OWASP

Open Web Application Security Project

# #DontTrustTheDarkSide

@c0rdis

OWASP EEE - Bucharest

# Whoami

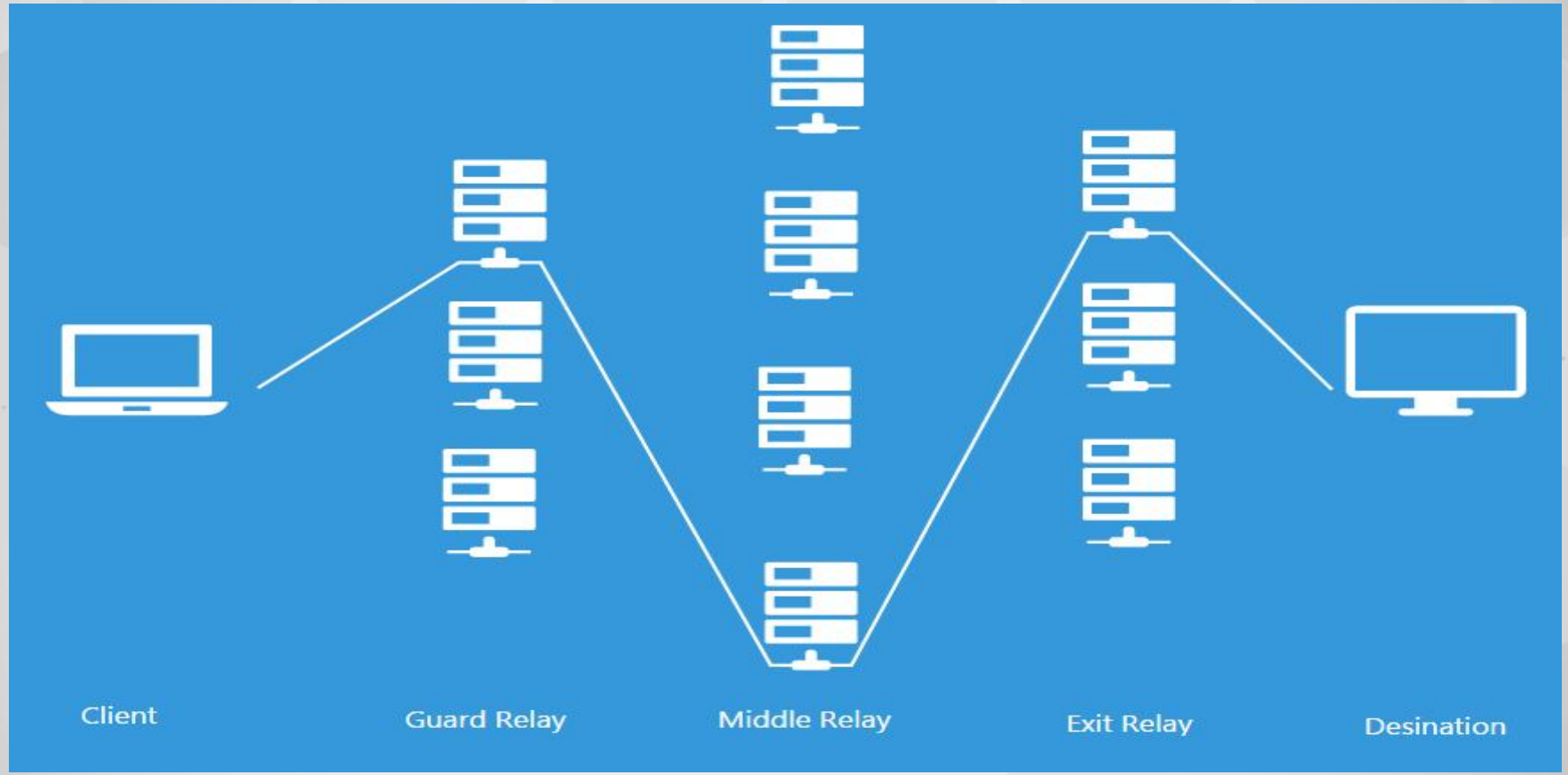
*Luke Skywalker in EY*

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

# 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

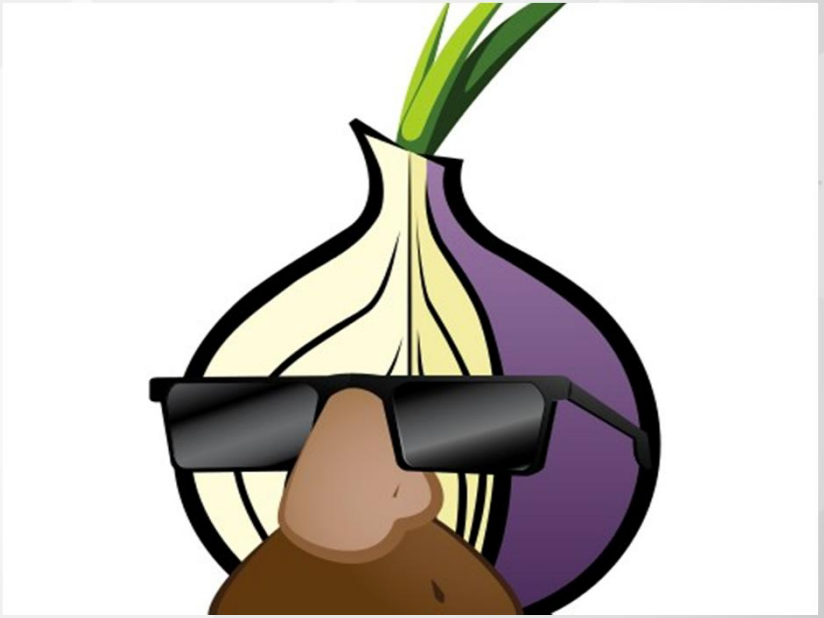
„… unfortunately for thrill-seekers, almost all the sites purporting to offer this type of content far have turned out to be fake, be that live streams of torture, hitmen for hire, or human trafficking.

