CERN

Shouldn't we all be a bit more like Howard?

Why computing needs more of a structured engineering approach and less of "we-physicists-can-do-it-all".

(And yes, I am a physicist, too)
(If you're engineer, lucky you)

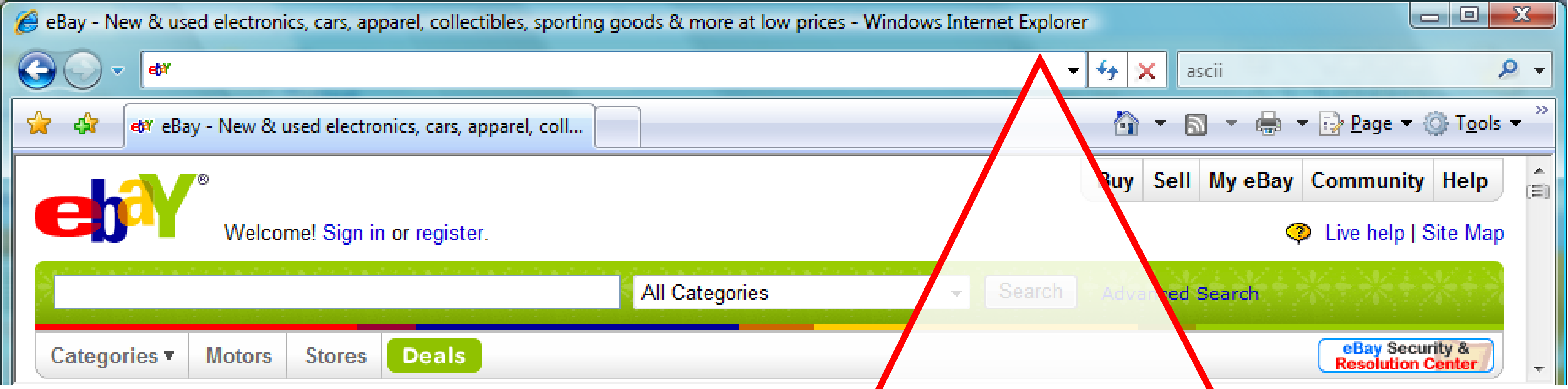
We are PHYSICIST

"May I point out that I do not have a tail and do not feel like being treated like a circus dog."

"Why there are idiotic policies in place to forbid use of certain technologies?"

"I fully recognise the importance of computer security at CERN. However, I am not sure that you have yet appreciated that computer security is not the raison d' être of CERN. Computer security must always be balanced with the need for CERN to carry out its experiments. I do not believe that [...] poses a strong security risk and you have not explained to us why it does."

"I failed to pass the security courses, the questions were so stupid, that sometimes it's difficult to answer. If you want to meet with me personally, I can teach you computer security."

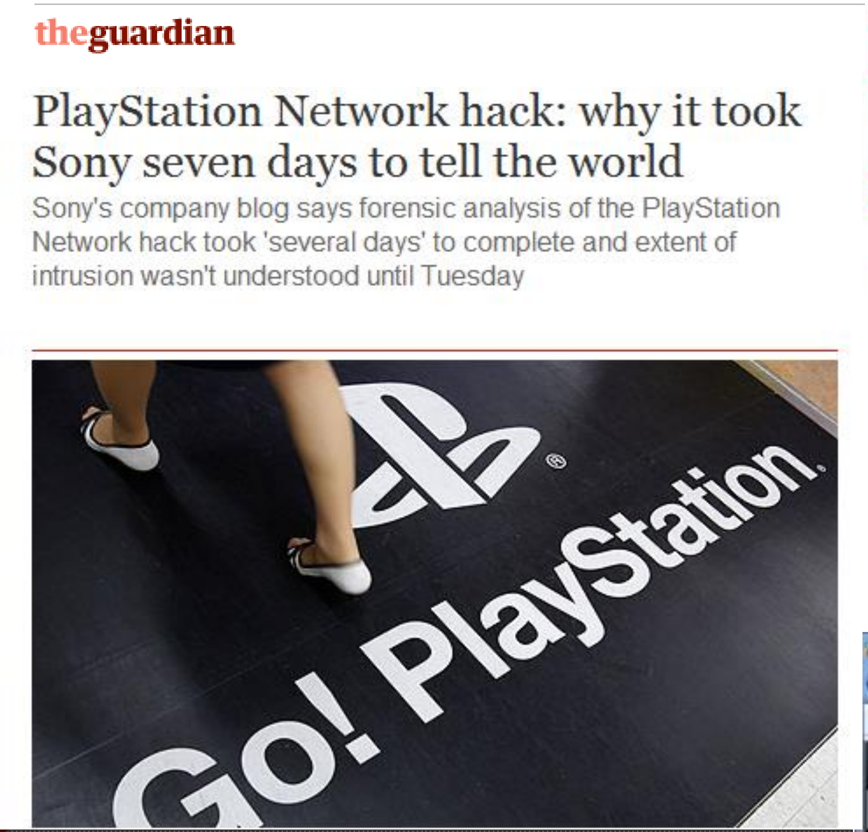

eBay - New & used electronics, cars, apparel, collectibles, sporting goods & more at low prices - Windows Internet Explorer
ascii
eBay - New & used electronics, cars, apparel, coll...
Page
Tools
Buy
Sell
My eBay
Community
Help
Welcome! Sign in or register.
Live help | Site Map
All Categories
Search
Advanced Search
Categories
Motors
Stores
Deals
eBay Security & Resolution Center

Quiz: Which URL leads you to www.ebay.com ?

- ✘ http://www.ebay.com\cgi-bin\login?ds=1%204324@%31%33%37%2e%31%33%38%2e%31%33%37%2e%31%37%37/p?uh3f223d
- ✘ http://www.ebay.com/ws/eBayISAPI.dll?SignIn
- ✓ http://scgi.ebay.com/ws/eBayISAPI.dll?RegisterEnterInfo&siteid=0&co_partnerid=2&usage=0&ru=http%3A%2F%2Fwww.ebay.com&rafId=0&encRafId=default
- ✘ http://secure-ebay.com

Attackers vs. DEFENSE

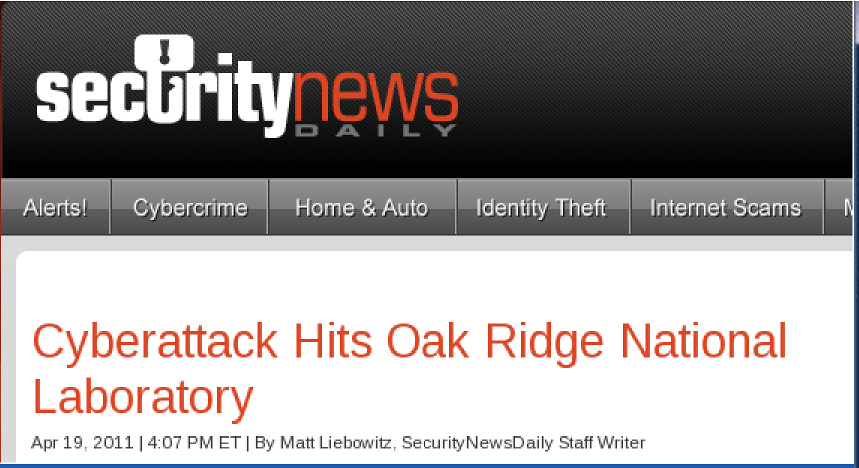
Defence is DIFFICULT!



theguardian

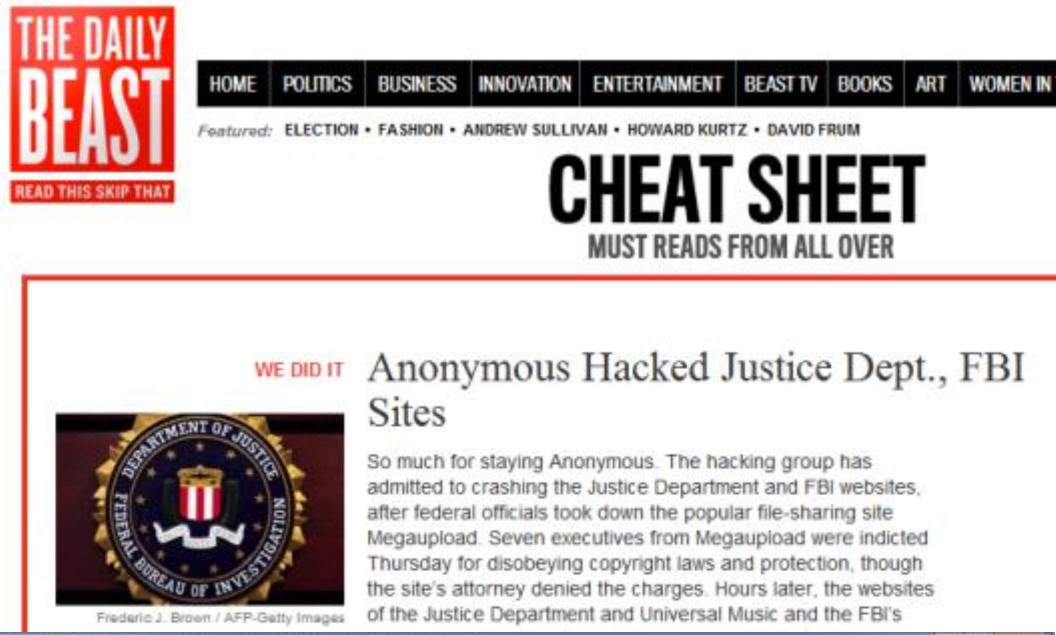
PlayStation Network hack: why it took Sony seven days to tell the world

