Im Workshop ***You're Watching Webapps – Tricks und Tools der Pentester*** werden die bekanntesten Angriffsvektoren auf Webanwendungen betrachtet.

Der eintägige Workshop richtet sich hauptsächlich an IT-Mitarbeiter von kleinen und mittelständischen Unternehmen, die die IT-Sicherheit Ihrer Webanwendung selbst überprüfen bzw. erhöhen möchten und/oder das Verständnis erlangen möchten, welchen Angriffen Webanwendungen ausgesetzt sind. Zunächst werden die verschiedenen Elemente von Webanwendungen analysiert, die bei unsicherer Implementierung Angriffe ermöglichen. Anschließend wird gezeigt, wie Schwachstellen entdeckt und ausgenutzt werden können.

Den Teilnehmenden werden Laptops mit der benötigten Software bereitgestellt. Es steht ein Labor-Netzwerk zur Verfügung, um das Gelernte direkt anzuwenden. Die Teilnehmenden erhalten eine Teilnahmebescheinigung.

Dieser Workshop ergänzt unseren zweitägigen Workshop ***You're Watching– Tricks und Tools der Pentester***, in dem lediglich ein kleiner Einblick in Websicherheit gegeben wird.

# Kontakt

## Inhaltliche Beratung


Prof. Dr. Arno Wacker
Professor für Datenschutz und Compliance

☎ 089 / 6004 - 7325
E-Mail: arno.wacker@unibw.de
Web: https://www.unibw.de/code

Forschungsinstitut Cyber Defence (CODE)
Universität der Bundeswehr München
Carl-Wery-Straße 22
81739 München


## Organisatorische Beratung


Dipl.-Päd. Karina Anders, MBA
Programmkoordinatorin
campus advanced studies center

☎ 089 / 6004 - 2086
E-Mail: info@casc.de
Web: https://www.unibw.de/casc

campus advanced studies center
Universität der Bundeswehr München
Werner-Heisenberg-Weg 39
85579 Neubiberg


der Bundeswehr Universität München

**Workshop**

# You're Watching

**Webapps**

Forschungsinstitut Cyber Defence
Universität der Bundeswehr München

Der eintägige Workshop besteht aus sechs Lerneinheiten. Im Folgenden werden diese näher beschrieben.

## Lerneinheit 1 – Grundlagen

In der ersten Lerneinheit werden die Grundlagen zu HTTP und zu einem allgemeinen Aufbau von Webanwendungen erläutert sowie eine Einführung zu SQL gegeben. Ziel dieser Einheit ist es, das Zusammenspiel von verschiedenen Elementen einer Webanwendung zu beleuchten und zu zeigen, wo Angriffspunkte sein können. Anschließend haben die Teilnehmenden die Möglichkeit, sich auf den bereitgestellten Laptops mit SQL vertraut zu machen, selbst eine Datenbank anzulegen und die gelernten SQL-Anweisungen anzuwenden.

## Lerneinheit 2 – Enumeration

Wir demonstrieren wie Informationen über eine Webanwendung zu sammeln und die ersten Schwachstellen zu entdecken sind. Es wird gezeigt, welche Informationen bereits über den in einem Webbrowser integrierten Webentwickler-Tools gesammelt werden können. Danach wird vorgeführt, wie nicht verlinkte Inhalte entdeckt werden können, welche Werkezeuge es dazu gibt und wie diese funktionieren. Anschließend wenden Sie diese Werkzeuge an, um sich ein Bild über mögliche Schwachstellen in einer Test-Webanwendung machen zu können.

## Lerneinheit 3 – XSS

Hier werden verschiedene Arten der Schwachstelle namens *Cross-Site-Scripting* (XSS) vorgestellt, voneinander abgegrenzt und die Ursachen für diese Schwachstellen beleuchtet. Es wird demonstriert, wie diese Schwachstelle für Angriffe ausgenutzt werden kann. Im praktischen Teil werden Sie selbst XSS-Angriffe ausführen. Abschließend wird diskutiert, wie solche Angriffe vorzubeugen sind.

## Lerneinheit 4 – SSRF

Es wird erklärt, was mit der Schwachstelle *Server-Side Request Forgery* (SSRF) gemeint ist, welche Arten dieser Schwachstelle unterschieden werden und was ihre Ursachen sind. Danach wird demonstriert, SSRF-Schwachstellen entdeckt werden können. Im praktischen Teil lernen Sie selbst SSRF-Schwachstelle zu entdecken und für Angriffe zu nutzen. Wie jede Lerneinheit, wird auch diese mit einer Diskussion zu Gegenmaßnahmen abschließen.

## Lerneinheit 5 – File Inclusion

Die Schwachstelle *Directory Traversal* wird erklärt, die Ursachen und wie sie für Angriffe ausgenutzt werden kann, erläutert. Im praktischen Teil üben Sie, die Schwachstelle Directory Traversal zu erkennen und sie für Angriffe auszunutzen.

## Lerneinheit 6 – Injection

In dieser Lerneinheit werden zwei unterschiedliche Arten von Injection-Schwachstellen behandelt, nämlich *Command Injection* und *SQL Injection*. Zunächst wird im theoretischen Teil erklärt, warum diese Angriffe funktionieren. Danach wird gezeigt, wie eine Web-Anwendung manuell auf Injection-Schwachstellen geprüft werden kann. Anschließend werden verschiedene Werkzeuge vorgeführt, um die Überprüfung automatisiert durchzuführen. Im praktischen Teil werden Sie diese Werkzeuge in der Laborumgebung selbst einsetzen, um ein Webportal auf die beiden Arten von Injection-Schwachstellen zu prüfen und anzugreifen.