
D C
74 96

Hacking routers as Web Hacker

WHOAMI

- Researcher @ hlsec.ru
- @cyberpunkych
- Attacking MongoDB @ ZN2012
- Database honeypot by design @ Defcon Russia
- Meme Master

Routers everywhere.

- Home
- Work
- Hospitals
- Banks
- In your bag
- etc

But I’m web hacker, what can I do?

- Router’s web control panel == web site
- Connect managers with web interface, such as Yota Access ☺
- ISP (statistics, billing, management, etc)

Routerzzz

OWASP TOP 10 for routers

- Default credentials
- Auth bypass
- XSS
- CSRF
- Command Injection
- Sensitive info leak
- Bugs in third party libraries
- RCE, XXE, etc

Default credentials

Should I say anything?

Authentication Bypass/No Auth

- Hello, Yota Many
- Hello, D-Link's backdoor
- Hello, MTS 4G Router
- Hello, others

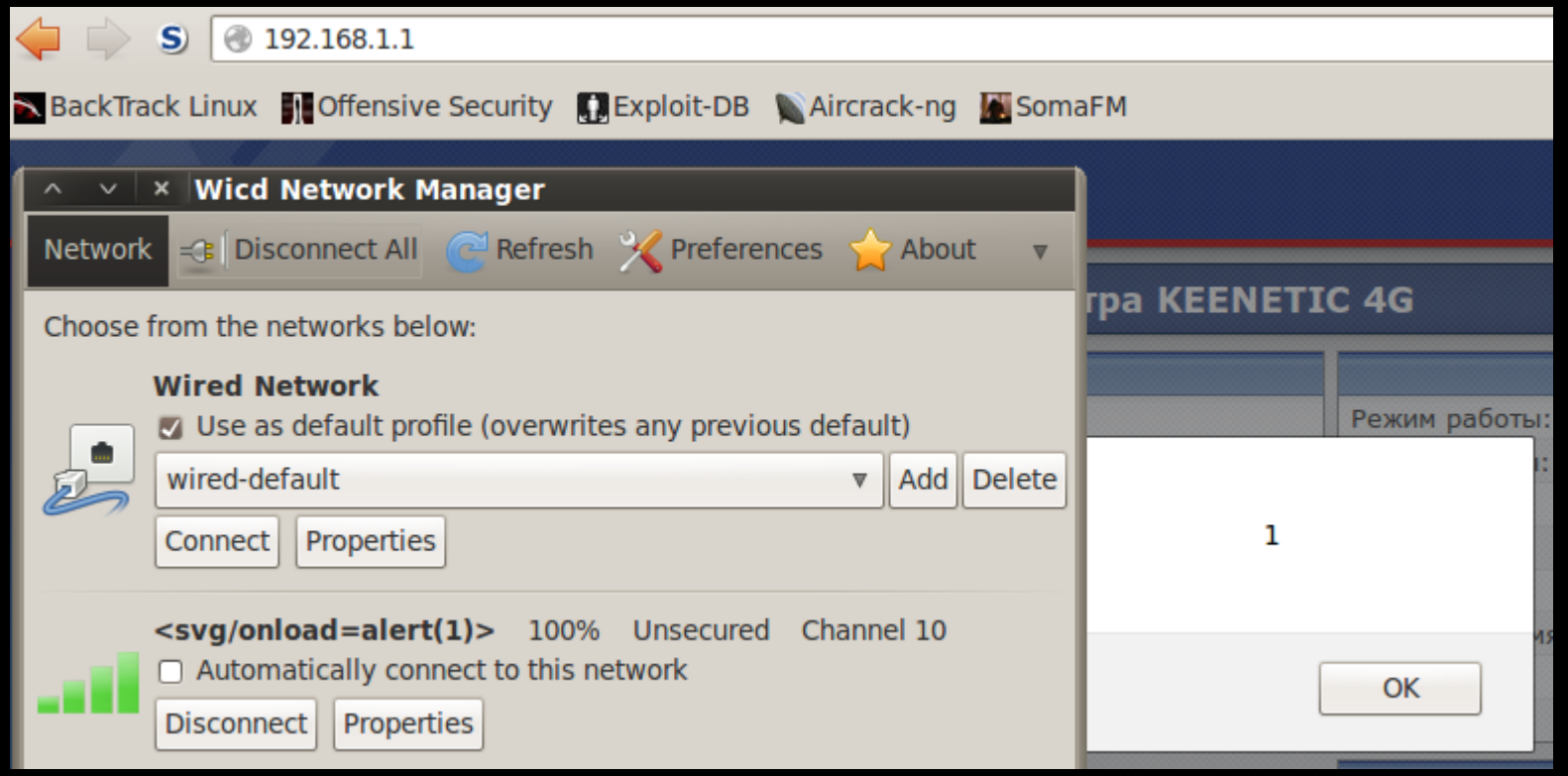
```
#define AUTH_OK 1
#define AUTH_FAIL -1

int alpha_auth_check(struct http_request_t *request)
{
    if(strstr(request->url, "graphic/") ||
       strstr(request->url, "public/") ||
       strcmp(request->user_agent, "xmlset_roodkcableoj28840ybtide") == 0)
    {
        return AUTH_OK;
    }
    else
    {
        // These arguments are probably user/pass or session info
        if(check_login(request->0xC, request->0xE0) != 0)
        {
            return AUTH_OK;
        }
    }

    return AUTH_FAIL;
}
```

(DIR-100, DI-524, DI-604, etc)