Sony's company blog says forensic analysis of the PlayStation Network hack took 'several days' to complete and extent of intrusion wasn't understood until Tuesday



Cyberattack Hits Oak Ridge National Laboratory

Apr 19, 2011 | 4:07 PM ET | By Matt Liebowitz, SecurityNewsDaily Staff Writer

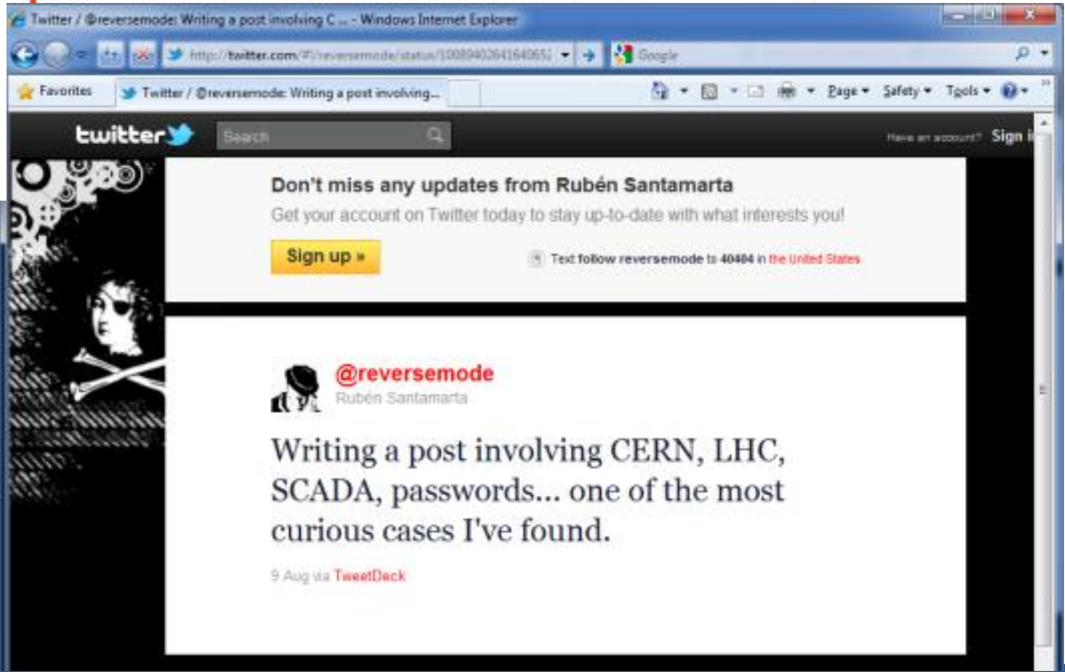


WE DID IT

Anonymous Hacked Justice Dept., FBI Sites

Frederic J. Brown / AFP-Getty Images

So much for staying Anonymous. The hacking group has admitted to crashing the Justice Department and FBI websites, after federal officials took down the popular file-sharing site Megaupload. Seven executives from Megaupload were indicted Thursday for disobeying copyright laws and protection, though the site's attorney denied the charges. Hours later, the websites of the Justice Department and Universal Music and the FBI's



Twitter / @reversemode: Writing a post involving C... - Windows Internet Explorer
Google
Favorites
Twitter / @reversemode: Writing a post involving...
Page
Safety
Tools
twitter
Search
Have an account?
Sign in
Sign up »

Don't miss any updates from Rubén Santamarta

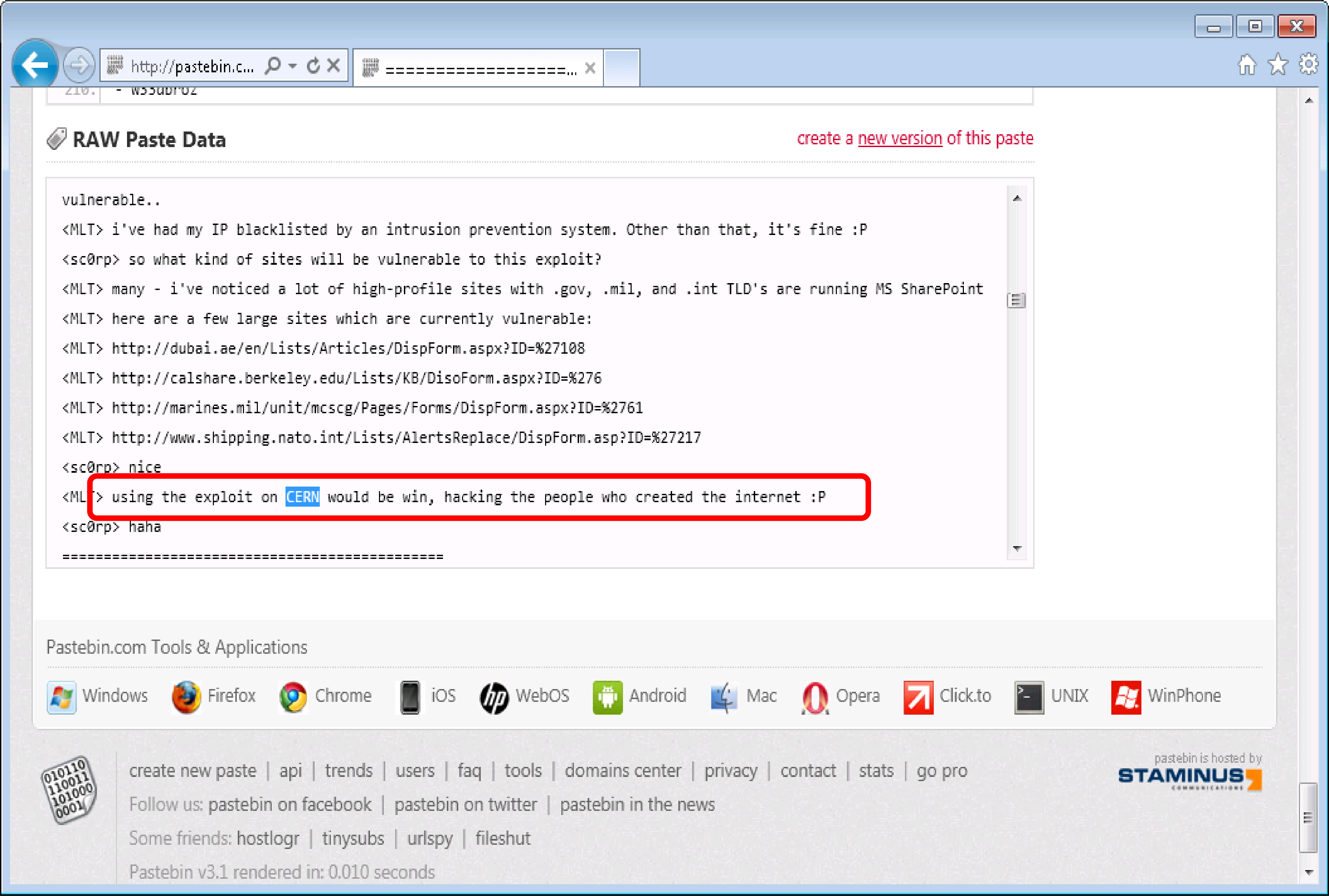
Get your account on Twitter today to stay up-to-date with what interests you!

Text follow reversemode to 40404 in the United States

@reversemode
Rubén Santamarta

Writing a post involving CERN, LHC, SCADA, passwords... one of the most curious cases I've found.

