Source code audit speed run

Bsides Canberra 2019

xen1thLabs

A DARKMATTER COMPANY

SMART AND SAFE DIGITAL

Content

01 Introduction

02 Theory

03 Vulnerabilities

04 Auditing

05 Vulnerability speed run

06 Conclusion

01

Introduction

Source code review

Code review (sometimes referred to as peer **review**) is a software quality assurance activity in which one or several humans check a program mainly by viewing and reading parts of its source **code**, and they do so after implementation or as an interruption of implementation.

Wikipedia

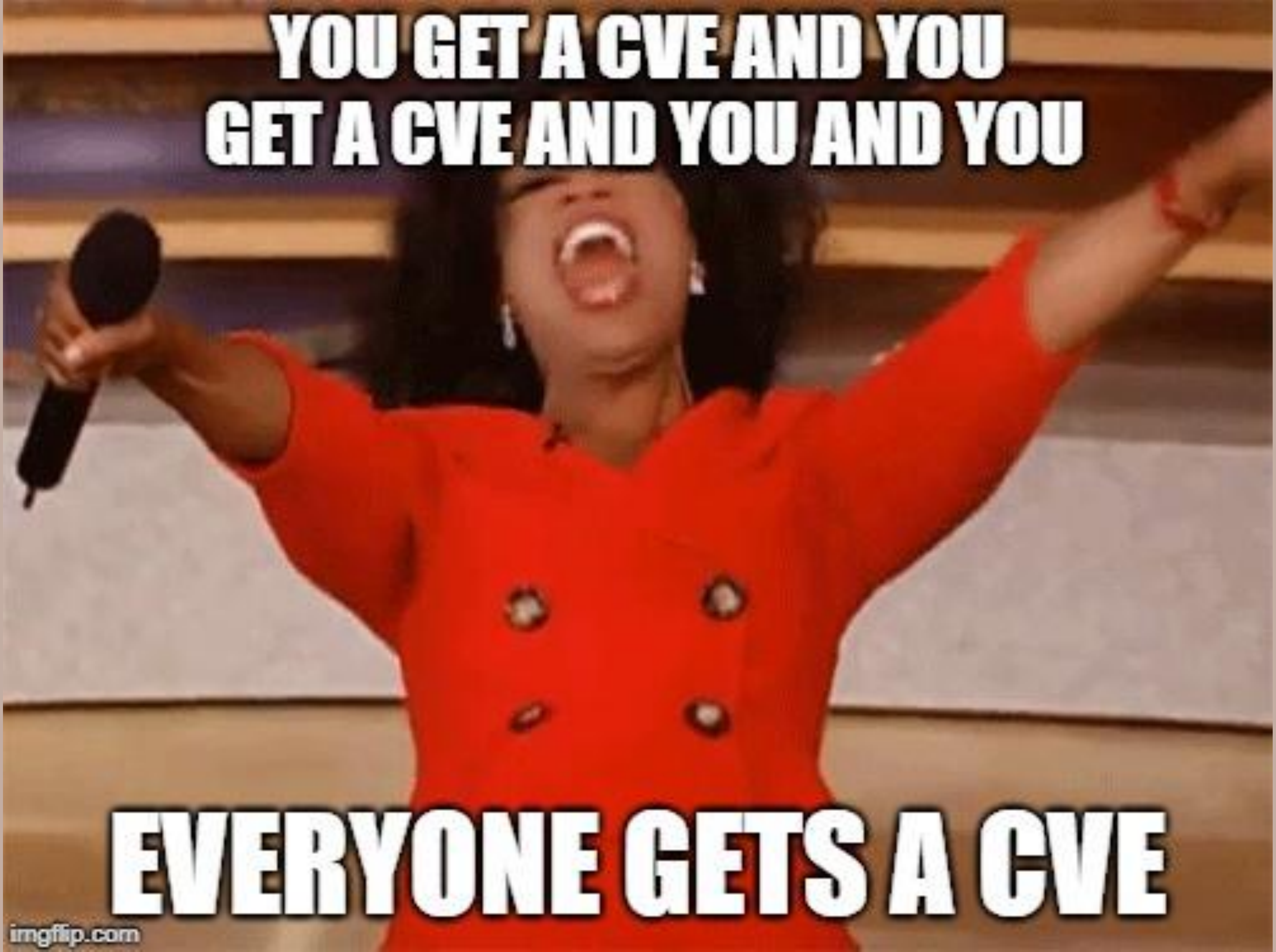
Security code review is the process of auditing the source code for an application to verify that the proper security controls are present, that they work as intended, and that they have been invoked in all the right places.

OWASP

Speed run is a play-through (or a recording thereof) of a video game performed with the intention of completing it as fast as possible.

Wikipedia

Introduce concepts to identify vulnerabilities in source code **fast**


YOU GET A CVE AND YOU GET A CVE AND YOU AND YOU
EVERYONE GETS A CVE
imgflip.com

`whoami`

Eldar Marcussen

Lead security researcher

Proven history of performing security research that result in 0day vulnerabilities, conference presentation and security tools. I have written a source code scanner and auditing source code is often part of my security research process. My past research and security tools have also featured in industry related cyber security text books.

A former

- Developer
- System administrator
- Penetration tester

Currently

- Husband and Father
- Security researcher
- Trainer

02

Theory

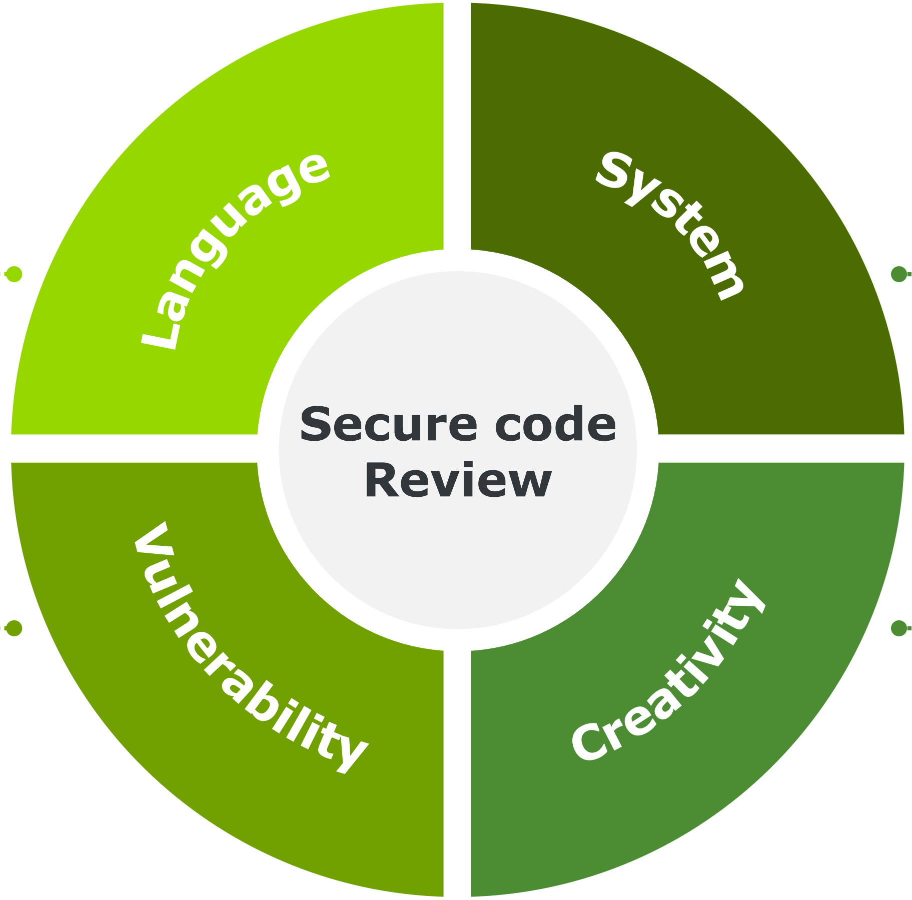
Code review is a skill

-- The Art Of Software Security Assessment

Skills and knowledge

Many security problems require in-depth knowledge of the language

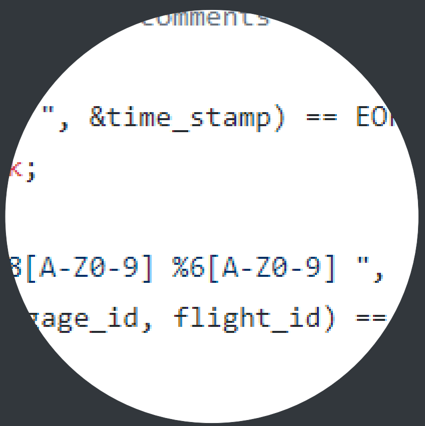
Understanding vulnerabilities helps identify their presence in source code



Knowledge about the system in use is helpful, size limits, permissions model, etc.

Many times you need to think outside of the box to identify and exploit vulnerabilities

```c
while (1) {
        unsigned int time_stamp;
        char luggage_id[LUGGAGE_ID_LENGTH + 1];
        char flight_id[FLIGHT_ID_LENGTH + 1];
        char departure[AIRPORT_CODE_LENGTH + 1];
        char arrival[AIRPORT_CODE_LENGTH + 1];
        char comments[COMMENTS_LENGTH + 1];
        comments[0] = 0; // comments are optional.

        if (scanf("%d ", &time_stamp) == EOF) {
                break;
        }
        if (scanf("%8[A-Z0-9] %6[A-Z0-9] ",
                  luggage_id, flight_id) == EOF) {
                break;
        }
        if (scanf("%3[A-Z] %3[A-Z]", departure, arrival) == EOF) {
                break;
        }
        if (scanf("%80[^\n]", comments) == EOF) {
                break;
        }

        RoutingDirective *new_directive =
                (RoutingDirective*) calloc(1, sizeof(RoutingDirective));
        new_directive->time_stamp = time_stamp;
        strcpy(new_directive->luggage_id, luggage_id);
        strcpy(new_directive->flight_id, flight_id);
```



```
comments

", &time_stamp) == EO
k;

8[A-Z0-9] %6[A-Z0-9] ",
age_id, flight_id) ==
```

Theory

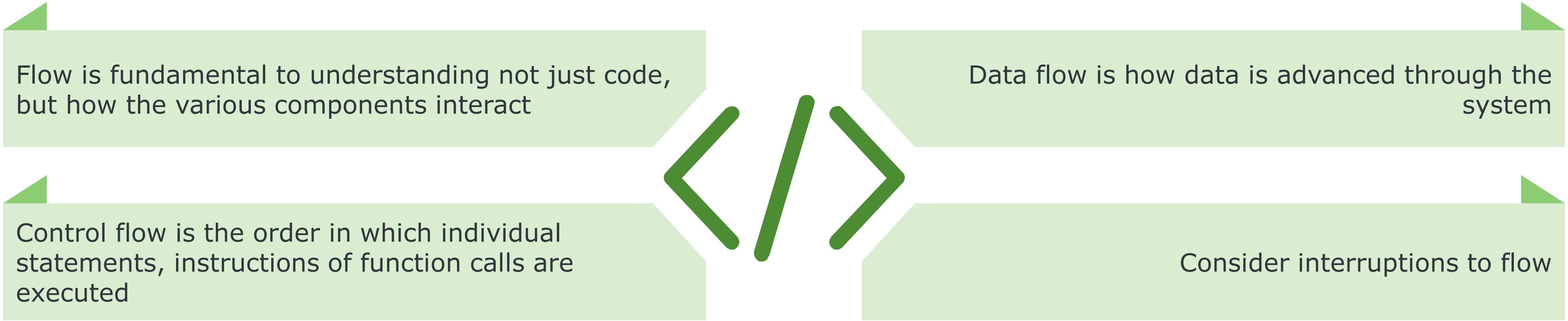
Considerations

- Systems don’t exist in a vacuum
  - ➢ Race conditions
  - ➢ PHP configuration
- Compiler optimizations can introduce vulnerabilities

Limitations

- Dynamic evaluation
- Callbacks
- Dynamic data operations

Flow



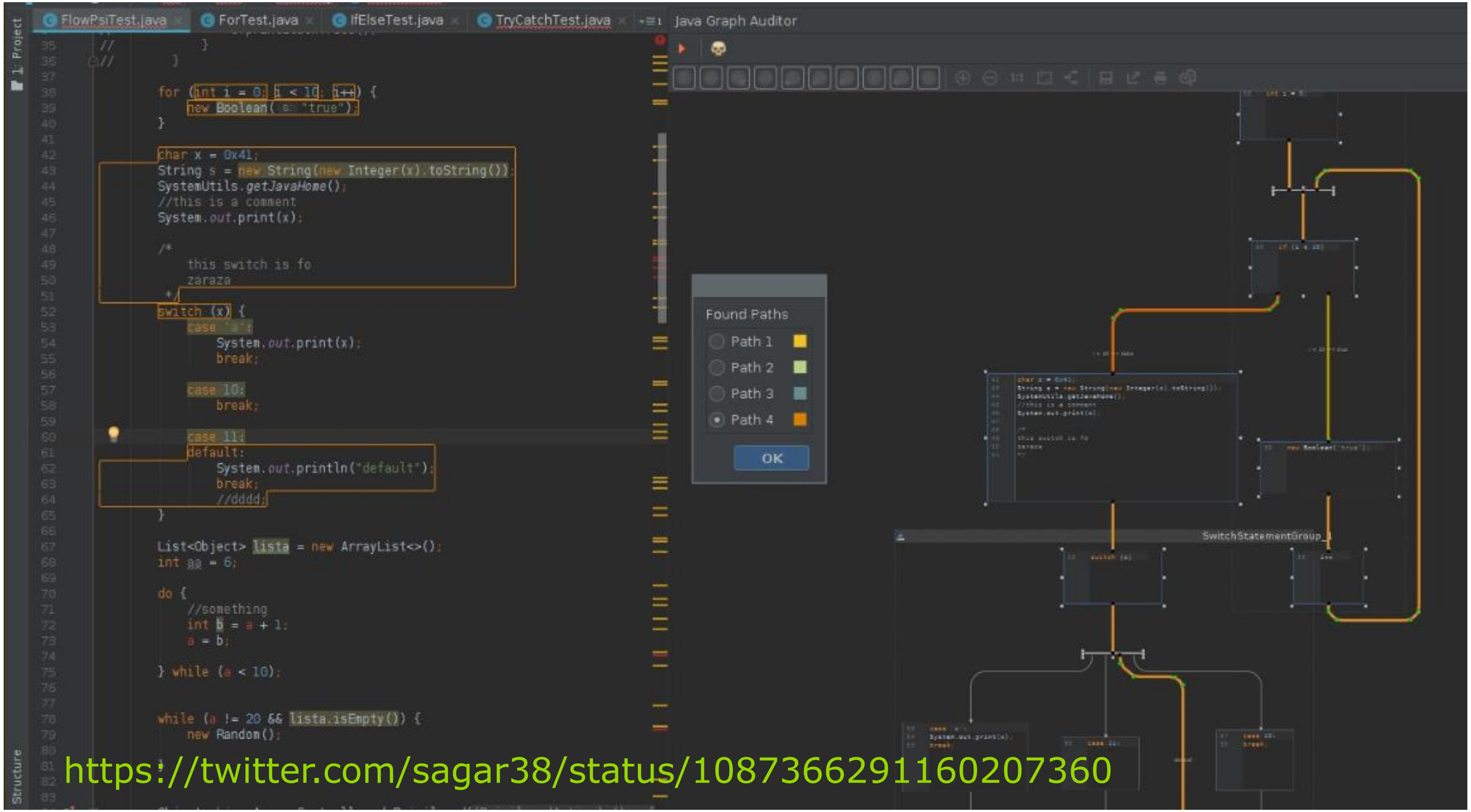
Flow is fundamental to understanding not just code, but how the various components interact

Data flow is how data is advanced through the system

Control flow is the order in which individual statements, instructions of function calls are executed

Consider interruptions to flow

Code flow graph



```
//        }
//    }

    for (int i = 0; i < 10; i++) {
        new Boolean( s: "true");
    }

    char x = 0x41;
    String s = new String(new Integer(x).toString());
    SystemUtils.getJavaHome();
    //this is a comment
    System.out.print(x);

    /*
        this switch is fo
        zaraza
     */
    switch (x) {
        case 'a':
            System.out.print(x);
            break;

        case 10:
            break;

        case 11:
        default:
            System.out.println("default");
            break;
            //dddd;
    }

    List<Object> lista = new ArrayList<>();
    int aa = 6;

    do {
        //something
        int b = a + 1;
        a = b;

    } while (a < 10);


    while (a != 20 && lista.isEmpty()) {
        new Random();

    }
```

