Praktikum Anwendungssicherheit

Hochschule der Medien Stuttgart

Protokoll

I: Informationsgewinnung

Verfasser:	Benjamin Zaiser
E-Mail:	bz003@hdm-stuttgart.de
Studiengang:	Computer Science and Media
Semester:	2
Datum:	22. September 2008

Inhaltsverzeichnis

1 Zum Aufbau des Protokolls

Das Protokoll ist wie folgt aufgebaut: zu jeder Übung gibt es ein Kapitel. Jedes Kapitel hat nach Möglichkeit folgende Unterpunkte:

Hintergrundinformationen Informationen, die für die Durchführung der Übung, bzw. für das Verständnis der Aufgabenstellung erforderlich sind.

Aufgabenstellung Welche Aufgabe soll durchgeführt werden; was ist das Ziel der Übung.

Lösung/Durchführung Wie wurde die Aufgabe gelöst; welche Probleme traten dabei auf.

Erkenntnis Was lernt man aus der Aufgabe; welche Erkenntnis könnte in die Entwicklung einer Web-Applikation einfließen.

2 Google Hacking

2.1 Hintergrundinformationen

Für die Informationsgewinnung eignen sich Web-Dienste (wie z.B. Suchmaschinen) hervorragend. Da ihre Hauptaufgabe die Informationssammlung auf Webseiten weltweit entspricht. Google eignet sich ganz besonders, da der Suchstring nicht nur aus gewöhnlichen Suchworten bestehen kann, sondern die Suchergebnisse auch durch verschiedene Befehle beeinflusst werden können.

inurl: Suchwort sucht nur in der URL nach dem Suchwort

intitle: Suchwort sucht nur in dem title-Tag der HTML Seite nach dem Suchwort

filetype: Dateiendung sucht nur nach bestimmten Dateitypen

site: domain sucht nur in der angegebenen Domain

2.2 Durchführung

Durch Verwendung von „inurl:view/view.shtml“ bekommt man z.B. eine Liste von diversen Webcams.

Mithilfe von „filetype:inc“ erhält man sogar Quellcode von Include Dateien, die in PHP Skripten verwendet werden können (z.B. „http://www.moskadr.ru/functions.inc“

Mit „filetype:log inurl:password“ bekommt man als Suchergebnis diverse Benutzernamen mit den dazugehörigen Passwörtern:

Abbildung 1: Mit Google Hacking Benutzer & Passwörter herausfinden

Aber auch mittels einer whois Abfrage bei DENIC.de erhält man viele Informationen über einen Domaineigentümer:

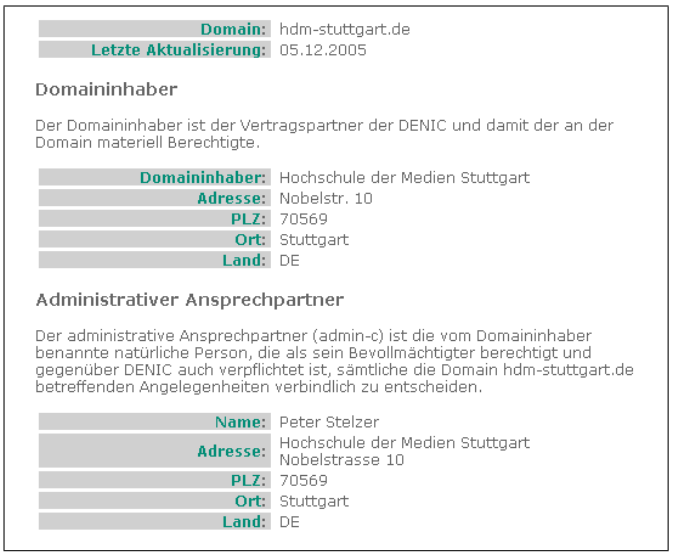

Abbildung 2: denic.de whois Abfrage: hdm-stuttgart.de

Sucht man nach etwas bestimmtem wie z.B. einer Person, so helfen manchmal auch spezielle Suchmaschinen (123people.de, yasni.de, ...) weiter:

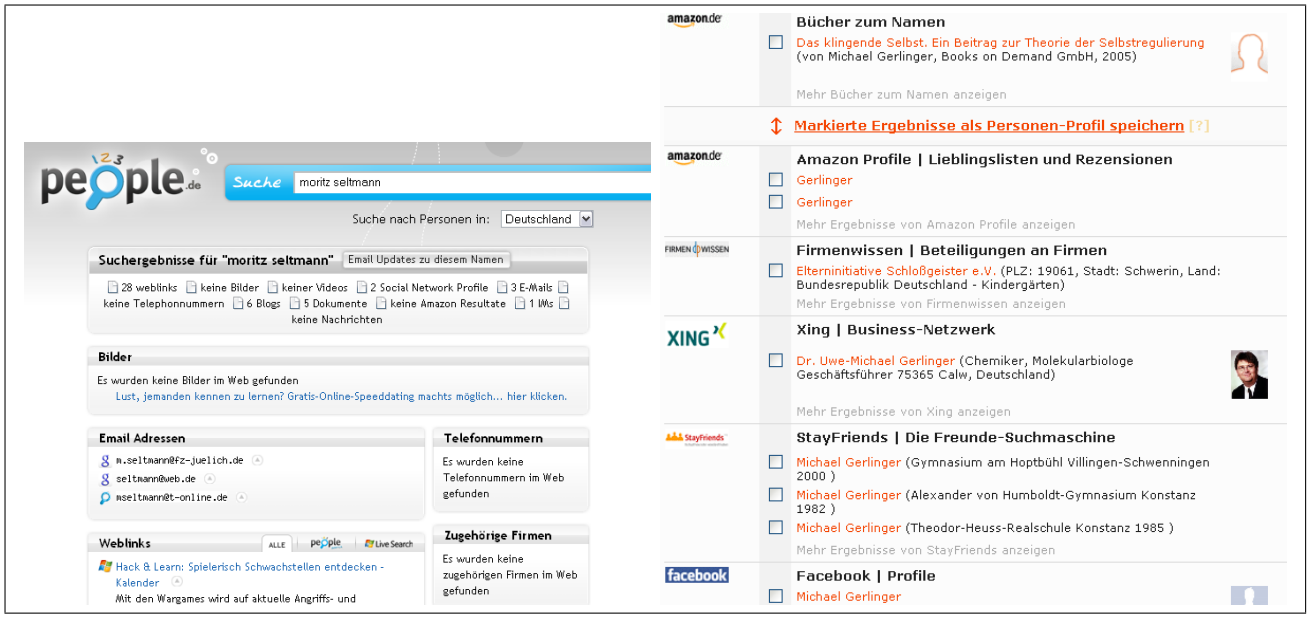

Abbildung 3: Personensuchmaschinen: 123people.de, yasni.de ;-)

3 Netzwerk Infrastruktur

Mithilfe diverser Tools können verschiedene Informationen über die Infrastruktur eines beliebigen Ziels ermittelt werden. Die einzelnen Tools wurden bereits im Skript näher erklärt. Hier nun eine Anwendungsmöglichkeit:

Durch Aufruf der Website „www.wieistmeineip.de“ erhält man die IP-Adresse des eigenen Internet-Anschlusses.

Abbildung 4: www.wieistmeineip.de

Nun könnte man z.B. mit `nmap -sP 88.67.133.216/24` ermitteln, welche Rechner sich sonst noch im selben Subnetz befinden.

```
beni@server:~$ nmap -sP 88.67.133.216/24

Starting Nmap 4.20 ( http://insecure.org ) at 2008-11-06 20:17 CET
Host dslb-088-067-133-079.pools.arcor-ip.net (88.67.133.79) appears to be up.
Host dslb-088-067-133-082.pools.arcor-ip.net (88.67.133.82) appears to be up.
Host dslb-088-067-133-104.pools.arcor-ip.net (88.67.133.104) appears to be up.
Host dslb-088-067-133-129.pools.arcor-ip.net (88.67.133.129) appears to be up.
Host dslb-088-067-133-151.pools.arcor-ip.net (88.67.133.151) appears to be up.
Host dslb-088-067-133-176.pools.arcor-ip.net (88.67.133.176) appears to be up.
Host dslb-088-067-133-179.pools.arcor-ip.net (88.67.133.179) appears to be up.
Host dslb-088-067-133-216.pools.arcor-ip.net (88.67.133.216) appears to be up.
Host dslb-088-067-133-243.pools.arcor-ip.net (88.67.133.243) appears to be up.
Nmap finished: 256 IP addresses (9 hosts up) scanned in 12.757 seconds
beni@server:~$
```

