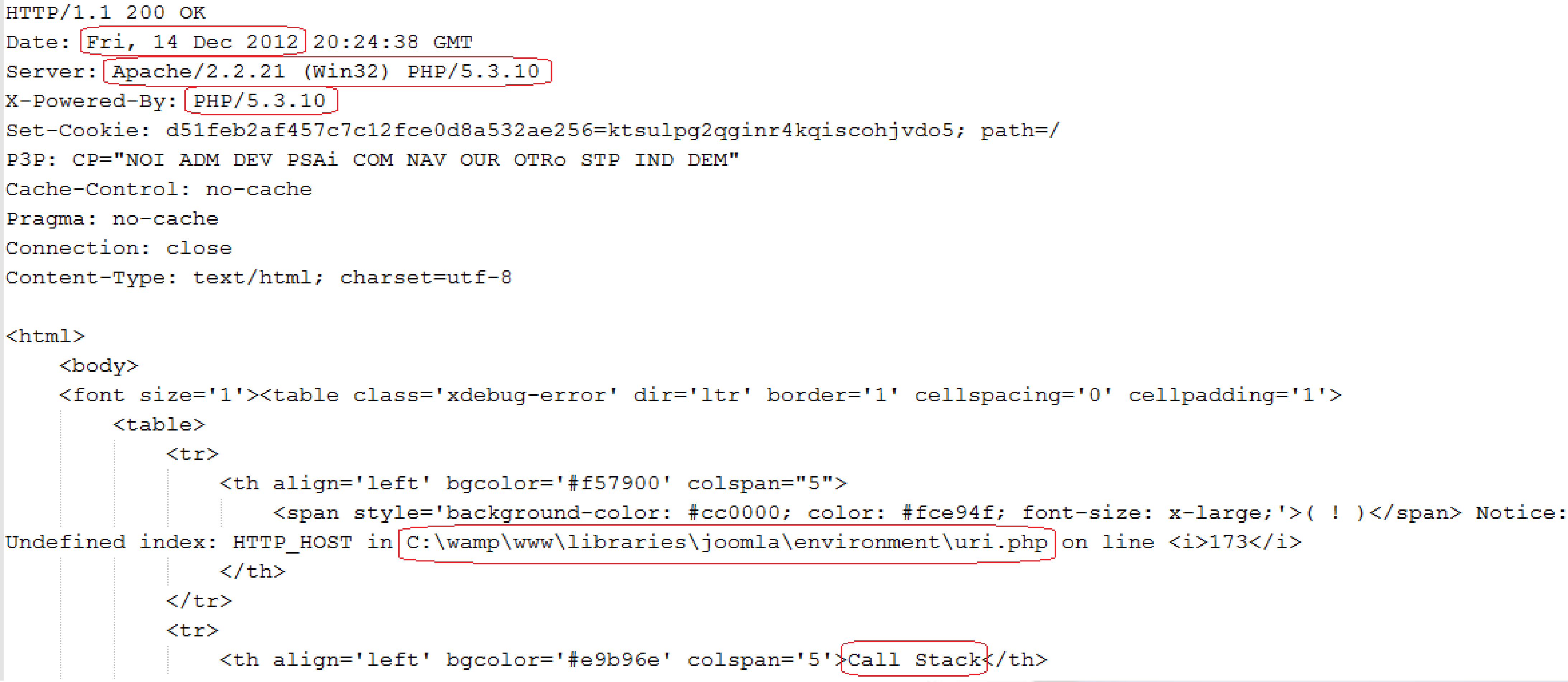
Sample data

Quoted-printable encoded



```
109.98.98.38     1343252700      1       HTTP/1.0=20200=20OK=0D=0AConnection:=20close=0D=0AContent-Length:=20181=0D=0ACo
109.98.98.75     1343247300      1       HTTP/1.0=20404=20Not=20Found=0D=0A=0D=0A
109.98.98.93     1343222100      1       HTTP/1.0=20404=20Not=20Found=0D=0A=0D=0A
109.98.98.136    1343288700      1       HTTP/1.1=20302=20Found=0D=0ADate:=20Thu,=2026=20Jul=202012=2011:53:49=20GMT=0D=
109.98.98.168    1343245500      1       HTTP/1.0=20404=20Not=20Found=0D=0A=0D=0A
109.98.98.173    1343249100      1       HTTP/1.1=20302=20Found=0D=0ADate:=20Wed,=2025=20Jul=202012=2019:53:58=20GMT=0D=
```

HTTP response decoded as:



```
HTTP/1.1 200 OK
Date: Fri, 14 Dec 2012 20:24:38 GMT
Server: Apache/2.2.21 (Win32) PHP/5.3.10
X-Powered-By: PHP/5.3.10
Set-Cookie: d51feb2af457c7c12fce0d8a532ae256=ktsulpg2qginr4kqiscohjvdo5; path=/
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Cache-Control: no-cache
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=utf-8

<html>
    <body>
    <font size='1'><table class='xdebug-error' dir='ltr' border='1' cellspacing='0' cellpadding='1'>
        <table>
            <tr>
                <th align='left' bgcolor='#f57900' colspan="5">
                    <span style='background-color: #cc0000; color: #fce94f; font-size: x-large;'>( ! )</span> Notice:
Undefined index: HTTP_HOST in C:\wamp\www\libraries\joomla\environment\uri.php on line <i>173</i>
                </th>
            </tr>
            <tr>
                <th align='left' bgcolor='#e9b96e' colspan='5'>Call Stack</th>
```

Vulnerability scanners

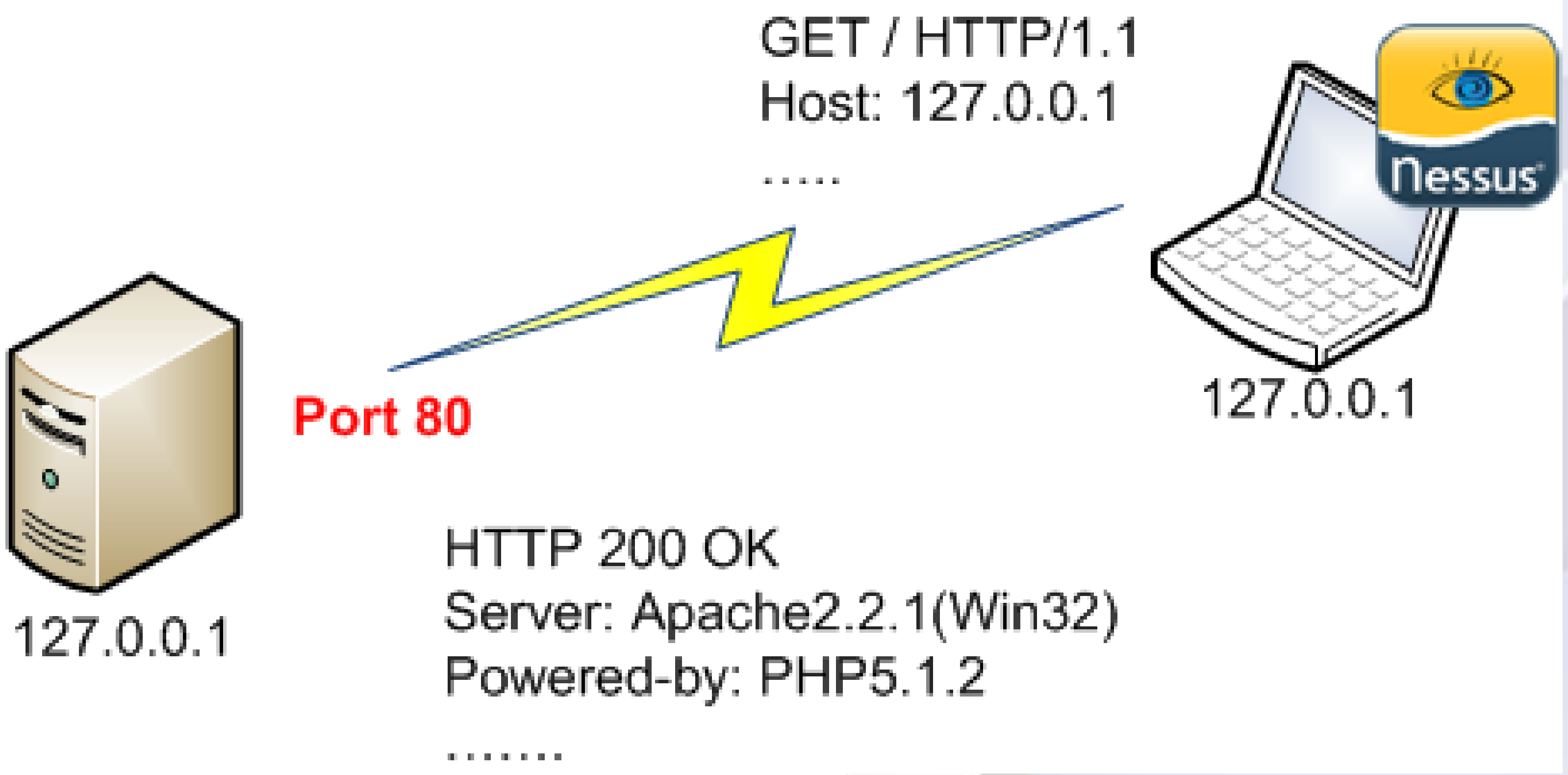
1. Nessus
2. Grep – search for vulns described in OWASP Top 10

Part 1: Nessus

Passive vulnerability scan (1)

Scanning approach:

- Simulate the target server on the local machine
- Scan the local machine with Nessus
- Respond to HTTP GET requests with the response of the real server



```
GET / HTTP/1.1
Host: 127.0.0.1
.....
```

```
HTTP 200 OK
Server: Apache2.2.1(Win32)
Powered-by: PHP5.1.2
.......
```

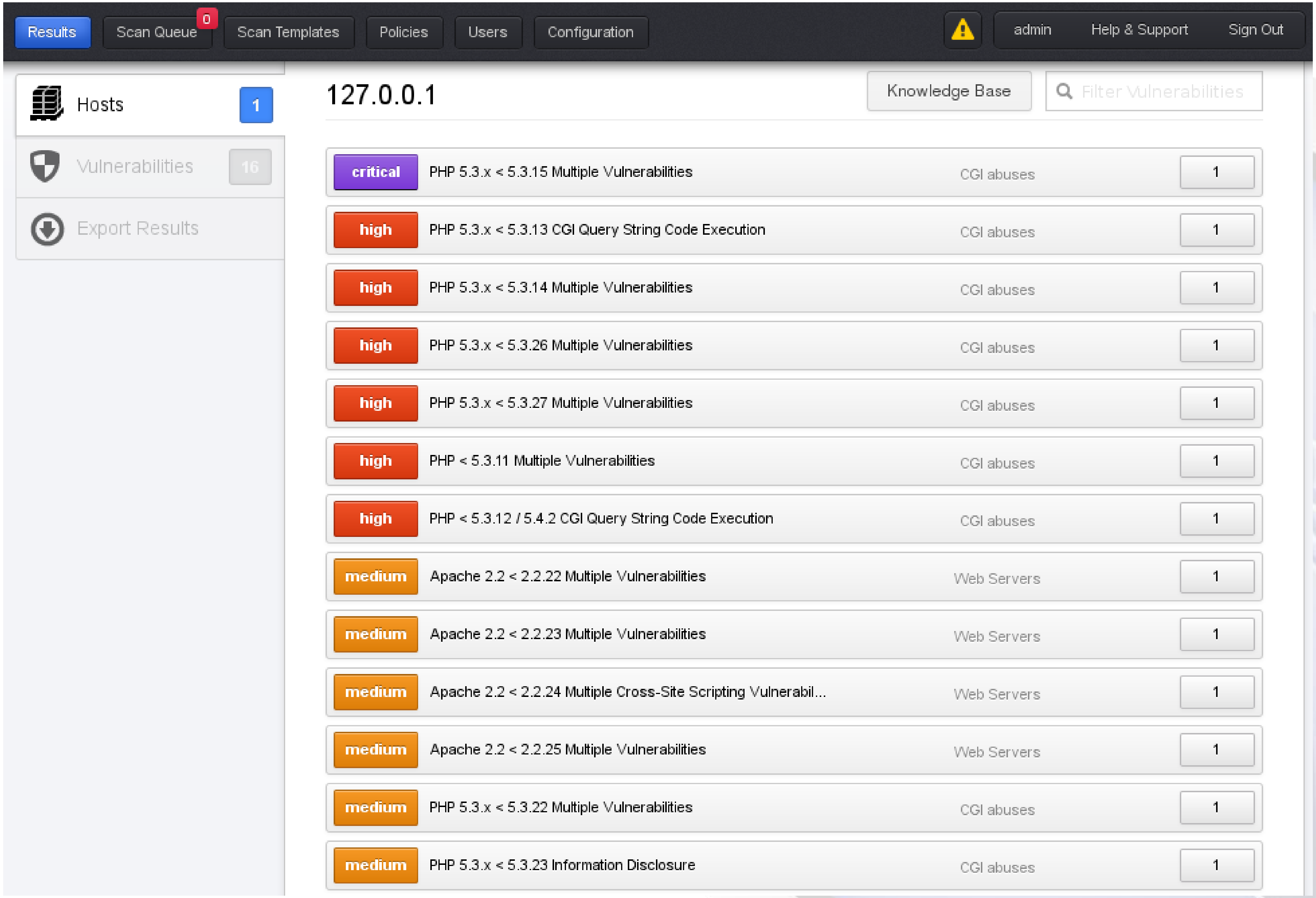
Passive vulnerability scan (2)

Enable only the following plugin families in Nessus:

- CGI Abuses
- Web Servers

Total 3527 plugins

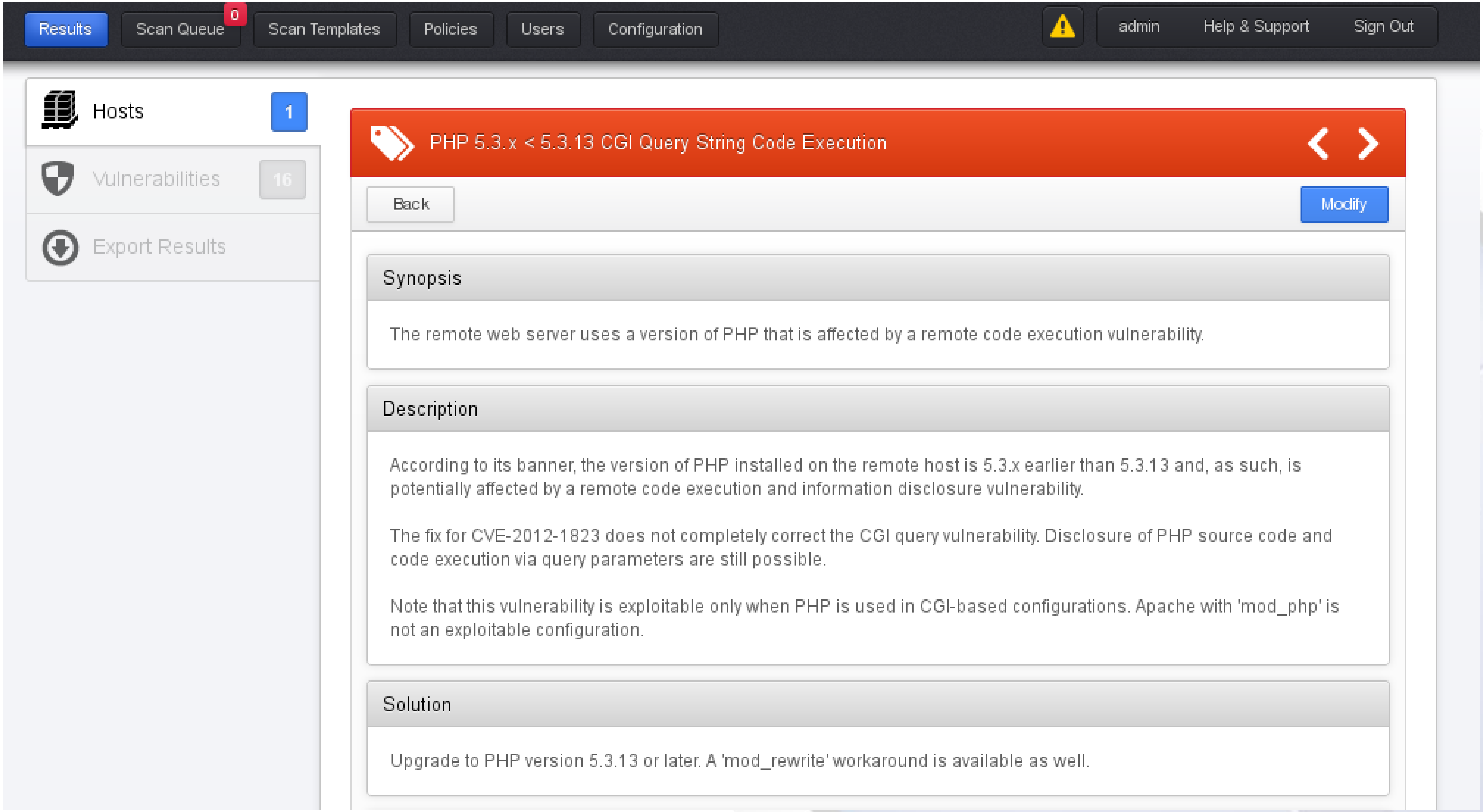
Nessus report on a single web server



127.0.0.1

critical	PHP 5.3.x < 5.3.15 Multiple Vulnerabilities	CGI abuses	1
high	PHP 5.3.x < 5.3.13 CGI Query String Code Execution	CGI abuses	1
high	PHP 5.3.x < 5.3.14 Multiple Vulnerabilities	CGI abuses	1
high	PHP 5.3.x < 5.3.26 Multiple Vulnerabilities	CGI abuses	1
high	PHP 5.3.x < 5.3.27 Multiple Vulnerabilities	CGI abuses	1
high	PHP < 5.3.11 Multiple Vulnerabilities	CGI abuses	1
high	PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution	CGI abuses	1
medium	Apache 2.2 < 2.2.22 Multiple Vulnerabilities	Web Servers	1
medium	Apache 2.2 < 2.2.23 Multiple Vulnerabilities	Web Servers	1
medium	Apache 2.2 < 2.2.24 Multiple Cross-Site Scripting Vulnerabil...	Web Servers	1
medium	Apache 2.2 < 2.2.25 Multiple Vulnerabilities	Web Servers	1
medium	PHP 5.3.x < 5.3.22 Multiple Vulnerabilities	CGI abuses	1
medium	PHP 5.3.x < 5.3.23 Information Disclosure	CGI abuses	1

Sample High risk vulnerability



PHP 5.3.x < 5.3.13 CGI Query String Code Execution

Synopsis

The remote web server uses a version of PHP that is affected by a remote code execution vulnerability.

Description

According to its banner, the version of PHP installed on the remote host is 5.3.x earlier than 5.3.13 and, as such, is potentially affected by a remote code execution and information disclosure vulnerability.

The fix for CVE-2012-1823 does not completely correct the CGI query vulnerability. Disclosure of PHP source code and code execution via query parameters are still possible.

Note that this vulnerability is exploitable only when PHP is used in CGI-based configurations. Apache with 'mod_php' is not an exploitable configuration.

Solution

Upgrade to PHP version 5.3.13 or later. A 'mod_rewrite' workaround is available as well.

Results

Top of Critical-risk vulnerabilities discovered

```
+----------+-------------------------------------------------------+---------------+--------+------------+
| Severity | Plugin Name                                           | CVE           | PlugID | Nr Servers |
+----------+-------------------------------------------------------+---------------+--------+------------+
| Critical | PHP 5.3.x < 5.3.15 Multiple Vulnerabilities           | CVE-2012-2688 |  60085 |    1959657 |
| Critical | PHP Unsupported Version Detection                     |               |  58987 |       9249 |
| Critical | Apache 2.2 < 2.2.15 Multiple Vulnerabilities          | CVE-2007-6750 |  45004 |       4902 |
| Critical | Apache 2.2 < 2.2.13 APR apr_palloc Heap Overflow      | CVE-2009-2412 |  57603 |       2833 |
| Critical | PHP 5.4.x < 5.4.5 _php_stream_scandir Overflow        | CVE-2012-2688 |  60086 |        371 |
| Critical | PHP 5.3.9 'php_register_variable_ex()' Code Execution | CVE-2012-0830 |  57825 |        335 |
| Critical | Apache mod_proxy Content-Length Overflow              | CVE-2004-0492 |  15555 |        264 |
| Critical | PHP 5.1.x < 5.1.5 Multiple Vulnerabilities            | CVE-2006-1017 |  17713 |        121 |
| Critical | Apache < 2.0.48 Multiple Vulnerabilities (OF, InfoDisc| CVE-2003-0789 |  11853 |         56 |
| Critical | Apache < 1.3.42 mod_proxy Integer Overflow            | CVE-2010-0010 |  44589 |          1 |
+----------+-------------------------------------------------------+---------------+--------+------------+
10 rows in set (0.30 sec)
```

Results

Top of High-risk vulnerabilities discovered (1)

```
+----------+------------------------------------------------------+---------------+--------+------------+
| Severity | Plugin Name                                          | CVE           | PlugID | Nr Servers |
+----------+------------------------------------------------------+---------------+--------+------------+
| High     | PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution | CVE-2012-1823 |  58988 |    1967941 |
| High     | PHP < 5.3.11 Multiple Vulnerabilities                | CVE-2011-1398 |  58966 |    1967914 |
| High     | PHP 5.3.x < 5.3.14 Multiple Vulnerabilities          | CVE-2012-2143 |  59529 |    1959046 |
| High     | PHP 5.3.x < 5.3.13 CGI Query String Code Execution   | CVE-2012-2311 |  59056 |    1958619 |
| High     | PHP < 5.3.9 Multiple Vulnerabilities                 | CVE-2011-3379 |  57537 |      12823 |
| High     | PHP < 5.2.11 Multiple Vulnerabilities                | CVE-2009-3291 |  41014 |       4703 |
| High     | PHP 5.2 < 5.2.14 Multiple Vulnerabilities            | CVE-2007-1581 |  48244 |       4149 |
| High     | Apache 2.2 < 2.2.14 Multiple Vulnerabilities         | CVE-2009-2699 |  42052 |       4092 |
| High     | PHP < 5.2.8 Multiple Vulnerabilities                 | CVE-2008-5814 |  35067 |       3081 |
| High     | PHP 5.3 < 5.3.7 Multiple Vulnerabilities             | CVE-2011-1148 |  55925 |       2288 |
| High     | PHP 5 < 5.2.7 Multiple Vulnerabilities               | CVE-2008-2371 |  35043 |       1950 |
| High     | Unsupported Web Server Detection                     |               |  34460 |       1918 |
| High     | PHP 5.3 < 5.3.6 Multiple Vulnerabilities             | CVE-2011-0421 |  52717 |       1916 |
| High     | Apache 2.0 < 2.0.65 Multiple Vulnerabilities         | CVE-2011-3192 |  68914 |       1393 |
| High     | PHP < 5.2.6 Multiple Vulnerabilities                 | CVE-2007-4850 |  32123 |       1344 |
| High     | PHP 5.3 < 5.3.4 Multiple Vulnerabilities             | CVE-2006-7243 |  51140 |       1151 |
| High     | PHP < 4.4.9 Multiple Vulnerabilities                 | CVE-2007-4850 |  33849 |       1091 |
| High     | PHP < 4.4.5 Multiple Vulnerabilities                 | CVE-2006-4625 |  24906 |       1056 |
| High     | PHP < 4.4.3 / 5.1.4 Multiple Vulnerabilities         | CVE-2006-0996 |  22268 |        755 |
| High     | Apache < 1.3.37 mod_rewrite LDAP Protocol URL Overfl | CVE-2006-3747 |  31654 |        721 |
| High     | PHP 5.3 < 5.3.3 Multiple Vulnerabilities             | CVE-2007-1581 |  48245 |        711 |
| High     | PHP < 4.4.4 Multiple Vulnerabilities                 | CVE-2006-1017 |  17710 |        662 |
| High     | Apache 2.0 < 2.0.64 Multiple Vulnerabilities         | CVE-2008-2364 |  50069 |        579 |
| High     | PHP < 4.4.1 / 5.0.6 Multiple Vulnerabilities         | CVE-2002-0229 |  20111 |        539 |
...
```

Results

Top of High-risk vulnerabilities discovered (2)

```
...
| High     | Apache < 2.0.59 mod_rewrite LDAP Protocol URL Overfl| CVE-2006-3747 |  31655 |         334 |
| High     | PHP 5.x < 5.2.2 Information Disclosure              | CVE-2007-1649 |  17797 |         323 |
| High     | PHP < 4.3.11 / 5.0.3 Multiple Unspecified Vulnerabil|               |  18033 |         304 |
| High     | Apache < 2.0.55 Multiple Vulnerabilities            | CVE-2005-1268 |  31656 |         282 |
| High     | PHP < 5.2.1 Multiple Vulnerabilities                | CVE-2006-6383 |  24907 |         259 |
| High     | Apache < 1.3.29 Multiple Modules Local Overflow     | CVE-2003-0542 |  11915 |         254 |
| High     | Apache < 1.3.28 Multiple Vulnerabilities (DoS, ID)  | CVE-2003-0460 |  11793 |         231 |
| High     | PHP 5.x < 5.2 Multiple Vulnerabilities              | CVE-2006-1015 |  31649 |         228 |
| High     | PHP < 4.3.10 / 5.0.3 Multiple Vulnerabilities       | CVE-2004-1018 |  15973 |         179 |
| High     | PHP 5.4.x < 5.4.4 Multiple Vulnerabilities          | CVE-2012-2143 |  59530 |         138 |
| High     | Apache <= 2.0.51 Satisfy Directive Access Ctl Bypass| CVE-2004-0811 |  14803 |         114 |
| High     | Apache Chunked Encoding Remote Overflow             | CVE-2002-0392 |  11030 |          62 |
| High     | Apache < 1.3.27 Multiple Vulnerabilities (DoS, XSS) | CVE-2002-0839 |  11137 |          61 |
| High     | PHP < 4.3.3 Multiple Vulnerabilities                | CVE-2002-1396 |  11850 |          54 |
| High     | mod_ssl ssl_util_uuencode_binary Remote Overflow    | CVE-2004-0488 |  12255 |          42 |
| High     | Apache mod_ssl ssl_engine_log.c mod_proxy Hook Funct| CVE-2004-0700 |  13651 |          35 |
| High     | PHP 4.x < 4.3.0 ZendEngine Integer Overflow         | CVE-2006-4812 |  17796 |          30 |
| High     | PHP 5.4.x < 5.4.3 Multiple Vulnerabilities          | CVE-2012-2311 |  59057 |          19 |
| High     | Oracle GlassFish Server 2.1.1 < 2.1.1.14            | CVE-2011-3559 |  58089 |          11 |
| High     | PHP 5.1.x < 5.1.2 Multiple Vulnerabilities          | CVE-2006-0200 |  17712 |          10 |
| High     | PHP 5.3.7 crypt() MD5 Incorrect Return Value        | CVE-2011-3189 |  55969 |           5 |
| High     | Apache-SSL SSLVerifyClient SSLFakeBasicAuth Certific| CVE-2004-0009 |  12046 |           3 |
| High     | PHP < 4.3.1 CGI Module Force Redirect Settings Bypas| CVE-2003-0097 |  11237 |           2 |
| High     | Apache mod_jk2 Host Header Multiple Fields Remote Ov| CVE-2007-6258 |  31786 |           1 |
| High     | Apache < 2.0.44 DOS Device Name Multiple Remote Vuln| CVE-2003-0016 |  11209 |           1 |
| High     | mod_python < 2.7.8 Module Importing Privilege Execut| CVE-2002-0185 |  10947 |           1 |
+----------+-----------------------------------------------------+---------------+--------+-------------+
50 rows in set (0.48 sec)
```

Results

Top of Medium-risk vulnerabilities discovered (1)

```
+----------+-----------------------------------------------------+---------------+--------+------------+
| Severity | Plugin Name                                         | CVE           | PlugID | Nr Servers |
+----------+-----------------------------------------------------+---------------+--------+------------+
| Medium   | Apache 2.2 < 2.2.23 Multiple Vulnerabilities        | CVE-2012-0883 |  62101 |      10938 |
| Medium   | Apache 2.2 < 2.2.22 Multiple Vulnerabilities        | CVE-2011-3368 |  57791 |       9672 |
| Medium   | Apache 2.2 < 2.2.21 mod_proxy_ajp DoS               | CVE-2011-3348 |  56216 |       8571 |
| Medium   | Apache 2.2 < 2.2.18 APR apr_fnmatch DoS             | CVE-2011-0419 |  53896 |       7463 |
| Medium   | Apache 2.2 < 2.2.17 Multiple Vulnerabilities        | CVE-2009-3560 |  50070 |       6713 |
| Medium   | Apache 2.2 < 2.2.16 Multiple Vulnerabilities        | CVE-2010-1452 |  48205 |       6299 |
| Medium   | PHP 5.2 < 5.2.17 / 5.3 < 5.3.5 String To Double Conv| CVE-2010-4645 |  51439 |       6205 |
| Medium   | PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities       | CVE-2010-1128 |  44921 |       5608 |
| Medium   | PHP < 5.2.12 Multiple Vulnerabilities               | CVE-2009-3557 |  43351 |       4843 |
| Medium   | PHP 5.2 < 5.2.15 Multiple Vulnerabilities           | CVE-2010-3436 |  51139 |       4481 |
| Medium   | PHP < 5.2.10 Multiple Vulnerabilities               | CVE-2009-2687 |  39480 |       3575 |
| Medium   | PHP < 5.2.9 Multiple Vulnerabilities                | CVE-2008-5498 |  35750 |       3312 |
| Medium   | Apache HTTP Server 403 Error Page UTF-7 Encoded XSS | CVE-2008-2168 |  17696 |       2935 |
| Medium   | Apache 2.x < 2.2.12 Multiple Vulnerabilities        | CVE-2009-0023 |  40467 |       2759 |
| Medium   | Apache < 2.2.9 Multiple Vulnerabilities (DoS, XSS)  | CVE-2007-6420 |  33477 |       1699 |
| Medium   | Apache < 2.2.8 Multiple Vulnerabilities (XSS, DoS)  | CVE-2007-5000 |  31118 |       1051 |
| Medium   | PHP < 5.2.5 Multiple Vulnerabilities                | CVE-2007-3996 |  28181 |        945 |
| Medium   | Apache < 2.2.6 Multiple Vulnerabilities (DoS, XSS)  | CVE-2006-5752 |  26023 |        944 |
| Medium   | PHP < 5.2.4 Multiple Vulnerabilities                | CVE-2007-1413 |  25971 |        858 |
| Medium   | Apache < 2.0.63 Multiple XSS Vulnerabilities        | CVE-2007-5000 |  31407 |        444 |
| Medium   | OpenSSL < 0.9.6m / 0.9.7d Multiple Remote DoS       | CVE-2004-0079 |  12110 |        415 |
| Medium   | PHP < 5.2.3 Multiple Vulnerabilities                | CVE-2007-1900 |  25368 |        392 |
| Medium   | OpenSSL < 0.9.6j / 0.9.7b Multiple Vulnerabilities  | CVE-2003-0078 |  11267 |        380 |
...
```

