W3WI_SE411 - Forschungsseminar Informatik / Advanced Practical IT Security

Dozent: Prof. Dr. Michael Eichberg
Kontakt: michael.eichberg@dhbw-mannheim.de, Raum 149B

Unterlagen: Moodle
Version: 23SEB (Rev 2025-11-27)

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/geschützte Daten - 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 somit auf praktische Aspekte der IT Sicherheit fokussieren. Theoretische Grundlagen sind nur in so weit relevant, dass sie in der Praxis eine Relevanz haben.

※ Hinweis

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

Es wird empfohlen sich eine virtuelle Maschine (z. B. mit VirtualBox) aufzusetzen, auf der Sie Linux (z. B. Kali Linux) installieren. Ggf. können Sie auch WSL2 unter Windows verwenden. Mac User können viele der Tools direkt installieren oder über Homebrew bzw. MacPorts beziehen.

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 mit praktischer Ausrichtung.
2. Studentische Präsentationen zur Vertiefung bzw. Betrachtung wichtiger Aspekte.
3. Aufgaben für die entsprechende Fragestellung.
4. Abgaben, die genau beschreiben wie Sie die Aufgaben 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.

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

1. Erstes Semester: Passwortwiederherstellung und Reverse Engineering

Was passiert wann im 1. Semester...

19. Nov. 2025:

- Einführung
- Themenvergabe für die Fachpräsentationen - Notenanteil: 15%

  Die folgenden Themen werden ggf. am 01.12.2025 bzw. 15.12.2025 weiter vorgestellt:

  - Einführung in Passwortwiederherstellung (Linux Shell und Reguläre Ausdrücke)
  - Einführung in Reverse Engineering

24. November 2025 (Online):

Unterstützung bei der Erstellung der Präsentationen (*Optional*)
BBB: https://bbb.dhbw.de/rooms/eic-dx8-r7g-ioa

01. Dezember 2025:

- **Präsentationen (Schwerpunkt: Themen mit Bezug Passwortwiederherstellung)**
- Ausgabe der Übung bzgl. Passwortwiederherstellung (🇺🇸 *Password Recovery*) - Notenanteil: 15%

15. Dezember 2025:

- **Präsentationen (Schwerpunkt: Themen mit Bezug Reverse Engineering)**
- Ausgabe der Übung bzg. Reverse Engineering - Notenanteil: 15%

12. Januar 2026 (Online):

Unterstützung bei der Bearbeitung der Aufgaben (*Optional*)
BBB: https://bbb.dhbw.de/rooms/eic-dx8-r7g-ioa

21. Januar 2026 (Ereignis):

Abgabe der Lösungen für alle Aufgaben als PDF Dokument über Moodle - Deadline 21.1.2026, 12:00 Uhr

22. Januar 2026 (Ereignis):

Zuteilung wer welchen Teil präsentiert über Moodle/Mail. Sollten Sie am 22.01. bis 19:00 Uhr weder eine Nachricht in Moodle noch eine E-Mail von mir erhalten haben, dann *melden Sie sich bitte umgehend* bei mir.

26. Januar 2026: **Abschlusspräsentationen - Notenanteil: 5%**

Die Präsentationsdauer pro Person ist 5 Minuten und soll die Vorgehensweise zur Lösung der entsprechenden Aufgabe präsentieren. D. h. die Präsentation kann auch eine „Live-Demo“ sein, die zeigt wie die Aufgabe gelöst wurde.

Erste Tips zur Gestaltung von Vorträgen finden Sie hier.

Sollten Sie eine Live-Demo machen, dann zeichnen Sie Ihren Probelauf auf (5 Minuten) und laden Sie diesen als Zip-Datei hoch. Alternativ können Sie Ihr 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! Das Video soll mindestens 3 Monate verfügbar sein.