9 Aug via TweetDeck

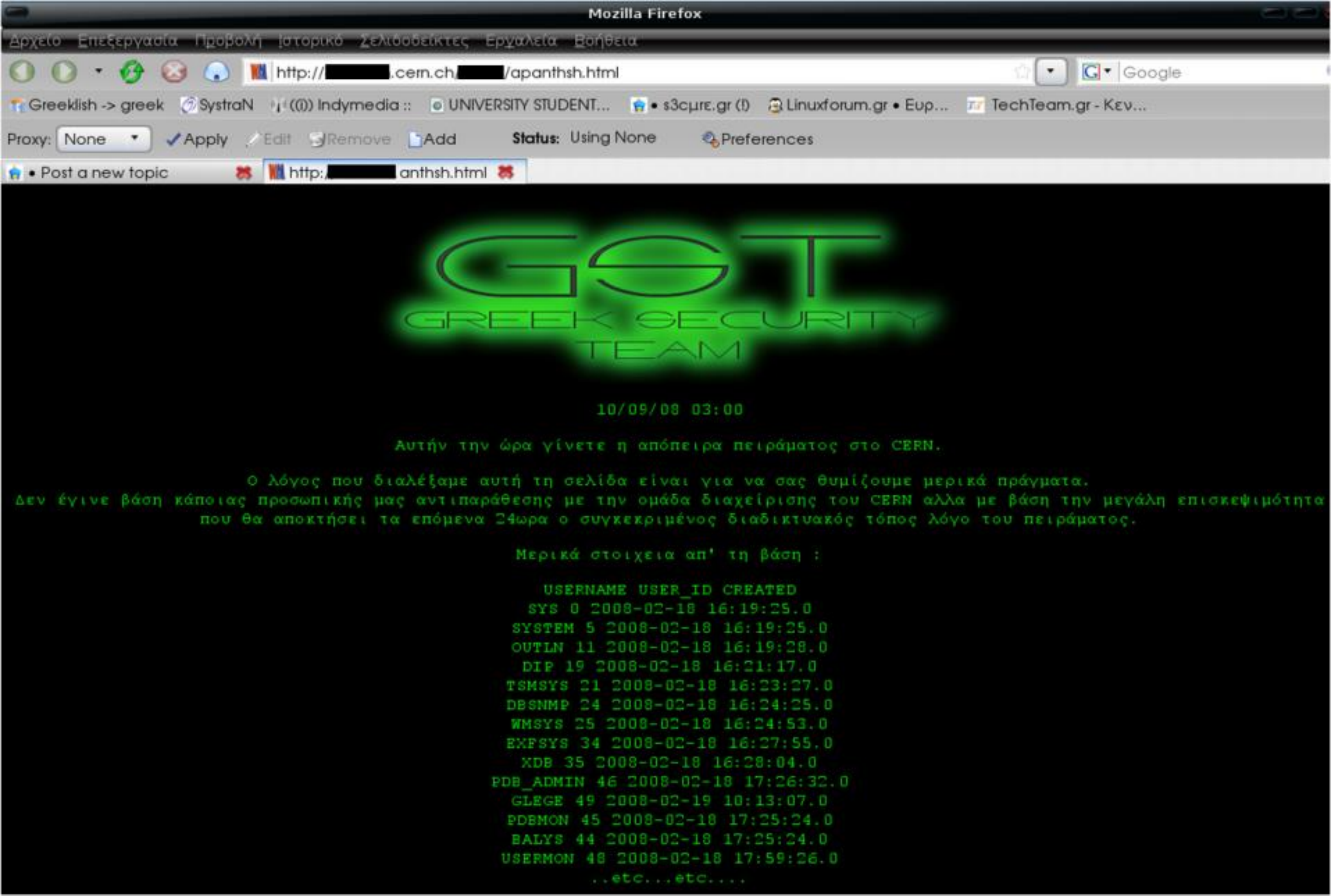


```
vulnerable..
<MLT> i've had my IP blacklisted by an intrusion prevention system. Other than that, it's fine :P
<sc0rp> so what kind of sites will be vulnerable to this exploit?
<MLT> many - i've noticed a lot of high-profile sites with .gov, .mil, and .int TLD's are running MS SharePoint
<MLT> here are a few large sites which are currently vulnerable:
<MLT> http://dubai.ae/en/Lists/Articles/DispForm.aspx?ID=%27108
<MLT> http://calshare.berkeley.edu/Lists/KB/DisoForm.aspx?ID=%276
<MLT> http://marines.mil/unit/mcscg/Pages/Forms/DispForm.aspx?ID=%2761
<MLT> http://www.shipping.nato.int/Lists/AlertsReplace/DispForm.asp?ID=%27217
<sc0rp> nice
<MLT> using the exploit on CERN would be win, hacking the people who created the internet :P
<sc0rp> haha
==============================================
```

Pastebin.com Tools & Applications
Windows
Firefox
Chrome
iOS
WebOS
Android
Mac
Opera
Click.to
UNIX
WinPhone
create new paste | api | trends | users | faq | tools | domains center | privacy | contact | stats | go pro
Follow us: pastebin on facebook | pastebin on twitter | pastebin in the news
Some friends: hostlogr | tinysubs | urlspy | fileshut
Pastebin v3.1 rendered in: 0.010 seconds
pastebin is hosted by STAMINUS

We are TARGET!

Shouldn't we…



10/09/08 03:00

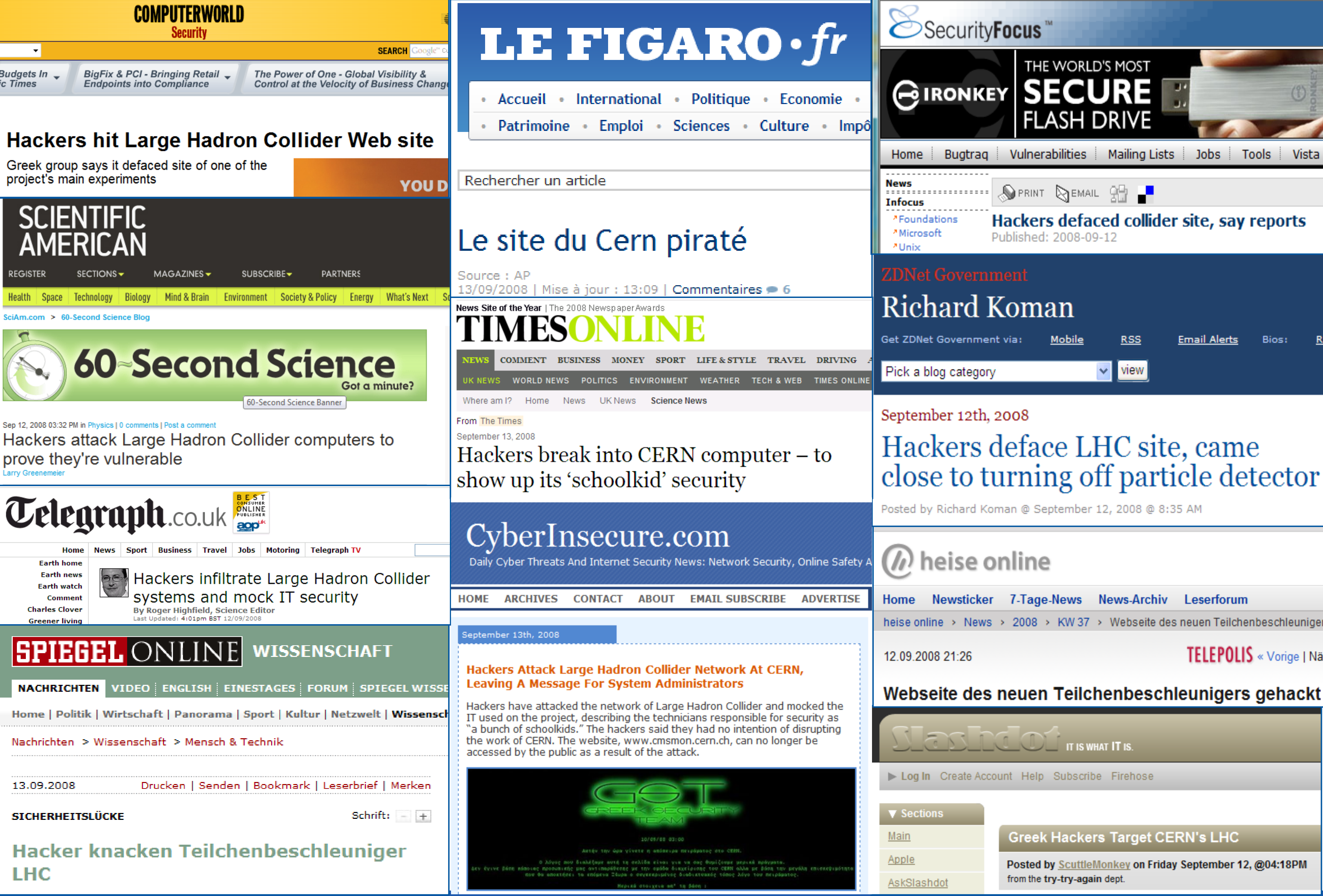
Αυτήν την ώρα γίνετε η απόπειρα πειράματος στο CERN.