Results
Top of Medium-risk vulnerabilities discovered (2)

```
...
| Medium   | Apache 2.4 < 2.4.3 Multiple Vulnerabilities            | CVE-2012-2687 |  61644 |    324 |
| Medium   | Apache < 1.3.41 Multiple Vulnerabilities (DoS, XSS)    | CVE-2007-3847 |  31408 |    303 |
| Medium   | PHP 5.3 < 5.3.1 Multiple Vulnerabilities               | CVE-2009-3557 |  42862 |    184 |
| Medium   | PHP php_variables.c Multiple Variable Open Bracket Mem | CVE-2004-0958 |  15436 |    156 |
| Medium   | Apache < 2.0.51 Multiple Vulnerabilities (OF, DoS)     | CVE-2004-0747 |  14748 |    113 |
| Medium   | PHP < 4.3.8 Multiple Vulnerabilities                   | CVE-2004-0594 |  13650 |     96 |
| Medium   | Apache < 2.0.50 Multiple Remote DoS                    | CVE-2004-0493 |  12293 |     96 |
| Medium   | lighttpd mod_fastcgi HTTP Request Header Remote Overfl | CVE-2007-4727 |  26057 |     92 |
| Medium   | F5 BIG-IP Cookie Remote Information Disclosure         |               |  20089 |     86 |
| Medium   | PHP Mail Function Header Spoofing                      | CVE-2002-0985 |  11444 |     67 |
| Medium   | PHP 5.x < 5.1.0 Multiple Vulnerabilities               | CVE-2005-3319 |  17711 |     57 |
| Medium   | PHP socket_iovec_alloc() Function Overflow             | CVE-2003-0166 |  11468 |     53 |
| Medium   | Apache < 1.3.31 / 2.0.49 Socket Connection Blocking Rac| CVE-2004-0174 |  12280 |     33 |
| Medium   | Apache 2.4 < 2.4.2 'LD_LIBRARY_PATH' Insecure Library L| CVE-2012-0883 |  58795 |     32 |
| Medium   | PHP < 4.3.3 php_check_safe_mode_include_dir Function Sa| CVE-2003-0863 |  11807 |     24 |
| Medium   | Apache < 2.0.47 Multiple Vulnerabilities (DoS, Enc)    | CVE-2003-0192 |  11788 |     23 |
| Medium   | PHP 5.4.x < 5.4.1 Multiple Vulnerabilities             | CVE-2012-1172 |  58967 |     16 |
| Medium   | Apache 2.2.18 APR apr_fnmatch DoS                      | CVE-2011-1928 |  54646 |     13 |
| Medium   | Oracle GlassFish Server 2.1.1 < 2.1.1.15 / 3.0.1 < 3.0.| CVE-2011-5035 |  58090 |     11 |
| Medium   | Oracle GlassFish Server 3.0.1 / 3.1.1 < 3.0.1.5 / 3.1.1| CVE-2012-0104 |  57805 |     11 |
| Medium   | Jetty < 4.2.19 HTTP Server HttpRequest.java Content-Len| CVE-2004-2381 |  17348 |      6 |
| Medium   | Apache < 2.0.43 Multiple Vulnerabilities (Log Injection| CVE-2002-1156 |  11408 |      4 |
| Medium   | IceWarp Merak WebMail Server < 9.4.2 Multiple Vulnerabi| CVE-2009-1467 |  38717 |      2 |
| Medium   | PHP Safe Mode mail Function 5th Parameter Arbitrary Cmd| CVE-2001-1246 |  10701 |      2 |
| Medium   | Sun NetBeans Java IDE HTTP Server IP Restriction Bypass| CVE-1999-1527 |  10149 |      1 |
| Medium   | ListManager < 9.3b / 9.2c / 8.95d Multiple Vulnerabilit| CVE-2007-6319 |  31134 |      1 |
+----------+--------------------------------------------------------+---------------+--------+--------+
49 rows in set (0.47 sec)
```

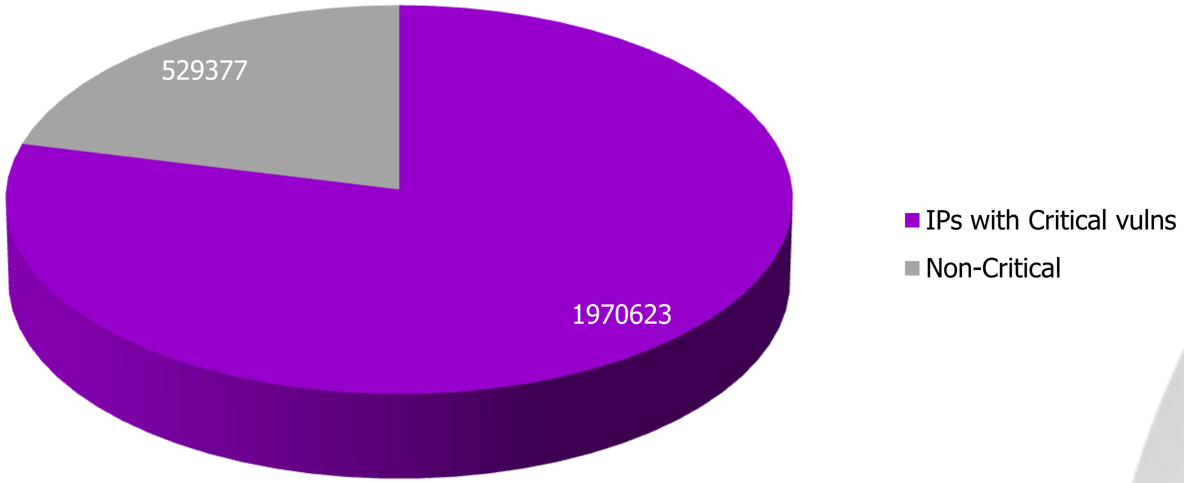
Results
Nessus plugins summary

Total 112 unique plugins triggered on all input data (3.1% of total 3527 plugins)

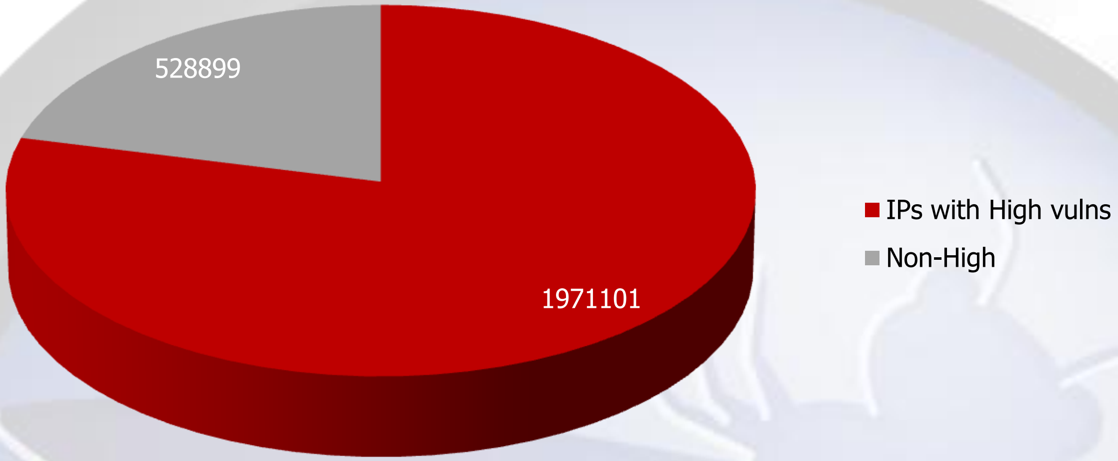
- 10 Critical risk
- 50 High risk
- 49 Medium risk
- 3 Low risk

Results
Vulnerability summary

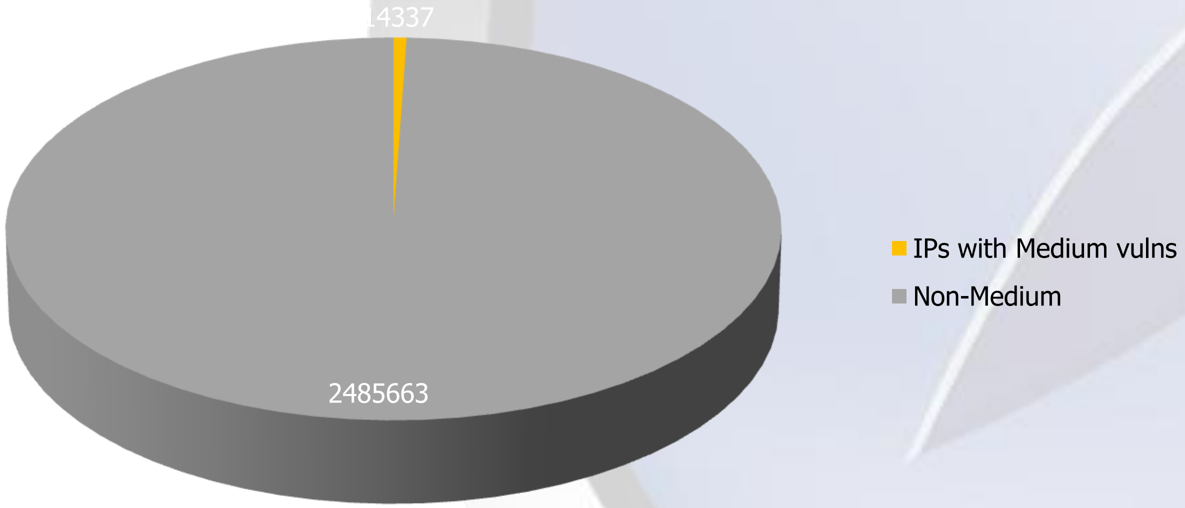
Critical Vulnerabilities (78%)



High vulnerabilities (78%)



Medium vulnerabilities (0.5%)



Results
Why so many vulnerabilities?

```
+----------+------------------------------------------------------+---------------+--------+------------+
| Severity | Plugin Name                                          | CVE           | PlugID | Nr Servers |
+----------+------------------------------------------------------+---------------+--------+------------+
| Critical | PHP 5.3.x < 5.3.15 Multiple Vulnerabilities          | CVE-2012-2688 |  60085 |    1959657 |
| High     | PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution | CVE-2012-1823 |  58988 |    1967941 |
| High     | PHP < 5.3.11 Multiple Vulnerabilities                | CVE-2011-1398 |  58966 |    1967914 |
| High     | PHP 5.3.x < 5.3.14 Multiple Vulnerabilities          | CVE-2012-2143 |  59529 |    1959046 |
| High     | PHP 5.3.x < 5.3.13 CGI Query String Code Execution   | CVE-2012-2311 |  59056 |    1958619 |
+----------+------------------------------------------------------+---------------+--------+------------+
```

All these plugins trigger on the following server signature:

Server: nginx/1.0.11

X-Powered-By: PHP/5.3.10

There are 1,905,288 devices with this signature (76% of total web servers).

What is the real risk?

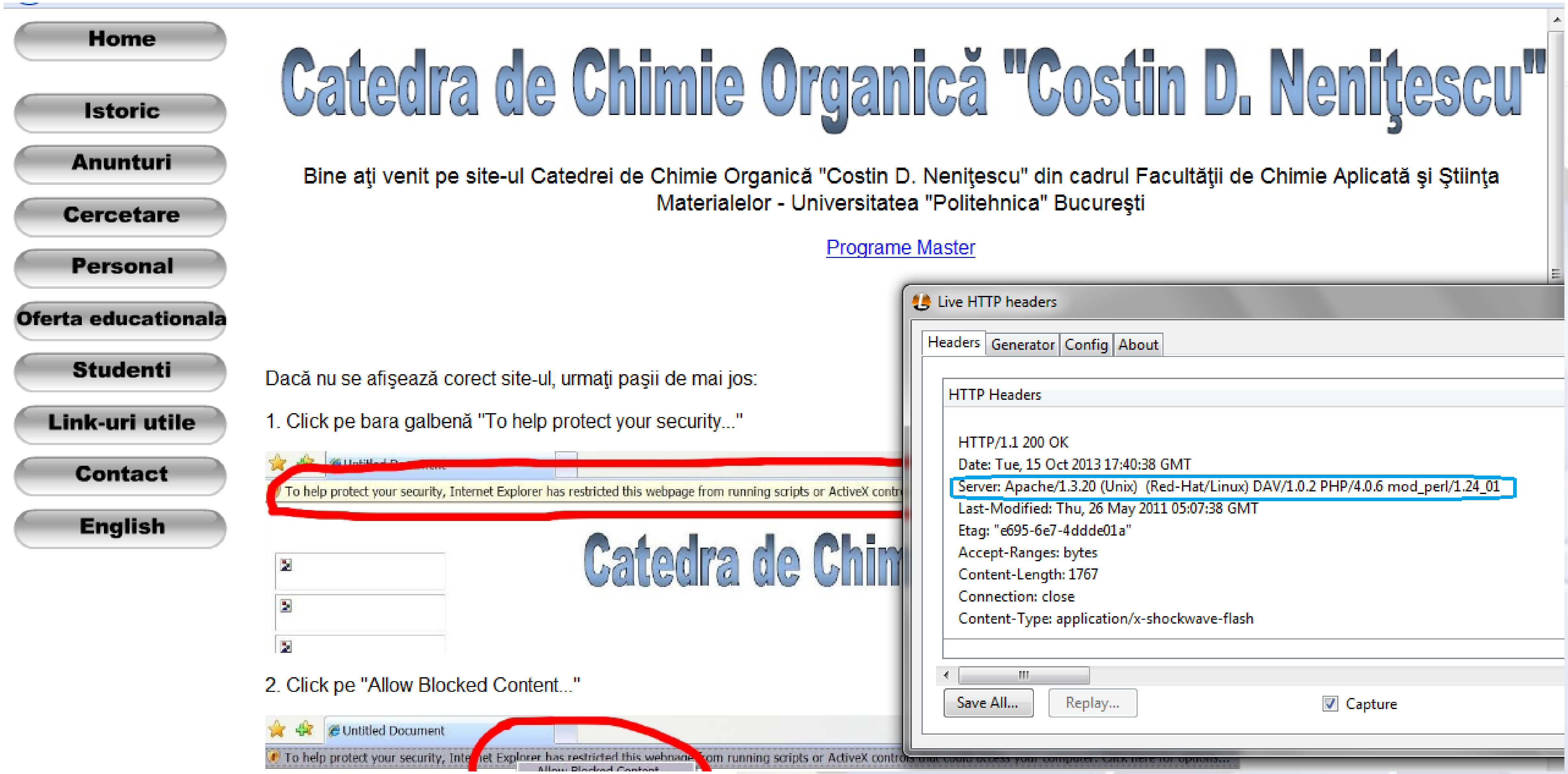
- Most of these vulnerabilities are not directly exploitable:
  - Locally exploitable
  - Specific configurations must be in place
  - But NOT impossible
- However, there are some high risk and easily exploitable vulnerabilities (Metasploit, public exploits):

```
+----------+------------------------------------------------------+---------------+--------+------------+
| Severity | Plugin Name                                          | CVE           | PlugID | Nr Servers |
+----------+------------------------------------------------------+---------------+--------+------------+
| High     | Apache Chunked Encoding Remote Overflow              | CVE-2002-0392 |  11030 |         62 |
| High     | Apache < 1.3.37 mod_rewrite LDAP Protocol URL Overfl | CVE-2006-3747 |  31654 |        721 |
| High     | PHP 5.3.x < 5.3.13 CGI Query String Code Execution   | CVE-2012-2311 |  59056 |    1958619 |
+----------+------------------------------------------------------+---------------+--------+------------+
```

Where are the exploitable vulnerabilities located?

