Moodle security:

Building trust through open collaboration

moodle™

Table of contents

Executive summary

Security isn't a feature. It's the foundation. If you're using, building, or managing Moodle, data protection is a part of your everyday thinking. That's why Moodle is designed to help you stay protected—no matter your role, industry, or scale.

At Moodle, we view security through the lens of transparency and shared responsibility. Our open-source model is not a liability; it is one of our greatest strengths. By making our code publicly available, we invite a global community of developers, researchers, and users to identify vulnerabilities, strengthen defenses, and improve resilience together. Open collaboration is one of the most powerful tools we have to stay ahead of emerging threats.

This whitepaper explores Moodle's comprehensive approach to security.

It addresses common misconceptions about open-source software, highlights the unique benefits and challenges that come with open-source development, and outlines actionable steps organizations can take to maintain a secure environment for their Moodle platform. Whether you are a government agency navigating compliance requirements, an IT professional safeguarding infrastructure, or a Moodle LMS user seeking detailed, transparent information, this guide aims to equip you with the tools and knowledge needed to keep your learning environments secure.

Because security isn't just about protecting data - it's about protecting trust.

Understanding open source and security

Open-source software (OSS) is built on a powerful concept: transparency. By making source code publicly available, OSS platforms like Moodle LMS benefit from collective innovation and faster identification of vulnerabilities compared to closed, proprietary systems. Rather than relying on a small internal team, open-source communities leverage the insights and expertise of thousands of developers worldwide.

However, misconceptions about open-source security persist. It's important to address these head-on.

Myth: "If the code is public, hackers can exploit it more easily."

While it's true that malicious actors can view open-source code, so can security researchers, ethical hackers, and developers who work tirelessly to identify and fix vulnerabilities quickly. The open review process often leads to stronger, more resilient systems compared to closed-source software, where vulnerabilities can remain hidden for long periods.

Myth: "Open and closed systems can't coexist."

Modern open-source platforms, including Moodle LMS, are built for interoperability. Secure APIs and robust plugin architectures enable Moodle to integrate seamlessly with proprietary systems, including CRMs, ERPs, and AI tools, without compromising security.

Myth: "Open-source users are on their own."

Choosing open source doesn't mean navigating security alone. Moodle's global community, alongside services provided by Moodle and Moodle Certified Partners, offers expert guidance, proactive threat monitoring, and enterprise-level support.

Myth: "Open-source platforms can't meet enterprise needs."

Moodle LMS - and Moodle Workplace, which extends LMS capabilities - demonstrates that open-source solutions can deliver scalability, security, and flexibility for enterprises, governments, and large organisations worldwide.

Today, Moodle LMS powers:

- Over **148,000** registered sites.
- More than **50 million** active courses.
- A global community of over **444 million** users across **237 countries.**

With over **3.1 billion** course enrolments and more than **10 billion** quiz questions created, Moodle proves that open-source platforms not only meet but exceed the demands of large-scale learning environments.

Moodle LMS

148,000+
registered
Moodle sites

50 million+
active courses

444 million+
users across
237 countries

3.1 billion+
course enrolments

10 billion+
quiz questions created

Why open source can be more secure

Open-source software offers distinct security advantages that are often overlooked. At its core, open-source transparency means that anyone - from developers to independent security researchers - can inspect the code, identify vulnerabilities, and propose fixes. This creates a collaborative environment where flaws are not hidden behind corporate walls but instead addressed openly and swiftly.

Collaborative flaw detection

One of the greatest strengths of open-source projects like Moodle LMS is collaborative flaw detection. With countless eyes reviewing the code daily, vulnerabilities can be identified and patched quickly, often faster than in proprietary systems where a smaller internal team is solely responsible for security. In the open-source model, “many eyes make bugs shallow,” leading to faster response times and more resilient systems.

Building trust through transparency

Transparency also builds trust. Rather than taking a vendor’s word that a platform is secure, users, developers, and independent auditors can verify it themselves. This openness not only fosters a culture of accountability but also strengthens user confidence - an essential quality in sectors like government, healthcare, and education where data protection is paramount.

