

Übungsblatt 02

Thomas Samy Dafir, Lex Winandy

Aufgabe 1

Gruppe: Konfigurieren Sie im Webserver einen VirtualHost, der auf port 8765 lauscht. Erstellen Sie ein separates DocumentRoot für diesen VirtualHost.

Aufgabe 2

Erstellen Sie eine passwortgeschützte URL. Verwenden Sie digest authentication. Was ist der Unterschied zu plain. Hinweis: .htaccess, mod_auth_digest.

Funktion: Der Client sendet eine Anfrage an den Server. Dieser antwortet mit "not authorized" und sendet einen einmal gültigen Zufallswert mit. Der Client wird zur Passworteingabe aufgefordert. Der User authentifiziert sich. Der Client sendet einen neuen Request, jetzt aber mit einem zusätzlichen Header: WWW-Authenticate. Enthält User, realm, qop, den Zufallswert und das gehashte Passwort: MD5 :(. Der Server vergleicht mit den Daten im Passwortfile und sendet entweder 200 OK oder wiederum 401 not authorized. Unterschied zu basic: password wird gehashed übertragen. Benötigte Module: mod_auth_digest + mod_authn_file, für User/Password file.

Verwendung:

1. Optionen für Modul spezifizieren (2 Möglichkeiten):
 - Über Directory Eintrag in der Apache config
 - Über eine .htaccess Datei im zu schützenden Verzeichnis
2. Datei mit "user:realm:password_hash" erstellen:
htdigest [-c] passwdfile realm username
Der Pfad zu "passwdfile" muss dann im .htaccess file angegeben werden

Settings:

- AuthType: Authentication Type (digest/basic)
- AuthName: Realm name. Muss mit realm im password-file übereinstimmen.
- AuthDigestAlgorithm: Hash Algorithmus (MD5)

- AuthDigestNonceLifetime: Zeitraum für den der aktuelle Zufallswert gültig ist (in s)
- AuthDigestDomain: Domains für die diese Authentifizierung gültig ist
- AuthDigestQop: Quality of Protection. Nur username/passwort oder + integrity check
- AuthUserFile: Pfad zum password file
- Require: Gibt Voraussetzungen für Zutritt an: all granted, alldened, valid-user(mit pwd file), user, group.

Aufgabe 3

Machen Sie sich mit dem Firefox Web Developer vertraut, insb. mit der 'Network' Ansicht. Öffnen Sie eine grössere Seite (z.B. www.uni-salzburg.at) welche HTTP Status Codes treten auf? Was bedeuten Sie?

Site: uni-salzburg.at

Statuscodes:

- 200 OK: Angefragter Inhalt wird ausgeliefert.
- 301 Moved Permanently: Permanenter Redirect. In diesem Fall eine Weiterleitung vom Port 80 (http) auf Port 443 (https). Erst danach wird der content ausgeliefert.
- 302 Moved Temporarily: Redirect auf definierte Error-Seite bei request einer nicht vorhandenen datei.
- 404 Not Found: Tritt nie auf. Immer redirect auf eine vordefinierte Error Seite.

Aufgabe 4

Wie sind HTTP 1.1 request und response prinzipiell aufgebaut? Illustrieren Sie mit einem eigenen Beispiel!

Aufbau:

Request = Request-Line
headers

CRLF
message body

Request-Line = Method SP Request-URI SP HTTP-Version CRLF
Method = "PUT" | "GET" | "POST" |
RequestURI = Pfad zur angefragten Datei
HTTP-Version = Protokoll version

headers = Accept-* | Authorization | Expect | From | Host
| User-Agent | Max-Forwards | cache-control |....

Response = Status-Line
headers
CRLF
message-body

Status-Line = HTTP-Version SP Status-Code SP Reason-Phrase CRLF
Status-Code = "1xx", "2xx", "3xx", "4xx", "5xx"
Reason-Phrase = "OK", "Not Found", "Permanent Redirect"

headers = Accept-Ranges | Age | ETag | Location | Proxy-Authenticate
| Retry-After | Server | Vary | WWW-Authenticate |....

Beispiele (apple.com):
Request:

Request URL:https://www.apple.com/
Request Method:GET
Accept:text/html,application/xhtml+xml,application/xml;q=0.9,
image/webp,image/apng,*/*;q=0.8
Accept-Encoding:gzip, deflate, br
Accept-Language:en-GB,en-US;q=0.9,en;q=0.8
Cache-Control:max-age=0
Connection:keep-alive
Host:www.apple.com
Upgrade-Insecure-Requests:1
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/64.0.3282.186 Safari/537.36 OPR/51.0.2830.55

Response:

Status Code:200 OK
Cache-Control:max-age=0
Connection:keep-alive
Content-Encoding:gzip
Content-Length:6434
Content-Type:text/html; charset=UTF-8
Date:Wed, 14 Mar 2018 13:02:58 GMT
Expires:Wed, 14 Mar 2018 13:02:58 GMT
Server:Apache
Vary:Accept-Encoding
X-Content-Type-Options:nosniff
X-Frame-Options:SAMEORIGIN
X-Xss-Protection:1; mode=block

Quelle: <https://www.w3.org/Protocols/rfc2616/rfc2616-sec5.html>

Aufgabe 5

Gruppe: Was bedeuten folgende Felder im HTTP request und response header? DNT, Connection: keep-alive, ETag, Content-Length

Aufgabe 6

Gruppe: Wie unterscheidet sich HTTP 1.1 von HTTP/2? Wie wird ausgehandelt welches Protokoll gesprochen wird? Zeichnen Sie den Netzwerkverkehr auf Hinweis: tcpdump + Wireshark oder Web Developer