Source Code Review Using Static Analysis Tools

CERN openlab Summer Students
Lightning Talks Sessions

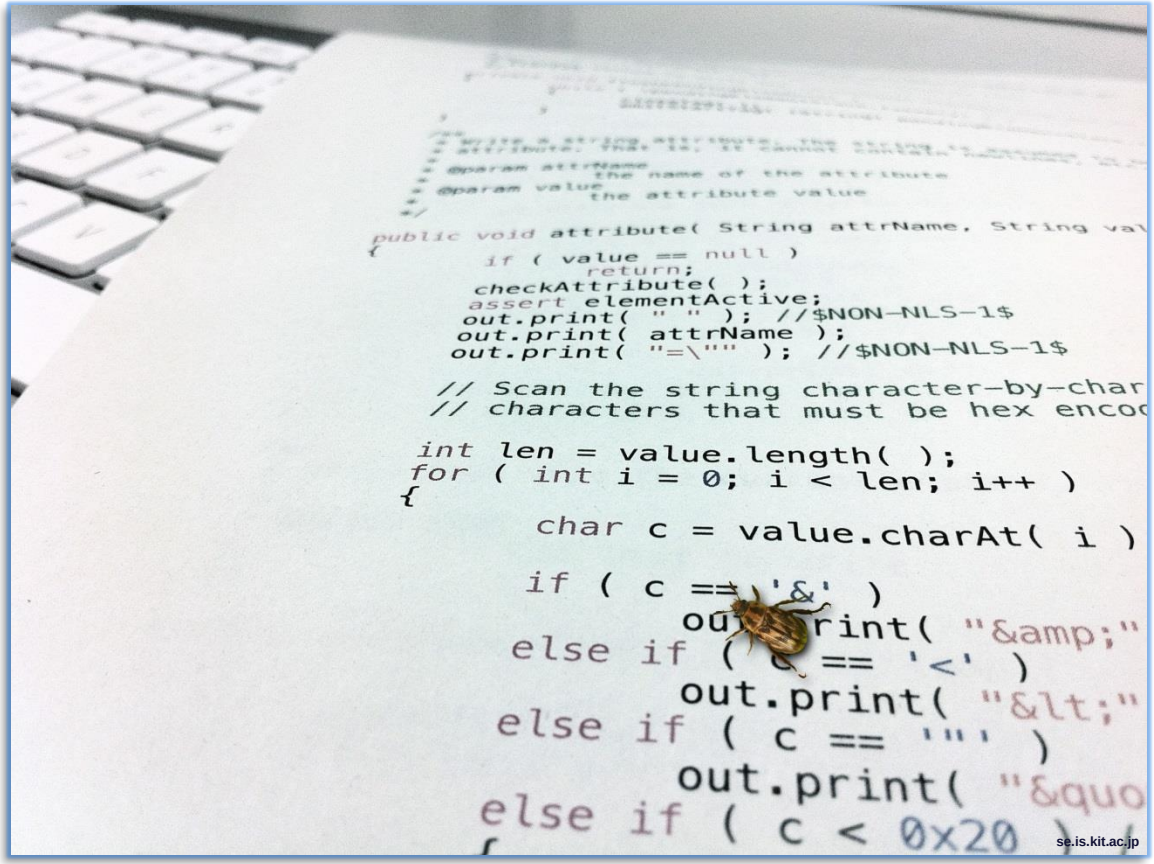
Stavros Moiras

steve@vipersec.com

Supervisors:
Stefan Lueders
Aimilios Tsouvelekakis

26/08/2015

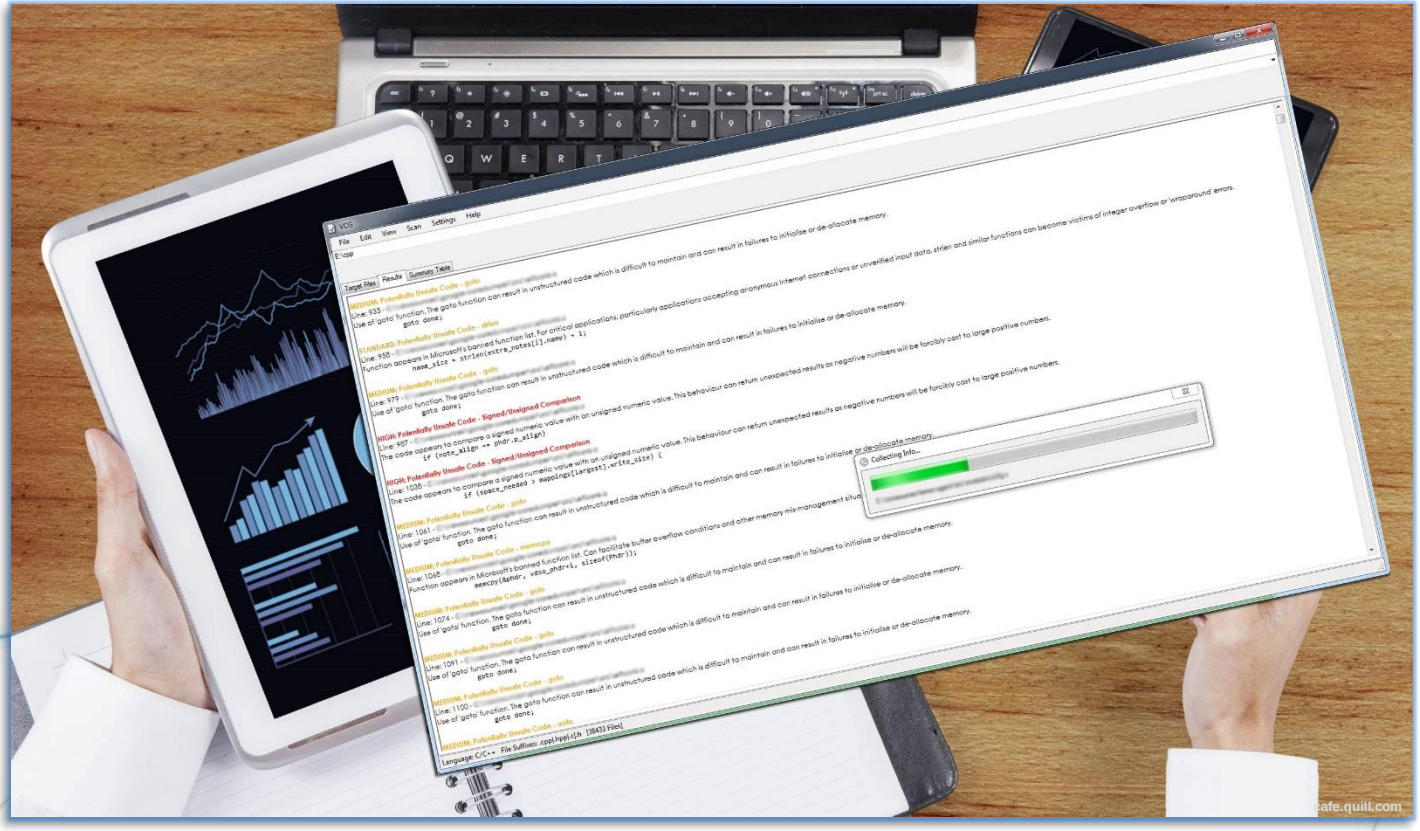
Bugs


public void attribute(String attrName, String val
{
if (value == null)
return;
checkAttribute( );
assert elementActive;
out.print(" "); //$NON-NLS-1$
out.print(attrName);
out.print("=\""); //$NON-NLS-1$
// Scan the string character-by-char
// characters that must be hex encod
int len = value.length( );
for (int i = 0; i < len; i++)
{
char c = value.charAt(i)
if (c == '&')
out.print("&"
else if (c == '<')
out.print("<"
else if (c == '"')
out.print("&quo
else if (c < 0x20)
se.is.kit.ac.jp

