

Hackerpraktikum SS 202

Philipp Schwarte, Lars Fischer

Universität Siegen

April 17, 2012

Organisation

- ▶ wöchentliche Übung mit Vorlesungsanteil
- ▶ alle zwei Wochen neue Aufgaben
- ▶ Abgabe der Aufgaben ist verpflichtender Teil
- ▶ Schein:
 - ▶ Ausarbeitung über einen Teilbereich nach Absprache
 - ▶ Kurzvortrag darüber in letzter Übung

Introduction

Philipp Schwarte



Dr. Lars Fischer

fischer@wiwi.usi...

- ▶ Studium: Uni Bremen
 - ▶ Rechnernetze
 - ▶ Betriebssysteme
 - ▶ Syntaktische Bilderzeugung
- ▶ Promotion: TU-Darmstadt
 - ▶ Verkettbarkeitsmetriken
 - ▶ IT-Sicherheit
 - ▶ Hackerpraktika
- ▶ IT-Sec Berater

Contents of Lecture

(vorläufig)

1. Web
2. Code Injection
3. Network Discovery
4. Network Games
5. Rootkits/Bots
6. "Scripten" und "Coden"

Literature

- ▶ Howard, LeBlanc, Viega: 24 deadly sins of software security
- ▶ Gary McGraw: Software Security
- ▶ Information Systems Security Framework (ISSAF)
- ▶ Open Source Testing Security Testing Methodology Manual (OSSTM 3)
- ▶ <http://phrack.com>
- ▶ <https://www.owasp.org>
- ▶ The Internet

Werkzeugkiste

- ▶ Shell, Script & Code
 - ▶ z.B. Bash, Ruby, Python, Erlang, C
- ▶ Editor (Code, Hex, low level. . .)
- ▶ Disassembler (Ida, ndisasm, objdump)
- ▶ nc, nmap, tcpdump, curl, john. . .
- ▶ Browser-Erweiterungen
- ▶ Frameworks
 - ▶ burpsuite, metasploit
 - ▶ Backtrack

Overview Lesson 01

Organisation

Remember the WWW

Network Stack

ISO/OSI:

7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data Link
1. Physical

HTTP Request

- ▶ Client-Server
- ▶ GET, POST, PUT, DELETE, OPTIONS,...
- ▶ Dokumente
- ▶ Header

GET /login HTTP/1.1

Name: Wert

Body

HTTP Response

- ▶ Response Codes (200, 404,...)
- ▶ Header (z.B. Cookie)

```
HTTP/1.1 200 OK  
Set-Cookie: Keksschachtel
```

```
<html><body></body></html>
```

Main Web Follies

- ▶ Missing Input Validation
- ▶ Missing Input Validation
- ▶ Missing Input Validation
- ▶ Missing Input Validation
- ▶ Missing Input Validation
- ▶ Missing Input Validation
- ▶ Missing Output Validation
- ▶ Missing Input Validation
- ▶ Missing Input Validation
- ▶ Missing Input Validation

Main Web Follies

- ▶ Missing Input Validation
- ▶ Missing Input Validation
- ▶ Missing Input Validation
- ▶ Missing Input Validation
- ▶ Missing Input Validation
- ▶ Missing Input Validation
- ▶ Missing Output Validation
- ▶ Missing Input Validation
- ▶ Missing Input Validation
- ▶ Missing Input Validation
- ▶ Cross-Side-Script (XSS)
- ▶ Session-Fixation
- ▶ User-determined Input
- ▶ Cross-Side-Request-Forgery (CSRF)
- ▶ Path Vulnerability
- ▶ Logical Errors
- ▶ Range/Type Errors
- ▶ Code Injection
- ▶ ...

Input Validation

- ▶ Which Input is expected?
- ▶ Whitelisting
- ▶ What is the input used for?
- ▶ Typecasting

HTML

- ▶ Hypertext Markup Language
- ▶ brought us **links**
- ▶ logical markup

```
<html>  
<head><script src="./script.js"/></head>  
<body>Some Text</body>  
</html>
```

Example: XSS

- ▶ Write script somewhere
- ▶ Executed if displayed by other

Session-Fixation

- ▶ predictable/prepared Session Id
- ▶ attacker fixes Id before Authentication
- ▶ URL-ID → special link
- ▶ Hidden-Form Field → special Form

Injection

- ▶ Methodology
 1. break out (e.g. parantheses)
 2. insert commands
 3. clean finish (e.g. comment)
- ▶ HTML-Injection
 - ▶ Server-Side Code
 - ▶ User defined variable
 - ▶ close mark, insert stuff, clean up
- ▶ SQL-Injection
- ▶ ...

Today's Assignment

- ▶ Email writing
- ▶ Setup Virtual Box
- ▶ Setup VPN-Keys
- ▶ WWW-beginnings