CSRF/XSS everywhere



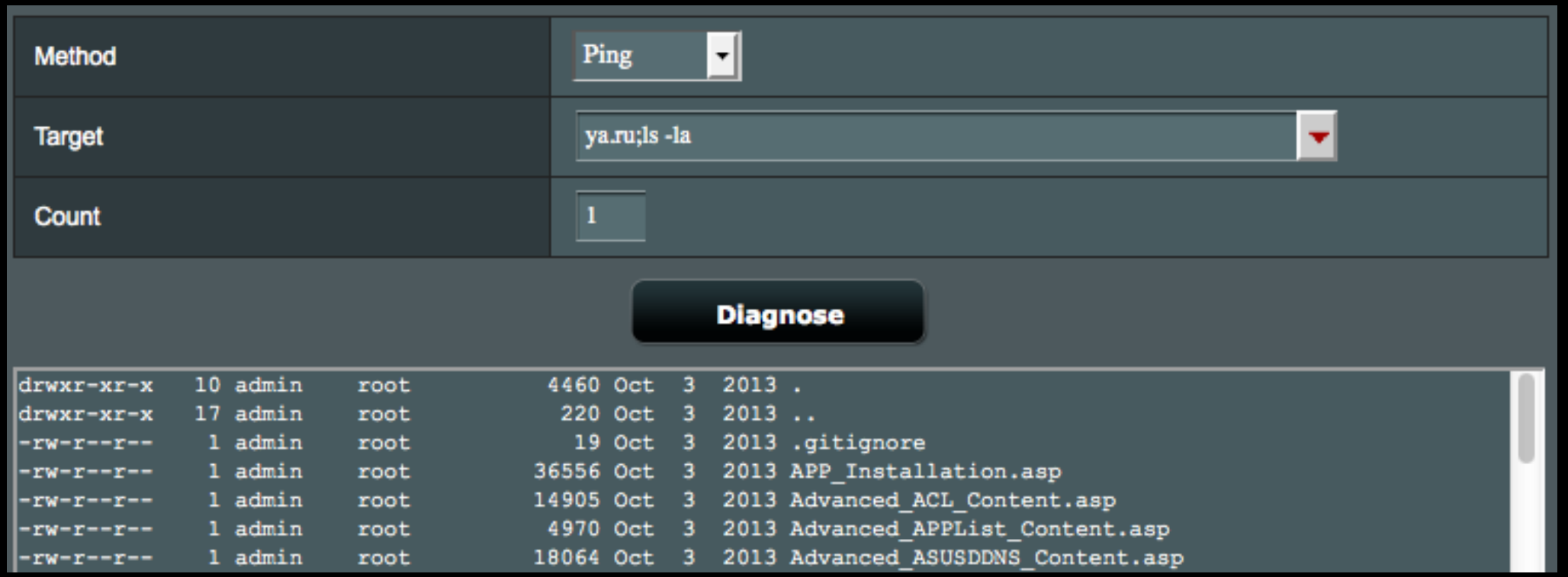
(Zyxel Keenetic v1)

Srlsy, it’s everywhere. But why?

Because **** you, that’s why.

Command injection

Always check network tools ☺

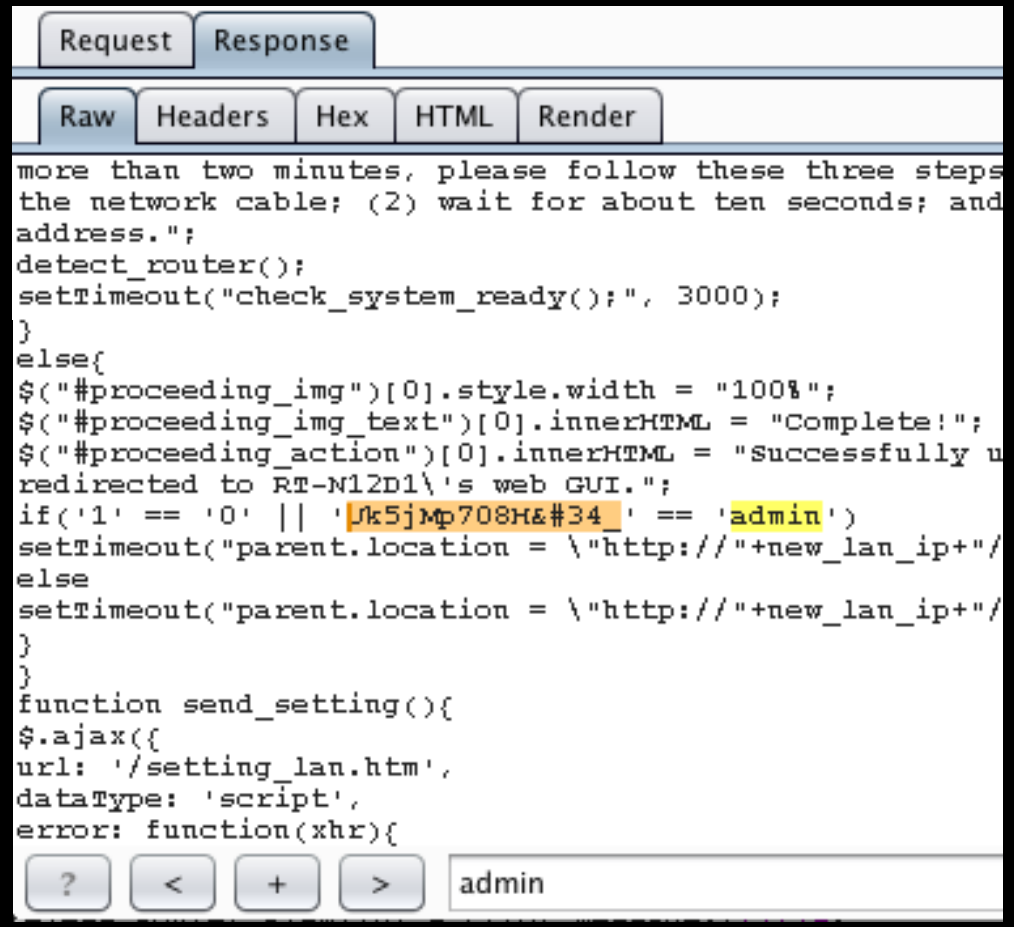


(ASUS RT-N10P)

