Bug hunting

with grep

$(whoami)

- Hacker
- Speaker
- Trainer
- Wireghoul

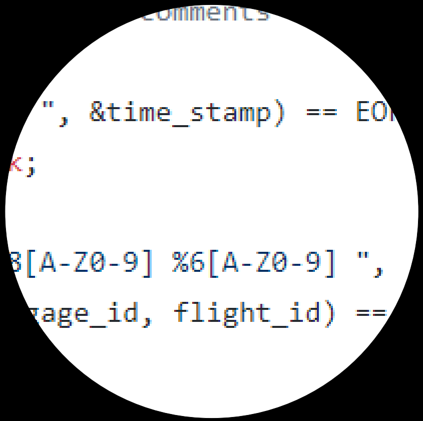
www.justanotherhacker.com

Bug hunting

- Collecting enough information to get
  - CVE
  - Shell

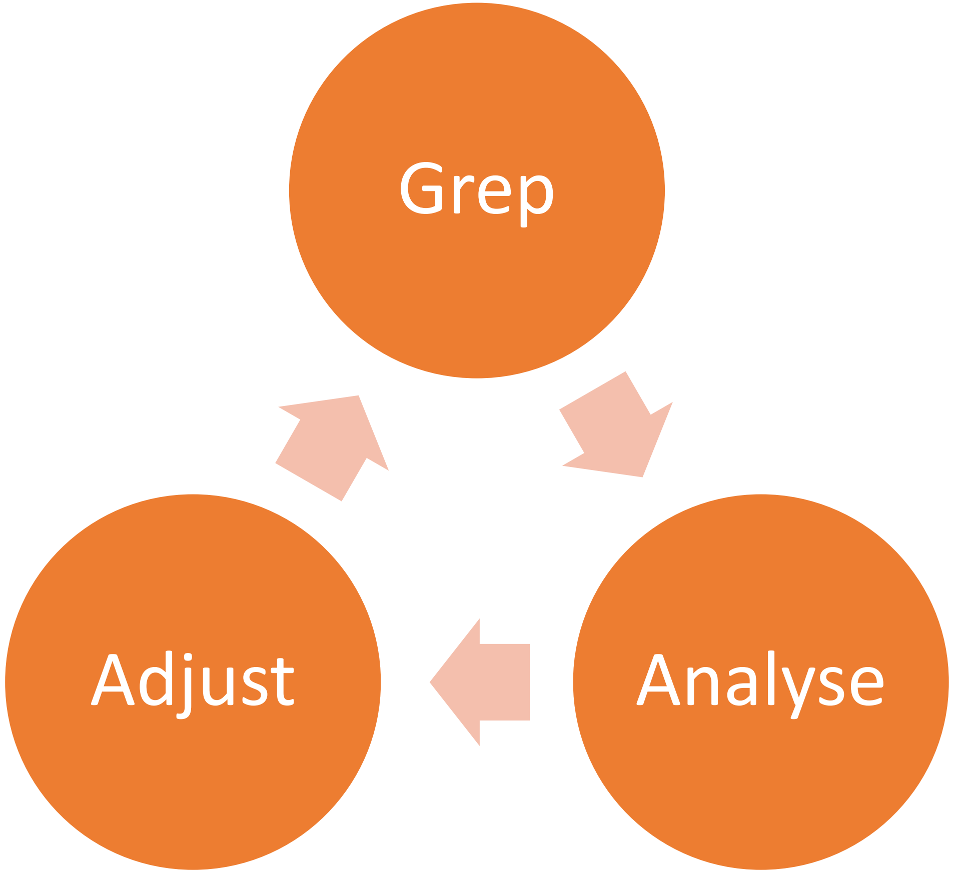
Bug hunting with grep

- Finding vulnerability candidates in source code
- grep is a filter
- Human analysis is required



```
comments

", &time_stamp) == EO
k;

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

Process



2grep ||

! 2grep

Benefits of grep

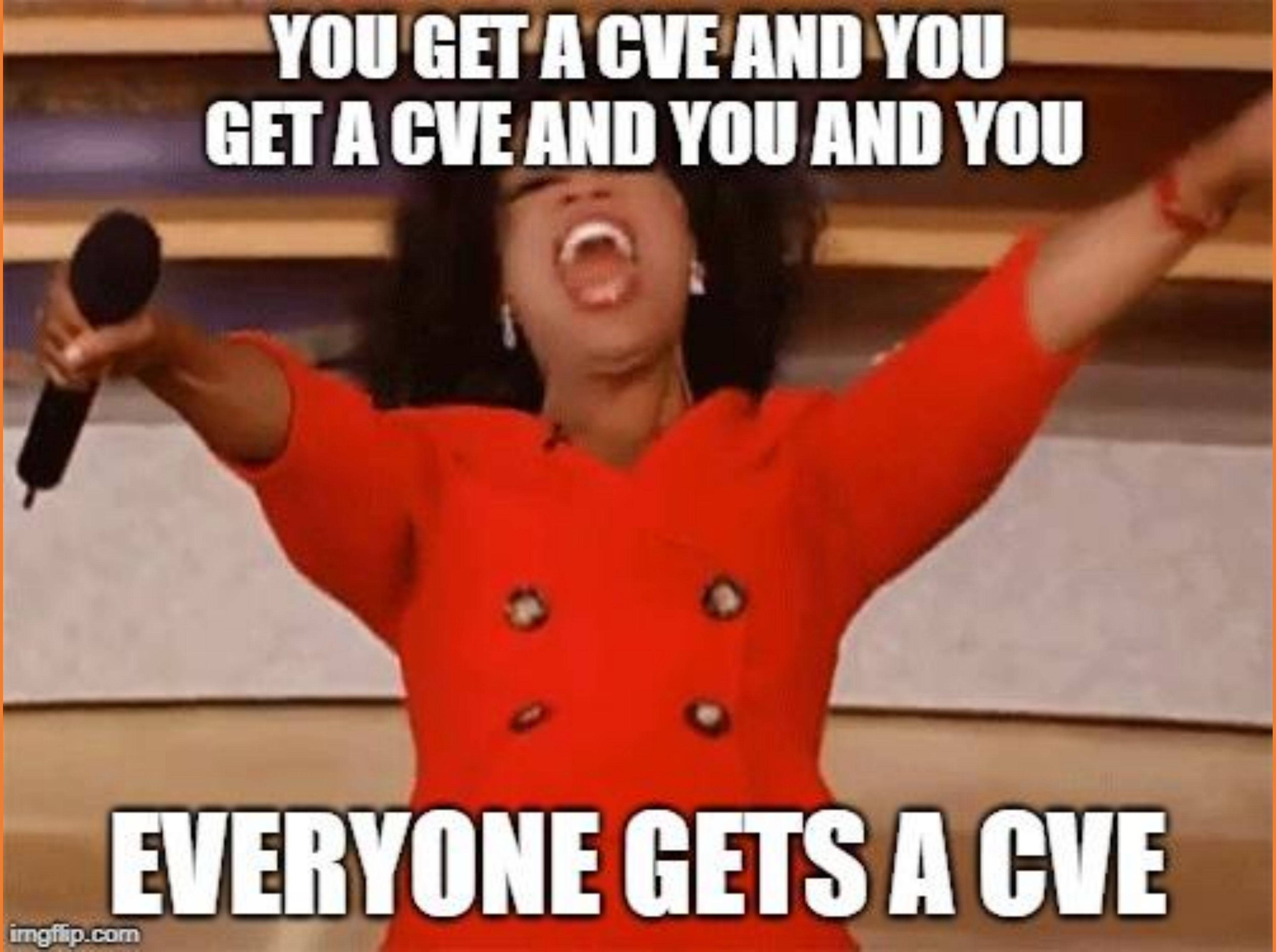
- Can be used on partial code
- Versatile cross platform support
- /Regex/
- Most programming languages are text based
- Easy to add support for new languages or frameworks
- Shows code directly

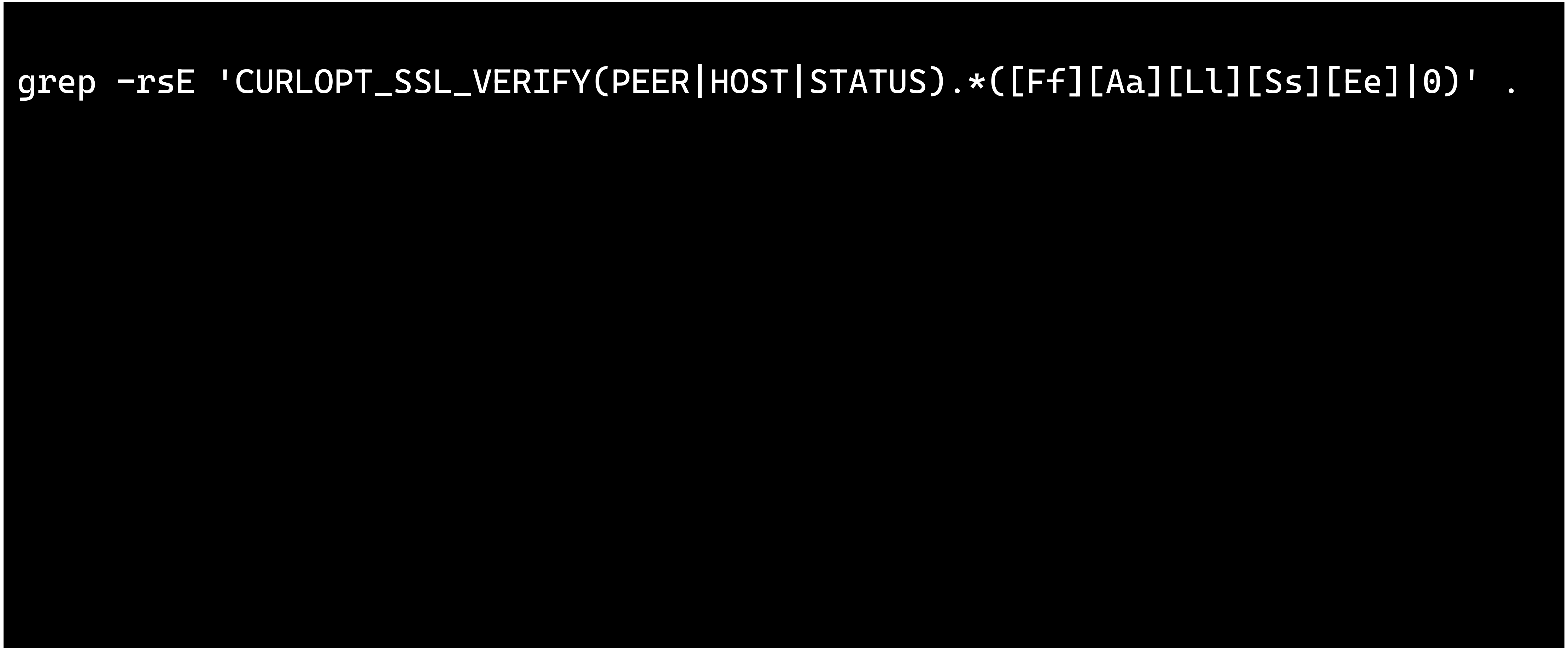
Limitations of grep

- Matching across lines
- Semantic understanding
- Only as good as the regex

Not greps

- coccinelle
- semgrep
- ripgrep
- more


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

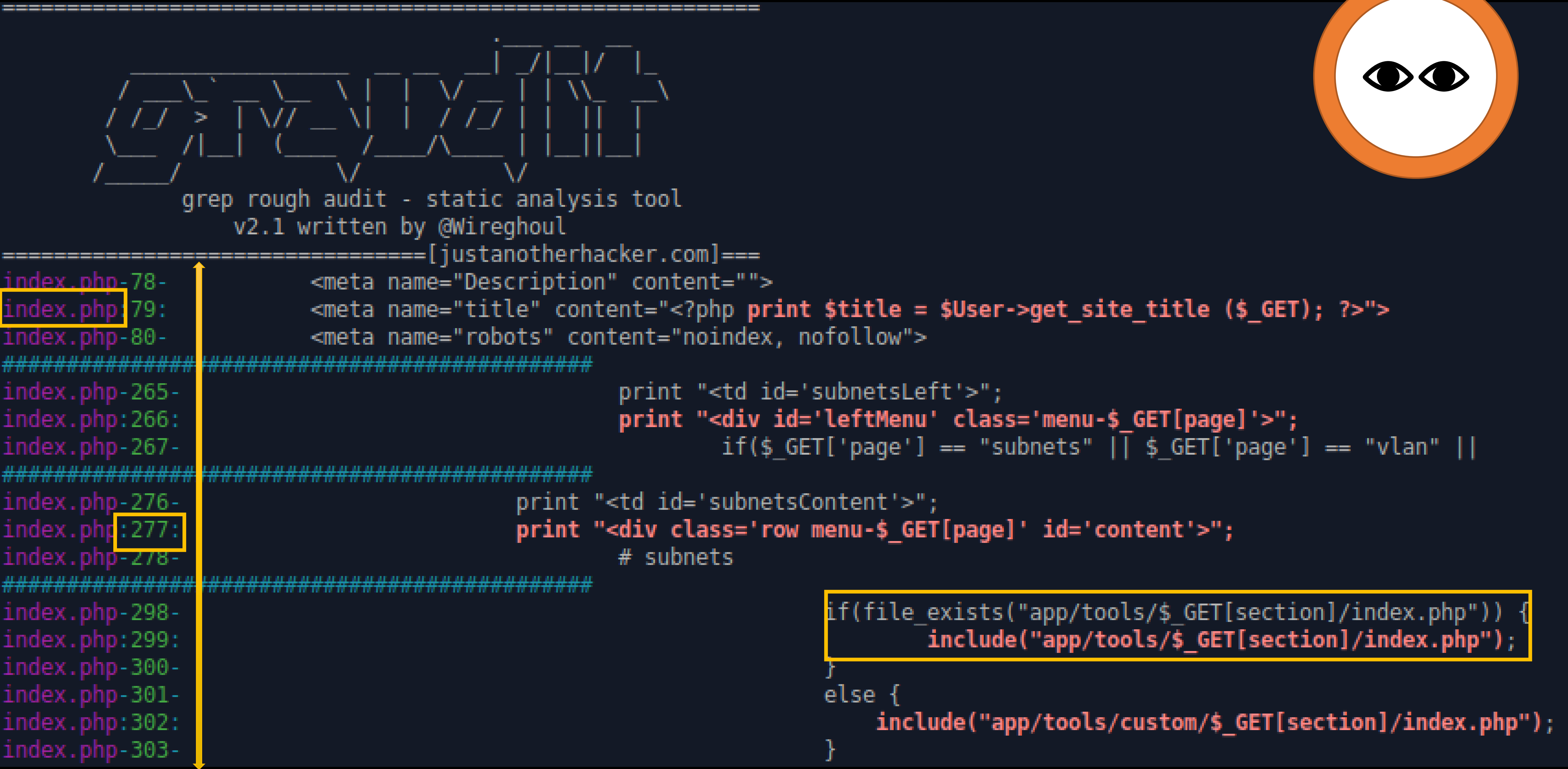