Found Paths

○ Path 1 🟨
○ Path 2 🟩
○ Path 3 🟦
● Path 4 🟧

OK

https://twitter.com/sagar38/status/1087366291160207360

Flow

Source

- The origin of the data as it enters the flow is the **“source”**
- Usually we only care about sources that introduce untrusted or user supplied data
- **Identifying user controlled data is not always simple**

Sink

- The function that the data ends up in is the **“sink”**
- The only sinks worth tracking is functions that must receive clean data
- **The source to sink flow may not direct or even intended to exist**

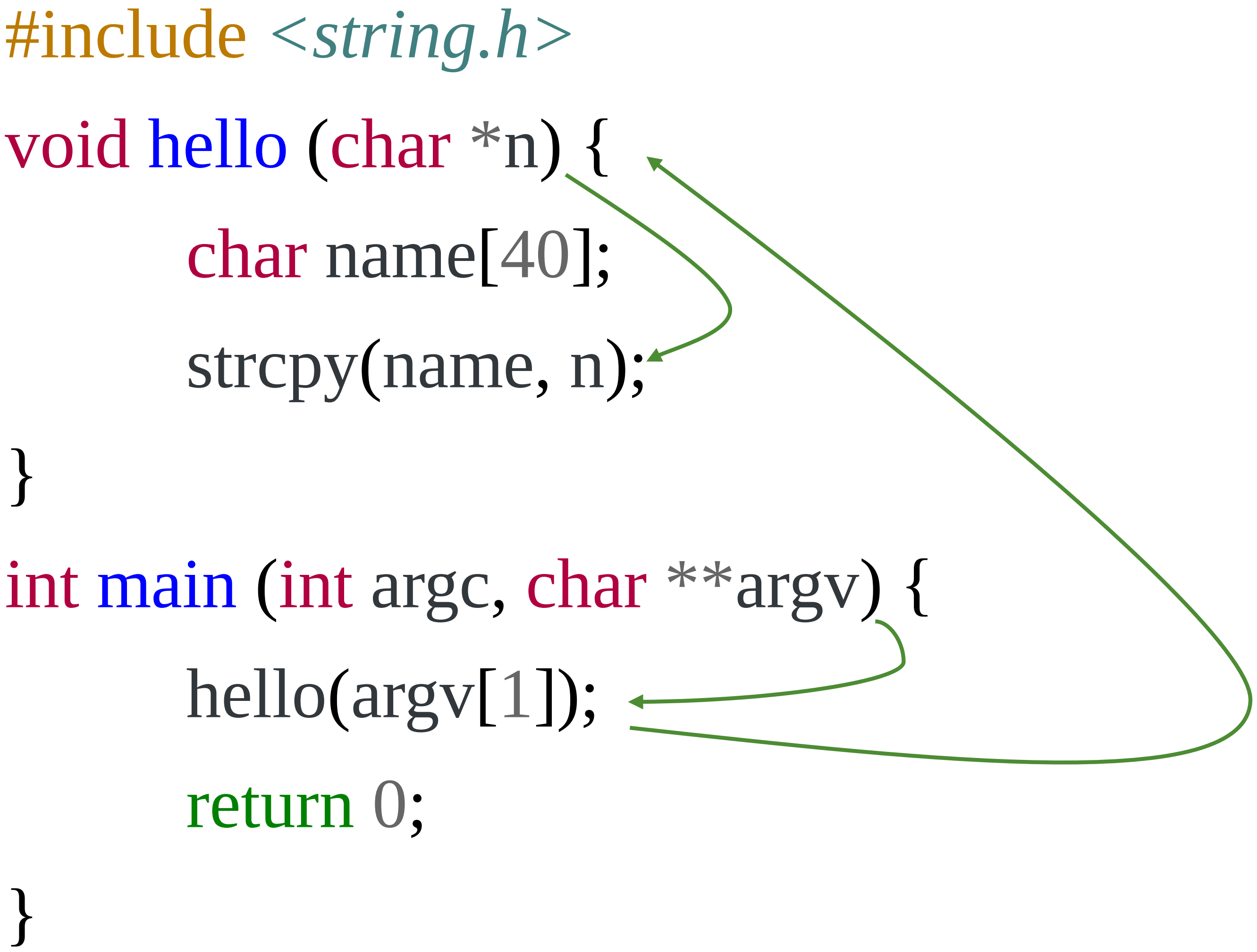
Other

- Trust boundaries
- State change

Taint analysis

```
#include <string.h>
void hello (char *n) {
        char name[40];
        strcpy(name, n);
}
int main (int argc, char **argv) {
        hello(argv[1]);
        return 0;
}
```

Taint analysis



```
#include <string.h>
void hello (char *n) {
        char name[40];
        strcpy(name, n);
}
int main (int argc, char **argv) {
        hello(argv[1]);
        return 0;
}
```

Approaches

Hot spot checking

Control flow sensitive

Data flow sensitive

Focus oriented

Forward tracing

Backwards tracing

03
Vulnerabilities

Vulnerability

> The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved.
>
> *ENISA*

Vulnerability classifaction

OWASP Top10

- While some are broad, it is only 10 categories of bugs
- Semi-static
- Based on commonality, not risk or impact
- Silos
  - ➢ Top10 Web
  - ➢ Top10 Mobile
- https://www.owasp.org/

Common Weakness Enumeration (CWE)

- Has classified 716 software weaknesses
- Typically has a good definition with source code examples and description
- https://cwe.mitre.org/

Other

- Web Application Security Consortium
- Detailed advisories
- White papers
- Conference presentations

Identifying weaknesses

- Read the documentation
- Learn to recognize weakness patterns in source code
- Learn to recognize weakness patterns in design/process
- Anticipate poor decision making
- Implement short test cases to verify behavior if unsure
- Take breaks from complex/difficult code

Presence of something

The code contains a flaw

Logical or functional

Examples:

- Insecure default variable value
- Format string
- Double free()

Absence of something

When the lack of code causes the vulnerability

Examples:

- Not halting execution
- Not encoding user supplied output in html/javascript/ whatever context
- Not using boundary checks

04
Auditing

Objectives

1 Identify weaknesses

2 Prioritize high impact vulnerabilities

3 Check exploitability

Tools

- STATIC SOURCE CODE ANALYSIS TOOLS
  - ➢ https://github.com/mre/awesome-static-analysis
  - ➢ https://www.owasp.org/index.php/Source_Code_Analysis_Tools
- **GREP**
- TOOLS CANNOT FIND SOME TYPES OF VULNERABILITIES
- **HUMAN ANALYSIS IS REQUIRED**

Not greps

Ack

Ag
(the silver
searcher)

ripgrep

more

Benefits of grep

- Can be used on incomplete code
- Cross platform support
- Text matching supports most programming languages
- Easy support for templating languages of custom framework APIs
- Regular expression support for better matching
- Text matching supports most programming languages
- Presents user with code view
- Versatile use due to large number of command line options

memsad

```
memset[[:space:]]*\([^,]+,[[:0,.*\);

memset[[:space:]]*\([^,]+,[^,]+,[[:space:]]*0\);
```

Wordpress rules

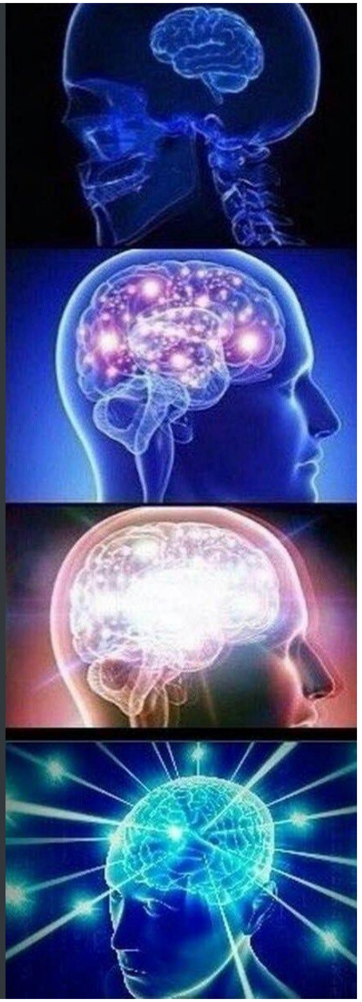
```
_weak_escape

_do_query

\$_(GET|POST|REQUEST|COOKIE|SERVER)

\$[^\,\;\(\> ]+\->prepare[[:space:]]*\(.*\$.*

\$[^\,\;\(\> ]+\->get_(row|col|var|results).*\$.*

\$[^\,\;\(\> ]+\->get_param.*\$.*

\$[^\,\;\(\> ]+\->get_body_param.*\$.*

\$[^\,\;\(\> ]+\->get_header.*

\$[^\,\;\(\> ]+\->get_json_params.*

\$[^\,\;\(\> ]+\->get_file_params.*

\$[^\,\;\(\> ]+\->get_query_param.*
```

Regular expressions

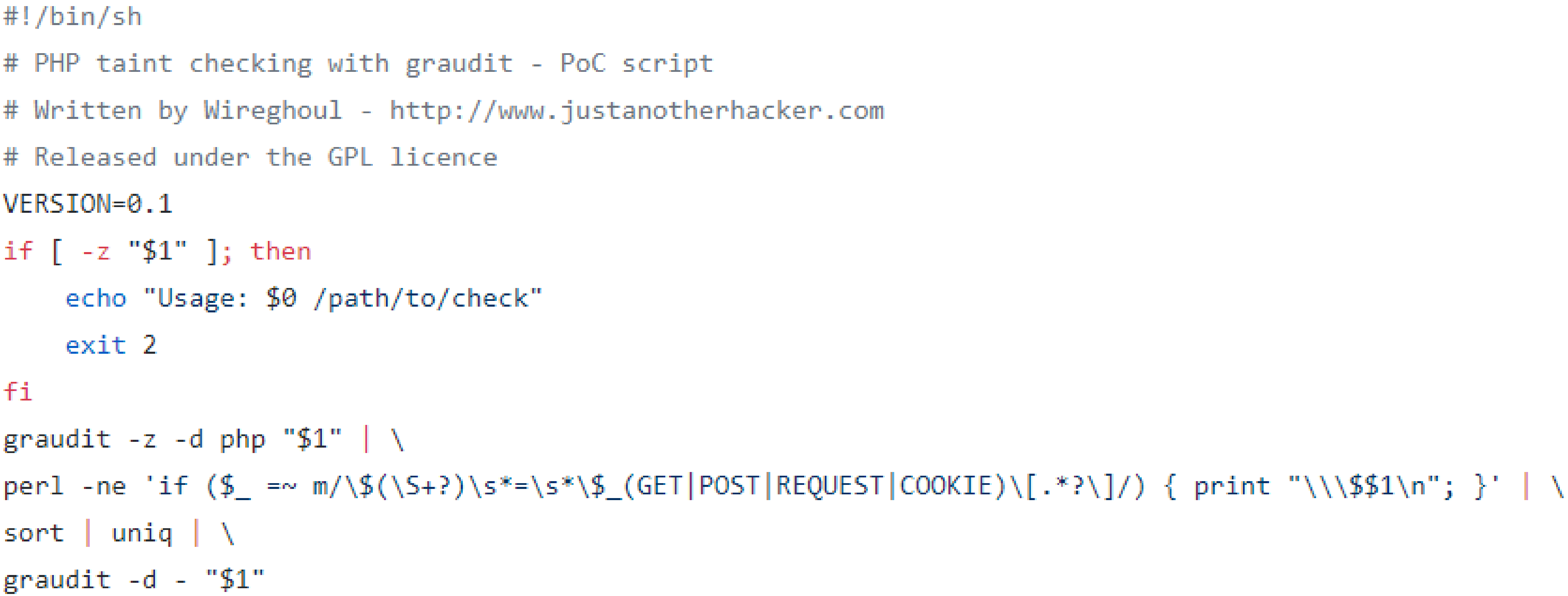
WHENEVER I LEARN A NEW SKILL I CONCOCT ELABORATE FANTASY SCENARIOS WHERE IT LETS ME SAVE THE DAY.
OH NO! THE KILLER MUST HAVE FOLLOWED HER ON VACATION!
BUT TO FIND THEM WE'D HAVE TO SEARCH THROUGH 200 MB OF EMAILS LOOKING FOR SOMETHING FORMATTED LIKE AN ADDRESS!
IT'S HOPELESS!
EVERYBODY STAND BACK.
I KNOW REGULAR EXPRESSIONS.
PERL!
TAP TAP

Rules/Regular expressions

```
require

require\(.*\$.*\);

(require|require_once)\(.*\$.*\);

require(_once)?[[:space:]]*(\(|\’\”).*\$_(GET|POST|REQUEST|ENV|COOKIE).*(\)|\’|\”)\;
```



Taint analysis with grep



```
#!/bin/sh
# PHP taint checking with graudit - PoC script
# Written by Wireghoul - http://www.justanotherhacker.com
# Released under the GPL licence
VERSION=0.1
if [ -z "$1" ]; then
    echo "Usage: $0 /path/to/check"
    exit 2
fi
graudit -z -d php "$1" | \
perl -ne 'if ($_ =~ m/\$(\S+?)\s*=\s*\$_(GET|POST|REQUEST|COOKIE)\[.*?\]/) { print "\\\$$1\n"; }' | \
sort | uniq | \
graudit -d - "$1"
```

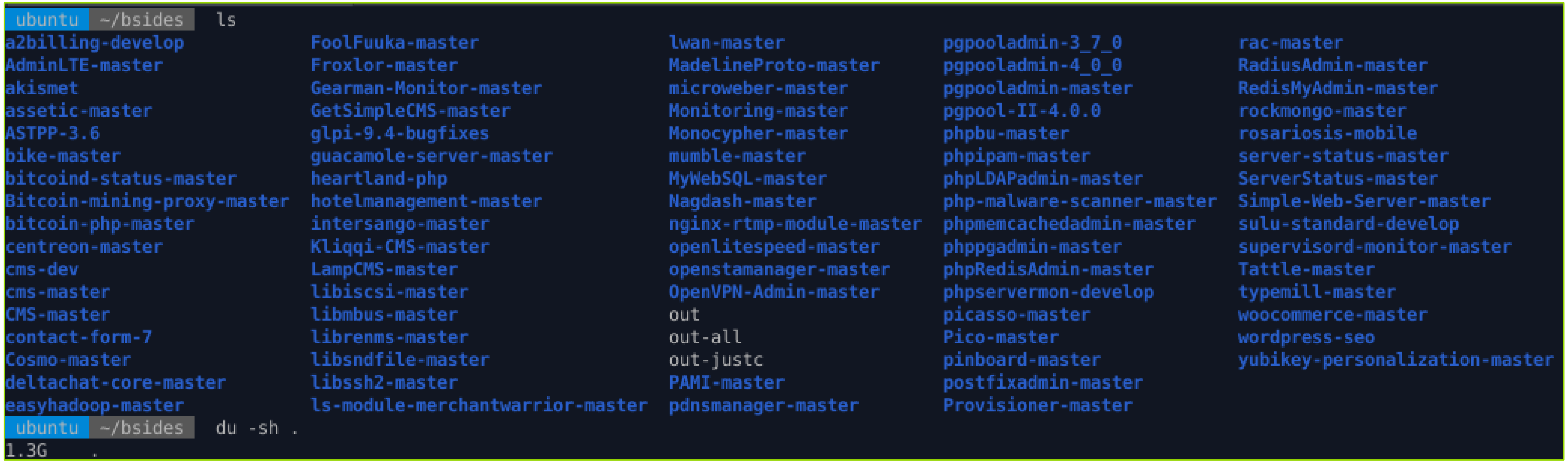
Quickly build custom scripts

```
#!/bin/sh

echo "function.*__(wakeup|destruct|autoload)[[:space:]]*\\(" | \

graudit –x *.js -d - -- -A 20 $1 | \

graudit –c 30 -d php -
```