Ο λόγος που διαλέξαμε αυτή τη σελίδα είναι για να σας θυμίζουμε μερικά πράγματα.
Δεν έγινε βάση κάποιας προσωπικής μας αντιπαράθεσης με την ομάδα διαχείρισης του CERN αλλα με βάση την μεγάλη επισκεψιμότητα
που θα αποκτήσει τα επόμενα 24ωρα ο συγκεκριμένος διαδικτυακός τόπος λόγο του πειράματος.

Μερικά στοιχεια απ' τη βάση :

```
USERNAME USER_ID CREATED
SYS 0 2008-02-18 16:19:25.0
SYSTEM 5 2008-02-18 16:19:25.0
OUTLN 11 2008-02-18 16:19:28.0
DIP 19 2008-02-18 16:21:17.0
TSMSYS 21 2008-02-18 16:23:27.0
DBSNMP 24 2008-02-18 16:24:25.0
WMSYS 25 2008-02-18 16:24:53.0
EXFSYS 34 2008-02-18 16:27:55.0
XDB 35 2008-02-18 16:28:04.0
PDB_ADMIN 46 2008-02-18 17:26:32.0
GLEGE 49 2008-02-19 10:13:07.0
PDBMON 45 2008-02-18 17:25:24.0
BALYS 44 2008-02-18 17:25:24.0
USERMON 48 2008-02-18 17:59:26.0
..etc...etc....
```

Compromized by BLUNDER


COMPUTERWORLD
Security
SEARCH
Budgets In
c Times
BigFix & PCI - Bringing Retail Endpoints into Compliance
The Power of One - Global Visibility & Control at the Velocity of Business Chang

Hackers hit Large Hadron Collider Web site

Greek group says it defaced site of one of the project's main experiments

Sep 12, 2008 03:32 PM in Physics | 0 comments | Post a comment

Hackers attack Large Hadron Collider computers to prove they're vulnerable

Larry Greenemeier

Hackers infiltrate Large Hadron Collider systems and mock IT security

By Roger Highfield, Science Editor
Last Updated: 4:01pm BST 12/09/2008

SPIEGEL ONLINE WISSENSCHAFT
NACHRICHTEN
VIDEO
ENGLISH
EINESTAGES
FORUM
SPIEGEL WISSE
Home | Politik | Wirtschaft | Panorama | Sport | Kultur | Netzwelt | Wissensch
Nachrichten > Wissenschaft > Mensch & Technik
Drucken | Senden | Bookmark | Leserbrief | Merken
Schrift:

13.09.2008

SICHERHEITSLÜCKE

Hacker knacken Teilchenbeschleuniger LHC

Le site du Cern piraté

Source : AP
13/09/2008 | Mise à jour : 13:09 | Commentaires 6

From The Times
September 13, 2008

Hackers break into CERN computer – to show up its 'schoolkid' security

CyberInsecure.com
Daily Cyber Threats And Internet Security News: Network Security, Online Safety A
HOME
ARCHIVES
CONTACT
ABOUT
EMAIL SUBSCRIBE
ADVERTISE

September 13th, 2008

Hackers Attack Large Hadron Collider Network At CERN, Leaving A Message For System Administrators

Hackers have attacked the network of Large Hadron Collider and mocked the IT used on the project, describing the technicians responsible for security as "a bunch of schoolkids." The hackers said they had no intention of disrupting the work of CERN. The website, www.cmsmon.cern.ch, can no longer be accessed by the public as a result of the attack.

Hackers defaced collider site, say reports

Published: 2008-09-12

Richard Koman

September 12th, 2008

Hackers deface LHC site, came close to turning off particle detector

Posted by Richard Koman @ September 12, 2008 @ 8:35 AM

12.09.2008 21:26

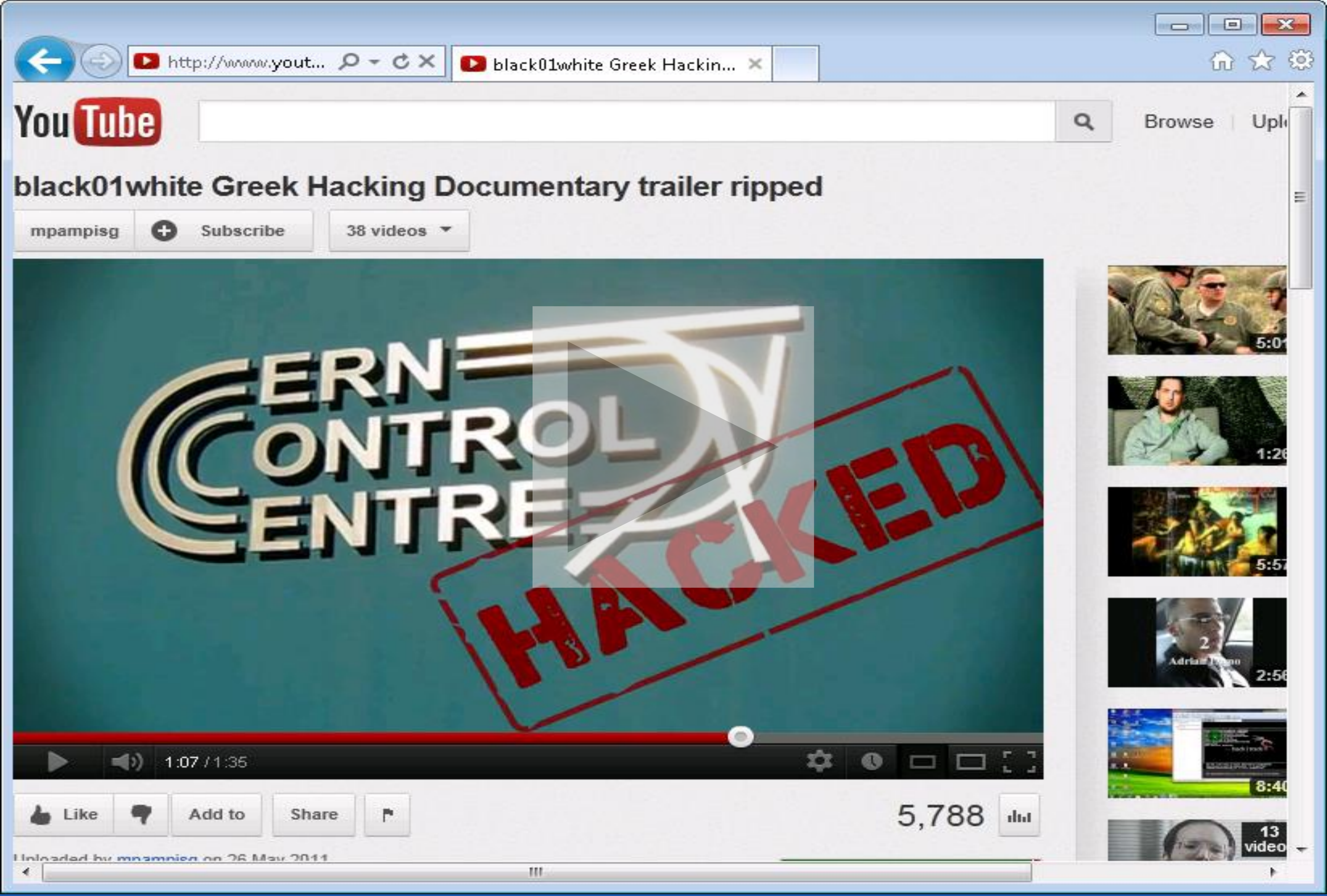
Webseite des neuen Teilchenbeschleunigers gehackt

Greek Hackers Target CERN's LHC

Posted by ScuttleMonkey on Friday September 12, @04:18PM
from the try-try-again dept.

