gunet / openeclass Public

Code Issues 19 Pull requests 2 Actions Projects Wiki ...

New issue

Jump to bottom

Improper Access Control by Directory Listing Misconfiguration #39

Open **emaragkos** opened this issue on Aug 17, 2020 · 7 comments

Assignees

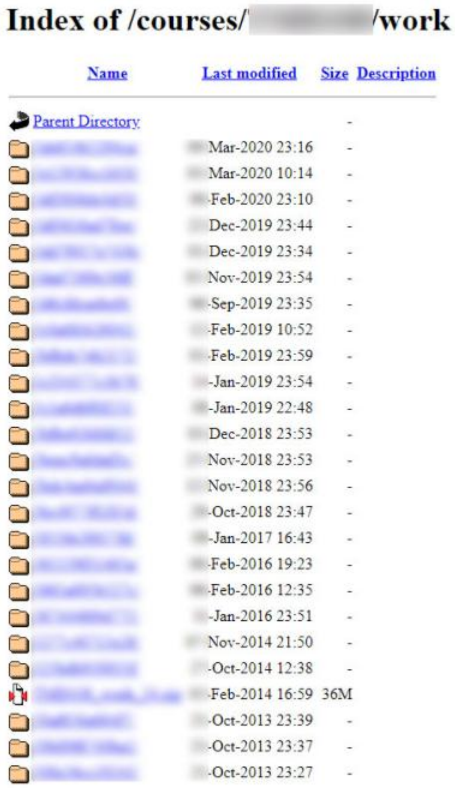
emaragkos commented on Aug 17, 2020 • edited

Improper Access Control by Directory Listing Misconfiguration that affects all versions

When the webapp is poorly configured (directory listing is enabled), an unauthenticated remote attacker will be able to read students' submitted assessments because it does not ensure that the web server blocks directory listing.

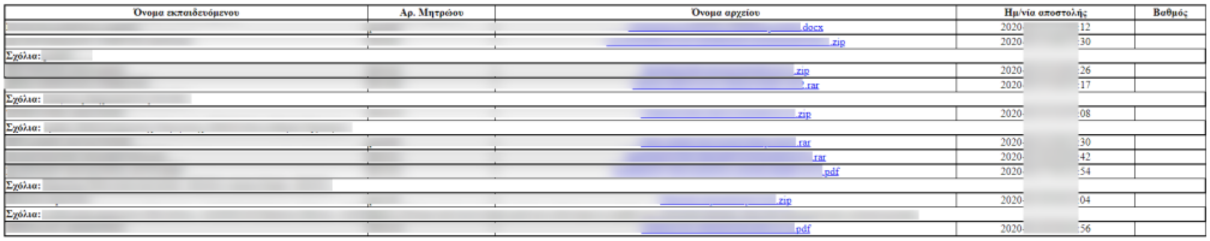
CVE-2020-24381
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24381
https://nvd.nist.gov/vuln/detail/CVE-2020-24381

PoC:
Course link
https://127.0.0.1/courses/CS101
Add "work" directory at the end
https://127.0.0.1/courses/CS101/work/

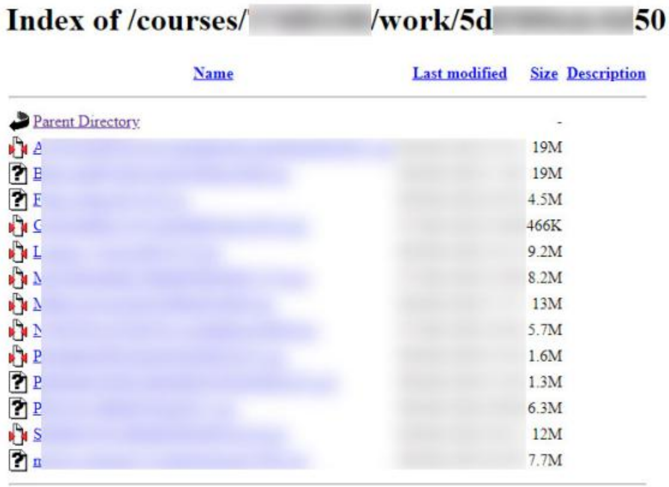


Index of /courses/[redacted]/work

Name	Last modified	Size	Description
Parent Directory		-	
[redacted]	[redacted]-Mar-2020 23:16	-	
[redacted]	[redacted]-Mar-2020 10:14	-	
[redacted]	[redacted]-Feb-2020 23:10	-	
[redacted]	[redacted]-Dec-2019 23:44	-	
[redacted]	[redacted]-Dec-2019 23:34	-	
[redacted]	[redacted]-Nov-2019 23:54	-	
[redacted]	[redacted]-Sep-2019 23:35	-	
[redacted]	[redacted]-Feb-2019 10:52	-	
[redacted]	[redacted]-Feb-2019 23:59	-	
[redacted]	[redacted]-Jan-2019 23:54	-	
[redacted]	[redacted]-Jan-2019 22:48	-	
[redacted]	[redacted]-Dec-2018 23:53	-	
[redacted]	[redacted]-Nov-2018 23:53	-	
[redacted]	[redacted]-Nov-2018 23:56	-	
[redacted]	[redacted]-Oct-2018 23:47	-	
[redacted]	[redacted]-Jan-2017 16:43	-	
[redacted]	[redacted]-Feb-2016 19:23	-	
[redacted]	[redacted]-Feb-2016 12:35	-	
[redacted]	[redacted]-Jan-2016 23:51	-	
[redacted]	[redacted]-Nov-2014 21:50	-	
[redacted]	[redacted]-Oct-2014 12:38	-	
[redacted]	[redacted]-Feb-2014 16:59	36M	
[redacted]	[redacted]-Oct-2013 23:39	-	
[redacted]	[redacted]-Oct-2013 23:37	-	
[redacted]	[redacted]-Oct-2013 23:27	-	



