

# HackerOne Code Security Audit

Leverage HackerOne's network of seasoned engineers to uncover and address weaknesses in your source code

## Secure Your Codebase with Expert Human-led Audits

Keeping your codebase secure is an ongoing challenge as attack surfaces expand and vulnerabilities grow more complex. **HackerOne Code Security Audit (CSA)** addresses this challenge by leveraging a network of 600+ vetted senior software engineers to conduct thorough human code audits.

CSA, also known in the industry as **Source Code Audit**, **Code-assisted (Whitebox) Pentesting**, or **Secure Code Review**, refers to the critical process of expert source code analysis for identifying security vulnerabilities. Regardless of the term used, the core concept remains the same: a detailed examination of your codebase to uncover security blind spots.

These in-depth code reviews surpass the capabilities of automated SAST tools, which are limited to predefined patterns and often generate false positives. CSA's proactive approach identifies and addresses deep-rooted design and implementation issues early in development, detecting vulnerabilities that automated tools might overlook. By establishing a strong security foundation at the code level, CSA significantly reduces costs compared to identifying and fixing issues post-release.

## Use Cases

### Legacy Programs

Review and secure large, monolithic, and legacy codebases to uncover hidden vulnerabilities.

### Release with Confidence

Identify and fix security vulnerabilities before major releases or cloud migrations.

### Compliance Assurance

Adhere to regulatory standards such as NIST, FS-ISAC, FISMA and PCI DSS.

### Mergers & Acquisitions (M&A)

Conduct detailed code reviews to assess and improve the security of newly acquired software assets.

### Supercharge Pentesting

Gain an immediate, comprehensive view of your codebase's security posture to enhance the quality of your security assessments.



Code Security Audit is the ideal solution for a comprehensive code review that levels the playing field on vulnerabilities. I don't want to deal with a dump of 1,000 potential issues and then have to figure out which ones are legitimate risks— that's a nightmare. With CSA, I get a point-in-time analysis that identifies real vulnerabilities and provides expert remediation advice, including specific fixes and broader security themes.

*Software Engineering Director of an Automotive Company*



## Key Advantages



### Expert Reviewer Network

Access the world's largest network of over 600 reviewers with extensive AppSec and engineering experience, all protected by strict NDAs and IP safeguards.



### Agile Delivery

Initiate CSA engagements within four business days and benefit from real-time feedback and collaboration with reviewers for rapid vulnerability resolution.



### Dedicated Technical Support

Leverage HackerOne's automation engine and technical engagement managers (TEMs) to fast-track the review process and prioritize high-risk areas of your codebase.



### Enhanced Access Control

Benefit from granular access control and identity governance with enforced least privilege access, comprehensive audit logs, and streamlined SSO for developers and security teams.



### Seamless Integrations

- Integrate your code with major supply chain management platforms like GitHub, GitLab, Azure DevOps, and Bitbucket.
- Efficiently manage code review activities, communicate findings, and prioritize responses through the HackerOne platform.



### Remediation Guidance

- Receive clear vulnerability explanations and detailed, actionable remediation guidance from reviewers.
- Empower both technical and non-technical team members to accurately implement fixes.