```
grep -rsE 'CURLOPT_SSL_VERIFY(PEER|HOST|STATUS).*([Ff][Aa][Ll][Ss][Ee]|0)' .
```

SSL/TLS Validation Failure

graudit

https://github.com/wireghoul/graudit



```
============================================================
                                       .___.__  __
          ________________   __ __  __| _/|__|/  |_
         / ___\_  __ \__  \ |  |  \/ __ | |  \   __\
        / /_/  >  | \// __ \|  |  / /_/ | |  ||  |
        \___  /|__|  (____  /____/\____ | |__||__|
       /_____/            \/           \/
              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-                                                  }
```

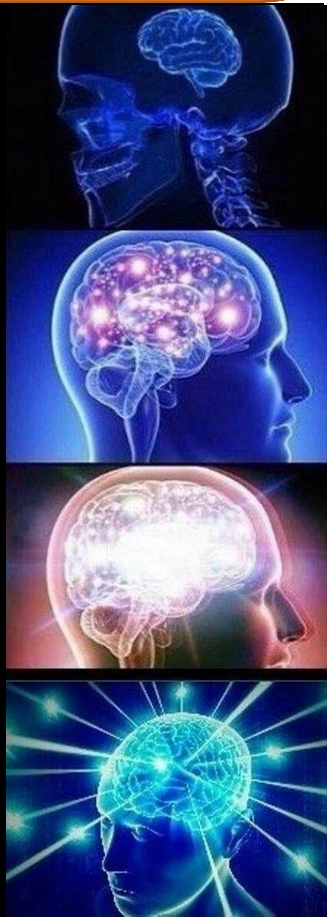
WHENEVER I LEARN A NEW SKILL I CONCOCT ELABORATE FANTASY SCENARIOS WHERE IT LETS ME SAVE THE DAY.
OH NO! THE KILLER MUST HAVE FOLLOWED HER ON VACATION!
BUT TO FIND THEM WE'D HAVE TO SEARCH THROUGH 200 MB OF EMAILS LOOKING FOR SOMETHING FORMATTED LIKE AN ADDRESS!
IT'S HOPELESS!
EVERYBODY STAND BACK.
I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

Regex

- Basic
- Extended
- PCRE

Rules

```
require

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

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

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



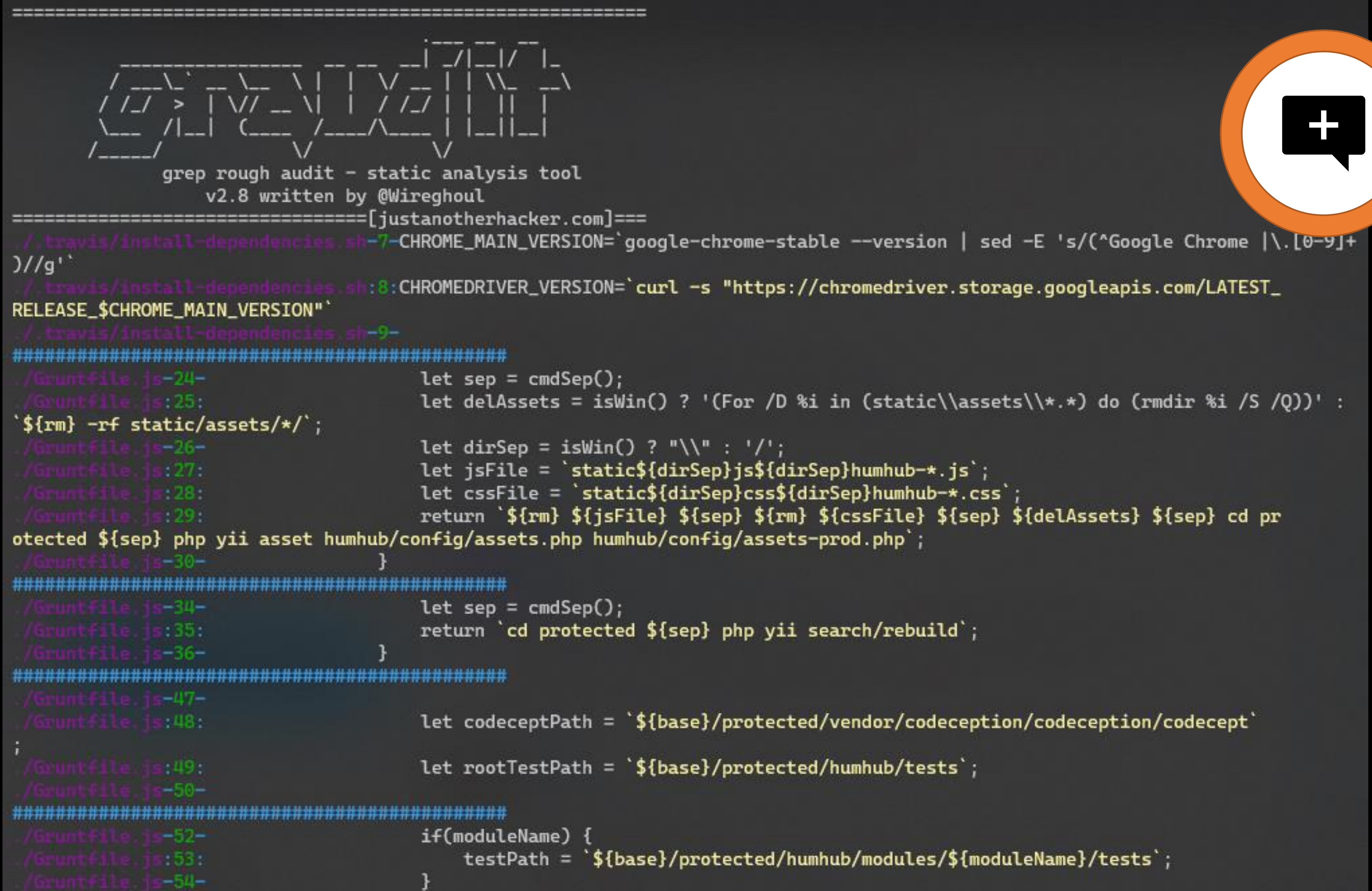
AMPscript / SSJS

```
runat
%%=[^%]+\@[^%]+=%%
%%\[
\]%%
[Rr][Ee][Qq][Uu][Ee][Ss][Tt][Pp][Aa][Rr][Aa
][Mm][Ee][Tt][Ee][Rr][[:space:]]*\(
Invoke(Create|Delete|Execute|Perform|Retrie
ve)
RaiseError[[:space:]]\(.*\@
SetObjectProperty
UpsertContact
AttachFile
BarCodeURL
BuildRowSetFrom(String|XML)
(Create|End|Set)SmsConversation(NextKeyword
)?
TreatAsContent(Area)?
ClaimRow(Value)?
CataExtensionRowCount
DeleteD(E|ata)[[:space:]]*\(
ExecuteFilter(OrderedRows)?
```

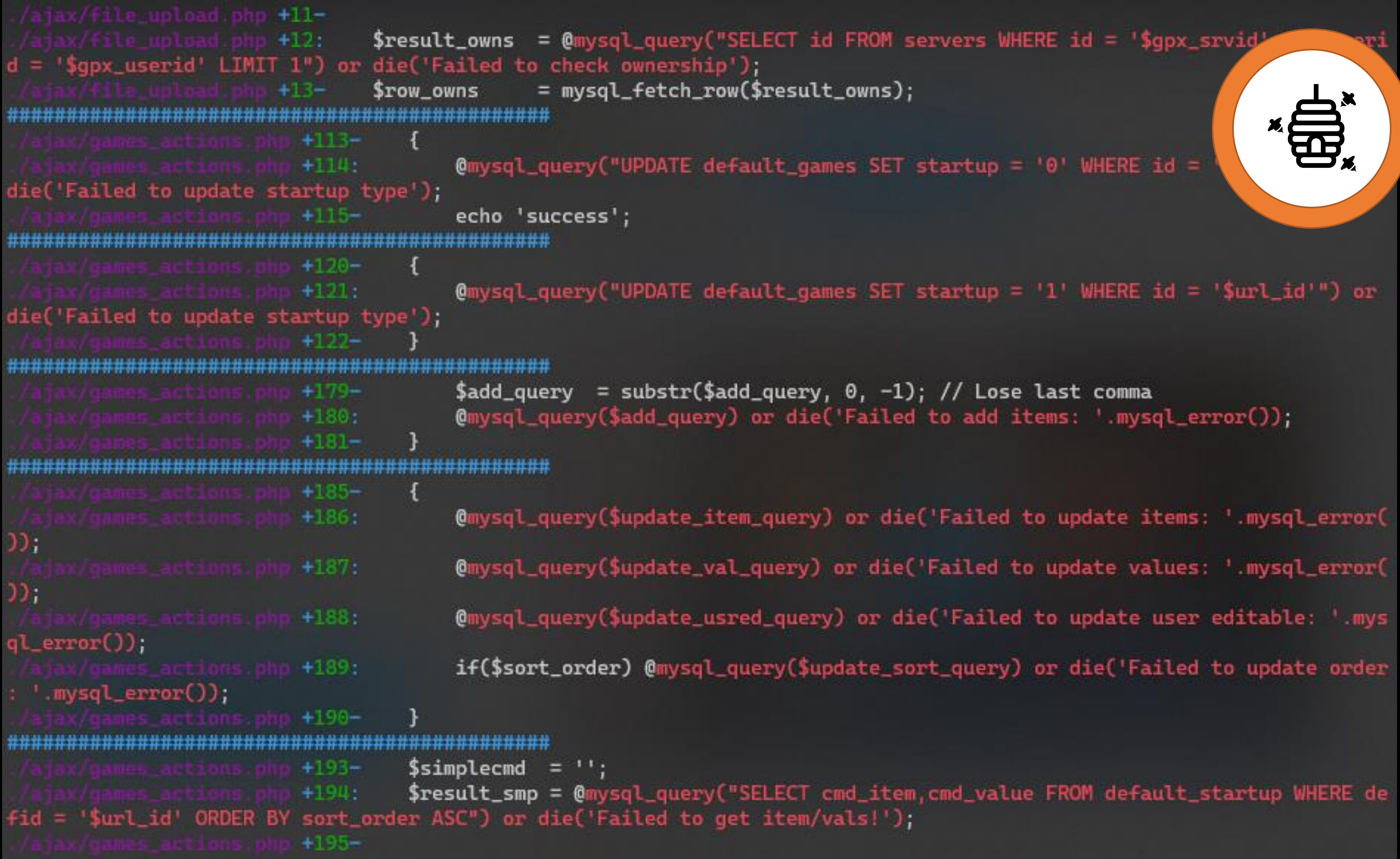
```
InsertD(E|ata)
Lookup[[:space:]]\([^,]+,[^,]+,[^,]+,[^,]+
Lookup(Ordered)?(Rows|RowsCS)
UpdateD(E|ata)[[:space:]]*\(
UpsertD(E|ata)[[:space:]]*\(
Base64(En|De)code[[:space:]]*\(
(En|De)cryptSymmetric
MD5[[:space:]]*\(
SHA(1|256|512)[[:space:]]*\(
HTTP(Get|Post|Post2|RequestHeader)
(Update|Upsert|SetState|Create|Retrieve)Msc
rmRecords?(FetchXML)?
AddMscrmListMember
DescribeMscrmEntit(ies|yAttributes)
(Create|Retrieve|UpdateSingle)Salesforce(Ob
ject|JobSource)s?
eval[[:space:]]*\([^\)\;]+[\'\"][[:space:]]
*\+[[:space:]]*[^\'\"]+
[\"\'][[Ss][Ee][Ll][Ee][Cc][Tt][[:space:]]+
```