Sensitive info leak

- /error_page.htm
- /DevInfo.php
- /rom-0

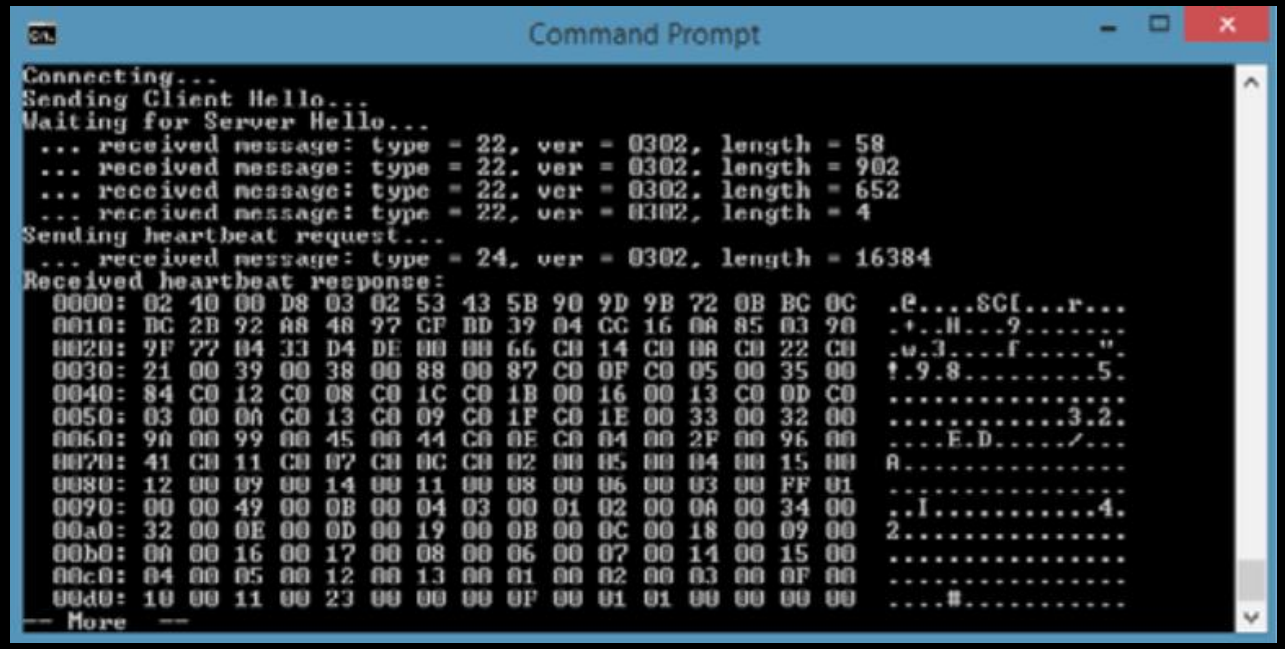
```
➜ ~  curl http://217.162.11.253:8080/DevInfo.php
Firmware External Version: V2.12
Firmware Internal Version: c1ik
Model Name: DIR-300
Hardware Version: Bx
WLAN Domain: GB
Kernel: 2.6.33.2
Language: en
Graphcal Authentication: Disable
LAN MAC: cc:b2:55:5c:a9:8a
WAN MAC: cc:b2:55:5c:a9:8b
WLAN MAC: cc:b2:55:5c:a9:8a
➜ ~
```



(ASUS RT-N12D1)

Bugs in third party libraries

- Heartbleed
- ShellShock
- RomPager
- etc



Hacking algorithm

WARNINNG!

ВАС ПРИСТРЕЛЯТ ПО УТРУ – НЕ РАБОТАЙТЕ ПО РУ!

1. Get the firmware

- Check vendor web site/ftp
- Get firmware source code (GPL profits)
- No firmware at all? Dump it via UART/SPI/JTAG (HW mode on)

```
root@kali06:~/Documents/cyberpunkych# wget http://ftp.dlink.ru/pub/Router/DIR-300/Firmware/DIR-300A1_FW105b09.bin
--2015-10-01 16:57:38--  http://ftp.dlink.ru/pub/Router/DIR-300/Firmware/DIR-300A1_FW105b09.bin
Resolving ftp.dlink.ru (ftp.dlink.ru)... 94.198.53.90
Connecting to ftp.dlink.ru (ftp.dlink.ru)|94.198.53.90|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2347136 (2.2M) [application/octet-stream]
Saving to: 'DIR-300A1_FW105b09.bin'

DIR-300A1_FW105b09.bin                    100%[=============================================================================>]

2015-10-01 16:57:38 (6.47 MB/s) - 'DIR-300A1_FW105b09.bin' saved [2347136/2347136]
```

2. Unpack it

- Binwalk -> search for signature and try to unpack
- Firmware-mod-kit pack/unpack
- If NO_SUCCESS -> analyze firmware entropy
- Sasquatch for squashfs, other fs -> google for tools

```
root@kali06:~/Documents/cyberpunkych# binwalk -Me DIR-300A1_FW105b09.bin

Scan Time:     2015-10-01 16:57:47
Target File:   DIR-300A1_FW105b09.bin
MD5 Checksum:  36c509231c61ce4dc72d26b546bbf1f5
Signatures:    285

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
96            0x60            LZMA compressed data, properties: 0x5D, dictionary size:
524384        0x80060         PackImg section delimiter tag, little endian size: 136384
524416        0x80080         Squashfs filesystem, big endian, version 2.0, size: 18192
```

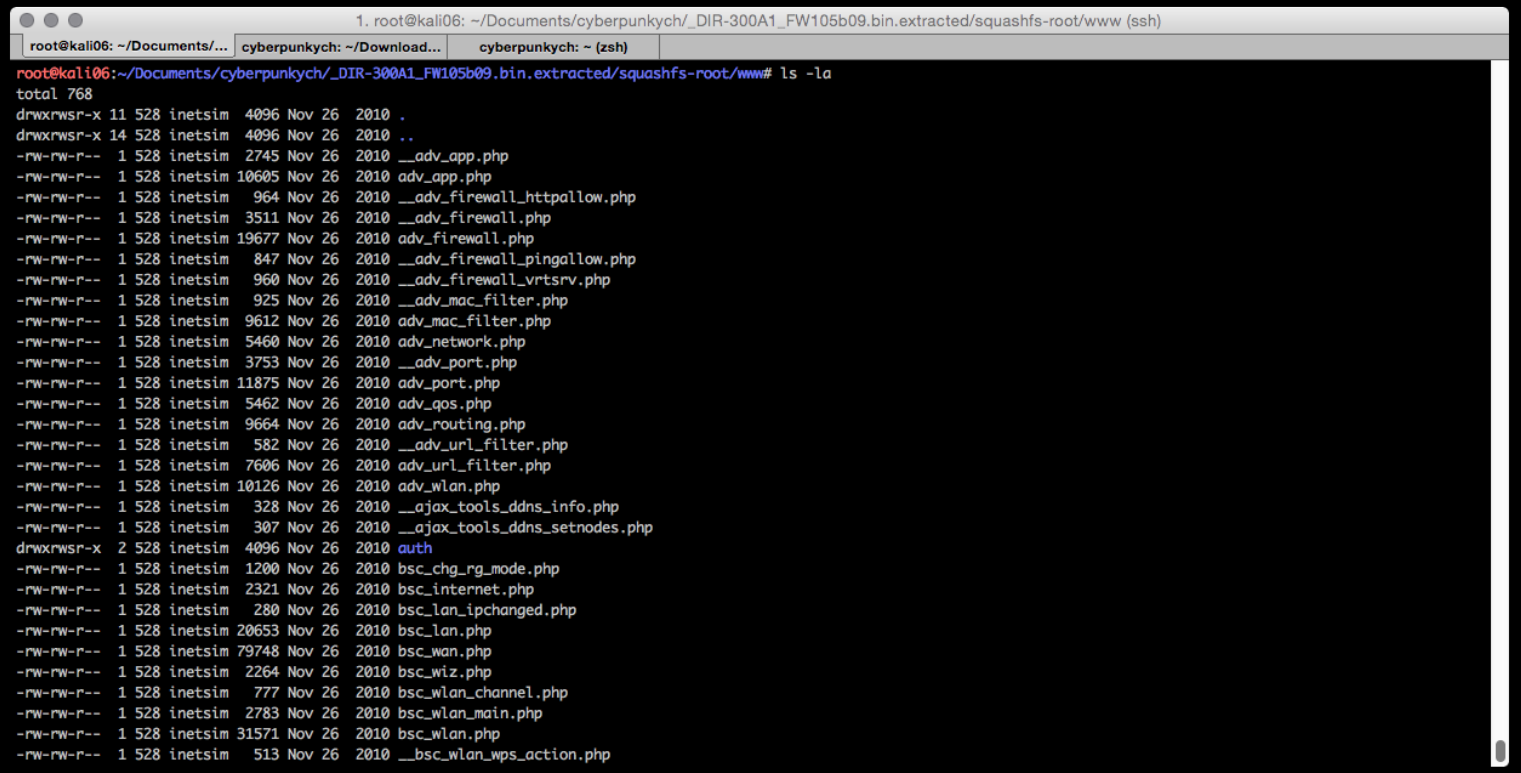
```
root@kali06:~/Documents/cyberpunkych/_DIR-300A1_FW105b09.bin.extracted# sasquatch 80080.squashfs
SquashFS version [512.0] / inode count [2130903040] suggests a SquashFS image of a different endianess
Reading a different endian SQUASHFS filesystem on 80080.squashfs
Parallel unsquashfs: Using 1 processor
Trying to decompress using default gzip decompressor...
Trying to decompress with lzma...
Trying to decompress with lzma-adaptive...
Detected lzma-adaptive compression
842 inodes (901 blocks) to write

[==========================================================================================

created 742 files
created 53 directories
created 100 symlinks
created 0 devices
created 0 fifos
```

