



OWASP

Open Web Application
Security Project



→ **#DontTrustTheDarkSide**

@c0rdis

OWASP EEE - Bucharest

Whoami

CONNECT.

LEARN.

GROW.

Luke Skywalker in EY

*OWASP Russia Chapter
Leader, co-org of EEE*



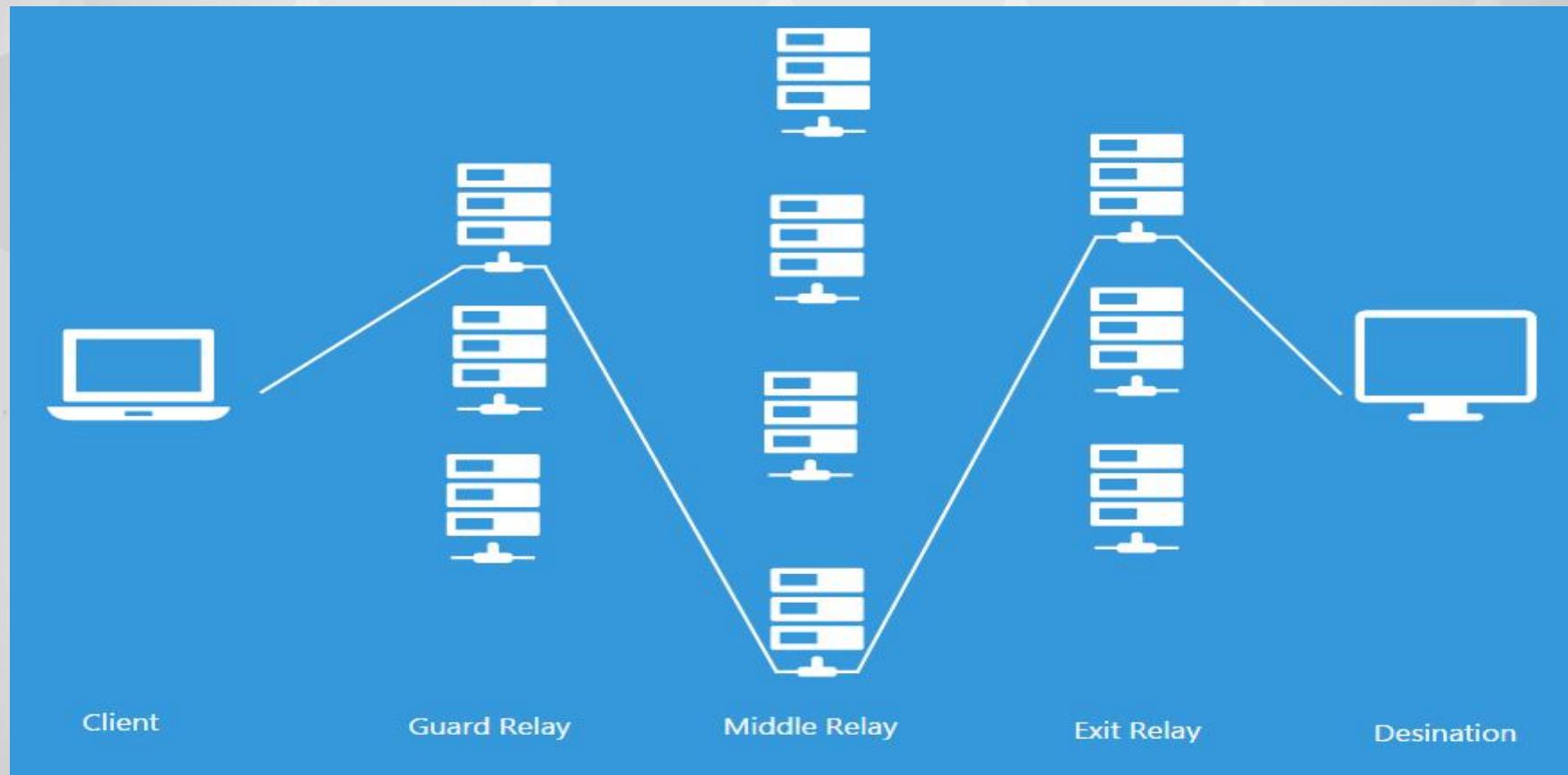
OWASP
Open Web Application
Security Project