Abbildung 5: nmap, um die IP-Adressen aller Rechner im gleichen Subnetz zu ermitteln

Bei einem der Rechner könnte man mithilfe von GeoIP Diensten den Ort des Zugangknotens herausfinden.

Abbildung 6: GeoIP Dienst zur Standortsermittlung

Oder einfach mal die IP im Browser eingeben.

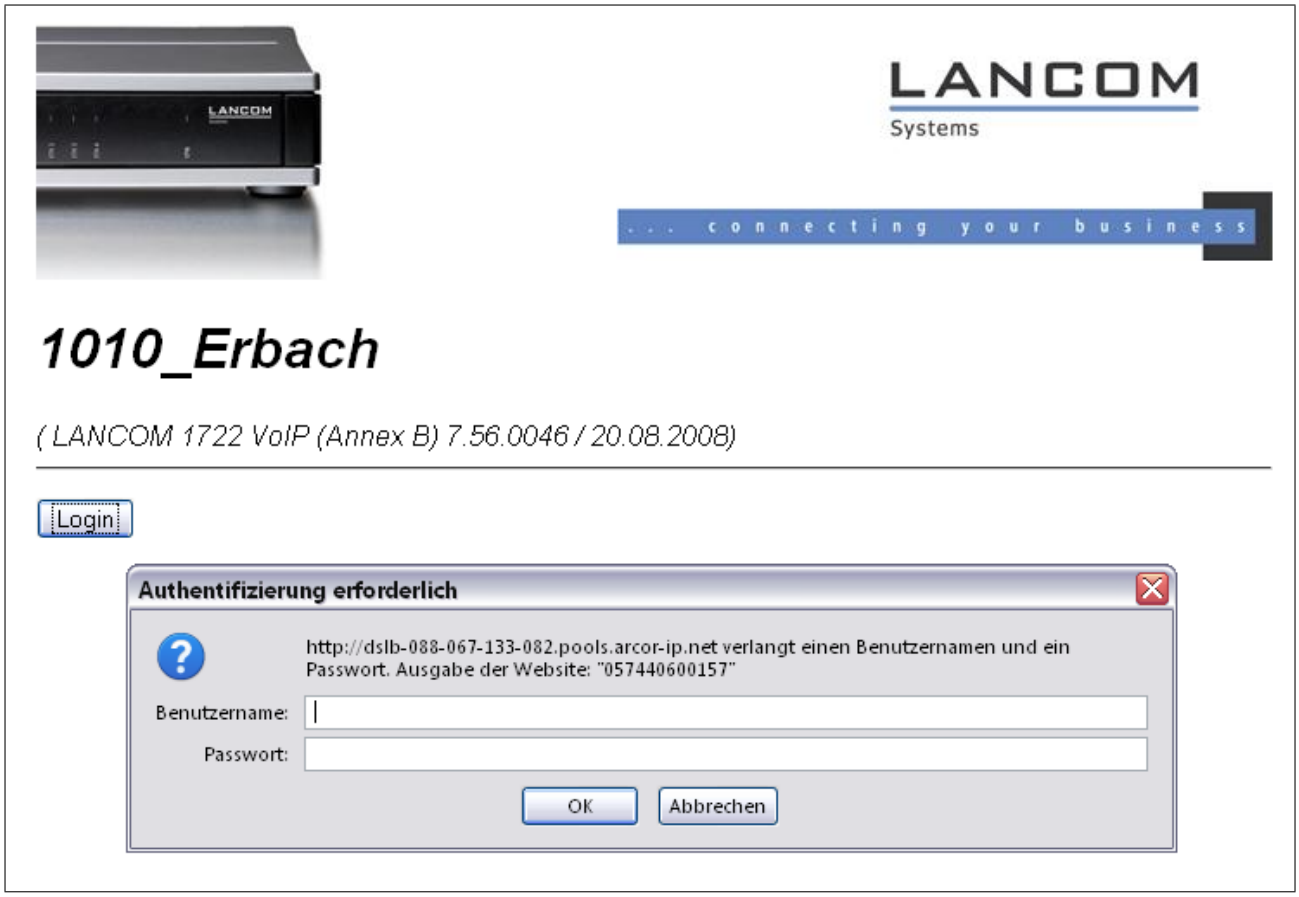

Abbildung 7: Admin-Login für VoIP Router

Vielleicht ist der Router schlecht konfiguriert und der Default Username und Passwort noch aktiv...

4 Fehlermeldungen

Fehlermeldungen in Produktivsystemen können unter Umständen viel Auskunft über den Quellcode oder Datenbankschema geben. Mithilfe der Google-Hacks (siehe 2) ist es relativ einfach solche Fehler zu finden.

Abbildung 8: SQL Statement gibt Auskunft über DB-Schema

4.1 Erkenntnis

In Produktivsystemen sollten keine Fehlermeldungen ausgeben werden und falls doch, nur kryptische Meldungen mit Fehlercode oder ähnlichem. Den LogLevel der Applikation auf die niedrigste Stufe setzen.

5 WebGoat: Code Quality

5.1 Hintergrundinformationen

Für Standard-Benutzer (ohne Login) der Website wird folgende Funktionalität angeboten: In einem Formular kann mithilfe einer Selectbox eine Datei, die sich auf dem Webserver befindet, ausgewählt werden. Durch Klick auf den Submit-Button wird die Datei ausgelesen und angezeigt.

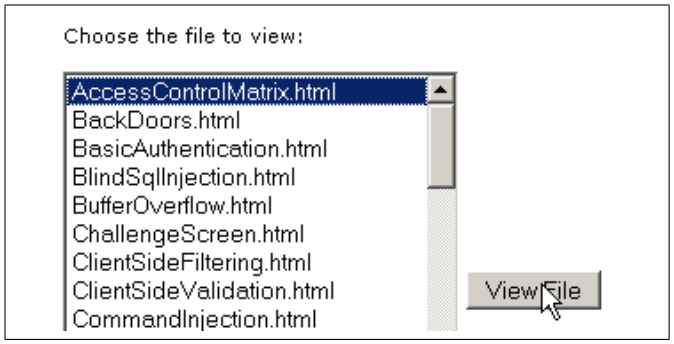

Abbildung 9: Formular zur Dateianzeige

5.2 Aufgabenstellung

Ziel der Übung ist es, Zugriff auf die Datei

`C:\WebGoat-5.2\tomcat\conf\tomcat-users.xml`

zu bekommen. Dabei könnten mögliche Schwachstellen in dem oben genannten Formular ausgenutzt werden.

5.3 Lösung/Durchführung

Zunächst wird der HTML-Quelltext mithilfe der Erweiterung „FireBug“ für den Mozilla Firefox Webbrowser untersucht. Auffällig ist, dass im Option-Tag der Select-Box als Value der Dateiname angegeben wird.

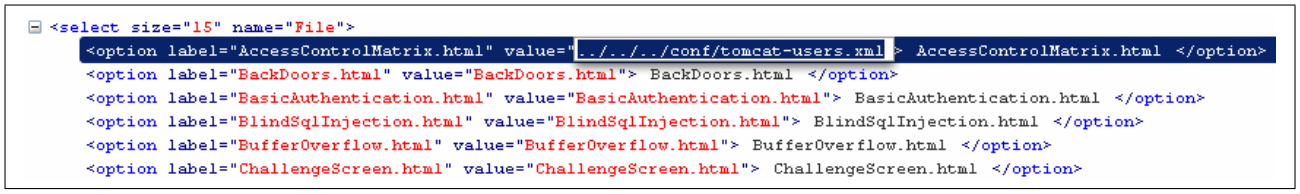

Abbildung 10: Formular zur Dateianzeige

Mithilfe der speziellen Ordnerbezeichnung „..“ kann in eine höher gelegene Ebene der Ordnerhierarchie im Dateisystem gewechselt werden.

