

# W3WI\_SE411 - Forschungsseminar Informatik / Advanced Practical IT Security

Dozent: Prof. Dr. Michael Eichberg  
Kontakt: [michael.eichberg@dhbw-mannheim.de](mailto:michael.eichberg@dhbw-mannheim.de), Raum 149B  
Unterlagen: Moodle  
Version: 23SEB

# Teaser

In dieser Veranstaltung werden wir uns mit den Grundlagen praktischer Angriffe und Verteidigungsmaßnahmen im Bereich IT Security auseinandersetzen. Wir werden uns der Frage widmen wie, wann und in welcher Form man - auf den ersten Blick abgesicherte Systeme - einerseits angreifen (🚩 *to exploit*) kann und wie man die Sicherheit weiter erhöhen kann.

Wir werden uns in diesem und dem nächsten Semester ausgewählten Themen widmen, die von der Sicherheit von Passwörtern und Angriffen auf selbige bis hin zu der Sicherheit von Netzwerken und Webanwendungen reichen. Wir werden uns dabei insbesondere an gängigen Angriffsszenarien orientieren.

Wir werden uns somit auf praktische Aspekte der IT Sicherheit fokussieren. Das Kennenlernen der theoretischen Grundlagen von Verschlüsselungsalgorithmen, Hashalgorithmen, Zertifikaten und Vergleichbarem ist nicht primärer Fokus dieser Veranstaltung.

## ※ Hinweis

Für diese Veranstaltung sind Grundkenntnisse in Linux/Unix/macOS hilfreich aber nicht notwendig. Notwendig ist aber Interesse an tiefergehenden technischen Details.

# Grober Ablauf

- 1. Semester: 6 Termine; (50% der Endnote)
- 2. Semester X Termine; (50% der Endnote)

## Genereller Ablauf

1. Einführung in ein für die IT-Sicherheit relevantes Thema in Hinblick auf praktische Anwendung
2. Präsentationen zur Vertiefung
3. Aufgaben für die entsprechende Fragestellung
4. Abgabe, die genau beschreibt wie Sie die Aufgabe gelöst haben. Darüber sammeln Sie Teilnoten, die am Ende verrechnet werden. D. h. es gibt Teilnoten pro Aufgabe. Die Punkte sind zwischen den Aufgaben nicht untereinander vergleichbar.
5. Jeder muss präsentieren.

# Inhalte

## ※ Hinweis

Diese Veranstaltung ist ergänzend zur Veranstaltung SE III IT-Sicherheit zu sehen. D. h. Inhalte die dort vermittelt werden, werden hier nicht noch einmal behandelt, sind aber potentiell relevant.

### 1. Semester

1. Passwortwiederherstellung (📄 *Password Recovery*)
2. Reverse Engineering 101

### 2. Semester

Pentesting von Webanwendungen

# Was passiert wann im 1. Semester..

19. Nov. 2025: Einführung & Passwortwiederherstellung (Teil 1)  
(Ggf. Linux Shell und Reguläre Ausdrücke.)

24. November 2025 (Online):  
(*Optional* - Unterstützung bei der Erstellung der Präsentationen)  
BBB: <https://bbb.dhbw.de/mannheim/eic-mn5-hvh-7qd>

01. Dezember 2025:

- Präsentationen zum Thema Password Recovery

Passwortwiederherstellung (Teil 2)

- Einführung in Reverse Engineering (und Netzwerkanalyse)
- Ausgabe der Übung bzgl. Password Recovery

15. Dezember 2025:

Präsentationen zum Thema Reverse Engineering  
Ausgabe der Übung

12. Januar 2026 (Online):  
(*Optional* - Unterstützung bei der Bearbeitung der Aufgaben)  
BBB: <https://bbb.dhbw.de/mannheim/eic-mn5-hvh-7qd>

26. Januar 2026: **Abgabe der Lösungen für alle Aufgaben als PDF Dokument (Moodle)**  
*(Ich werde am 29. zuteilen wer welchen Teil präsentiert; bitte schauen Sie in Moodle. Sollten Sie am 30. Okt. bis 22:00 Uhr weder eine Nachricht in Moodle noch eine E-Mail von mir erhalten haben, dann melden Sie sich bitte umgehend bei mir.)*

## Abschlusspräsentationen

Die Präsentationsdauer ist am Inhalt zu orientieren; darf max. 30 min pro Person jedoch nicht überschreiten. Jeder soll in der Lage sein alle Schritte nachvollziehen zu können. D. h. die Präsentation kann auch eine „Live-Demo“ sein, die zeigt wie die Aufgabe gelöst wurde.