Noise/Signal

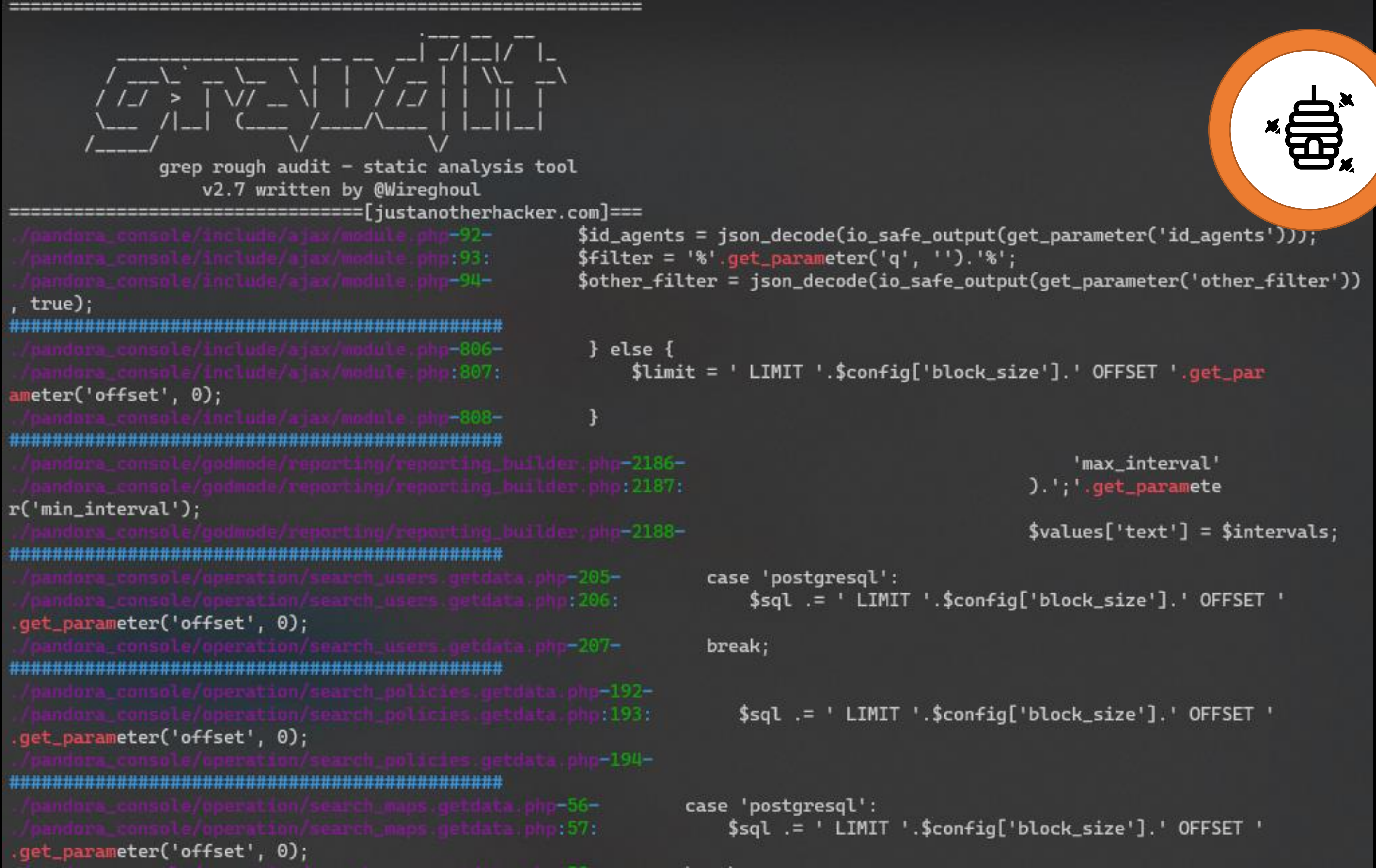
```
graudit -d php .

graudit -d default .

echo "rule" | graudit -d - .

graudit -d php/ssl .

graudit -d fruit .

graudit -d flatline .
```



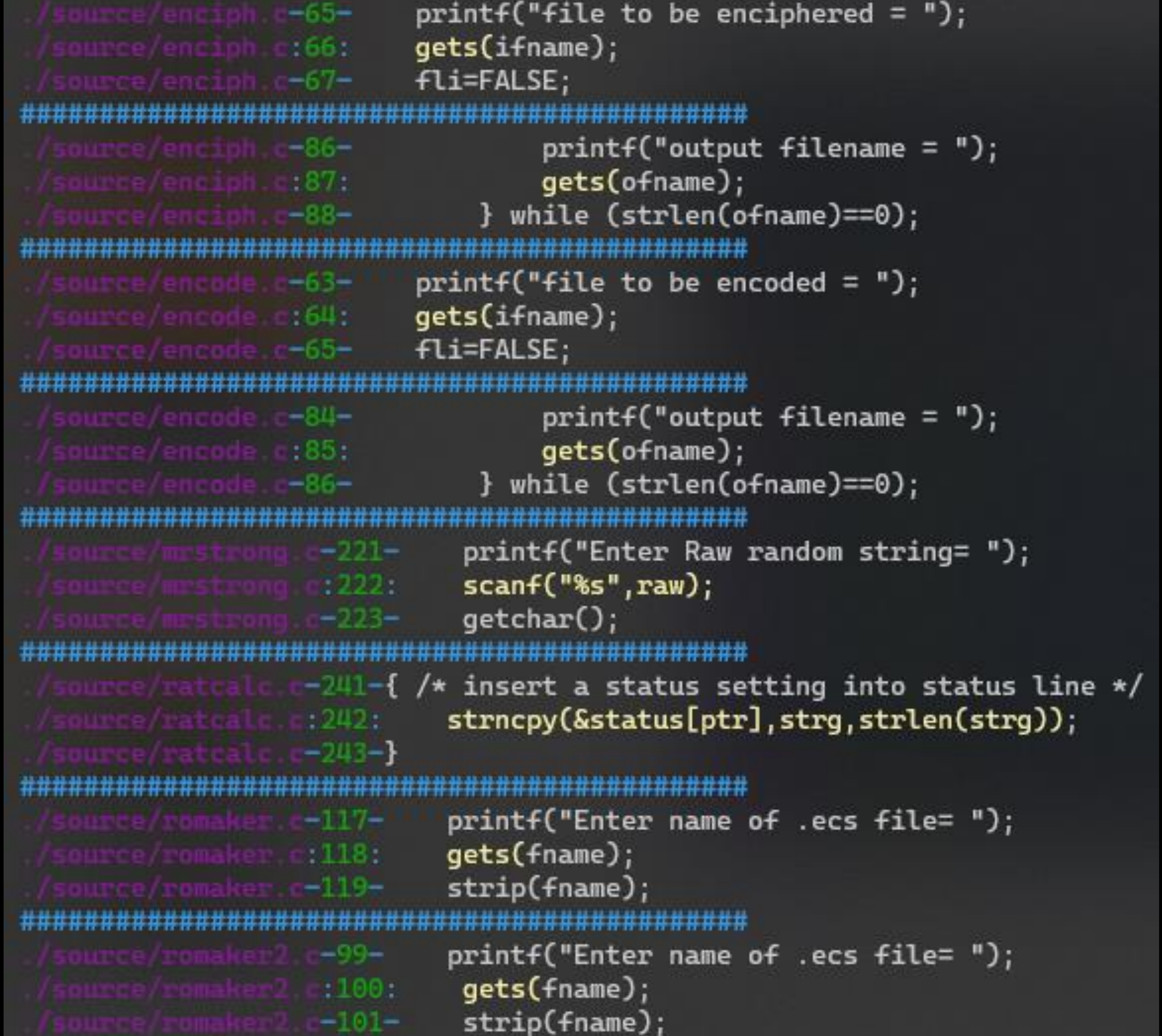
```
===========================================================
                                      .___ __  __
          _________________  __ __  __| _/|__|/  |_
         / ___\_` __ \__  \ |  |  \/ __ | | \\_  __\
        / /_/  >  | \// __ \|  |  / /_/ | |  ||  |
        \___  /|__|  (____  /____/\____ | |__||__|
       /_____/            \/           \/
              grep rough audit - static analysis tool
                  v2.8 written by @Wireghoul
=================================[justanotherhacker.com]===
./.travis/install-dependencies.sh-7-CHROME_MAIN_VERSION=`google-chrome-stable --version | sed -E 's/(^Google Chrome |\.[0-9]+
)//g'`
./.travis/install-dependencies.sh:8:CHROMEDRIVER_VERSION=`curl -s "https://chromedriver.storage.googleapis.com/LATEST_
RELEASE_$CHROME_MAIN_VERSION"`
./.travis/install-dependencies.sh-9-
##############################################
./Gruntfile.js-24-                  let sep = cmdSep();
./Gruntfile.js:25:                  let delAssets = isWin() ? '(For /D %i in (static\\assets\\*.*) do (rmdir %i /S /Q))' :
`${rm} -rf static/assets/*/`;
./Gruntfile.js-26-                  let dirSep = isWin() ? "\\" : '/';
./Gruntfile.js:27:                  let jsFile = `static${dirSep}js${dirSep}humhub-*.js`;
./Gruntfile.js:28:                  let cssFile = `static${dirSep}css${dirSep}humhub-*.css`;
./Gruntfile.js:29:                  return `${rm} ${jsFile} ${sep} ${rm} ${cssFile} ${sep} ${delAssets} ${sep} cd pr
otected ${sep} php yii asset humhub/config/assets.php humhub/config/assets-prod.php`;
./Gruntfile.js-30-              }
##############################################
./Gruntfile.js-34-                  let sep = cmdSep();
./Gruntfile.js:35:                  return `cd protected ${sep} php yii search/rebuild`;
./Gruntfile.js-36-              }
##############################################
./Gruntfile.js-47-
./Gruntfile.js:48:                  let codeceptPath = `${base}/protected/vendor/codeception/codeception/codecept`
;
./Gruntfile.js:49:                  let rootTestPath = `${base}/protected/humhub/tests`;
./Gruntfile.js-50-
##############################################
./Gruntfile.js-52-                  if(moduleName) {
./Gruntfile.js:53:                      testPath = `${base}/protected/humhub/modules/${moduleName}/tests`;
./Gruntfile.js-54-                  }
```