05

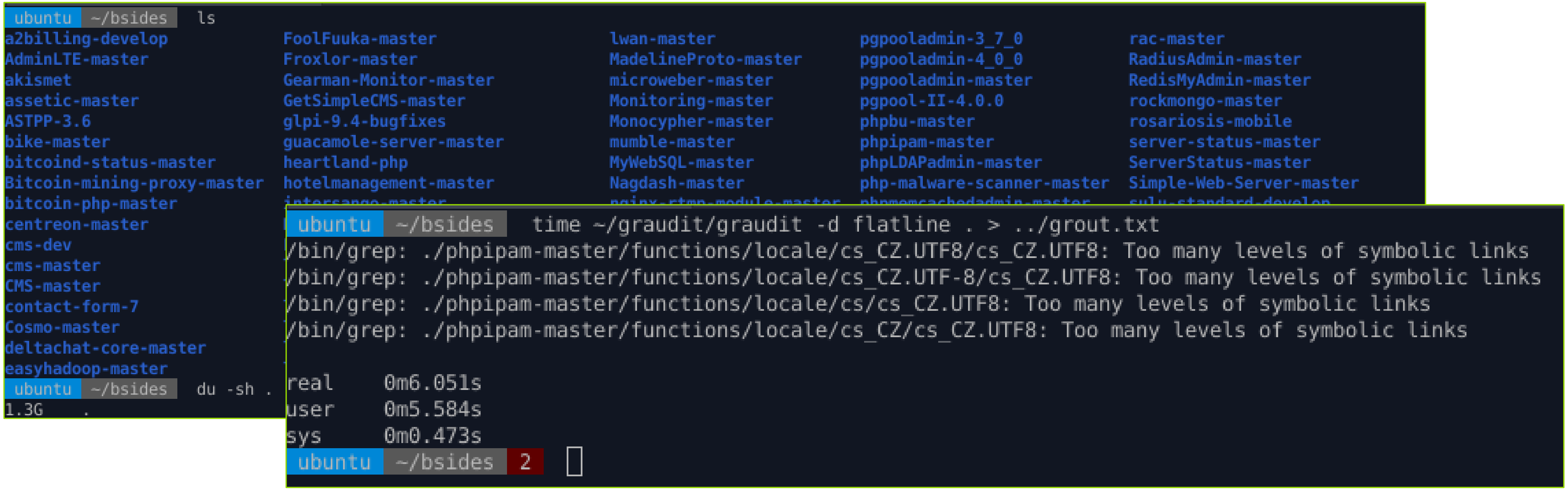
Vulnerability speed run

Computer time



```
ubuntu  ~/bsides   ls
a2billing-develop            FoolFuuka-master                  lwan-master               pgpooladmin-3_7_0           rac-master
AdminLTE-master              Froxlor-master                    MadelineProto-master      pgpooladmin-4_0_0           RadiusAdmin-master
akismet                      Gearman-Monitor-master            microweber-master         pgpooladmin-master          RedisMyAdmin-master
assetic-master               GetSimpleCMS-master               Monitoring-master         pgpool-II-4.0.0             rockmongo-master
ASTPP-3.6                    glpi-9.4-bugfixes                 Monocypher-master         phpbu-master                rosariosis-mobile
bike-master                  guacamole-server-master           mumble-master             phpipam-master              server-status-master
bitcoind-status-master       heartland-php                     MyWebSQL-master           phpLDAPadmin-master         ServerStatus-master
Bitcoin-mining-proxy-master  hotelmanagement-master            Nagdash-master            php-malware-scanner-master  Simple-Web-Server-master
bitcoin-php-master           intersango-master                 nginx-rtmp-module-master  phpmemcachedadmin-master    sulu-standard-develop
centreon-master              Kliqqi-CMS-master                 openlitespeed-master      phppgadmin-master           supervisord-monitor-master
cms-dev                      LampCMS-master                    openstamanager-master     phpRedisAdmin-master        Tattle-master
cms-master                   libiscsi-master                   OpenVPN-Admin-master      phpservermon-develop        typemill-master
CMS-master                   libmbus-master                    out                       picasso-master              woocommerce-master
contact-form-7               librenms-master                   out-all                   Pico-master                 wordpress-seo
Cosmo-master                 libsndfile-master                 out-justc                 pinboard-master             yubikey-personalization-master
deltachat-core-master        libssh2-master                    PAMI-master               postfixadmin-master
easyhadoop-master            ls-module-merchantwarrior-master  pdnsmanager-master        Provisioner-master
ubuntu  ~/bsides   du -sh .
1.3G    .
```

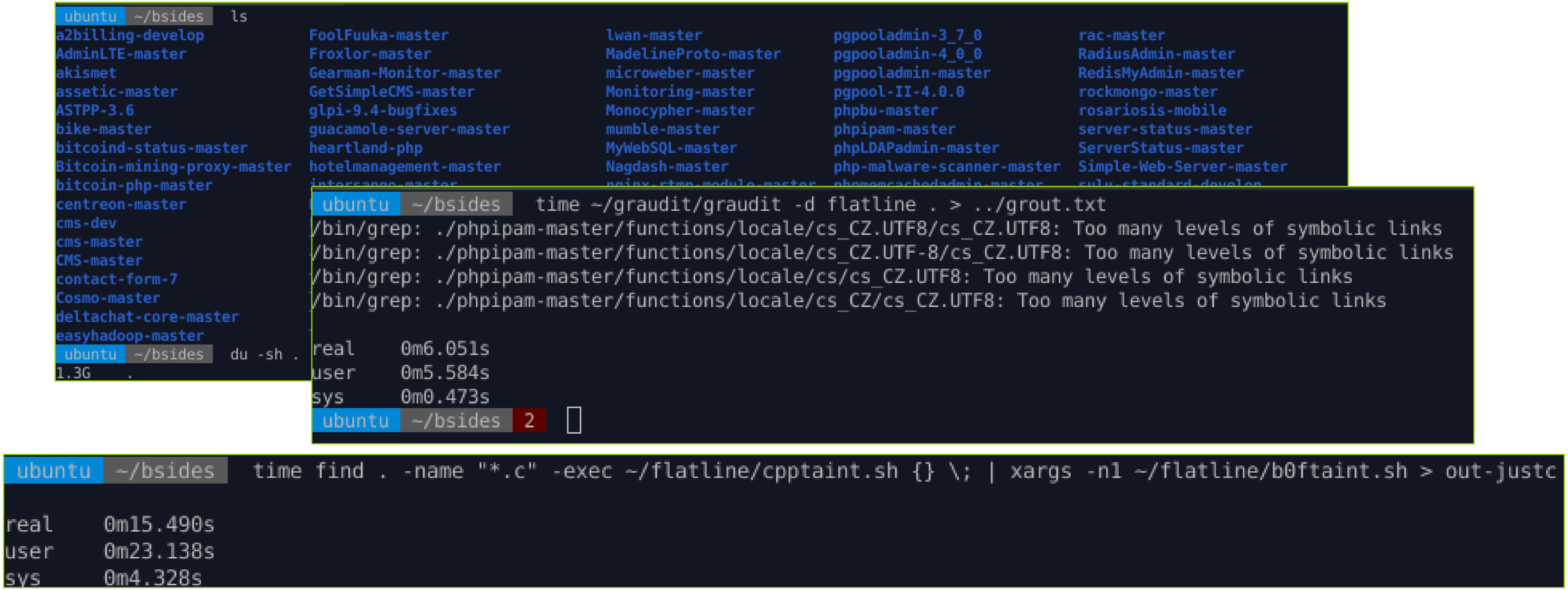
Computer time



```
ubuntu  ~/bsides   ls
a2billing-develop           FoolFuuka-master           lwan-master               pgpooladmin-3_7_0            rac-master
AdminLTE-master             Froxlor-master             MadelineProto-master      pgpooladmin-4_0_0            RadiusAdmin-master
akismet                     Gearman-Monitor-master     microweber-master         pgpooladmin-master           RedisMyAdmin-master
assetic-master              GetSimpleCMS-master        Monitoring-master         pgpool-II-4.0.0              rockmongo-master
ASTPP-3.6                   glpi-9.4-bugfixes          Monocypher-master         phpbu-master                 rosariosis-mobile
bike-master                 guacamole-server-master    mumble-master             phpipam-master               server-status-master
bitcoind-status-master      heartland-php              MyWebSQL-master           phpLDAPadmin-master          ServerStatus-master
Bitcoin-mining-proxy-master hotelmanagement-master     Nagdash-master            php-malware-scanner-master   Simple-Web-Server-master
bitcoin-php-master          intersango-master          nginx-rtmp-module-master  phpmemcachedadmin-master     sulu-standard-develop
centreon-master
cms-dev
cms-master
CMS-master
contact-form-7
Cosmo-master
deltachat-core-master
easyhadoop-master
ubuntu  ~/bsides   du -sh .
1.3G    .
```

```
ubuntu  ~/bsides   time ~/graudit/graudit -d flatline . > ../grout.txt
/bin/grep: ./phpipam-master/functions/locale/cs_CZ.UTF8/cs_CZ.UTF8: Too many levels of symbolic links
/bin/grep: ./phpipam-master/functions/locale/cs_CZ.UTF-8/cs_CZ.UTF8: Too many levels of symbolic links
/bin/grep: ./phpipam-master/functions/locale/cs/cs_CZ.UTF8: Too many levels of symbolic links
/bin/grep: ./phpipam-master/functions/locale/cs_CZ/cs_CZ.UTF8: Too many levels of symbolic links

real    0m6.051s
user    0m5.584s
sys     0m0.473s
ubuntu  ~/bsides  2  
```

Computer time



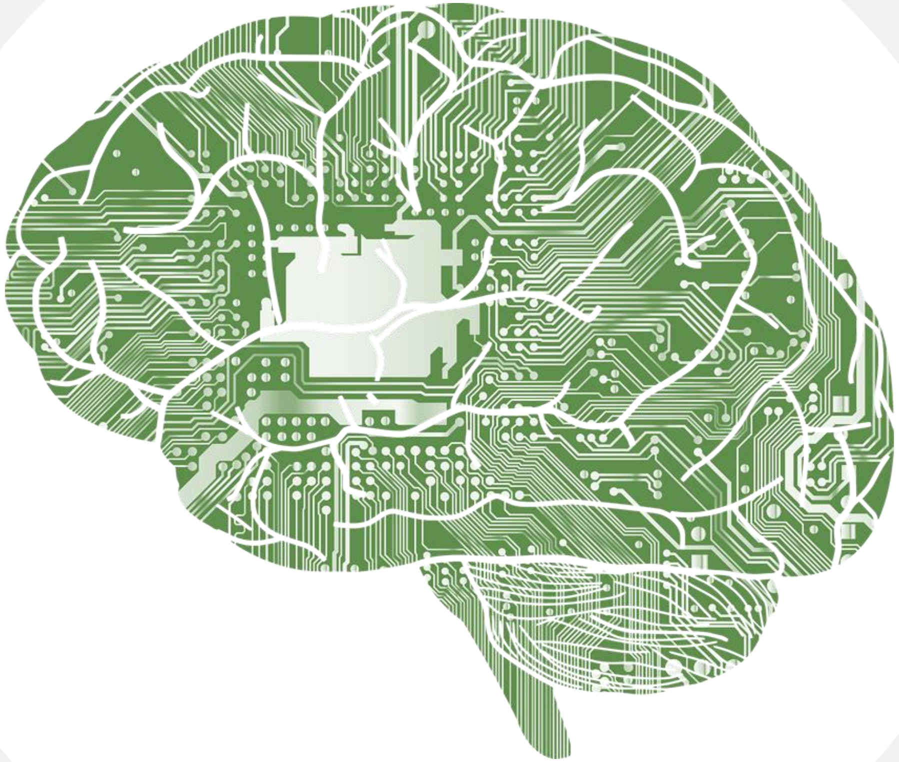
```
ubuntu  ~/bsides   ls
a2billing-develop           FoolFuuka-master           lwan-master               pgpooladmin-3_7_0            rac-master
AdminLTE-master             Froxlor-master             MadelineProto-master      pgpooladmin-4_0_0            RadiusAdmin-master
akismet                     Gearman-Monitor-master     microweber-master         pgpooladmin-master           RedisMyAdmin-master
assetic-master              GetSimpleCMS-master        Monitoring-master         pgpool-II-4.0.0              rockmongo-master
ASTPP-3.6                   glpi-9.4-bugfixes          Monocypher-master         phpbu-master                 rosariosis-mobile
bike-master                 guacamole-server-master    mumble-master             phpipam-master               server-status-master
bitcoind-status-master      heartland-php              MyWebSQL-master           phpLDAPadmin-master          ServerStatus-master
Bitcoin-mining-proxy-master hotelmanagement-master     Nagdash-master            php-malware-scanner-master   Simple-Web-Server-master
bitcoin-php-master          intersango-master          nginx-rtmp-module-master  phpmemcachedadmin-master     sulu-standard-develop
centreon-master
cms-dev
cms-master
CMS-master
contact-form-7
Cosmo-master
deltachat-core-master
easyhadoop-master
ubuntu  ~/bsides   du -sh .
1.3G    .
```

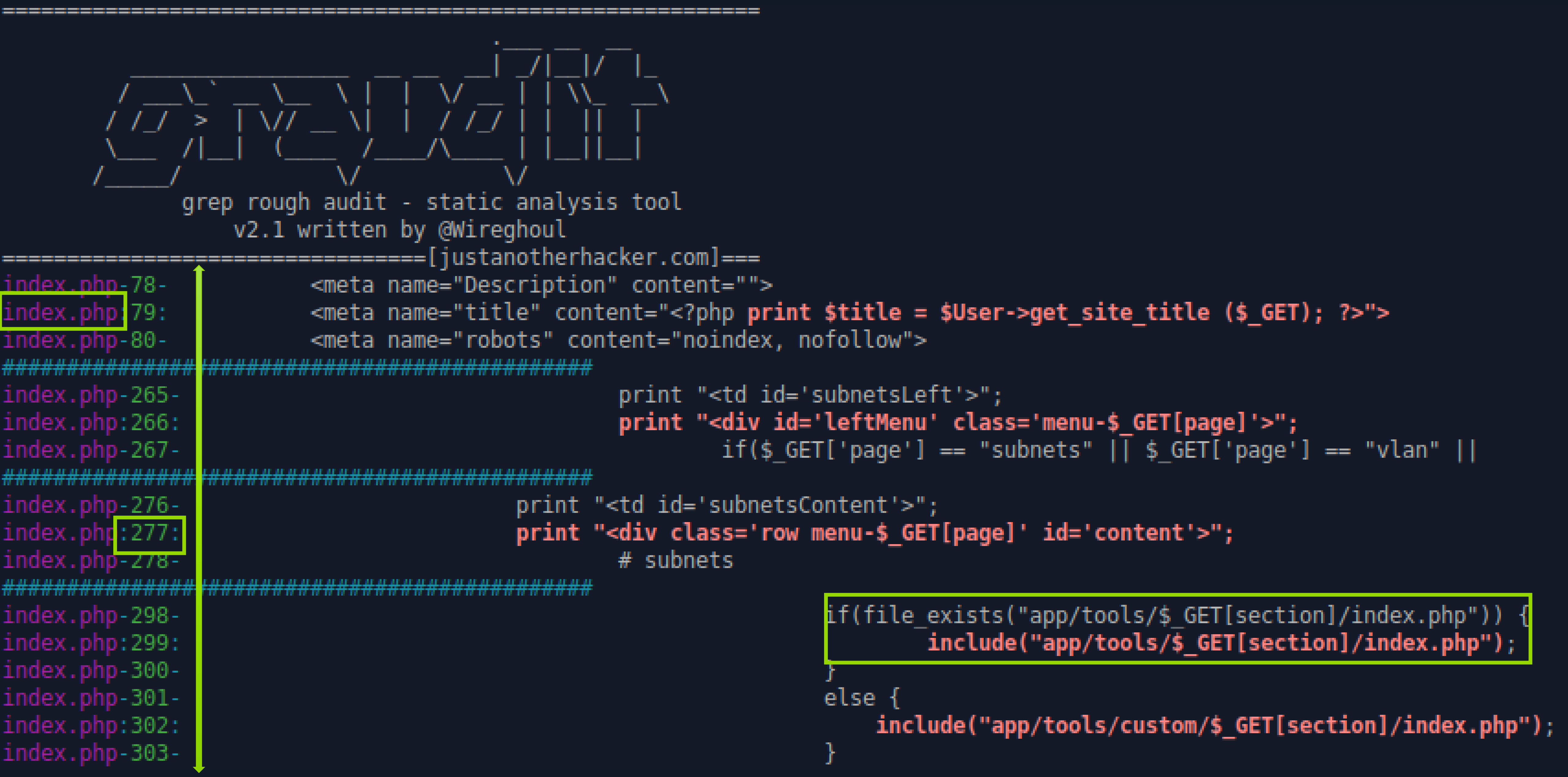
```
ubuntu  ~/bsides   time ~/graudit/graudit -d flatline . > ../grout.txt
/bin/grep: ./phpipam-master/functions/locale/cs_CZ.UTF8/cs_CZ.UTF8: Too many levels of symbolic links
/bin/grep: ./phpipam-master/functions/locale/cs_CZ.UTF-8/cs_CZ.UTF8: Too many levels of symbolic links
/bin/grep: ./phpipam-master/functions/locale/cs/cs_CZ.UTF8: Too many levels of symbolic links
/bin/grep: ./phpipam-master/functions/locale/cs_CZ/cs_CZ.UTF8: Too many levels of symbolic links

real    0m6.051s
user    0m5.584s
sys     0m0.473s
ubuntu  ~/bsides  2  
```

```
ubuntu  ~/bsides   time find . -name "*.c" -exec ~/flatline/cpptaint.sh {} \; | xargs -n1 ~/flatline/b0ftaint.sh > out-justc

real    0m15.490s
user    0m23.138s
sys     0m4.328s
```