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

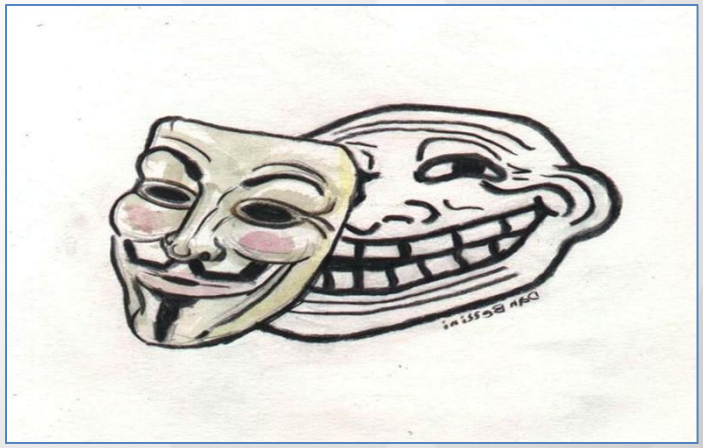
# Some known darknet attacks

- 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

# How it all started

# 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

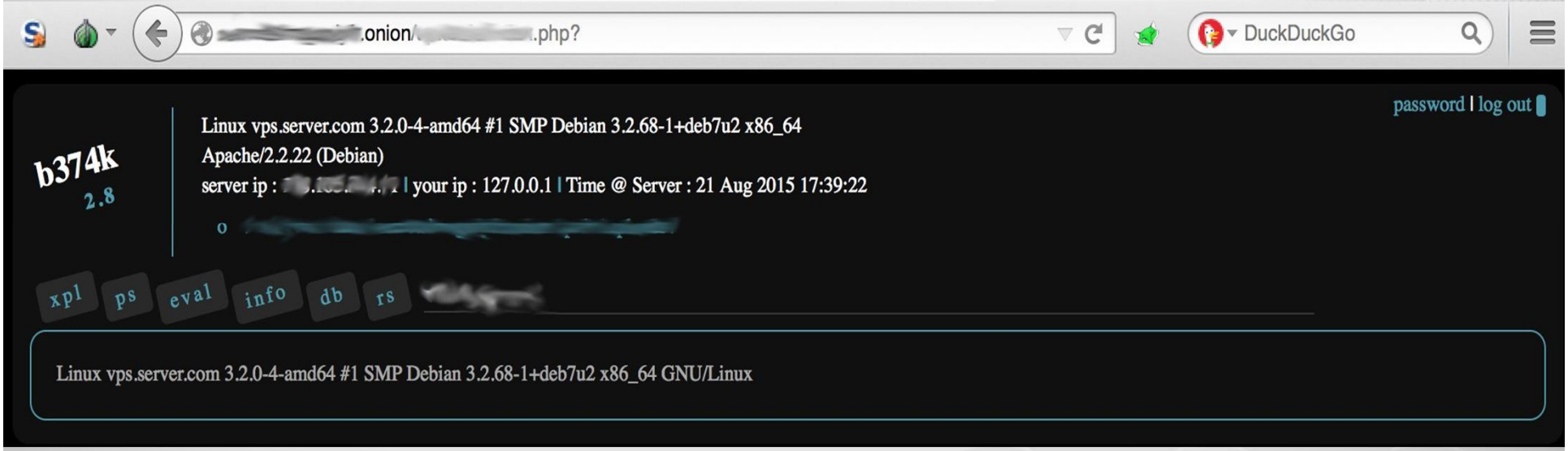
```
HTTP/1.1 302 Found
Date: Fri, 21 Aug 2015 16:30:32 GMT
Server: Apache/2.2.22 (Debian)
Location: http://[redacted].onion/index.html
Vary: Accept-Encoding
Content-Length: 224
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
```

# Shodan

- Lazy bastard way

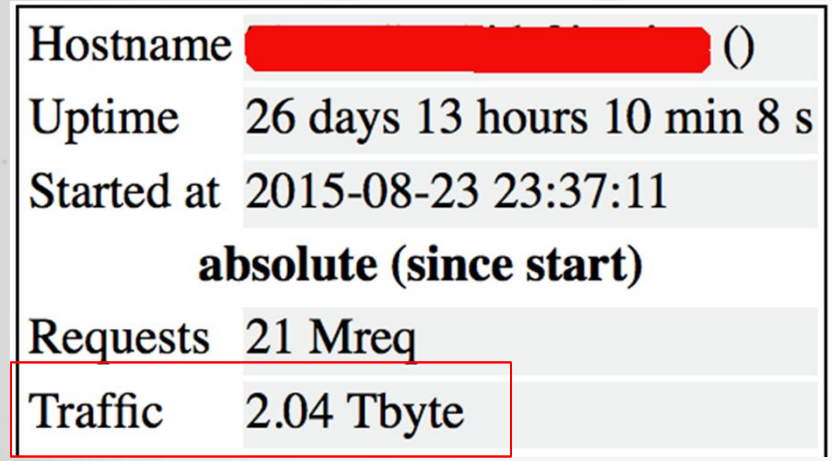
# General appsec

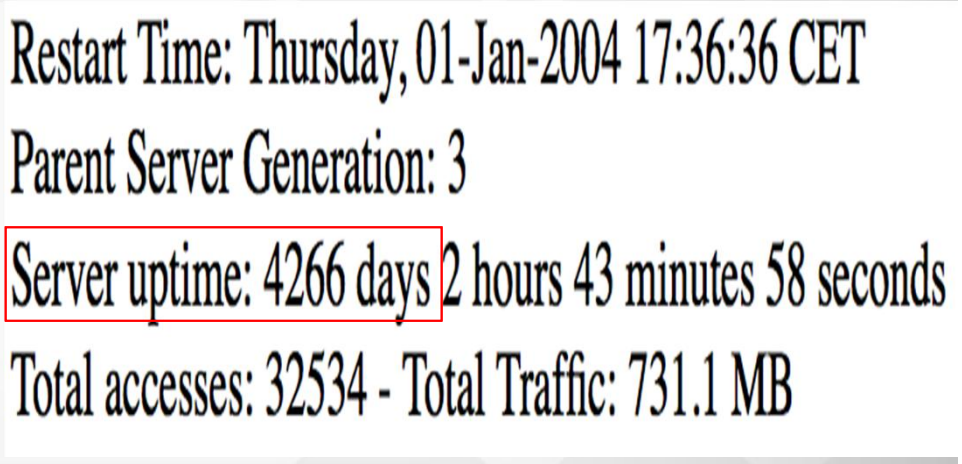
- Nothing really new
- Access to the server (SQLi, command injection, upload restrictions bypass and so on) → ~~privacy~~



# Special word for /server-status

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



# 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%2Fwikit[redacted].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%2Fimage[redacted].onion%2F&q=12y

*Variant of Dark Google*

# Special word for /server-status

- “About 2% of the known darknet is controlled by one organization” ≈ 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
  - Monitor

1 0 0.2 0.33 401.02 [redacted] vps.server.com GET /[redacted] HTTP/1.1

Your scanner's IP

Real hidden IP

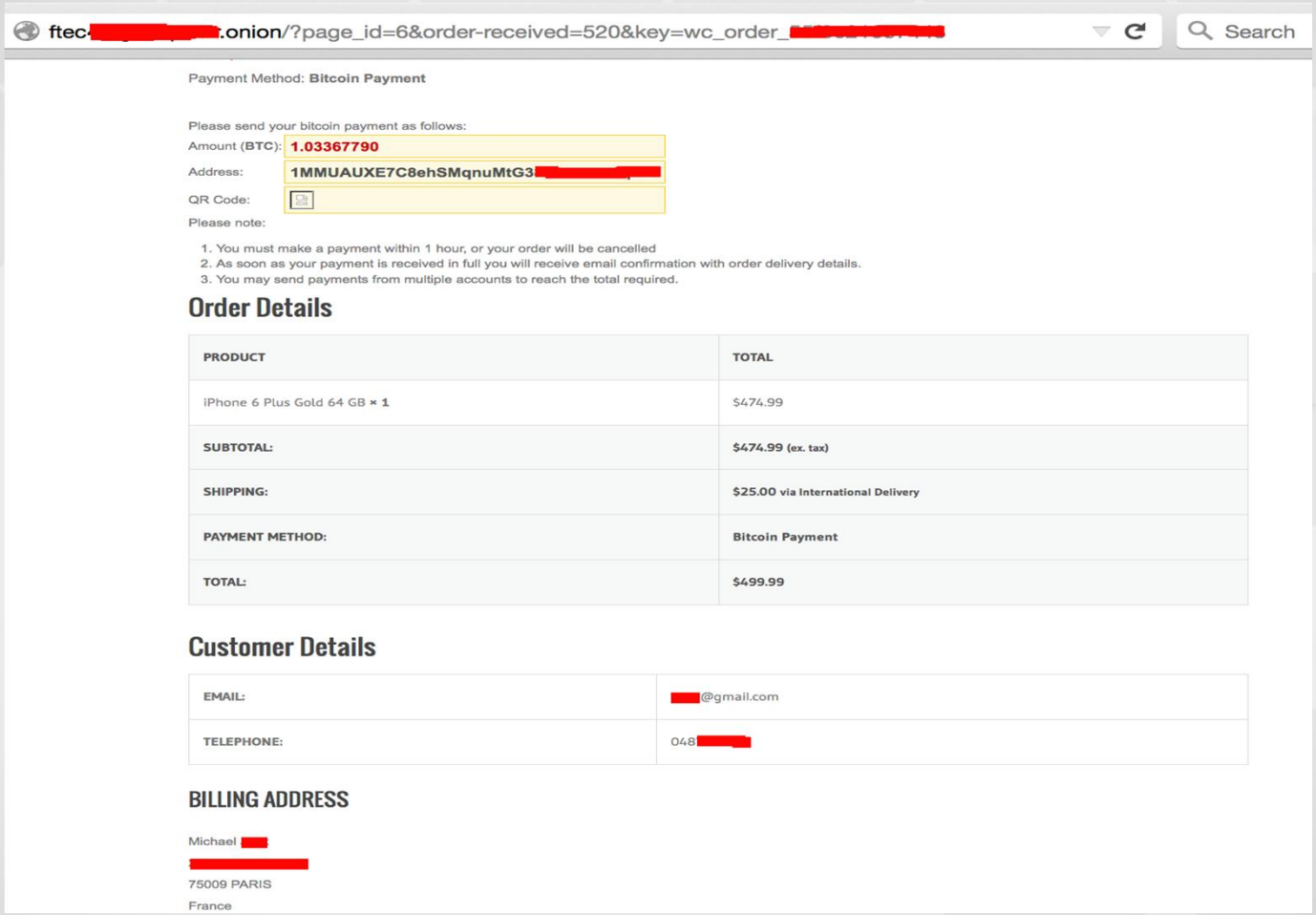
# Special word for /server-status

- 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_[redacted]

- Guess what happens next.