Darkweb



The Tor network is a group of volunteer-operated servers that allows people *to improve their privacy and security* on the Internet. Tor's users employ this network by connecting through a series of virtual tunnels rather than making a direct connection, thus allowing both organizations and individuals to share information over public networks without compromising their privacy.

Darkweb



Picture from <http://jordan-wright.com/>

Darkweb

„... unfortunately for thrill-seekers, almost all the sites purporting to offer this type of content far have turned out to be fake, be that live streams of torture, hitmen for hire, or human trafficking.

In reality, the dark web is a relatively tiny collection of difficult-to-reach sites, that, for criminals, deal in drugs, weapons, stolen data, and child pornography. On the brighter side, are sites for dropping sensitive documents to journalists, and that page that just endlessly tells cat jokes.”

http://motherboard.vice.com/en_ca/read/the-real-dark-web-doesnt-exist

Some known darknet attacks

- Controlling nodes
(MitM/traffic confirmation/timing/correlation attacks)
- Exploits against Flash/FF/...
- Vulnerable protocols



Approach

- Conventionally low-risk vulnerabilities of all kinds of information disclosure
- In a normal pentest that would rather be marked as recommended
- In darknet it can be game over for one's privacy



Similar research

- Hyperion Gray – [Mass 'Dark Web' Scanning with PunkSPIDER](#)

Outcomes:

- hidden service web apps are actually reasonably secure as a general whole
- hidden services aren't trivial to attack in an automated way reliably, decreasing the effectiveness of script kiddies
- vulnerabilities do exist in hidden services (maybe this was obvious) and they can have a serious impact on privacy

Similar research

- [@cthulhusec](#)



the grugq @thegrugq · Aug 22

“@c0rdis: Deanonymization made simple: [aan.sh/Ob2M](#)” << same techniques that [@CthulhuSec](#) uses in his blog post. Cool

RETWEETS

23

FAVORITES

24



12:35 PM - 22 Aug 2015 · Details



...



OWASP
Open Web Application
Security Project

CONNECT. LEARN. GROW.

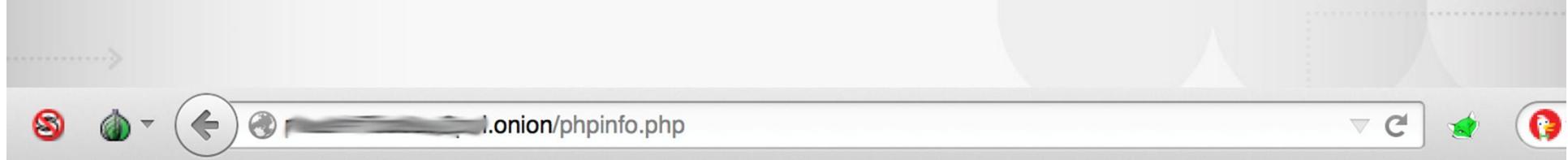
How it all started



OWASP
Open Web Application
Security Project

Instant win

- /phpinfo.php ~ 1% (10 out of 1000)
- /server-info ~ 0% (1 out of 1000, rather exception)



Who really puts a phpinfo file at the root of their server? Nice try though. In the meantime try learning some hacking.