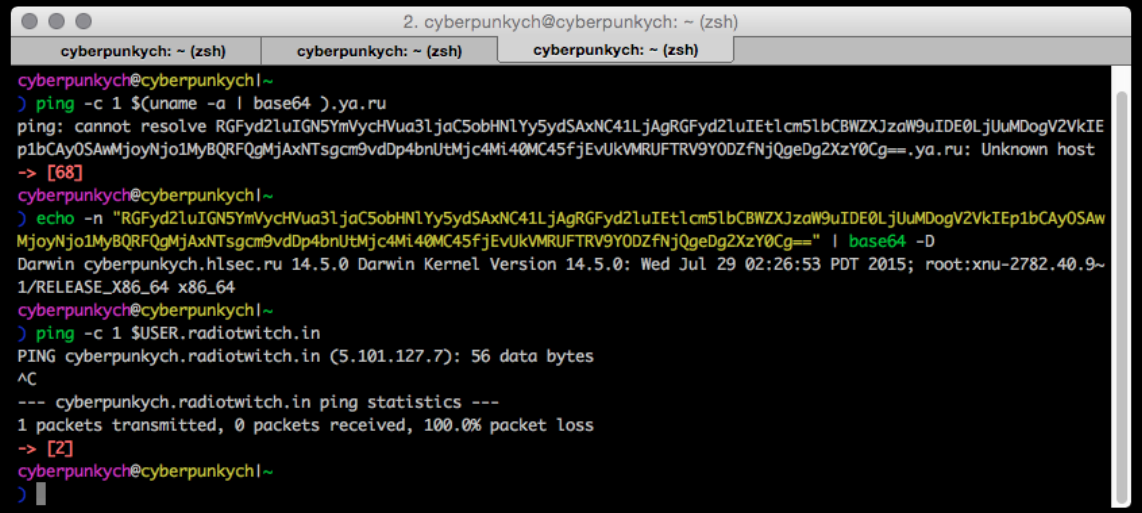
3. CHECK AUTH

- Black Box => White Box
- for i in *; do curl http://router_ip/$i; done
- You know what to do ;)



4. CHECK CMD INJECTION

- PING -> ya.ru;ls
- CONFIG backup to FTP/TFTP
- Any place where command execution is used
- Check all shell symbols
- Error-based command injection for output




```
# ping ya.ru || ls
# ping $(uname)
# ping `uname`
# ping ya.ru && ls
# ping ya.ru; ls
# ping $USER.ya.ru
```

...

5. Check for XSS

- <script>alert(1)</script> for every param!
- Check hostname, sometimes it can help you ☺
- Even 1 XSS => PROFIT!!1
- Stored XSS => Compromised web interface

5. Check for XSS

- <script>alert(1)</script> for every param!
- Check hostname, sometimes it can help you ☺
- Even 1 XSS => PROFIT!!1
- Stored XSS => Compromised web interface