Notenzusammenstellung - 1. Semester

Leistungsnachweis	Notenanteil
Fachpräsentation (10 Minuten pro Person)	15%
Lösungen der Aufgaben bzg. Passwortwiederherstellung	15%
Lösungen der Aufgaben bzgl. Reverse Engineering	15%
Lösungspräsentationen (5 Minuten pro Person)	5%

Fachpräsentationen

Vortragsthemen 1.12.2025

- scrpyt, bcrypt und Argon2: moderne Passwort Hashing Algorithmen - Vorstellung und Shout-out
  (3 Personen)
- John the Ripper: Passwort Cracking Tool - Einführung und Demonstration
  (1 Person)
- WIFI Passwortsicherheit: Hacking WEP und WPA2 mit Aircrack-ng - Einführung und Demonstration; WPA3: Besprechung von Dragonblood
  (2 Personen)
- Wireshark: Einführung in die Konzepte und praktische Anwendung (Kali Linux, Mac OS, Windows) - Anwendung bei verschlüsselten Protokollen (TLS, HTTPS, ...)
  (3 Personen)
- YSoSerial: Java Deserialization Exploits (aka Serialization gadgets) - Einführung in das Thema und Demonstration/Besprechung von Beispielen
  (2 Person)
- Fuzzy Hashing und Yara: Malware Detection/Description
  (1 Person)

Vortragsthemen 15.12.2025

- Aufbau von APKs (Android Apps) und der grobe Aufbau des Dex File Formats
  (2 Person)
- DexGuard und Proguard: Obfuscator für Android und Java Anwendungen - Einführung und Demonstration (z.B. mit Hilfe von JadX, CFR/JD-GUI)
  (1 Personen)
- Einsatz von FRIDA zur dynamischen Instrumentierung von Android und iOS Anwendungen
  (1 Personen)
- xdbg64 (Windows): Hacking Applications mit dem x64 Debugger - Einführung und Demonstration
  (1 Person)
- Native Binary Reverse Engineering

  (Bitte Gegenseitig absprechen, um Überschneidungen zu vermeiden!)

  - Assembler: x86 oder ARM Assembler Grundlagen für Reverse Engineering
    (2 Personen)
  - *Function Call Semantics* in Binaries und *Syscalls*
    (1 Person)

- Virtuelle Methodenaufrufe und deren Umsetzung in Assembler
  (1 Person)
- Sicherheitsmechanismen in Native-Binaries: insbesondere Stack canaries, Position-independent Code & Address Space Layout Randomization
  (1 Person)
- Ghidra: Binary-Reverse-Engineering - kurze Einführung und Demonstration
  (2 Personen)

8

Themenvergabe

Thema	Personen
scrypt, bcrypt und Argon2	3
John the Ripper	1
WIFI Passwortsicherheit	2
Wireshark	3
YSoSerial	2
Fuzzy Hashing und Yara	1
Aufbau von APKs und Dex	2
DexGuard und Proguard	1
FRIDA	1
xdbg64	1
Assembler Einführung	2
Function Call Semantics	1
Virtuelle Methodenaufrufe	1
Sicherheitsmechanismen in Native-Binaries	1
Ghidra	2

Bewertete Abgaben

1. Passwortwiederherstellung - Aufgaben
2. Reverse Engineering - Aufgaben

2. Zweites Semester: Pentesting von Webanwendungen

Die folgenden Informationen sind vorläufig und können/werden sich bis zum Start des 2. Semesters ändern.

⚠ Achtung!

Aufgrund des massiven Einsatzes von KI sind die Bewertungskriterien für alle Abgaben (Präsentationen, Dokumentationen) verschärft worden.

- Jede Aussage, die faktisch falsch ist, führt unmittelbar zu Punktabzug am Ende (und wird nicht ignoriert werden).
- Jede Aussage, die blödsinnig ist, führt zu Punktabzug.
- Jede Aussage, die überflüssig ist (*„Blah Blah“*) und nicht dem Thema der Aufgabe/Präsentation dient, führt zu Punktabzug.
- Unnötige Aussagen, die bekannte Inhalte (zum Beispiel aus dieser oder anderen Vorlesungen) wiederholen, führen zu Punktabzug.
- Jede Aussage, die nicht durch eine Quelle oder durch eigene Experimente belegt werden kann, führt zu Punktabzug.
- Qualifizierende Attribute („schneller“, „besser“, „schwerer“ …) müssen durch konkrete Metriken belegt bzw. definiert werden, ansonsten führen sie zu Punktabzug.

Ablauf

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.

YYYY 2026

- Halten der Präsentationen
- 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.

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)
  (Network discovery and security auditing.)
- Zed Attack Proxy (ZAP)
  (Wep App Scanner)
- Burp Suite inkl. Dastardly
  (Penetration testing toolkit.)
- Metasploit
  (Penetration testing framework.)
- Shodan und recon ng

Dauer pro Person: XX 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)