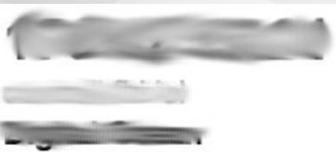
Redirects

- Generally bad practice of having clear- and darknet services enabled at the same time (we will see it many times today ☺)
- Simple access to the IP address may lead to fail

```
HTTP/1.1 302 Found
Date: Fri, 21 Aug 2015 16:30:32 GMT
Server: Apache/2.2.22 (Debian)
Location: http://[REDACTED].onion/index.html
Vary: Accept-Encoding
Content-Length: 224
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
```

Shodan

- Lazy bastard way



Added on 2015-08-16 11:42:34 GMT

United States

[Details](#)

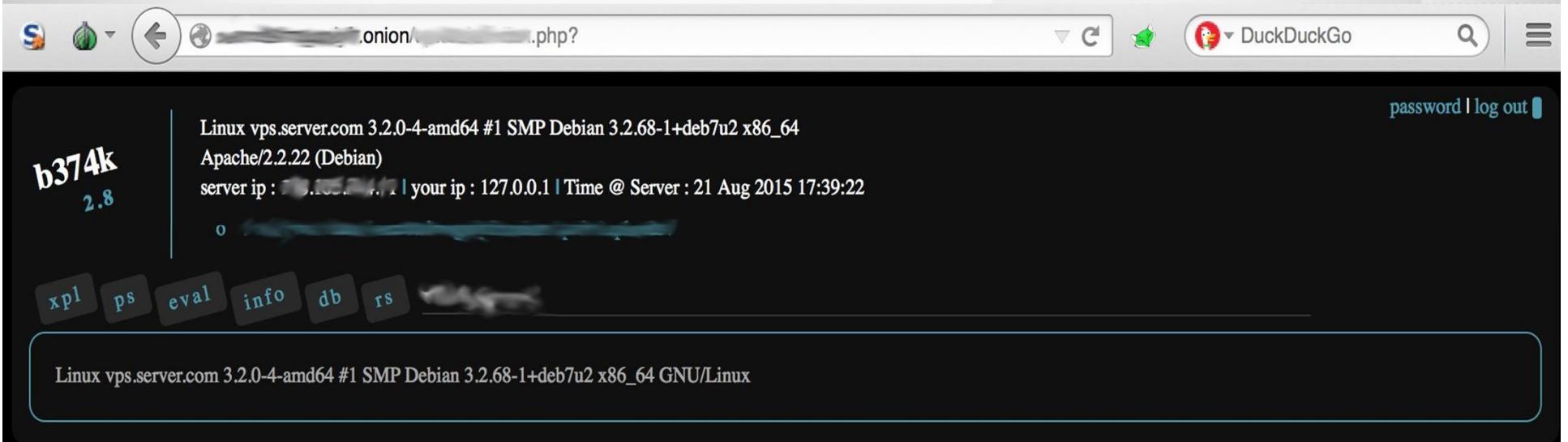
HTTP/1.1 301 Moved Permanently
Date: Sun, 16 Aug 2015 11:42:31 GMT
Server: Apache
Location: http://[REDACTED].onion/
Content-Length: 10
Content-Type: text/html; charset=iso-8859-1



OWASP
Open Web Application
Security Project

General appsec

- Nothing really new
- Access to the server (SQLi, command injection, upload restrictions bypass and so on) → ~~privacy~~



A screenshot of a web browser window. The address bar shows an onion URL: [http://\[REDACTED\].onion/\[REDACTED\].php?](http://[REDACTED].onion/[REDACTED].php?). The browser interface includes standard buttons for back, forward, and search. The main content area displays a terminal-like interface with a dark background and light text. On the left, there is a sidebar with the text "b374k" and "2.8". The main terminal area shows system information: "Linux vps.server.com 3.2.0-4-amd64 #1 SMP Debian 3.2.68-1+deb7u2 x86_64" and "Apache/2.2.22 (Debian)". It also displays the server's IP and the user's IP as "127.0.0.1". The timestamp "Time @ Server : 21 Aug 2015 17:39:22" is shown. Below the terminal, there are several small, rounded buttons with labels: "xpl", "ps", "eval", "info", "db", and "rs". At the bottom of the terminal area, there is a message: "Linux vps.server.com 3.2.0-4-amd64 #1 SMP Debian 3.2.68-1+deb7u2 x86_64 GNU/Linux".