Improving human processing time

- AVOID FALSE POSITIVES
- THIS MIGHT MEAN MISSING VULNERABILITIES (false negatives)
  - You can always take another look later
- SHORTLIST OF VULNERABILITY CLASSES
  - Easy to analyse
  - Avoid drowning in XSS
  - Rules can be tweaked to match the worst developer habits





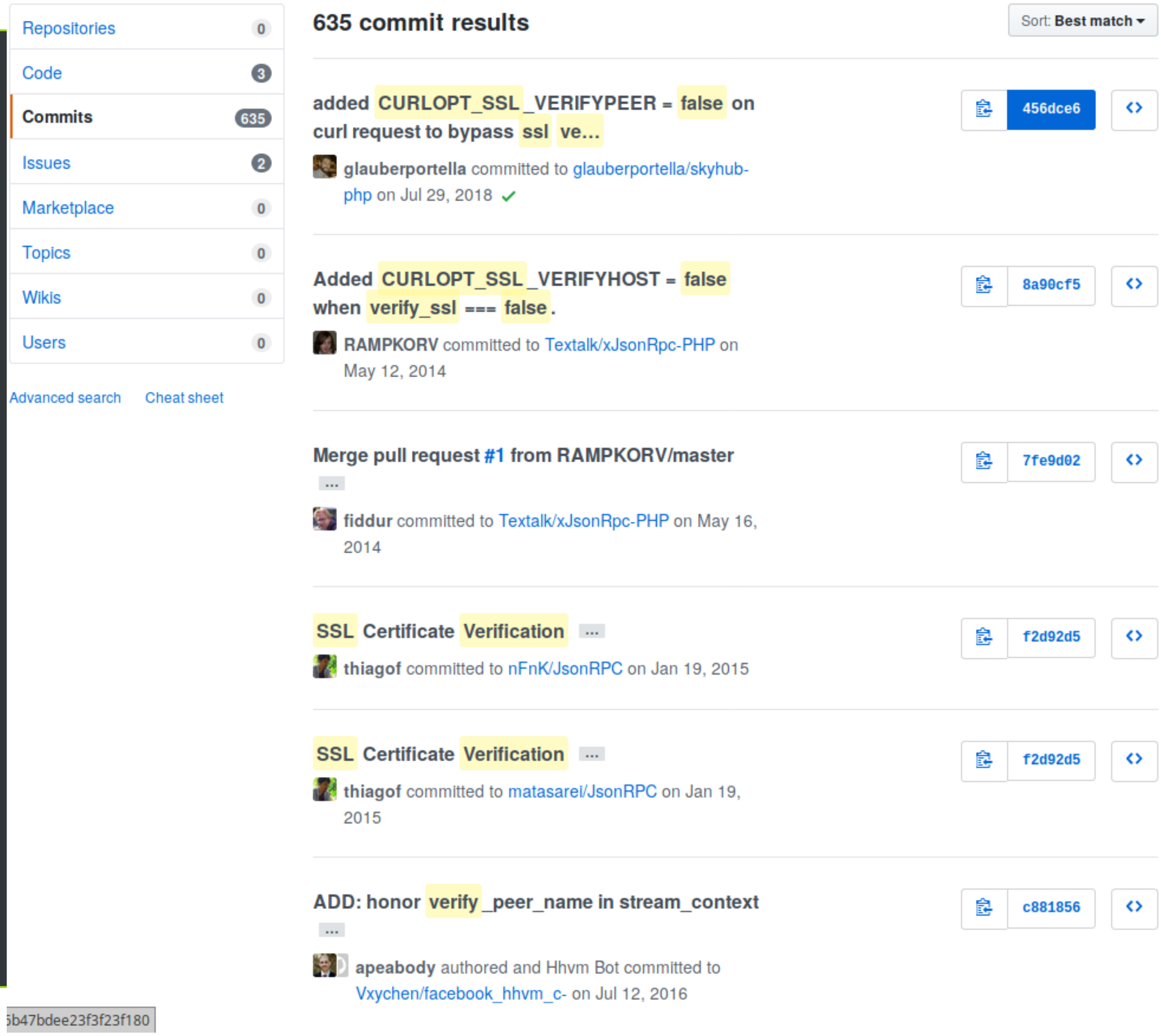
```
==========================================================

                                      .___.__  __
          ________________   __ __  __| _/|__|/  |_
         / ___\_  __ \__  \ |  |  \/ __ | |  \   __\
        / /_/  >  | \// __ \|  |  / /_/ | |  ||  |
        \___  /|__|  (____  /____/\____ | |__||__|
       /_____/            \/           \/
              grep rough audit - static analysis tool
                  v2.1 written by @Wireghoul
=================================[justanotherhacker.com]===
index.php-78-           <meta name="Description" content="">
index.php:79:           <meta name="title" content="<?php print $title = $User->get_site_title ($_GET); ?>">
index.php-80-           <meta name="robots" content="noindex, nofollow">
##############################################
index.php-265-                                  print "<td id='subnetsLeft'>";
index.php:266:                                  print "<div id='leftMenu' class='menu-$_GET[page]'>";
index.php-267-                                          if($_GET['page'] == "subnets" || $_GET['page'] == "vlan" ||
##############################################
index.php-276-                          print "<td id='subnetsContent'>";
index.php:277:                          print "<div class='row menu-$_GET[page]' id='content'>";
index.php-278-                                  # subnets
##############################################
index.php-298-                                                  if(file_exists("app/tools/$_GET[section]/index.php")) {
index.php:299:                                                          include("app/tools/$_GET[section]/index.php");
index.php-300-                                                  }
index.php-301-                                                  else {
index.php:302:                                                      include("app/tools/custom/$_GET[section]/index.php");
index.php-303-                                                  }
```

SSL/TLS Validation Failure

```
grep -rsE 'CURLOPT_SSL_VERIFY(PEER|HOST|STATUS).*([Ff][Aa][Ll][Ss][Ee]|0)' .
```

SSL/TLS Validation Failure

```
grep -rsE 'CURLOPT_SSL_VERIFY(PEER|
```



635 commit results

added CURLOPT_SSL_VERIFYPEER = false on curl request to bypass ssl ve...
glauberportella committed to glauberportella/skyhub-php on Jul 29, 2018 ✓
456dce6

Added CURLOPT_SSL_VERIFYHOST = false when verify_ssl === false.
RAMPKORV committed to Textalk/xJsonRpc-PHP on May 12, 2014
8a90cf5

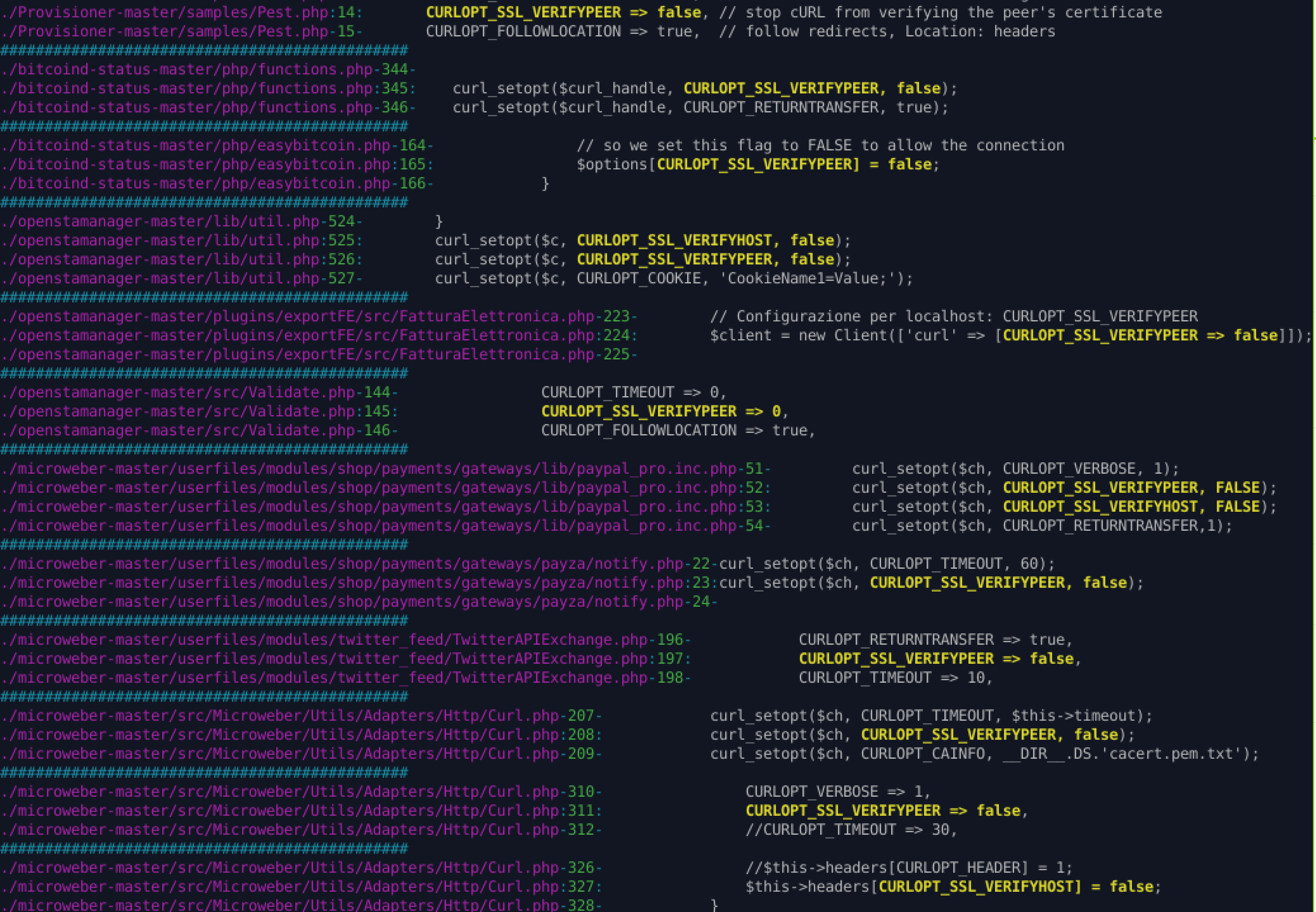
Merge pull request #1 from RAMPKORV/master
…
fiddur committed to Textalk/xJsonRpc-PHP on May 16, 2014
7fe9d02

SSL Certificate Verification …
thiagof committed to nFnK/JsonRPC on Jan 19, 2015
f2d92d5

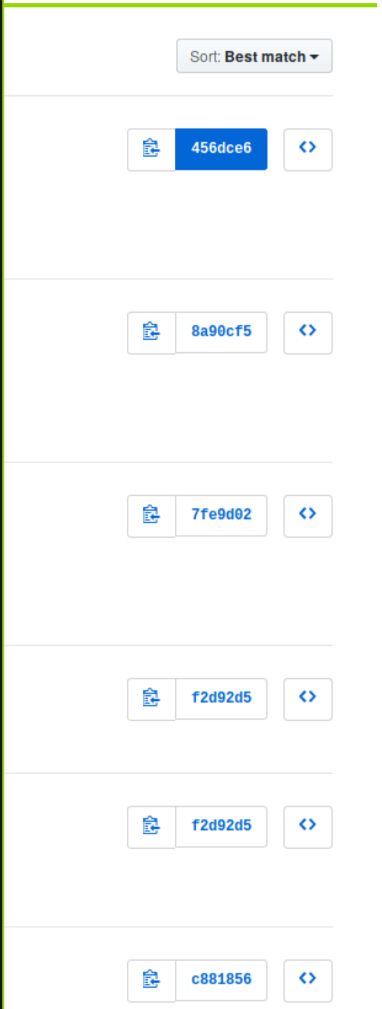
SSL Certificate Verification …
thiagof committed to matasarei/JsonRPC on Jan 19, 2015
f2d92d5

ADD: honor verify_peer_name in stream_context
…
apeabody authored and Hhvm Bot committed to Vxychen/facebook_hhvm_c- on Jul 12, 2016
c881856

5b47bdee23f3f23f180



```
./Provisioner-master/samples/Pest.php:14:       CURLOPT_SSL_VERIFYPEER => false, // stop cURL from verifying the peer's certificate
./Provisioner-master/samples/Pest.php-15-       CURLOPT_FOLLOWLOCATION => true,  // follow redirects, Location: headers
##############################################
./bitcoind-status-master/php/functions.php-344-
./bitcoind-status-master/php/functions.php:345:    curl_setopt($curl_handle, CURLOPT_SSL_VERIFYPEER, false);
./bitcoind-status-master/php/functions.php-346-    curl_setopt($curl_handle, CURLOPT_RETURNTRANSFER, true);
##############################################
./bitcoind-status-master/php/easybitcoin.php-164-                // so we set this flag to FALSE to allow the connection
./bitcoind-status-master/php/easybitcoin.php:165:                $options[CURLOPT_SSL_VERIFYPEER] = false;
./bitcoind-status-master/php/easybitcoin.php-166-            }
##############################################
./openstamanager-master/lib/util.php-524-        }
./openstamanager-master/lib/util.php:525:        curl_setopt($c, CURLOPT_SSL_VERIFYHOST, false);
./openstamanager-master/lib/util.php:526:        curl_setopt($c, CURLOPT_SSL_VERIFYPEER, false);
./openstamanager-master/lib/util.php-527-        curl_setopt($c, CURLOPT_COOKIE, 'CookieName1=Value;');
##############################################
./openstamanager-master/plugins/exportFE/src/FatturaElettronica.php-223-        // Configurazione per localhost: CURLOPT_SSL_VERIFYPEER
./openstamanager-master/plugins/exportFE/src/FatturaElettronica.php:224:        $client = new Client(['curl' => [CURLOPT_SSL_VERIFYPEER => false]]);
./openstamanager-master/plugins/exportFE/src/FatturaElettronica.php-225-
##############################################
./openstamanager-master/src/Validate.php-144-                CURLOPT_TIMEOUT => 0,
./openstamanager-master/src/Validate.php:145:                CURLOPT_SSL_VERIFYPEER => 0,
./openstamanager-master/src/Validate.php-146-                CURLOPT_FOLLOWLOCATION => true,
##############################################
./microweber-master/userfiles/modules/shop/payments/gateways/lib/paypal_pro.inc.php-51-         curl_setopt($ch, CURLOPT_VERBOSE, 1);
./microweber-master/userfiles/modules/shop/payments/gateways/lib/paypal_pro.inc.php:52:         curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, FALSE);
./microweber-master/userfiles/modules/shop/payments/gateways/lib/paypal_pro.inc.php:53:         curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, FALSE);
./microweber-master/userfiles/modules/shop/payments/gateways/lib/paypal_pro.inc.php-54-         curl_setopt($ch, CURLOPT_RETURNTRANSFER,1);
##############################################
./microweber-master/userfiles/modules/shop/payments/gateways/payza/notify.php-22-curl_setopt($ch, CURLOPT_TIMEOUT, 60);
./microweber-master/userfiles/modules/shop/payments/gateways/payza/notify.php:23:curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, false);
./microweber-master/userfiles/modules/shop/payments/gateways/payza/notify.php-24-
##############################################
./microweber-master/userfiles/modules/twitter_feed/TwitterAPIExchange.php-196-            CURLOPT_RETURNTRANSFER => true,
./microweber-master/userfiles/modules/twitter_feed/TwitterAPIExchange.php:197:            CURLOPT_SSL_VERIFYPEER => false,
./microweber-master/userfiles/modules/twitter_feed/TwitterAPIExchange.php-198-            CURLOPT_TIMEOUT => 10,
##############################################
./microweber-master/src/Microweber/Utils/Adapters/Http/Curl.php-207-            curl_setopt($ch, CURLOPT_TIMEOUT, $this->timeout);
./microweber-master/src/Microweber/Utils/Adapters/Http/Curl.php:208:            curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, false);
./microweber-master/src/Microweber/Utils/Adapters/Http/Curl.php-209-            curl_setopt($ch, CURLOPT_CAINFO, __DIR__.DS.'cacert.pem.txt');
##############################################
./microweber-master/src/Microweber/Utils/Adapters/Http/Curl.php-310-                CURLOPT_VERBOSE => 1,
./microweber-master/src/Microweber/Utils/Adapters/Http/Curl.php:311:                CURLOPT_SSL_VERIFYPEER => false,
./microweber-master/src/Microweber/Utils/Adapters/Http/Curl.php-312-                //CURLOPT_TIMEOUT => 30,
##############################################
./microweber-master/src/Microweber/Utils/Adapters/Http/Curl.php-326-
./microweber-master/src/Microweber/Utils/Adapters/Http/Curl.php:327:                //$this->headers[CURLOPT_HEADER] = 1;
./microweber-master/src/Microweber/Utils/Adapters/Http/Curl.php-328-                $this->headers[CURLOPT_SSL_VERIFYHOST] = false;
            }
```