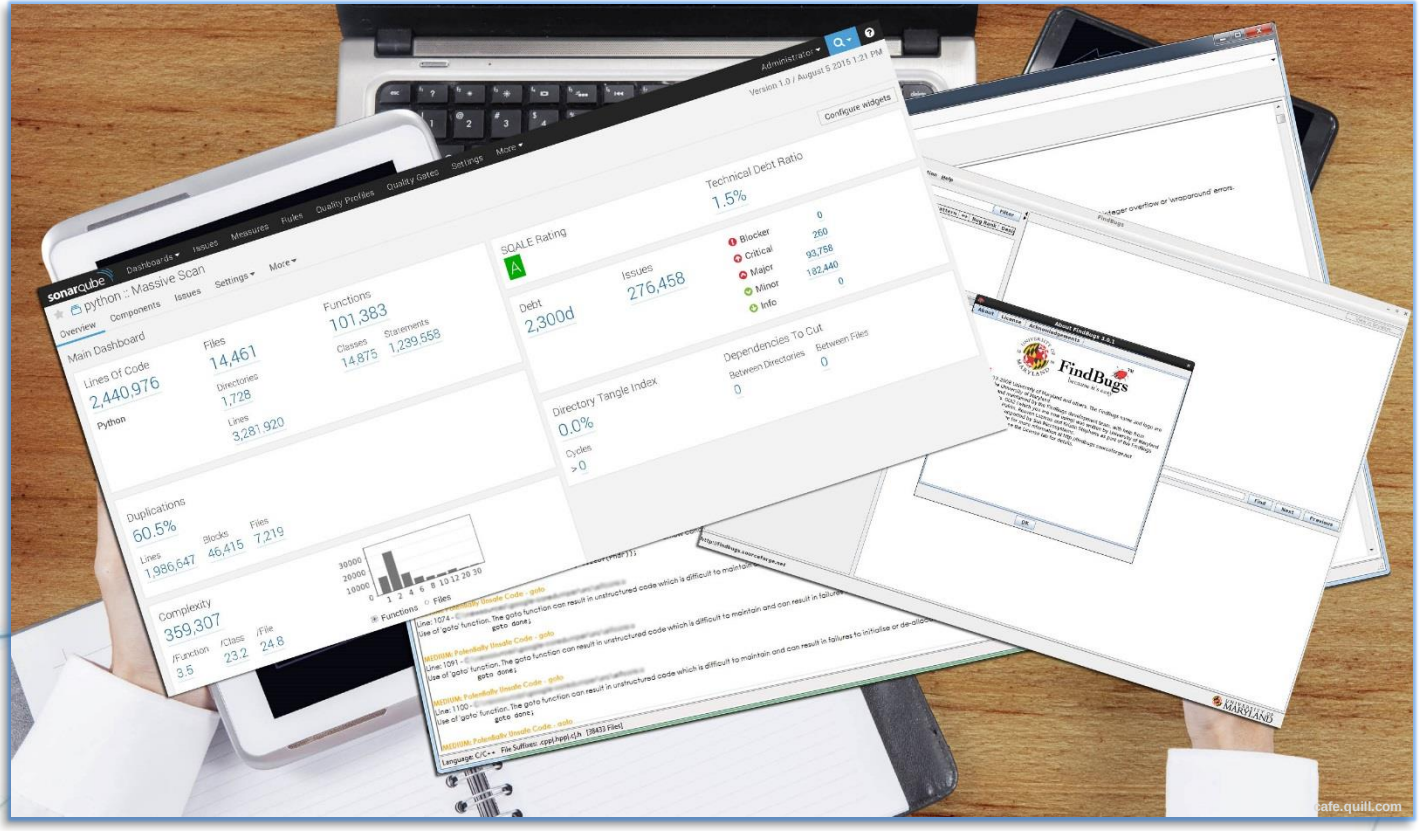
Attackers

Static Analysis Tools

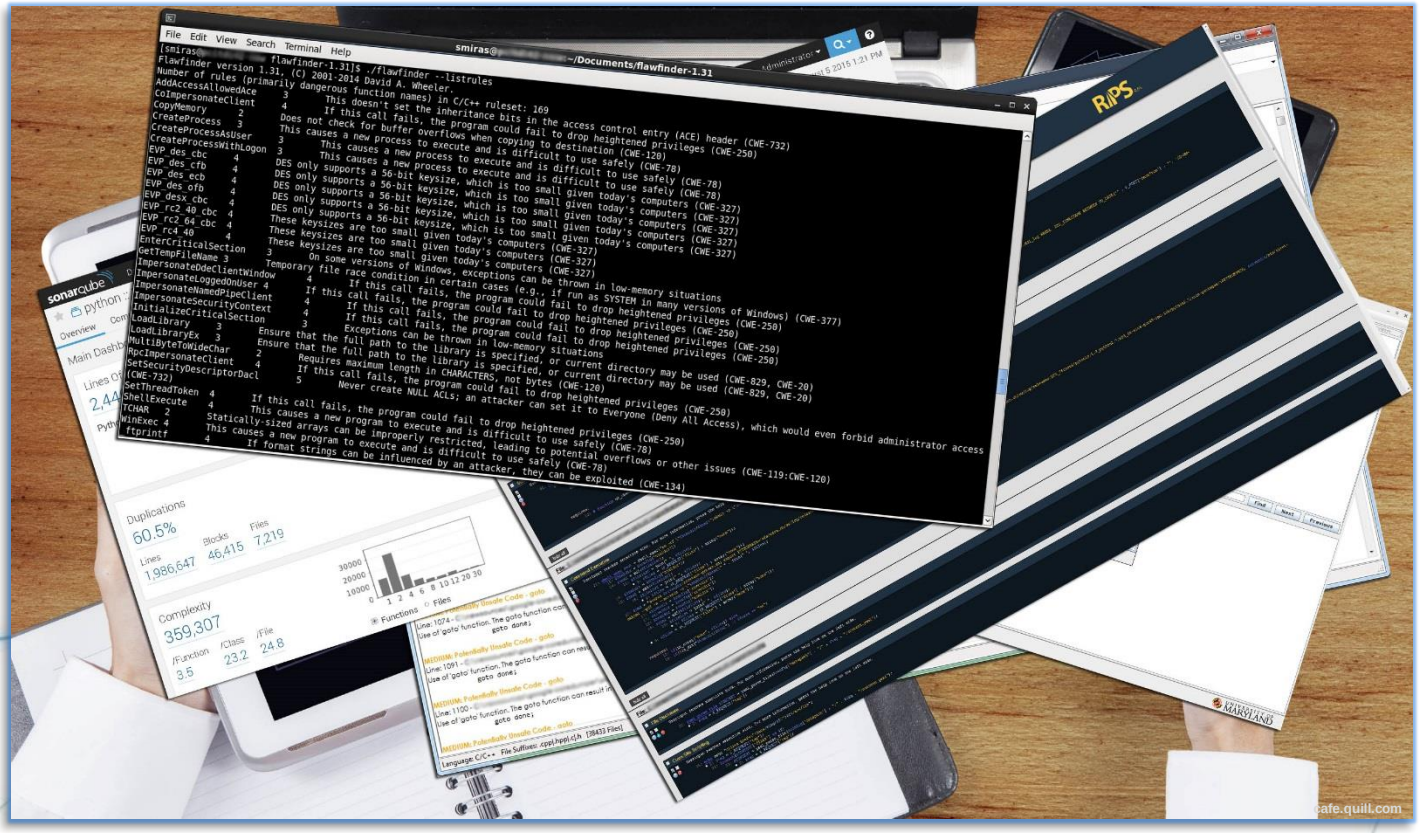
Static Analysis Tools



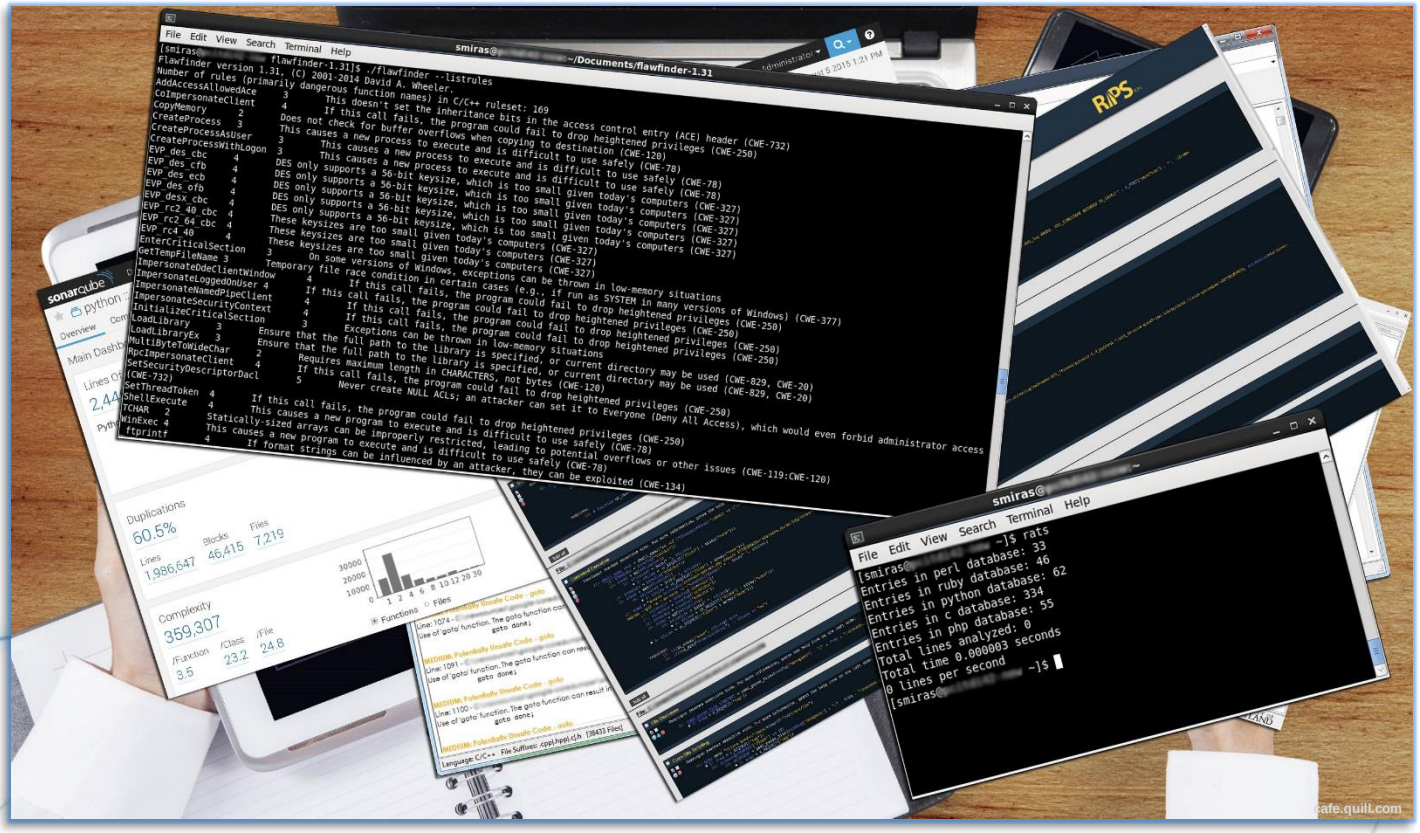
Static Analysis Tools



Static Analysis Tools

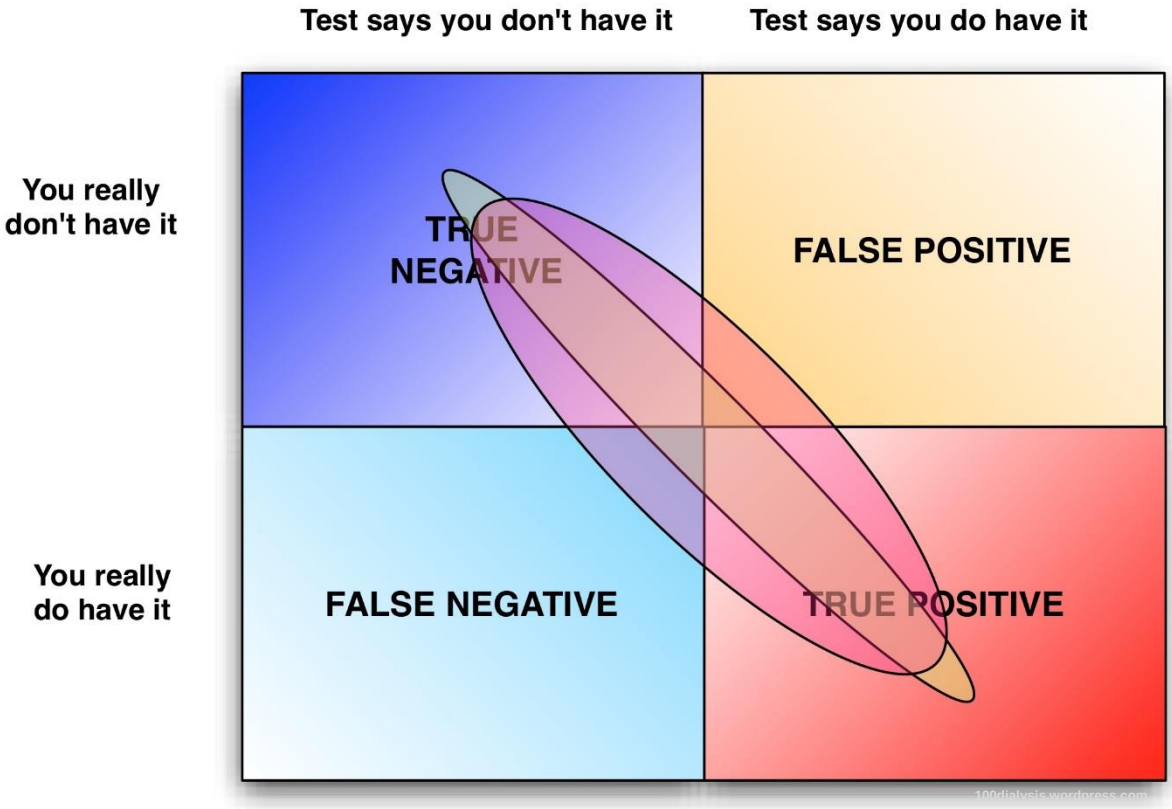


Static Analysis Tools

