Cross-site Scripting (XSS) - Stored in autolab/autolab

0

Valid Reported on Mar 2nd 2022

Description

Autolab is vulnerable to stored cross-site-scripting in the upload files functionality in courses feature, this can be used to execute XSS attack against the victim who is a student/teacher.

Steps to Reproduce (PoC)

login to autolab
go to https://DOMAIN/courses/COURSENAME/attachments/new
upload the below file as something.svg

```
<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN" "http://www.w3.org/Graphics/

<svg version="1.1" baseProfile="full" xmlns="http://www.w3.org/2000/svg">
   <rect width="300" height="100" style="fill:rgb(0,0,255);stroke-width:3;s
   <script type="text/javascript">
      alert("xssed");
   </script>
```

go to https://DOMAIN/courses/COURSENAME/attachments
view the file you just uploaded, you'll get the alert fn executed.

Impact

This can be used to perform XSS attacks on other users as other users such as students/teachers can also view attachments, xss can be weaponized to trick them to do unwanted actions by executing malicious javascript at their end.

Proof

https://prnt.sc/LGy-cYXA37sK

Fix / Mitigation

Check file types while uploading, and allow only corresponding types, It is recommended to have a whitelist based approach to check the file type in server-side and to reject/accept the file while uploading.

Reporters

Abhishek S (abhiabhi2306@gmail.com)
Vidhun K (vidhunedl@gmail.com)
Srikar R (xzeltronx@gmail.com)
Varun Nair (varun199700@gmail.com)

References

- CWE-79

CVE
CVE-2022-0936
(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Stored

Severity
High (7.6)

Visibility
Public

Status
Fixed

Found by

Abhishek S
@abhiabhi2306
unranked

Fixed by

Fan Pu

@fanpu

maintainer

This report was seen 413 times.

We are processing your report and will contact the **autolab** team within 24 hours. 9 months ago

We created a **GitHub Issue** asking the maintainers to create a `SECURITY.md` 9 months ago

We have contacted a member of the **autolab** team and are waiting to hear back 9 months ago

We have sent a follow up to the **autolab** team. We will try again in 7 days. 9 months ago

A **autolab/autolab** maintainer validated this vulnerability 9 months ago

Abhishek S has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Abhishek S 9 months ago — Researcher

Hello @admin, would it be possible for you to assign a CVE ID for this as this project is used by alot of educational organizations? the user base is quite large for this product.

Kind Regards,
Abhi

Jamie Slome 9 months ago — Admin

@researcher - of course, that is definitely something we can support.

We do first require a confirmation from the maintainer before we assign and publish a CVE.

@maintainer - are you happy to assign and publish a CVE for this report?

We have sent a fix follow up to the **autolab** team. We will try again in 7 days

A **autolab/autolab** maintainer 8 months ago — Maintainer

Hi @Abhishek and @Jamie, thank you for reporting this vulnerability! I am able to replicate it, and note that this affects both course and assessment attachments. I also checked if it affects the Speedgrader view and annotations, it does not appear to be.

Instructors and admins are the only ones allowed to upload attachments, so students in general should not be able to pull this off. We will consider a whitelist-based approach as you noted.

We are happy to publish a CVE for this report. It is actually our first time receiving a disclosure, do you have any guidance with regards to publishing a CVE? Thanks again.

Jamie Slome 8 months ago — Admin

Thanks for your follow up and detailed response @maintainer.

We automate and take care of the entire CVE process for you. I will assign a CVE to this report for you, and once you have confirmed the fix, the CVE will be published to the NVD/MITRE database.

Let me know if you have any questions.

Jamie Slome 8 months ago — Admin

`CVE-2022-0936` assigned to the report - please go ahead and confirm the fix once you are ready for the CVE and report to go public 👍

Abhishek S 8 months ago — Researcher

Thank you Autolab Team and Jamie, that's great to know.

We have sent a second fix follow up to the **autolab** team. We will try again in 10 days. 8 months ago

We have sent a third and final fix follow up to the **autolab** team. This report is now considered stale. 8 months ago

Fan Pu marked this as fixed in **2.8.0** with commit **02d76a** 8 months ago

Fan Pu has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Fan Pu 8 months ago Maintainer

Vulnerability has been fixed in https://github.com/autolab/Autolab/pull/1490 by forcing downloads so browser-based attacks from file downloads are no longer possible

Jamie Slome 8 months ago Admin

Great, thank you for your contribution 👍

Sign in to join this conversation