Reliance acsn

Penetration Testing: Code Review

Find and remediate application coding flaws – before they are exploited

Your organisation - and the applications that it develops – is deeply vulnerable to attacks that exploit coding flaws and errors. The Open Web Application Security Project (OWASP) lists multiple such errors in its 2020 top vulnerabilities list, each of which is potentially a financial, operational, reputational or even legal risk if you fail to eradicate it from your application source code before release or deployment.

Industry sources recently report that some 96% of business applications contain vulnerabilities, and that the volume of attacks against them has increased. Clearly, the problem is both widespread and growing, driven also by the ever-increasing use of applications by organisations and their supply chain.

Reliance acsn's Code Review verifies the security of your application source code and finds security flaws that could leave it vulnerable to attack. We investigate web, mobile, IoT and desktop applications and help you take action to prevent damaging and costly post-release/post-deployment breaches.

We review existing code but we also assess code as it is produced, across the Software Development Lifecycle (SDLC), to secure your applications from the ground up, today and in the future.

What Code Review delivers

Reliance acsn's Code Review combines long-established secure coding expertise from our independent vulnerability research department, highly automated technology, and custom-built tooling, delivered both as a standalone service and as part of a wider range of Penetration Testing offerings.

A review identifies even the most complex, organisation-specific vulnerabilities or errors, and dynamically validates them against current, running copies of the applications.

Proven, multidisciplinary code expertise

Our researchers have identified and published security weaknesses in high-profile code bases including the Linux kernel, Android, Java, Microsoft .NET, Mozilla Firefox, Edge, Chrome and many more.

Extensive security mechanism coverage

Authentication, authorisation, session management, data validation, error handling, logging, encryption, plus organisation-specific requirements.

OWASP-aligned vulnerability review

Covering injection, broken access control, security misconfigurations, XML external entities, cross-site scripting, vulnerable components, etc.

De-risked growth

As your organisation grows through mergers and acquisitions, we review the acquired products' source code to reduce the business risks of unidentified security issues.

How our approach benefits you

At Reliance acsn, before Code Review even gets underway, we first work closely with you to fully understand the business imperatives of the applications you develop.

This enables us to tailor our activities not only to secure the code that underlies them, but to secure the brand value, revenue and productivity they deliver to your business.

1 We focus on the big issues

With coding error attacks recently reported to have grown by 60%, Coding Review is at the top of our agenda.

2 We prove what we say

We test the identified coding errors under both simulated and dynamic, real-world conditions, to validate their risk.

3 We tailor our testing to you

We know every organisation is different, so we customise our code review around what your applications and assets offer to an attacker – not anybody else's.

4 We speak your experts' language

Our Code Review team know coders because they are coders. Dialogue between experts gets security done quicker, better.

5 We propose clear next steps

Focused on the realities of your business, and help you through them, in language all your stakeholders can understand.

6 We're there as long as you need us

From discrete review of new or existing application code, to ongoing review of every application you produce, we're on hand.

About Reliance acsn

Across five continents, enterprise and government clients depend on Reliance acsn to defend them against cyber threats like nobody else can.

Our managed security and consultancy services support organisations throughout the challenges of assurance, awareness, detection, response and prevention, 24 x 7, and focus on business risk – securing not just assets and data, but revenues, too.

- Reliance acsn's history goes back to 2003, with the founding of global cyber security specialist ACSN.
- In 2016, a merger created Reliance acsn in London, UK, to deliver real-time Managed Detection and Response (MDR)
- We've helped scores of the world's top brands plan, deploy and manage robust security solutions, in banking, telecoms, retail, government and insurance.
- Our people are accredited across all the major standards in IT security – including PCI, ISO27001, G-Cloud, CISSP, CREST, and many more – and accredited to support virtually any technology you have in place or are planning to procure.