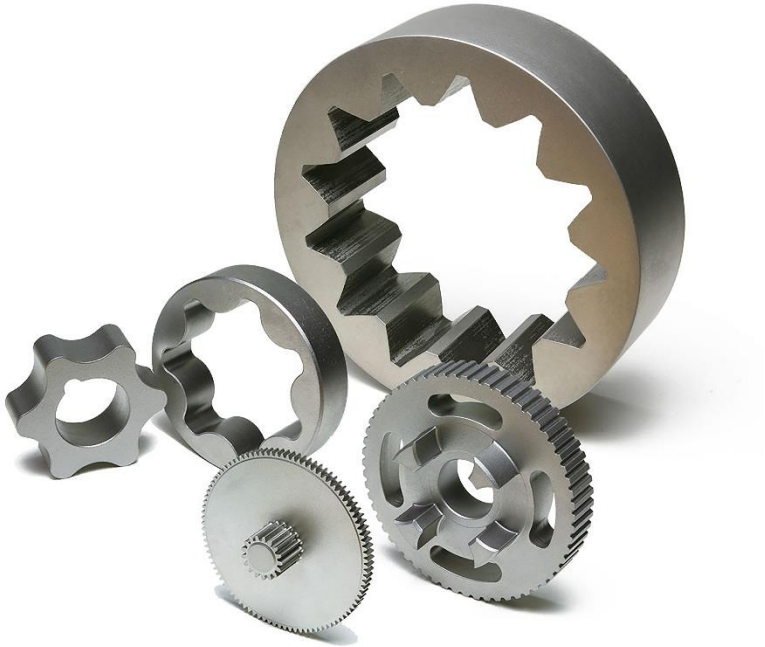


Strengths and weaknesses

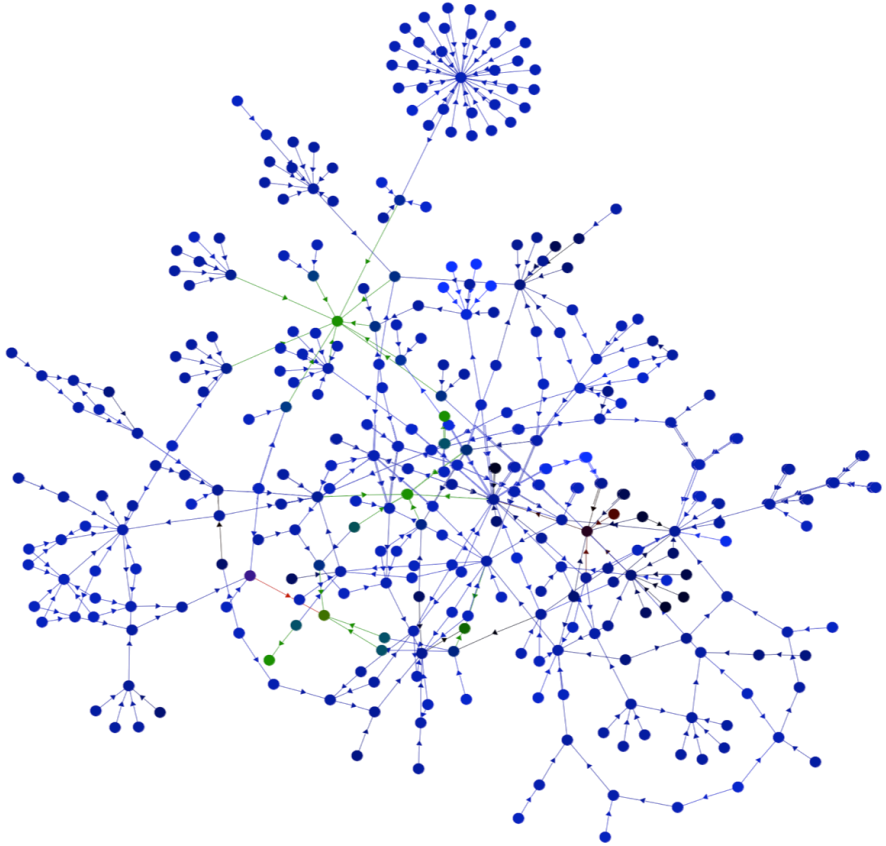
✖ High False Positive Rate



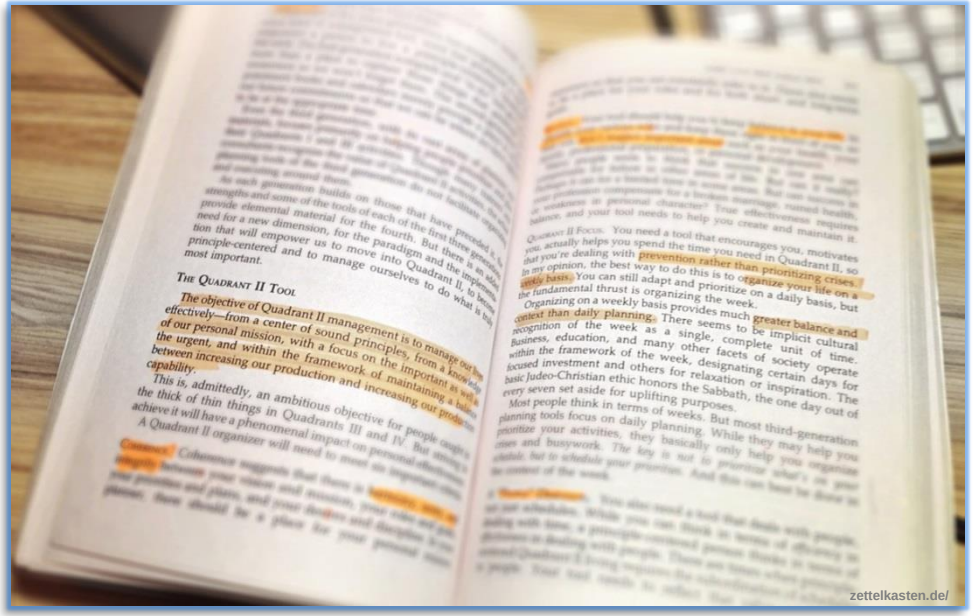
✖ Undetected Configuration Issues



✓ Scalability

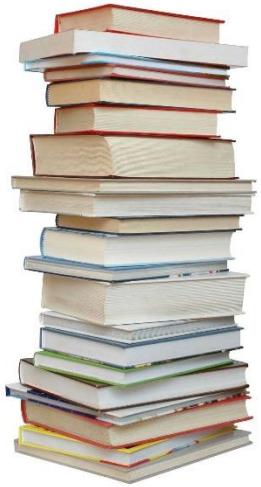