Die Präsentation ist bis zum 3. Nov. 2024 23:59 Uhr in Moodle hochzuladen. Sollten Sie eine Live-Demo machen, dann zeichnen Sie Ihren Probelauf auf und laden Sie diesen als Zip-Datei hoch. Alternativ können Sie Ihre Video auch in Youtube stellen oder per OneDrive, Dropbox, ... zur Verfügung stellen. In diesem Falle laden Sie eine Textdatei mit der URL zum Video hoch! Nutzen Sie nicht Moodle für die Videos, da diese häufig Probleme bereitet!

Erste Tips zur Gestaltung von Vorträgen finden Sie hier.

Notenanteil: 15%

# Was passiert wann im 2. Semester..

XXXX 2026

- Ausgabe der Themen zur Bearbeitung
- Kurze Einführung in das Thema Pentesting.

YYYY 2026

**Bearbeitung der Themen** mit dem Ziel „Hands-on“; bei Bedarf stehe ich für Rückfragen *online* zur Verfügung: <https://bbb.dhbw.de/mannheim/eic-mn5-hvh-7qd>.

YYYY 2026

- Halten der Präsentationen - Notenanteil: 20%
- Vergabe der Aufgabe für das Pentesting

## ▲ Achtung!

Die Vorträge müssen am Abend vorher hochgeladen sein.

YYYY 2026

**Durchführung des Pentesting;** bei Bedarf stehe ich für Rückfragen *online* zur Verfügung: <https://bbb.dhbw.de/mannheim/eic-mn5-hvh-7qd>.

YYYY 2026

Vorstellung der mittels Pentesting gefundenen Lücken - Notenanteil: 20%

## ▲ Achtung!

Die Vorträge müssen am Abend vorher hochgeladen sein.

Ende des Semesters

Abgabe der Dokumentation der Ergebnisse des Pentesting inkl. Bewertung als PDF Dokument (Moodle) - Notenanteil: 10%

# Vortragsthemen

- **Nmap (und ncat)** (1 Person)  
(Network discovery and security auditing.)
- **Zed Attack Proxy (ZAP)** (1 Person)  
(Web App Scanner)
- **Burp Suite inkl. Dastardly** (1 Person)  
(Penetration testing toolkit.)
- **Metasploit** (2 Personen)  
(Penetration testing framework.)

**Dauer pro Person: 25 Minuten**



# Bewertungskriterien

## Für die Präsentationen

- Vermittelt die Präsentation einen guten ersten Einblick in das Tool (Fähigkeiten und Grenzen)
- Qualität der (Live-)Demonstration (und ggf. des Backups)  
(ggf. ist das Aufsetzen einer (kleinen) virtuellen Maschine sinnvoll/notwendig.)
- Reduktion auf das Wesentliche
- Qualität der Beantwortung von Fragen
- Persönliches Auftreten
- Einhaltung der Dauer der Präsentation

Notenanteil: 20% (max. 20 Punkte von 100 Punkten)

## für das Pentesting

- Anzahl der gefundenen Schwachstellen
- Qualität der Präsentation der Schwachstellen
- Beantwortung von Fragen

Notenanteil: 25% (max. 25 Punkte von 100 Punkten)

## für die Dokumentation

- Qualität der Dokumentation (leserlich, strukturiert, frei von Tippfehlern, ...)
- Ist die Einschätzung der Lücken nachvollziehbar

Notenanteil: 5% (max 5. Punkte von 100 Punkten)