

Safer:

The History and Future of Open edX Security



<https://tinyurl.com/oec-2023-security-wg>



Hello!



Feanil Patel

Architect @ Axim (tCRIL)



Alison Langston

Engineer @ 2U



Phil Shiu

Engineer @ 2U

Agenda



<https://tinyurl.com/oec-2023-security-wg>

- History
- CVSS Scoring
- Prior System Pitfalls
- OEP-60 & ✨ Security WG ✨
 - Github Security Advisories
 - Coordinated Disclosures
 - Maintainer Responsibilities
- Proactive Security Work

What is a security vulnerability?

A vulnerability is a **hole** or a **weakness** in the application, that allows an attacker to cause **harm** to the stakeholders of an application.

—OWASP

What is a security vulnerability?

A vulnerability is a hole or a weakness in the application, that allows an attacker to cause harm to the **stakeholders** of an application.

—OWASP

What is a security vulnerability?

1. Broken access control

How public should this be?

2. Cryptographic failures

Should this be encrypted?

3. Injection

Is user input validated?

4. Insecure design

How can this be abused?

5. Security misconfig

What is on by default?

6. Outdated components

How to keep this up-to-date?

7. Auth failures

Is it hard to cheat auth?

8. Integrity failures

Who is trusted and why?

9. Observability failures

Is it easy to observe my app?

10. URL forgeries

Can I trust my URLs?

Source

Who sends security-related emails?

~70

issues per year

45%

by maintainers

Other reporters include:

governments

security labs

security researchers

operators

(and you!)



Previously on SWG...

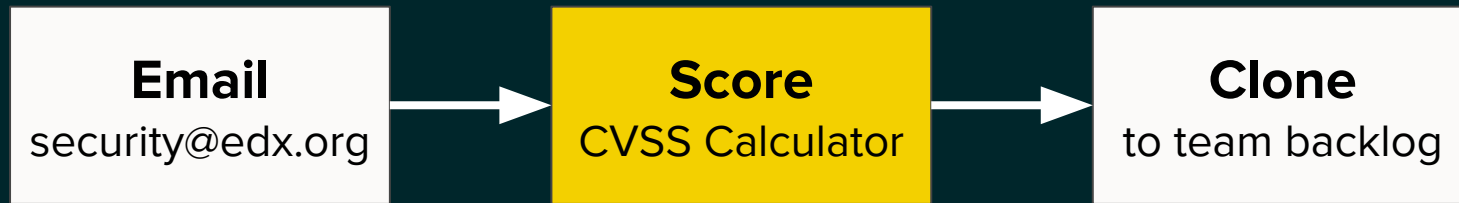
Previously on SWG...

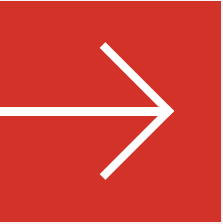


- **edX** handled all security issues
- Fixes were made by teams internal to edX
- Patches were published to a small group first and then made public.

Previously on SWG...

“Security scoring as a service”

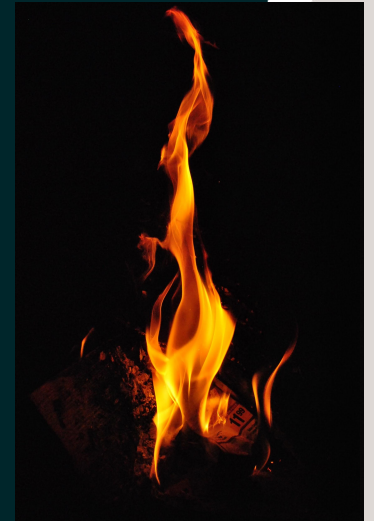




CVSS Scoring

CVSS → Severity

Severity	Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0



Base Score

Attack Vector (AV)

Network (N) Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC)

Low (L) High (H)

Privileges Required (PR)

None (N) Low (L) High (H)

User Interaction (UI)

None (N) Required (R)

Scope (S)

Unchanged (U) Changed (C)

Confidentiality (C)

None (N) Low (L) High (H)

Integrity (I)

None (N) Low (L) High (H)

Availability (A)

None (N) Low (L) High (H)

Select values for all base metrics to generate score

An XSS Vulnerability in the Wiki

Base Score

9.3
(Critical)