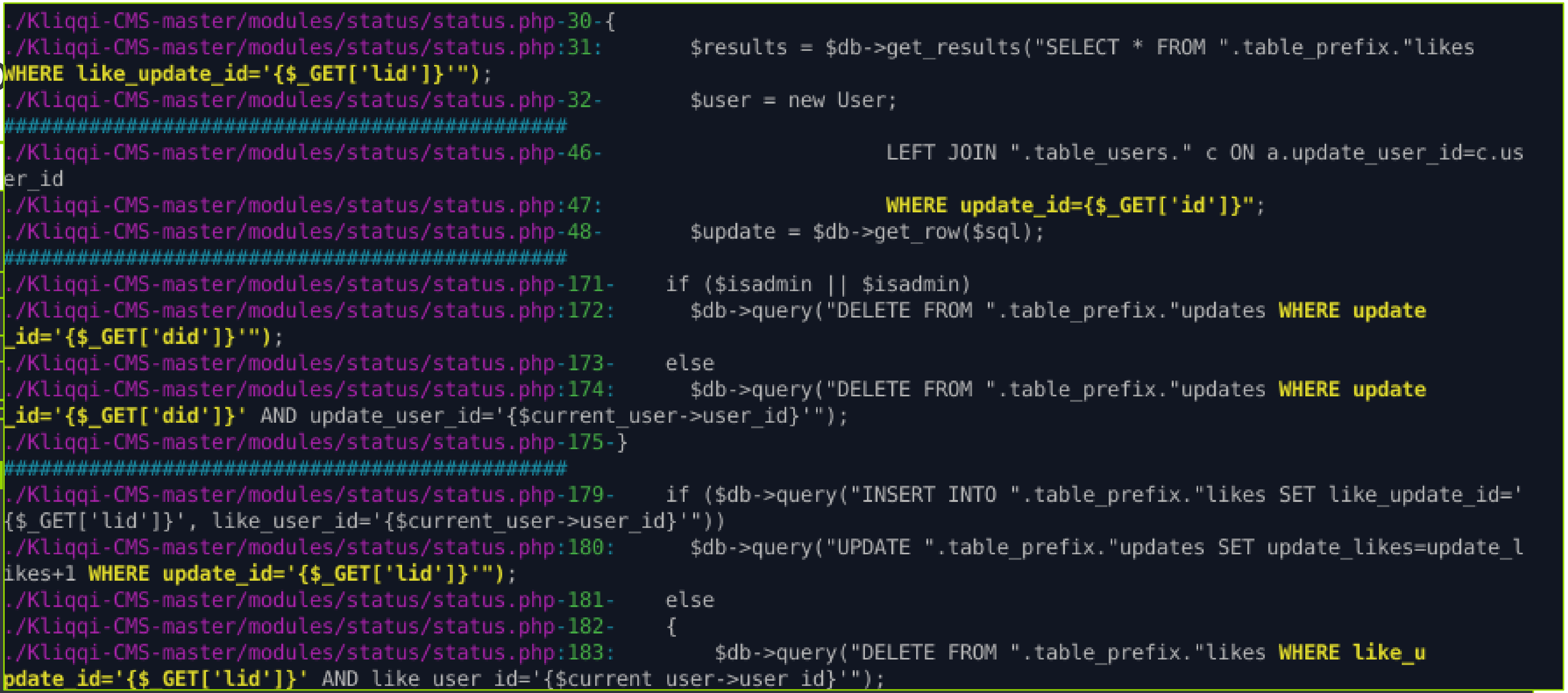


SQL injection

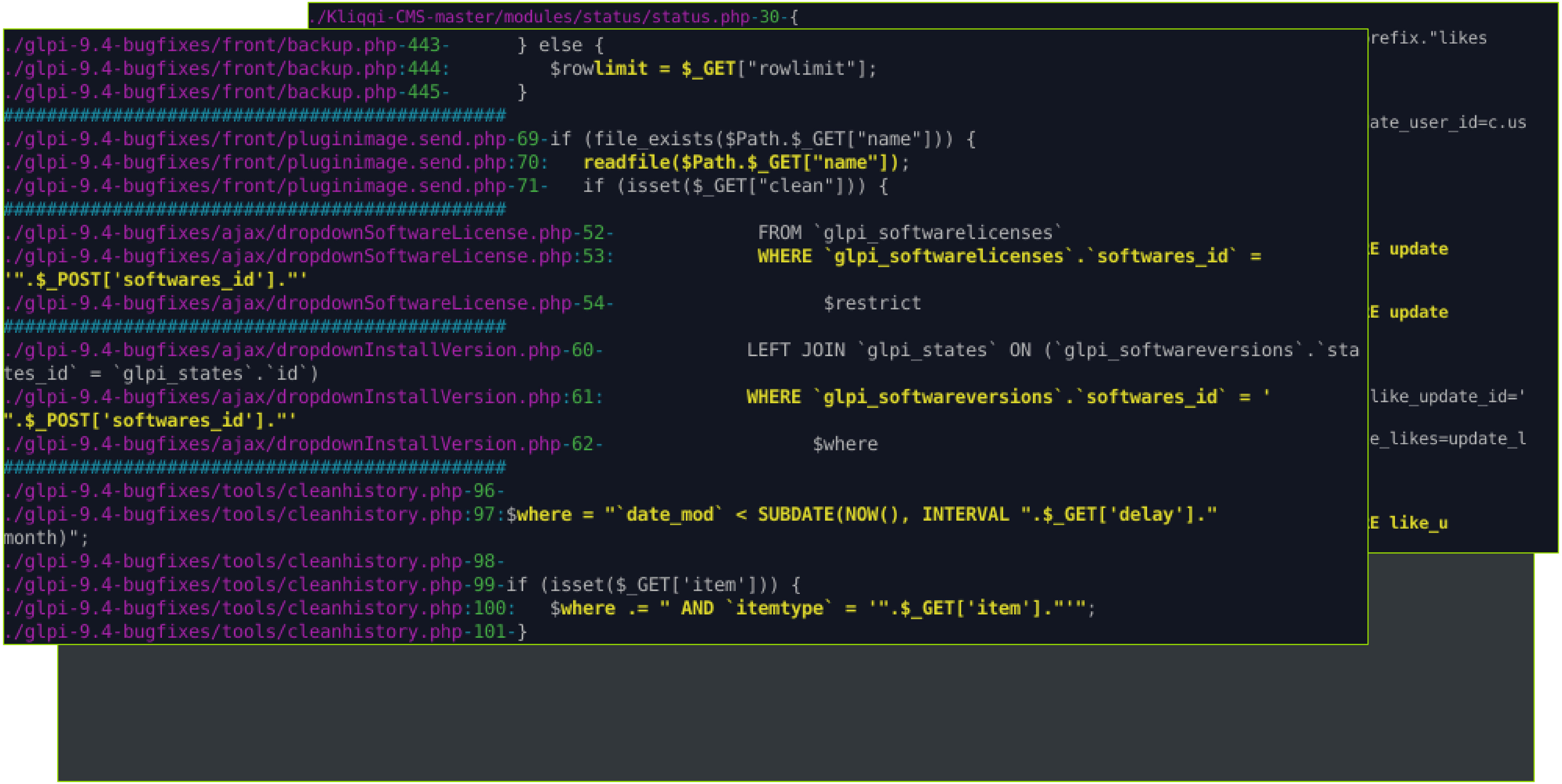
```
query[[:space:]]*\(.*\$_(GET|POST|REQUEST|COOKIE)\[

[Ss][Ee][Ll][Ee][Cc][Tt].*\$_(GET|POST|REQUEST|COOKIE)\[.*[Ff][Rr][Oo][Mm]

[Ss][Ee][Ll][Ee][Cc][Tt].*[Ff][Rr][Oo][Mm].*\$_(GET|POST|REQUEST|COOKIE)\[

[Ww][Hh][Ee][Rr][Ee].*=.*\$_(GET|POST|REQUEST|COOKIE)\[

[\"\']([Aa][Nn][Dd]|[Oo][Rr]).*=.*\$_(GET|POST|REQUEST|COOKIE)\[
```

SQL injectio

```
query[[:space:]]*\(
[Ss][Ee][Ll][Ee][Cc]
[Ss][Ee][Ll][Ee][Cc]
[Ww][Hh][Ee][Rr][E
[\"\']([Aa][Nn][Dd]|
```

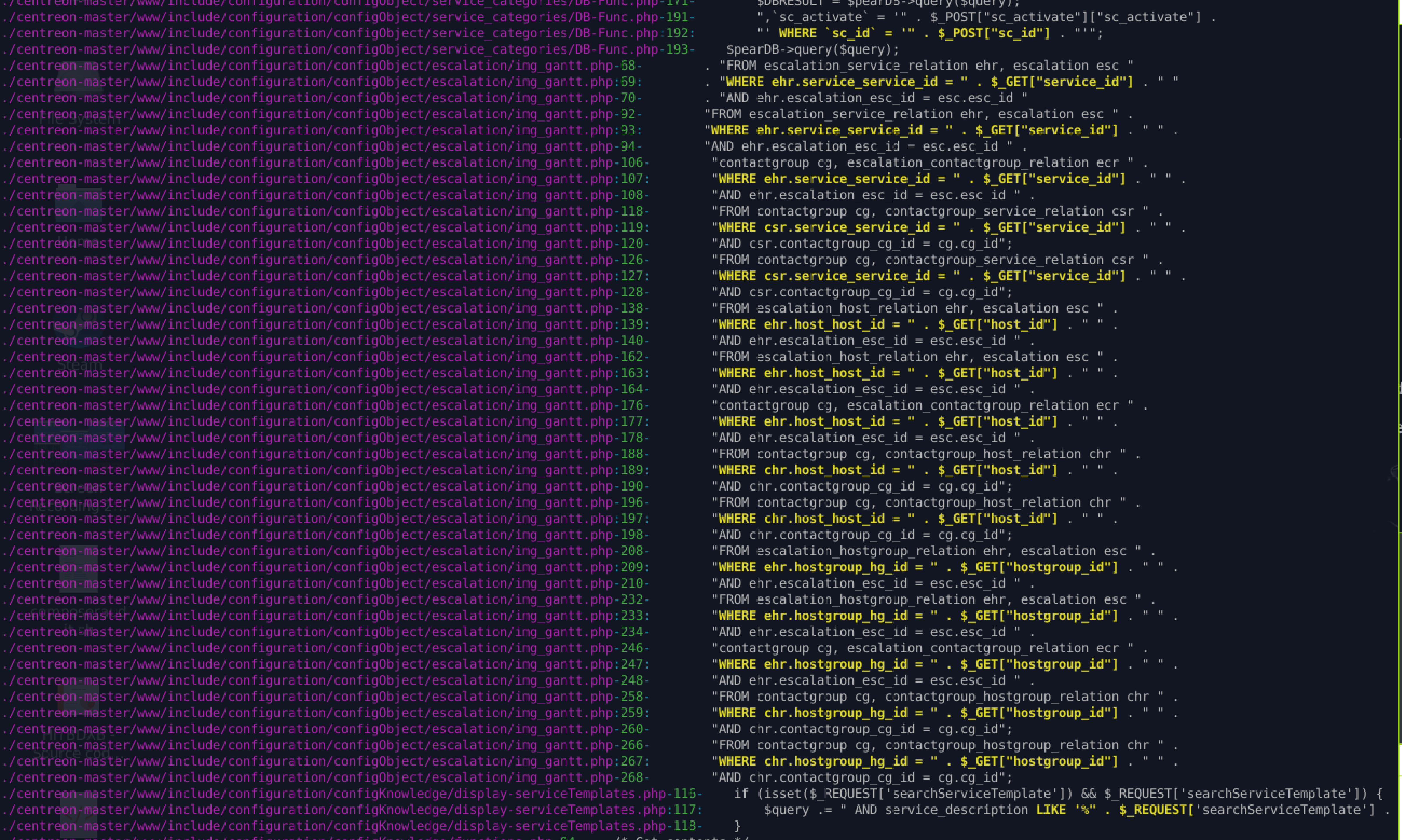


```
./Kliqqi-CMS-master/modules/status/status.php-30-{
./Kliqqi-CMS-master/modules/status/status.php:31:        $results = $db->get_results("SELECT * FROM ".table_prefix."likes
WHERE like_update_id='{$_GET['lid']}'");
./Kliqqi-CMS-master/modules/status/status.php-32-        $user = new User;
##############################################
./Kliqqi-CMS-master/modules/status/status.php-46-                                LEFT JOIN ".table_users." c ON a.update_user_id=c.us
er_id
./Kliqqi-CMS-master/modules/status/status.php:47:                                WHERE update_id={$_GET['id']}";
./Kliqqi-CMS-master/modules/status/status.php-48-        $update = $db->get_row($sql);
##############################################
./Kliqqi-CMS-master/modules/status/status.php-171-    if ($isadmin || $isadmin)
./Kliqqi-CMS-master/modules/status/status.php:172:      $db->query("DELETE FROM ".table_prefix."updates WHERE update
_id='{$_GET['did']}'");
./Kliqqi-CMS-master/modules/status/status.php-173-    else
./Kliqqi-CMS-master/modules/status/status.php:174:      $db->query("DELETE FROM ".table_prefix."updates WHERE update
_id='{$_GET['did']}' AND update_user_id='{$current_user->user_id}'");
./Kliqqi-CMS-master/modules/status/status.php-175-}
##############################################
./Kliqqi-CMS-master/modules/status/status.php-179-    if ($db->query("INSERT INTO ".table_prefix."likes SET like_update_id='
{$_GET['lid']}', like_user_id='{$current_user->user_id}'"))
./Kliqqi-CMS-master/modules/status/status.php:180:      $db->query("UPDATE ".table_prefix."updates SET update_likes=update_l
ikes+1 WHERE update_id='{$_GET['lid']}'");
./Kliqqi-CMS-master/modules/status/status.php-181-    else
./Kliqqi-CMS-master/modules/status/status.php-182-    {
./Kliqqi-CMS-master/modules/status/status.php:183:        $db->query("DELETE FROM ".table_prefix."likes WHERE like_u
pdate_id='{$_GET['lid']}' AND like_user_id='{$current_user->user_id}'");
```



```
./Kliqqi-CMS-master/modules/status/status.php-30-{
./glpi-9.4-bugfixes/front/backup.php-443-      } else {
./glpi-9.4-bugfixes/front/backup.php:444:         $rowlimit = $_GET["rowlimit"];
./glpi-9.4-bugfixes/front/backup.php-445-      }
##############################################
./glpi-9.4-bugfixes/front/pluginimage.send.php-69-if (file_exists($Path.$_GET["name"])) {
./glpi-9.4-bugfixes/front/pluginimage.send.php:70:   readfile($Path.$_GET["name"]);
./glpi-9.4-bugfixes/front/pluginimage.send.php-71-   if (isset($_GET["clean"])) {
##############################################
./glpi-9.4-bugfixes/ajax/dropdownSoftwareLicense.php-52-             FROM `glpi_softwarelicenses`
./glpi-9.4-bugfixes/ajax/dropdownSoftwareLicense.php:53:             WHERE `glpi_softwarelicenses`.`softwares_id` =
'".$_POST['softwares_id']."'
./glpi-9.4-bugfixes/ajax/dropdownSoftwareLicense.php-54-                   $restrict
##############################################
./glpi-9.4-bugfixes/ajax/dropdownInstallVersion.php-60-             LEFT JOIN `glpi_states` ON (`glpi_softwareversions`.`sta
tes_id` = `glpi_states`.`id`)
./glpi-9.4-bugfixes/ajax/dropdownInstallVersion.php:61:             WHERE `glpi_softwareversions`.`softwares_id` = '
".$_POST['softwares_id']."'
./glpi-9.4-bugfixes/ajax/dropdownInstallVersion.php-62-                   $where
##############################################
./glpi-9.4-bugfixes/tools/cleanhistory.php-96-
./glpi-9.4-bugfixes/tools/cleanhistory.php:97:$where = "`date_mod` < SUBDATE(NOW(), INTERVAL ".$_GET['delay']."
month)";
./glpi-9.4-bugfixes/tools/cleanhistory.php-98-
./glpi-9.4-bugfixes/tools/cleanhistory.php-99-if (isset($_GET['item'])) {
./glpi-9.4-bugfixes/tools/cleanhistory.php:100:   $where .= " AND `itemtype` = '".$_GET['item']."'";
./glpi-9.4-bugfixes/tools/cleanhistory.php-101-}
```

```
refix."likes
ate_user_id=c.us
E update
E update
like_update_id='
e_likes=update_l
E like_u
```