- University websites
- Public institutions websites
- Old company websites
- Surveillance systems
- Special systems

Where are the exploitable vulnerabilities located?



Catedra de Chimie Organică "Costin D. Neniţescu"

Bine aţi venit pe site-ul Catedrei de Chimie Organică "Costin D. Neniţescu" din cadrul Facultăţii de Chimie Aplicată şi Ştiinţa Materialelor - Universitatea "Politehnica" Bucureşti

Programe Master

Dacă nu se afişează corect site-ul, urmaţi paşii de mai jos:

1. Click pe bara galbenă "To help protect your security..."

To help protect your security, Internet Explorer has restricted this webpage from running scripts or ActiveX contr

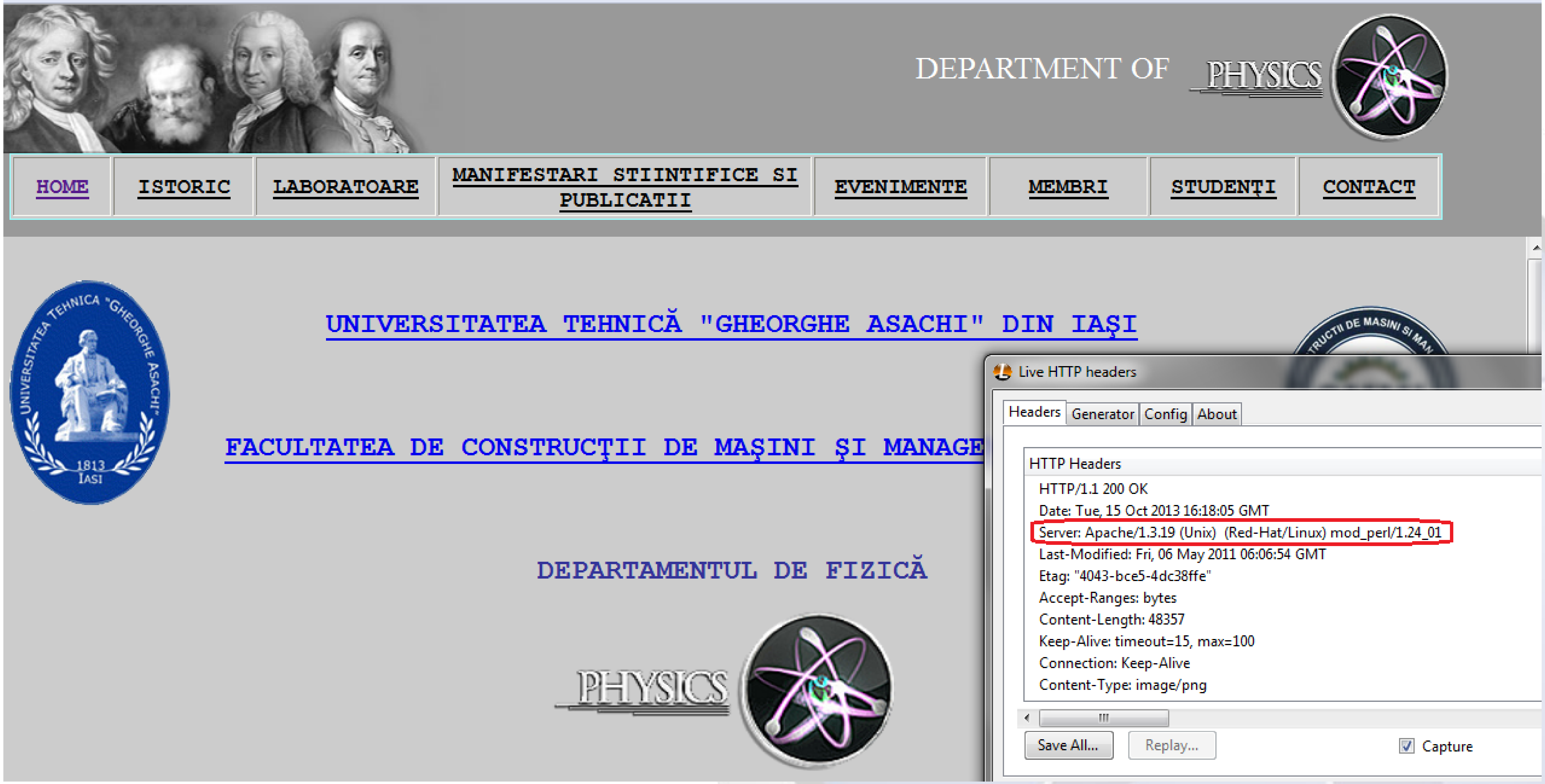
Catedra de Chim

2. Click pe "Allow Blocked Content..."

To help protect your security, Inte net Explorer has restricted this webpage from running scripts or ActiveX controls that could access your computer. Click here for options...

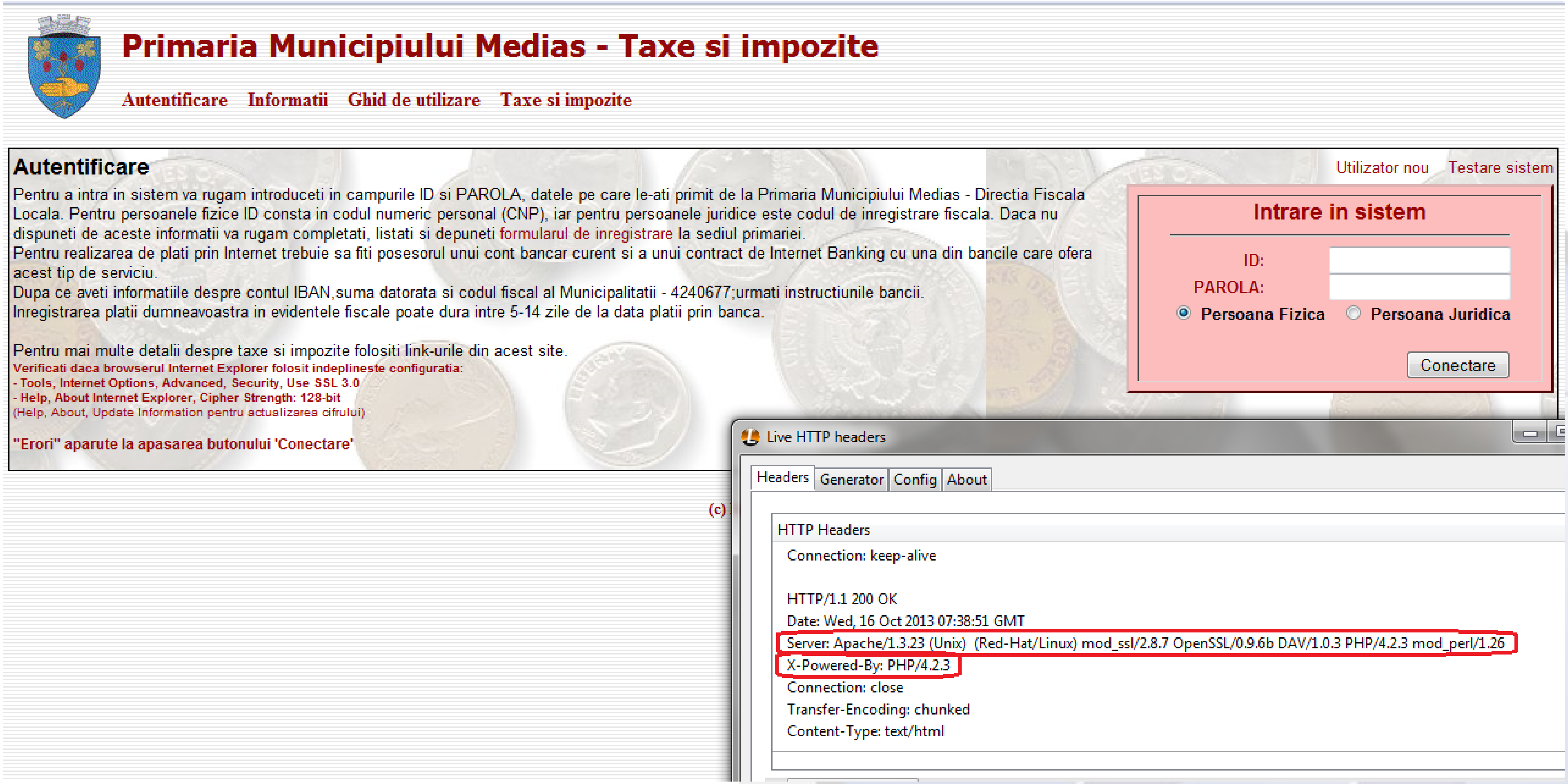
```
HTTP/1.1 200 OK
Date: Tue, 15 Oct 2013 17:40:38 GMT
Server: Apache/1.3.20 (Unix)  (Red-Hat/Linux) DAV/1.0.2 PHP/4.0.6 mod_perl/1.24_01
Last-Modified: Thu, 26 May 2011 05:07:38 GMT
Etag: "e695-6e7-4ddde01a"
Accept-Ranges: bytes
Content-Length: 1767
Connection: close
Content-Type: application/x-shockwave-flash
```

Where are the exploitable vulnerabilities located?



```
HTTP/1.1 200 OK
Date: Tue, 15 Oct 2013 16:18:05 GMT
Server: Apache/1.3.19 (Unix)  (Red-Hat/Linux) mod_perl/1.24_01
Last-Modified: Fri, 06 May 2011 06:06:54 GMT
Etag: "4043-bce5-4dc38ffe"
Accept-Ranges: bytes
Content-Length: 48357
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: image/png
```

Where are the exploitable vulnerabilities located?



Primaria Municipiului Medias - Taxe si impozite

Autentificare

Pentru a intra in sistem va rugam introduceti in campurile ID si PAROLA, datele pe care le-ati primit de la Primaria Municipiului Medias - Directia Fiscala Locala. Pentru persoanele fizice ID consta in codul numeric personal (CNP), iar pentru persoanele juridice este codul de inregistrare fiscala. Daca nu dispuneti de aceste informatii va rugam completati, listati si depuneti formularul de inregistrare la sediul primariei.
Pentru realizarea de plati prin Internet trebuie sa fiti posesorul unui cont bancar curent si a unui contract de Internet Banking cu una din bancile care ofera acest tip de serviciu.
Dupa ce aveti informatiile despre contul IBAN,suma datorata si codul fiscal al Municipalitatii - 4240677;urmati instructiunile bancii.
Inregistrarea platii dumneavoastra in evidentele fiscale poate dura intre 5-14 zile de la data platii prin banca.

Pentru mai multe detalii despre taxe si impozite folositi link-urile din acest site.
Verificati daca browserul Internet Explorer folosit indeplineste configuratia:
- Tools, Internet Options, Advanced, Security, Use SSL 3.0
- Help, About Internet Explorer, Cipher Strength: 128-bit
(Help, About, Update Information pentru actualizarea cifrului)

"Erori" aparute la apasarea butonului 'Conectare'

(c)

Intrare in sistem

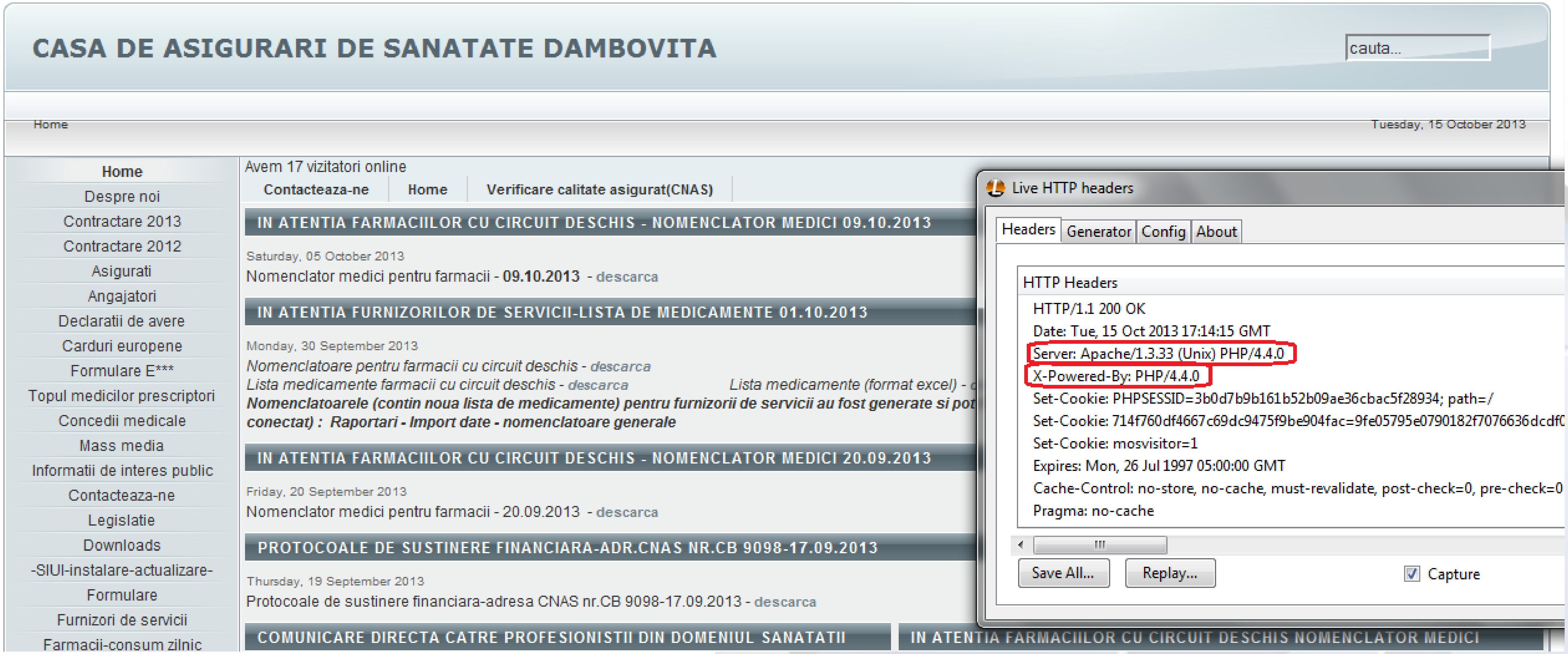
ID:
PAROLA:
● Persoana Fizica ○ Persoana Juridica

HTTP Headers

```
Connection: keep-alive

HTTP/1.1 200 OK
Date: Wed, 16 Oct 2013 07:38:51 GMT
Server: Apache/1.3.23 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.7 OpenSSL/0.9.6b DAV/1.0.3 PHP/4.2.3 mod_perl/1.26
X-Powered-By: PHP/4.2.3
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html
```

Where are the exploitable vulnerabilities located?