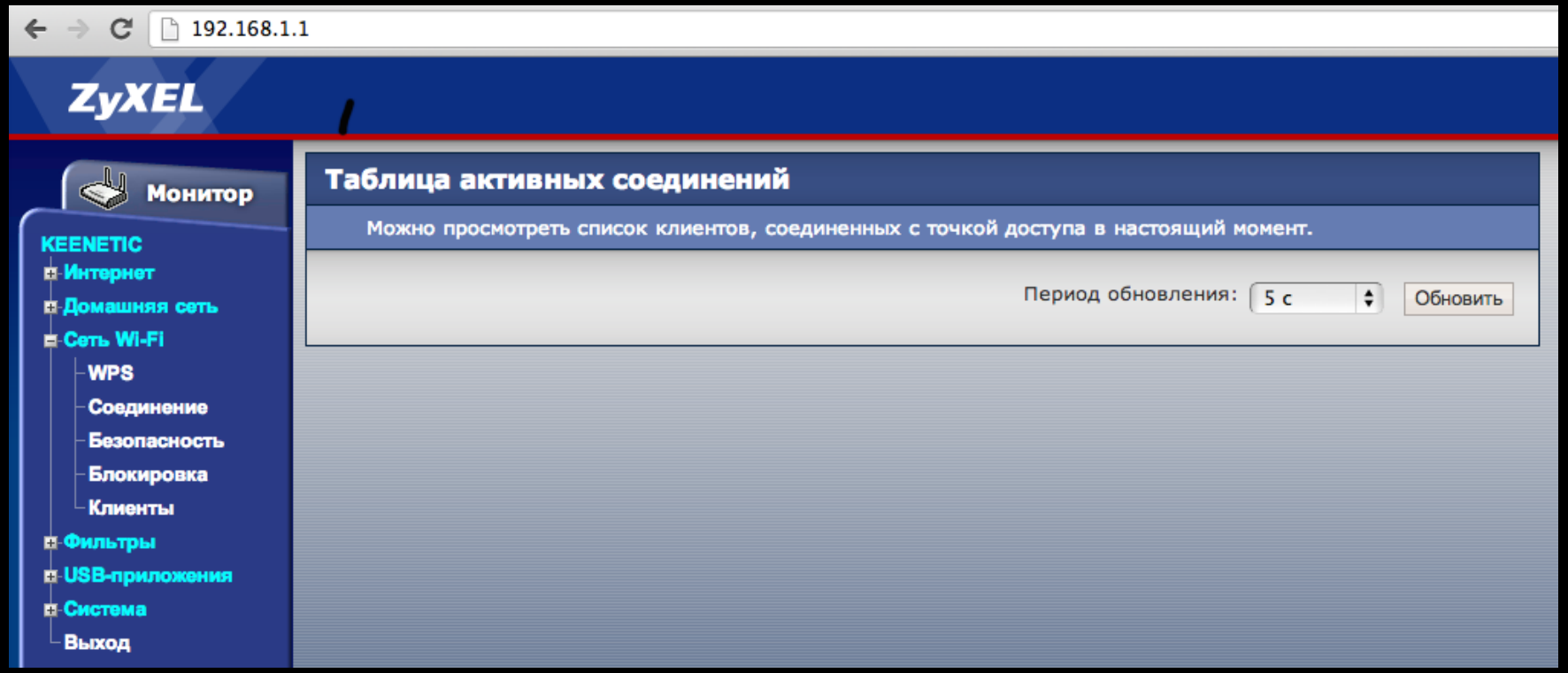
Typical attack scheme:

Link/Page with XSS => AJAX => getElementsByTagName('input')[*].value => log data

Hide myself from web aka rookit hostname

Hello, 1'}]"); !

Hide’n’seek from browser via xss in Zyxel Keenetic.



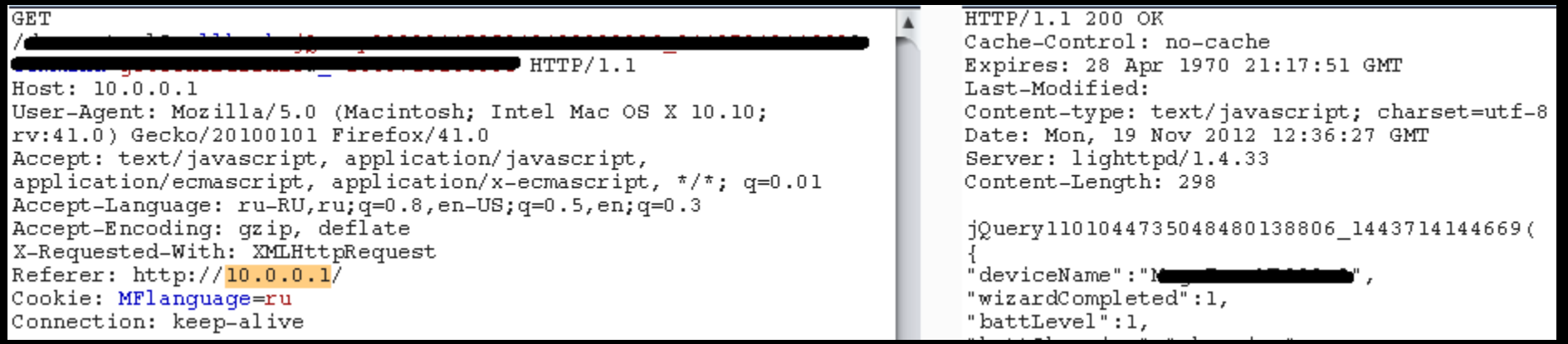
6. Check for CSRF

- Inspect for anti-csrf tokens
- Check X-Requested-With
- Referer check

6. Check for CSRF

- Inspect for anti-csrf tokens
- Check X-Requested-With
- **Referer check**

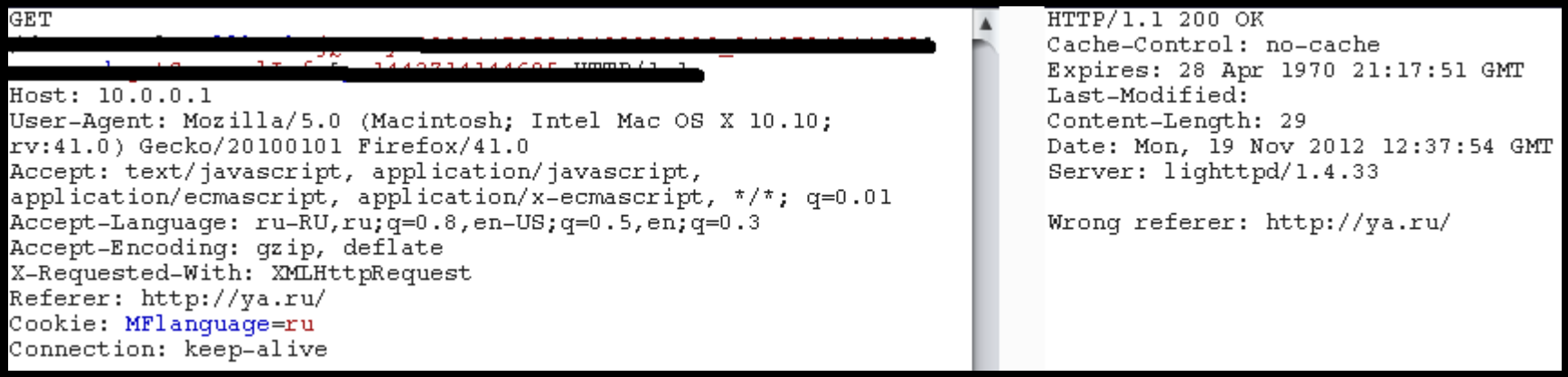
Referer checking:



6. Check for CSRF

- Inspect for anti-csrf tokens
- Check X-Requested-With
- **Referer check**

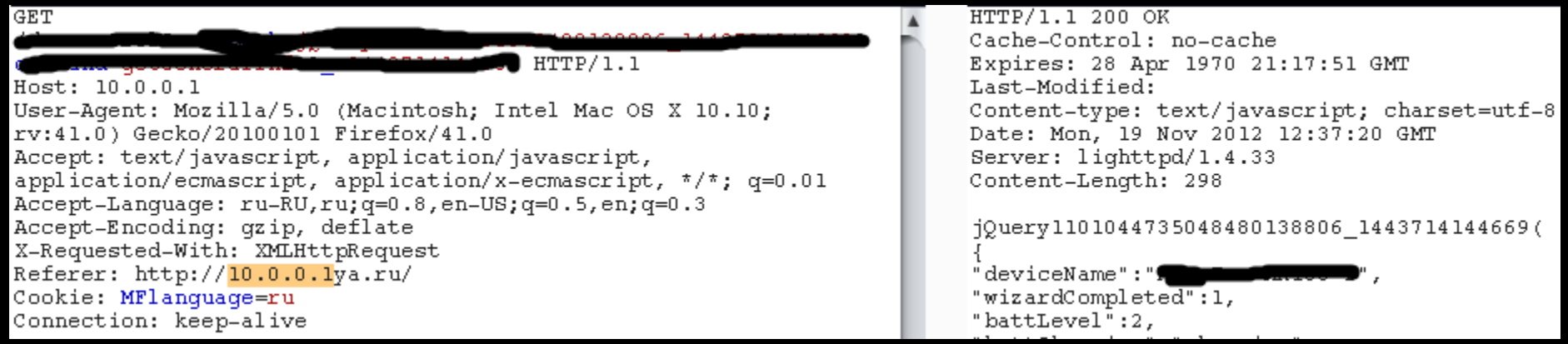
Any other == bad referer:



6. Check for CSRF

- Inspect for anti-csrf tokens
- Check X-Requested-With
- **Referer check**

Open Redirect trick to bypass regexp:



CSRF => MITM

All you need is ~~love~~ CSRF via updating DNS settings!

(<img src="csrf">, habrahabr, you know.)

XSS + Smart CSRF

1. Get the internal IP address using a nice WebRTC hack
2. Get router IP (no so many requests 8))
3. Make CSRF Request via XSS payload (better for stored XSS)
4. Get all data (sometimes passwords stored in *input.value*'s)
5. Redirect to page with XSS
6. ???
7. All your data are belong to us!

Support Software

Support Software

- %operator_name% Connect (Huawei modems), Yota Access, etc
- **Sometimes they also use web inside apps!**
- Binary bugs (BOF, etc)
- Bugs with bad privileges
- Sniff requests to ISP => new bugs

Support Software

From CSRF to RCE!

video_here

ISP

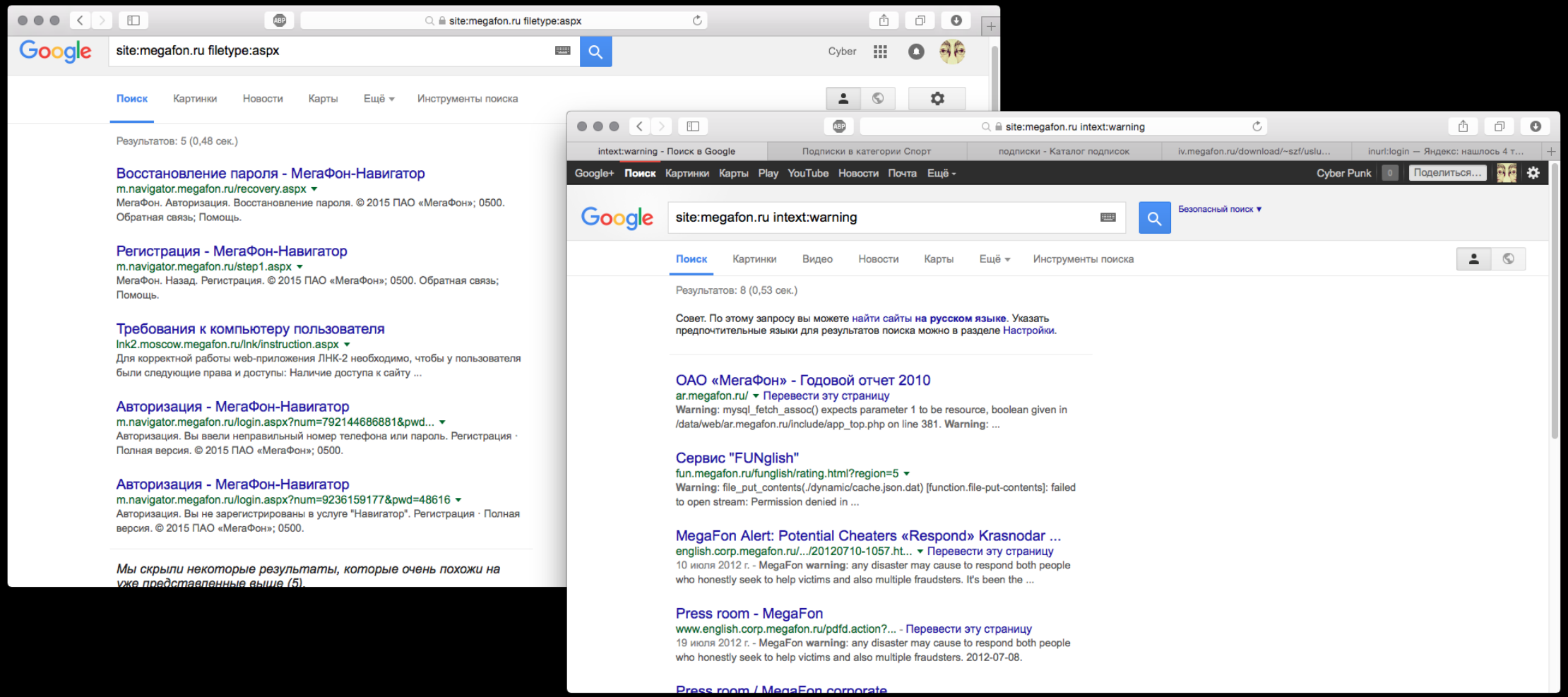
ISP – Just another target

- Google/Yandex dork
- Cabinet/Balance/etc on provider’s site
- Subdomains
- Popular services

