

SECURITY CODE REVIEW

A person is shown from the chest up, working on a laptop. The image has a strong blue color cast. Overlaid on the image are various digital elements: binary code (0s and 1s) at the bottom, and snippets of code (like 'struct', 'void', 'if', 'while') floating in the background. The person's hands are on the laptop keyboard.

COMSEC

ARE YOU SURE YOU KNOW WHAT IS HIDDEN IN YOUR SYSTEM'S SOURCE CODE?

What is Security Code Review?

"Security code review is the process of auditing the source code for an application to verify that the proper security controls are present, that they work as intended, and that they have been invoked in all the right places", OWASP

Core Value

It is commonly known that designing and implementing a secure application is a difficult task. Programmers rarely have the required expertise or the time to invest in system security. The result is that applications have many vulnerabilities, with severe implications for the system's security. Such programming vulnerabilities may enable legitimate system users or hackers to perform unauthorized operations.

By exploiting such security vulnerabilities, whether internally or externally, malicious entities can cause security breaches and damage information availability, integrity and confidentiality. When you perform a Security Code Review you can identify potential threats embedded at the system code level and mitigate them in the early system development stages.

❗ Clients Problems

- 1 | Developers create three vulnerabilities in every 10,000 lines of code they write. This means that there will be 15 vulnerabilities in a small system of 50,000 lines of code, and more than 300 vulnerabilities in a large system of 1 million lines of code!!!
- 2 | In most cases security testing is carried out after development has been completed. Mitigation at this stage is expensive and in some cases delays the target date for promoting the system/version to the production environment.
- 3 | In huge systems there may be hundreds of vulnerabilities. In most cases Penetration Testing will reveal only a small sample of each type of vulnerability. For example, the Penetration Testing Report will indicate a vulnerability such as XSS. However Penetration Testing will never detect all instances of this vulnerability in the code and their exact location, hindering the ability to fix them.

✅ Comsec's Solutions

The Security Code Review enables you to detect vulnerabilities that would take months to find, if at all, with Penetration Testing. Using automated tools, we can scan huge amounts of code. Furthermore, the security code review can also be performed manually and at the early stages before the system is deployed to the production environment, even if we only have partial code or non-compiling code. We can find the exact location of the vulnerability in the source code and pinpoint the specific line of code causing the problem.

Benefits

Professionalism

Our dedicated team specializes in and performs only security code review projects.

Experience

We scan millions of lines of code every month and have 20 years of experience performing security code reviews.

Responsiveness

We can start work on very short notice.

Efficiency

Our methodology is based on many years of proven experience and enables us to conduct an efficient audit, saving you time and money.

End-to-end service

As your partners we are part of the process.

- We can advise when to perform the review.
- We can advise about the scope of the review.
- We will explain the vulnerabilities that we detected.
- We can assist development programmers and help mitigate the
- vulnerabilities found in the source code.



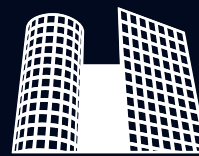
Comsec UK

33rd floor, Euston Tower
286 Euston Road
London, NW1 3DP, England
Tel: +44 (0) 2034638727
info@comsecglobal.com



Comsec BV

Hogehilweg 4
1101 CC Amsterdam
The Netherlands
Tel: +31 (0) 102881010
info@comsecglobal.com



Comsec HQ

Yegia Kapayim St. 21D
P.O.Box 3474, Petach-Tikva
Israel 49130
Tel: +972 (0) 39234646
info@comsecglobal.com