Avem 17 vizitatori online

IN ATENTIA FARMACIILOR CU CIRCUIT DESCHIS - NOMENCLATOR MEDICI 09.10.2013

Saturday, 05 October 2013

Nomenclator medici pentru farmacii - **09.10.2013** - descarca

IN ATENTIA FURNIZORILOR DE SERVICII-LISTA DE MEDICAMENTE 01.10.2013

Monday, 30 September 2013

Nomenclatoare pentru farmacii cu circuit deschis - descarca

Lista medicamente farmacii cu circuit deschis - descarca *Lista medicamente (format excel)* - d

Nomenclatoarele (contin noua lista de medicamente) pentru furnizorii de servicii au fost generate si pot

conectat) : Raportari - Import date - nomenclatoare generale

IN ATENTIA FARMACIILOR CU CIRCUIT DESCHIS - NOMENCLATOR MEDICI 20.09.2013

Friday, 20 September 2013

Nomenclator medici pentru farmacii - 20.09.2013 - descarca

PROTOCOALE DE SUSTINERE FINANCIARA-ADR.CNAS NR.CB 9098-17.09.2013

Thursday, 19 September 2013

Protocoale de sustinere financiara-adresa CNAS nr.CB 9098-17.09.2013 - descarca

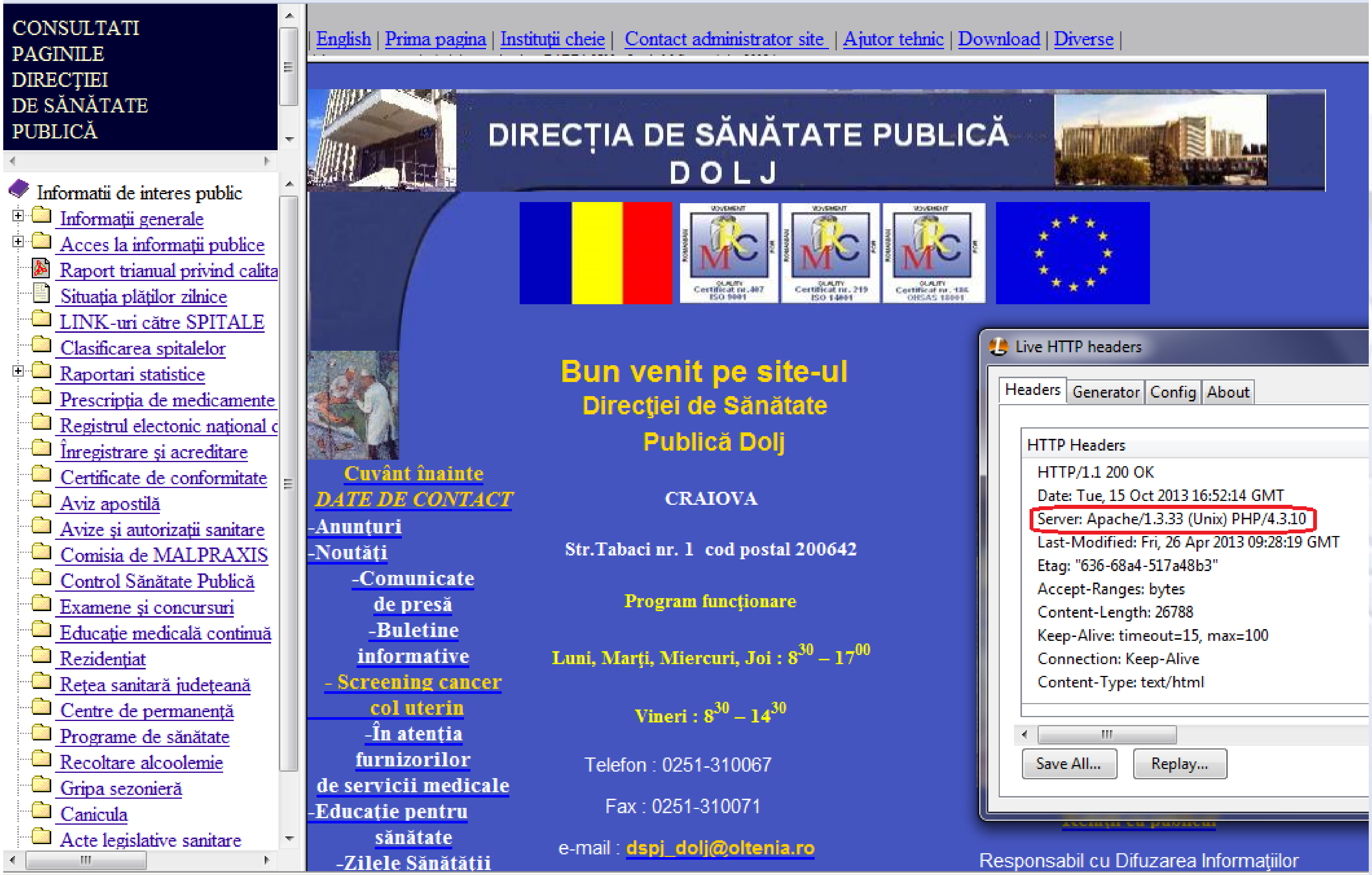
COMUNICARE DIRECTA CATRE PROFESIONISTII DIN DOMENIUL SANATATII

IN ATENTIA FARMACIILOR CU CIRCUIT DESCHIS NOMENCLATOR MEDICI

HTTP Headers

```
HTTP/1.1 200 OK
Date: Tue, 15 Oct 2013 17:14:15 GMT
Server: Apache/1.3.33 (Unix) PHP/4.4.0
X-Powered-By: PHP/4.4.0
Set-Cookie: PHPSESSID=3b0d7b9b161b52b09ae36cbac5f28934; path=/
Set-Cookie: 714f760df4667c69dc9475f9be904fac=9fe05795e0790182f7076636dcdf0
Set-Cookie: mosvisitor=1
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
```

Where are the exploitable vulnerabilities located?


CONSULTATI PAGINILE DIRECŢIEI DE SĂNĂTATE PUBLICĂ
Informatii de interes public
Informații generale
Acces la informații publice
Raport trianual privind calita
Situația plăților zilnice
LINK-uri către SPITALE
Clasificarea spitalelor
Raportari statistice
Prescripția de medicamente
Registrul electronic național c
Înregistrare și acreditare
Certificate de conformitate
Aviz apostilă
Avize și autorizații sanitare
Comisia de MALPRAXIS
Control Sănătate Publică
Examene și concursuri
Educație medicală continuă
Rezidențiat
Rețea sanitară județeană
Centre de permanență
Programe de sănătate
Recoltare alcoolemie
Gripa sezonieră
Canicula
Acte legislative sanitare
English | Prima pagina | Instituții cheie | Contact administrator site | Ajutor tehnic | Download | Diverse |
DIRECȚIA DE SĂNĂTATE PUBLICĂ
DOLJ
Cuvânt înainte
DATE DE CONTACT
-Anunțuri
-Noutăți
-Comunicate de presă
-Buletine informative
- Screening cancer col uterin
-În atenția furnizorilor de servicii medicale
-Educație pentru sănătate
-Zilele Sănătății
Live HTTP headers
Headers
Generator
Config
About
HTTP Headers
Save All...
Replay...

Bun venit pe site-ul Direcţiei de Sănătate Publică Dolj

CRAIOVA

Str.Tabaci nr. 1 cod postal 200642

Program funcționare

Luni, Marți, Miercuri, Joi : 8^{30} – 17^{00}

Vineri : 8^{30} – 14^{30}

Telefon : 0251-310067

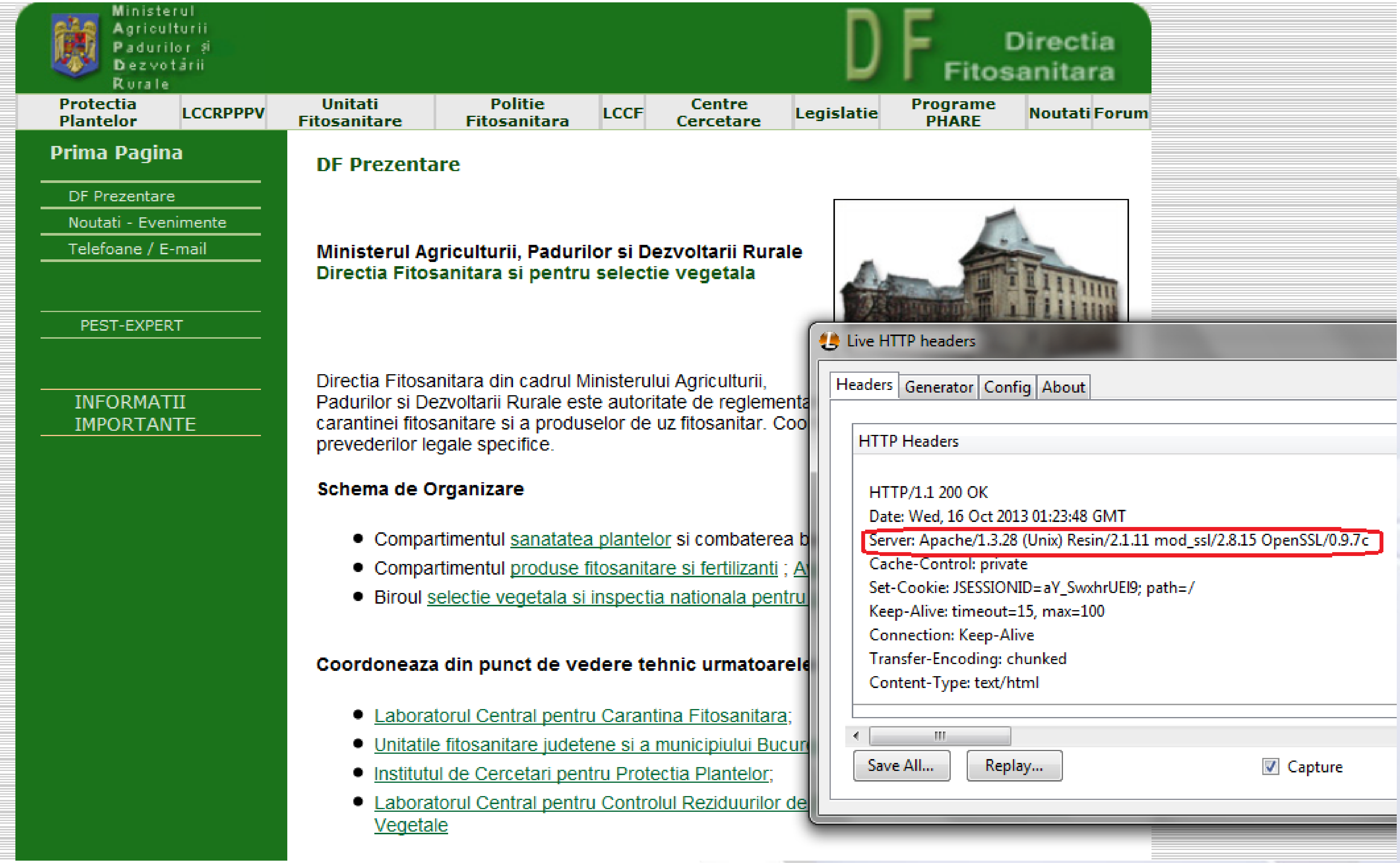
Fax : 0251-310071

e-mail : dspj_dolj@oltenia.ro

Responsabil cu Difuzarea Informațiilor

```
HTTP/1.1 200 OK
Date: Tue, 15 Oct 2013 16:52:14 GMT
Server: Apache/1.3.33 (Unix) PHP/4.3.10
Last-Modified: Fri, 26 Apr 2013 09:28:19 GMT
Etag: "636-68a4-517a48b3"
Accept-Ranges: bytes
Content-Length: 26788
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html
```

Where are the exploitable vulnerabilities located?



DF Prezentare

Ministerul Agriculturii, Padurilor si Dezvoltarii Rurale
Directia Fitosanitara si pentru selectie vegetala

Directia Fitosanitara din cadrul Ministerului Agriculturii, Padurilor si Dezvoltarii Rurale este autoritate de reglementa carantinei fitosanitare si a produselor de uz fitosanitar. Coo prevederilor legale specifice.