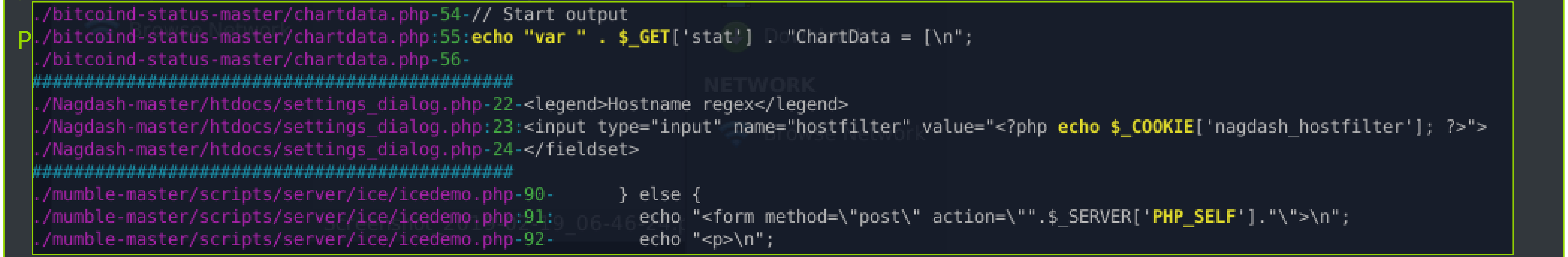
```
./centreon-master/www/include/configuration/configObject/service_categories/DB-Func.php-171-        $DBRESULT = $pearDB->query($query);
./centreon-master/www/include/configuration/configObject/service_categories/DB-Func.php-191-        ",`sc_activate` = '" . $_POST["sc_activate"]["sc_activate"] .
./centreon-master/www/include/configuration/configObject/service_categories/DB-Func.php:192:        "' WHERE `sc_id` = '" . $_POST["sc_id"] . "'";
./centreon-master/www/include/configuration/configObject/service_categories/DB-Func.php-193-    $pearDB->query($query);
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php-68-       . "FROM escalation_service_relation ehr, escalation esc "
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php:69:       . "WHERE ehr.service_service_id = " . $_GET["service_id"] . " "
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php-70-       . "AND ehr.escalation_esc_id = esc.esc_id "
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php-92-       "FROM escalation_service_relation ehr, escalation esc " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php:93:       "WHERE ehr.service_service_id = " . $_GET["service_id"] . " " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php-94-       "AND ehr.escalation_esc_id = esc.esc_id " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php-106-       "contactgroup cg, escalation_contactgroup_relation ecr " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php:107:       "WHERE ehr.service_service_id = " . $_GET["service_id"] . " " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php-108-       "AND ehr.escalation_esc_id = esc.esc_id " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php-118-       "FROM contactgroup cg, contactgroup_service_relation csr " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php:119:       "WHERE csr.service_service_id = " . $_GET["service_id"] . " " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php-120-       "AND csr.contactgroup_cg_id = cg.cg_id";
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php-126-       "FROM contactgroup cg, contactgroup_service_relation csr " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php:127:       "WHERE csr.service_service_id = " . $_GET["service_id"] . " " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php-128-       "AND csr.contactgroup_cg_id = cg.cg_id";
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php-138-       "FROM escalation_host_relation ehr, escalation esc " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php:139:       "WHERE ehr.host_host_id = " . $_GET["host_id"] . " " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php-140-       "AND ehr.escalation_esc_id = esc.esc_id " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php-162-       "FROM escalation_host_relation ehr, escalation esc " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php:163:       "WHERE ehr.host_host_id = " . $_GET["host_id"] . " " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php-164-       "AND ehr.escalation_esc_id = esc.esc_id " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php-176-       "contactgroup cg, escalation_contactgroup_relation ecr " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php:177:       "WHERE ehr.host_host_id = " . $_GET["host_id"] . " " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php-178-       "AND ehr.escalation_esc_id = esc.esc_id " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php-188-       "FROM contactgroup cg, contactgroup_host_relation chr " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php:189:       "WHERE chr.host_host_id = " . $_GET["host_id"] . " " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php-190-       "AND chr.contactgroup_cg_id = cg.cg_id";
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php-196-       "FROM contactgroup cg, contactgroup_host_relation chr " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php:197:       "WHERE chr.host_host_id = " . $_GET["host_id"] . " " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php-198-       "AND chr.contactgroup_cg_id = cg.cg_id";
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php-208-       "FROM escalation_hostgroup_relation ehr, escalation esc " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php:209:       "WHERE ehr.hostgroup_hg_id = " . $_GET["hostgroup_id"] . " " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php-210-       "AND ehr.escalation_esc_id = esc.esc_id " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php-232-       "FROM escalation_hostgroup_relation ehr, escalation esc " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php:233:       "WHERE ehr.hostgroup_hg_id = " . $_GET["hostgroup_id"] . " " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php-234-       "AND ehr.escalation_esc_id = esc.esc_id " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php-246-       "contactgroup cg, escalation_contactgroup_relation ecr " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php:247:       "WHERE ehr.hostgroup_hg_id = " . $_GET["hostgroup_id"] . " " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php-248-       "AND ehr.escalation_esc_id = esc.esc_id " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php-258-       "FROM contactgroup cg, contactgroup_hostgroup_relation chr " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php:259:       "WHERE chr.hostgroup_hg_id = " . $_GET["hostgroup_id"] . " " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php-260-       "AND chr.contactgroup_cg_id = cg.cg_id";
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php-266-       "FROM contactgroup cg, contactgroup_hostgroup_relation chr " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php:267:       "WHERE chr.hostgroup_hg_id = " . $_GET["hostgroup_id"] . " " .
./centreon-master/www/include/configuration/configObject/escalation/img_gantt.php-268-       "AND chr.contactgroup_cg_id = cg.cg_id";
./centreon-master/www/include/configuration/configKnowledge/display-serviceTemplates.php-116-    if (isset($_REQUEST['searchServiceTemplate']) && $_REQUEST['searchServiceTemplate']) {
./centreon-master/www/include/configuration/configKnowledge/display-serviceTemplates.php:117:        $query .= " AND service_description LIKE '%" . $_REQUEST['searchServiceTemplate'] .
./centreon-master/www/include/configuration/configKnowledge/display-serviceTemplates.php-118-    }
./centreon-master/www/include/configuration/configKnowledge/functions.php-94-      /* Get contents */
```

Cross site scripting

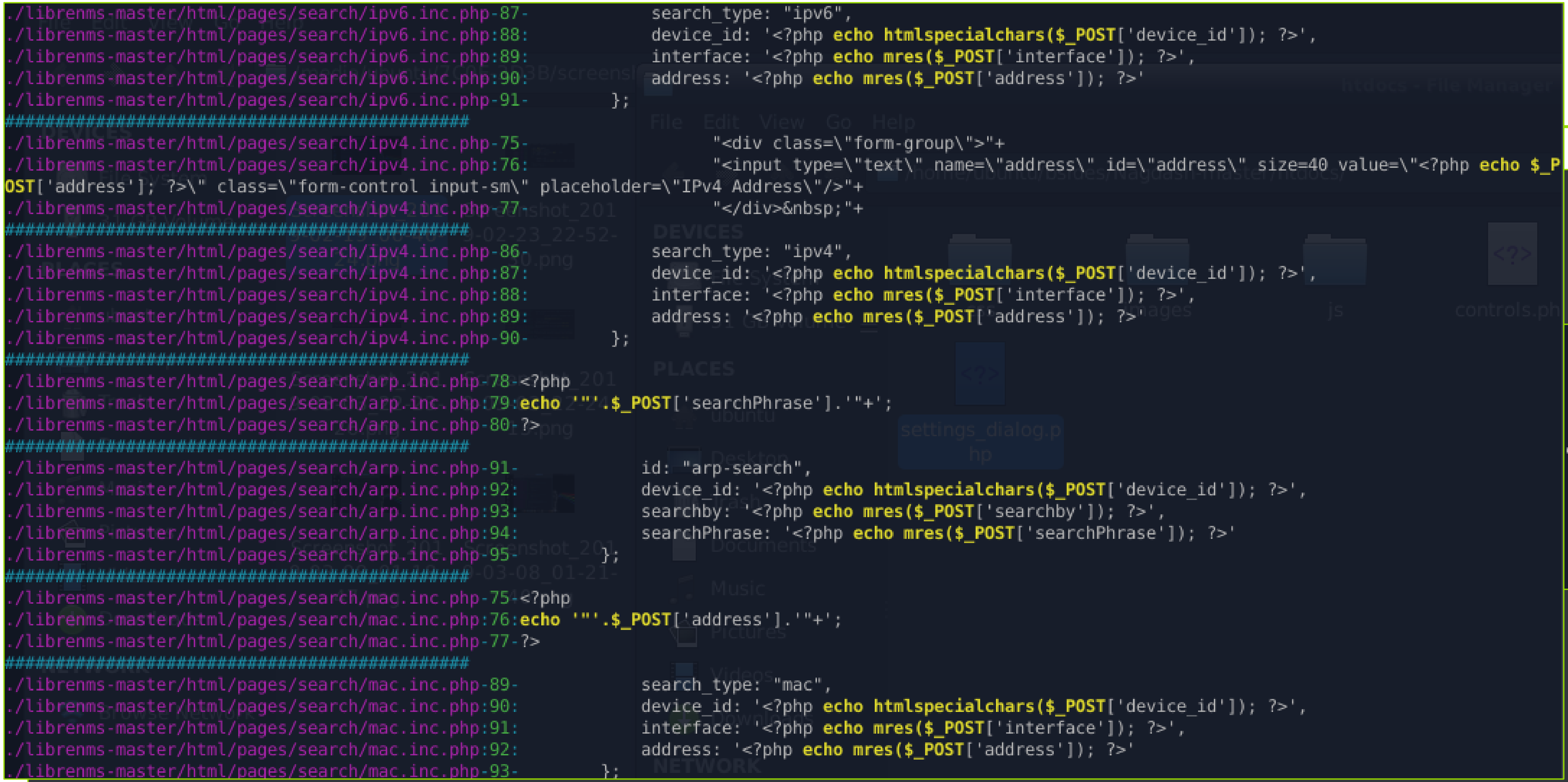
```
<?=.*\$_(GET|POST|REQUEST|COOKIE|SERVER)

echo.*\$_(GET|POST|REQUEST|COOKIE)

print.*\$_(GET|POST|REQUEST|COOKIE)

PHP_SELF
```

Cross site scripting

```
<?=.*\$_(GET|POST|REQUEST|COOKIE|SERVER)

echo.*\$_(GET|POST|REQUEST|COOKIE)

print.*\$_(GET|POST|REQUEST|COOKIE)

P
```



```
./bitcoind-status-master/chartdata.php-54-// Start output
./bitcoind-status-master/chartdata.php:55:echo "var " . $_GET['stat'] . "ChartData = [\n";
./bitcoind-status-master/chartdata.php-56-
##############################################
./Nagdash-master/htdocs/settings_dialog.php-22-<legend>Hostname regex</legend>
./Nagdash-master/htdocs/settings_dialog.php:23:<input type="input" name="hostfilter" value="<?php echo $_COOKIE['nagdash_hostfilter']; ?>">
./Nagdash-master/htdocs/settings_dialog.php-24-</fieldset>
##############################################
./mumble-master/scripts/server/ice/icedemo.php-90-      } else {
./mumble-master/scripts/server/ice/icedemo.php:91:        echo "<form method=\"post\" action=\"".$_SERVER['PHP_SELF']."\">\n";
./mumble-master/scripts/server/ice/icedemo.php-92-        echo "<p>\n";
```

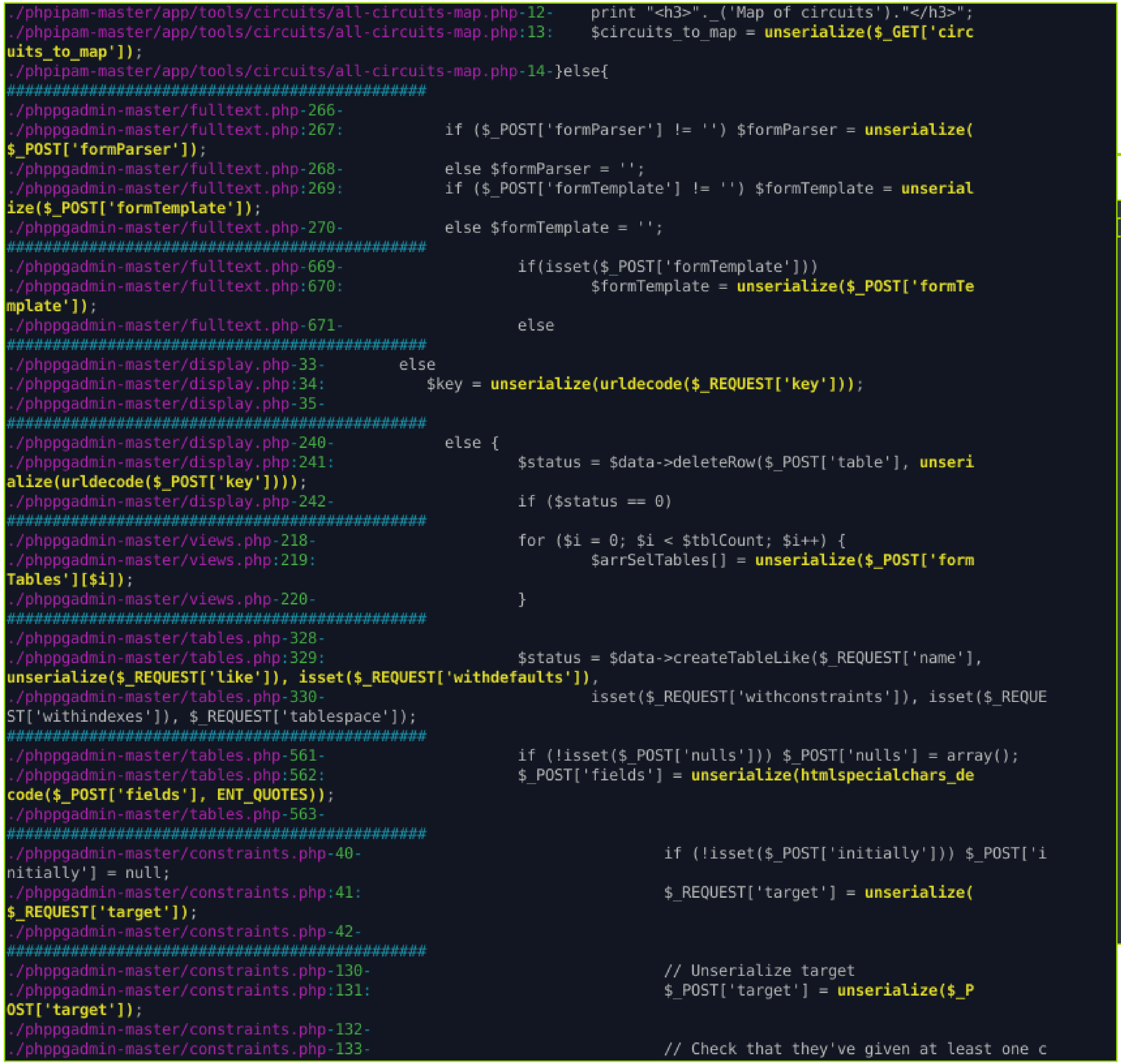


```
./librenms-master/html/pages/search/ipv6.inc.php-87-            search_type: "ipv6",
./librenms-master/html/pages/search/ipv6.inc.php:88:            device_id: '<?php echo htmlspecialchars($_POST['device_id']); ?>',
./librenms-master/html/pages/search/ipv6.inc.php:89:            interface: '<?php echo mres($_POST['interface']); ?>',
./librenms-master/html/pages/search/ipv6.inc.php:90:            address: '<?php echo mres($_POST['address']); ?>'
./librenms-master/html/pages/search/ipv6.inc.php-91-        };
##############################################
./librenms-master/html/pages/search/ipv4.inc.php-75-                  "<div class=\"form-group\">"+
./librenms-master/html/pages/search/ipv4.inc.php:76:                  "<input type=\"text\" name=\"address\" id=\"address\" size=40 value=\"<?php echo $_P
OST['address']; ?>\" class=\"form-control input-sm\" placeholder=\"IPv4 Address\"/>"+
./librenms-master/html/pages/search/ipv4.inc.php-77-                  "</div>&nbsp;"+
##############################################
./librenms-master/html/pages/search/ipv4.inc.php-86-            search_type: "ipv4",
./librenms-master/html/pages/search/ipv4.inc.php:87:            device_id: '<?php echo htmlspecialchars($_POST['device_id']); ?>',
./librenms-master/html/pages/search/ipv4.inc.php:88:            interface: '<?php echo mres($_POST['interface']); ?>',
./librenms-master/html/pages/search/ipv4.inc.php:89:            address: '<?php echo mres($_POST['address']); ?>'
./librenms-master/html/pages/search/ipv4.inc.php-90-        };
##############################################
./librenms-master/html/pages/search/arp.inc.php-78-<?php
./librenms-master/html/pages/search/arp.inc.php:79:echo '"'.$_POST['searchPhrase'].'"+';
./librenms-master/html/pages/search/arp.inc.php-80-?>
##############################################
./librenms-master/html/pages/search/arp.inc.php-91-            id: "arp-search",
./librenms-master/html/pages/search/arp.inc.php:92:            device_id: '<?php echo htmlspecialchars($_POST['device_id']); ?>',
./librenms-master/html/pages/search/arp.inc.php:93:            searchby: '<?php echo mres($_POST['searchby']); ?>',
./librenms-master/html/pages/search/arp.inc.php:94:            searchPhrase: '<?php echo mres($_POST['searchPhrase']); ?>'
./librenms-master/html/pages/search/arp.inc.php-95-        };
##############################################
./librenms-master/html/pages/search/mac.inc.php-75-<?php
./librenms-master/html/pages/search/mac.inc.php:76:echo '"'.$_POST['address'].'"+';
./librenms-master/html/pages/search/mac.inc.php-77-?>
##############################################
./librenms-master/html/pages/search/mac.inc.php-89-            search_type: "mac",
./librenms-master/html/pages/search/mac.inc.php:90:            device_id: '<?php echo htmlspecialchars($_POST['device_id']); ?>',
./librenms-master/html/pages/search/mac.inc.php:91:            interface: '<?php echo mres($_POST['interface']); ?>',
./librenms-master/html/pages/search/mac.inc.php:92:            address: '<?php echo mres($_POST['address']); ?>'
./librenms-master/html/pages/search/mac.inc.php-93-        };
```