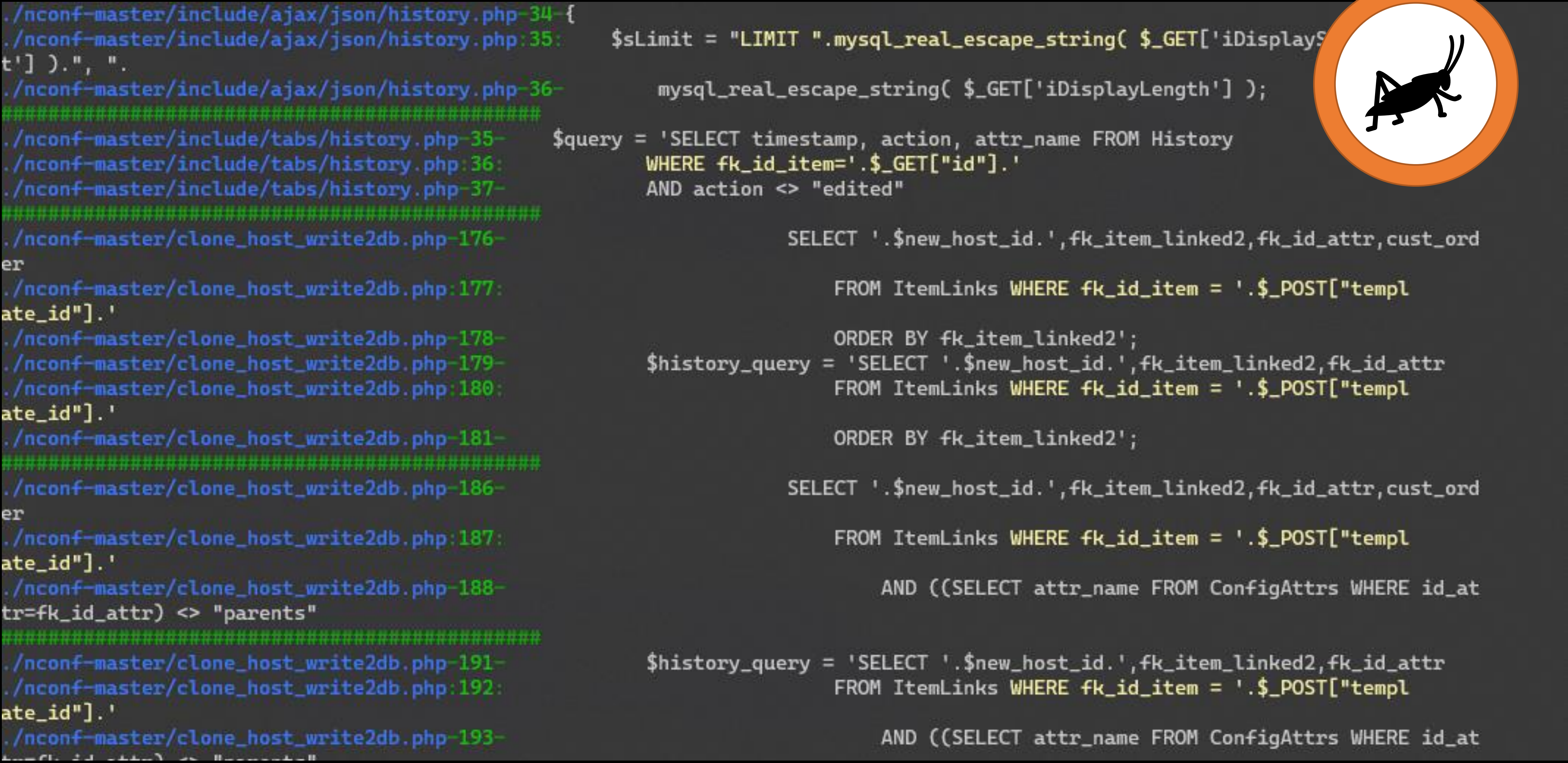
```
./ajax/file_upload.php +11-
./ajax/file_upload.php +12:     $result_owns  = @mysql_query("SELECT id FROM servers WHERE id = '$gpx_srvid'       eri
d = '$gpx_userid' LIMIT 1") or die('Failed to check ownership');
./ajax/file_upload.php +13-     $row_owns     = mysql_fetch_row($result_owns);
##############################################
./ajax/games_actions.php +113-    {
./ajax/games_actions.php +114:        @mysql_query("UPDATE default_games SET startup = '0' WHERE id = '
die('Failed to update startup type');
./ajax/games_actions.php +115-        echo 'success';
##############################################
./ajax/games_actions.php +120-    {
./ajax/games_actions.php +121:        @mysql_query("UPDATE default_games SET startup = '1' WHERE id = '$url_id'") or
die('Failed to update startup type');
./ajax/games_actions.php +122-    }
##############################################
./ajax/games_actions.php +179-        $add_query  = substr($add_query, 0, -1); // Lose last comma
./ajax/games_actions.php +180:        @mysql_query($add_query) or die('Failed to add items: '.mysql_error());
./ajax/games_actions.php +181-    }
##############################################
./ajax/games_actions.php +185-    {
./ajax/games_actions.php +186:        @mysql_query($update_item_query) or die('Failed to update items: '.mysql_error(
));
./ajax/games_actions.php +187:        @mysql_query($update_val_query) or die('Failed to update values: '.mysql_error(
));
./ajax/games_actions.php +188:        @mysql_query($update_usred_query) or die('Failed to update user editable: '.mys
ql_error());
./ajax/games_actions.php +189:        if($sort_order) @mysql_query($update_sort_query) or die('Failed to update order
: '.mysql_error());
./ajax/games_actions.php +190-    }
##############################################
./ajax/games_actions.php +193-    $simplecmd  = '';
./ajax/games_actions.php +194:    $result_smp = @mysql_query("SELECT cmd_item,cmd_value FROM default_startup WHERE de
fid = '$url_id' ORDER BY sort_order ASC") or die('Failed to get item/vals!');
./ajax/games_actions.php +195-
```



```
===========================================================
                                        .___ __  __
          _________________  __ __  __| _/|__|/  |_
         / ___\_`  __ \__  \ |  |  \/ __ | |  \   __\
        / /_/  >  | \// __ \|  |  / /_/ | |  ||  |
        \___  /|__|  (____  /____/\____ | |__||__|
       /_____/             \/           \/
              grep rough audit - static analysis tool
                  v2.7 written by @Wireghoul
=================================[justanotherhacker.com]===
./pandora_console/include/ajax/module.php-92-          $id_agents = json_decode(io_safe_output(get_parameter('id_agents')));
./pandora_console/include/ajax/module.php:93:          $filter = '%'.get_parameter('q', '').'%';
./pandora_console/include/ajax/module.php-94-          $other_filter = json_decode(io_safe_output(get_parameter('other_filter'))
, true);
##############################################
./pandora_console/include/ajax/module.php-806-          } else {
./pandora_console/include/ajax/module.php:807:              $limit = ' LIMIT '.$config['block_size'].' OFFSET '.get_par
ameter('offset', 0);
./pandora_console/include/ajax/module.php-808-          }
##############################################
./pandora_console/godmode/reporting/reporting_builder.php-2186-                                   'max_interval'
./pandora_console/godmode/reporting/reporting_builder.php:2187:                               ).';'.get_paramete
r('min_interval');
./pandora_console/godmode/reporting/reporting_builder.php-2188-                               $values['text'] = $intervals;
##############################################
./pandora_console/operation/search_users.getdata.php-205-          case 'postgresql':
./pandora_console/operation/search_users.getdata.php:206:              $sql .= ' LIMIT '.$config['block_size'].' OFFSET '
.get_parameter('offset', 0);
./pandora_console/operation/search_users.getdata.php-207-          break;
##############################################
./pandora_console/operation/search_policies.getdata.php-192-
./pandora_console/operation/search_policies.getdata.php:193:          $sql .= ' LIMIT '.$config['block_size'].' OFFSET '
.get_parameter('offset', 0);
./pandora_console/operation/search_policies.getdata.php-194-
##############################################
./pandora_console/operation/search_maps.getdata.php-56-          case 'postgresql':
./pandora_console/operation/search_maps.getdata.php:57:              $sql .= ' LIMIT '.$config['block_size'].' OFFSET '
.get_parameter('offset', 0);
```



```
./source/enciph.c-65-    printf("file to be enciphered = ");
./source/enciph.c:66:    gets(ifname);
./source/enciph.c-67-    fli=FALSE;
##############################################
./source/enciph.c-86-            printf("output filename = ");
./source/enciph.c:87:            gets(ofname);
./source/enciph.c-88-        } while (strlen(ofname)==0);
##############################################
./source/encode.c-63-    printf("file to be encoded = ");
./source/encode.c:64:    gets(ifname);
./source/encode.c-65-    fli=FALSE;
##############################################
./source/encode.c-84-            printf("output filename = ");
./source/encode.c:85:            gets(ofname);
./source/encode.c-86-        } while (strlen(ofname)==0);
##############################################
./source/mrstrong.c-221-    printf("Enter Raw random string= ");
./source/mrstrong.c:222:    scanf("%s",raw);
./source/mrstrong.c-223-    getchar();
##############################################
./source/ratcalc.c-241-{ /* insert a status setting into status line */
./source/ratcalc.c:242:    strncpy(&status[ptr],strg,strlen(strg));
./source/ratcalc.c-243-}
##############################################
./source/romaker.c-117-    printf("Enter name of .ecs file= ");
./source/romaker.c:118:    gets(fname);
./source/romaker.c-119-    strip(fname);
##############################################
./source/romaker2.c-99-    printf("Enter name of .ecs file= ");
./source/romaker2.c:100:    gets(fname);
./source/romaker2.c-101-    strip(fname);
```