Highlight Source Files and Lines



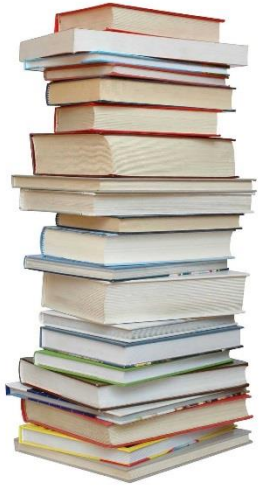
Automatic Detection

Automatic Detection



Overflows

Automatic Detection

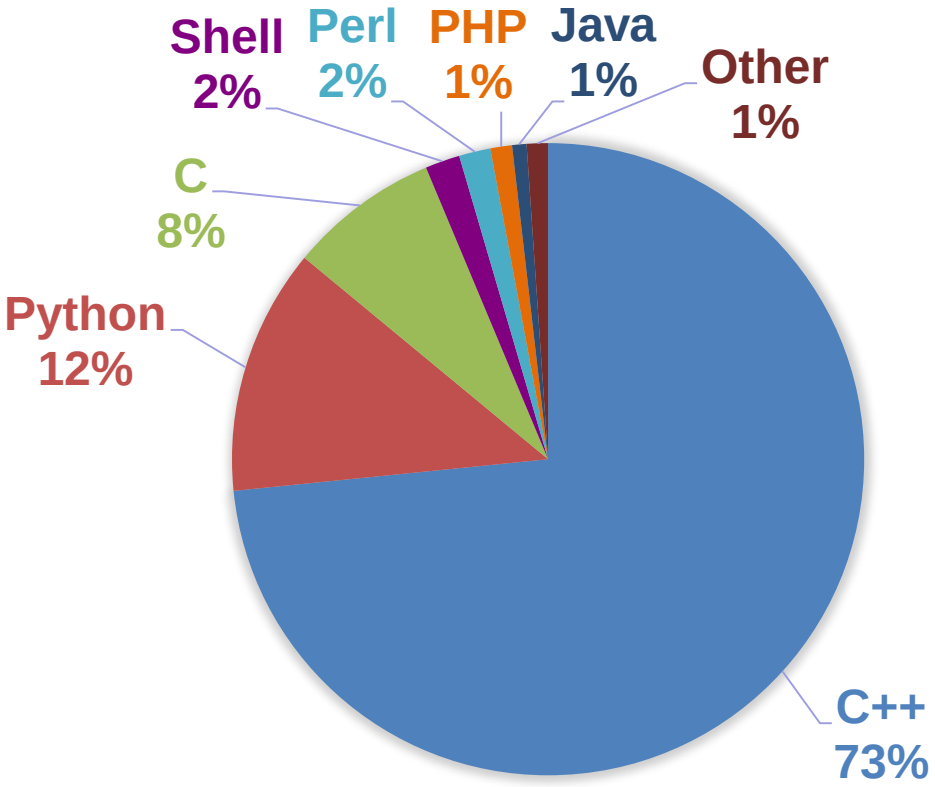


Overflows

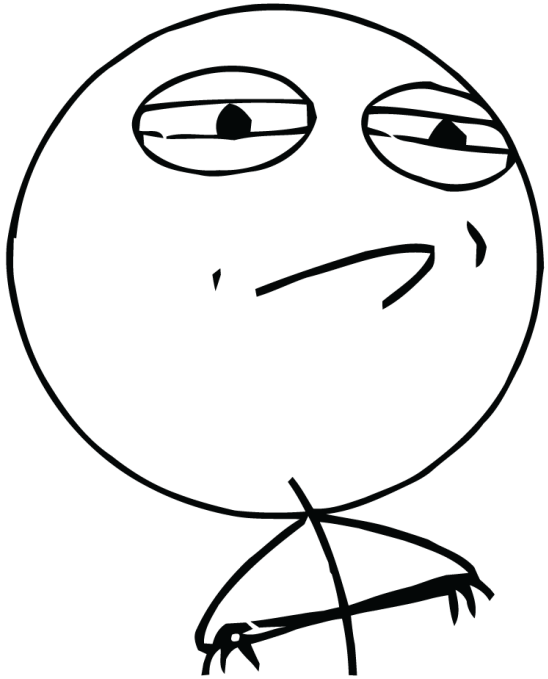
Injections

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;