password | log out

b374k 2.8

Linux vps.server.com 3.2.0-4-amd64 #1 SMP Debian 3.2.68-1+deb7u2 x86_64
Apache/2.2.22 (Debian)
server ip : [REDACTED] | your ip : 127.0.0.1 | Time @ Server : 21 Aug 2015 17:39:22

xpl ps eval info db rs

Linux vps.server.com 3.2.0-4-amd64 #1 SMP Debian 3.2.68-1+deb7u2 x86_64 GNU/Linux

 OWASP
Open Web Application
Security Project

Special word for /server-status

- 7% of the known darkweb (~500 out of 7000)

Hostname	[REDACTED] 0
Uptime	26 days 13 hours 10 min 8 s
Started at	2015-08-23 23:37:11
	absolute (since start)
Requests	21 Mreq
Traffic	2.04 Tbyte

Restart Time: Thursday, 01-Jan-2004 17:36:36 CET

Parent Server Generation: 3

Server uptime: 4266 days 2 hours 43 minutes 58 seconds

Total accesses: 32534 - Total Traffic: 731.1 MB



OWASP
Open Web Application
Security Project

Special word for /server-status

127.0.1.1:80 NULL

127.0.1.1:80 GET /index.php?q=Mushroom+kingdom&session=536976303&numRo

127.0.1.1:80 GET /server-status HTTP/1.1

actual misconfiguration

not Evil

127.0.1.1:80 OPTIONS * HTTP/1.0

127.0.1.1:80 GET /r.php?url=http%3A%2F%2Fwikipedia.onion%2F&q=necro

127.0.1.1:80 OPTIONS * HTTP/1.0

127.0.1.1:80 GET /r.php?url=http%3A%2F%2Fimagehosting.onion%2F&q=12y

Variant of Dark Google



OWASP
Open Web Application
Security Project

Special word for /server-status

- “About 2% of the known darknet is controlled by one organization” \approx 350 out of 7000
- Would you really trust your identity to someone else?
- ... especially if it might be (IS) vulnerable? ☺

Special word for /server-status

- "It works!"/"Forbidden" on your IP address access?
- Bots/scanners → full GET-request along real IP-address
- If "deanonymizer" accesses it, it will be reflected too!
 - Zmap / Masscan / your variant of global scanner
 - Access <http://xxx.XXX.XXX.XXX/xxx.XXX.XXX.XXX.XXX>
 - Monitor



Special word for /server-status

- Clients of such services might be vulnerable even if no clearnet accesses were made! (if no real IP addresses were logged)
- Example: poor auth scheme with "key" as a unique identifier

```
127.0.0.1 apple.onion:8082    GET /?page_id=6&order-received=520&key=wc_order_1
```

- Guess what happens next.



OWASP
Open Web Application
Security Project

Special word for /server-status

ftec[REDACTED].onion/?page_id=6&order-received=520&key=wc_order[REDACTED]

Payment Method: Bitcoin Payment

Please send your bitcoin payment as follows:

Amount (BTC): **1.03367790**

Address: **1MMUUAUXE7C8ehSMqnuMtG3[REDACTED]**

QR Code: 

Please note:

1. You must make a payment within 1 hour, or your order will be cancelled
2. As soon as your payment is received in full you will receive email confirmation with order delivery details.
3. You may send payments from multiple accounts to reach the total required.

Order Details

PRODUCT	TOTAL
iPhone 6 Plus Gold 64 GB × 1	\$474.99
SUBTOTAL:	\$474.99 (ex. tax)
SHIPPING:	\$25.00 via International Delivery
PAYMENT METHOD:	Bitcoin Payment
TOTAL:	\$499.99

Customer Details

EMAIL:	[REDACTED]@gmail.com
TELEPHONE:	048[REDACTED]

BILLING ADDRESS

Michael [REDACTED]
[REDACTED]
75009 PARIS
France



OWASP
Open Web Application
Security Project

CONNECT. LEARN. GROW.

