CYBERGYM's Secure Code Review Service

Uncover hidden vulnerabilities in your source code

A secure code review uncovers hidden vulnerabilities and design flaws in your application's code, and verifies that key security controls are implemented. Using a combination of scanning tools and manual review, our Red Team of hacking experts - themselves former members of government security agencies – are able to detect insecure coding practices, backdoors, injection flaws, cross-site scripting flaws, insecure handling of external resources, weak cryptography, and more.

Process

In the course of our Secure Code Review Service, we will carry out the following stages.

Reconnaissance

To gain an insight into how your application is intended to work, our Red Team carries out an inspection of it in action. We also conduct a brief overview of the codebase's structure and any libraries being used, to help our Red Team to get started.

Threat assessment

Conducting a threat assessment of applications identified as critical enables us to better understand the application's architecture. The threats identified will then form the list of vulnerabilities that we will prioritize during the code review itself.

Automated code review

Automated tools are widely used in analyzing large codebases. During the automation stage, we use different commercial/open-source tools to compare the codebases of your application against millions of lines of code, enhancing the throughput of the code review process.

Manual code review

Certain critical security controls - including access control, encryption, data protection, logging, and back-end system communications and usage - can only be verified by a manual code review. A manual review is also important in tracing the attack surface of an application, and identifying how the data flows from its sources to its sinks. Going through the code line by line gives us better clarity of the code, and helps remove false positives.

Confirmation & POC

After the automated and manual reviews have been completed, we create a thorough checklist of the possible risks that have been discovered, and the possible fixes that can be used to patch a particular vulnerability in the codebase.

Reporting

When all the above steps have been completed, we create a report of all our findings – including every issue in the code and the relevant patching solution – and present it in a clear and concise format. The issues raised and our recommendations are then discussed between your development team and the CYBERGYM Red Team.

What you gain

1. An accurate picture of your application's cybersecurity
2. A comprehensive report outlining any weakness in your code, security exposure points, root causes and high impact recommendations
3. A security roadmap and action plan, detailing how to resolve issues that have been identified
4. Enhanced protection of your business intelligence, data and IT systems, brand and reputation

CONTACT INFORMATION

Sales@cybergym.com | www.cybergym.com