

Web Engineering

Blatt 1: Apache Webserver, HTTP

Aufgabe 1: Apache Webserver

Ich habe den Quellcode des Apache Webserver in der Version 2.0.55 heruntergeladen, übersetzt und auf der wsl31 im Linuxpool installiert. Anschließend habe ich an der Konfigurationsdatei „httpd.conf“ an drei Stellen folgende Änderungen vorgenommen:

Port auf den der Webserver hören soll

Listen 18080

IP-Bereich der auf den Webserver zugreifen darf

Allow from 134.60.0.0/16

Selbstauskunft im „Server“-Feld des Response Headers begrenzen auf „Server: Apache“

ServerTokens Prod

Dann habe ich im Dokumentenverzeichnis „htdocs“ eine Datei index.html und ein Bild apache_logo.gif abgelegt. Um den Webserver zu testen habe ich von einem anderen Rechner aus, per Firefox, lynx und netcat darauf zugegriffen. Als ich von einem Rechner außerhalb des Uni-Netzes zugreifen wollte, lieferte der Apache eine Fehlermeldung. Die Zugriffsbeschränkung schien also auch zu funktionieren. Da die laufenden Prozesse im Linuxpool in regelmäßigen Abständen beendet werden, habe ich die Serverantworten als Screenshot und Textausschnitt gesichert

Forbidden

You don't have permission to access / on this server.

Apache Server at wsl31.informatik.uni-ulm.de Port 18080



```
ff7@wsl01:~$ nc wsl31 18080
GET / HTTP/1.1
Host: wsl31
```

```
HTTP/1.1 200 OK
Date: Tue, 01 Nov 2005 16:16:52 GMT
Server: Apache
Last-Modified: Thu, 27 Oct 2005 19:44:51 GMT
ETag: "7fb0c4-3db-9b31b2c0"
Accept-Ranges: bytes
Content-Length: 987
Content-Type: text/html
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<title>Testinstallation Apache Webserver | Web Engineering WS05/06</title>
</head>
<body bgcolor="#333333" link="#FFFFFF">
<div align="center">
<p>&nbsp;</p>
<p></p>
<n><h><font size="4" color="#FFFFFF">Web Engineering | &luml;ungsblatt 1</font></h></n>
```

Aufgabe 2: HTTP Authentisierung

In der RFC 2616 wird bei der Frage der Authentisierung auf die RFC 2617 „HTTP Authentication: Basic and Digest Access Authentication,“ verwiesen. Dort werden die beiden Methoden „Basic“ und „Digest“ näher erläutert.

Basic Authentication

Sendet der Client einen Request für eine Resource die eine Authentisierung bedarf, so antwortet der Server mit dem Fehlercode 401 (Unauthorized) und einem Headerfeld „WWW-Authenticate: Basic realm="beliebigerString“. Je nach Browser wird nun nach einer UserID und einem Passwort gefragt. UserID und Passwort werden nach dem untenstehenden Schema kodiert und im Headerfeld „Authorization“ eines erneuten Requests an den Server geschickt.

Authorization: Basic basic-credentials

basic-credentials = base64-user-pass

base64-user-pass = <base64 [4] encoding of user-pass,

user-pass = userid ":" password

*userid = *TEXT excluding ":">*

*password = *TEXT*

Digest Access Authentication

Dieses Verfahren benutzt das Prinzip eines gemeinsamen Geheimnisses. Es ist im Gegensatz zur Basic Authentication nicht mehr notwendig die UserID und das Passwort im Klartext zu übertragen. Stattdessen sendet der Client eine MD5-Prüfsumme über folgende Werte:

username, the password, the given nonce value, the HTTP method, and the requested URI

Aufgabe 3: URI, URL, URN

1. URI (URL): <http://wsl31.informatik.uni-ulm.de/index.html>
2. URI (URL): <ftp://flerli.de@ftp2.kontent.de/www/>
3. URI (URN): URN:ISBN:0-395-36341-1