Attack Vector (AV)

Network (N) Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC)

Low (L) High (H)

Privileges Required (PR)

None (N) Low (L) High (H)

User Interaction (UI)

None (N) Required (R)

Scope (S)

Unchanged (U) Changed (C)

Confidentiality (C)

None (N) Low (L) High (H)

Integrity (I)

None (N) Low (L) High (H)

Availability (A)

None (N) Low (L) High (H)

Session_id Cookie Not marked Secure

Base Score

7.1
(High)

Attack Vector (AV)

Network (N) Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC)

Low (L) High (H)

Privileges Required (PR)

None (N) Low (L) High (H)

User Interaction (UI)

None (N) Required (R)

Scope (S)

Unchanged (U) Changed (C)

Confidentiality (C)

None (N) Low (L) High (H)

Integrity (I)

None (N) Low (L) High (H)

Availability (A)

None (N) Low (L) High (H)

Session Cookie not expiring at Logout

Base Score

3.2
(Low)

Attack Vector (AV)

Network (N) Adjacent (A) Local (L) **Physical (P)**

Attack Complexity (AC)

Low (L) High (H)

Privileges Required (PR)

None (N) Low (L) High (H)

User Interaction (UI)

None (N) **Required (R)**

Scope (S)

Unchanged (U) Changed (C)

Confidentiality (C)

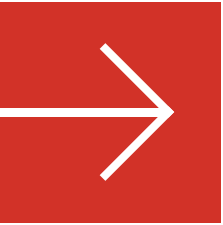
None (N) **Low (L)** High (H)

Integrity (I)

None (N) **Low (L)** High (H)

Availability (A)

None (N) Low (L) High (H)

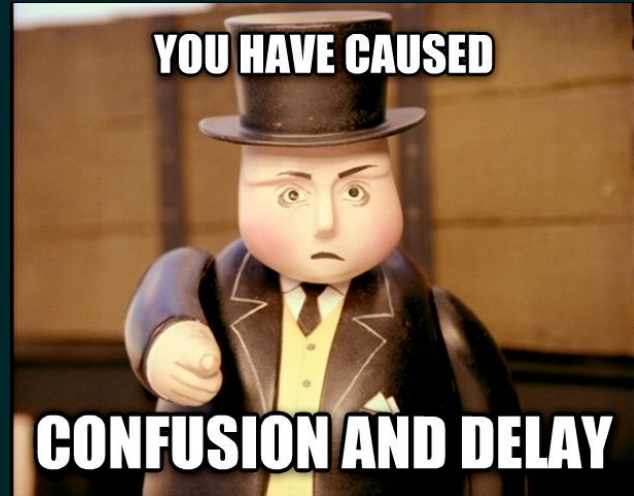


Previously on SWG...

there were some issues...

Previously on SWG...there were some issues...

- Notification was complicated
 - security-notifications@edx.org
 - git patches
 - Different for different repos



Previously on SWG...there were some issues...

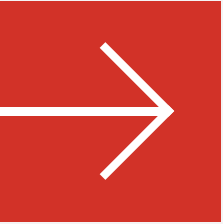
- edX/2U didn't always have the experts.
 - Expertise lived across the community
 - Experts had left



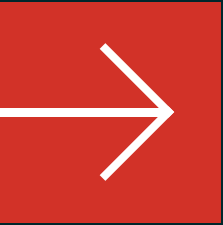
Previously on SWG...there were some issues...

- Not all Open edX deployments are the same
 - Different critical services
 - Different features enabled
 - Different security vulnerability surface area





OEP-60



Introducing the Open edX Security Working Group!

Hello!



Feanil Patel

Architect @ Axim (tCRIL)



Alison Langston

Engineer @ 2U



Phil Shiu

Engineer @ 2U

SWG Responsibilities

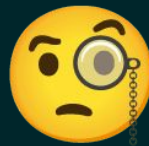


Triage open source vulnerabilities

SWG Responsibilities



Triage open source vulnerabilities



Advise maintainers on security matters

SWG Responsibilities



Triage open source vulnerabilities



Advise maintainers on security matters



Work on proactive security measures

Security Release Process

GitHub Security Advisories



Coordinated Disclosures

Vulnerability in LTI 1.3 Grade Pass Back Implementation

Published Low alangsto published GHSA-7j9p-67mm-5g87 on Jan 24 · 16 comments

Package	Affected versions	Patched versions
xblock-lti-consumer (pip)	>= 7.0.0	7.2.2

alangsto opened on Dec 16, 2022

Description

Problem

TL;DR: Any LTI tool that is integrated with on the Open edX platform can post a grade back for any LTI XBlock so long as it knows or can guess the block location for that XBlock.