# Special word for /server-status



# Some better examples?

riseup.net

*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://yfm6sdhnfbulplsw.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


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[redacted] HTTP/1.1


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

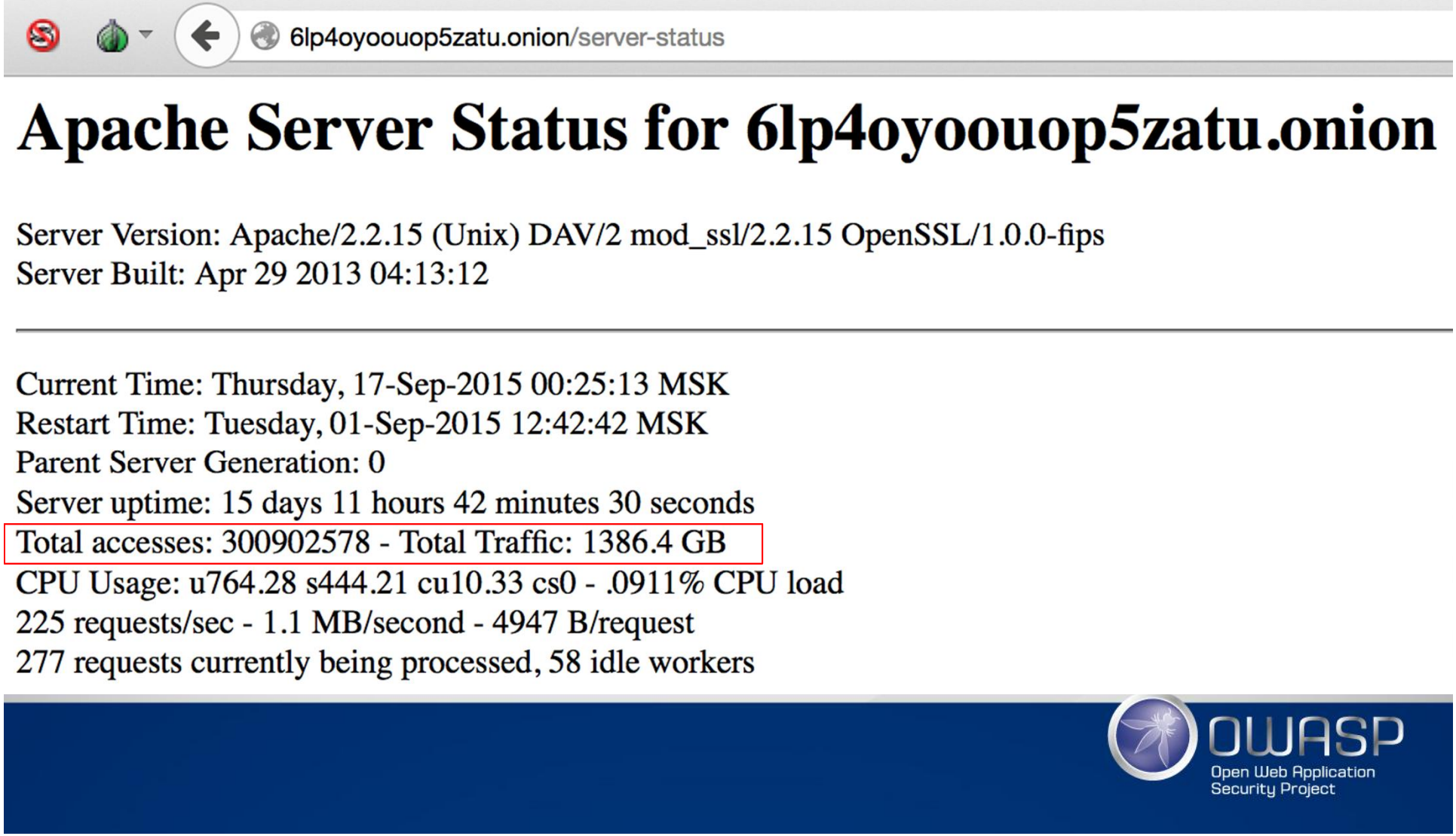
```
127.0.0.1 api.black.riseup.net      GET /users/677f7ad7b5849c7f28e32259876746ce HTTP/1.1
127.0.0.1 api.black.riseup.net      POST /1/sessions.json HTTP/1.1
127.0.0.1 cwoiopiifrlzcuos.onion GET /server-status HTTP/1.1
127.0.0.1 api.black.riseup.net      PUT /1/sessions/c0rdis.json HTTP/1.1
```


