QAEXPERTS

Security Testing OWASP TOP10

Security Testing OWASP TOP10

As a rising trend in IT industry, cyber security has exponentially increasing demand around the world.

Within our 2-day workshop you will learn about TOP 10 vulnerabilities defined by OWASP and exploit each of them by yourself in practice using various tools and methods. As well, you get to know how to protect your software from each vulnerability, plan such tests and automate where possible. This is going to be fun, meet you there!

 Workshop format:

- 2 trainers
- 16 or less participants
- 2 days (16+ hours)

 Requirements:

- Professional level: Middle Manual QA and higher
- Laptop: Wifi, Windows OS

QAEXPERTS

Security Testing OWASP TOP10

DAY 1

Introduction into Security Testing

- Introducing the speakers and auditory to each other. Describing the workshop goals.

- History security.
- Hacker attacks.
- Security testing in SDLC.
- Tools for Security testing.
- OWASP TOP 10 - Brief introduction.

A1:Injection

- What it is “Injection” attack.
- Examples of attacks.
- Causes of “Injection” vulnerability.
- Tools for search SQL injection.

  Demo and Practice: in search SQL injection

- Protection Recommendations.

A2:Broken Authentication

- What it is “Broken Authentication”.
- Examples of attacks.
- Causes of “Broken Authentication” vulnerability.
- Tools for search “Broken Authentication”.

  Demo and Practice: in search “Broken Authentication”

- Protection Recommendations.

QAEXPERTS

Security Testing OWASP TOP10

A3:Sensitive Data Exposure

- What it is “Sensitive Data Exposure”.
- Examples of attacks.
- Causes of “Sensitive Data Exposure” vulnerability.
- Tools for search “Sensitive Data Exposure”.

Demo and Practice: in search “Sensitive Data Exposure”

- Protection Recommendations.

A4:XML External Entities (XXE)

- What it is “XML External Entities (XXE)”.
- Examples of attacks.
- Causes of “XML External Entities (XXE)” vulnerability.
- Tools for search “XML External Entities (XXE)”.

Demo and Practice: in search “XML External Entities (XXE)”

- Protection Recommendations.

A5:Broken Access Control

- What it is “Broken Access Control”.
- Examples of attacks.
- Causes of “Broken Access Control” vulnerability.
- Tools for search “Broken Access Control”.

Demo and Practice: in search “Broken Access Control”

- Protection Recommendations.

Homework

QAEXPERTS

Security Testing OWASP TOP10

DAY 2

A6:Security Misconfiguration

- Home work discussion and Questions/Answers.
- Reminder of the things learned previous day.
- What it is “Security Misconfiguration” attack.
- Examples of attacks.
- Causes of “Security Misconfiguration” vulnerability.
- Protection Recommendations.

A7: Cross-Site Scripting (XSS)

- What it is “Cross-Site Scripting (XSS)” attack.
- Examples of attacks.
- Causes of “Cross-Site Scripting (XSS)” vulnerability.
- Tools for search "Cross-Site Scripting (XSS)".

  Demo and Practice: in search "Cross-Site Scripting (XSS)"

- Protection Recommendations.

A8:Insecure Deserialization

- What it is “Insecure Deserialization”.
- Examples of attacks.
- Causes of “Insecure Deserialization” vulnerability.
- Tools for search “Insecure Deserialization”.

  Demo and Practice: in search “Insecure Deserialization”

- Protection Recommendations.

QAEXPERTS

Security Testing OWASP TOP10

A9:Using Components with Known Vulnerabilities

- What it is?.
- Examples of attacks.
- Causes of vulnerability.
- Tools for search vulnerability.

  Demo and Practice: in search vulnerability

- Protection Recommendations.

A10:Insufficient Logging & Monitoring

- What it is “Insufficient Logging & Monitoring” attack.
- Examples of attacks.
- Causes of “Insufficient Logging & Monitoring” vulnerability.
- Protection Recommendations.

Closing-Up

- Conclusions.
- Literature.
- Recommendations on further steps.
- Certificates Awarding ceremony.