Bad CONSEQUENCES…

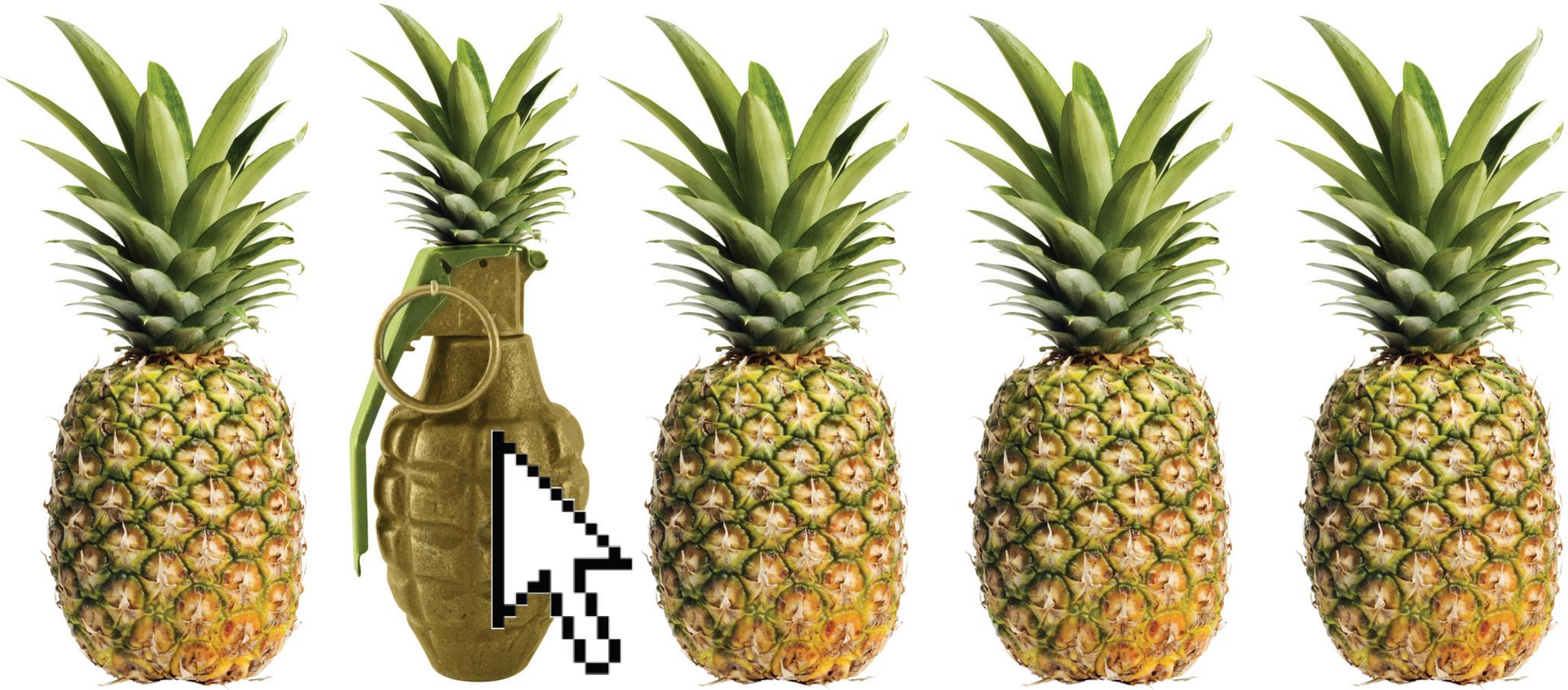
Shouldn't we…



black01white Greek Hacking Documentary trailer ripped

Uploaded by mpampisg on 26 May 2011

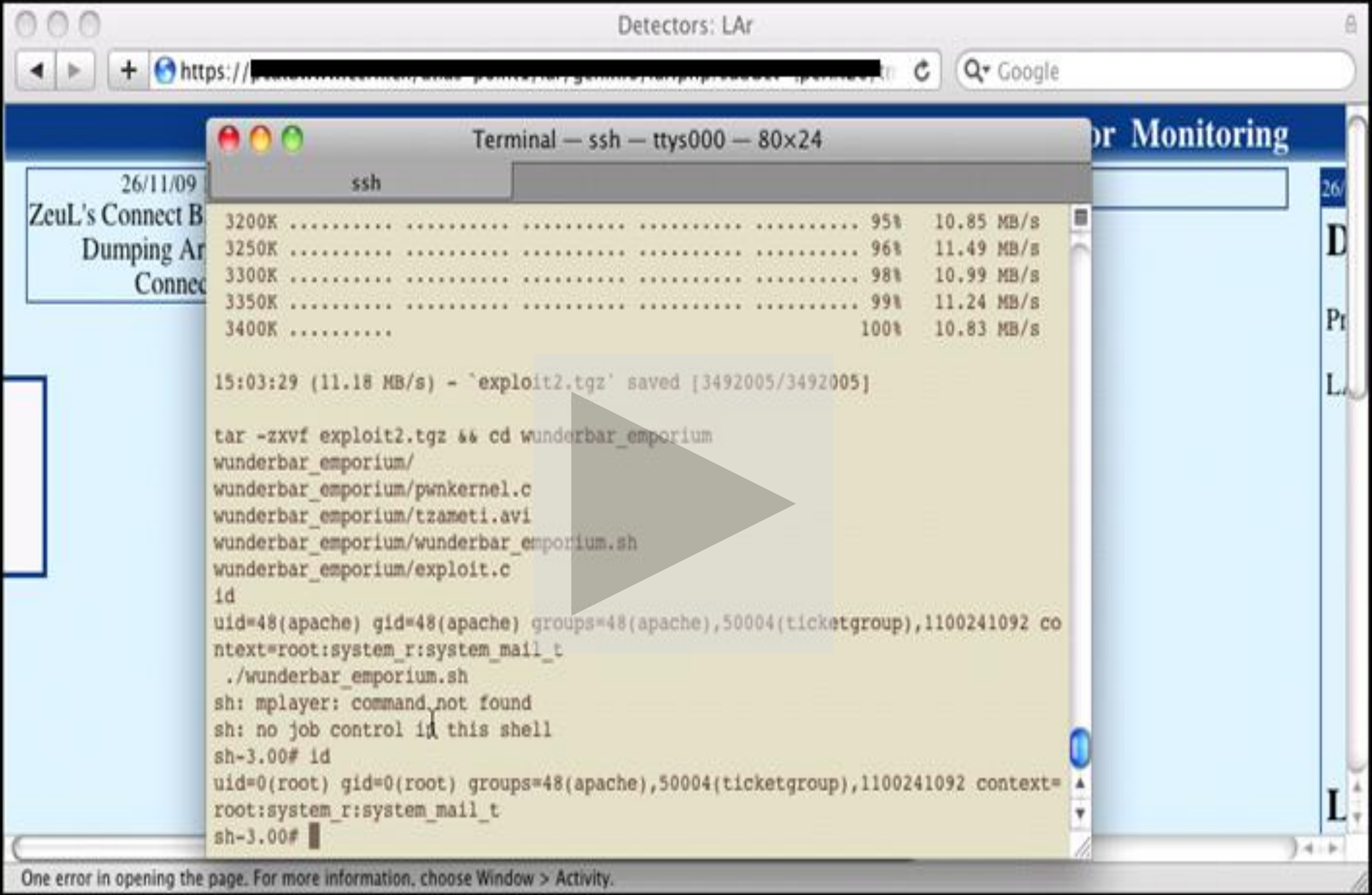
…even years LATER!



We can do BETTER!

```
220-<<<<<<>==< Haxed by A¦0n3 >==<>>>>>>
220- ¸,ø¤°°^°°¤ø,¸¸,ø¤°°^°°¤ø,¸¸,ø¤°°^°°¤ø,¸¸,ø¤°°^°°¤ø,¸
220-/
220-|    Welcome  to this fine str0
220-|    Today is: Thursday 12 January, 2006
220-|
220-|    Current througput: 0.000 Kb/sec
220-|    Space For Rent: 5858.57 Mb
220-|
220-|    Running: 0 days, 10 hours, 3
220-|    Users Connected : 1 Total :
220-|
220^°°¤ø,¸¸,ø¤°°^°°¤ø,¸¸,ø¤°°^°°¤ø,¸¸,ø¤       ¤ø,¸¸,ø¤
```

