



MDLShield - Expert security code reviews for Moodle™ plugin developers

Alexander Bias | ssystems GmbH



Disclaimer



Disclaimer

- ▶ MDLShield is a new commercial service by LMSCloud Limited, more known by its founder Marina Glancy.
- ▶ MDLShield is not affiliated with Moodle HQ.
- ▶ Neither ssystems nor myself are commercially affiliated with MDLShield.

We also do not benefit if you buy MDLShield credits after this session.



Demo, part 1

Anyone here who wants her / his
published plugin scanned for free?



Motivation



Motivation

- ▶ Vulnerabilities in Moodle plugins (and Moodle code in general, of course) threaten educational institutions.
- ▶ Moodle plugins have to adhere the same security guidelines and best practices as Moodle core.
- ▶ Unfortunately, Moodle plugin developers are not always aware of all best practices. And glitches can always happen.

Motivation

- ▶ Please ask yourself:
 - ▶ As developer, do you want to be the plugin author whose plugin was used as attack vector to bring down hundreds of Moodle sites?
 - ▶ As admin, do you read every single line of code which you deploy on your Moodle instance? Do you know and trust all the developers whose Moodle plugins you run?



Motivation

- ▶ As the answer to these questions is probably no, MDLShield allows you to:
 - ▶ Catch vulnerabilities before your users do.
 - ▶ Protect the institutions that rely on your code.
 - ▶ Build a reputation for secure, trustworthy plugins.



Service functionality



How is it done

- ▶ It's done with AI, of course.
- ▶ Everyone can run a good AI security review from home nowadays.

But MDLShield goes beyond:

- ▶ MDLShield scans your Moodle plugin codebase with a full Moodle core codebase as context.
- ▶ MDLShield knows all Moodle best practices and checks your plugin against them.
- ▶ MDLShield is a member of the
Anthropic Cyber Verification Program



What do you get

- ▶ A logically structured security report, highlighting all findings and their impact.
- ▶ For each finding, you get an explanation of the attack vector and possible exploits.
- ▶ For each finding, you get actionable fix guidance (i.e. a suggested fix).



What else do you get

- ▶ An overall audit of the quality of the plugin, including non-security related aspects.
- ▶ The possibility to publish the audit report.
- ▶ And a badge for your repository's readme file ;)



Some figures

- ▶ The service is live for several weeks now.

And, up to now, it has already:

- ▶ 6.0M+ lines reviewed
- ▶ 910 findings surfaced
- ▶ 212 security issues found



Service scope

What can be scanned

- ▶ Published plugins which are published on moodle.org
- ▶ Pre-releases of such plugins (new!)
- ▶ Private plugins as bring-your-own-repository review via Git (new!)



What's planned to come next

- ▶ Plugin release monitoring to automatically trigger a review.
- ▶ CI pipeline integration and native Github App.
- ▶ "Copy to LLM/Agent" button and automated pull requests for fixes.
- ▶ Publish private repository reviews.
- ▶ New publish mode "Summary" with vulnerability, code, exploit details redacted - more of an "Attestation", especially for private plugins.
- ▶ Export review in Markdown/Other formats.



Pricing



Pricing

- ▶ 2 AI reviews per month are free for published, non-commercial plugins
 - ▶ This is an appreciation to the work of part-time Moodle developers who just maintain one / few plugins
- ▶ The intended workflow with these credits:
 1. Scan your plugin
 2. Fix the findings in your plugin
 3. Scan your plugin again
 4. Publish your A+ report ;)



Pricing

- ▶ \$25 per AI review
- ▶ Use the *MOOTDACH26* promo code to get a 50% discount.
The code is valid until the end of the week
as an appreciation to the Moodle D-A-CH community.
- ▶ Furthermore:
Human expert audits, whole-site audits and custom work
can be discussed on request.



Take home message

Moodle plugin AI security reviews are here to stay:
Scan and fix your plugins before the bad guys do



Demo, part 2

Let's have a look at the scan report
&
Ask your questions!

ssystems

Ihr Partner für innovative Digitalisierung

online studieren



abias@ssystems.de



030202360710



www.ssystems.de