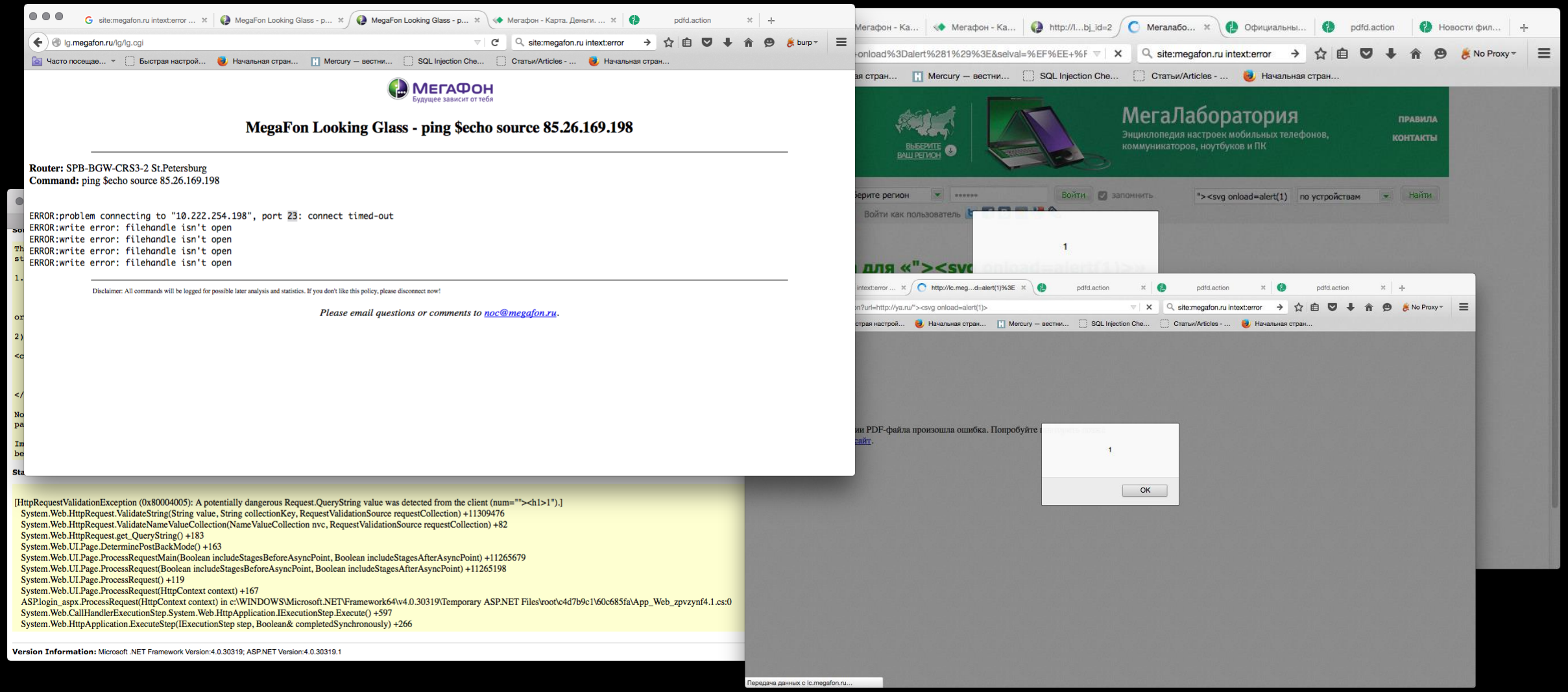
Why it is important?

- Update server control
- Client-side tricks (crossdomain.xml)
- Remote device administration
- New default credentials
- Attack firmware developers

Google it!