In LTI 1.3, LTI tools can "pass back" scores that learners earn while using LTI tools to the edX platform. The edX platform then stores those LTI scores in a separate table. If the right conditions are met, these scores are then persisted to the LMS grades tables.

Severity

Low 3.7 / 10

CVSS base metrics

Attack vector	Network
Attack complexity	High
Privileges required	Low
User interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity	Low
Availability	None

CVSS:3.1(AV:N/A,C:H,PR:L,UI:R,S:U,C:L,I:L,A:N)

CVE ID

CVE-2023-23611

Upcoming Security Release: xblock-lti-consumer

Announcements Security

giovannicimolin Giovanni Cimolin (OpenCraft) - <https://opencraft.com/help> Core Contributor Jan 19

On Tuesday, January 24, we'll be releasing version 7.2.2 of xblock-lti-consumer. This release will contain a **Low** level security fix as determined using CVSS.

Affected repository: xblock-lti-consumer.

Vulnerability Score: Low (CVSS Score 3.7).

Patch release date & time: 2023-01-24 (time TBD).

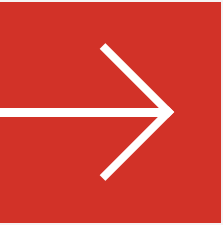
This post will be updated with the vulnerability details **after** the patch is released.

3 ❤️ Reply

created Jan 19 last reply Feb 7 8 replies 126 views 6 users 7 likes 7 links

1 / 9
Jan 19
Jan 19

Feb 7



GitHub Security Advisories

GitHub Security Advisories

- Reduce complexities for security fixes
 - Avoids the intricacies that were part of the 2U internal private release process

GitHub Security Advisories

- Reduce complexities for security fixes
 - Avoids the intricacies that were part of the 2U internal private release process
- Provide collaborative, private environment
 - Allows vulnerabilities to be discussed and patched prior to release
 - Any maintainer can resolve a vulnerability

GitHub Security Advisories

- Reduce complexities for security fixes
 - Avoids the intricacies that were part of the 2U internal private release process
- Provide collaborative, private environment
 - Allows vulnerabilities to be discussed and patched prior to release
 - Any maintainer can resolve a vulnerability
- Consistent across repositories
 - Any vulnerability in any repository can now be fixed



Vulnerability in LTI 1.3 Grade Pass Back Implementation

Edit advisory

Published Low alangsto published GHSA-7j9p-67mm-5g87 on Jan 24 · 16 comments

Package

 xblock-lti-consumer (pip)

Affected versions

>= 7.0.0

Patched versions

7.2.2

Severity

Low 3.7 / 10

alangsto opened on Dec 16, 2022

Description

Problem

TL;DR: Any LTI tool that is integrated with on the Open edX platform can post a grade back for any LTI XBlock so long as it knows or can guess the block location for that XBlock.

In LTI 1.3, LTI tools can "pass back" scores that learners earn while using LTI tools to the edX platform. The edX platform then stores those LTI scores in a separate table. If the right conditions are met, these scores are then persisted to the LMS grades tables.

CVSS base metrics

Attack vector	Network
Attack complexity	High
Privileges required	Low
User interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity	Low
Availability	None

CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:N

CVE ID

CVE-2023-23611

Collaborate on a patch

HTTPS

SSH

GitHub CLI

org-6811672@github.com:octo-org/octo-repo-ghsa-



Use [the temporary private fork](#) to collaborate on a patch for this advisory.