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

| | | |
|---|---|---|
| 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.[redacted].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.[redacted].152 | | |

# Megafon

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



# Megafon

General user activity with phone numbers

6lp4oyoouop5zatu.onion/server-status

Search

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 8 | 1279 | 0 | 0.0 | 0.60 | 1792.87 | ? | ? | ..reading.. |
| 5 | 555 | 0 | 0.0 | 2.62 | 1604.91 | [redacted] | wap.megafonpro.ru | GET /is3nwp/servicing/historynew.jsp?m=2&msisdn=7920[redacted] HTT |
| 5 | 1017 | 121 | 0.0 | 2.07 | 1516.14 | ? | ? | ..reading.. |
| 6 | 514 | 0 | 0.0 | 4.02 | 1638.38 | ? | ? | ..reading.. |
| 8 | 15 | 139 | 0.0 | 1.71 | 1618.18 | ? | ? | ..reading.. |
| 1 | 1 | 0 | 0.0 | 0.61 | 1507.09 | ? | ? | ..reading.. |
| 1 | 0 | 6 | 2.6 | 0.59 | 1543.58 | [redacted] | wap.megafonpro.ru | GET /is3nwp/psmcaptcha?captcha=q49iGNZIN33S&psmsid=.01&ctype=0 |
| 0 | 560 | 0 | 0.0 | 5.10 | 1571.16 | [redacted] | wap.megafonpro.ru | GET /is3nwp/servicing/historynew.jsp?m=2&msisdn=7920[redacted] HTT |
| 1 | 2 | 6 | 0.0 | 0.05 | 1900.58 | ? | ? | ..reading.. |
| 0 | 0 | 26 | 0.0 | 0.04 | 1593.87 | [redacted] | podpiskipro.ru | GET /is3nwp/psm/auth?service_id=2251&return_url=mds4%2Fpartner% |
| 3 | 1126 | 0 | 0.0 | 1.87 | 1856.69 | ? | ? | ..reading.. |
| 6 | 2 | 3 | 0.0 | 0.28 | 1542.16 | ? | ? | ..reading.. |
| 2 | 0 | 0 | 2.2 | 0.17 | 1568.04 | [redacted] | 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 | ? | ? | ..reading.. |
| 4 | 27 | 26 | 0.0 | 0.68 | 1763.10 | ? | ? | ..reading.. |
| 9 | 156 | 0 | 0.0 | 4.42 | 1541.46 | ? | ? | ..reading.. |
| 1 | 561 | 0 | 0.0 | 0.67 | 1497.73 | [redacted] | wap.megafonpro.ru | GET /is3nwp/servicing/historynew.jsp?m=2&msisdn=7920[redacted] HTT |
| 1 | 1368 | 20 | 0.0 | 5.64 | 1685.96 | ? | ? | ..reading.. |
| 8 | 3 | 0 | 0.0 | 1.47 | 1548.73 | ? | ? | ..reading.. |
| 6 | 490 | 0 | 0.0 | 0.79 | 1597.36 | ? | ? | ..reading.. |
| 2 | 8 | 5 | 0.0 | 1.41 | 1511.18 | ? | ? | ..reading.. |
| 3 | 0 | 23 | 0.0 | 3.07 | 1509.90 | [redacted] | podpiskipro.ru | GET /is3nwp/psm/auth?service_id=2251&return_url=mds4%2Fpartner% |