Schema de Organizare

- Compartimentul sanatatea plantelor si combaterea b
- Compartimentul produse fitosanitare si fertilizanti ; A
- Biroul selectie vegetala si inspectia nationala pentru

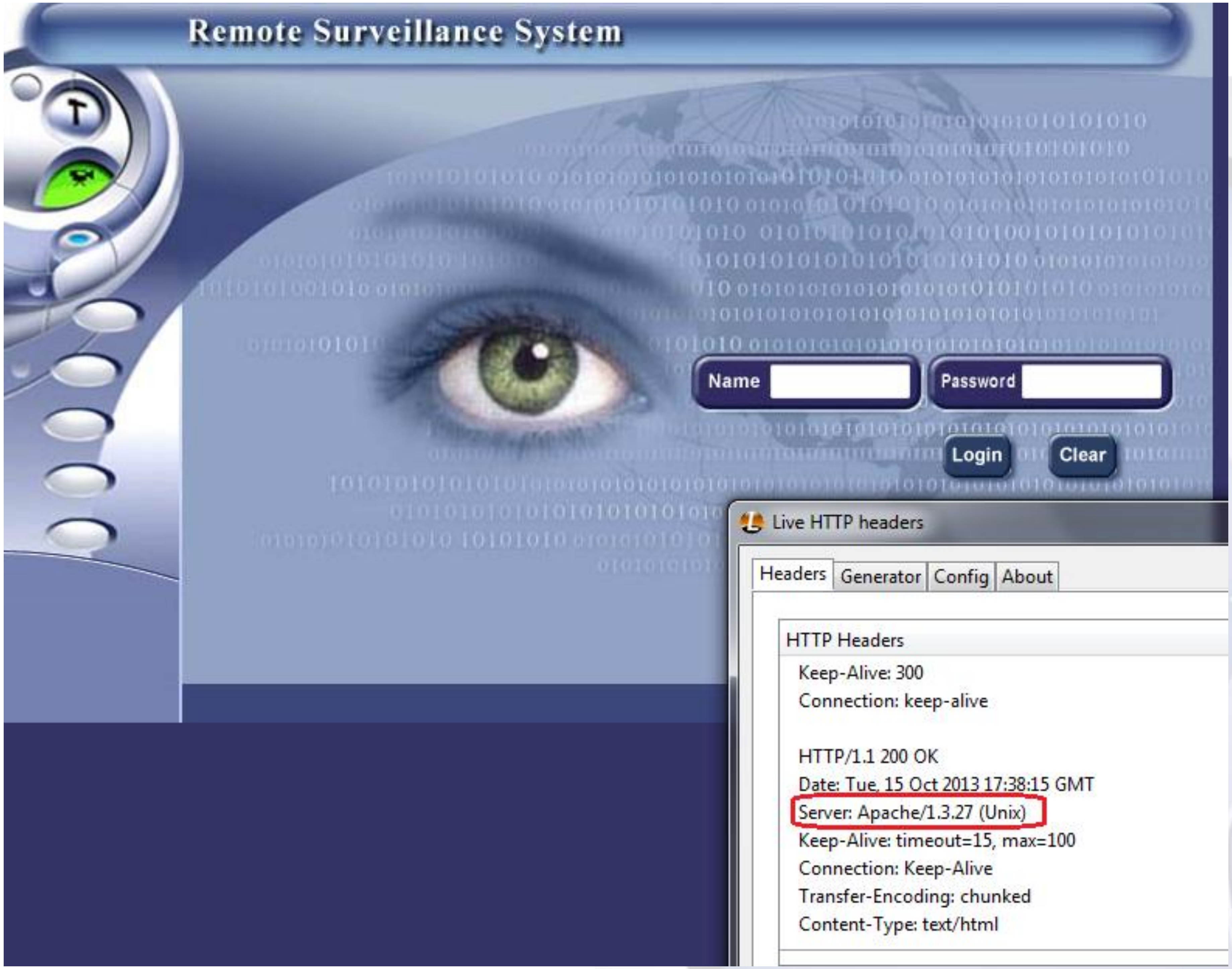
Coordoneaza din punct de vedere tehnic urmatoarele

- Laboratorul Central pentru Carantina Fitosanitara;
- Unitatile fitosanitare judetene si a municipiului Bucur
- Institutul de Cercetari pentru Protectia Plantelor;
- Laboratorul Central pentru Controlul Reziduurilor de Vegetale

HTTP Headers

```
HTTP/1.1 200 OK
Date: Wed, 16 Oct 2013 01:23:48 GMT
Server: Apache/1.3.28 (Unix) Resin/2.1.11 mod_ssl/2.8.15 OpenSSL/0.9.7c
Cache-Control: private
Set-Cookie: JSESSIONID=aY_SwxhrUEI9; path=/
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html
```

Where are the exploitable vulnerabilities located?

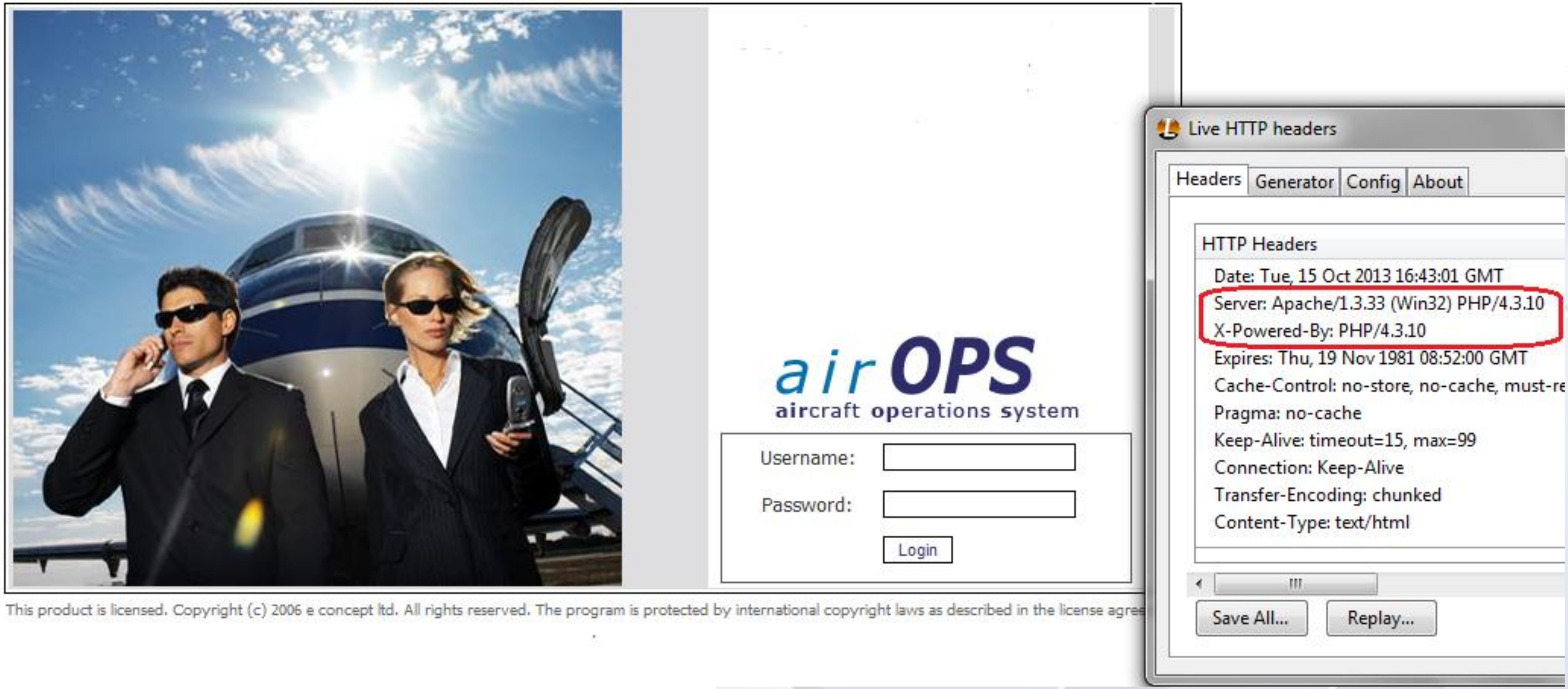


HTTP Headers

```
Keep-Alive: 300
Connection: keep-alive

HTTP/1.1 200 OK
Date: Tue, 15 Oct 2013 17:38:15 GMT
Server: Apache/1.3.27 (Unix)
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html
```

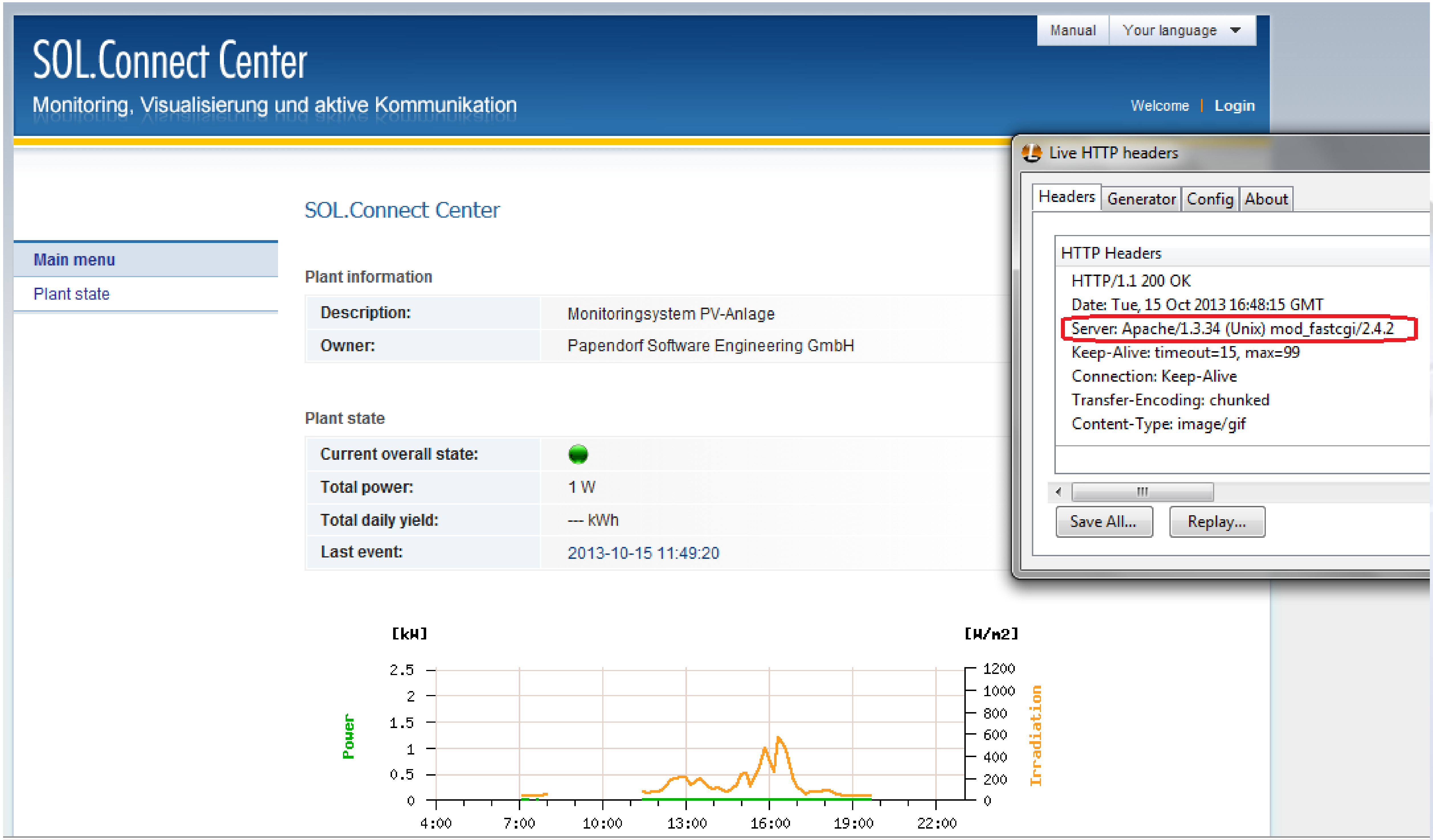
Where are the exploitable vulnerabilities located?



This product is licensed. Copyright (c) 2006 e concept ltd. All rights reserved. The program is protected by international copyright laws as described in the license agree

```
HTTP Headers
  Date: Tue, 15 Oct 2013 16:43:01 GMT
  Server: Apache/1.3.33 (Win32) PHP/4.3.10
  X-Powered-By: PHP/4.3.10
  Expires: Thu, 19 Nov 1981 08:52:00 GMT
  Cache-Control: no-store, no-cache, must-re
  Pragma: no-cache
  Keep-Alive: timeout=15, max=99
  Connection: Keep-Alive
  Transfer-Encoding: chunked
  Content-Type: text/html
```

Where are the exploitable vulnerabilities located?



SOL.Connect Center

Monitoring, Visualisierung und aktive Kommunikation

SOL.Connect Center

Plant information

Description:	Monitoringsystem PV-Anlage
Owner:	Papendorf Software Engineering GmbH

Plant state

Current overall state:	●
Total power:	1 W
Total daily yield:	--- kWh
Last event:	2013-10-15 11:49:20

```
HTTP/1.1 200 OK
Date: Tue, 15 Oct 2013 16:48:15 GMT
Server: Apache/1.3.34 (Unix) mod_fastcgi/2.4.2
Keep-Alive: timeout=15, max=99
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: image/gif
```

Part 2: Grep (all mighty)

OWASP Top 10 - 2013

“The Ten Most Critical Web Applications Security Risks”

#	Top 10 Name	Included	What exactly?
A1	Injection	X	
A2	Broken Authentication and Session Management	X	
A3	Cross-Site Scripting (XSS)	X	
A4	Insecure Direct Object References	X	
A5	Security Misconfiguration	✓	- Outdated server type and CGI version (already done with Nessus) - SQL and PHP error messages - Directory listing - Default passwords - Admin pages publicly accessible
A6	Sensitive Data Exposure	✓	- Admin pages with no SSL - WWW-Authentication - Plain text passwords - Email addresses - Private IP disclosure - Source code disclosure
A7	Missing Function Level Access Control	X	
A8	Cross-Site Request Forgery	X	
A9	Using Components with Known Vulnerabilities	-	May be done
A10	Unvalidated Redirects and Forwards	X	

SQL and PHP error messages (1)

[Total: 171 websites]

```
HTTP/1.1 200 OK
Date: Wed, 25 Jul 2012 12:06:04 GMT
Server: Apache
Set-Cookie: PHPSESSID=8hn66359c00qad7vqe6gs87f52; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 864
Connection: close
Content-Type: text/html

-> EROARE <-
Eroare MySQL! Conexiunea 'Resource id #9', la query-ul:
---------------------------------------------------------------------------
Nu am putut selecta baza de date a magazinului
---------------------------------------------------------------------------
A aparut urmatoarea eroare:
Error 1044: Access denied for user 'dev'@'%' to database 'netrisk_asigura2'
                              Pagina: http://beta.asigurari360.ro/
                              Data: 25.07.2012 15:06:04
                              ID magazin: 1
                              ID utilizator: NULL
                              ID client: NULL
                              IP: 182.150.134.62,
                              LAN: NULL,
                              URL: /,
                              Useragent: NULL,
                              Actiune: NULL,
                              Subactiune: NULL,
                              Referrer: NULL
                              GET: NULL
                              POST: NULL
                              Timp SQL: 0,
                              Timp total: 0.015,
                              ID categorie: NULL
                              ID producator: NULL
                              ID produs: NULL</pre>
```

```
$ whois 182.150.134.62
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '182.144.0.0 - 182.151.255.255'

inetnum:        182.144.0.0 - 182.151.255.255
netname:        CHINANET-SC
descr:          CHINANET Sichuan province network
descr:          Data Communication Division
descr:          China Telecom
country:        CN
```

SQL and PHP error messages (2) [Total: 171 websites]

```
HTTP/1.1 200 OK
Date: Wed, 25 Jul 2012 19:48:27 GMT
Server: Apache/2.0.55 (Ubuntu) PHP/5.1.2
X-Powered-By: PHP/5.1.2
Content-Length: 403
Connection: close
Content-Type: text/html; charset=UTF-8

<b>Warning</b>:  pg_pconnect() [<a href='function.pg-pconnect'>function.pg-pconnect</a>]: Unable to connect to PostgreSQL server: could not
connect to server: No route to host
             Is the server running on host &quot;192.168.1.130&quot; and accepting
             TCP/IP connections on port 5432? in <b>/home/vftp/comenzi.ruris.ro/dbconnection.php</b> on line <b>41</b><br />
can not connect to PostgreSQL server
```

```
HTTP/1.0 200 OK
Date: Wed, 25 Jul 2012 13:08:13 GMT
Server: LiteSpeed
Connection: close
X-Powered-By: PHP/5.2.17
Set-Cookie: cba19ac07617cbccdb85f183c0d1adf1=a137cb6b8ebb579dd4174347f4f93b76; path=/
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Content-Type: text/html

jtablesession::Store Failed<br />DB function failed with error number 1146<br /><font color="red">Table 'rilievi_tt.jos_session' doesn't exist
SQL=INSERT INTO `jos_session` ( `session_id`,`time`,`username`,`gid`,`guest`,`client_id` ) VALUES (
'a137cb6b8ebb579dd4174347f4f93b76','1343221693','','0','1','0' )</font><br />
<b>Fatal error</b>:  Allowed memory size of 134217728 bytes exhausted (tried to allocate 72 bytes) in
<b>/home/rilievi/public_html/libraries/joomla/error/exception.php</b> on line <b>117</b><br />
```