Clone and create a new branch

```
git clone org-6811672@github.com:octo-org/octo-repo-ghsa-6qw9-j83m-6jcj.git
cd octo-repo-ghsa-6qw9-j83m-6jcj
git checkout -b advisory-fix-1
```



Make your changes, then push

```
git push -u origin advisory-fix-1
```



Collaborate on a patch

HTTPS


SSH


GitHub CLI

org-6811672@github.com:octo-org/octo-repo-ghsa-



Use [the temporary private fork](#) to collaborate on a patch for this advisory.

 octocat-patch-1-1 (less than a minute ago)

 Compare & pull request

Important to Note

- Only repository admins can
 - Create a security advisory
 - Create a private fork
 - Add collaborators
 - Merge a PR
 - Publish a security advisory

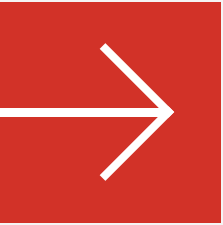
Important to Note

- Only repository admins can
 - Create a security advisory
 - Create a private fork
 - Add collaborators
 - Merge a PR
 - Publish a security advisory

- Once a private fork has been merged
 - Publish the security advisory
 - Add reply to the security announcement post on discuss.openedx.org
 - ... within 2 hours!

Important to Note

- Only repository admins can
 - Create a security advisory
 - Create a private fork
 - Add collaborators
 - Merge a PR
 - Publish a security advisory
- Once a private fork has been merged
 - Publish the security advisory
 - Add reply to the security announcement post on discuss.openedx.org
 - ... within 2 hours!
- Additional info on security advisories can be found on [GitHub](#)



Coordinated Disclosure Process



Security Announcements

Now in Discourse

The screenshot shows a web browser window displaying the Open edX Security Announcements page. The browser's address bar shows the URL `discuss.openedx.org/c/announcements/security/19`. The page features the Open edX logo and a search bar. A prominent orange banner at the top reads "Security" with the subtitle "Official security announcements". Below this, there are navigation tabs for "Announcements", "Security", and "all tags". The main content area is divided into two columns: a list of topics on the left and a notification settings sidebar on the right.

Topics:

- Topic
- About the Security category
Official security announcements
- Package Publishing to NPM Temporarily Disabled
- Upcoming Security Release: xblock-lti-consumer
- Security: Git vulnerabilities patched, please upgrade
- Introducing: the Security Working Group
working-groups
- Security: Patch for disable user refreshable JWT token

Notification Settings:

- Watching**
You will automatically watch all topics in this category. You will be notified of every new post in every topic, and a count of new replies will be shown.
- Tracking**
You will automatically track all topics in this category. You will be notified if someone mentions your @name or replies to you, and a count of new replies will be shown.
- Watching First Post**
You will be notified of new topics in this category but not replies to the topics.
- Normal**
You will be notified if someone mentions your @name or replies to you.
- Muted**
You will never be notified of anything about new topics in this category, and they will not appear in latest.

The bottom of the page shows a table of recent posts with columns for user avatars, topic titles, reply counts, and dates.