Some better examples?



OWASP
Open Web Application
Security Project



Your riseup.net email account is a wonderful thing. Although we don't provide as much storage quota as surveillance-funded corporate email providers, riseup.net email has many unusual features: <...> we do not log internet addresses of anyone using riseup.net services, including email.

- <http://nzh3fv6jc6jskki3.onion/server-status> - help.* , lyre.* , riseup.net
- <http://cwoiopiifrlzcuos.onion/server-status> - black.* , api.black.*
- <http://zsolxunfmbfuq7wf.onion/server-status> - cotinga.* , mail.*
- <http://yfm6sdhnbulp1sw.onion/server-status> - labs.* , bugs.otr.im*
- <http://xpgylzydxykgdqyg.onion/server-status> - lists.* , whimbrel.*
- <http://j6uhdvbhz74oefxf.onion/server-status> - user.*
- <http://7lvd7fa5yfbdqaii.onion/server-status> - we.*

On darknet since 2012



OWASP
Open Web Application
Security Project



Riseup has three types of accounts sorted by security level: **GREEN** (lists, wiki), **RED** (email, shell, OpenVPN) and **BLACK** (Bitmask enhanced security). In this section I will concentrate on red and black accounts, since green ones do not seem to have that much importance in terms of privacy.

RED : currently logged in user, and his actions

user.riseup.net

POST /user/settings/jvl  HTTP/1.1



OWASP
Open Web Application
Security Project



BLACK: correlation between real user login and his unique hash ID, which is used later to anonymize all the activities he makes

127.0.0.1	api.black.riseup.net	GET /users/ <u>677f7ad7b5849c7f28e32259876746ce</u> HTTP/1.1
127.0.0.1	api.black.riseup.net	POST /1/sessions.json HTTP/1.1
127.0.0.1	cwoiopiifrlzcuos.onion	GET /server-status HTTP/1.1
127.0.0.1	api.black.riseup.net	PUT /1/sessions/c0rdis.json HTTP/1.1





RED : remote IP address of the current user, his actions and address book contacts

CONNECT LEARN GROW

127.0.0.1	mail.riseup.net:443	GET /rc/skins/larry/images/listicons.png?v=1877.13442 HTTP/1.1
127.0.0.1	mail.riseup.net:443	GET /rc/program/js/common.min.js?s=1433508438 HTTP/1.1
127.0.0.1	mail.riseup.net:443	NULL
127.0.0.1	mail.riseup.net:443	POST /rc/?_task=mail&_action=refresh HTTP/1.1
127.0.0.1	mail.riseup.net:443	GET /rc/?_task=addressbook&_action=photo&_email=joha%40riseup.n
127.0.0.1	mail.riseup.net:443	NULL
127.0.0.1	mail.riseup.net:443	NULL
209.████████.105		
127.0.0.1	mail.riseup.net:443	NULL
127.0.0.1	mail.riseup.net:443	POST /rc/?_task=mail&_action=refresh HTTP/1.1
127.0.0.1	mail.riseup.net:443	POST /rc/?_task=mail&_action=refresh HTTP/1.1
127.0.0.1	mail.riseup.net:443	POST /rc/?_task=settings&_action=refresh HTTP/1.1
127.0.0.1	mail.riseup.net:443	POST /rc/?_task=mail&_action=refresh HTTP/1.1
77.████.152		



OWASP
Open Web Application
Security Project

Megafon

One of the largest Russian mobile operators. In this case, it was set of old subscription services along with WAP.

 6lp4oyooouop5zatu.onion/server-status

Apache Server Status for 6lp4oyooouop5zatu.onion

Server Version: Apache/2.2.15 (Unix) DAV/2 mod_ssl/2.2.15 OpenSSL/1.0.0-fips

Server Built: Apr 29 2013 04:13:12

Current Time: Thursday, 17-Sep-2015 00:25:13 MSK

Restart Time: Tuesday, 01-Sep-2015 12:42:42 MSK

Parent Server Generation: 0

Server uptime: 15 days 11 hours 42 minutes 30 seconds

Total accesses: 300902578 - Total Traffic: 1386.4 GB

CPU Usage: u764.28 s444.21 cu10.33 cs0 - .0911% CPU load

225 requests/sec - 1.1 MB/second - 4947 B/request

277 requests currently being processed, 58 idle workers



OWASP
Open Web Application
Security Project

Megafon

General user activity with phone numbers

General user activity with phone numbers						
Index	MSISDN	Count	Time	IP	Request	Method
8	1279	0	0.0	0.60	1792.87 ?	?
5	555	0	0.0	2.62	1604.91 ?	wap.megafonpro.ru GET /is3nwp/servicing/historynew.jsp?m=2&msisdn=7920
5	1017	121	0.0	2.07	1516.14 ?	?
6	514	0	0.0	4.02	1638.38 ?	?
8	15	139	0.0	1.71	1618.18 ?	?
1	1	0	0.0	0.61	1507.09 ?	?
1	0	6	2.6	0.59	1543.58 ?	wap.megafonpro.ru GET /is3nwp/psmcaptcha?captcha=q49iGNZIN33S&psmsid=.01&ctype=0
0	560	0	0.0	5.10	1571.16 ?	wap.megafonpro.ru GET /is3nwp/servicing/historynew.jsp?m=2&msisdn=7920
1	2	6	0.0	0.05	1900.58 ?	?
0	0	26	0.0	0.04	1593.87 ?	podpiskipro.ru GET /is3nwp/psm/auth?service_id=2251&return_url=mds4%2Fpartner%
3	1126	0	0.0	1.87	1856.69 ?	?
6	2	3	0.0	0.28	1542.16 ?	?
2	0	0	2.2	0.17	1568.04 ?	wap.megafonpro.ru GET /is3nwp/tpl_content/ic_ero_lust_net_100r_5d_qv_WAP_1/player
7	16	0	0.0	6.52	1529.98 ?	?
4	27	26	0.0	0.68	1763.10 ?	?
9	156	0	0.0	4.42	1541.46 ?	?
1	561	0	0.0	0.67	1497.73 ?	wap.megafonpro.ru GET /is3nwp/servicing/historynew.jsp?m=2&msisdn=7920
1	1368	20	0.0	5.64	1685.96 ?	?
8	3	0	0.0	1.47	1548.73 ?	?
6	490	0	0.0	0.79	1597.36 ?	?
2	8	5	0.0	1.41	1511.18 ?	?
3	0	23	0.0	3.07	1509.90 ?	podpiskipro.ru GET /is3nwp/psm/auth?service_id=2251&return_url=mds4%2Fpartner%



OWASP
Open Web Application
Security Project

Megafon

Admin credentials to vulnerable services

0	4	0.0	2.14	644.05	46.47.██████	iclickpro.ru	GET /is3nwp/psm/profile?login=████████&password=████████&service_i
444	3	0.0	0.00	661.53	46.47.██████	iclickpro.ru	GET /is3nwp/psm/allprofiles?login=████████&password=████████&m

Disclaimer: admin credentials were not used by me to break into the system, however, log analysis has shown that further attack on other Megafon systems is very likely from there.



OWASP
Open Web Application
Security Project

Several more examples...



CRYPTO
COPARTY

CRYPTO.JS
A CYPHERPUNK PROJECT

CYPHER
PUNKS

SWISS PRIVACY
FOUNDATION

OWASP
Open Web Application
Security Project

Something is wrong here...



OWASP
Open Web Application
Security Project

Zen



Default state of status.conf:

```
<Location /server-status>
  SetHandler server-status
  Order deny,allow
  Deny from all
  Allow from 127.0.0.1 ::1
  #Allow from
  192.0.2.0/24
</Location>
```

Local attacker

Hi, [@ircmaxell!](#)



CONNECT LEARN GROW

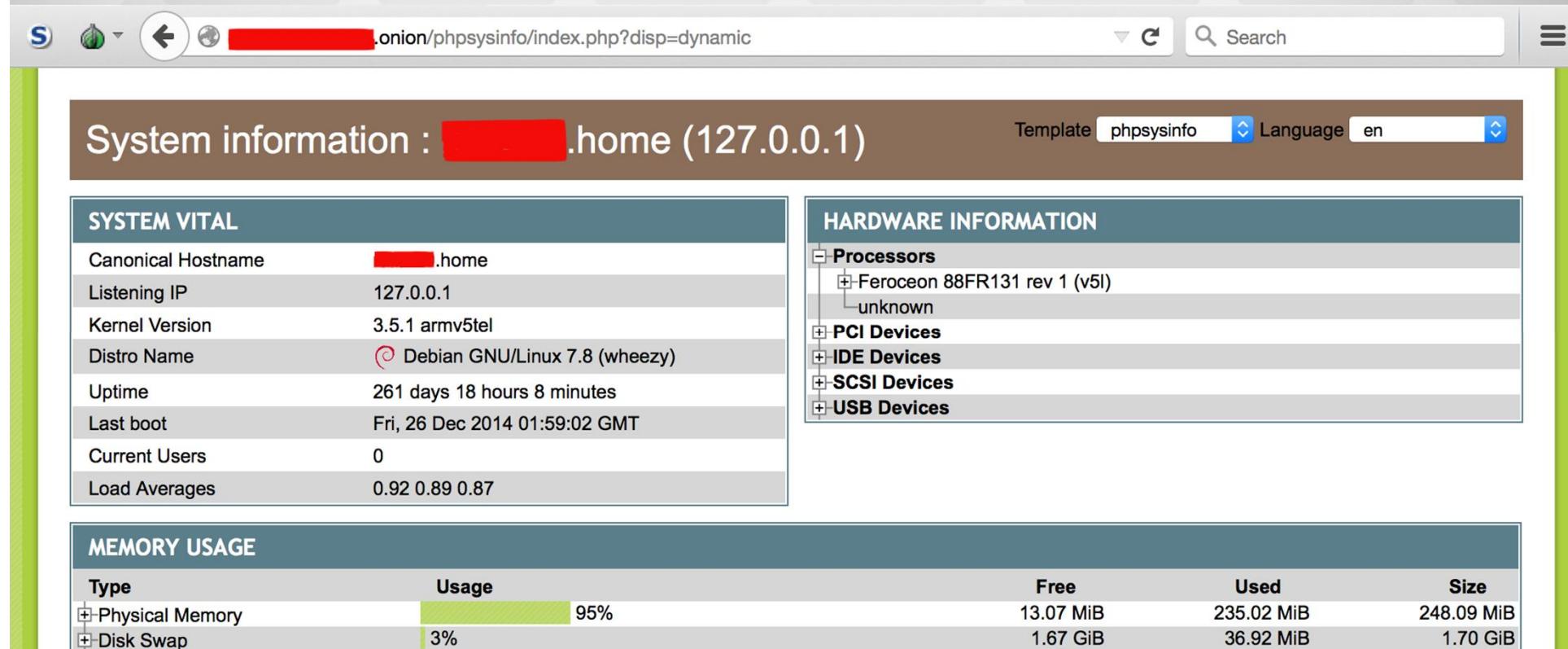
... this new menu item was named "Admin". Curious, I clicked the link, figuring I'd be immediately denied access. What happened next surprised me. Not only was I not denied access, but I was granted full access to everything. I had the developer console to see what people were doing. I had a database query interface where I could directly query any database that I wanted. I had admin access to chat"

X-Forwarded-For by default!!!



OWASP
Open Web Application
Security Project

Trust model seems to be overlooked...