Directory listing [Total: 131 websites]

```
HTTP/1.1 200 OK
Date: Wed, 25 Jul 2012 09:59:08 GMT
Server: Apache/2.2.22 (Unix) PHP/5.3.14
Vary: Accept-Encoding
Content-Length: 1131
Connection: close
Content-Type: text/html;charset=ISO-8859-1

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /</title>
 </head>
 <body>
<h1>Index of /</h1>
<ul><li><a href="arhsite.tgz"> arhsite.tgz</a></li>
<li><a href="autoclubs/"> autoclubs/</a></li>
<li><a href="backupcraiova.sql"> backupcraiova.sql</a></li>
<li><a href="backups/"> backups/</a></li>
<li><a href="beta/"> beta/</a></li>
<li><a href="captiv.tgz"> captiv.tgz</a></li>
<li><a href="craiovanet/"> craiovanet/</a></li>
<li><a href="face.htacces"> face.htacces</a></li>
<li><a href="fun/"> fun/</a></li>
<li><a href="host/"> host/</a></li>
<li><a href="lang-ro.php"> lang-ro.php</a></li>
<li><a href="netsat/"> netsat/</a></li>
<li><a href="oldba/"> oldba/</a></li>
<li><a href="servxx/"> servxx/</a></li>
<li><a href="sms/"> sms/</a></li>
<li><a href="video/"> video/</a></li>
<li><a href="work/"> work/</a></li>
<li><a href="workauto/"> workauto/</a></li>
</ul>
</body></html>
```

Default credentials for admin interfaces

[Total: 53424 servers (WWW-Auth)]

```
HTTP/1.1 401 Unauthorized
AServer: GoAhead-Webs
Date: Wed Jan 12 17:32:16 2000
WWW-Authenticate: Basic realm="Default: admin/1234"
Pragma: no-cache
Cache-Control: no-cache
Content-Type: text/html

<html>
    <head>
        <title>Document Error: Unauthorized</title>
    </head>
    <body>
        <h2>Access Error: Unauthorized</h2>
    </body>
</html>
```

realm="Default: admin/1234"	- 1292 devices
realm="Default: admin/admin	- 21
realm="Default: admin/airlive	- 2
realm="Default password:1234	- 4
realm="Default USER:admin	- 1
realm="Wireless AP (username: admin)	- 5
realm="Wireless Router (username: admin)	- 50
realm="DVR Remote System (Default Login : root / 0000)	- 1

+ default passwords based on device type/version

Private IP disclosure [Total: 2684 websites]

```
HTTP/1.1  200  OK
Content-Length:  332
Content-Type:  text/html
Content-Location:  http://172.16.0.113/index.html
Last-Modified:  Mon,  25  Jun  2012  19:32:38  GMT
Server:  Microsoft-IIS/6.0
Date:  Wed,  25  Jul  2012  18:42:42  GMT
Connection:  close

<?xml  version=3D"1.0"  encoding=3D"UTF-8"?>
<!DOCTYPE  html  PUBLIC  "-//W3C//DTD  XHTML  1.0  Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html  xmlns=3D"http://www.w3.org/1999/xhtml">
        <head>
                <title></title>
                <meta  http-equiv=3D"refresh"  content="0;url=Snippets_of_Thoughts/Blog/Blog.html"  />
        </head>
        <body>
        </body>
</html>
```

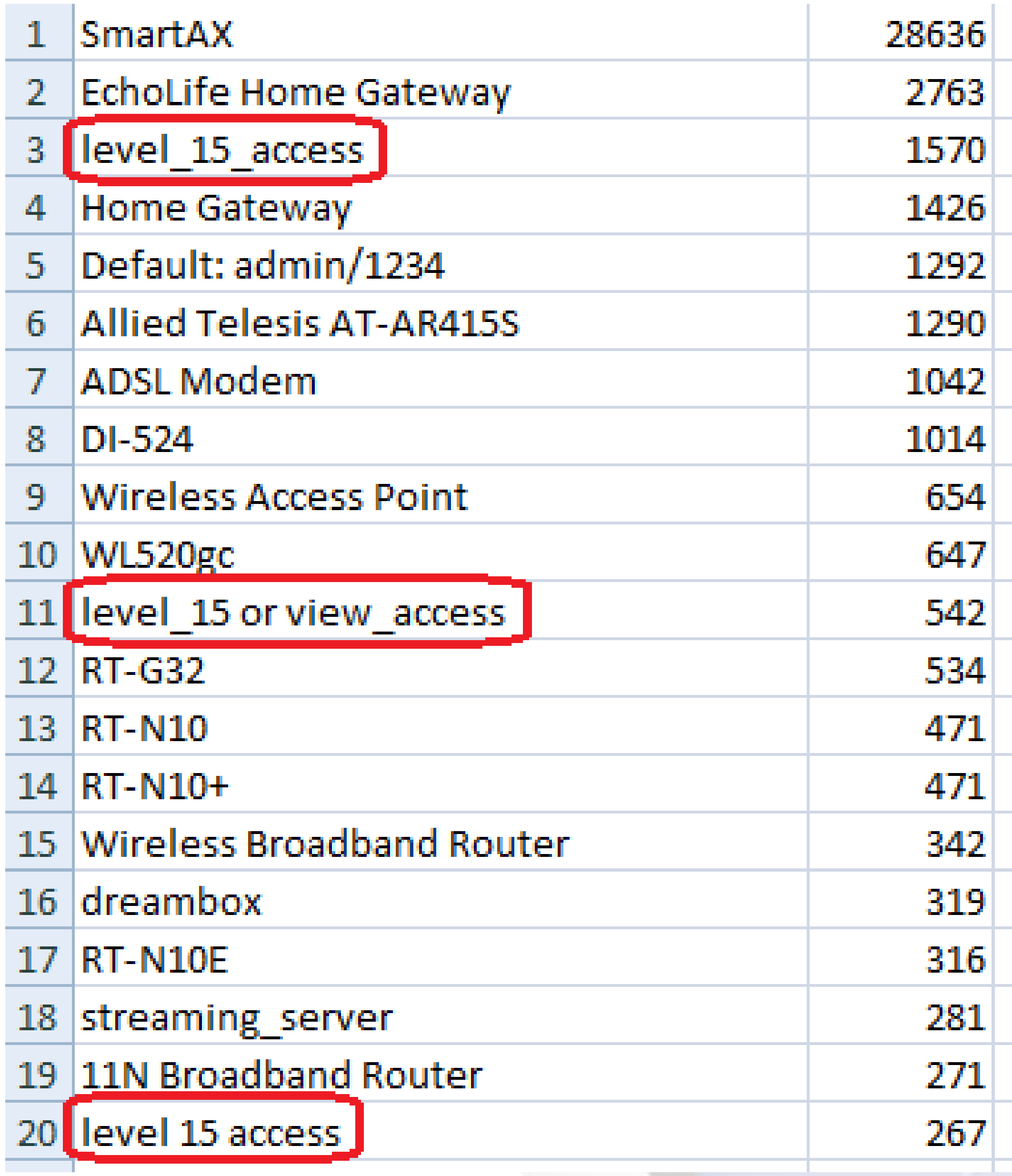
Other interesting stuff...

Ream strings suggesting the usage of the systems (WWW-Authentication):

realm="Access permis doar pentru utilizatorii ANM"
realm="Access permis doar pentru utilizatorii faro"
realm="Access permis doar pentru utilizatorii Meteo Romania"
realm="Access permis doar pentru utilizatorii Radar"
realm="Access permis pentru utilizatorii Administratiei Nationale de Meteorologie"
realm="Administrare retea infraserver"
realm="Birou Contabilitate"
realm="BlueNote Nagios Access"
realm="Cacti monitoring server"
realm="Innerlook CRM Platform"
realm="Innerlook Recruiting Platform"
realm="IntelEmbeddedWeb@Express460T"
realm="Intelligent Switch"
realm="IntermediaTV Botosani"
realm="Lotus Notes Traveler (HQLNA1/RADIOCOM)"
realm="Lotus Notes Traveler (Traveler/EMON)"
realm="Lotus Notes Traveler (Traveler/FRISOMAT)"

Other interesting stuff...

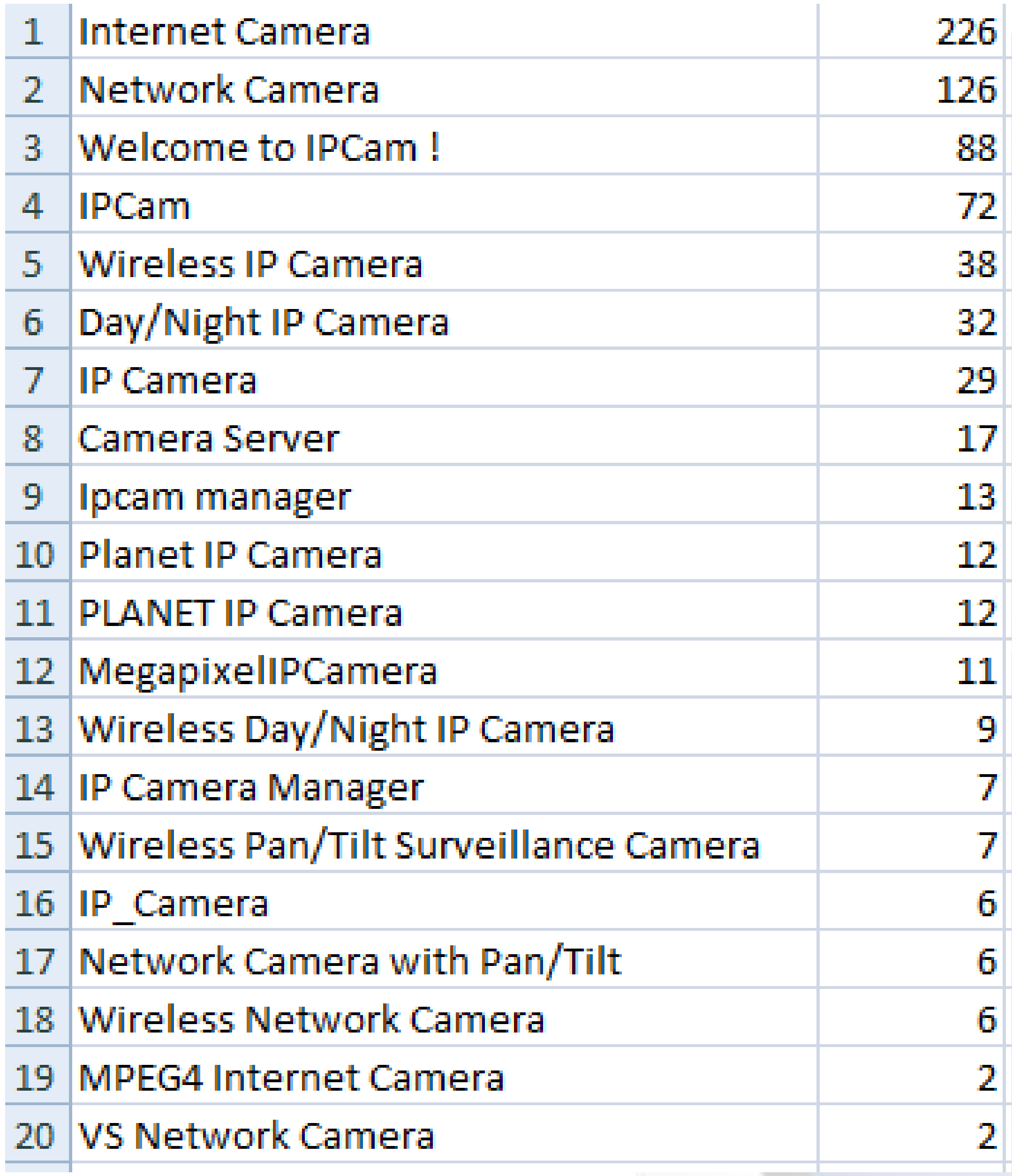
Top 20 realm strings (WWW-Authentication):



1	SmartAX	28636
2	EchoLife Home Gateway	2763
3	level_15_access	1570
4	Home Gateway	1426
5	Default: admin/1234	1292
6	Allied Telesis AT-AR415S	1290
7	ADSL Modem	1042
8	DI-524	1014
9	Wireless Access Point	654
10	WL520gc	647
11	level_15 or view_access	542
12	RT-G32	534
13	RT-N10	471
14	RT-N10+	471
15	Wireless Broadband Router	342
16	dreambox	319
17	RT-N10E	316
18	streaming_server	281
19	11N Broadband Router	271
20	level 15 access	267

Other interesting stuff...

IP cameras connected to the internet: **756** (based on realm string)



1	Internet Camera	226
2	Network Camera	126
3	Welcome to IPCam !	88
4	IPCam	72
5	Wireless IP Camera	38
6	Day/Night IP Camera	32
7	IP Camera	29
8	Camera Server	17
9	Ipcam manager	13
10	Planet IP Camera	12
11	PLANET IP Camera	12
12	MegapixelIPCamera	11
13	Wireless Day/Night IP Camera	9
14	IP Camera Manager	7
15	Wireless Pan/Tilt Surveillance Camera	7
16	IP_Camera	6
17	Network Camera with Pan/Tilt	6
18	Wireless Network Camera	6
19	MPEG4 Internet Camera	2
20	VS Network Camera	2

See the video of this talk:

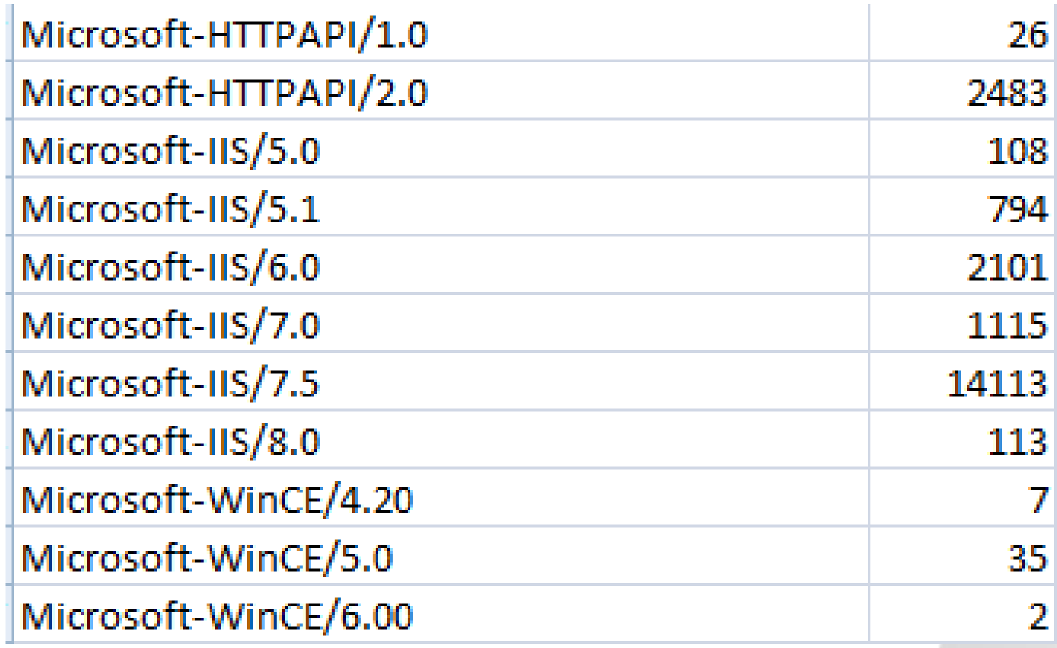
“Do you know who's watching you?: An in-depth examination of IP cameras attack surface”

Francisco Falcon and Nahuel Riva

Hack.lu 2013

Other interesting stuff...