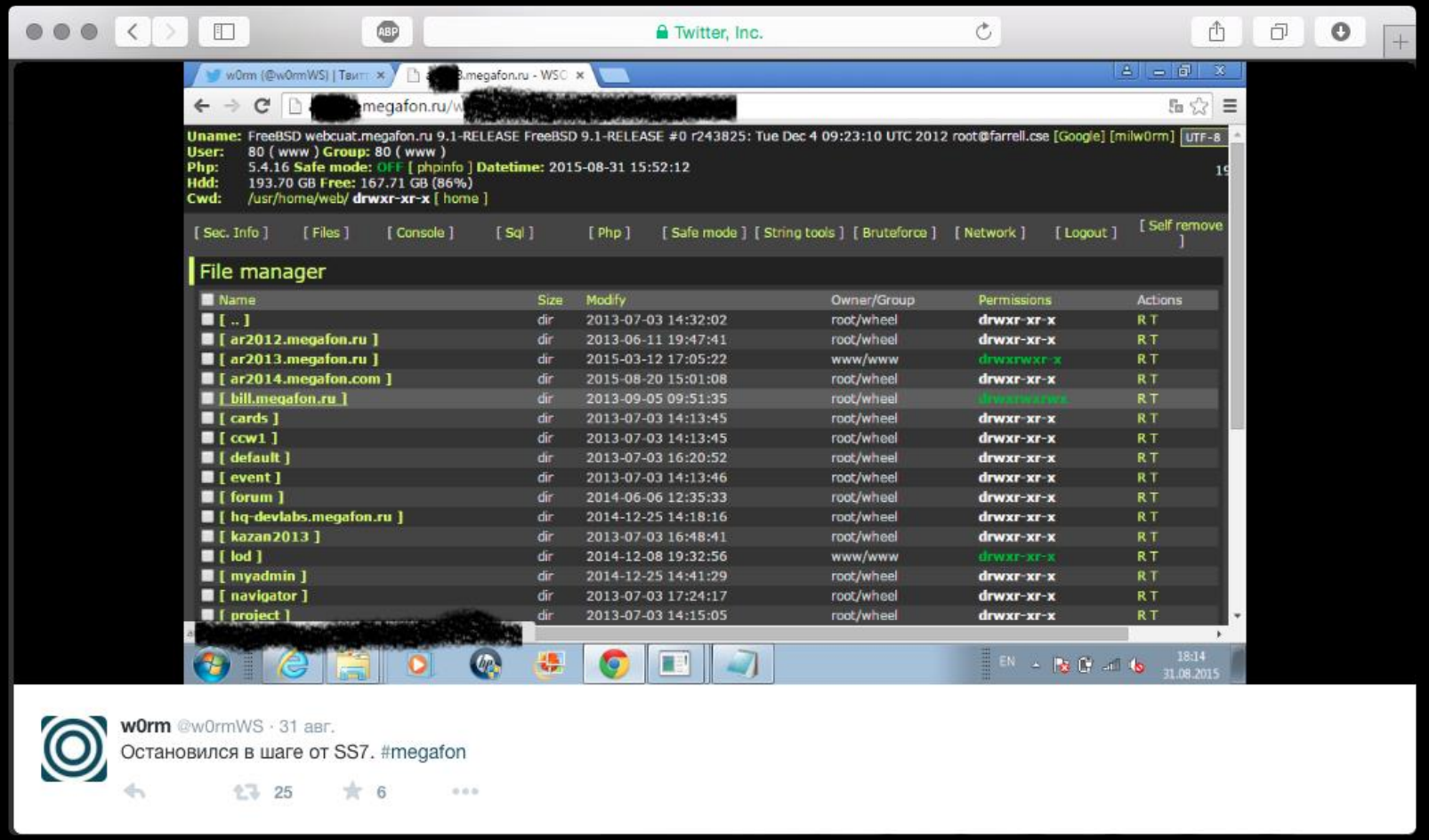

site:megafon.ru filetype:aspx
Google
site:megafon.ru filetype:aspx
Поиск Картинки Новости Карты Ещё Инструменты поиска
Результатов: 5 (0,48 сек.)
Восстановление пароля - МегаФон-Навигатор
m.navigator.megafon.ru/recovery.aspx
МегаФон. Авторизация. Восстановление пароля. © 2015 ПАО «МегаФон»; 0500. Обратная связь; Помощь.
Регистрация - МегаФон-Навигатор
m.navigator.megafon.ru/step1.aspx
МегаФон. Назад. Регистрация. © 2015 ПАО «МегаФон»; 0500. Обратная связь; Помощь.
Требования к компьютеру пользователя
lnk2.moscow.megafon.ru/lnk/instruction.aspx
Для корректной работы web-приложения ЛНК-2 необходимо, чтобы у пользователя были следующие права и доступы: Наличие доступа к сайту ...
Авторизация - МегаФон-Навигатор
m.navigator.megafon.ru/login.aspx?num=792144686881&pwd...
Авторизация. Вы ввели неправильный номер телефона или пароль. Регистрация · Полная версия. © 2015 ПАО «МегаФон»; 0500.
Авторизация - МегаФон-Навигатор
m.navigator.megafon.ru/login.aspx?num=9236159177&pwd=48616
Авторизация. Вы не зарегистрированы в услуге "Навигатор". Регистрация · Полная версия. © 2015 ПАО «МегаФон»; 0500.
Мы скрыли некоторые результаты, которые очень похожи на уже представленные выше (5).
site:megafon.ru intext:warning
intext:warning - Поиск в Google
Подписки в категории Спорт
подписки - Каталог подписок
Google+ Поиск Картинки Карты Play YouTube Новости Почта Ещё
Cyber Punk
Поделиться...
Google
site:megafon.ru intext:warning
Безопасный поиск
Поиск Картинки Видео Новости Карты Ещё Инструменты поиска
Результатов: 8 (0,53 сек.)
Совет. По этому запросу вы можете найти сайты на русском языке. Указать предпочтительные языки для результатов поиска можно в разделе Настройки.
ОАО «МегаФон» - Годовой отчет 2010
ar.megafon.ru/ Перевести эту страницу
Warning: mysql_fetch_assoc() expects parameter 1 to be resource, boolean given in /data/web/ar.megafon.ru/include/app_top.php on line 381. Warning: ...
Сервис "FUNglish"
fun.megafon.ru/funglish/rating.html?region=5
Warning: file_put_contents(./dynamic/cache.json.dat) [function.file-put-contents]: failed to open stream: Permission denied in ...
MegaFon Alert: Potential Cheaters «Respond» Krasnodar ...
english.corp.megafon.ru/.../20120710-1057.ht... Перевести эту страницу
10 июля 2012 г. - MegaFon warning: any disaster may cause to respond both people who honestly seek to help victims and also multiple fraudsters. It's been the ...
Press room - MegaFon
www.english.corp.megafon.ru/pdfd.action?... - Перевести эту страницу
19 июля 2012 г. - MegaFon warning: any disaster may cause to respond both people who honestly seek to help victims and also multiple fraudsters. 2012-07-08.

Just google.


lg.megafon.ru/lg/lg.cgi
site:megafon.ru intext:error
МЕГАФОН
Будущее зависит от тебя
MegaFon Looking Glass - ping $echo source 85.26.169.198
Router: SPB-BGW-CRS3-2 St.Petersburg
Command: ping $echo source 85.26.169.198
ERROR:problem connecting to "10.222.254.198", port 23: connect timed-out
ERROR:write error: filehandle isn't open
ERROR:write error: filehandle isn't open
ERROR:write error: filehandle isn't open
ERROR:write error: filehandle isn't open
Disclaimer: All commands will be logged for possible later analysis and statistics. If you don't like this policy, please disconnect now!
Please email questions or comments to noc@megafon.ru.
МегаЛаборатория
Энциклопедия настроек мобильных телефонов, коммуникаторов, ноутбуков и ПК
ПРАВИЛА
КОНТАКТЫ
Войти
Найти
1
OK
[HttpRequestValidationException (0x80004005): A potentially dangerous Request.QueryString value was detected from the client (num="><h1>1").]
System.Web.HttpRequest.ValidateString(String value, String collectionKey, RequestValidationSource requestCollection) +11309476
System.Web.HttpRequest.ValidateNameValueCollection(NameValueCollection nvc, RequestValidationSource requestCollection) +82
System.Web.HttpRequest.get_QueryString() +183
System.Web.UI.Page.DeterminePostBackMode() +163
System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +11265679
System.Web.UI.Page.ProcessRequest(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +11265198
System.Web.UI.Page.ProcessRequest() +119
System.Web.UI.Page.ProcessRequest(HttpContext context) +167
ASP.login_aspx.ProcessRequest(HttpContext context) in c:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\c4d7b9c1\60c685fa\App_Web_zpvzynf4.1.cs:0
System.Web.CallHandlerExecutionStep.System.Web.HttpApplication.IExecutionStep.Execute() +597
System.Web.HttpApplication.ExecuteStep(IExecutionStep step, Boolean& completedSynchronously) +266
Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.0.30319.1

WARNINNG! WARNINNG! WARNINNG!

Example from real life



Conclusion

- Router == web site
- Black Box => White Box
- XSS/CSRF everywhere
- Vuln1+vuln2->vuln3
- The RCE is out there
- R.E.S.H.E.T.O.

INFO:
@cyberpunkych

Links:
http://www.routerpwn.com
http://routersecurity.org
http://seclists.org
http://dsec.ru/upload/medialibrary/589/589327eb24133e5c615fa11950340e05.pdf
http://goo.gl/0P2rgl
https://github.com/devttys0/sasquatch
https://github.com/0x90/kali-scripts/blob/master/embedded.sh
https://goo.gl/x3XjLU

Any questions?

Thnx:
@090h
@n3tw0rk_