Coordinated Disclosure Process

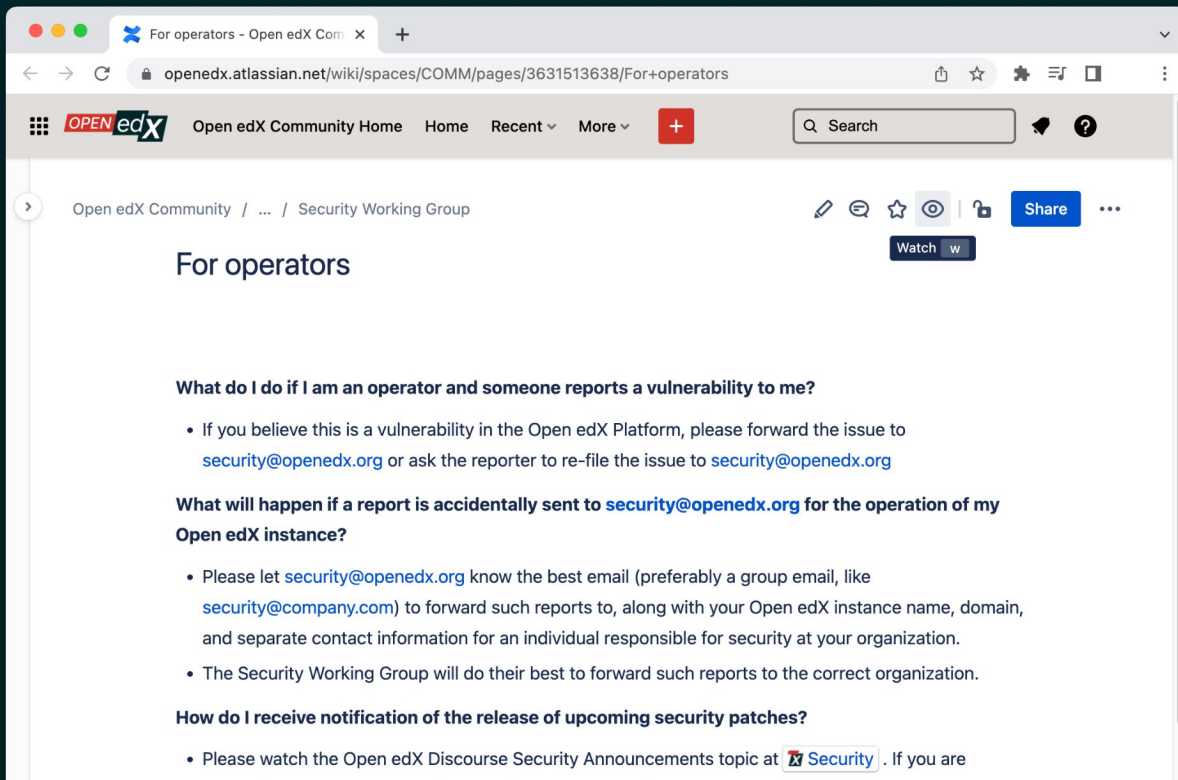
The screenshot shows a browser window with the URL `discuss.openedx.org/t/upcoming-security-release-xblock-lti-consumer/9165`. The forum post is titled "Upcoming Security Release: xblock-lti-consumer" and is categorized under "Announcements" and "Security". It was posted by **giovannicimolin** (Giovanni Cimolin) on Jan 19. The post content includes:

- On Tuesday, January 24, we'll be releasing version 7.2.2 of `xblock-lti-consumer`. This release will contain a **Low** level security fix as determined using CVSS.
- Affected repository:** `xblock-lti-consumer`.
- Vulnerability Score:** Low (CVSS Score 1).
- Patch release date & time:** 2023-01-24 (time TBD).

The post notes it will be updated with vulnerability details after the patch is released. It has 3 likes and 8 replies. A summary bar shows 1/9 replies from Jan 19. A reply from **zhancock_edx** (Zach Hancock) on Feb 7 is partially visible at the bottom.

Operator Q&A

[Find it in Confluence](#)



The screenshot shows a web browser window with the following elements:

- Browser Tab:** For operators - Open edX Com
- Address Bar:** openedx.atlassian.net/wiki/spaces/COMM/pages/3631513638/For+operators
- Navigation:** Open edX Community Home, Home, Recent, More, and a search bar.
- Breadcrumbs:** Open edX Community / ... / Security Working Group
- Page Title:** For operators
- Actions:** Edit, Comment, Star, Watch, Lock, Share, and a Watch button.
- Content:**
 - Section:** What do I do if I am an operator and someone reports a vulnerability to me?
 - Text:** If you believe this is a vulnerability in the Open edX Platform, please forward the issue to security@openedx.org or ask the reporter to re-file the issue to security@openedx.org
 - Section:** What will happen if a report is accidentally sent to security@openedx.org for the operation of my Open edX instance?
 - Text:** Please let security@openedx.org know the best email (preferably a group email, like security@company.com) to forward such reports to, along with your Open edX instance name, domain, and separate contact information for an individual responsible for security at your organization.
 - Text:** The Security Working Group will do their best to forward such reports to the correct organization.
 - Section:** How do I receive notification of the release of upcoming security patches?
 - Text:** Please watch the Open edX Discourse Security Announcements topic at [Security](#). If you are



For Maintainers

Maintainer Runbook

For maintainers - Open edX Co. x +

openedx.atlassian.net/wiki/spaces/COMM/pages/3630923873/For+maintainers

OPEN edX Open edX Community Home Home Recent Spaces Teams Apps Templates Create Q Search 9+ ?

