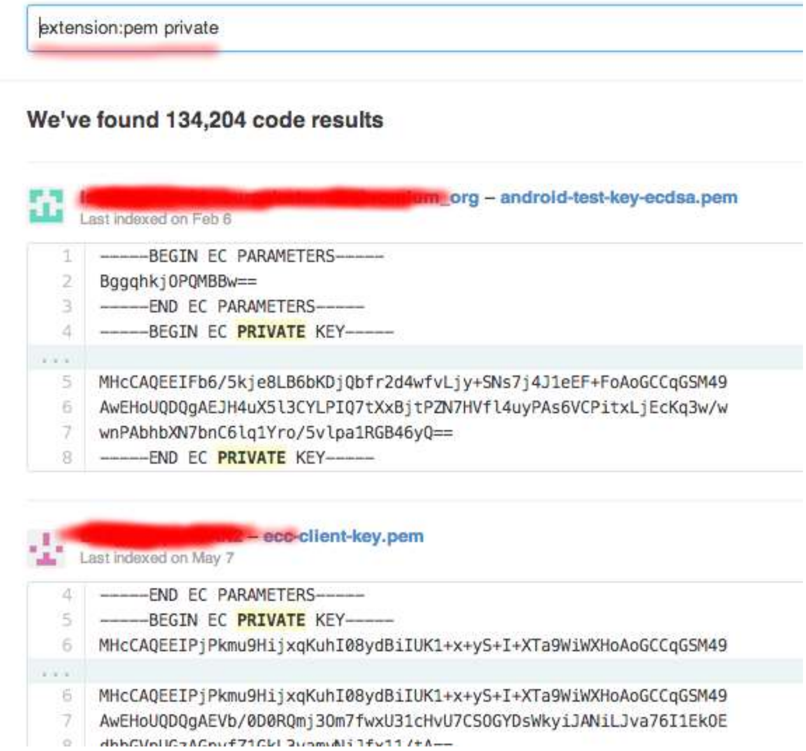
Github Hacking for fun and… sensitive data search!

19 de junho de 2013 / Conviso / Segurança de Aplicação / 0 comments

Conviso Research and Development Team is usually reading thousands and thousands of information daily and we make some filters and pay attention to some special words. We saw a very interesting post at Full Disclosure about advanced GitHub Search.

Right after reading what we shared in our internal list, this information and a little bit of Github Hacking proved that GitHub is a Disneyland of information leakage. We tried a lot of different searches and some interesting or I could say, VERY INTERESTING, as you see below.

Private Key



extension:pem private

We've found 134,204 code results

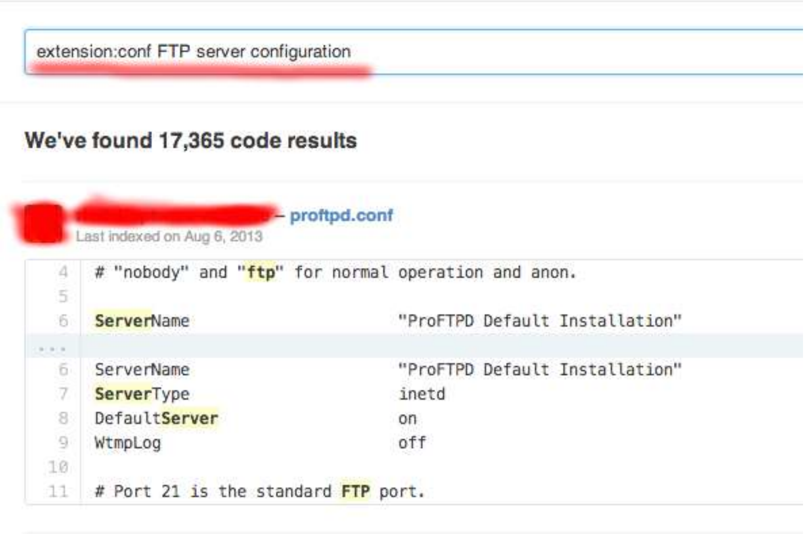
[redacted]_org – android-test-key-ecdsa.pem
Last indexed on Feb 6

```
-----BEGIN EC PARAMETERS-----
BggqhkjOPQMBBw==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
...
MHcCAQEEIFb6/5kje8LB6bKDjQbfr2d4wfvLjy+SNs7j4J1eEF+FoAoGCCqGSM49
AwEHoUQDQgAEJH4uX5l3CYLPIQ7tXxBjtPZN7HVfl4uyPAs6VCPitxLjEcKq3w/w
wnPAbhbXN7bnC6lq1Yro/5vlpa1RGB46yQ==
-----END EC PRIVATE KEY-----
```

[redacted] – ecc-client-key.pem
Last indexed on May 7

```
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIPjPkmu9HijxqKuhI08ydBiIUK1+x+yS+I+XTa9WiWXHoAoGCCqGSM49
...
MHcCAQEEIPjPkmu9HijxqKuhI08ydBiIUK1+x+yS+I+XTa9WiWXHoAoGCCqGSM49
AwEHoUQDQgAEVb/0D0RQmj3Om7fwxU31cHvU7CSOGYDsWkyiJANiLJva76I1EkOE
dbbGVpUGzAGpvf71GkL3vamyNi1fx11/tA==
```

FTP information



extension:conf FTP server configuration

We've found 17,365 code results

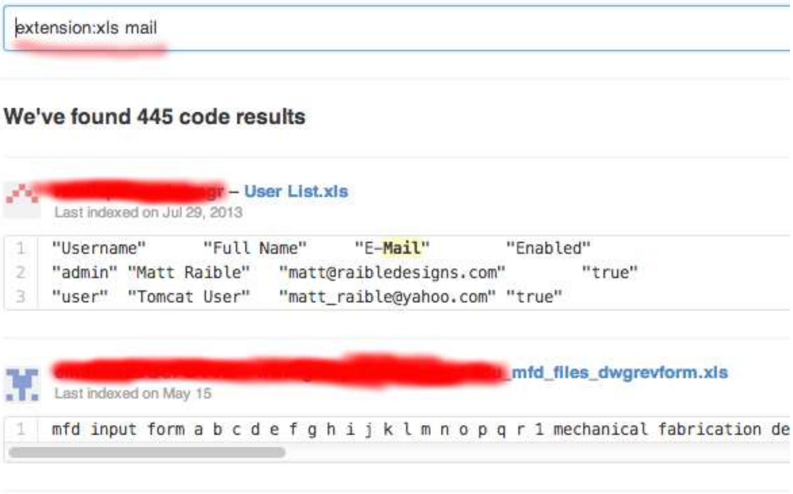
[redacted] – proftpd.conf
Last indexed on Aug 6, 2013

```
# "nobody" and "ftp" for normal operation and anon.

ServerName                      "ProFTPD Default Installation"
...
ServerName                      "ProFTPD Default Installation"
ServerType                      inetd
DefaultServer                   on
WtmpLog                         off

# Port 21 is the standard FTP port.
```

E-mail information



extension:xls mail

We've found 445 code results

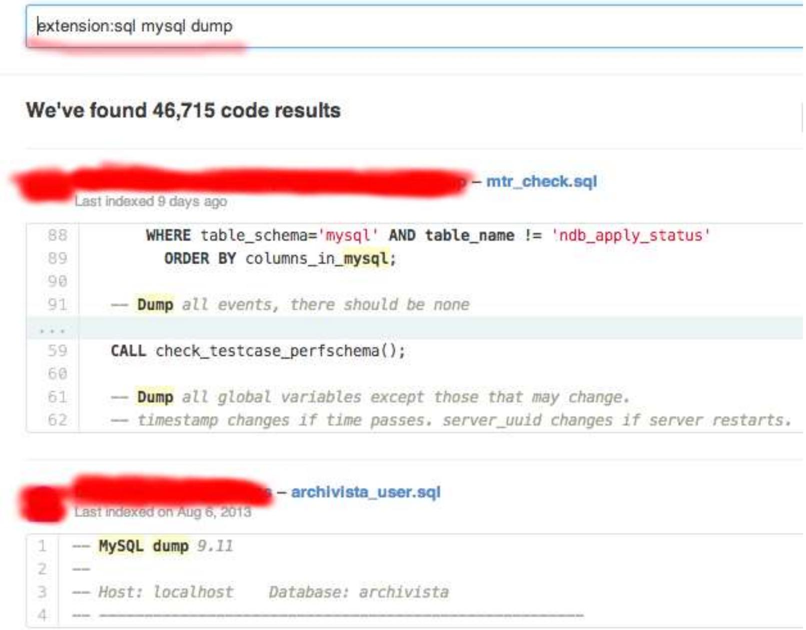
[redacted] – User List.xls
Last indexed on Jul 29, 2013

```
"Username"      "Full Name"      "E-Mail"        "Enabled"
"admin" "Matt Raible"   "matt@raibledesigns.com"        "true"
"user"  "Tomcat User"   "matt_raible@yahoo.com" "true"
```

[redacted]_mfd_files_dwgrevform.xls
Last indexed on May 15

```
mfd input form a b c d e f g h i j k l m n o p q r 1 mechanical fabrication de
```

MySQL Password / History



extension:sql mysql dump

We've found 46,715 code results

[redacted] – mtr_check.sql
Last indexed 9 days ago

```
    WHERE table_schema='mysql' AND table_name != 'ndb_apply_status'
      ORDER BY columns_in_mysql;

  -- Dump all events, there should be none
...
  CALL check_testcase_perfschema();

  -- Dump all global variables except those that may change.
  -- timestamp changes if time passes. server_uuid changes if server restarts.
```

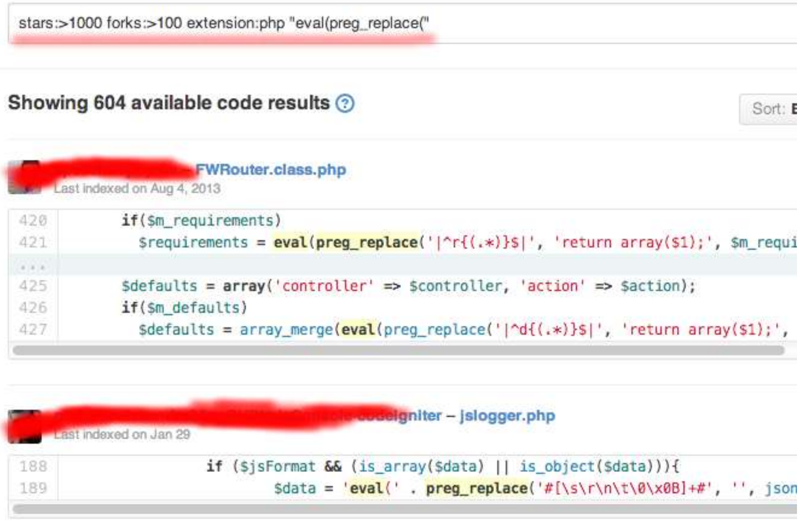
[redacted] – archivista_user.sql
Last indexed on Aug 6, 2013

```
-- MySQL dump 9.11
--
-- Host: localhost    Database: archivista
-- ------------------------------------------------------
```

How about finding some possible 0days? Backdoors? Hell yeah! It's possible too.
Check out this GitHub "Dork":

```
stars:>1000 forks:>100 extension:php "eval(preg_replace("
```

We searched for big projects who have more than 1000 stars, 100 forks, files with PHP extension and a possible flaw that allows Remote Code Execution.



stars:>1000 forks:>100 extension:php "eval(preg_replace("

Showing 604 available code results

Sort: E

[redacted]FWRouter.class.php
Last indexed on Aug 4, 2013

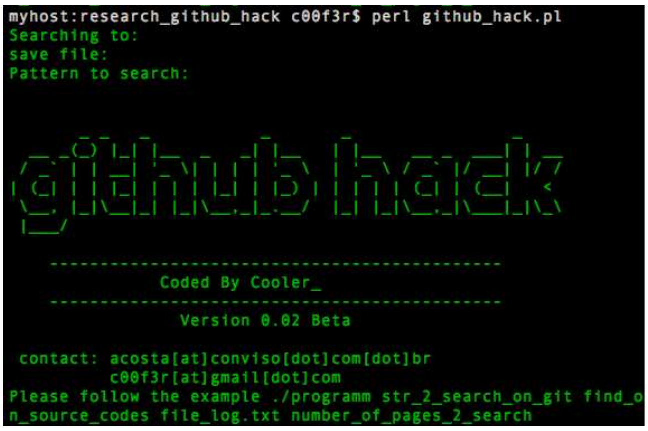
```
        if($m_requirements)
          $requirements = eval(preg_replace('|^r{(.*)}$|', 'return array($1);', $m_requi
...
        $defaults = array('controller' => $controller, 'action' => $action);
        if($m_defaults)
          $defaults = array_merge(eval(preg_replace('|^d{(.*)}$|', 'return array($1);',
```

[redacted] – jslogger.php
Last indexed on Jan 29

```
                if ($jsFormat && (is_array($data) || is_object($data))){
                        $data = 'eval(' . preg_replace('#[\s\r\n\t\0\x0B]+#', '', json
```

Check out other prefixes that might help you keeping your search improved GitHub Search Cheat Sheet. Lots of FUN isn't ? We could probably find just about anything, the sky is the limit!

So to make our lives easier we developed a tool to grab those information in a more automated way:



```
myhost:research_github_hack c00f3r$ perl github_hack.pl
Searching to:
save file:
Pattern to search:


       _ _   _           _       _                _
  __ _(_) |_| |__  _   _| |__   | |__   __ _  ___| | __
 / _` | | __| '_ \| | | | '_ \  | '_ \ / _` |/ __| |/ /
| (_| | | |_| | | | |_| | |_) | | | | | (_| | (__|   <
 \__, |_|\__|_| |_|\__,_|_.__/  |_| |_|\__,_|\___|_|\_\
 |___/

    ------------------------------------------------
                  Coded By Cooler_
    ------------------------------------------------
                     Version 0.02 Beta

 contact: acosta[at]conviso[dot]com[dot]br
          c00f3r[at]gmail[dot]com
Please follow the example ./programm str_2_search_on_git find_o
n_source_codes file_log.txt number_of_pages_2_search
```

You can check the code and download it from here (but keep in mind that it is still in beta version).

Take care about what information you share. Lots of sensitive information could probably be over there. Search for information about your company before the bad guys do.

Originalmente postado no Blog da Conviso Application Security – Siga-nos no Twitter @conviso Google+

Like 0 G+1

TAGS Ferramentas

Autor: Conviso

POSTAGENS RELACIONADAS

4 erros de segurança de dados para evitar

Segurança de aplicações: investimento ou custo?