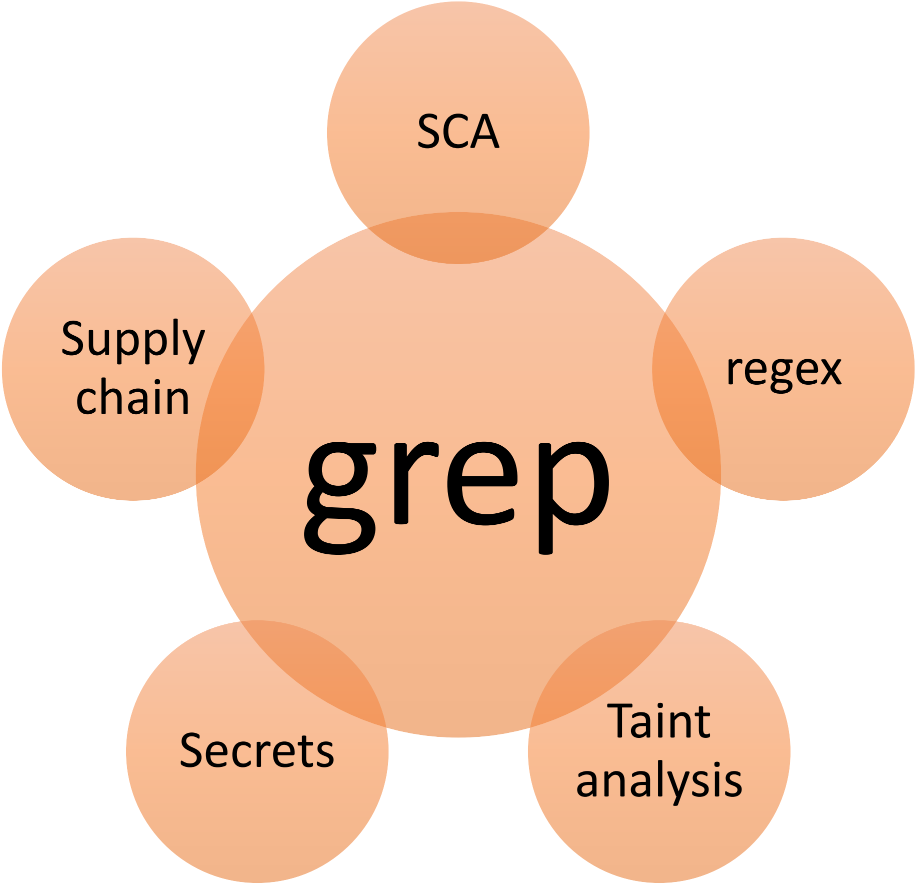


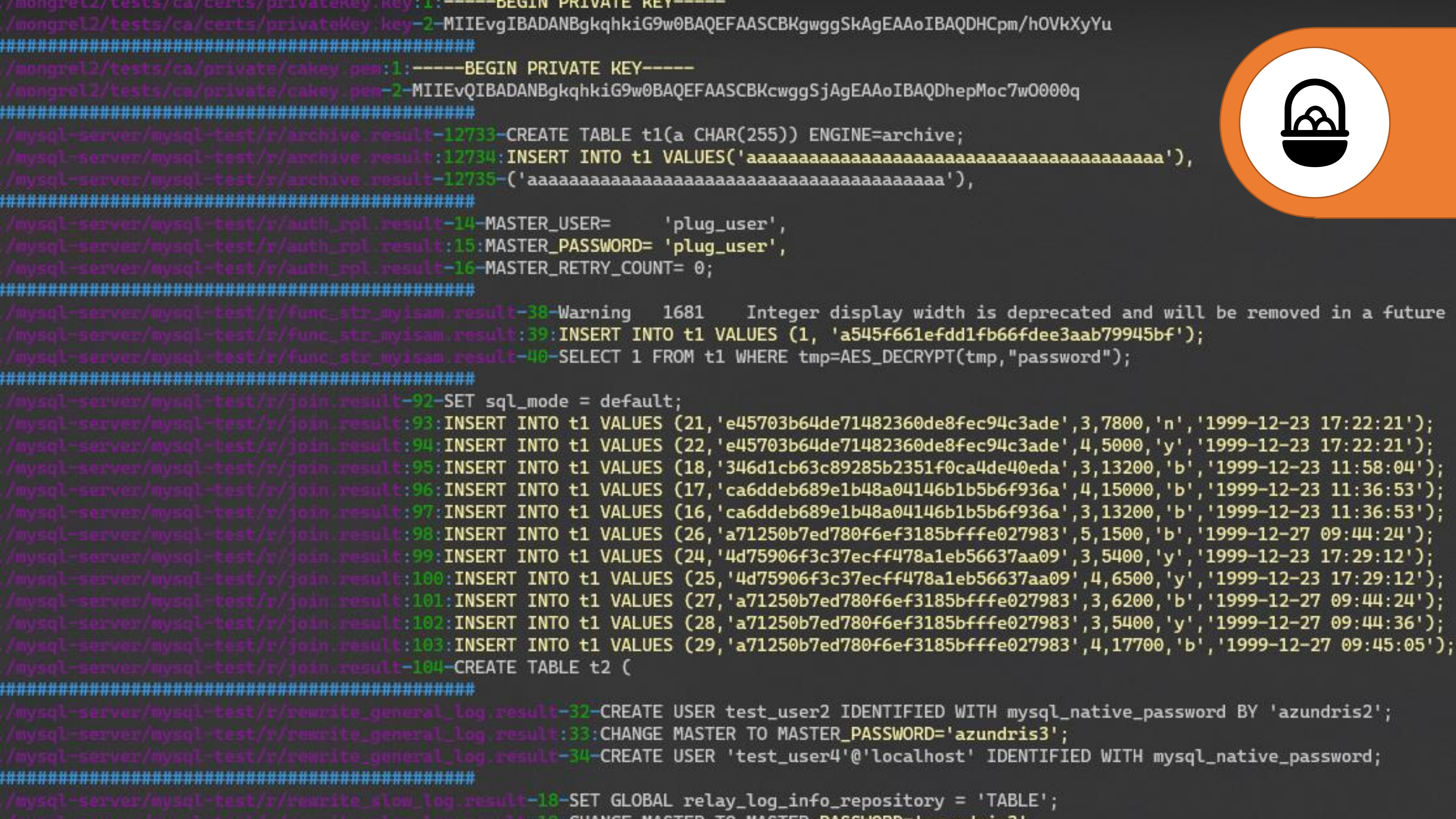
```
./nconf-master/include/ajax/json/history.php-34-{
./nconf-master/include/ajax/json/history.php:35:    $sLimit = "LIMIT ".mysql_real_escape_string( $_GET['iDisplayS
t'] ).", ".
./nconf-master/include/ajax/json/history.php-36-        mysql_real_escape_string( $_GET['iDisplayLength'] );
#############################################
./nconf-master/include/tabs/history.php-35-    $query = 'SELECT timestamp, action, attr_name FROM History
./nconf-master/include/tabs/history.php:36:            WHERE fk_id_item='.$_GET["id"].'
./nconf-master/include/tabs/history.php-37-            AND action <> "edited"
#############################################
./nconf-master/clone_host_write2db.php-176-                        SELECT '.$new_host_id.',fk_item_linked2,fk_id_attr,cust_ord
er
./nconf-master/clone_host_write2db.php:177:                            FROM ItemLinks WHERE fk_id_item = '.$_POST["templ
ate_id"].'
./nconf-master/clone_host_write2db.php-178-                            ORDER BY fk_item_linked2';
./nconf-master/clone_host_write2db.php-179-        $history_query = 'SELECT '.$new_host_id.',fk_item_linked2,fk_id_attr
./nconf-master/clone_host_write2db.php:180:                            FROM ItemLinks WHERE fk_id_item = '.$_POST["templ
ate_id"].'
./nconf-master/clone_host_write2db.php-181-                            ORDER BY fk_item_linked2';
#############################################
./nconf-master/clone_host_write2db.php-186-                        SELECT '.$new_host_id.',fk_item_linked2,fk_id_attr,cust_ord
er
./nconf-master/clone_host_write2db.php:187:                            FROM ItemLinks WHERE fk_id_item = '.$_POST["templ
ate_id"].'
./nconf-master/clone_host_write2db.php-188-                                AND ((SELECT attr_name FROM ConfigAttrs WHERE id_at
tr=fk_id_attr) <> "parents"
#############################################
./nconf-master/clone_host_write2db.php-191-        $history_query = 'SELECT '.$new_host_id.',fk_item_linked2,fk_id_attr
./nconf-master/clone_host_write2db.php:192:                            FROM ItemLinks WHERE fk_id_item = '.$_POST["templ
ate_id"].'
./nconf-master/clone_host_write2db.php-193-                                AND ((SELECT attr_name FROM ConfigAttrs WHERE id_at
tr=fk_id_attr) <> "parents"
```

When all you have

Is a hammer!

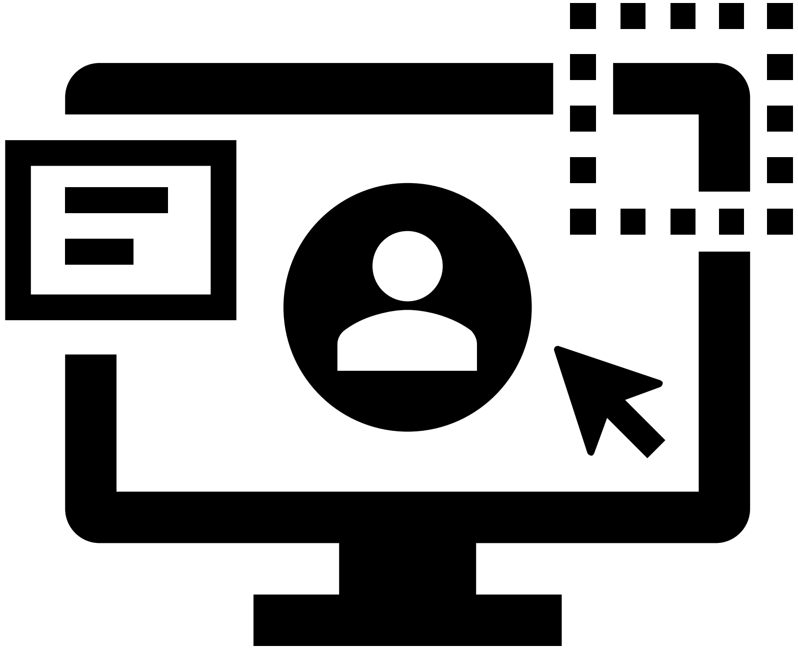
Everything looks like a nail



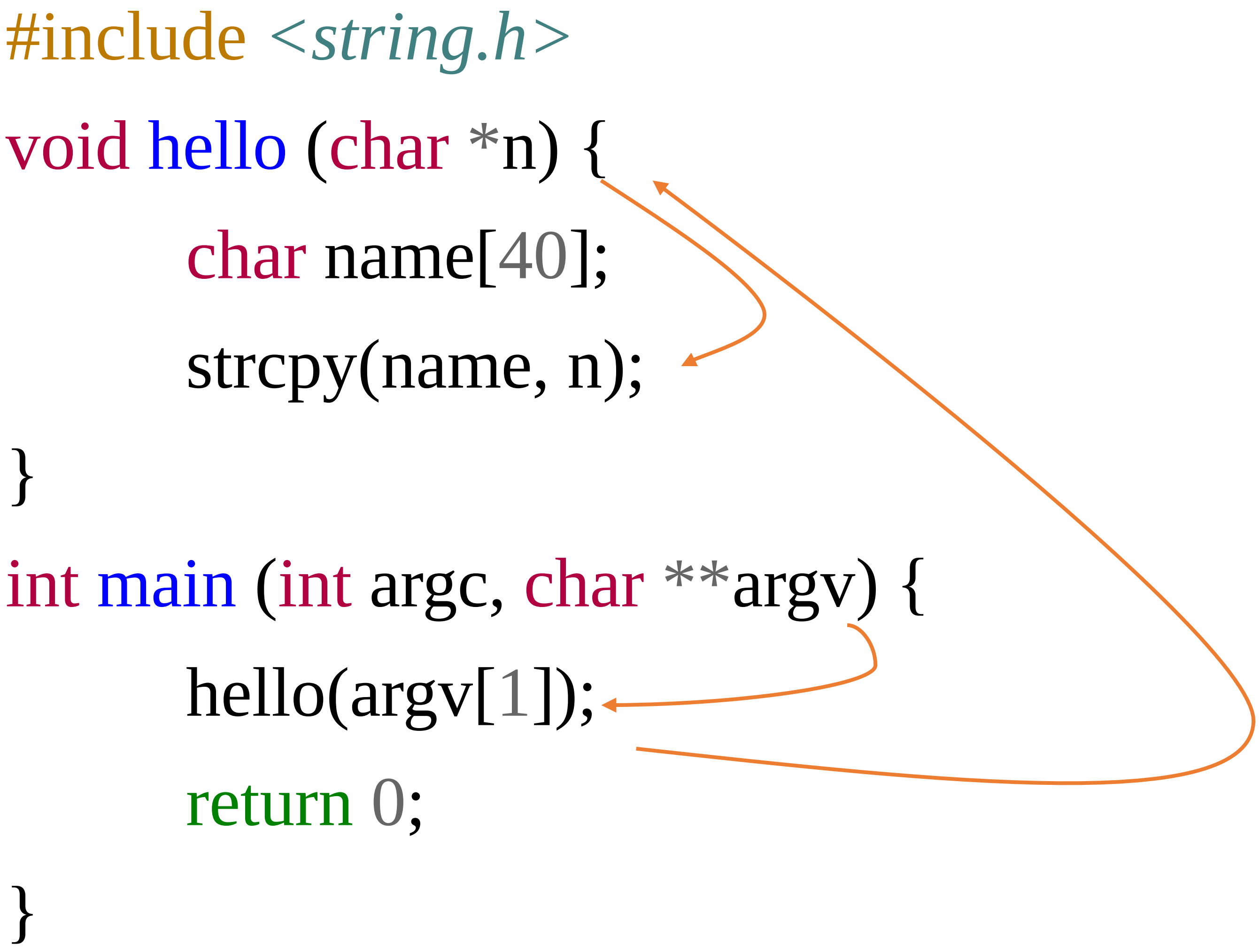


```
./mongrel2/tests/ca/certs/privateKey.key:1:-----BEGIN PRIVATE KEY-----
./mongrel2/tests/ca/certs/privateKey.key-2-MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDHCpm/hOVkXyYu
###########################################
./mongrel2/tests/ca/private/cakey.pem:1:-----BEGIN PRIVATE KEY-----
./mongrel2/tests/ca/private/cakey.pem-2-MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDhepMoc7wO000q
###########################################
./mysql-server/mysql-test/r/archive.result-12733-CREATE TABLE t1(a CHAR(255)) ENGINE=archive;
./mysql-server/mysql-test/r/archive.result:12734:INSERT INTO t1 VALUES('aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa'),
./mysql-server/mysql-test/r/archive.result-12735-('aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa'),
###########################################
./mysql-server/mysql-test/r/auth_rpl.result-14-MASTER_USER=     'plug_user',
./mysql-server/mysql-test/r/auth_rpl.result:15:MASTER_PASSWORD= 'plug_user',
./mysql-server/mysql-test/r/auth_rpl.result-16-MASTER_RETRY_COUNT= 0;
###########################################
./mysql-server/mysql-test/r/func_str_myisam.result-38-Warning   1681    Integer display width is deprecated and will be removed in a future
./mysql-server/mysql-test/r/func_str_myisam.result:39:INSERT INTO t1 VALUES (1, 'a545f661efdd1fb66fdee3aab79945bf');
./mysql-server/mysql-test/r/func_str_myisam.result-40-SELECT 1 FROM t1 WHERE tmp=AES_DECRYPT(tmp,"password");
###########################################
./mysql-server/mysql-test/r/join.result-92-SET sql_mode = default;
./mysql-server/mysql-test/r/join.result:93:INSERT INTO t1 VALUES (21,'e45703b64de71482360de8fec94c3ade',3,7800,'n','1999-12-23 17:22:21');
./mysql-server/mysql-test/r/join.result:94:INSERT INTO t1 VALUES (22,'e45703b64de71482360de8fec94c3ade',4,5000,'y','1999-12-23 17:22:21');
./mysql-server/mysql-test/r/join.result:95:INSERT INTO t1 VALUES (18,'346d1cb63c89285b2351f0ca4de40eda',3,13200,'b','1999-12-23 11:58:04');
./mysql-server/mysql-test/r/join.result:96:INSERT INTO t1 VALUES (17,'ca6ddeb689e1b48a04146b1b5b6f936a',4,15000,'b','1999-12-23 11:36:53');
./mysql-server/mysql-test/r/join.result:97:INSERT INTO t1 VALUES (16,'ca6ddeb689e1b48a04146b1b5b6f936a',3,13200,'b','1999-12-23 11:36:53');
./mysql-server/mysql-test/r/join.result:98:INSERT INTO t1 VALUES (26,'a71250b7ed780f6ef3185bfffe027983',5,1500,'b','1999-12-27 09:44:24');
./mysql-server/mysql-test/r/join.result:99:INSERT INTO t1 VALUES (24,'4d75906f3c37ecff478a1eb56637aa09',3,5400,'y','1999-12-23 17:29:12');
./mysql-server/mysql-test/r/join.result:100:INSERT INTO t1 VALUES (25,'4d75906f3c37ecff478a1eb56637aa09',4,6500,'y','1999-12-23 17:29:12');
./mysql-server/mysql-test/r/join.result:101:INSERT INTO t1 VALUES (27,'a71250b7ed780f6ef3185bfffe027983',3,6200,'b','1999-12-27 09:44:24');
./mysql-server/mysql-test/r/join.result:102:INSERT INTO t1 VALUES (28,'a71250b7ed780f6ef3185bfffe027983',3,5400,'y','1999-12-27 09:44:36');
./mysql-server/mysql-test/r/join.result:103:INSERT INTO t1 VALUES (29,'a71250b7ed780f6ef3185bfffe027983',4,17700,'b','1999-12-27 09:45:05');
./mysql-server/mysql-test/r/join.result-104-CREATE TABLE t2 (
###########################################
./mysql-server/mysql-test/r/rewrite_general_log.result-32-CREATE USER test_user2 IDENTIFIED WITH mysql_native_password BY 'azundris2';
./mysql-server/mysql-test/r/rewrite_general_log.result:33:CHANGE MASTER TO MASTER_PASSWORD='azundris3';
./mysql-server/mysql-test/r/rewrite_general_log.result-34-CREATE USER 'test_user4'@'localhost' IDENTIFIED WITH mysql_native_password;
###########################################
./mysql-server/mysql-test/r/rewrite_slow_log.result-18-SET GLOBAL relay_log_info_repository = 'TABLE';
./mysql-server/mysql-test/r/rewrite_slow_log.result:19:CHANGE MASTER TO MASTER_PASSWORD='azundris3';
```

