chamilo / **chamilo-lms** Public

Code | Issues 415 | Pull requests 12 | Discussions | Actions | Projects

Commit `4efb5ee`

ywarnier committed 3 weeks ago

```
Security: Avoid information disclosure through direct access to .tpl files
```

1.11.x · v1.11.38

1 parent 9748f1f commit 4efb5ee

2 files changed +39 -0 lines changed

Top

Filter files…

- documentation
  - security.html
- main/template
  - .htaccess

2 files changed +39 -0 lines changed

Search within code

documentation/security.html

```
@@ -29,6 +29,7 @@ <h2><b>Contents</b></h2>
29 29   <li><a href="#9.Change-password-first-login">Change password on first login</a></li>
30 30   <li><a href="#10.Hide-breadcrumb">Hide breadcrumb on unauthorized page load</a></li>
31 31   <li><a href="#11.SVG-and-XSS">SVG and XSS</a></li>
   32 +   <li><a href="#12.Template-files-access">Restricting access to template files</a></li>
32 33   </ol>
33 34
34 35   <h2><a id="1.Disclosing-server-info"></a>1. Disclosing server info</h2>
```

```
@@ -280,6 +281,38 @@ <h2><a id="11.SVG-and-XSS">SVG and XSS</a></h2>
280 281         </ul>
281 282         </p>
282 283
    284 + <h2><a id="12.Template-files-access"></a>12. Restricting access to template files</h2>
    285 +     <p>
    286 +         Twig template files (<code>.tpl</code>) under <code>main/template/</code> are
    287 +         not meant to be served directly over HTTP. They are loaded by PHP from the
    288 +         filesystem. If left accessible, they expose internal application logic,
    289 +         AJAX endpoint URLs, admin panel structure, and variable names to
    290 +         unauthenticated users.
    291 +     </p>
    292 +     <p>
    293 +         Chamilo ships a <code>.htaccess</code> file in <code>main/template/</code>
    294 +         that blocks direct access. If your Apache configuration does not support
    295 +         <code>.htaccess</code> overrides, add the following to your VirtualHost
    296 +         definition (replace <code>/var/www/URL</code> with your Chamilo root):
    297 +     </p>
    298 +     <pre>
    299 +   &lt;Directory /var/www/URL/main/template&gt;
    300 +     &lt;FilesMatch "\.tpl$"&gt;
    301 +       Require all denied
    302 +     &lt;/FilesMatch&gt;
    303 +   &lt;/Directory&gt;
    304 +     </pre>
    305 +     <p>
    306 +         For Nginx, add this rule near the top of your location blocks (before
    307 +         any generic location rules) so it takes priority:
    308 +     </p>
    309 +     <pre>
    310 +   location ~* \.tpl$ {
    311 +     deny all;
    312 +     return 403;
    313 +   }
```

```
      314  +      </pre>
      315  +
283   316         <h2>Authors</h2>
284   317       <ul>
285   318       <li>Yannick Warnier, Chamilo Project Leader, Zend Certified PHP Engineer,
                  BeezNest Belgium SPRL,
```

main/template/.htaccess

```
      •••  @@ -0,0 +1,6 @@
      1    + # Deny direct access to template files.
      2    + # Templates are loaded by PHP internally via the filesystem, not via HTTP,
      3    + # so they never need to be web-accessible.
      4    + <FilesMatch "\.tpl$">
      5    +     Require all denied
      6    + </FilesMatch>
```

Comments 0

Please sign in to comment.