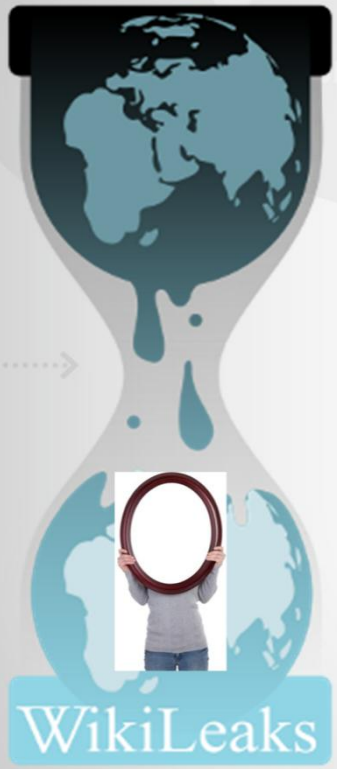
# Megafon

Admin credentials to vulnerable services

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 4 | 0.0 | 2.14 | 644.05 | 46.47.[redacted] | iclickpro.ru | GET /is3nwp/psm/profile?login=mc[redacted]&password=[redacted]&service_i |
| 444 | 3 | 0.0 | 0.00 | 661.53 | 46.47.[redacted] | iclickpro.ru | GET /is3nwp/psm/allprofiles?login=pl[redacted]&password=[redacted]&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.*

