WEB APPLICATION SECURITY TESTING

COMSEC

What is Web Application Security Testing?

Comsec offers Web Application Security Testing on multiple technology stacks, to assist the organization to identify application vulnerabilities which could lead to data disclosure or tampering and simulate real-life attack scenarios against its products and internal/external facing applications.

We work with the client to identify the key risks to which the application exposes the organization, potential scenarios by which these risks could occur, demonstrate whether these scenarios are possible or not and provide assistance in mitigating the issue.

The final report will include a high-level executive summary, an explanation of our methodology as well as detailed technical documentation of the findings. Every vulnerability is rated according to the likelihood of exploitation and the impact which is caused. The report will also contain mitigation recommendations per vulnerability to improve the component's security level.
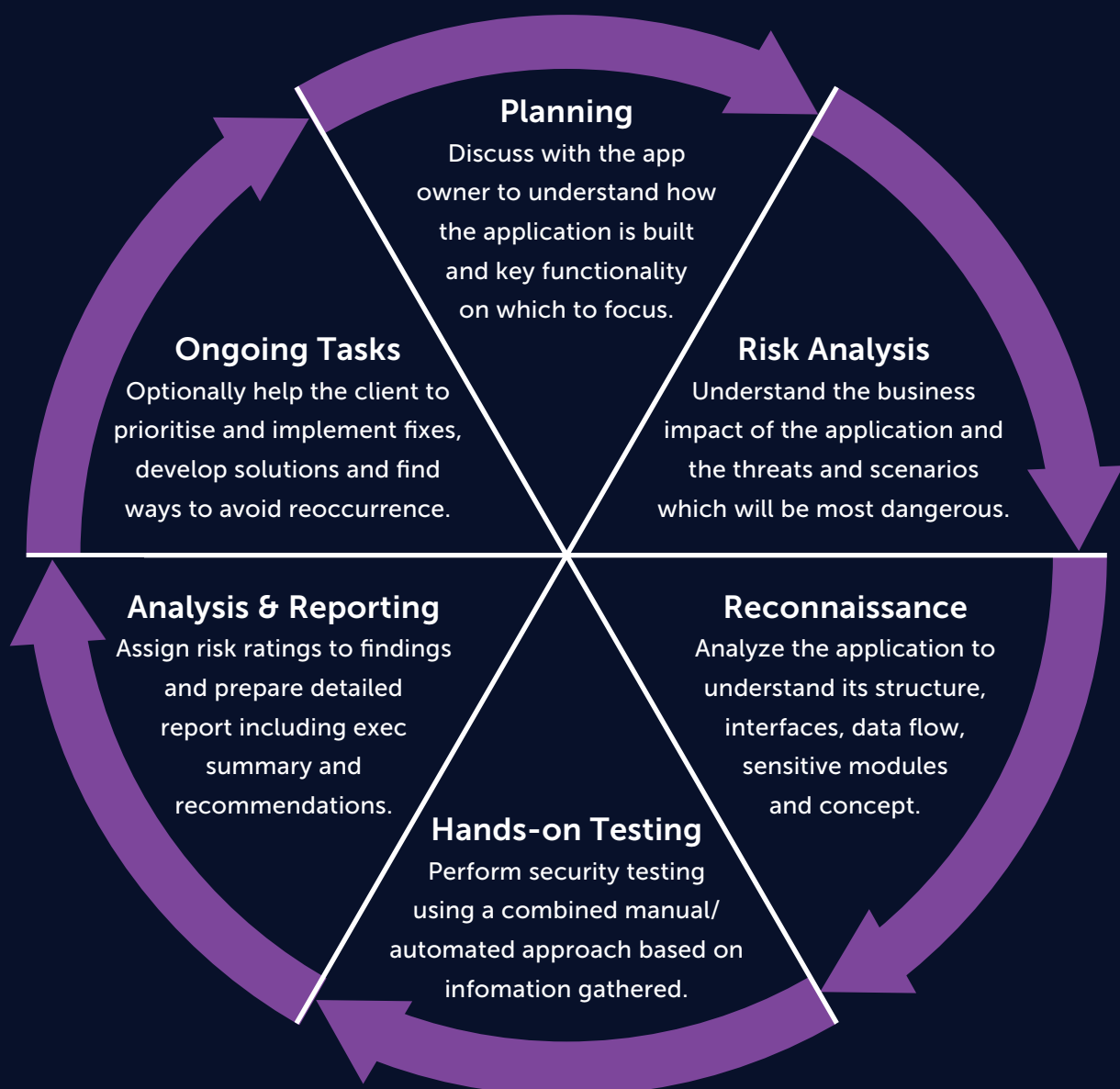
⚠ Clients Problems

We are seeing more and more organizations storing and relying on sensitive data and at the same time data privacy and protection regulations are becoming more widespread and strict. This means that the reputational and regulatory cost of a data breach should be a key concern to any organization which stores or works with sensitive data.

Application Security is a particular area where we are seeing a rapid increase in new vulnerabilities alongside a significant shortage of skilled and experienced practitioners. Most organizations do not have the resources to discover and address these vulnerabilities which can endanger not just data stored by the specific application but other data assets on the same network.

COMSEC

Comsec's Web Application Security Testing

Comsec's Application Security Testing service includes testing web applications, mobile applications and thick client/client-server applications for vulnerabilities which could lead to data/network compromise or loss of availability. The team uses a similar approach, as shown below, in all cases although the specific tests will be customized based on the type of application being tested.

Planning
Discuss with the app owner to understand how the application is built and key functionality on which to focus.

Risk Analysis
Understand the business impact of the application and the threats and scenarios which will be most dangerous.

Reconnaissance
Analyze the application to understand its structure, interfaces, data flow, sensitive modules and concept.

Hands-on Testing
Perform security testing using a combined manual/automated approach based on infomation gathered.

Analysis & Reporting
Assign risk ratings to findings and prepare detailed report including exec summary and recommendations.

Ongoing Tasks
Optionally help the client to prioritise and implement fixes, develop solutions and find ways to avoid reoccurrence.

COMSEC

Why Comsec

One of Comsec's most unique values is that the security test is tailor-made to the client's product. The team focuses on identifying the most critical risks and assets and ensuring they are considered throughout the testing phase. The team will always try to create a unique Proof of Concept exploit per vulnerability (whether it is a common vulnerability or not) in order to show the real business impact as an outcome.

Additional key points:

- UnderstandinExperience with a wide range of web frameworks from monolithic, server-side middleware systems to JavaScript-heavy Single Page Applications.

- Emphasis on a high standard of reporting with every report going through at least one separate quality review by another experienced consultant.

- Standardized testing plans based on standards such as the OWASP Testing Guide but customized to our needs to ensure that nothing is missed whilst allowing space for application specific tests.

- Careful consideration of the real risk with the finding risk rating taking into account aggravating and mitigating factors.

- We don't want to deliver a report and leave, we want to support the client with how, where and when the fixes should be made and to ensure that they get implemented correctly.
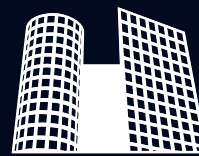
COMSEC

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

COMSEC