System information : [REDACTED].home (127.0.0.1) Template phpsysinfo Language en

SYSTEM VITAL	
Canonical Hostname	[REDACTED].home
Listening IP	127.0.0.1
Kernel Version	3.5.1 armv5tel
Distro Name	Debian GNU/Linux 7.8 (wheezy)
Uptime	261 days 18 hours 8 minutes
Last boot	Fri, 26 Dec 2014 01:59:02 GMT
Current Users	0
Load Averages	0.92 0.89 0.87

MEMORY USAGE				
Type	Usage	Free	Used	Size
+ Physical Memory	95%	13.07 MiB	235.02 MiB	248.09 MiB
+ Disk Swap	3%	1.67 GiB	36.92 MiB	1.70 GiB

HARDWARE INFORMATION

- Processors
 - + Feroceon 88FR131 rev 1 (v5l)
 - unknown
- + PCI Devices
- + IDE Devices
- + SCSI Devices
- + USB Devices

„Home, sweet home“

Local attacker

It's not just about auth bypass!

- PHPSESSID is generated based on remote IP address
 $\text{hash}(\text{client IP} . \text{timestamp} . \text{microseconds1} . \text{php_combined_lcg}())$
- Flood detection
- Brute force / lockouts
- Any other security measure based on IP address

Fin



hlofftnkkom7l2t4.onion/server-status

Search

0	K	0.87	9	0	0.3	0.01	365.03	176.██████████	check.torproject.org	GET /?TorButton=true	HTTP/1.1
5	K	0.73	12	0	0.3	0.00	351.09	93.██████████	check.torproject.org	GET /?TorButton=true	HTTP/1.1
5	K	1.14	1	0	0.3	0.00	350.05	89.██████████	check.torproject.org	GET /?TorButton=true	HTTP/1.1
0	_	1.16	0	2	0.0	0.02	369.44	77.██████████	check.torproject.org	GET /	HTTP/1.1
2	K	0.69	14	0	1.1	0.01	364.62	77.██████████	check.torproject.org	GET /favicon.ico	HTTP/1.1
3	K	1.10	2	0	0.3	0.00	376.06	171.██████████	check.torproject.org	GET /?TorButton=true	HTTP/1.1
0	K	0.78	11	0	0.3	0.00	350.54	171.██████████	check.torproject.org	GET /?TorButton=true	HTTP/1.1
1	K	0.77	12	0	0.3	0.00	369.29	109.██████████	check.torproject.org	GET /?TorButton=true	HTTP/1.1
0	K	1.15	0	0	0.3	0.18	355.29	185.██████████	check.torproject.org	GET /?TorButton=true	HTTP/1.1
2	K	0.79	11	0	12.4	0.01	343.88	185.██████████	check.torproject.org	GET /torcheck/img/tor-not.png	HTTP/1.1
3	K	0.70	14	0	0.1	0.00	356.42	176.██████████	check.torproject.org	GET /RecommendedTBBVersions	HTTP/1.1
1	K	0.89	8	0	0.3	0.01	358.68	112.██████████	check.torproject.org	GET /	HTTP/1.1
5	K	0.74	12	0	0.3	0.00	345.91	91.██████████	check.torproject.org	GET /?TorButton=true	HTTP/1.1
5	K	0.79	11	0	0.3	0.00	345.01	209.1.██████████	check.torproject.org	GET /?TorButton=true	HTTP/1.1
0	K	1.16	0	0	20.9	0.02	377.14	127.0.0.1	sergii.torproject.org	GET /TRUST_ME_I_M_LOCALHOST	HTTP/1.1
1	K	0.99	5	0	0.1	0.16	354.02	80.██████████	check.torproject.org	GET /RecommendedTBBVersions	HTTP/1.1
3	K	0.96	5	0	0.3	0.06	359.59	37.██████████	check.torproject.org	GET /?TorButton=true	HTTP/1.1



OWASP
Open Web Application
Security Project