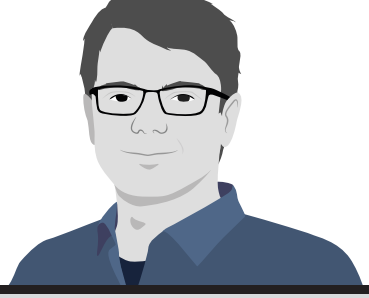
Sichere Webentwicklung

IT-Sicherheit Schulung



Schulungsinhalte

(3 TAGE)

Webapplikationen sind verführerisch einfach zu erstellen. In der heutigen Zeit genügen bereits ein paar Zeilen Code, um eine Webapplikation weltweit verfügbar zu machen. Programmierer werden von der einfachen Entwicklung jedoch oft dazu verleitet, wichtige Sicherheitsaspekte zu vernachlässigen. Dadurch entstehen weltweit zugängliche Einfallstore für Angreifer, die oft mit einfachsten Mitteln für Hackerangriffe genutzt werden können.

In der Intensivschulung *Sichere Webentwicklung* wird den Teilnehmern anhand von Real-Life Beispielen vermittelt, wie ein Angreifer Sicherheitslücken findet und ausnutzt. In der Schulung werden die nachfolgenden Fragen beantwortet:

- WWie untersucht ein Angreifer Webapplikationen? Welche Tools und Methoden werden genutzt?
- Wie gut ist meine Webapplikation vor Angriffen geschützt? An welchen Stellen ist sie verwundbar?
- Wie kann ich meine Webapplikation mit wenigen Handgriffen gegen Angriffe härten?
- Welche Maßnahmen sind nötig um zukünftige Angriffe auf meine Webapplikation zu verhindern oder zumindest abzuschwächen?

Voraussetzungen

Der Kurs richtet sich grundsätzlich an Personen, die sich mit der Thematik des Web-Hacking vertraut machen möchten. Idealerweise sind Sie im Webumfeld beheimatet. Dieser Kurs hilft u. a. Webentwicklern (Front- und Backend), Leitern einer Webentwicklungsabteilung und Information Security Officers. Es ist hilfreich, wenn Sie grundlegende Kenntnisse in HTML mitbringen.

Dozent

Marcus Niemietz

Seit über einer Dekade ist Marcus Niemietz als Penetrationstester und Web-Security-Trainer aktiv. Als Mitgründer von Hackmanit ist er seit 2014 für den Bereich der Websicherheit verantwortlich. Darüber hinaus forscht er aktiv an der Ruhr-Universität Bochum, um sowohl UI-Redressing als auch Cross-Site Scripting Angriffe zu verhindern. Er ist als Sprecher auf zahlreichen internationalen IT-Security Konferenzen aktiv; in der Vergangenheit u. a. auf der renomierten Hackerkonferenz von Microsoft, der Black Hat sowie der USENIX Security. Herr Niemietz ist ein publizierender Buchautor im Bereich Websicherheit.

Kontakt

marcus.niemietz@hackmanit.de
www.hackmanit.de

HACKMANIT

Universitätsstraße 150 (ID 2/469)
44801 Bochum

TAG 1

- Kurzeinführung
  - HTTP, HTML, CSS, XML, DOM
- Social Engineering
- Information Disclosure
- Logical Flaws
- Same-Origin Policy
- Cross-Site Request Forgery
- Cross-Site Scripting
  - Nichtpersistentes XSS
  - Persistentes XSS
  - DOM-basiertes XSS
  - Self-XSS
  - Mutation-basiertes XSS
  - Scriptless Attacks

TAG 2

- Session Hijacking und Session Fixation
- UI-Redressing und Clickjacking
- DOM Clobbering
- File Inclusions und Path Traversal
- Remote Command und Code Execution
- SQL- und noSQL-Injections

TAG 3

- Secure-Coding
  - OWASP TOP-10
  - Zeichensätze
  - DOCTYPE-Switch
  - Content Security Policy
  - Feature und Referrer Policy
  - Burp Suite
- Security Requirements