Community-driven resilience

Community-driven resilience is another defining characteristic of open-source security. When a vulnerability is discovered in Moodle LMS, the global community - including Moodle, Moodle Certified Partners, and independent developers - mobilises to implement a fix. In this model, security is not the sole responsibility of a single organisation but a continuous, collective effort.

The strengths of open-source community security include:

- Rapid identification and resolution of vulnerabilities.
- Shared responsibility for ongoing improvement.
- Broader scrutiny across diverse sectors and use cases.

Adaptability, collaboration, and stronger security

Finally, open-source adaptability allows organizations to tailor security measures to their specific needs. With Moodle LMS, organizations can implement custom encryption protocols, integrate multiple authentication methods, and adapt the platform to meet evolving regulatory requirements. This flexibility enables users to proactively strengthen their own security posture rather than waiting for vendor-driven updates.

Open source doesn't mean insecure - it means transparent, accountable, adaptable, and resilient. Moodle embodies these principles, ensuring that open collaboration leads to stronger security for everyone.

Managing challenges in open source security

While open-source software brings remarkable advantages, it also introduces specific security challenges that must be actively managed. The very openness that enables collaboration can also expose vulnerabilities if proper processes are not followed.

The need for rigorous peer review

One of the most significant challenges lies in the diversity of contributors. With individuals and organisations around the world submitting improvements, there is a risk that some code changes may not undergo sufficiently rigorous review. Without a strong peer review process, flaws such as buffer overflows, improper input validation, or configuration weaknesses could inadvertently be introduced. To mitigate this, Moodle implements structured peer review protocols, requiring that contributions are thoroughly assessed before being accepted into the codebase.

Transparency alone is not enough

Another common misconception is that visibility alone guarantees security. Simply making code available for public inspection does not automatically mean that vulnerabilities will be found and resolved. A false sense of security can develop if organisations assume that "someone else" will spot issues. Open-source projects must combine transparency with proactive security measures, including:

- Formal security audits.
- Independent penetration testing.
- Structured responsible disclosure programmes.

Moodle actively undertakes all of these efforts to ensure that transparency is backed by rigorous, continuous improvement.

The importance of timely updates and patch management

Managing updates and patches is another area that demands vigilance. Organisations using Moodle LMS often rely on multiple plugins and external libraries, each with their own update cycles. This can lead to delays in applying critical security patches if not carefully monitored. To address this, Moodle encourages automated patch management practices, ensuring that updates are identified, prioritised by risk level, and applied promptly to maintain a strong security posture.

Collaboration as a strength

Despite these challenges, the benefits of open-source collaboration far outweigh the risks. By implementing robust review processes, prioritising proactive security measures, and promoting a culture of collective responsibility, Moodle ensures that the platform remains both innovative and resilient against evolving threats.

Moodle's security approach

At Moodle, security is embedded into every stage of our development and operations processes. Our commitment to safeguarding users' data and protecting learning environments is rooted in a **security by design** philosophy, meaning that security considerations are prioritised from the earliest stages of software development through to deployment and ongoing support.

Secure development practices

Moodle developers adhere to rigorous coding standards informed by internationally recognised frameworks, including the **OWASP Top Ten**, **Common Weakness Enumeration (CWE)**, and the **CIS Critical Security Controls.** By systematically embedding secure development practices, we reduce the risk of vulnerabilities and ensure our software evolves safely alongside emerging threats.

Proactive monitoring and responsible disclosure

Operationally, Moodle follows a proactive approach to security monitoring and vulnerability management. Through our structured **Vulnerability Disclosure Programme (VDP)**, we invite security researchers and users worldwide to report issues securely. All reports are assessed, prioritised, and resolved with urgency, following responsible disclosure practices that ensure patches are available before vulnerabilities are publicly announced.

Independent verification

Moodle's commitment to independent verification is evident through initiatives such as the SOC 2 Type 2 and SOC 3 certification achieved by Moodle services in the U.S. - a respected cybersecurity compliance standard that validates operational security practices.