Der Wert des Value-Attributes des ersten Eintrages der Select-Box kann nun entsprechend der gesuchten Datei angepasst werden: durch den Wert: „../../../conf/tomcat-users.xml“ wird in den entsprechenden Ordner gewechselt und die Datei ausgewählt (siehe Abbildung 10). Nach der Anpassung von dem HTML-Quelltext, wird nun der erste Eintrag der Select-Box ausgewählt und der Submit-Button angeklickt. Der Webserver liest das Value Attribut aus und zeigt die entsprechende Datei an.

Abbildung 11: Die Datei wurde angezeigt

5.4 Erkenntnis

Der Webserver untersucht den Wert des Value Attributs hinsichtlich der „..“-Zeichenkette nicht. Es wird angenommen, dass der Quelltext vom Benutzer nicht verändert wird. Diese Annahme ist leider falsch, da der Quelltext mit ganz einfachen Mitteln geändert werden kann. Um die Sicherheit der Applikation zu erhöhen, sollte grundsätzlich jeder eingelesene Wert, der vom Client gesendet wird, auf seine Gültigkeit hin untersucht und bei unerlaubten Zeichen entsprechend behandelt werden.

6 WebGoat: Access Control Flaws

6.1 Hintergrundinformationen

Der Bequemlichkeit wegen könnten (unseriöse) Entwickler für die Security eines Systems hochrelevante Daten als Kommentar in den Quelltext einfügen. Normalerweise ist dies kein Problem, da der Quellcode nicht für fremde Augen sichtbar ist. Bei HTML Quelltext ist dies allerdings anders. Alles was im HTML Text steht, wird lesbar zum Client übertragen - auch die Kommentare.

6.2 Aufgabenstellung

Ziel der Übung ist es, Zugang zu dem System durch Eingabe von Username und Passwort zu bekommen.

6.3 Lösung/Durchführung

Mithilfe der „FireBug“ Erweiterung des Mozilla Firefox Browsers wurde zunächst der Quelltext rund um das Login-Formular analysiert. Allerdings muss man bedenken, dass FireBug im Standard-Modus keine Kommentare anzeigt! Erst nach dem Aktivieren der Kommentare in den Optionen, wird das fahrlässige Handeln des Entwicklers sichtbar. Dieser hat Username und Passwort des Administrators in den HTML Quelltext eingetragen.

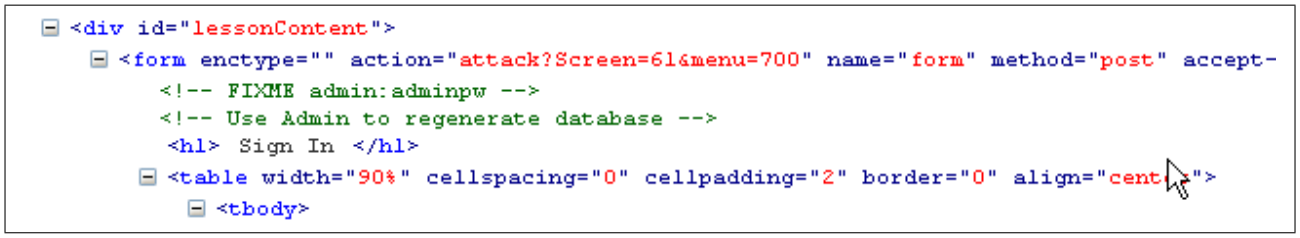

Abbildung 12: Credentials als HTML Kommentar

Abbildung 13: Der Login war erfolgreich

6.4 Erkenntnis

Niemals Credentials in den Quellcode schreiben. Testaccounts vor der Veröffentlichung der Applikation löschen. Beim Testen auf den Quelltext achten. Hierbei muss aber beachtet werden, dass das Tool für die Quelltext-Betrachtung manche Teile des Codes anders oder vielleicht gar nicht darstellt.