```

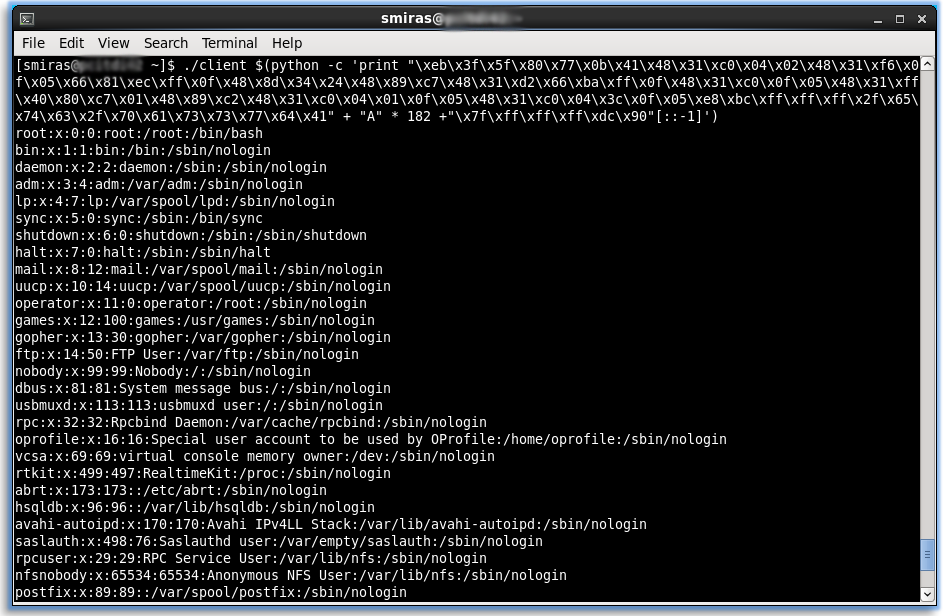
C source file length : 3193 lines : 164 Ln : 9 Col : 16 Sel : 10 | 0 UNIX UTF-8 INS

Detected Vulnerabilities

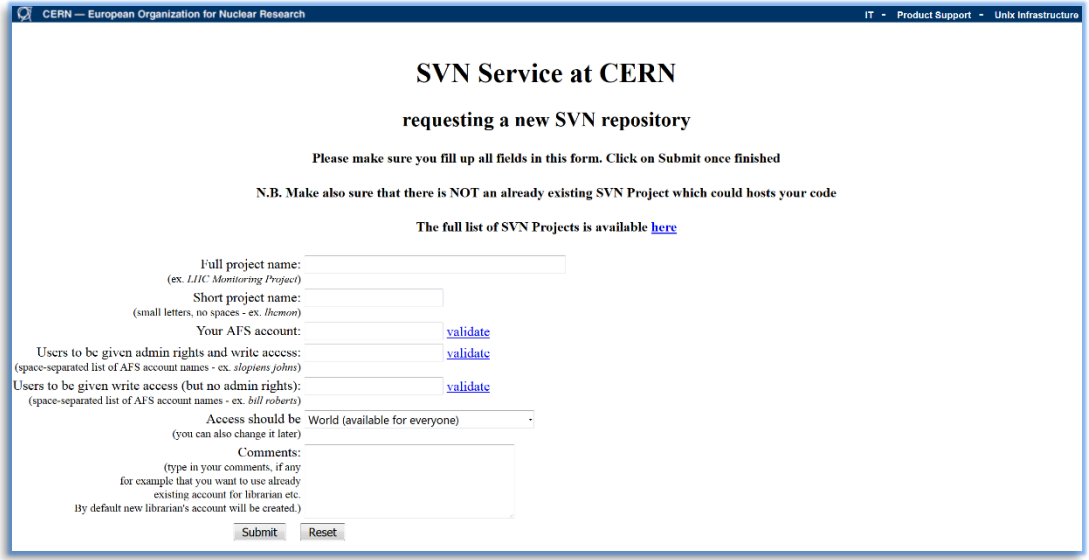
```
3  #include <time.h>
4  #include <string.h>
5  #include <stdio.h>
6
7  char str[80];
8  char str_res[10][80];
9  char client_str[80];
10 int no_link = -1;
11 float no_link_float = -1.0;
12 char buff[80];
13
14 typedef struct {
15     int i;
16     int j;
17     int k;
18     double d;
19     short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