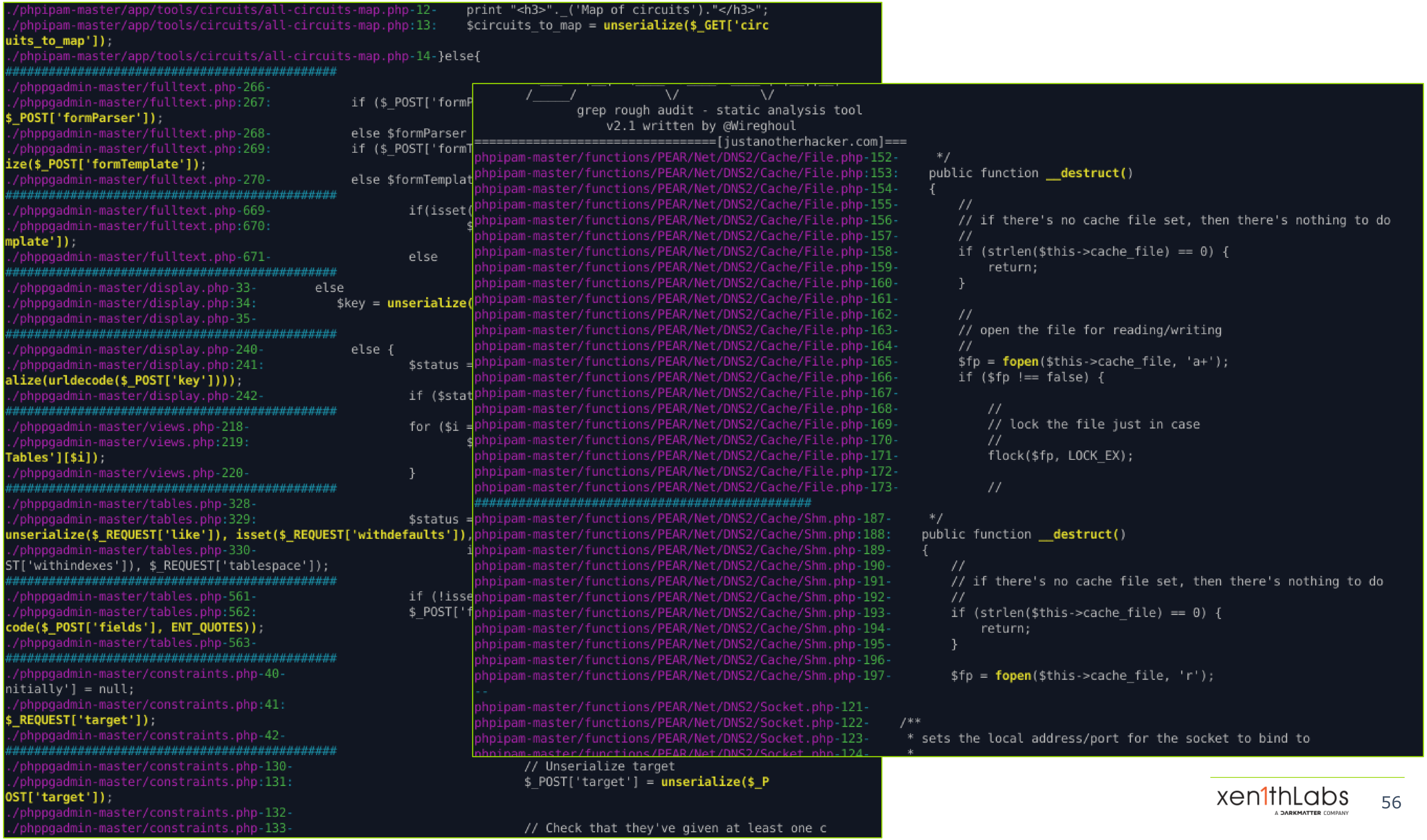
Unsafe deserialization

```
unserialize[[:space:]]*\(.*\$_(GET|POST|REQUEST|COOKIE|SERVER|SESSION)
```

ON)



```
./phpipam-master/app/tools/circuits/all-circuits-map.php-12-    print "<h3>"._('Map of circuits')."</h3>";
./phpipam-master/app/tools/circuits/all-circuits-map.php:13:    $circuits_to_map = unserialize($_GET['circ
uits_to_map']);
./phpipam-master/app/tools/circuits/all-circuits-map.php-14-}else{
##############################################
./phppgadmin-master/fulltext.php-266-
./phppgadmin-master/fulltext.php:267:           if ($_POST['formParser'] != '') $formParser = unserialize(
$_POST['formParser']);
./phppgadmin-master/fulltext.php-268-           else $formParser = '';
./phppgadmin-master/fulltext.php:269:           if ($_POST['formTemplate'] != '') $formTemplate = unserial
ize($_POST['formTemplate']);
./phppgadmin-master/fulltext.php-270-           else $formTemplate = '';
##############################################
./phppgadmin-master/fulltext.php-669-                   if(isset($_POST['formTemplate']))
./phppgadmin-master/fulltext.php:670:                           $formTemplate = unserialize($_POST['formTe
mplate']);
./phppgadmin-master/fulltext.php-671-                   else
##############################################
./phppgadmin-master/display.php-33-         else
./phppgadmin-master/display.php:34:             $key = unserialize(urldecode($_REQUEST['key']));
./phppgadmin-master/display.php-35-
##############################################
./phppgadmin-master/display.php-240-            else {
./phppgadmin-master/display.php:241:                    $status = $data->deleteRow($_POST['table'], unseri
alize(urldecode($_POST['key'])));
./phppgadmin-master/display.php-242-                    if ($status == 0)
##############################################
./phppgadmin-master/views.php-218-                      for ($i = 0; $i < $tblCount; $i++) {
./phppgadmin-master/views.php:219:                              $arrSelTables[] = unserialize($_POST['form
Tables'][$i]);
./phppgadmin-master/views.php-220-                      }
##############################################
./phppgadmin-master/tables.php-328-
./phppgadmin-master/tables.php:329:                     $status = $data->createTableLike($_REQUEST['name'],
unserialize($_REQUEST['like']), isset($_REQUEST['withdefaults']),
./phppgadmin-master/tables.php-330-                             isset($_REQUEST['withconstraints']), isset($_REQUE
ST['withindexes']), $_REQUEST['tablespace']);
#############################################
./phppgadmin-master/tables.php-561-                     if (!isset($_POST['nulls'])) $_POST['nulls'] = array();
./phppgadmin-master/tables.php:562:                     $_POST['fields'] = unserialize(htmlspecialchars_de
code($_POST['fields'], ENT_QUOTES));
./phppgadmin-master/tables.php-563-
##############################################
./phppgadmin-master/constraints.php-40-                         if (!isset($_POST['initially'])) $_POST['i
nitially'] = null;
./phppgadmin-master/constraints.php:41:                         $_REQUEST['target'] = unserialize(
$_REQUEST['target']);
./phppgadmin-master/constraints.php-42-
##############################################
./phppgadmin-master/constraints.php-130-                        // Unserialize target
./phppgadmin-master/constraints.php:131:                        $_POST['target'] = unserialize($_P
OST['target']);
./phppgadmin-master/constraints.php-132-
./phppgadmin-master/constraints.php-133-                        // Check that they've given at least one c
```



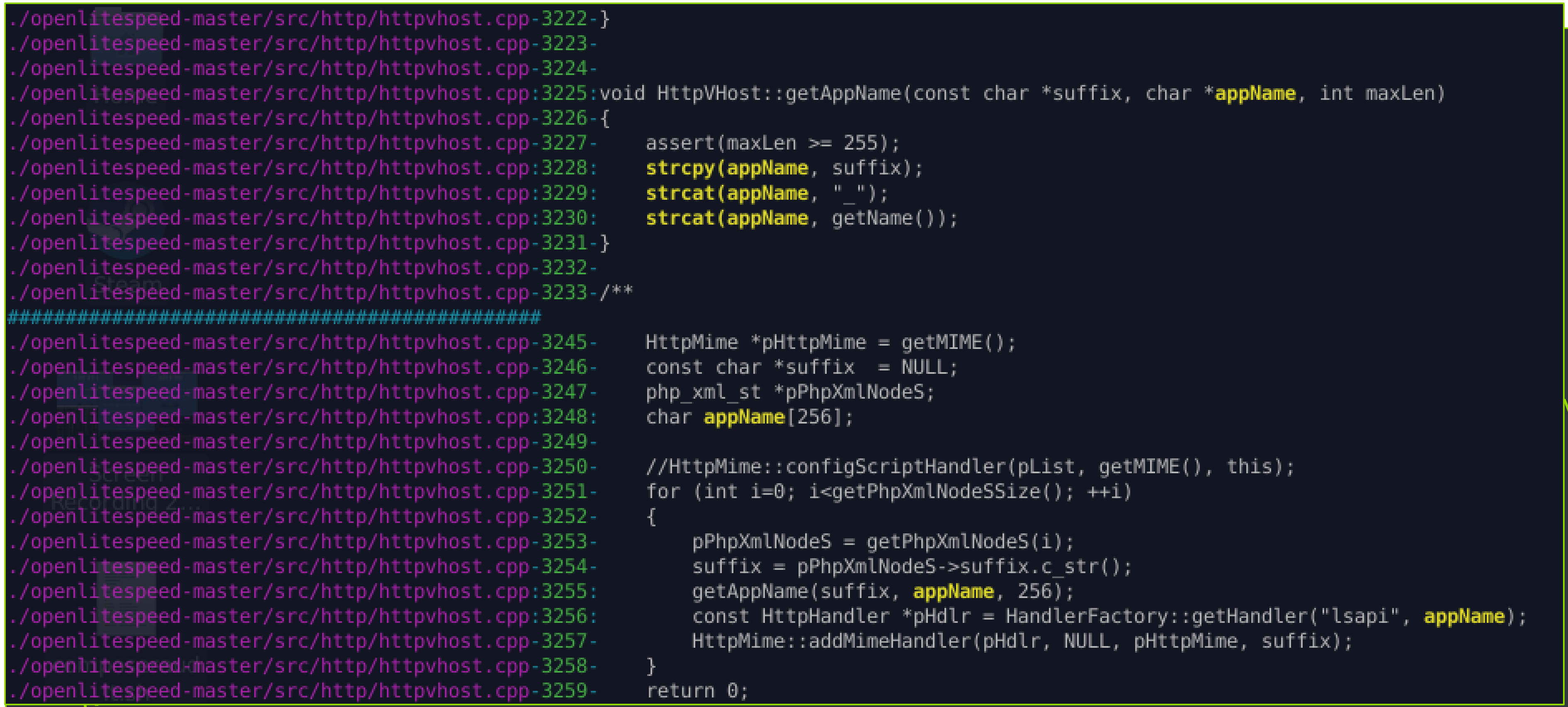
```
./phpipam-master/app/tools/circuits/all-circuits-map.php-12-    print "<h3>"._('Map of circuits')."</h3>";
./phpipam-master/app/tools/circuits/all-circuits-map.php:13:    $circuits_to_map = unserialize($_GET['circ
uits_to_map']);
./phpipam-master/app/tools/circuits/all-circuits-map.php-14-}else{
##############################################
./phppgadmin-master/fulltext.php-266-
./phppgadmin-master/fulltext.php:267:           if ($_POST['formP
$_POST['formParser']);
./phppgadmin-master/fulltext.php-268-           else $formParser
./phppgadmin-master/fulltext.php:269:           if ($_POST['formT
ize($_POST['formTemplate']);
./phppgadmin-master/fulltext.php-270-           else $formTemplat
##############################################
./phppgadmin-master/fulltext.php-669-                   if(isset(
./phppgadmin-master/fulltext.php:670:                           $
mplate']);
./phppgadmin-master/fulltext.php-671-                   else
##############################################
./phppgadmin-master/display.php-33-         else
./phppgadmin-master/display.php:34:             $key = unserialize(
./phppgadmin-master/display.php-35-
##############################################
./phppgadmin-master/display.php-240-            else {
./phppgadmin-master/display.php:241:                    $status =
alize(urldecode($_POST['key'])));
./phppgadmin-master/display.php-242-                    if ($stat
##############################################
./phppgadmin-master/views.php-218-                      for ($i =
./phppgadmin-master/views.php:219:                              $
Tables'][$i]);
./phppgadmin-master/views.php-220-                      }
##############################################
./phppgadmin-master/tables.php-328-
./phppgadmin-master/tables.php:329:                     $status =
unserialize($_REQUEST['like']), isset($_REQUEST['withdefaults']),
./phppgadmin-master/tables.php-330-                             i
ST['withindexes']), $_REQUEST['tablespace']);
##############################################
./phppgadmin-master/tables.php-561-                     if (!isse
./phppgadmin-master/tables.php:562:                     $_POST['f
code($_POST['fields'], ENT_QUOTES));
./phppgadmin-master/tables.php-563-
##############################################
./phppgadmin-master/constraints.php-40-
nitially'] = null;
./phppgadmin-master/constraints.php:41:
$_REQUEST['target']);
./phppgadmin-master/constraints.php-42-
##############################################
./phppgadmin-master/constraints.php-130-                // Unserialize target
./phppgadmin-master/constraints.php:131:                $_POST['target'] = unserialize($_P
OST['target']);
./phppgadmin-master/constraints.php-132-
./phppgadmin-master/constraints.php-133-                // Check that they've given at least one c
```

```
       /_____/          \/            \/
          grep rough audit - static analysis tool
               v2.1 written by @Wireghoul
================================[justanotherhacker.com]===
phpipam-master/functions/PEAR/Net/DNS2/Cache/File.php-152-      */
phpipam-master/functions/PEAR/Net/DNS2/Cache/File.php:153:     public function __destruct()
phpipam-master/functions/PEAR/Net/DNS2/Cache/File.php-154-     {
phpipam-master/functions/PEAR/Net/DNS2/Cache/File.php-155-         //
phpipam-master/functions/PEAR/Net/DNS2/Cache/File.php-156-         // if there's no cache file set, then there's nothing to do
phpipam-master/functions/PEAR/Net/DNS2/Cache/File.php-157-         //
phpipam-master/functions/PEAR/Net/DNS2/Cache/File.php-158-         if (strlen($this->cache_file) == 0) {
phpipam-master/functions/PEAR/Net/DNS2/Cache/File.php-159-             return;
phpipam-master/functions/PEAR/Net/DNS2/Cache/File.php-160-         }
phpipam-master/functions/PEAR/Net/DNS2/Cache/File.php-161-
phpipam-master/functions/PEAR/Net/DNS2/Cache/File.php-162-         //
phpipam-master/functions/PEAR/Net/DNS2/Cache/File.php-163-         // open the file for reading/writing
phpipam-master/functions/PEAR/Net/DNS2/Cache/File.php-164-         //
phpipam-master/functions/PEAR/Net/DNS2/Cache/File.php-165-         $fp = fopen($this->cache_file, 'a+');
phpipam-master/functions/PEAR/Net/DNS2/Cache/File.php-166-         if ($fp !== false) {
phpipam-master/functions/PEAR/Net/DNS2/Cache/File.php-167-
phpipam-master/functions/PEAR/Net/DNS2/Cache/File.php-168-             //
phpipam-master/functions/PEAR/Net/DNS2/Cache/File.php-169-             // lock the file just in case
phpipam-master/functions/PEAR/Net/DNS2/Cache/File.php-170-             //
phpipam-master/functions/PEAR/Net/DNS2/Cache/File.php-171-             flock($fp, LOCK_EX);
phpipam-master/functions/PEAR/Net/DNS2/Cache/File.php-172-
phpipam-master/functions/PEAR/Net/DNS2/Cache/File.php-173-             //
###############################################
phpipam-master/functions/PEAR/Net/DNS2/Cache/Shm.php-187-      */
phpipam-master/functions/PEAR/Net/DNS2/Cache/Shm.php:188:     public function __destruct()
phpipam-master/functions/PEAR/Net/DNS2/Cache/Shm.php-189-     {
phpipam-master/functions/PEAR/Net/DNS2/Cache/Shm.php-190-         //
phpipam-master/functions/PEAR/Net/DNS2/Cache/Shm.php-191-         // if there's no cache file set, then there's nothing to do
phpipam-master/functions/PEAR/Net/DNS2/Cache/Shm.php-192-         //
phpipam-master/functions/PEAR/Net/DNS2/Cache/Shm.php-193-         if (strlen($this->cache_file) == 0) {
phpipam-master/functions/PEAR/Net/DNS2/Cache/Shm.php-194-             return;
phpipam-master/functions/PEAR/Net/DNS2/Cache/Shm.php-195-         }
phpipam-master/functions/PEAR/Net/DNS2/Cache/Shm.php-196-
phpipam-master/functions/PEAR/Net/DNS2/Cache/Shm.php-197-         $fp = fopen($this->cache_file, 'r');
--
phpipam-master/functions/PEAR/Net/DNS2/Socket.php-121-
phpipam-master/functions/PEAR/Net/DNS2/Socket.php-122-     /**
phpipam-master/functions/PEAR/Net/DNS2/Socket.php-123-      * sets the local address/port for the socket to bind to
phpipam-master/functions/PEAR/Net/DNS2/Socket.php-124-      *
```