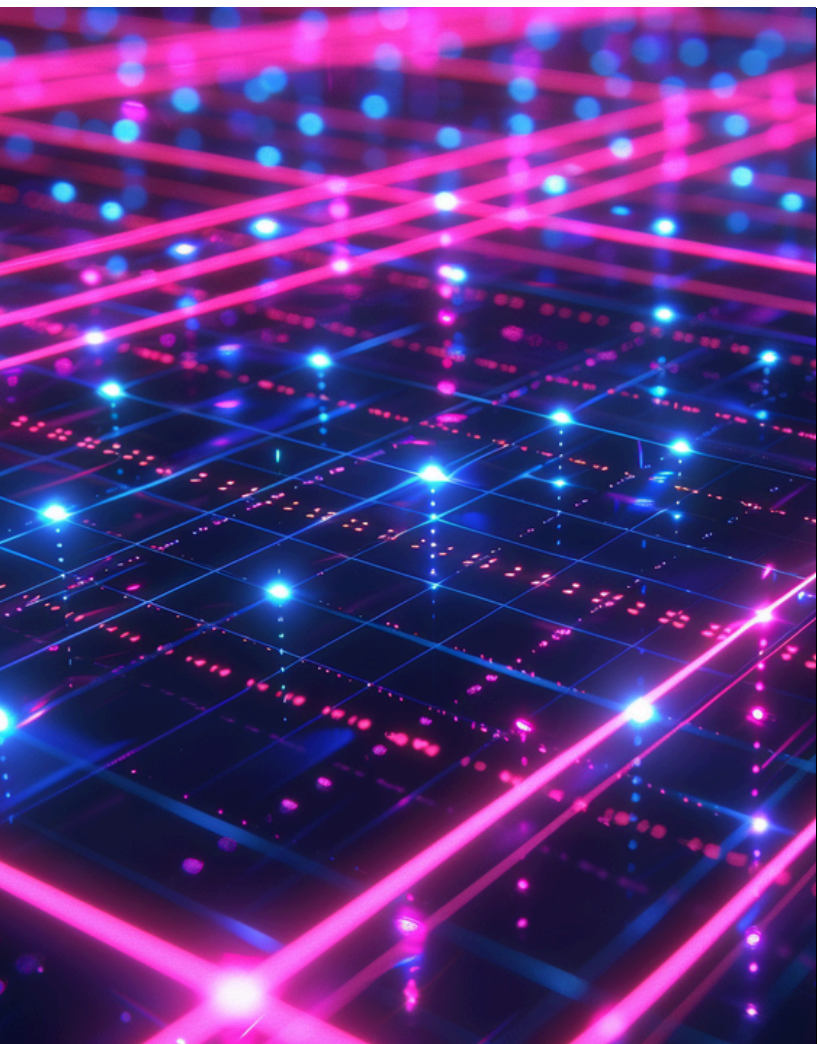
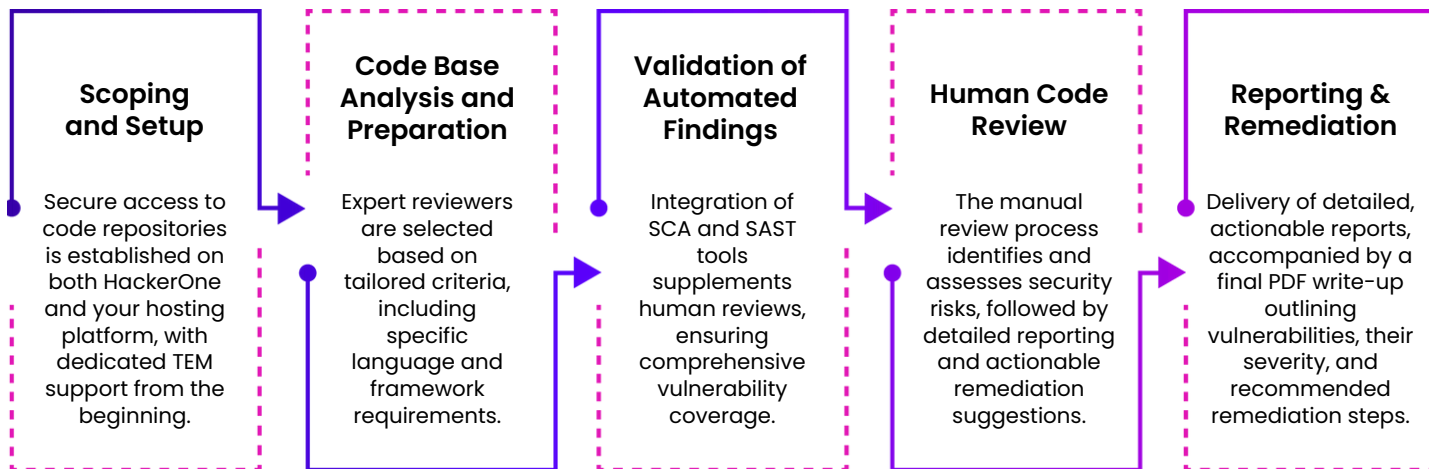
This was our first time using HackerOne Code Security Audit. We didn't know what to expect, but it turned out to be everything we had hoped for. The analysts' feedback was specific, well-documented, and security-focused. The communication between all parties was excellent and timely. The Fidlar team's security expertise has grown during this experience with HackerOne.