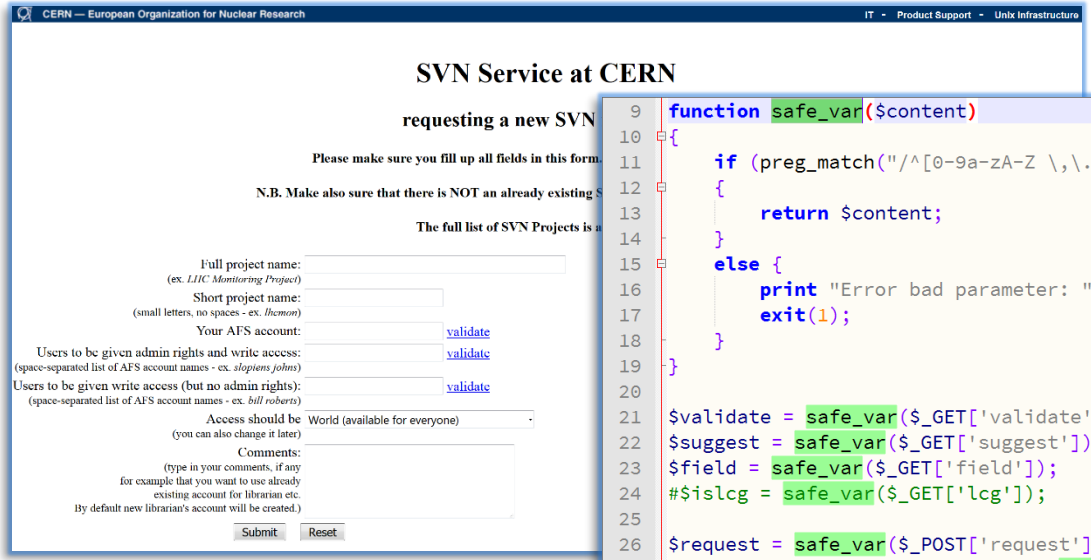
Exploitation



Detected Vulnerabilities



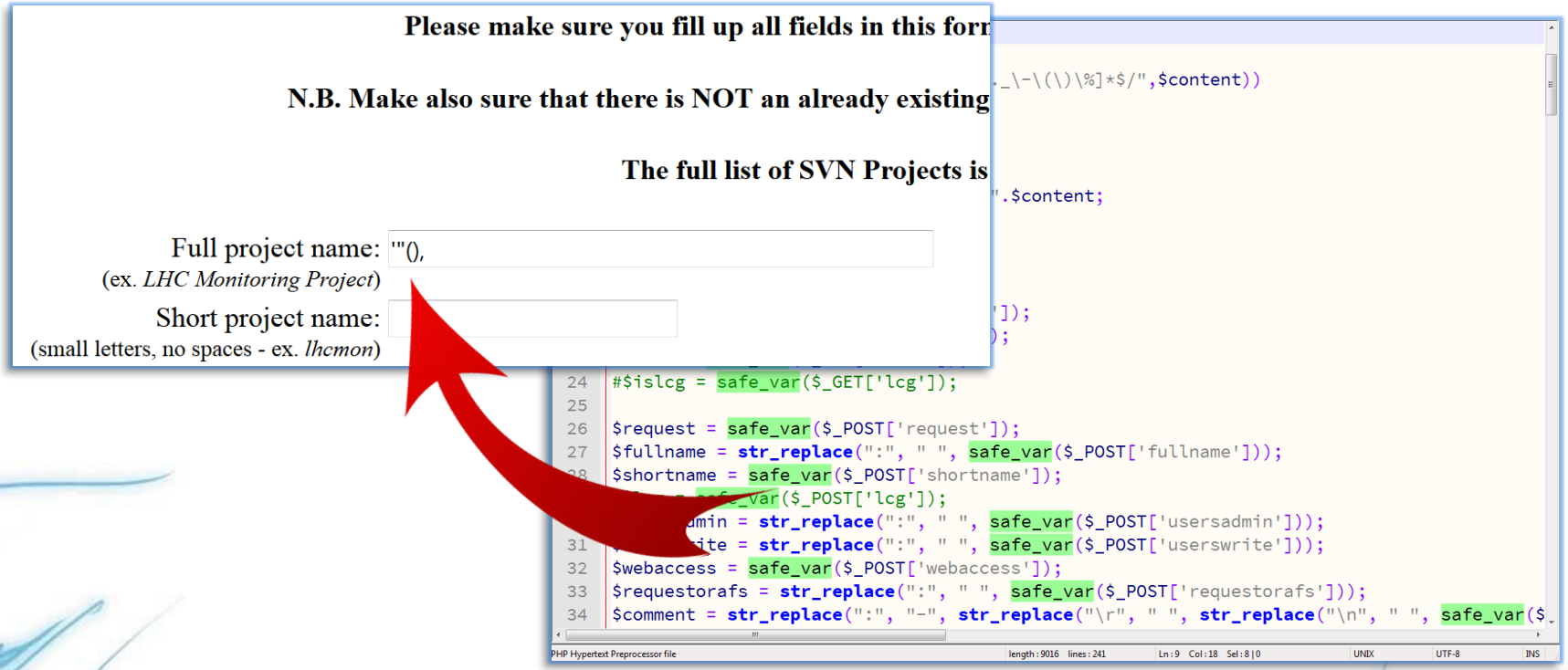
Detected Vulnerabilities




```php
function safe_var($content)
{
    if (preg_match("/^[0-9a-zA-Z \,\._\-\(\)\%]*$/",$content))
    {
        return $content;
    }
    else {
        print "Error bad parameter: ".$content;
        exit(1);
    }
}

$validate = safe_var($_GET['validate']);
$suggest = safe_var($_GET['suggest']);
$field = safe_var($_GET['field']);
#$islcg = safe_var($_GET['lcg']);

$request = safe_var($_POST['request']);
$fullname = str_replace(":", " ", safe_var($_POST['fullname']));
$shortname = safe_var($_POST['shortname']);
#$lcg = safe_var($_POST['lcg']);
$usersadmin = str_replace(":", " ", safe_var($_POST['usersadmin']));
$userswrite = str_replace(":", " ", safe_var($_POST['userswrite']));
$webaccess = safe_var($_POST['webaccess']);
$requestorafs = str_replace(":", " ", safe_var($_POST['requestorafs']));
$comment = str_replace(":", "-", str_replace("\r", " ", str_replace("\n", " ", safe_var($
```

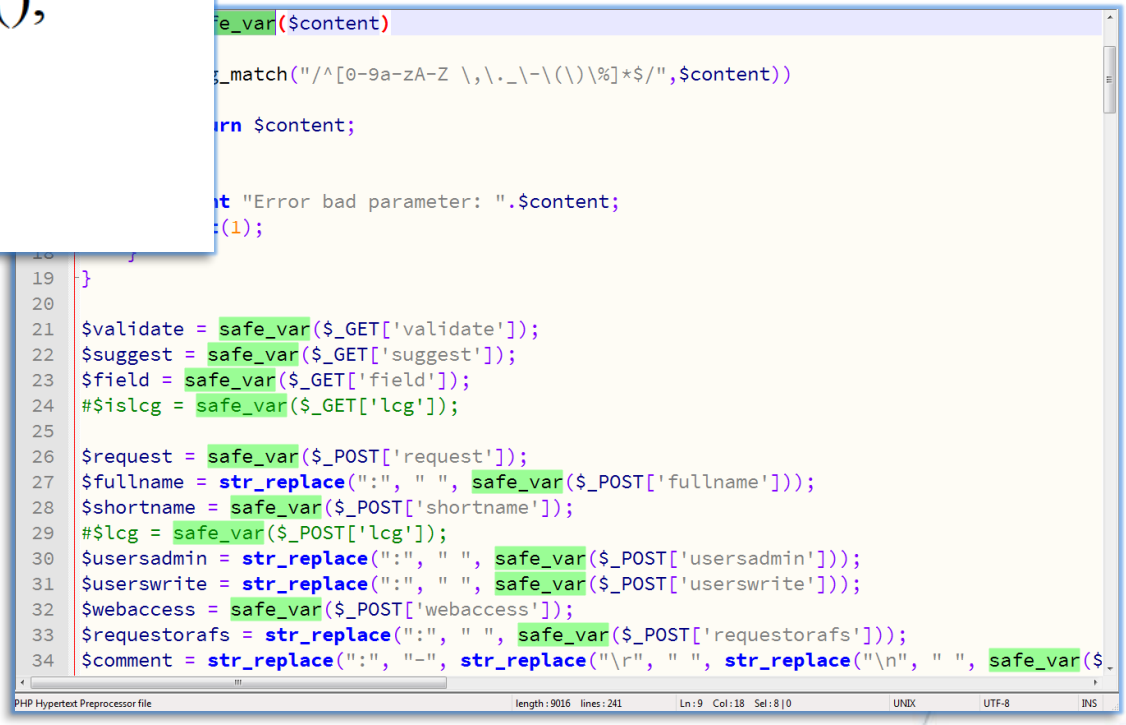
PHP Hypertext Preprocessor file | length : 9016 | lines : 241 | Ln : 9 | Col : 18 | Sel : 8 | 0 | UNIX | UTF-8 | INS

