

InfoSight's Mobile, API & Code Review

Overview - The Challenge

Applications have become a tremendous target for cybercriminals because of their heightened value of stored information. Weaknesses and flaws in an application's source code can result in exploit compromising confidential data.

Additionally, so much data is shared with APIs, they have also become a large source of compromise that is gaining momentum. This also includes not just traditional applications but also mobile apps as well.

How We Solve It

InfoSight's Code Reviews, which can include API & Mobile Testing Services assist in identifying any underlying security issues with the application by providing a comprehensive review of Application code and API's to identify vulnerabilities and ensure your applications meet the latest security best practice standards. InfoSight's testing consists of Static Analysis, Dynamic Analysis and Penetration Testing. Once these reviews are complete, we provide you with a high level report on our findings.

The Outcome


Recommendations for remedial action will be made at the conclusion of the testing procedure, with the option of additional security testing following post-change. Following the reports, we suggest maintaining a change management log of all code changes and/or architectural changes. This change management log must include, at minimum, code check-in/check-out log, code change diff files, administrative or management code acceptance evidence, evidence of regression testing, or impact analysis performed for each code change, and difference files or documentation showing code changes in an A/B fashion. InfoSight can provide follow up services upon further discussion with your IT team.


Security Mechanisms


- Authentication
- Authorization
- Session Management
- Data Validation
- Error Handling
- Logging
- Encryption


InfoSight's Mobile, API & Code Review

Comprehensive scanning will consist of four stages:

- 

Injection: An injection code technique will be used to attack web applications, in which malicious statements are inserted into an entry field for execution. Injection is mostly known as an attack vector for websites and APIs but can be used to attack any type of applications.
- 

Gathering: Information Gathering is the most critical step of an application security test. By using public tools (search engines), scanners, sending simple HTTP requests, or specially crafted requests, it is possible to force the application to leak information, e.g., disclosing error messages or revealing the versions and technologies used.
- 

Server: Server security is the protection of information assets that can be accessed on and from a server. Server security is important for any organization that has a public or private API connected to the Internet. It requires a layered defense and is especially important for organizations with customer-facing APIs.
- 

Usage: Usage of weak authentication methods makes it easy for an attacker to intercept credentials, replay them to other hosts, and trick users into providing the credentials to the wrong location.

Why InfoSight

- 24x7x365 US-Based SOC
- SOC 2 Certified
- 25+ years of proven outcomes
- Offering full threat lifecycle services from Detection and Response to Mitigation and Remediation
- Flexible pricing models that can be 24x7, 8x5, or off-peak 7pm to 7am only coverage
- Solutions are Regulatory Compliance driven (GLBA, PCI, HIPAA, NERC, AWWA, etc.)
- Offering Services for the Data Center, Cloud and Hybrid environments
- Certified Experts (CISSP, CISA, CEH, OSCP, AWS, AWWA, etc.)