**Kimberly Albrecht,**  
Software Developer at Fidlar Technologies



# Streamlined Code Security Audits

Our CSA engagement process closely follows [OWASP's Code Review Guide](#) to provide broad and in-depth coverage of your source code. Throughout the process, your dedicated TEM ensures that reviewers stay on track by offering guidance on timelines, providing necessary context and code, and monitoring the program.



Our team is dedicated to delivering secure code, but it's challenging to catch every potential vulnerability. The Code Security Audit provided a fresh perspective and uncovered specific issues that our internal auditing processes didn't detect on GitHub. The CSA was a valuable learning experience, helping us enhance our team's skills and strengthen our secure coding practices moving forward.



**Andrew Winter,**  
Chief Technology and Product Officer at Zaiko

# Examples of Reviewed Code and CSA Coverage

SOLUTION BRIEF



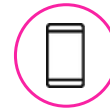
## Web

Perform deep code reviews to identify vulnerabilities from both front-end and back-end components.



## Cloud

Provide thorough reviews for cloud-hosted applications, focusing on common misconfigurations and security practices for AWS, Azure, and GCP.



## Mobile (iOS/Android)

Conduct code reviews that include checks for both iOS and Android platforms.



## Infrastructure as Code & Server

Examine codebases involving Terraform, Jenkins, Docker, Kubernetes, Ansible, Cloudformation, GitlabCI, and Github Actions. Target banks and other financial institutions relying heavily on robust server applications.



## Desktop

Audit security for desktop application code, particularly for game developers and software utilizing complex logic. Support for languages like C, C++, C#, Java, and others typically used in desktop app development.



## Programming Languages

Get extensive coverage across a variety of programming languages including JavaScript, TypeScript, Elixir, Ruby, Golang, and more.



## Frameworks

Review applications built on multiple popular frameworks such as React, .NET, Django, Angular, and Rails.



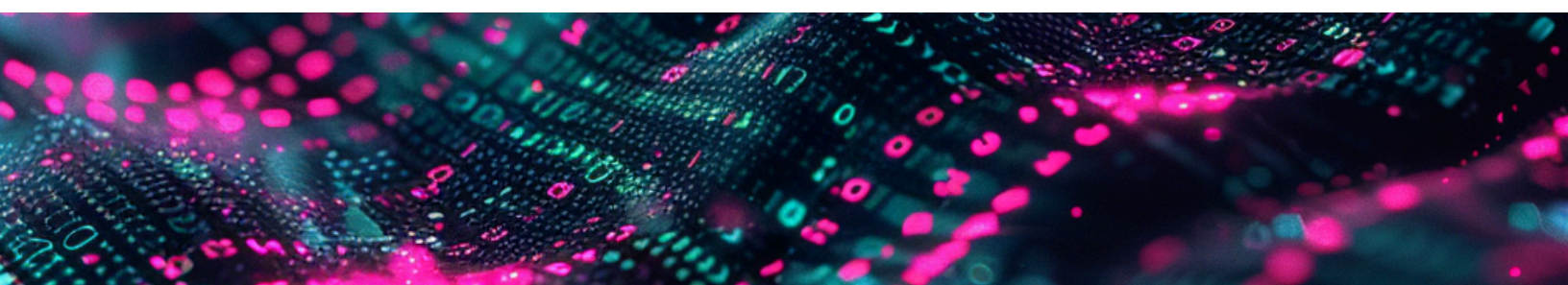
## Crypto Industry

Review code for digital asset custodians, Web 3.0 wallets and SDKs, and custom blockchain architectures. Assess Lightning Network deployments, key sharding logic, and cryptocurrency protocols.



## Online Streaming and Automotive Manufacturing

Review code focusing on Over-the-Air (OTA) updates. Include assessments for both the supporting infrastructure and application layers.



**Reach out** to our specialists today to discover how HackerOne Code Security Audit can secure your codebase from the foundation up, at the speed of your development pace.