

Hacking Webapplications

Kurs 1012

© 2005-2012 OpenSource Training Ralf Spenneberg

Am Bahnhof 3-5

48565 Steinfurt

<http://www.opensource-training.de>

<http://www.os-t.de>

Copyright

Die in diesem Kurs zur Verfügung gestellten Folien, Unterlagen und Übungen sind urheberrechtlich geschützt. Wir behalten uns alle Rechte vor, auch die der fotomechanischen Wiedergabe und der Speicherung in elektronischen Medien. Die gewerbliche Nutzung ist nicht erlaubt.

Die Informationen in diesem Produkt werden ohne Rücksicht auf einen eventuellen Patentschutz veröffentlicht. Warennamen werden ohne Gewährleistung der freien Verwendbarkeit genutzt. Fast alle Hardware- und Softwarebezeichnungen, die in dieser Unterlage erwähnt werden, sind gleichzeitig auch eingetragene Warenzeichen.

Bei der Zusammenstellung der Texte und Abbildungen wurde mit größter Sorgfalt vorgegangen. Jedoch können Fehler nicht vollständig ausgeschlossen werden. Die Firma OpenSource Training Ralf Spenneberg kann für fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen.

Für Verbesserungsvorschläge und Hinweise auf Fehler sind wir dankbar.

Inhaltsverzeichnis

1	Introduction	5
1.1	Die gute alte Zeit	5
1.2	Entwicklung	7
1.3	Heute	9
1.4	Firewalls noch zeitgemäß?	11
2	Attack Possibilities	13
2.1	Angriffsmöglichkeiten	13
2.2	Netzwerk	15
2.3	Betriebssystem	17
2.4	Webserverapplikation	19
2.5	Webapplikation	21
3	Was ist HTTP	23
4	Injections in Depth	39
4.1	Injektionen	39
4.2	Ursache und Lösung	41
4.3	SQL Injections	43
4.4	Blind Injections	67
4.5	SQLMap	69
4.6	LDAP Injections	75
5	Cross-Site-Scripting	77
6	Attacking Sessionhandling	91
6.1	Guessing SessionIDs	91
6.2	Cross-Site-Request-Forgery	111
7	AJAX	115
8	Phishing und Pharming	127
9	SPAM-Versand	131
10	Directory Traversal	135
11	Shell Command Injection	137
12	Nullbyte	139
13	Remote File Inclusion	141

14 HTTP Response Splitting	143
15 SOAP	157
16 Werkzeuge	167
17 Verteidigung	171
17.1 Probleme	173
17.2 Sichere Programmierung	183
17.3 Administrative Maßnahmen	191