Security enhancements in every release

Every new Moodle LMS release integrates enhanced security features. For example, recently Moodle LMS introduced:

- Multi-factor authentication (MFA)
- Support for physical security keys
- Strengthened password protection through the use of **password "peppers"**
- Read-once web service tokens to secure API interactions
- Customisable security settings for administrators.

The Moodle **Release page** provides links to all information regarding Moodle LMS releases, including security updates.

Within Moodle LMS, the **Security Overview Report** empowers site managers to monitor and improve their site's security posture proactively.

External audits and community collaboration

Beyond our internal organisational efforts, Moodle LMS benefits from external scrutiny. Many of our users - including governments, healthcare providers, and financial institutions - conduct rigorous security audits. Insights from these reviews often contribute to platform improvements that benefit the entire Moodle community.
By combining robust secure development practices, proactive vulnerability management, transparent communication, and collaboration with our global community, Moodle ensures a resilient foundation for secure online learning.

Why hosting matters: The backbone of Moodle platform security

The security of a Moodle LMS site does not depend solely on the software itself; it is equally shaped by where and how the site is hosted. Even the most secure platform can become vulnerable if deployed on inadequate infrastructure or without appropriate maintenance practices. Moodle hosting is not just a technical decision - it is a security decision.

Choosing a secure hosting environment

Choosing a well-managed and secure hosting environment can help ensure that Moodle LMS runs efficiently and is protected against common threats. Many organisations that host with Moodle Certified Partners benefit from timely updates, strong security configurations, and active monitoring practices. These approaches are designed to support a more stable, secure, and reliable learning environment.

Key hosting security best practices include:

- **Reliable, optimised infrastructure**
  Hosting with a Moodle Certified Partner ensures that your site is on a secure, well-maintained environment tailored for Moodle's performance and security needs.
- **Automatic security updates**
  A managed service ensures that Moodle core software, server components, and security patches are applied without delays.
- **SSL encryption on all pages**
  Protects data in transit by enforcing HTTPS for all users.
- **Proactive monitoring and threat detection**
  Certified providers continuously monitor for security risks, unauthorized access attempts, and system vulnerabilities.
- **Regular backups and disaster recovery**
  Managed hosting includes automated backups, ensuring quick recovery in case of an issue.

The risks of poor hosting

By contrast, poor hosting environments can expose Moodle LMS sites to serious threats. Delayed updates leave known vulnerabilities open to exploitation. A lack of threat monitoring can allow breaches to go undetected. Insufficient backup and disaster recovery planning can result in catastrophic data loss should an incident occur.

Signs of a poorly managed hosting environment include:

- Outdated Moodle LMS versions and unpatched server software.
- Missing or improperly configured SSL certificates.
- No regular backup schedule or unclear disaster recovery procedures.
- Little or no visibility into security monitoring or incident response processes.

These vulnerabilities can undermine even the most well-designed Moodle site.

How Moodle Certified Partners mitigate hosting risks

Moodle Certified Partners address these risks by offering hosting environments tailored specifically for Moodle LMS and Moodle Workplace. Typical services provided by Certified Partners include automatic software updates, SSL encryption across pages, continuous system monitoring, regular security audits, and comprehensive disaster recovery plans. Moodle Certified Partners also help organisations meet important compliance requirements, such as GDPR and HIPAA, by implementing rigorous data protection policies and protocols.

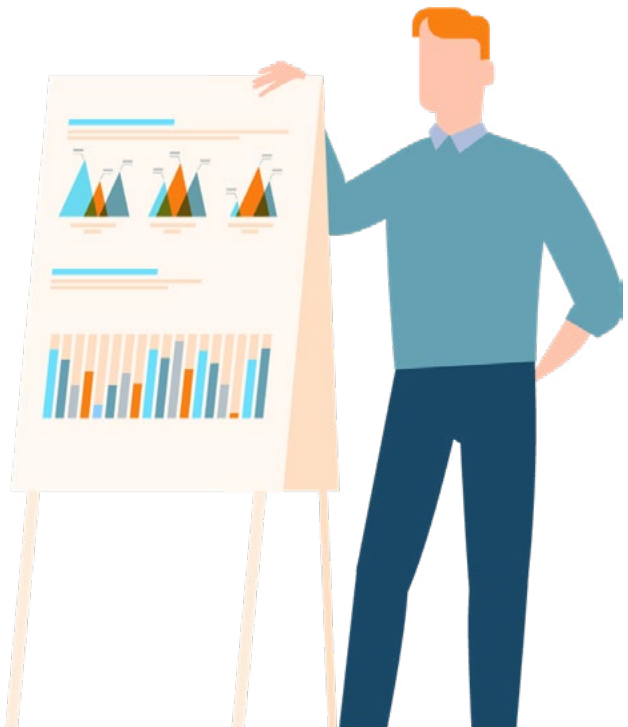
Hosting security as a strategic foundation