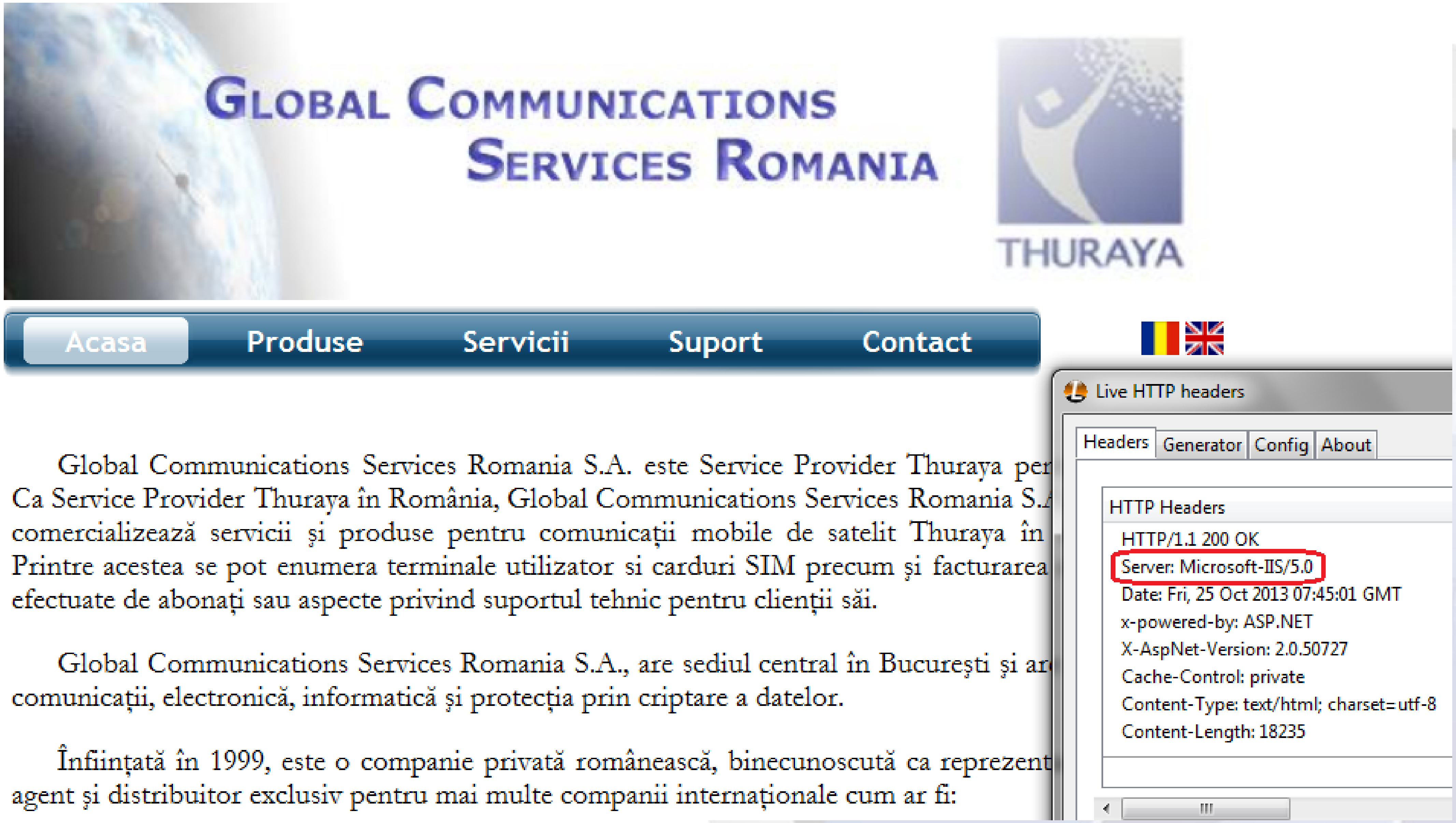
Interesting web servers…



Microsoft-HTTPAPI/1.0	26
Microsoft-HTTPAPI/2.0	2483
Microsoft-IIS/5.0	108
Microsoft-IIS/5.1	794
Microsoft-IIS/6.0	2101
Microsoft-IIS/7.0	1115
Microsoft-IIS/7.5	14113
Microsoft-IIS/8.0	113
Microsoft-WinCE/4.20	7
Microsoft-WinCE/5.0	35
Microsoft-WinCE/6.00	2

Apache rulz (by the numbers)
Lighttpd
Nginx
RomPager
…

Low hanging fruit (examples)



Global Communications Services Romania S.A. este Service Provider Thuraya per
Ca Service Provider Thuraya în România, Global Communications Services Romania S.A
comercializează servicii şi produse pentru comunicaţii mobile de satelit Thuraya în
Printre acestea se pot enumera terminale utilizator si carduri SIM precum şi facturarea
efectuate de abonaţi sau aspecte privind suportul tehnic pentru clienţii săi.

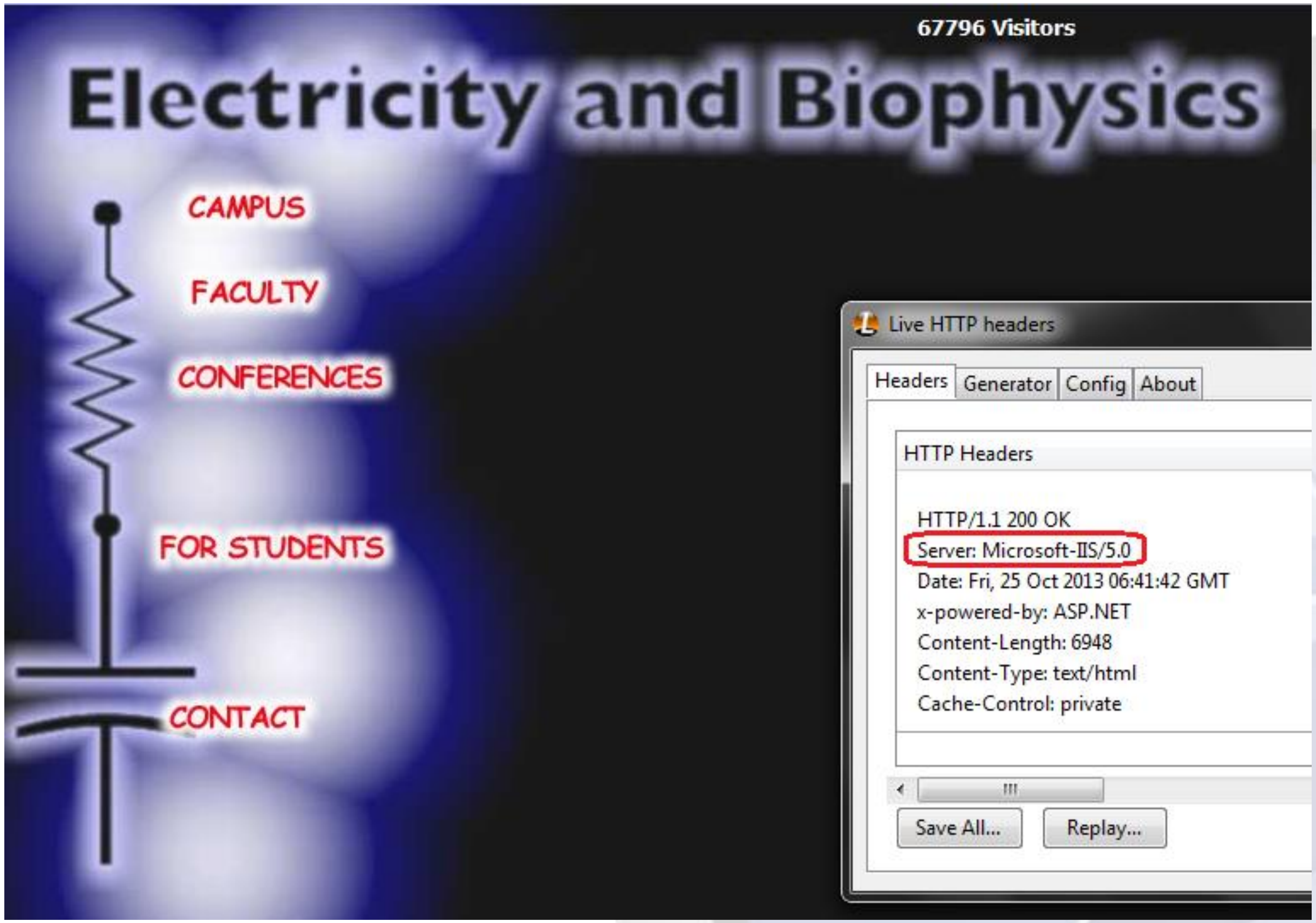
Global Communications Services Romania S.A., are sediul central în Bucureşti şi ar
comunicaţii, electronică, informatică şi protecţia prin criptare a datelor.

Înfiinţată în 1999, este o companie privată românească, binecunoscută ca reprezent
agent şi distribuitor exclusiv pentru mai multe companii internaţionale cum ar fi:

HTTP Headers

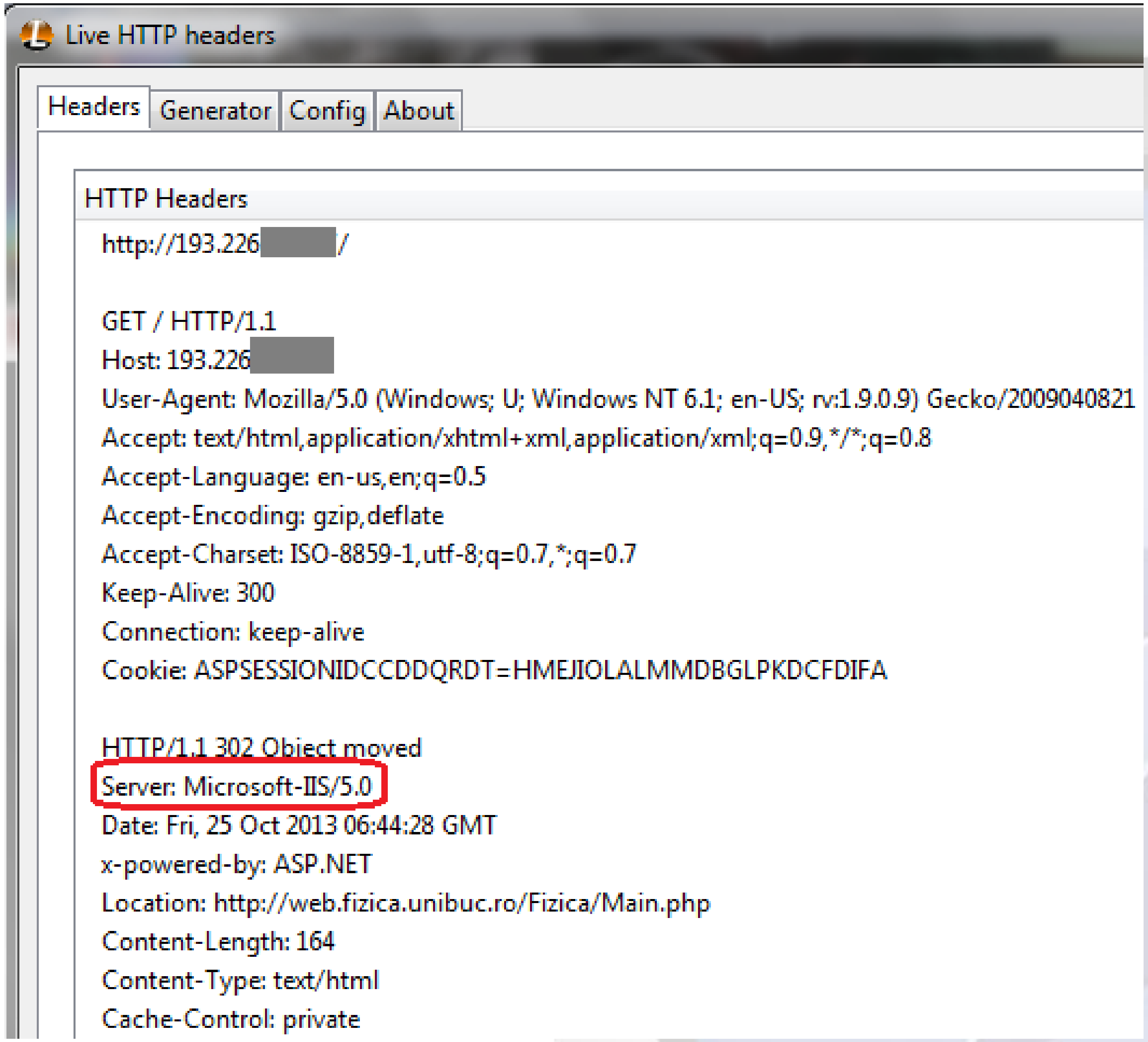
```
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Fri, 25 Oct 2013 07:45:01 GMT
x-powered-by: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 18235
```

Low hanging fruit (examples)



```
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Fri, 25 Oct 2013 06:41:42 GMT
x-powered-by: ASP.NET
Content-Length: 6948
Content-Type: text/html
Cache-Control: private
```

Low hanging fruit (examples)



```
http://193.226[redacted]/

GET / HTTP/1.1
Host: 193.226[redacted]
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.0.9) Gecko/2009040821
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: ASPSESSIONIDCCDDQRDT=HMEJIOLALMMDBGLPKDCFDIFA

HTTP/1.1 302 Object moved
Server: Microsoft-IIS/5.0
Date: Fri, 25 Oct 2013 06:44:28 GMT
x-powered-by: ASP.NET
Location: http://web.fizica.unibuc.ro/Fizica/Main.php
Content-Length: 164
Content-Type: text/html
Cache-Control: private
```

End of fun part

What should we do about it?

- ❑ Increase the security awareness level to all people (technical and non-technical)
  - ○ Upgrade software periodically
- ❑ Create and implement a national security program to periodically evaluate the security of IT systems belonging to public institutions and academia.
- ❑ Perform vulnerability assessment AND penetration testing periodically in the private sector.

Further work

❑ Do the same vulnerability scan for other common ports (all data is available):

- 8080
- 21
- 22
- 23
- 25
- 110
- …

???

Q & A

Thank You!

Adrian Furtună, PhD, OSCP, CEH
adif2k8@gmail.com
http://ro.linkedin.com/in/adrianfurtuna