Taint analysis

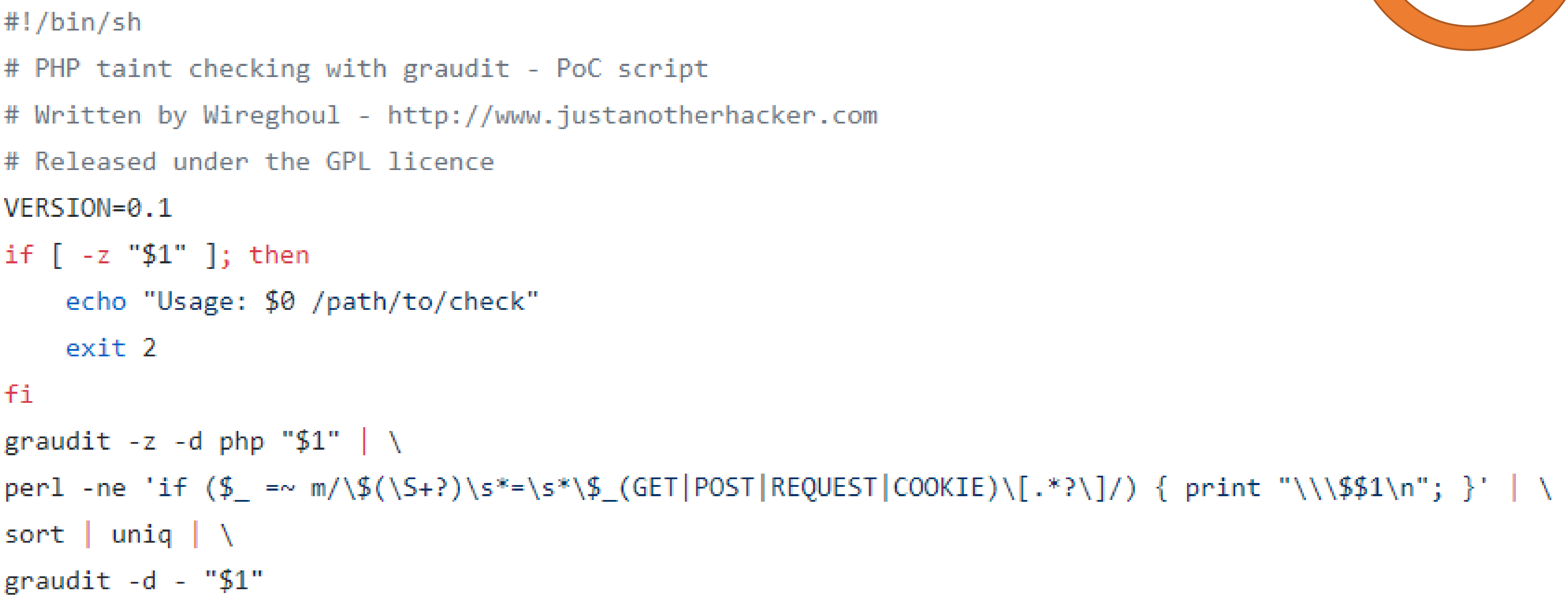


Taint analysis



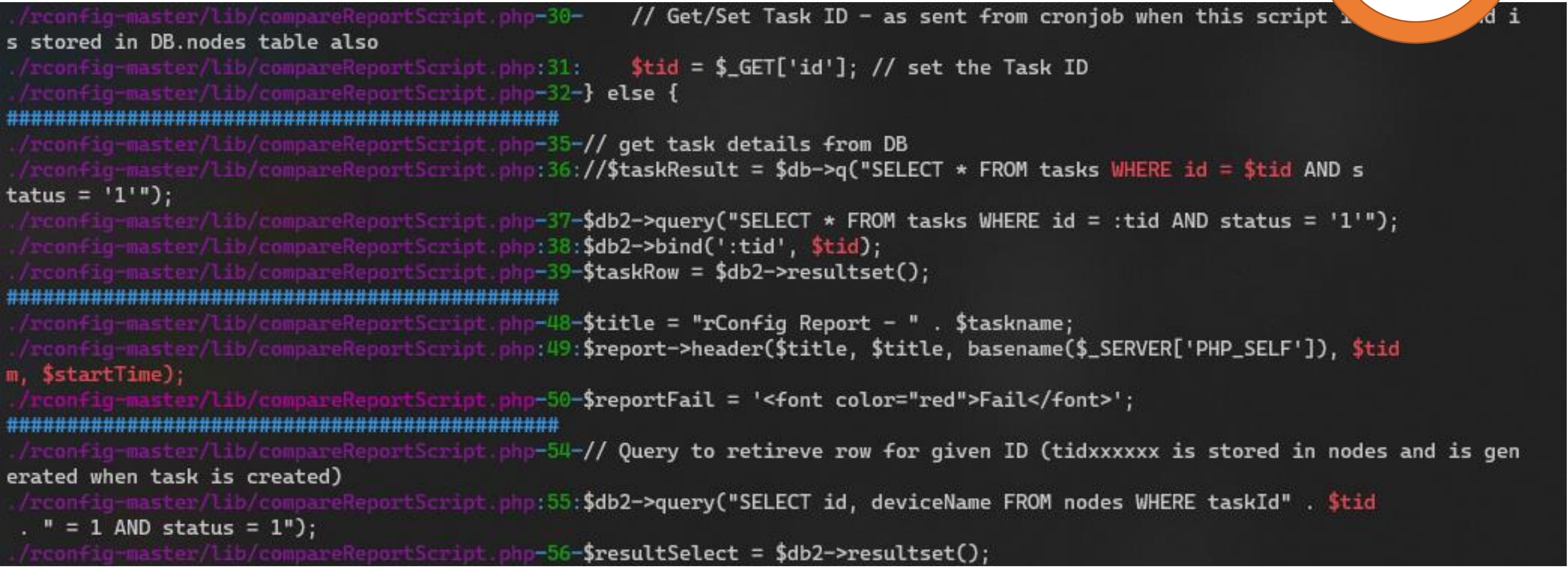
```
#include <string.h>
void hello (char *n) {
        char name[40];
        strcpy(name, n);
}
int main (int argc, char **argv) {
        hello(argv[1]);
        return 0;
}
```

Taint analysis



```
#!/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"
```

Taint analysis

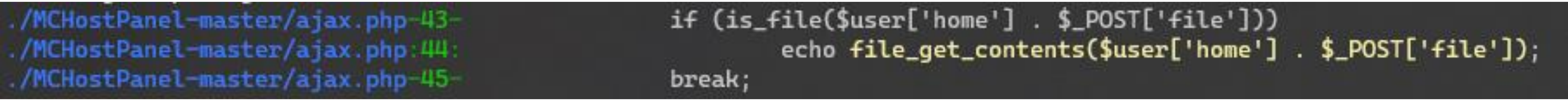


```
./rconfig-master/lib/compareReportScript.php-30-    // Get/Set Task ID - as sent from cronjob when this script i        d i
s stored in DB.nodes table also
./rconfig-master/lib/compareReportScript.php:31:    $tid = $_GET['id']; // set the Task ID
./rconfig-master/lib/compareReportScript.php-32-} else {
##############################################
./rconfig-master/lib/compareReportScript.php-35-// get task details from DB
./rconfig-master/lib/compareReportScript.php:36://$taskResult = $db->q("SELECT * FROM tasks WHERE id = $tid AND s
tatus = '1'");
./rconfig-master/lib/compareReportScript.php-37-$db2->query("SELECT * FROM tasks WHERE id = :tid AND status = '1'");
./rconfig-master/lib/compareReportScript.php:38:$db2->bind(':tid', $tid);
./rconfig-master/lib/compareReportScript.php-39-$taskRow = $db2->resultset();
##############################################
./rconfig-master/lib/compareReportScript.php-48-$title = "rConfig Report - " . $taskname;
./rconfig-master/lib/compareReportScript.php:49:$report->header($title, $title, basename($_SERVER['PHP_SELF']), $tid
m, $startTime);
./rconfig-master/lib/compareReportScript.php-50-$reportFail = '<font color="red">Fail</font>';
##############################################
./rconfig-master/lib/compareReportScript.php-54-// Query to retireve row for given ID (tidxxxxxx is stored in nodes and is gen
erated when task is created)
./rconfig-master/lib/compareReportScript.php:55:$db2->query("SELECT id, deviceName FROM nodes WHERE taskId" . $tid
 . " = 1 AND status = 1");
./rconfig-master/lib/compareReportScript.php-56-$resultSelect = $db2->resultset();
```

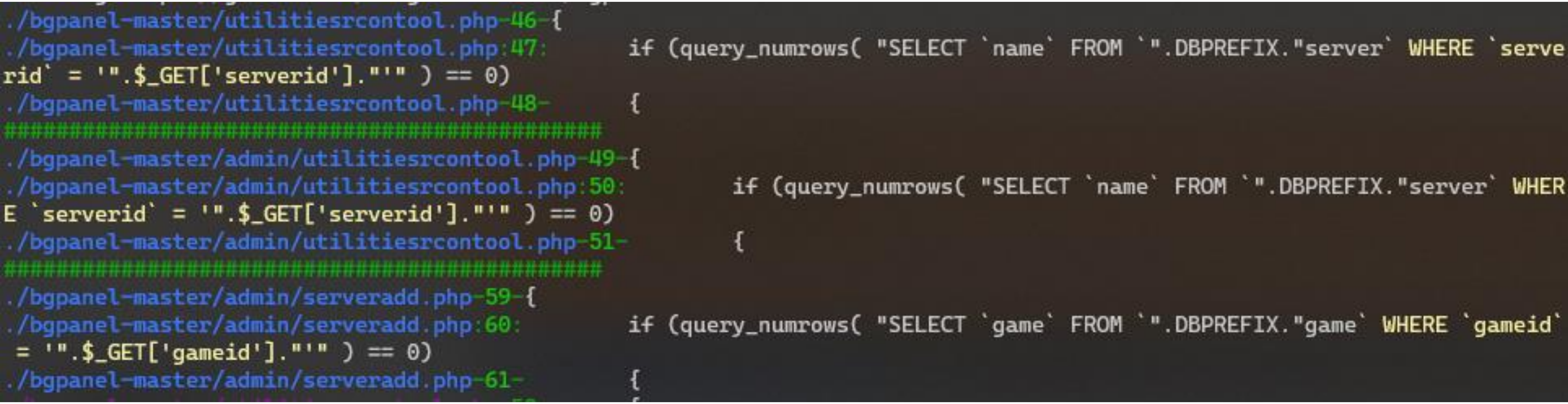
Auto taint

- Sink and source on same line
- fruit and flatline databases

Auto taint



```
./MCHostPanel-master/ajax.php-43-            if (is_file($user['home'] . $_POST['file']))
./MCHostPanel-master/ajax.php:44:                    echo file_get_contents($user['home'] . $_POST['file']);
./MCHostPanel-master/ajax.php-45-            break;
```