Ονομα εκπαιδευόμενου	Αρ. Μητρώου	Όνομα αρχείου	Ημ/νία αποστολής	Βαθμός
[redacted]	[redacted]	[redacted].docx	2020-[redacted]12	
[redacted]	[redacted]	[redacted].zip	2020-[redacted]30	
Σχόλια: [redacted]				
[redacted]	[redacted]	[redacted].zip	2020-[redacted]26	
[redacted]	[redacted]	[redacted].rar	2020-[redacted]17	
Σχόλια: [redacted]				
[redacted]	[redacted]	[redacted].zip	2020-[redacted]08	
Σχόλια: [redacted]				
[redacted]	[redacted]	[redacted].rar	2020-[redacted]30	
[redacted]	[redacted]	[redacted].rar	2020-[redacted]42	
[redacted]	[redacted]	[redacted].pdf	2020-[redacted]54	
Σχόλια: [redacted]				
[redacted]	[redacted]	[redacted].zip	2020-[redacted]04	
Σχόλια: [redacted]				
[redacted]	[redacted]	[redacted].pdf	2020-[redacted]56	



Index of /courses/[redacted]/work/5d[redacted]50

Name	Last modified	Size	Description
Parent Directory		-	
A[redacted]	[redacted]	19M	
B[redacted]	[redacted]	19M	
F[redacted]	[redacted]	4.5M	
C[redacted]	[redacted]	466K	
L[redacted]	[redacted]	9.2M	
M[redacted]	[redacted]	8.2M	
M[redacted]	[redacted]	13M	
N[redacted]	[redacted]	5.7M	
P[redacted]	[redacted]	1.6M	
P[redacted]	[redacted]	1.3M	
P[redacted]	[redacted]	6.3M	
S[redacted]	[redacted]	12M	
n[redacted]	[redacted]	7.7M	

👍 1

iamaldi commented on Aug 17, 2020 • edited

Hi,

I was wondering if there's a responsible disclosure policy that we can follow instead of disclosing security issues in the public?

GitHub has added the Security panel to every repository but seems like this one is not configured yet.

Thanks

XhmikosR commented on May 23, 2021

@adia: has this been taken care of in v3.10.x? The changelog is a little cryptic...

adia commented on May 23, 2021 Contributor

Hello, and thanks for reminding us of this bug report. You are right, this is still a problem, especially for smaller installations on shared hosting where directory listings might be enabled and admins might not notice the problem. We do advise disabling them in our installation instructions.

We were preparing a new release (3.11) for tomorrow, and we'll make sure this is addressed by adding an empty "index.html" in all new subdirectories and creating it on upgrade in case it doesn't exist.

As for a disclosure policy, we'll publish something more official in GitHub's Security panel, but if you find any vulnerabilities, please report them by email to eclass@gunet.gr (which is read only by the core team).

Thanks again, and sorry for not taking care of your report earlier.

adia self-assigned this on May 23, 2021

XhmikosR commented on May 23, 2021 • edited

@adia: please make sure you mention it properly in the release notes and also have someone update the CVE details. The report here was a valid one IMHO and this has been in public for so long...

If this is fixed, you might have to release new patch versions for 3.9.x etc; I'm unsure what's your support policy.

On a side note, at least the Bootstrap version you are using has known security issues, specifically quite a few XSS issues. You should update to the latest 3.4.1. jQuery and probably other plugins have further security issues too.

> Thanks again, and sorry for not taking care of your report earlier.

Not my report, you should give credits to **@emaragkos** when you publish a security advisory along with any other actions for your supported versions.

PS. I'm still not sure if the files should be accessible from the outside without authentication... Right now anyone with a link can access the file even if they are not authenticated.

adia commented on May 23, 2021 Contributor

Will do about giving credit and upgrading our JS dependencies - that "your report" was addressed to everyone participating here, but of course, thanks and credit goes to **@emaragkos**. Although - we knew that if directory listings are enabled, no files are secure, and that's why disabling directory indexes is one of the first installation steps we recommend.

The proper fix is to support putting the data directory outside the web root, so that there's no need for configuration on the web server to limit direct access, but given our scant development resources we haven't prioritized that. We'll try to work on this for the next release.

Our policy is that all installations should upgrade to the latest release, but if anyone asks, and offers a justification for not being able to upgrade (e.g. being in the middle of exams period so that any changes are unwelcome) we work with them to provide fixes for known problems, as long as the changes are localized - for wider changes we always recommend upgrading to the latest release since we can't properly test big back-ported changes properly.

XhmikosR commented on May 23, 2021 • edited

The thing is that right now even search engines have crawled plenty of files in some cases (the one I have access on). So, even if you place an empty `index.html` file or the organization fixes their bogus installation, the files are still accessible and easily found in public.

emaragkos commented on May 23, 2021 Author

This issue might seem of little importance at first, but given the fact that during covid19 quarantine many institutions used eClass as a solution for online remote exams, it poses a huge impact on confidentiality of private and sensitive data.
It does not only expose students' personal data (name, surname, email, student ID, even photos with gov or academic ID used for proof of identity) but also exposes private semester assessments, unreleased exam subjects and submitted answers resulting in compromising the integrity of the whole examination process.
I think this should be fixed asap with a temporary patch such as the index.html mentioned until there is time for a proper solution.
I'm sorry for posting it here in the first place, I wasn't aware of the recommended alternative way to report similar issues.

👍 1

adia added a commit that referenced this issue on May 24, 2021

`Upgrade: Create index.html in all course directories to hinder listin…` … fc96d52

Assignees

adia

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants