Combined C/C++, Java and Web Application Security

Training Calendar

<table>
<thead>
<tr>
<th>Date</th>
<th>Training Time</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>15 July 2019</td>
<td>4 Days</td>
<td>Bilginç IT Academy</td>
</tr>
<tr>
<td>09 December 2019</td>
<td>4 Days</td>
<td>Bilginç IT Academy</td>
</tr>
</tbody>
</table>

Training Details

- **Training Time**: 4 Days
- **Capacity**: 12
- **Prerequisites**: There are no prerequisites for this course.

About Training

To serve in the best way heterogeneous development groups that are using various platforms simultaneously during their everyday work, we have merged various topics into a combined course that presents diverse secure coding subjects in didactic manner on a single training event. This course combines C/C++ and Java platform security to provide an extensive, cross-platform secure coding expertise.

Concerning C/C++, common security vulnerabilities are discussed, backed by practical exercises about the attacking methods that exploit these vulnerabilities, with the focus on the mitigation techniques that can be applied to prevent the occurrences of these dangerous bugs, detect them before market launch.

Security components and service of Java are discussed by presenting the different APIs and tools through a number of practical exercises where participants can gain hands-on experience in using...
them. The course also covers security issues of web services and the related Java services that can be applied to prevent the most aching threats of the Internet based services. Finally, web- and Java-related security vulnerabilities are demonstrated by easy-to-understand exercises, which not only show the root cause of the problems, but also demonstrate the attack methods along with the recommended mitigation and coding techniques in order to avoid the associated security problems.

What You'll Learn

- Understand basic concepts of security, IT security and secure coding
- Learn Web vulnerabilities beyond OWASP Top Ten and know how to avoid them
- Learn about XML security
- Learn client-side vulnerabilities and secure coding practices
- Learn to use various security features of the Java development environment
- Have a practical understanding of cryptography
- Realize the severe consequences of unsecure buffer handling in native code
- Understand the architectural protection techniques and their weaknesses
- Realize the severe consequences of unsecure buffer handling
- Learn about typical coding mistakes and how to avoid them
- Get information about some recent vulnerabilities in the Java framework
- Get sources and further readings on secure coding practices

Who Should Attend

C/C++ and Java developers, architects and testers.

Outline

- IT security and secure coding
- Web application security
- Client-side security
- Foundations of Java security
- Practical cryptography
- Java security services
- x86 machine code, memory layout and stack operations
- Buffer overflow
- Some additional native code-related vulnerabilities
- Common coding errors and vulnerabilities
- Principles of security and secure coding
- Knowledge sources