Runbooks

After getting a "New security vulnerability" email from security@openedx.org

1. Fix the vulnerability in a temporary private fork. Do not merge yet. [\[GitHub docs\]](#)
2. Post a release time in [Security Announcements](#).
 - a. Don't post until you test your fix.
 - b. Make the release time on a weekday at least 48 hours after your post.
- c. Template:
 - i. Title:

```
1 Security: Upcoming Security Release for {{repository_name}} on {{YYYY-MM-DD}}
```
 - ii. Body:

```
1 **openedx/{{repository_name}}** version **{{version_number}}** will be release
2
3 It will fix one security defect with a "{{severity}}" [CVSS 3.1 severity rating]
4
5 Details will be published here after release: [GitHub security advisory]{{github_advisory}}
```
- d. Example:
 - i. Title:

```
1 Security: Upcoming Security Release for xblock-drag-and-drop-v2 on {{2023-01-2}}
```
 - ii. Body:



Maintainer Responsibilities

- Notify security@openedx.org if a security vulnerability is found
- Resolve disclosed security vulnerabilities

263 Lines (186 sloc) | 13.5 KB

Raw Blame

repository to resolve the vulnerability.

Maintainer Responsibility

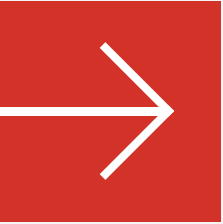
Maintainers are ultimately responsible for resolving disclosed security vulnerabilities.

To assist the maintainer with tracking their repository's vulnerabilities, the Security Working Group will create a [GitHub repository security advisory](#) pre-assigned with the scored severity. Security advisories in a draft state are not visible to the public.

Maintainers should inform the Security Working Group if they judge a vulnerability to be a different severity than what was originally triaged. The Security Working Group must accept the maintainer's adjudication, but should comment on any considerations around the adjudication.

Maintainers will be routinely reminded to remediate disclosures in a frequency proportional to the severity of the disclosure. The following table shows the default reminder frequency until resolution of each severity classification:

Severity	Score	Reminder frequency
Low	≥0.1	Twice a year
Medium	≥4.0	Once a quarter
High	≥7.0	Once a month
Critical	≥9.0	Once a week



Proactive Security Work

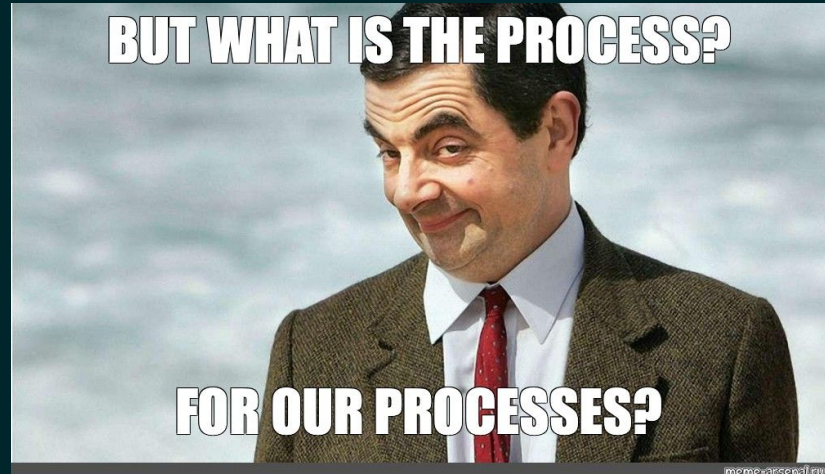
Collaboration

- Transition from 2U internal SWG to Open edX SWG
- Coordinate with other WGs
 - Outline process for updating dependencies
 - Advise on best practices
- "Spot the Vuln" puzzle hunt



Process Improvements

- Annual security survey
- Standardize GitHub security config
- Make & improve runbooks



Technology Improvements

- Better visibility for supply chain security issues
- Adding security suites to GitHub CI

... and more!



Get Involved!

If you ...

- Want to join the Security WG...
- Find a security vulnerability...
- Have questions about fixing vulnerabilities...
- Want to help fix vulnerabilities...
- Have ideas of how to better fix security vulnerabilities...

Email security@openedx.org !

We'd love to hear from you.

Thank you!

 security@openedx.org

 [#wg-security](#) (disclosures by email)

 Learn more about [OEP-60](#)

 See what we're doing on [GitHub](#)

 Find us on [Confluence](#)

Questions?