# Several more examples…




CRYPTO PARTY

CRYPTO.IS
A CYPHERPUNK PROJECT

CYPHER PUNKS

SWISS PRIVACY FOUNDATION

# Something is wrong here...

# 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>
```

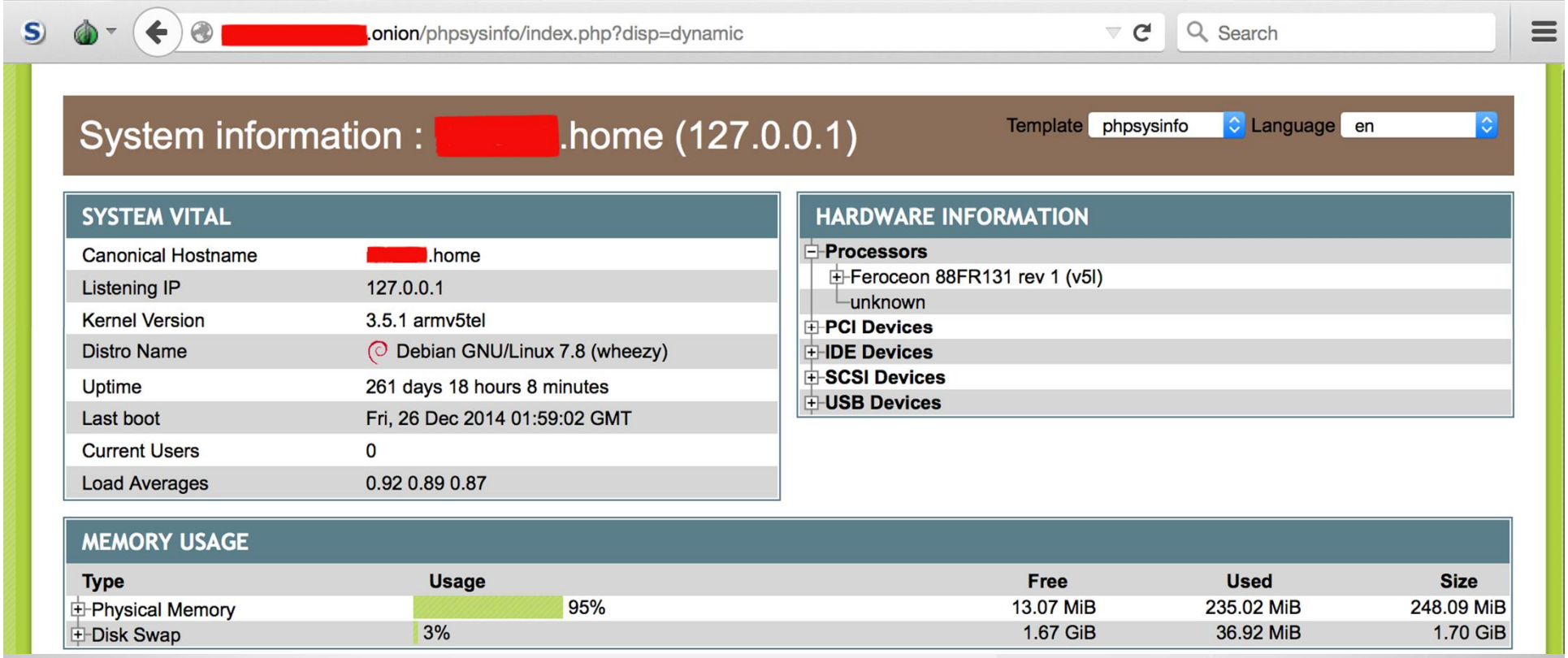
# Local attacker

Hi, @ircmaxell!


*"... 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!!!**

# Trust model seems to be overlooked…




*„Home, sweet home"*

# Local attacker

## It’s not just about auth bypass!

- PHPSESSID is generated based on remote IP address

*hash( client IP . timestamp . microseconds1 . php_combined_lcg() )*

- Flood detection
- Brute force / lockouts
- Any other security measure based on IP address

# Fin

hlofftnkkom7l2t4.onion/server-status

Search

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ) | K | 0.87 | 9 | 0 | 0.3 | 0.01 | 365.03 | 176.[redacted] | check.torproject.org GET /?TorButton=true HTTP/1.1 |
| 5 | K | 0.73 | 12 | 0 | 0.3 | 0.00 | 351.09 | 93.[redacted] | check.torproject.org GET /?TorButton=true HTTP/1.1 |
| 5 | K | 1.14 | 1 | 0 | 0.3 | 0.00 | 350.05 | 89.[redacted] | check.torproject.org GET /?TorButton=true HTTP/1.1 |
| ) | _ | 1.16 | 0 | 2 | 0.0 | 0.02 | 369.44 | 77.[redacted] | check.torproject.org GET / HTTP/1.1 |
| 2 | K | 0.69 | 14 | 0 | 1.1 | 0.01 | 364.62 | 77.[redacted] | check.torproject.org GET /favicon.ico HTTP/1.1 |
