Web Service Security

IT-Security Training

Training Contents (2 DAYS)

Web services are used by many applications and are essential in many scenarios nowadays. For example, they enable to connect applications to social networks or to provide own services for third parties. However, web services have become the target of serious attacks due to implementation flaws in recent years. These attacks take advantage of the complexity of the XML standards and allow attackers to read sensitive data from external servers or to decrypt confidential data.

Due to the importance of integrating web services into your enterprise ecosystem, it is essential to understand and address the problems of these technologies. The training will address the following questions, among others:

► How do I use an XML parser correctly?

► How do I check an XML document's signature correctly?

► Which risks need to be considered when using WS-* extensions?

► Is encrypting my messages with TLS sufficient?

► How can I protect my systems against attackers?

Requirements

This training is designed for two groups: For developers who practically use XML and web services. Further on, penetration testers and security researchers who want to learn how to evaluate the security of those systems are addressed.

Lecturer

Dr. Juraj Somorovsky

Juraj Somorovsky is a co-founder of Hackmanit and a security researcher at the Ruhr University Bochum. With more than ten years of experience in the field of IT security, he has acquired profound knowledge regarding cryptography and web security. He is the main developer of the analysis tool "TLS-Attacker" and author of numerous attacks on TLS. These include, for example, DROWN and ROBOT, which each won the Pwnie award for the Best Cryptographic Attack. Juraj Somorovsky presented his work at renowned scientific and industrial conferences, including USENIX Security, Black Hat, DeepSec and OWASP Europe.

Contact

juraj.somorovsky@hackmanit.de
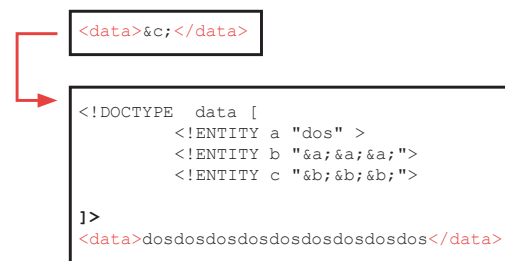www.hackmanit.de

HACKMANIT

Universitätsstraße 150 (ID 2/469)
44801 Bochum
Germany

DAY 1

- XML and SOAP-based Web Services
- XML Schema and WS-Policy
- WS-Addressing and WS-Addressing Spoofing
- XML Parsing (DOM vs. SAX)
- XML-specific Denial-of-Service Attacks
- XML Security and WS-Security
  – Differences to SSL/TLS
- XML Signature
  – ID- and XPath-based XML Signatures

DAY 2

- XML Signature Wrapping Attacks
- XML Encryption
  – Attacks on Symmetric Encryption
  – Attacks on Asymmetric Encryption
- Penetration Testing with WS-Attacker
- Outlook: SAML-based Single Sign-On
- REST-based Web Services
  – Attacks and Best Practices

```
<data>&c;</data>
```

```
<!DOCTYPE  data [
        <!ENTITY a "dos" >
        <!ENTITY b "&a;&a;&a;">
        <!ENTITY c "&b;&b;&b;">
]>
<data>dosdosdosdosdosdosdosdosdos</data>
```

Impact: 200 Byte ➡ 3.5 GB