chamilo / **chamilo-lms** Public

Code | Issues 399 | Pull requests 13 | Discussions | Actions | Projects

Commit 62671e5

AngelFQC committed 2 weeks ago · ✕ 2 / 6 · Verified

```
Security: Sanitize shell command inputs using escapeshellarg to prevent command injection vulnerabilities

See advisory GHSA-59cv-qh65-vvrr

Proposed by @elliSzAt
```

master · v2.0.0 v2.0.0-RC.3

1 parent 2b389fa commit 62671e5

2 files changed +17 -10 lines changed

Top

Filter files…

- public/main/inc
  - ajax
    - gradebook.ajax.php
  - lib
    - document.lib.php

2 files changed +17 -10 lines changed

Search within code

public/main/inc/ajax/gradebook.ajax.php

```
@@ -57,9 +57,9 @@
57  57              break;*/
58  58          case 'export_all_certificates':
59  59              if (!api_is_allowed_to_edit(null, true) && !api_is_student_boss()) {
60      -               echo '';
61      -               break;
```

```
      60 +             exit;
62    61           }
      62 +
63    63           $categoryId = (int) $_GET['cat_id'];
64    64           $filterOfficialCodeGet = isset($_GET['filter']) ?
           Security::remove_XSS($_GET['filter']) : null;
65    65
           @@ -82,7 +82,14 @@
82    82
83    83           $userList = implode(',', $userList);
84    84
85        -        shell_exec("php $commandScript $courseCode $sessionId $categoryId
           $userList > /dev/null &");
      85 +        shell_exec(sprintf(
      86 +            "php %s %s %s %s %s > /dev/null &",
      87 +            escapeshellarg($commandScript),
      88 +            escapeshellarg($courseCode),
      89 +            escapeshellarg((string) $sessionId),
      90 +            escapeshellarg((string) $categoryId),
      91 +            escapeshellarg($userList)
      92 +        ));
86    93           break;
87    94       case 'verify_export_all_certificates':
88    95           $categoryId = (int) $_GET['cat_id'];
```

public/main/inc/lib/document.lib.php

```
           @@ -2057,27 +2057,27 @@ public static function
           get_text_content($doc_path, $doc_mime)
2057  2057                   fclose($handle);
2058  2058                   break;
2059  2059               case 'application/pdf':
2060        -                exec("pdftotext $doc_path -", $output, $ret_val);
      2060 +                exec("pdftotext ".escapeshellarg($doc_path)." -", $output,
           $ret_val);
2061  2061                   break;
2062  2062               case 'application/postscript':
2063  2063                   $temp_file = tempnam(sys_get_temp_dir(), 'chamilo');
2064        -                exec("ps2pdf $doc_path $temp_file", $output, $ret_val);
```

```
2064 +                  exec("ps2pdf ".escapeshellarg($doc_path)." ".escapeshellarg($temp_file), $output, $ret_val);
2065 2065                  if (0 !== $ret_val) { // shell fail, probably 127 (command not found)
2066 2066                      return false;
2067 2067                  }
2068 2068                  exec("pdftotext $temp_file -", $output, $ret_val);
2069 2069                  unlink($temp_file);
2070 2070                  break;
2071 2071              case 'application/msword':
2072 -                    exec("catdoc $doc_path", $output, $ret_val);
     2072 +                exec("catdoc ".escapeshellarg($doc_path), $output, $ret_val);
2073 2073                  break;
2074 2074              case 'text/html':
2075 -                    exec("html2text $doc_path", $output, $ret_val);
     2075 +                exec("html2text ".escapeshellarg($doc_path), $output, $ret_val);
2076 2076                  break;
2077 2077              case 'text/rtf':
2078 2078                  // Note: correct handling of code pages in unrtf
2079 2079                  // on debian lenny unrtf v0.19.2 can not, but unrtf v0.20.5 can
2080 -                    exec("unrtf --text $doc_path", $output, $ret_val);
     2080 +                exec("unrtf --text ".escapeshellarg($doc_path), $output, $ret_val);
2081 2081                  if (127 == $ret_val) { // command not found
2082 2082                      return false;
2083 2083                  }
     @@ -2095,10 +2095,10 @@ public static function get_text_content($doc_path, $doc_mime)
2095 2095                  }
2096 2096                  break;
2097 2097              case 'application/vnd.ms-powerpoint':
2098 -                    exec("catppt $doc_path", $output, $ret_val);
     2098 +                exec("catppt ".escapeshellarg($doc_path), $output, $ret_val);
2099 2099                  break;
2100 2100              case 'application/vnd.ms-excel':
2101 -                    exec("xls2csv -c\" \" $doc_path", $output, $ret_val);
     2101 +                exec("xls2csv -c\" \" ".escapeshellarg($doc_path), $output, $ret_val);
```

```
2102  2102                      break;
2103  2103              }
2104  2104
```

Comments 0

Please sign in to comment.