Buffer overflow

```
#!/bin/sh
VERSION=0.1
if [ -z "$1" ]; then
    echo "Usage: $0 /path/to/check‟
    exit 2
Fi
echo 'char[[:space:]]+[a-zA-Z0-9\.\-\_][a-zA-Z0-9\.\-\_]+\[' | ~/flatline/graudit -B -z -d - "$1" | \
perl -ne 'if ($_ =~ m/char\s+([a-zA-Z0-9\.\-\_]+)\[/) {
    @rulz=(
      "strc(at|py)[[:space:]]*\\(",
      "sprintf[[:space:]]*\\(“,
     );
    print "$1\n" . join("\n", map $_."$1", @rulz) . "\n";
}' | \sort | uniq | \~/flatline/graudit -c 3 -B -d - "$1"
```

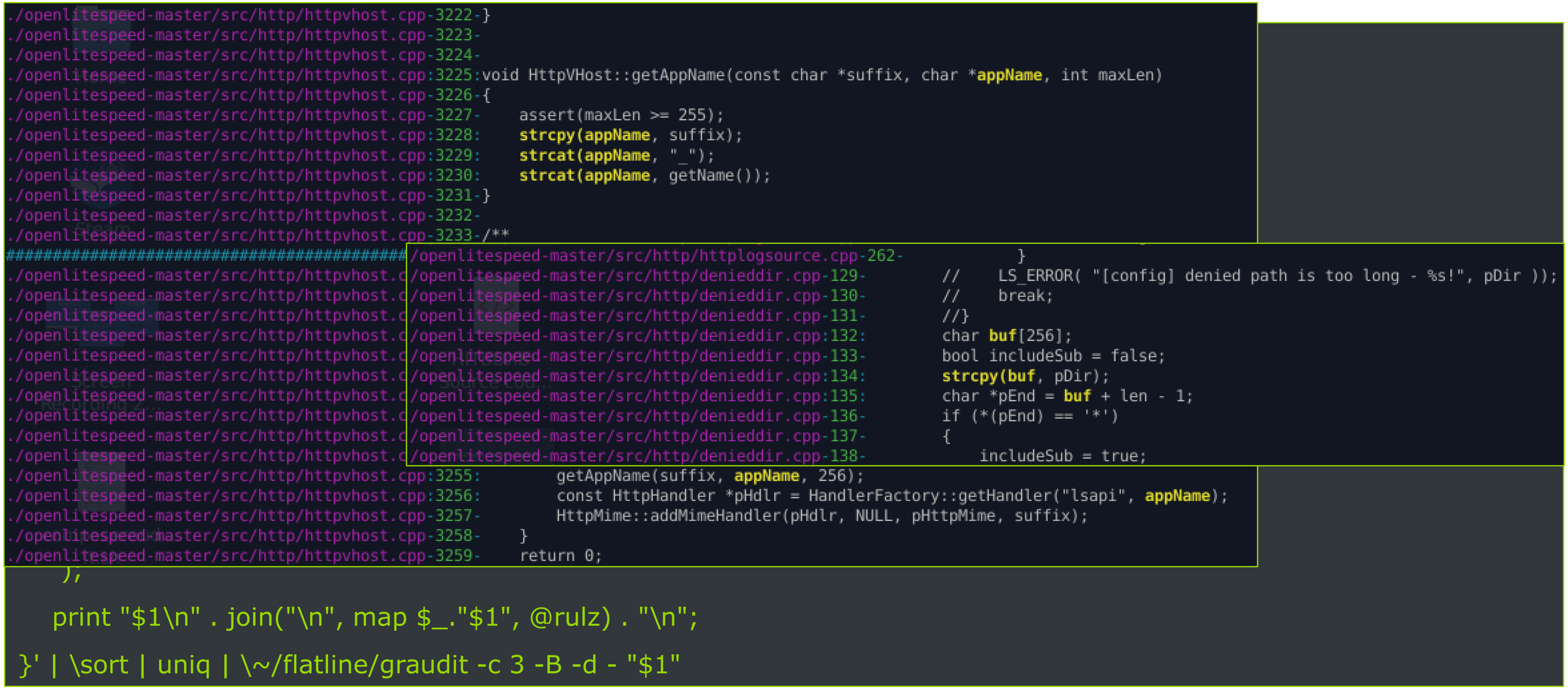
Buffer overflow



```
./openlitespeed-master/src/http/httpvhost.cpp-3222-}
./openlitespeed-master/src/http/httpvhost.cpp-3223-
./openlitespeed-master/src/http/httpvhost.cpp-3224-
./openlitespeed-master/src/http/httpvhost.cpp:3225:void HttpVHost::getAppName(const char *suffix, char *appName, int maxLen)
./openlitespeed-master/src/http/httpvhost.cpp-3226-{
./openlitespeed-master/src/http/httpvhost.cpp-3227-    assert(maxLen >= 255);
./openlitespeed-master/src/http/httpvhost.cpp:3228:    strcpy(appName, suffix);
./openlitespeed-master/src/http/httpvhost.cpp:3229:    strcat(appName, "_");
./openlitespeed-master/src/http/httpvhost.cpp:3230:    strcat(appName, getName());
./openlitespeed-master/src/http/httpvhost.cpp-3231-}
./openlitespeed-master/src/http/httpvhost.cpp-3232-
./openlitespeed-master/src/http/httpvhost.cpp-3233-/**
###############################################
./openlitespeed-master/src/http/httpvhost.cpp-3245-    HttpMime *pHttpMime = getMIME();
./openlitespeed-master/src/http/httpvhost.cpp-3246-    const char *suffix  = NULL;
./openlitespeed-master/src/http/httpvhost.cpp-3247-    php_xml_st *pPhpXmlNodeS;
./openlitespeed-master/src/http/httpvhost.cpp:3248:    char appName[256];
./openlitespeed-master/src/http/httpvhost.cpp-3249-
./openlitespeed-master/src/http/httpvhost.cpp-3250-    //HttpMime::configScriptHandler(pList, getMIME(), this);
./openlitespeed-master/src/http/httpvhost.cpp-3251-    for (int i=0; i<getPhpXmlNodeSSize(); ++i)
./openlitespeed-master/src/http/httpvhost.cpp-3252-    {
./openlitespeed-master/src/http/httpvhost.cpp-3253-        pPhpXmlNodeS = getPhpXmlNodeS(i);
./openlitespeed-master/src/http/httpvhost.cpp-3254-        suffix = pPhpXmlNodeS->suffix.c_str();
./openlitespeed-master/src/http/httpvhost.cpp:3255:        getAppName(suffix, appName, 256);
./openlitespeed-master/src/http/httpvhost.cpp:3256:        const HttpHandler *pHdlr = HandlerFactory::getHandler("lsapi", appName);
./openlitespeed-master/src/http/httpvhost.cpp-3257-        HttpMime::addMimeHandler(pHdlr, NULL, pHttpMime, suffix);
./openlitespeed-master/src/http/httpvhost.cpp-3258-    }
./openlitespeed-master/src/http/httpvhost.cpp-3259-    return 0;
```

```
    );
    print "$1\n" . join("\n", map $_."$1", @rulz) . "\n";
}' | \sort | uniq | \~/flatline/graudit -c 3 -B -d - "$1"
```

Buffer overflow



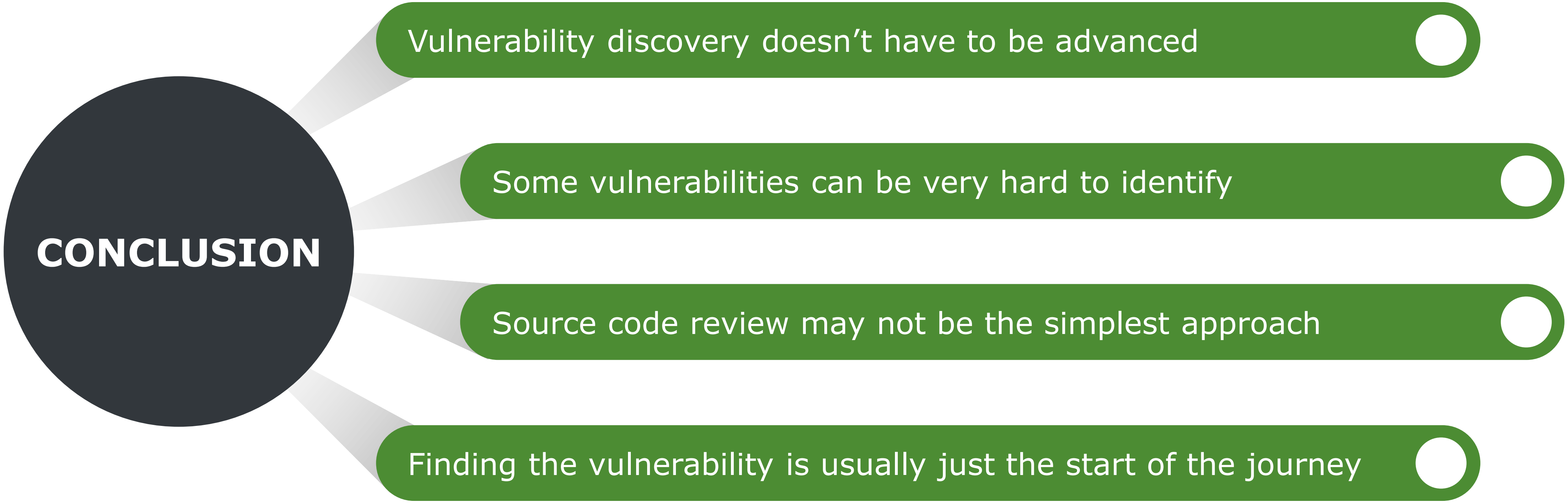
```
./openlitespeed-master/src/http/httpvhost.cpp-3222-}
./openlitespeed-master/src/http/httpvhost.cpp-3223-
./openlitespeed-master/src/http/httpvhost.cpp-3224-
./openlitespeed-master/src/http/httpvhost.cpp:3225:void HttpVHost::getAppName(const char *suffix, char *appName, int maxLen)
./openlitespeed-master/src/http/httpvhost.cpp-3226-{
./openlitespeed-master/src/http/httpvhost.cpp-3227-    assert(maxLen >= 255);
./openlitespeed-master/src/http/httpvhost.cpp:3228:    strcpy(appName, suffix);
./openlitespeed-master/src/http/httpvhost.cpp:3229:    strcat(appName, "_");
./openlitespeed-master/src/http/httpvhost.cpp:3230:    strcat(appName, getName());
./openlitespeed-master/src/http/httpvhost.cpp-3231-}
./openlitespeed-master/src/http/httpvhost.cpp-3232-
./openlitespeed-master/src/http/httpvhost.cpp-3233-/**
############################################
./openlitespeed-master/src/http/httpvhost.c
./openlitespeed-master/src/http/httpvhost.c
./openlitespeed-master/src/http/httpvhost.c
./openlitespeed-master/src/http/httpvhost.c
./openlitespeed-master/src/http/httpvhost.c
./openlitespeed-master/src/http/httpvhost.c
./openlitespeed-master/src/http/httpvhost.c
./openlitespeed-master/src/http/httpvhost.c
./openlitespeed-master/src/http/httpvhost.c
./openlitespeed-master/src/http/httpvhost.c
./openlitespeed-master/src/http/httpvhost.cpp:3255:        getAppName(suffix, appName, 256);
./openlitespeed-master/src/http/httpvhost.cpp:3256:        const HttpHandler *pHdlr = HandlerFactory::getHandler("lsapi", appName);
./openlitespeed-master/src/http/httpvhost.cpp-3257-        HttpMime::addMimeHandler(pHdlr, NULL, pHttpMime, suffix);
./openlitespeed-master/src/http/httpvhost.cpp-3258-    }
./openlitespeed-master/src/http/httpvhost.cpp-3259-    return 0;
```

```
/openlitespeed-master/src/http/httplogsource.cpp-262-            }
/openlitespeed-master/src/http/denieddir.cpp-129-        //    LS_ERROR( "[config] denied path is too long - %s!", pDir ));
/openlitespeed-master/src/http/denieddir.cpp-130-        //    break;
/openlitespeed-master/src/http/denieddir.cpp-131-        //}
/openlitespeed-master/src/http/denieddir.cpp:132:        char buf[256];
/openlitespeed-master/src/http/denieddir.cpp-133-        bool includeSub = false;
/openlitespeed-master/src/http/denieddir.cpp:134:        strcpy(buf, pDir);
/openlitespeed-master/src/http/denieddir.cpp:135:        char *pEnd = buf + len - 1;
/openlitespeed-master/src/http/denieddir.cpp-136-        if (*(pEnd) == '*')
/openlitespeed-master/src/http/denieddir.cpp-137-        {
/openlitespeed-master/src/http/denieddir.cpp-138-            includeSub = true;
```

```
    );
    print "$1\n" . join("\n", map $_."$1", @rulz) . "\n";
}' | \sort | uniq | \~/flatline/graudit -c 3 -B -d - "$1"
```

06

Conclusion



CONCLUSION

- Vulnerability discovery doesn’t have to be advanced
- Some vulnerabilities can be very hard to identify
- Source code review may not be the simplest approach
- Finding the vulnerability is usually just the start of the journey

Questions?