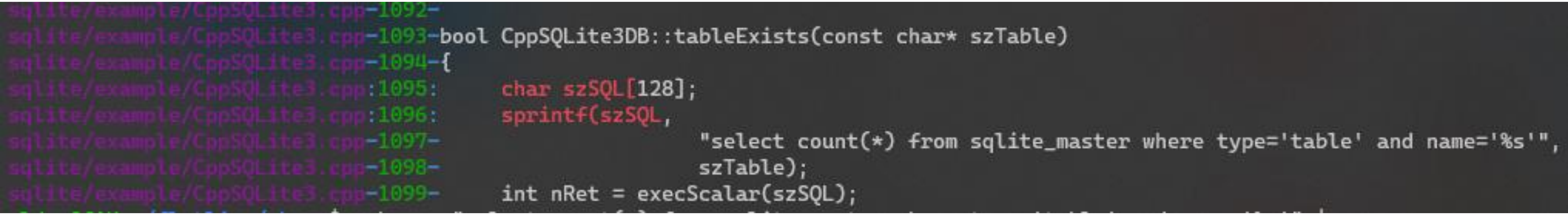


```
./bgpanel-master/utilitiesrcontool.php-46-{
./bgpanel-master/utilitiesrcontool.php:47:      if (query_numrows( "SELECT `name` FROM `".DBPREFIX."server` WHERE `serve
rid` = '".$_GET['serverid']."'" ) == 0)
./bgpanel-master/utilitiesrcontool.php-48-      {
###############################################
./bgpanel-master/admin/utilitiesrcontool.php-49-{
./bgpanel-master/admin/utilitiesrcontool.php:50:        if (query_numrows( "SELECT `name` FROM `".DBPREFIX."server` WHER
E `serverid` = '".$_GET['serverid']."'" ) == 0)
./bgpanel-master/admin/utilitiesrcontool.php-51-        {
###############################################
./bgpanel-master/admin/serveradd.php-59-{
./bgpanel-master/admin/serveradd.php:60:        if (query_numrows( "SELECT `game` FROM `".DBPREFIX."game` WHERE `gameid`
 = '".$_GET['gameid']."'" ) == 0)
./bgpanel-master/admin/serveradd.php-61-        {
```

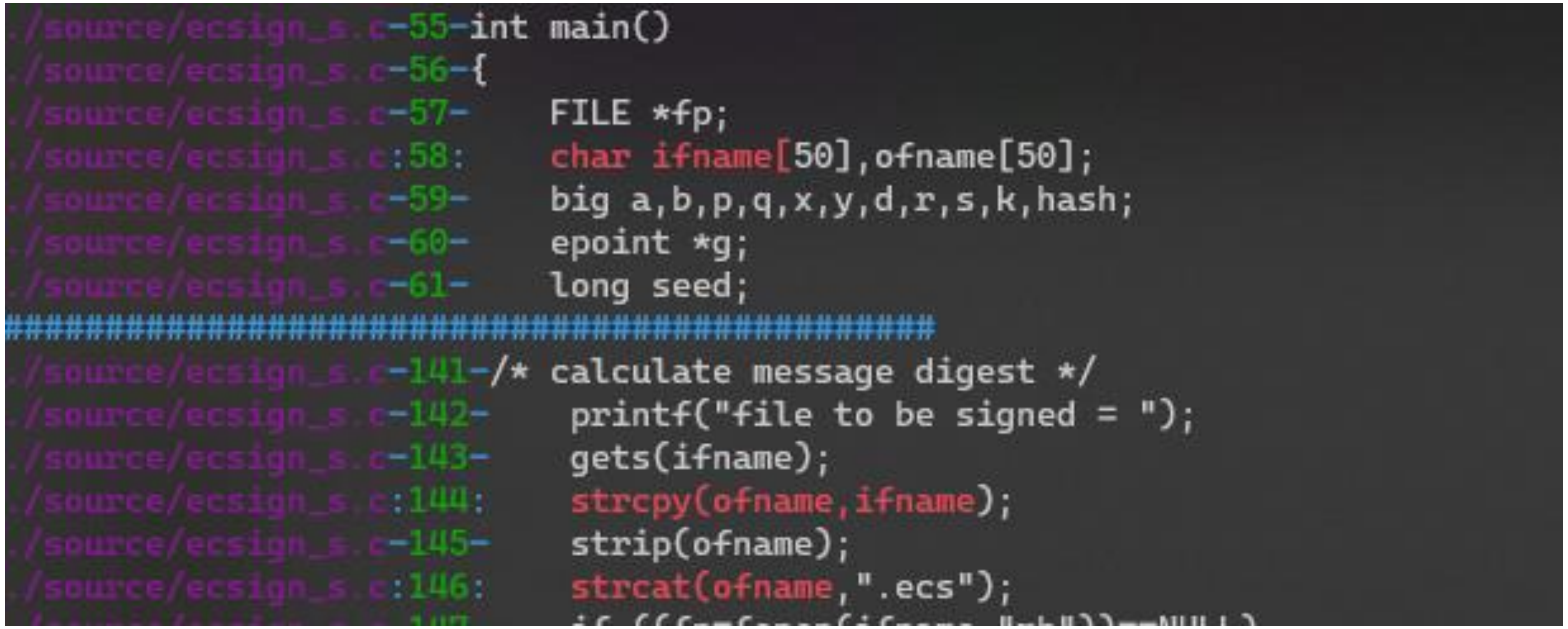
BOf taint

```
#!/bin/sh
#testing C taint
echo 'char[[:space:]]+[a-zA-Z0-9\.\-\_][a-zA-Z0-9\.\-\_]+\[' | \
~/flatline/graudit -B -z -d /dev/stdin -c 0 $1 | \
perl -ne 'if ($_ =~ m/char\s+([a-zA-Z0-9\.\-\_]+)\[/) { print "$1\n"; }’ | \
sort -u > /tmp/test
while read var; do
echo "(memcpy|strcat|strcpy|sprintf).*$var"
done </tmp/test | \
~/flatline/graudit -B -z -d /dev/stdin -c 0 $1 | \
grep -o -f /tmp/test | sort -u > /tmp/taint
while read var; do
echo "char[[:space:]]+[\*]?$var\["
echo "(memcpy|strcat|strcpy|sprintf).*$var"
done </tmp/taint | \
~/flatline/graudit -c 3 -d /dev/stdin $1
```

Buffer overflow



```
sqlite/example/CppSQLite3.cpp-1092-
sqlite/example/CppSQLite3.cpp-1093-bool CppSQLite3DB::tableExists(const char* szTable)
sqlite/example/CppSQLite3.cpp-1094-{
sqlite/example/CppSQLite3.cpp:1095:     char szSQL[128];
sqlite/example/CppSQLite3.cpp:1096:     sprintf(szSQL,
sqlite/example/CppSQLite3.cpp-1097-                     "select count(*) from sqlite_master where type='table' and name='%s'",
sqlite/example/CppSQLite3.cpp-1098-                     szTable);
sqlite/example/CppSQLite3.cpp-1099-     int nRet = execScalar(szSQL);
```

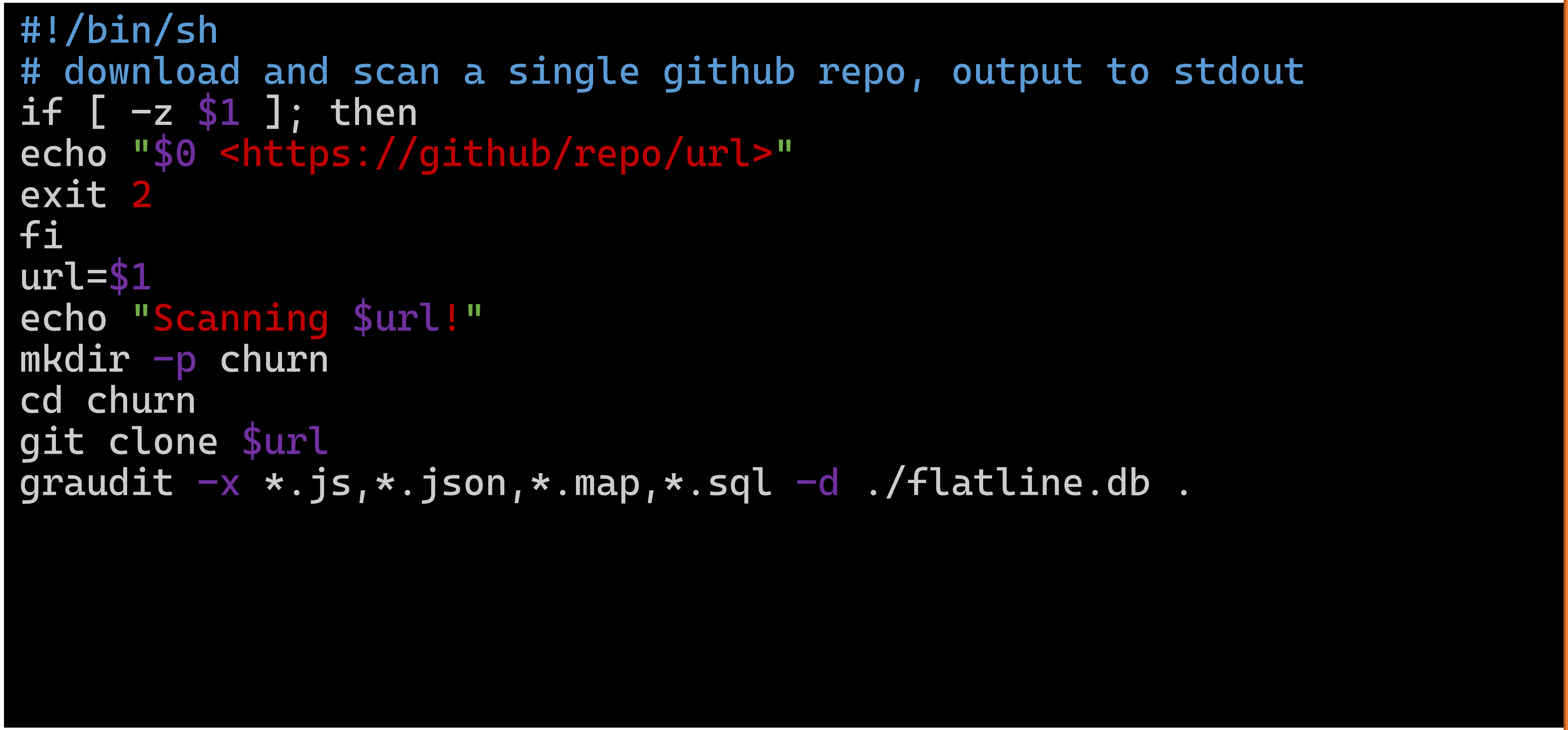


```
./source/ecsign_s.c-55-int main()
./source/ecsign_s.c-56-{
./source/ecsign_s.c-57-    FILE *fp;
./source/ecsign_s.c:58:    char ifname[50],ofname[50];
./source/ecsign_s.c-59-    big a,b,p,q,x,y,d,r,s,k,hash;
./source/ecsign_s.c-60-    epoint *g;
./source/ecsign_s.c-61-    long seed;
###############################################
./source/ecsign_s.c-141-/* calculate message digest */
./source/ecsign_s.c-142-     printf("file to be signed = ");
./source/ecsign_s.c-143-     gets(ifname);
./source/ecsign_s.c:144:     strcpy(ofname,ifname);
./source/ecsign_s.c-145-     strip(ofname);
./source/ecsign_s.c:146:     strcat(ofname,".ecs");
```

