Security Analysis of Software Source Code

Security Assessment Services

Version 1.3
22 April 2020
About Us

We are a team of cybersecurity professionals from Ukraine. Our consulting services include the assessment and implementation of information security, as well as training and workshops.

We cover all stages of the system life cycle – from planning and engineering to security management and incident investigations. Our experience includes both security governance and deep technical skills, including software reverse engineering, 0-day vulnerability research, manual security review of source code, Red Team exercises, etc.

H-X Cyber Security Consulting Services
We have wide experience and competence in corporate security:

- **Security Assessment**: IT audits, information security audits, security review of source code, audit of smart contracts.

- **Managed compliance** with GDPR, ISO 27001, PCI DSS, HIPAA, ITIL, ISF, NIST, COBIT, etc.


- **Security Operations Center (SOC)** Implementation and SOC as a Service, including: technical vulnerability management, security event monitoring, security incident response and investigations, etc.

- **Enterprise Risk Management** and IT-related Risk Management.

- **Business Continuity Management** and Disaster Recovery Planning.

- Physical security and other security areas.
Application Security Services

Our Application Security Services include customizable parts: Secure Software Development Lifecycle (SDLC) Management for your company, Product Security Management (including Security DevOps) for your products and solutions, and Secure SDLC training for your personnel.

These service components are usually combined. When you and we define your needs and analyze your products, we choose how many work hours of our specialists you need for each component.

Security Analysis of Source Code can be a part of Product Security Management.
Security Analysis of Source Code – Objectives

The objective of this analysis is security assessment of the source code of your systems or applications: checking integrity and consistency of your code, secure coding principles, finding unsafe or deprecated functions, hidden logical bombs and traps, backdoors, undocumented features, non-optimal coding practices and OWASP top 10 vulnerabilities:

• **A1:2017**-Injection
• **A2:2017**-Broken Authentication
• **A3:2017**-Sensitive Data Exposure
• **A4:2017**-XML External Entities (XXE)
• **A5:2017**-Broken Access Control
• **A6:2017**-Security Misconfiguration
• **A7:2017**-Cross-Site Scripting (XSS)
• **A8:2017**-Insecure Deserialization
• **A9:2017**-Using Components with Known Vulnerabilities
• **A10:2017**-Insufficient Logging&Monitoring
Security Analysis of Source Code – Methods and Results

To achieve the objectives, the auditors use two methods:

• SAST (Static Application Security Testing), which allows analyzing source code for known vulnerabilities using automated tools.

• Manual source code review and analysis, in order to reveal unsafe and non-optimal coding practices, hidden logical bombs and traps, backdoors and undocumented features.

Report on Security Analysis of Source Code includes:

• Executive summary

• Identified technical and functional vulnerabilities

• Modeling of attack vectors, proof of concept and exploitation of vulnerabilities

• Risk assessment

• Prioritized list of recommendations to mitigate identified weaknesses

https://h-xtech.com
Security Analysis of Source Code – Languages

We support the following languages and technologies:

- .Net/ASP.Net
- Java EE (JBoss, Tomcat, etc.)
- Java Android
- Objective-C/Swift iOS/MacOS
- PHP
- Javascript
- Python
- C/C++/Assembler
- Solidity
- Golang
- Lua
- your language or platform

- Containers: Docker stack (Compose, Swarm, Machine, Registry), GCE Kubernetes, AWS ECS, Terraform, Vault
- Frameworks and technologies: NodeJS, Socket.IO, WebRTC, PhantomJS, YF framework, Yii, Laravel, Symfony components
- Frontend: Angular 2, AngularJS, ReactJS, JQuery, Less/Sass, Grunt/Gulp/Webpack, Bootstrap 3/4, etc.
- Mobile development (hybrid): Cordova, Ionic framework 1-4, NativeScript, ReactNative
- Desktop development (hybrid): Electron, NWJS, ReactNative
- RDBMS: MySQL / MariaDB / Percona, PostgreSQL, Oracle
- NoSQL: Redis, CouchBase, MongoDB, Cassandra, GCloud Datastorage
- Queues: RabbitMQ, Kafka, Redis, Beanstackd, AWS SQS
- Automation / CI / CD: Jenkins, GitlabCI, TravisCI, CircleCI, Ansible, Bash scripting
- Different virtualization technologies, OSes, SCM, web / proxy / mail servers, cloud and dedicated hosting services, monitoring and backup technologies, blockchain technologies, payment gateways, etc.
Security Analysis of Source Code – Pricing