Working with a trusted Moodle hosting provider ensures that security best practices are embedded into the core of the site's operation - allowing administrators and educators to focus on delivering exceptional learning experiences rather than worrying about technical vulnerabilities.

Secure hosting is not just a best practice. It is a cornerstone of safeguarding your learning platform and the users who rely on it.

Reporting and resolving security issues

At Moodle, we recognise that no platform can be entirely free from vulnerabilities. What matters most is how quickly and responsibly security issues are identified, assessed, and resolved. Our Security procedures outline a structured approach to vulnerability management that ensures that risks are minimised and that users and administrators can continue to rely on Moodle platforms with confidence.



Clear and confidential reporting

The first step in addressing a potential security issue is clear and confidential reporting. Moodle operates a Vulnerability Disclosure Programme (VDP) in partnership with Bugcrowd, a trusted platform that enables security researchers and users to report vulnerabilities securely. Reports can also be submitted through the Moodle Tracker, with appropriate settings to keep sensitive information private during assessment.

Triage and issue assessment

Once an issue is reported, Bugcrowd's triage team conducts an initial review to determine its validity and severity. If confirmed, the issue is escalated to Moodle's internal security team. Every vulnerability is carefully assessed to understand its potential impact across all supported versions of Moodle LMS.

Patch development and testing

When a valid issue is identified, Moodle's development team works rapidly to create a fix. Thorough testing is conducted in a controlled environment to ensure that the patch not only resolves the vulnerability but does not introduce any unintended side effects. Stability, compatibility, and security are all rigorously validated before any update is released.

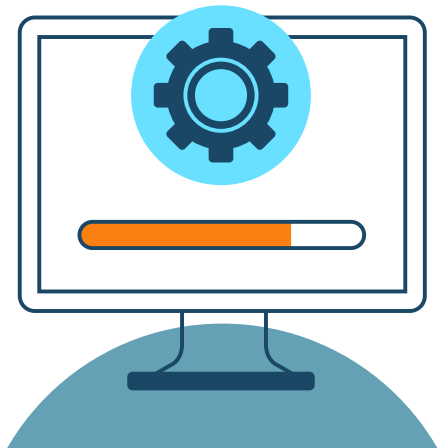
The key steps in our resolution process include:

- Developing and testing a fix in a secure environment.
- Coordinating advance notifications to site administrators.
- Assigning a Common Vulnerabilities and Exposures (CVE) identifier to confirmed issues.
- Publishing patches through the official Moodle LMS download site.

Coordinated disclosure and public announcement

After successful testing, Moodle prepares a coordinated disclosure. Administrators are given time to apply patches before the issue is publicly announced. Once an appropriate window has passed, resolved issues are announced through the Moodle Security News forum and other official channels. Contributors who report valid security issues are credited for their role in strengthening the platform.

Moodle does not currently operate a public bug bounty programme, but contributions through our VDP are actively acknowledged and valued. By encouraging responsible disclosure and fostering a collaborative security culture, we continue to strengthen the resilience of the entire Moodle ecosystem.



Reporting a security issue: How to do it right

If you come across a security issue, it's important to handle it the right way. Moodle has a clear process in place to ensure that vulnerabilities are reported, fixed, and kept under wraps until they're fully resolved. If a potential security issue is identified, follow these steps to report it securely:

How to guide

Step 1:

Report the issue

Use the Bugcrowd submission form: The quickest way to report a security issue is through Bugcrowd's submission form. Provide clear, step-by-step details so our security team can get a clear picture of the problem. If you're a developer and already have a fix, feel free to submit that, too.