Detected Vulnerabilities



Detected Vulnerabilities

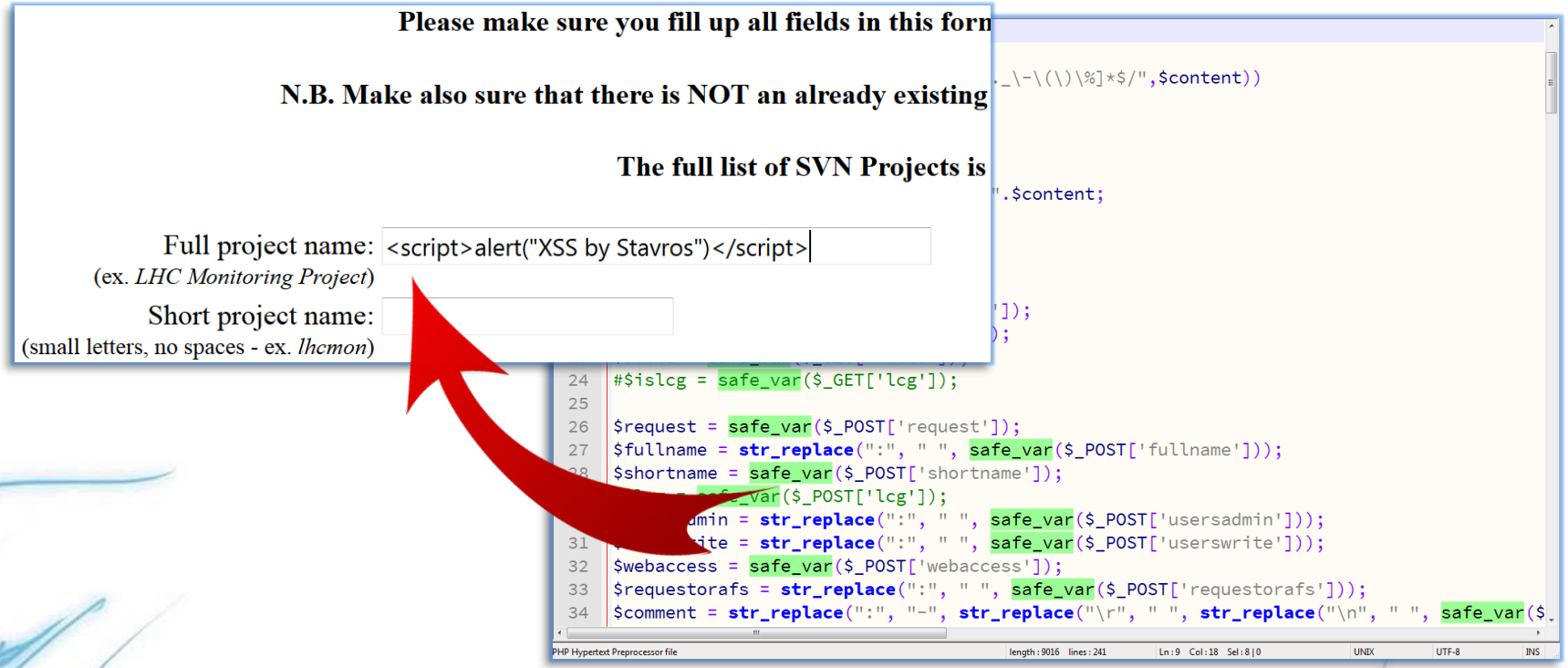
Error bad parameter: '"(),



```
fe_var($content)

g_match("/^[0-9a-zA-Z \,\._\-\(\)\%]*$/",$content))

urn $content;


nt "Error bad parameter: ".$content;
t(1);
}

$validate = safe_var($_GET['validate']);
$suggest = safe_var($_GET['suggest']);
$field = safe_var($_GET['field']);
#$islcg = safe_var($_GET['lcg']);

$request = safe_var($_POST['request']);
$fullname = str_replace(":", " ", safe_var($_POST['fullname']));
$shortname = safe_var($_POST['shortname']);
#$lcg = safe_var($_POST['lcg']);
$usersadmin = str_replace(":", " ", safe_var($_POST['usersadmin']));
$userswrite = str_replace(":", " ", safe_var($_POST['userswrite']));
$webaccess = safe_var($_POST['webaccess']);
$requestorafs = str_replace(":", " ", safe_var($_POST['requestorafs']));
$comment = str_replace(":", "-", str_replace("\r", " ", str_replace("\n", " ", safe_var($
```

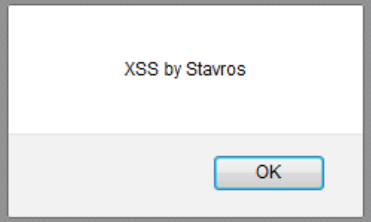
PHP Hypertext Preprocessor file | length : 9016 | lines : 241 | Ln : 9 | Col : 18 | Sel : 8 | 0 | UNIX | UTF-8 | INS

Exploitation



Exploitation

Error bad parameter:




```
]*$/",$content))

;

$suggest = safe_var($_GET['suggest']);
$field = safe_var($_GET['field']);
#$islcg = safe_var($_GET['lcg']);

$request = safe_var($_POST['request']);
$fullname = str_replace(":", " ", safe_var($_POST['fullname']));
$shortname = safe_var($_POST['shortname']);
#$lcg = safe_var($_POST['lcg']);
$usersadmin = str_replace(":", " ", safe_var($_POST['usersadmin']));
$userswrite = str_replace(":", " ", safe_var($_POST['userswrite']));
$webaccess = safe_var($_POST['webaccess']);
$requestorafs = str_replace(":", " ", safe_var($_POST['requestorafs']));
$comment = str_replace(":", "-", str_replace("\r", " ", str_replace("\n", " ", safe_var($
```

PHP Hypertext Preprocessor file | length : 9016 | lines : 241 | Ln : 9 | Col : 18 | Sel : 8 | 0 | UNIX | UTF-8 | INS

Exploitation

Error bad parameter:

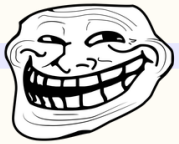
```
9  function safe_var($content)
10 {
11     if (preg_match("/^[0-9a-zA-Z \,\._\-\(\)\%]*$/",$content))
12     {
13         return $content;
14     }
15     else {
16         print "Error bad parameter: ".$content;
17         exit(1);
18     }
19 }
20
21 $validate = safe_var($_GET['validate']);
22 $suggest = safe_var($_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 $comment = str_replace(":", "-", str_replace("\r", " ", str_replace("\n", " ", safe_var($
```

PHP Hypertext Preprocessor file | length : 9016 lines : 241 | Ln : 16 Col : 47 Sel : 7 | 0 | UNIX | UTF-8 | INS

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 $comment = str_replace(":", "-", str_replace("\r", " ", str_replace("\n", " ", safe_var($
```



PHP Hypertext Preprocessor file | length : 9016 lines : 241 | Ln : 16 Col : 47 Sel : 7 | 0 | UNIX | UTF-8 | INS

Future Work

- Integration with Jenkins

Stavros Moiras

steve@vipersec.com