Project price and duration can be defined using the formula, the table or the diagram:

\[
\text{Project price} = \left(\frac{\text{lines of code}}{1000}\right)^{0.6} \times 210 + 2650 \text{ USD}
\]

\[
\text{Project duration} = \left(\frac{\text{lines of code}}{1000}\right)^{0.6} \times 0.84 + 11 \text{ days}
\]

<table>
<thead>
<tr>
<th>Thousand lines</th>
<th>Days</th>
<th>Price, USD</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>14</td>
<td>3486</td>
</tr>
<tr>
<td>50</td>
<td>20</td>
<td>4846</td>
</tr>
<tr>
<td>100</td>
<td>24</td>
<td>5978</td>
</tr>
<tr>
<td>200</td>
<td>31</td>
<td>7695</td>
</tr>
<tr>
<td>500</td>
<td>46</td>
<td>11392</td>
</tr>
<tr>
<td>1000</td>
<td>64</td>
<td>15900</td>
</tr>
<tr>
<td>1500</td>
<td>79</td>
<td>19550</td>
</tr>
<tr>
<td>2000</td>
<td>91</td>
<td>22733</td>
</tr>
</tbody>
</table>
Why Us?

The highest qualification, flexibility and reliability are our main distinctions:

Experience in information security. We work in cyber security since 2001, in different sectors. Late in 2015, we initiated the H-X project.

International security certifications. We earned and keep up-to-date internationally recognized security certifications (CISSP, CEH, OSCP, CLPTP, etc.).

Absolute legitimacy and confidentiality. The employees of H-X technologies strictly adhere to laws, regulations, corporate Code of Ethics and Penetration Testing Code of Ethics. We are ethical, white-hat hackers. Our specialists sign your commitment forms personally, just like your employees.

The highest customization and flexibility. Our approach allows the customer to understand more accurately what they pay for. This is our know-how and our main distinction from competitors.

The highest quality. H-X uses modern comprehensive methodologies and tools. In every project, we develop suggestions for continuous improvement and track changes in the security of our customers over the years.
Our certificates

• (ISC)2: Certified Information Systems Security Professional (CISSP)
• Offensive Security: Offensive Security Certified Professional (OSCP)
• EC Council: Certified Ethical Hacker (CEH)
• ISACA: Certified Information Security Auditor (CISA), Certified Information Security Manager (CISM)
• PCI SSC: Payment Card Industry Professional (PCIP)
• SANS: Security-560. Training course at SANS, USA
• PECB: Certified Lead Pen Test Professional (CLPTP)
• Other certificates
CUSTOMER REFERENCES

The H-X team has conducted a detailed project planning to assess the security of our infrastructure. They have showed a creative approach, and have properly implemented the security assessment plan. The security assessment has provided valuable information on priorities of security enhancements for our company, including strategic objectives and tactical activities.

Dmytro Dniprovskyi, Information Security Manager, Intercracy Group

We were facing serious challenges related to our customers' requirements for formal compliance with international and industry information security standards. The H-X team very quickly helped us to evaluate and fill the current organizational and technical gaps, and they continue to help.

Artem Savotin, Managing Director, Ameria Ukraine

The H-X team have completed a technical security assessment of one of our products, and we've been surprised by the high quality of the results. H-X specialists have provided a detailed consultation on secure software development. They've helped to improve the quality of our development and testing processes.

Viktoriia Pogrebniak, IT Manager, FluentPro
Thank you for your attention!

Please ask your questions, try our free automated security assessment, vulnerability scanning or penetration test at https://h-xtech.com/services or call us +380958860891