Use Moodle Tracker if needed: If you're submitting a fix through the Tracker, set the security level to "Serious security issue" or "Minor security issue" to keep things private. If you're not sure whether an issue is a security risk, mark it as "Could be a security issue."

Step 2:

Bugcrowd's triage team takes a look

Once your issue is submitted, Bugcrowd's triage team will review it to determine whether it's valid or duplicate. If it's valid, it moves on to the Moodle security team for further evaluation.

Step 3:

Security review

The Moodle security team will assess the issue and its potential impact on all supported versions of Moodle. We may work with you directly to better understand the issue, but we'll keep things private until we have a fix in place.

Step 4:

Fix and test

Once we know what needs fixing, we'll develop a patch and test it thoroughly to ensure it solves the problem without creating new ones. This testing phase is critical to making sure the fix works.

Step 5:

Patch release and CVE notification

After testing, the patch is ready. We'll apply for a CVE identifier, then post the patch for download on **download.moodle.org**. Moodle site administrators will be notified by email about the fix, with a window to upgrade their sites before the issue is disclosed publicly.

Step 6:

Public announcement

Once the patch is out and site admins have had time to apply it, we'll announce the fix in the Moodle Security News forum. The issue has also been reported to the Open Source Software Security community so that everyone stays informed.

Step 7:

Closing the Issue

The Bugcrowd platform will mark the issue as fixed, and you'll get notified if you report it. This means the issue has been resolved and closed.

Best practices for maintaining a secure Moodle LMS site

Maintaining a secure Moodle LMS environment requires an ongoing commitment to best practices, from the initial hosting decision through to day-to-day site management. A secure foundation begins with choosing the right hosting partner - but it extends into every aspect of how the platform is operated and maintained. Periodically reviewing Moodle's Security recommendations can help make sure administrators are aware of emerging threats and new protective measures.

Manage third-party plugins thoughtfully

Third-party plugins can significantly enhance Moodle LMS functionality, but they can also introduce vulnerabilities if not carefully managed. It is critical to install only trusted plugins, preferably those available through the official **Moodle Plugins Directory**. Organisations should review installed plugins regularly, remove any that are unnecessary, and apply updates promptly to maintain a strong security posture.

Strengthen access controls and user authentication

Controlling who can access your site - and how - is essential for protecting sensitive data. Moodle LMS offers powerful **role-based** access controls that should be applied carefully. Administrators should:

- Enforce strong **password policies** for all users.
- Enable **multi-factor authentication (MFA)** wherever possible.
- Audit user accounts regularly to ensure **permissions** match current roles.
- **Limit failed login attempts** to prevent brute-force attacks.
- Enable **reCAPTCHA** for user registrations and require email verification for new accounts.

Applying these controls strengthens the site's overall resilience against unauthorised access and automated attacks.

Review and fine-tune site security settings

Administrators should take full advantage of Moodle's built-in **Site Security Settings** to harden their environments. This includes requiring users to log in before viewing profiles or pictures, enforcing stronger password policies, managing upload limits and quotas, and restricting risky features such as embedded content. Regularly reviewing and adjusting these settings ensures that the site maintains a high security baseline even as organisational needs evolve.

Keep your Moodle LMS site up-to-date

Keeping Moodle LMS updated is critical for maintaining a secure and stable environment. Administrators should:

- Upgrade regularly to the latest supported Moodle version to receive security patches and improvements.
- Apply minor updates (point releases) promptly when they are released.
- Prioritise upgrading to Long-Term Support (LTS) versions if longer maintenance cycles and stability are important.

LTS versions of Moodle receive critical security updates for a longer period than standard releases, making them an excellent choice for organisations seeking a balance between security and upgrade flexibility.

Administrators can find detailed information about Moodle LMS version releases, security support periods, and upgrade schedules on the **Moodle Releases** page. This resource outlines the latest stable releases, LTS versions, and provides target dates for future updates, helping organisations plan upgrades and maintain compliance with supported versions.

