

Web Application Security

New applications are increasingly more accessible and usable with web technologies. Web Applications provide the end users with many advantages over traditional applications. However, the accessibility and flexibility offered by this technology can also be abused by malicious parties.

At EnableSecurity we have assessed the security of various Web Applications and web technology and constantly research into the area.

These are some of the services we offer:

- In-depth analysis of the current security posture of a Web Application
- Recommendations on how to reduce exposure to any identified vulnerabilities
- Step by step instructions and easy to use tools to reproduce any security flaws found
- Tests cover both standard vulnerabilities such as SQL injection and Cross Site Scripting as well as logic problems such as backdoors and inconsistent access control

Wireless Security Assessment

There are situations where wireless is a solution to many problems with traditional networking. However, due to its nature, wireless networks are very hard to secure and can expose sensitive systems to attack from external attackers.

We can help you mitigate the risk associated with the use of wireless technologies and as well as demonstrate any vulnerabilities identified by making use of our equipment and security tools.

Security Research and Design

At EnableSecurity we build our own tools or customize existing ones to fit our needs. We also do our own research on public security flaws and solutions, as well as work on new unpublished research.

Some projects that we have recently been working on:

- Session Hijack proof of concept tools
- VoIP security tools
- Custom password auditing tools
- Custom built fuzzing software to automate certain security tests

We offer the following:

- Development of custom security solutions
- Research into security vulnerabilities and solutions

Application Security Testing

Similar to Web Applications, server and client applications prove to be excellent solutions for many business needs. Applications are known to have many possible pitfalls - from file format parser vulnerabilities to RPC vulnerabilities to incorrect implementation of cryptographic solutions.

What we provide:

- Reverse engineering of applications and network protocols to identify possible flaws
- Source code auditing
- Application Fuzzing
- Analysis of the overall system from a security standpoint

Network Security Assessment

On many corporate networks the infrastructure is constantly changing. While such changes are a necessary part of conducting business, they can very easily introduce security flaws and create situations that can raise a security concern.

We can help you better the security of your network by providing the following services:

- Internal Penetration Testing - simulating an internal attack by a disgruntled employee or a malware infected workstation
- External Penetration Testing - simulating an external performing a targeted attack
- Vulnerability Assessment - identification of potential security flaws within the network by looking at the overall network as well as at each component that makes up the network
- Mitigate security vulnerabilities identified and where possible, instructions on how to fix the security flaws reported.

Incident Handling

It is only a matter of time until a security incident occurs. It is therefore important to have a reliable way to identify the security issues exploited and mitigate.

How can we help?

- Online and offline forensics
- Investigation of potential security breaches or fraudulent activities, including forensic investigation