Sicherheit in Web-Anwendungen

Proseminar

technische universität

Fakultät Informatik
Lehrstuhl für

Vorstellung

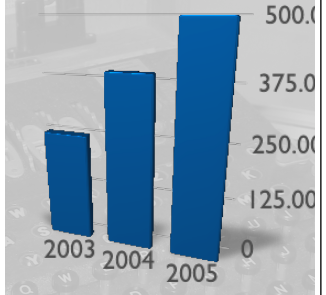
- Dipl.-Inf. Christian Bockermann
  - WiMi am Lehrstuhl 8
- Forschungsgebiete
  - Web-Sicherheit durch intelligente Methoden (Data-Mining, KI)
  - Data-Mining in verteilten Umgebungen

Überblick

- Warum ein Proseminar zum Thema „Sicherheit in Web-Anwendungen“ ?
- Ziele des Proseminars
- Erwartungen an das Proseminar
- Themenvorstellung und Vergabe
- Vorführung: WebGoat

Web-Sicherheit

- Immer mehr Dienste werden im Web verfügbar gemacht
- Web-Anwendungen leicht angreifbar (z.B. mit Browser)
- Zahl der Angriffe im Web steigt
- Experten: ca. **2500 erfolgreiche Angriffen pro Stunde** aus



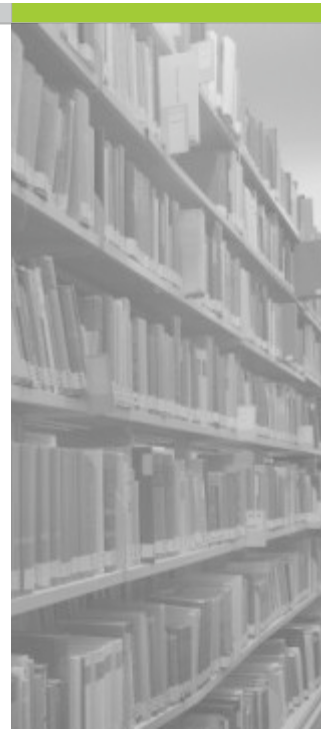
Quelle: h-zone

Web-Sicherheit

- Gründe für erfolgreiche Angriffe oftmals **fehlerhafte Anwendungen**
- **Zeit-/Kostendruck** führt zu Einsparungen in der Entwicklung
- Validierung von Software bzw. **Code-Reviews** oft sehr **aufwendig**
- Gefahr von Angriffen den Entwicklern oft nicht „bewusst“

Proseminar

- Strukturiertes, selbstständiges Arbeiten
- Erlernen von **Literatur-Recherche**
  - Exkurs zur Uni-Bibliothek
  - Bibliographieren
- Präsentationstechnik
- Erlernen von Sachwissen im Bereich Web-Sicherheit



Proseminar

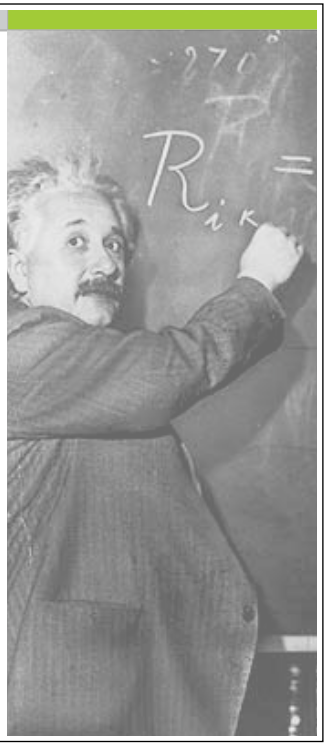
- Strukturen und Schwachstellen von Anwendungen aufzeigen
- Wissen über Angriffe erforderlich für wirksame Sicherheitsmaßnahmen
- Das Proseminar ist **KEIN Hacker-Kurs**!

Proseminar

- **Anwesenheitspflicht**!
- Jeder Teilnehmer hält **Vortrag:**
  - Umfang ca. 60-75 Minuten
  - Anschliessende **Diskussion**
    - kurze Feedback-Runde zum Präsentationsstil
    - fachliche Diskussion, Moderation durch „Paten“

Vortrag

- Vortragender sollte das **Thema verstanden** haben
- Wahl des **Abstraktionsgrades**
  - So viel Detail, wie für Verständnis der Zuhörer notwendig
- **Klare Strukturierung**, „roter Faden“ sollte immer erkennbar sein
  - Aussagekräftige Folien

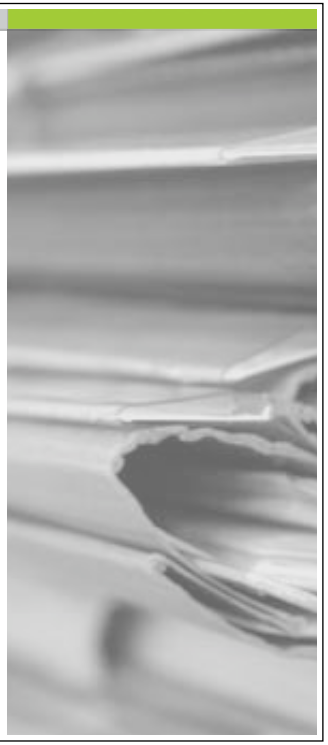


Vortrag

- **Zeiteinteilung**
  - Gebt vorher an, wie lange ihr benötigt
- **Probevortrag vor Paten**?
- 3 Wochen vor Vortragstermin Folien an den Betreuer

Proseminar

- **Ausarbeitung** zum Vortrag
  - ca. 4-6 Seiten
  - Abgabe bis 2 Wochen nach Vortragstermin
- **Bewertung** des Vortrags -> Note
  - durch Seminarteilnehmer
  - durch Seminarbetreuer (endgültige Note)



Hilfe

- Fragen zur Vortragsstruktur, inhaltliche Fragen, ...
- Sprechstunde
  - prinzipiell von 10 - 18 Uhr erreichbar
  - christian.bockermann@udo.edu
  - Tel.: 755-6487
  - GB4 / Raum 119

Vorstellungsrunde

Seminar-Themen

technische universität
Fakultät Informatik
Lehrstuhl für

Themenblöcke

- Aufteilung in drei Abschnitte:
  - **Struktur und Aufbau** von Web-Anwendungen
  - **Sicherheitsproblematik** und **Angriffe**
  - **Sicherheitsmaßnahmen** in Web-Umgebungen

Themen

- **Struktur und Aufbau**
  - Das HTTP Protokoll
  - SSL und HTTPS (2)
  - Common Gateway Interface (CGI)
  - PHP als Web-Sprache
  - Web-Anwendungen mit Java: JSP und Servlets
  - JavaScript / AJAX
  - Web-Services

Themen

- **Angriffe**
  - Form-Tampering/SQL-Injection/ Blind SQL-Injection
  - Path-Traversal und Remote-File Inclusion
  - Session-Fixation und Session-Hijacking
  - XSS und Cross-Site Request Forgery

Themen

- **Sicherheitsmaßnahmen**
  - Security-Scanner
  - Web Application Firewalls (ModSecurity)
  - „Abstracting Web Application Security“ (Paper)
  - Anomalie-Erkennung in Web-Anwendungen (2)

Ansatzpunkte

- Open Web-Application Security Project (OWASP)
  - WebGoat Anwendung zum Lernen/ Verstehen von Angriffen
  - Vielzahl von Dokumenten, Präsentation zu Web-Sicherheit
  - Google, CiteSeer, RFC
  - Einige (wenige) Paper zum Thema IDS und Web-Sicherheit