| 3 | K | 1.10 | 2 | 0 | 0.3 | 0.00 | 376.06 | 171.[redacted] | check.torproject.org GET /?TorButton=true HTTP/1.1 |
| ) | K | 0.78 | 11 | 0 | 0.3 | 0.00 | 350.54 | 171.[redacted] | check.torproject.org GET /?TorButton=true HTTP/1.1 |
| 1 | K | 0.77 | 12 | 0 | 0.3 | 0.00 | 369.29 | 109.[redacted] | check.torproject.org GET /?TorButton=true HTTP/1.1 |
| ) | K | 1.15 | 0 | 0 | 0.3 | 0.18 | 355.29 | 185.[redacted] | check.torproject.org GET /?TorButton=true HTTP/1.1 |
| 2 | K | 0.79 | 11 | 0 | 12.4 | 0.01 | 343.88 | 185.[redacted] | 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.[redacted] | check.torproject.org GET /RecommendedTBBVersions HTTP/1.1 |
| 4 | K | 0.89 | 8 | 0 | 0.3 | 0.01 | 358.68 | 112.[redacted] | check.torproject.org GET / HTTP/1.1 |
| 5 | K | 0.74 | 12 | 0 | 0.3 | 0.00 | 345.91 | 91.[redacted] | check.torproject.org GET /?TorButton=true HTTP/1.1 |
| 5 | K | 0.79 | 11 | 0 | 0.3 | 0.00 | 345.01 | 209.[redacted] | check.torproject.org GET /?TorButton=true HTTP/1.1 |
| ) | 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 |
| . | K | 0.99 | 5 | 0 | 0.1 | 0.16 | 354.02 | 80.[redacted] | check.torproject.org GET /RecommendedTBBVersions HTTP/1.1 |
| 3 | K | 0.96 | 5 | 0 | 0.3 | 0.06 | 359.59 | 37.[redacted] | check.torproject.org GET /?TorButton=true HTTP/1.1 |