Monitor, audit, and partner for security

Maintaining security is not a one-time task; it requires ongoing monitoring, auditing, and collaboration. Administrators should make regular use of Moodle's **Security Overview Report** to identify potential configuration issues and review **system logs** to detect suspicious activity early. Many organisations benefit from partnering with a Moodle Certified Service Provider to access expert security support, proactive monitoring, and specialist advice tailored to their needs.

Conclusion

Security is not a single feature or a one-time achievement - it is a continuous commitment that underpins everything Moodle does. From our open-source development philosophy to our structured vulnerability management processes, Moodle LMS is built to empower organisations with a platform that is open, transparent, resilient, and secure.

By choosing Moodle LMS, organisations are not simply selecting a learning management system; they are joining a global community that shares responsibility for strengthening the platform. Through collaboration with security researchers, developers, Moodle Certified Partners, and users worldwide, we are able to identify risks quickly, resolve vulnerabilities responsibly, and drive continuous improvement.

Maintaining a secure Moodle LMS site requires more than software. It demands best practices in hosting, plugin management, user authentication, monitoring, and ongoing vigilance. For many, partnering with a Moodle Certified Provider offers the confidence that security, compliance, and operational excellence are embedded into every aspect of the learning environment.

At Moodle, we are proud of the trust placed in us by educators, governments, businesses, and communities across the globe. We are committed to safeguarding that trust every day, and to shaping a future where open, secure, and flexible learning environments are accessible to all.

Security is not an afterthought - it is our foundation.

Appendix

To support organisations in building and maintaining secure Moodle environments, the following resources offer further guidance, best practices, and technical references.

- **Authentication** - The process of verifying the identity of a user or system.
- **Bugcrowd** - A third-party platform that connects organisations with a global community of security researchers to identify and report vulnerabilities.
- **Common Vulnerabilities and Exposures (CVE)** - A public identifier assigned to a confirmed security vulnerability to help track and share information across platforms and organisations.
- **Encryption -** The method of converting information into a secure format that cannot be easily understood without authorised access.
- **Long-Term Support (LTS) -** A type of software release that receives security updates and critical fixes for an extended period, offering greater stability over time.
- **MFA (Multi-Factor Authentication)** - A security measure that requires users to verify their identity with two or more methods, such as a password and a physical token.
- **Password peppers** - Random secret values added to passwords, alongside salts, to strengthen protection against brute-force and dictionary attacks.
- **Patch management** - The process of distributing and applying updates to software to fix vulnerabilities.
- **Penetration testing** - Simulated cyberattacks conducted by security professionals to identify and address vulnerabilities before they can be exploited.
- **Read-once tokens** - Security tokens designed to be valid for a single use only, preventing replay attacks and protecting web service interactions.

- **Responsible disclosure** - A security practice where vulnerabilities are reported privately to developers and fixed before the details are made public.
- **Security overview report** - A Moodle LMS tool that summarises key security settings and identifies areas for improvement on a site.
- **SOC 2 Type 2 and SOC 3** - Independent certifications that verify an organisation's operational security, confidentiality, and data protection practices over a period of time.
- **Trusted content** - A Moodle LMS permission setting that allows trusted users to post content without it being automatically cleaned or filtered for security risks.
- **Triage (in security context)** - The process of reviewing, validating, and prioritising reported security issues based on their severity and potential impact.
- **Vulnerability Disclosure Programme (VDP)** - A structured process that allows security researchers and users to report vulnerabilities securely and confidentially.

Moodle Security Resources

- Moodle Security Recommendations
- Moodle Security Overview Report
- Moodle Development: Security by Design
- Moodle Vulnerability Disclosure Programme

External Resources

- OWASP Top Ten
- Common Weakness Enumeration (CWE)
- CIS Critical Security Controls

Ready to take the next step?

Whether you need help hosting your site securely, upgrading to a supported version, or managing security best practices, a Moodle Certified Partner or Service Provider can help.

Get expert guidance tailored to your organisation's needs - so you can focus on delivering secure, effective learning experiences.

Get in touch today