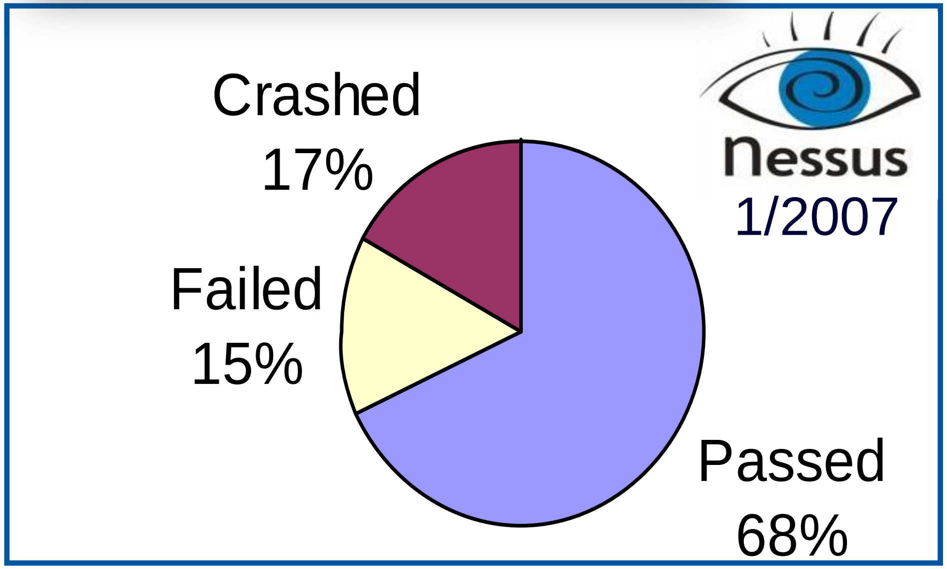
Think of PATCHING

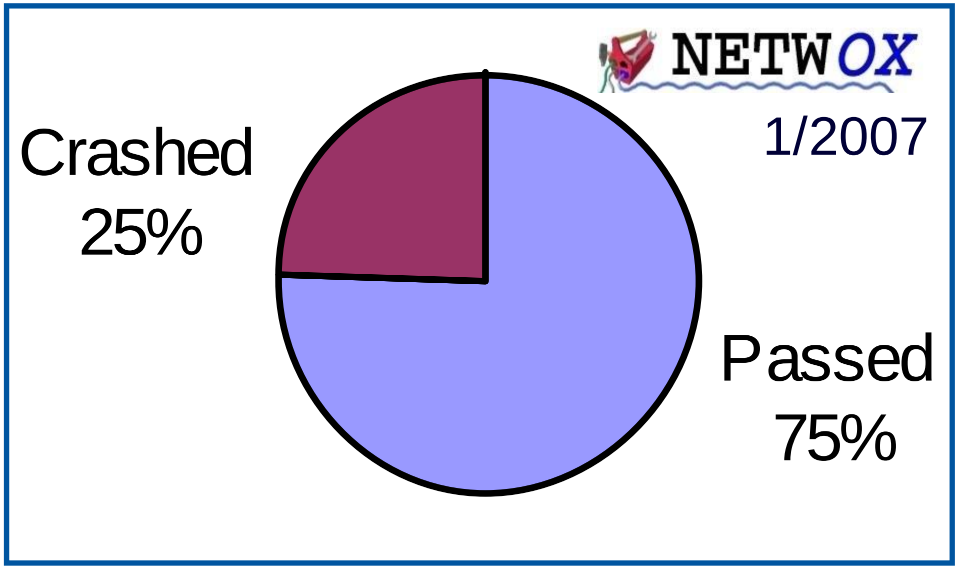


```
 3200K .......... .......... .......... .......... .......... 95%  10.85 MB/s
 3250K .......... .......... .......... .......... .......... 96%  11.49 MB/s
 3300K .......... .......... .......... .......... .......... 98%  10.99 MB/s
 3350K .......... .......... .......... .......... .......... 99%  11.24 MB/s
 3400K ..........                                            100%  10.83 MB/s

15:03:29 (11.18 MB/s) - `exploit2.tgz' saved [3492005/3492005]

tar -zxvf exploit2.tgz && cd wunderbar_emporium
wunderbar_emporium/
wunderbar_emporium/pwnkernel.c
wunderbar_emporium/tzameti.avi
wunderbar_emporium/wunderbar_emporium.sh
wunderbar_emporium/exploit.c
id
uid=48(apache) gid=48(apache) groups=48(apache),50004(ticketgroup),1100241092 co
ntext=root:system_r:system_mail_t
 ./wunderbar_emporium.sh
sh: mplayer: command not found
sh: no job control in this shell
sh-3.00# id
uid=0(root) gid=0(root) groups=48(apache),50004(ticketgroup),1100241092 context=
root:system_r:system_mail_t
sh-3.00# 
```

One error in opening the page. For more information, choose Window > Activity.

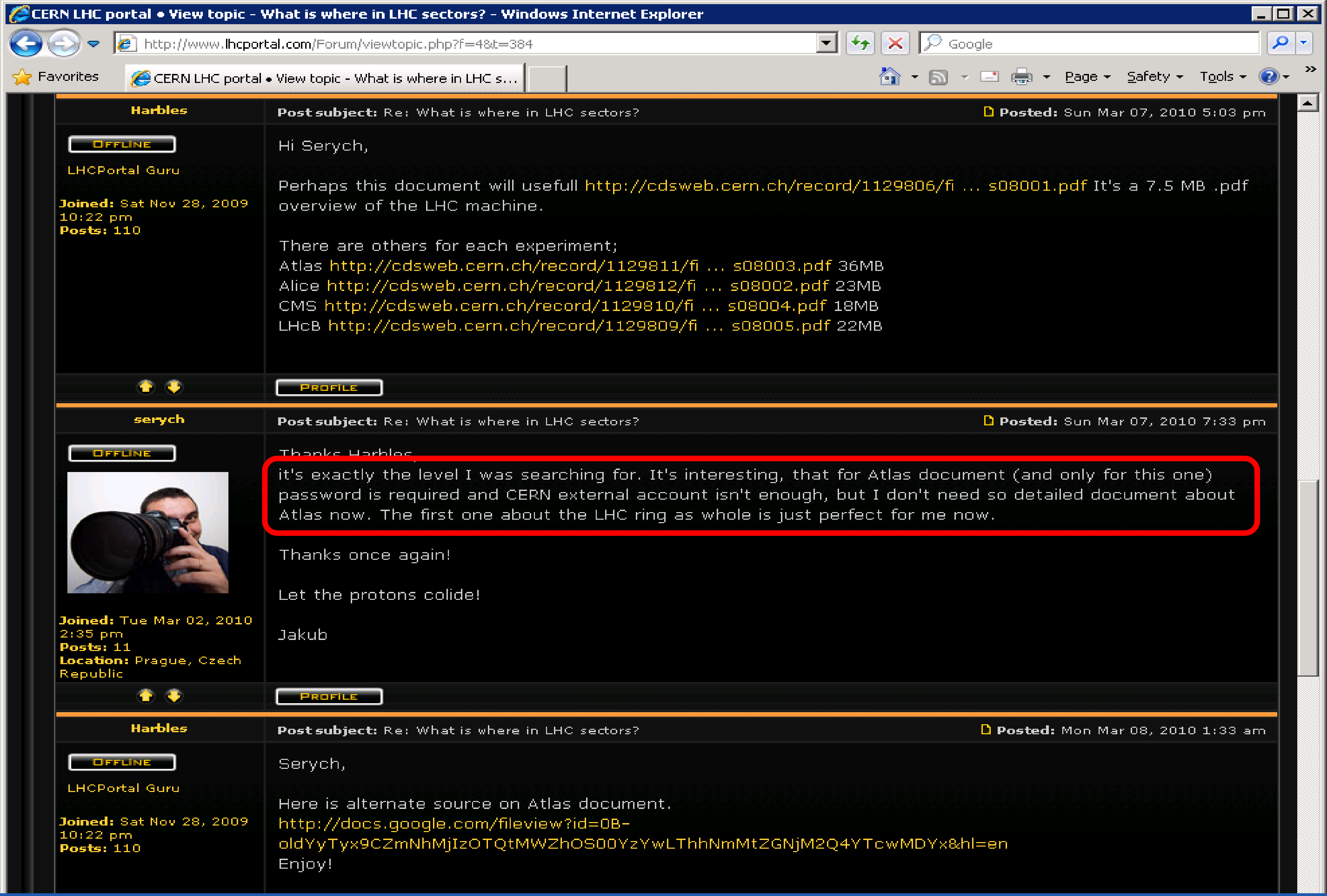
Think of INPUT VERIFICATION





Think of SYSTEM HARDENING

Shouldn't we…


CERN LHC portal • View topic - What is where in LHC sectors? - Windows Internet Explorer
http://www.lhcportal.com/Forum/viewtopic.php?f=4&t=384
Google
Favorites
CERN LHC portal • View topic - What is where in LHC s...
Page
Safety
Tools

Harbles

OFFLINE

LHCPortal Guru

Joined: Sat Nov 28, 2009 10:22 pm
Posts: 110

Post subject: Re: What is where in LHC sectors?

Posted: Sun Mar 07, 2010 5:03 pm

Hi Serych,

Perhaps this document will usefull http://cdsweb.cern.ch/record/1129806/fi ... s08001.pdf It's a 7.5 MB .pdf overview of the LHC machine.

There are others for each experiment;
Atlas http://cdsweb.cern.ch/record/1129811/fi ... s08003.pdf 36MB
Alice http://cdsweb.cern.ch/record/1129812/fi ... s08002.pdf 23MB
CMS http://cdsweb.cern.ch/record/1129810/fi ... s08004.pdf 18MB
LHcB http://cdsweb.cern.ch/record/1129809/fi ... s08005.pdf 22MB

PROFILE

serych

OFFLINE

Joined: Tue Mar 02, 2010 2:35 pm
Posts: 11
Location: Prague, Czech Republic

Post subject: Re: What is where in LHC sectors?

Posted: Sun Mar 07, 2010 7:33 pm

Thanks Harbles,
it's exactly the level I was searching for. It's interesting, that for Atlas document (and only for this one) password is required and CERN external account isn't enough, but I don't need so detailed document about Atlas now. The first one about the LHC ring as whole is just perfect for me now.

Thanks once again!

Let the protons colide!

Jakub

PROFILE

Harbles

OFFLINE

LHCPortal Guru

Joined: Sat Nov 28, 2009 10:22 pm
Posts: 110

Post subject: Re: What is where in LHC sectors?

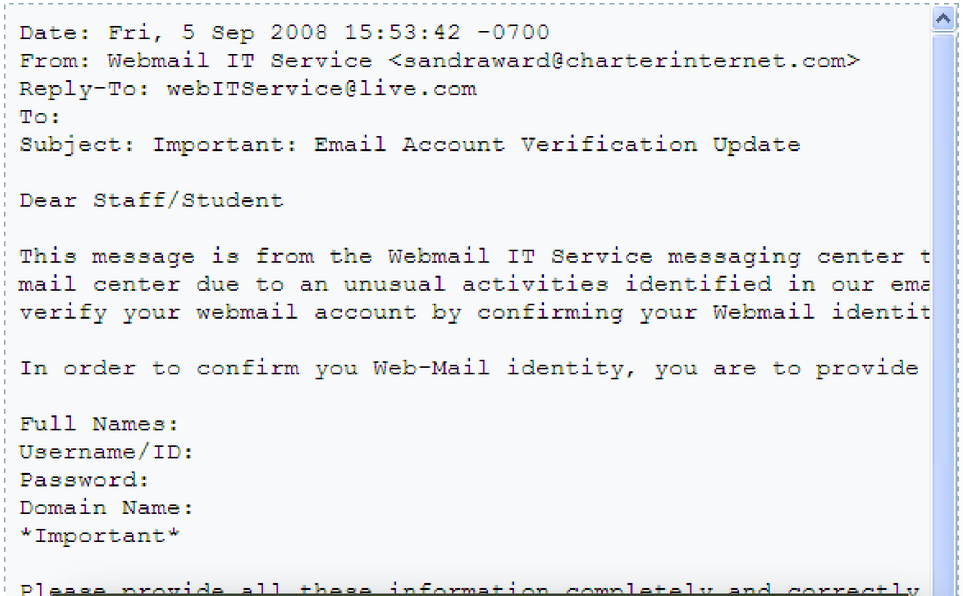
Posted: Mon Mar 08, 2010 1:33 am

Serych,

Here is alternate source on Atlas document.
http://docs.google.com/fileview?id=0B-oldYyTyx9CZmNhMjIzOTQtMWZhOS00YzYwLThhNmMtZGNjM2Q4YTcwMDYx&hl=en
Enjoy!

Think of DATA PROTECTION

Shouldn't we…



Date: Fri, 5 Sep 2008 15:53:42 -0700
From: Webmail IT Service <sandraward@charterinternet.com>
Reply-To: webITService@live.com
To:
Subject: Important: Email Account Verification Update

Dear Staff/Student

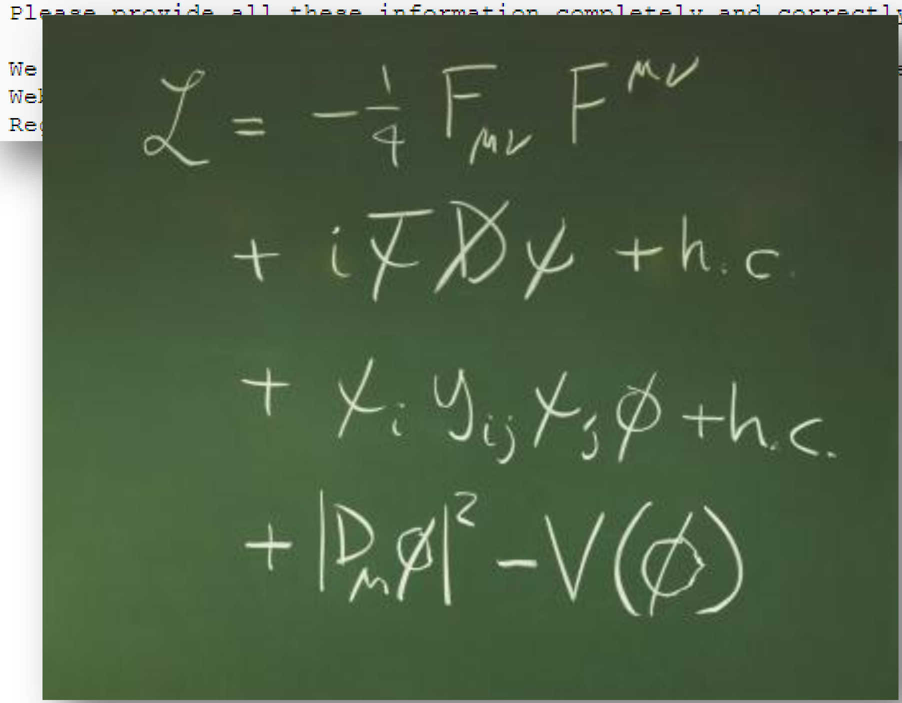
This message is from the Webmail IT Service messaging center t
mail center due to an unusual activities identified in our ema
verify your webmail account by confirming your Webmail identit

In order to confirm you Web-Mail identity, you are to provide

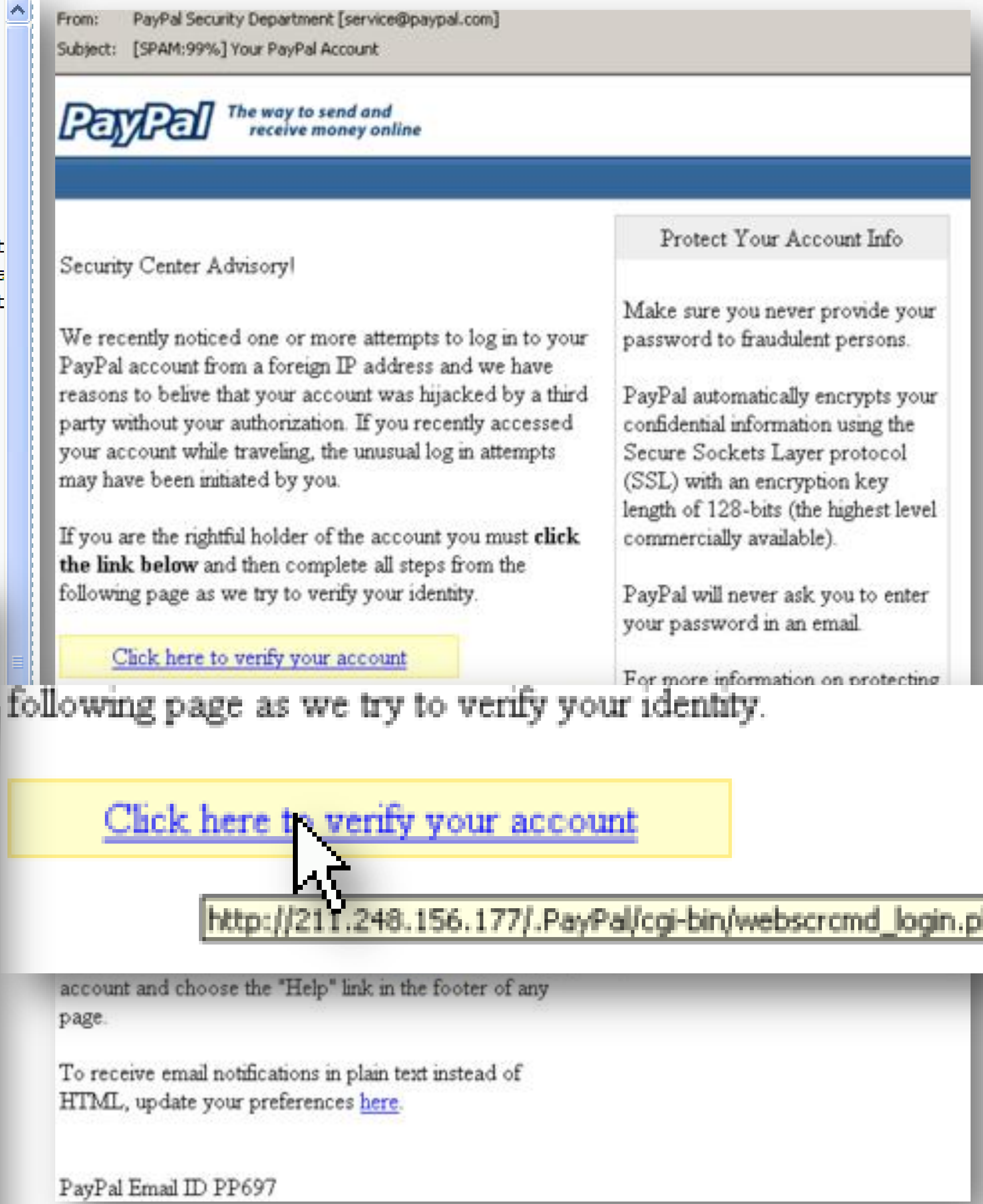
Full Names:
Username/ID:
Password:
Domain Name:
Important

Please provide all these information completely and correctly

We
Wel
Re



$$\mathcal{L} = -\frac{1}{4} F_{\mu\nu} F^{\mu\nu} + i \bar{\psi} \not{D} \psi + h.c. + \psi_i y_{ij} \psi_j \phi + h.c. + |D_\mu \phi|^2 - V(\phi)$$



From: PayPal Security Department [service@paypal.com]
Subject: [SPAM:99%] Your PayPal Account

Security Center Advisory!

We recently noticed one or more attempts to log in to your PayPal account from a foreign IP address and we have reasons to belive that your account was hijacked by a third party without your authorization. If you recently accessed your account while traveling, the unusual log in attempts may have been initiated by you.

If you are the rightful holder of the account you must **click the link below** and then complete all steps from the following page as we try to verify your identity.

Click here to verify your account

Protect Your Account Info

Make sure you never provide your password to fraudulent persons.

PayPal automatically encrypts your confidential information using the Secure Sockets Layer protocol (SSL) with an encryption key length of 128-bits (the highest level commercially available).

PayPal will never ask you to enter your password in an email.

For more information on protecting

following page as we try to verify your identity.

Click here to verify your account

http://211.248.156.177/.PayPal/cgi-bin/webscrcmd_login.p

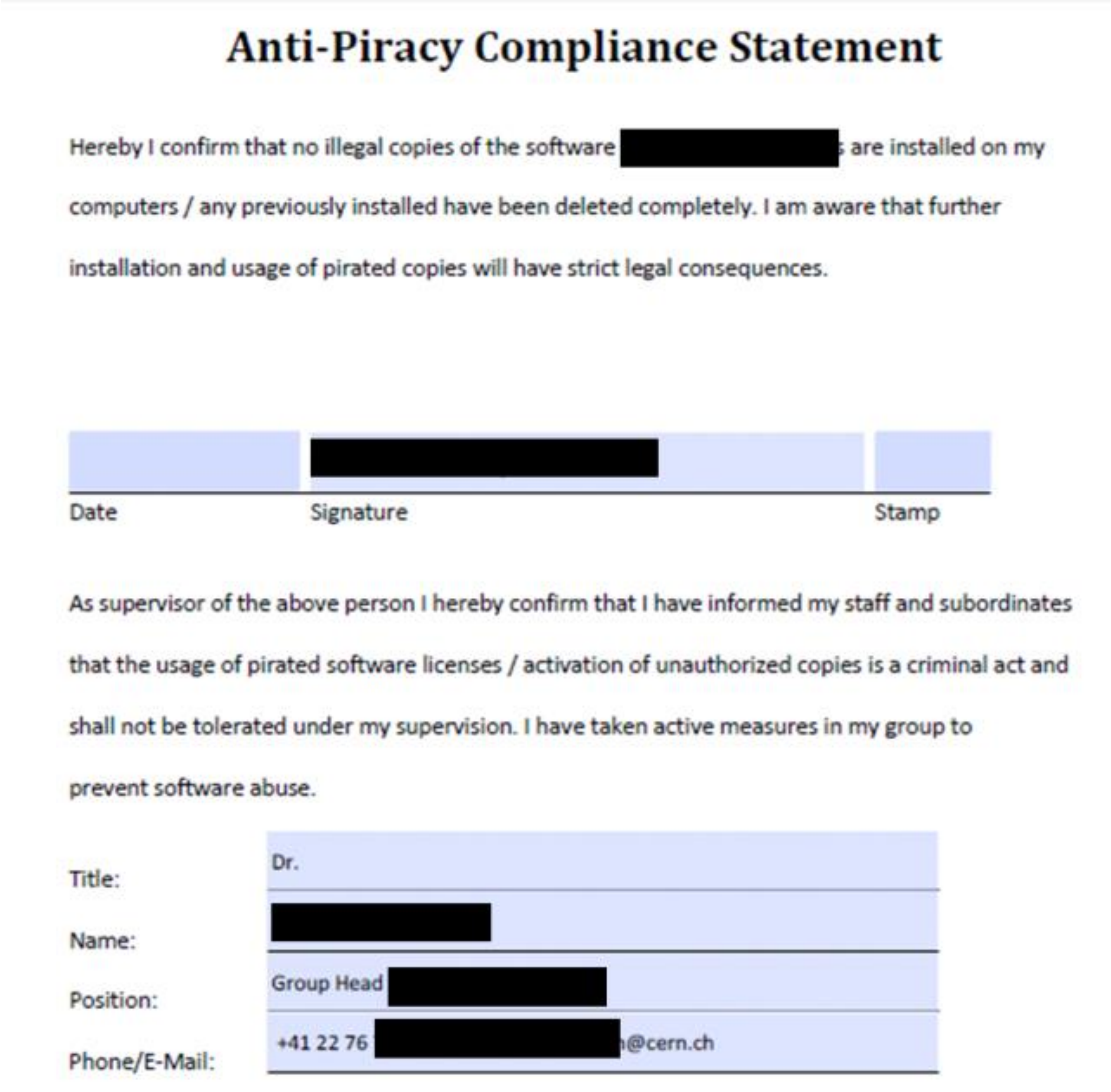
account and choose the "Help" link in the footer of any page.

To receive email notifications in plain text instead of HTML, update your preferences here.

PayPal Email ID PP697

Think of YOUR PASSWORD

Shouldn't we…



Anti-Piracy Compliance Statement

Hereby I confirm that no illegal copies of the software [redacted] are installed on my computers / any previously installed have been deleted completely. I am aware that further installation and usage of pirated copies will have strict legal consequences.

	[redacted]	
Date	Signature	Stamp

As supervisor of the above person I hereby confirm that I have informed my staff and subordinates that the usage of pirated software licenses / activation of unauthorized copies is a criminal act and shall not be tolerated under my supervision. I have taken active measures in my group to prevent software abuse.

Title:	Dr.
Name:	[redacted]
Position:	Group Head [redacted]
Phone/E-Mail:	+41 22 76 [redacted]@cern.ch

Think of COPYRIGHTS

Recall. It's all about –**ity**:
Functional**ity**, availabil**ity**, usabil**ity**, maintainabil**ity**, and secur**ity.**

Think secure.
Apply patches & harden your system, protect you data & your password, respect copyrights.

Ensure a proper software development life-cycle:
Design your code before you touch the keyboard and start coding, test – test – test in-between, and have plans how to maintain your code/system on the long run.

Do penetration testing…
…and vulnerability scanning.

Do not screw up. If you don't know what your doing, don't do. Ask an expert, read a book, get some training, or forget it.

Do not reinvent the wheel. Focus on your core work.
Check with your local IT department and use their services. Let them take care on maintenance & security.

My PLEA

Shouldn't we…
Dr. Stefan.Lueders@cern.ch
EIROforum School of Instrumentation, May 31st 2013, CERN

Thanks.

And please,
don't program like Penny.