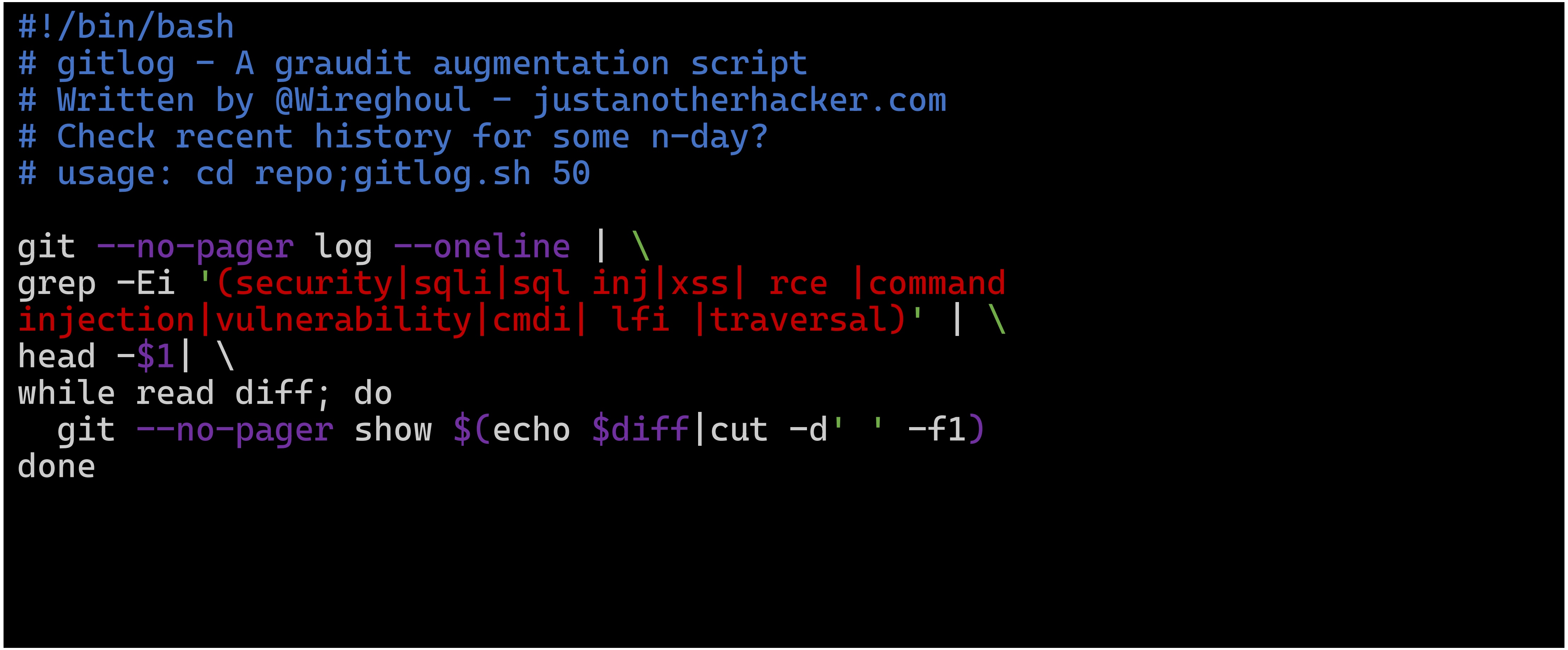
Bug hunting

at scale

gitscan

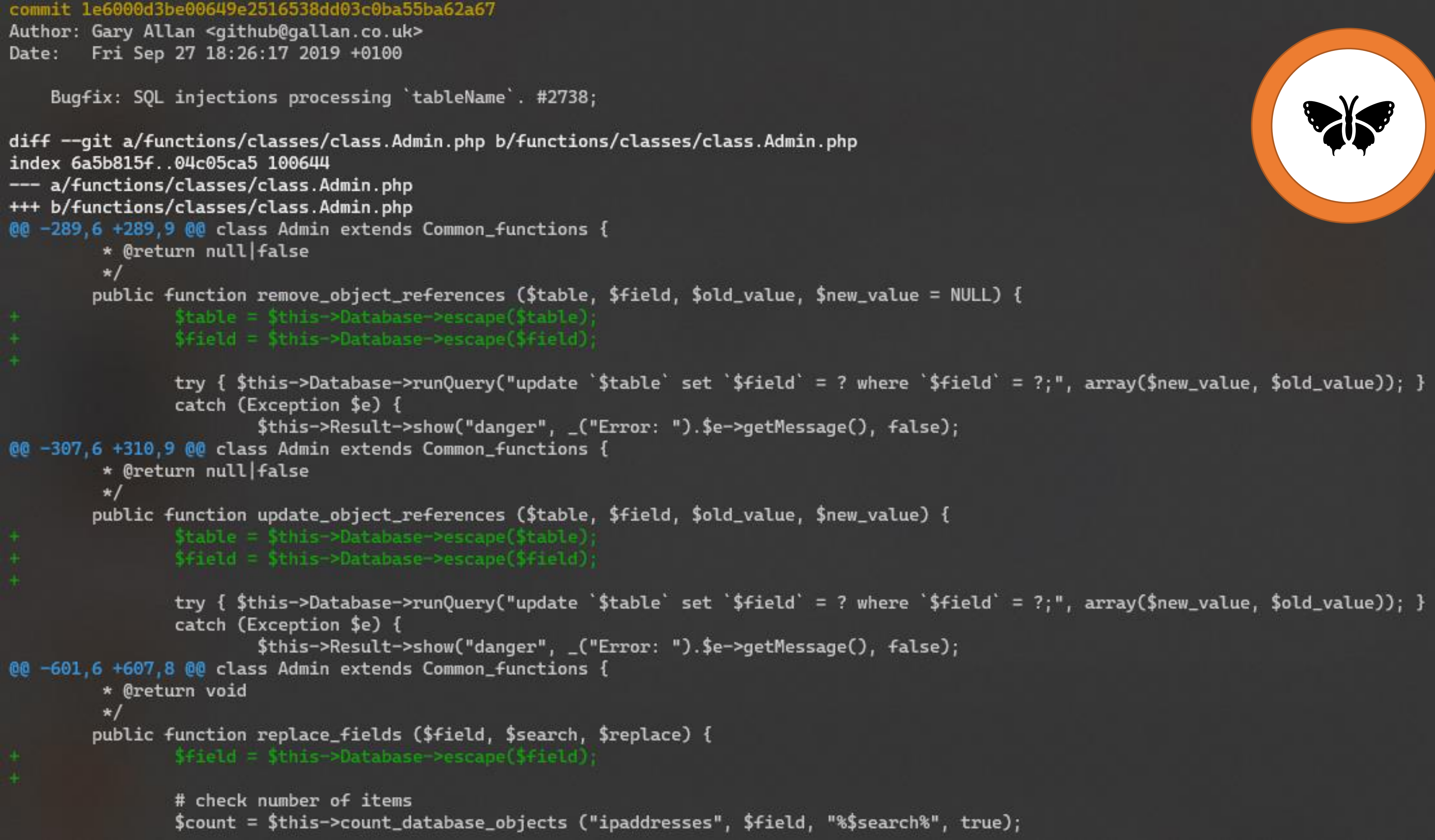


```
#!/bin/sh
# download and scan a single github repo, output to stdout
if [ -z $1 ]; then
echo "$0 <https://github/repo/url>"
exit 2
fi
url=$1
echo "Scanning $url!"
mkdir -p churn
cd churn
git clone $url
graudit -x *.js,*.json,*.map,*.sql -d ./flatline.db .
```



```
#!/bin/bash
# gitlog - A graudit augmentation script
# Written by @Wireghoul - justanotherhacker.com
# Check recent history for some n-day?
# usage: cd repo;gitlog.sh 50

git --no-pager log --oneline | \
grep -Ei '(security|sqli|sql inj|xss| rce |command
injection|vulnerability|cmdi| lfi |traversal)' | \
head -$1| \
while read diff; do
  git --no-pager show $(echo $diff|cut -d' ' -f1)
done
```

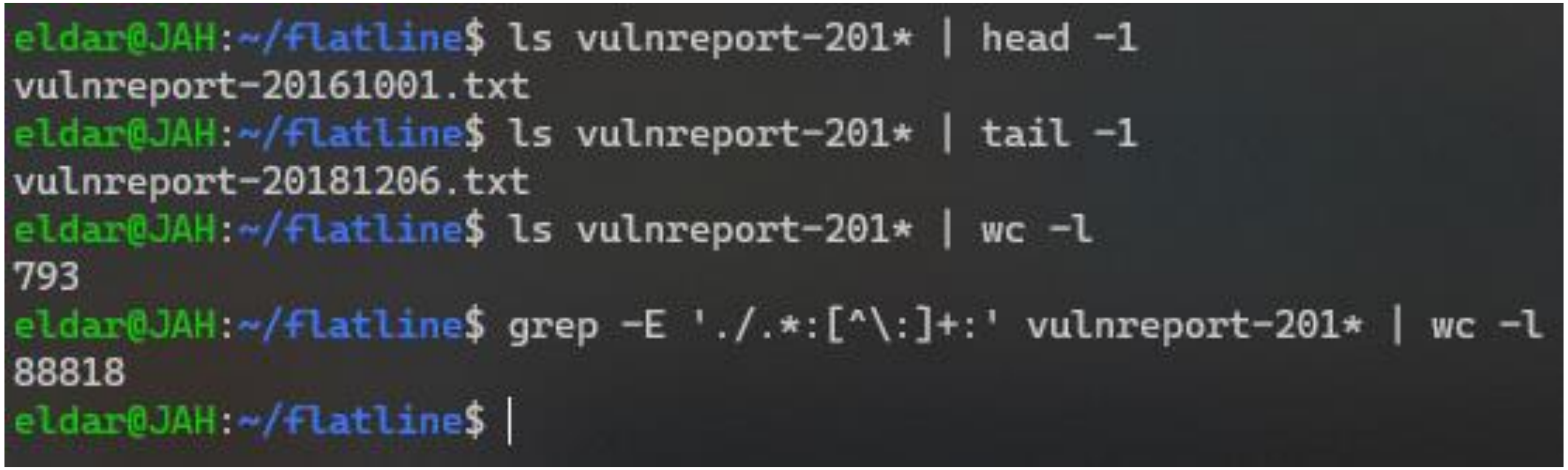
gitlog.sh



```
commit 1e6000d3be00649e2516538dd03c0ba55ba62a67
Author: Gary Allan <github@gallan.co.uk>
Date:   Fri Sep 27 18:26:17 2019 +0100

  Bugfix: SQL injections processing `tableName`. #2738;

diff --git a/functions/classes/class.Admin.php b/functions/classes/class.Admin.php
index 6a5b815f..04c05ca5 100644
--- a/functions/classes/class.Admin.php
+++ b/functions/classes/class.Admin.php
@@ -289,6 +289,9 @@ class Admin extends Common_functions {
         * @return null|false
         */
        public function remove_object_references ($table, $field, $old_value, $new_value = NULL) {
+               $table = $this->Database->escape($table);
+               $field = $this->Database->escape($field);
+
                try { $this->Database->runQuery("update `$table` set `$field` = ? where `$field` = ?;", array($new_value, $old_value)); }
                catch (Exception $e) {
                        $this->Result->show("danger", _("Error: ").$e->getMessage(), false);
@@ -307,6 +310,9 @@ class Admin extends Common_functions {
         * @return null|false
         */
        public function update_object_references ($table, $field, $old_value, $new_value) {
+               $table = $this->Database->escape($table);
+               $field = $this->Database->escape($field);
+
                try { $this->Database->runQuery("update `$table` set `$field` = ? where `$field` = ?;", array($new_value, $old_value)); }
                catch (Exception $e) {
                        $this->Result->show("danger", _("Error: ").$e->getMessage(), false);
@@ -601,6 +607,8 @@ class Admin extends Common_functions {
         * @return void
         */
        public function replace_fields ($field, $search, $replace) {
+               $field = $this->Database->escape($field);
+
                # check number of items
                $count = $this->count_database_objects ("ipaddresses", $field, "%$search%", true);
```

Automated scanning

- Daily gitscan cron for PHP updated repos
- Flatline rules and basic taint analysis
- ~112 vulnerability candidates a day on average



```
eldar@JAH:~/flatline$ ls vulnreport-201* | head -1
vulnreport-20161001.txt
eldar@JAH:~/flatline$ ls vulnreport-201* | tail -1
vulnreport-20181206.txt
eldar@JAH:~/flatline$ ls vulnreport-201* | wc -l
793
eldar@JAH:~/flatline$ grep -E './.*:[^\:]+:' vulnreport-201* | wc -l
88818
eldar@JAH:~/flatline$ 
```

Conclusion

- Vulnerability discovery doesn’t have to be advanced
- Some bug classes are harder to detect than others
- Finding a vulnerability is usually only the start of the journey

Questions?