RUB

SHORTGUIDE
ZUGRIFFSBESCHRÄNKUNG AUF ZENTRALEN WEBSERVERN

FÜR MITGLIEDER UND ANGEHÖRIGE DER RUB

Grundlagen

Es gibt zwei verschiedene Möglichkeiten, Zugriffsbeschränkungen für WWW-Seiten auf den Servern der Ruhr-Universität zu realisieren. Zum einen über Benutzername und Passwort und zum anderen über die IP-Adresse des Rechners, der eine WWW-Seite anfordert. Bei beiden Möglichkeiten wird immer eine Datei mit dem Namen .htaccess benötigt. In dieser Datei wird die Art der Zugriffsbeschränkung festgelegt. Bei der Zugriffsbeschränkung durch Benutzername und Passwort muss zusätzlich die Datei .htpasswd, die Benutzernamen und verschlüsselte Passwörter enthält, erstellt werden.

Grundsätzlich müssen beide Dateien als reine Textdateien vorliegen. Nehmen Sie zum Editieren ein geeignetes Programm wie den Windows Editor Notepad oder jeden anderen Text-Editor und speichern Sie die Dateien als Textdateien ohne Endung bzw. entfernen Sie die Dateiendung nach dem Speichern.

Nach dem Editieren müssen Sie die Datei(en) mit einem beliebigen SFTP-Programm auf den Webserver laden. Die Datei .htaccess steuert nun den Zugriff auf das Verzeichnis, in dem sie liegt. Die Einstellungen gelten auch für etwaige Unterverzeichnisse und dort vorhandene Dateien, sofern dort keine weitere .htaccess Datei mit anderen Einstellungen liegt. Sie können auch einzelne Dateien mit einer Zugriffsbeschränkung belegen (siehe Seite 3).

Auf dem Homepage- und dem WWW-Server läuft als Webserver Apache.

ZUGRIFFSBESCHRÄNKUNGEN EINRICHTEN

Zugriffsbeschränkung durch Benutzername und Passwort

Zunächst sollten Sie die Datei .htpasswd erstellen. In diese Datei tragen Sie zeilenweise Benutzername und dazugehöriges verschlüsseltes Passwort, jeweils durch einen Doppelpunkt getrennt, ein. Hier ein Beispiel:

```
Benutzer1:p8KRGXDSQX/qQ
Benutzer2:p8lX4erUUYGJI
```

Zur einfachen Erstellung eines verschlüsselten Passworts haben wir folgendes Skript auf unseren Seiten bereitgestellt: https://www.ruhr-uni-bochum.de/system/tools/htpasswd
Geben Sie den gewünschten Benutzernamen und das gewünschte Passwort in das Formular ein, drücken Sie die Eingabetaste und kopieren Sie das nun angezeigte verschlüsselte Passwort in die Datei .htpasswd. Nun sollten Sie die Datei .htaccess erstellen. Hier ein Beispiel

```
AuthName "Name des geschützten Bereiches"
AuthType Basic
AuthUserFile /var/www/html/loginid/webseite/.htpasswd
Require valid-user
#oder
Require user Benutzername
```

Zur Erläuterung:

Zeile 1: Geben Sie in Anführungsstrichen einen frei wählbaren Namen für den geschützten Bereich ein. Dieser Name wird beim Aufrufen des geschützten Bereiches im Eingabefenster für Benutzername und Passwort angezeigt. Einige Browser speichern das Passwort unter diesem Namen ab.
Zeile 2: Übernehmen Sie diese Zeile ohne Änderungen.
Zeile 3: Hier muss der vollständige Pfad zur Datei .htpasswd angegeben werden. Die häufigste Fehlerquelle bei der Zugriffsbeschränkung durch Benutzername und Passwort liegt an dieser Stelle an einer falschen Pfadangabe. Da die Server auf einem UNIX System laufen, muss die Pfadangabe mit dem Slash ("/") und nicht mit Backslash ("\") gebildet werden.
Die Regeln zur Bildung der vollen Pfadangabe:

- Funktionsmailboxen mit Webspace
`/var/www/html/`**`loginid`**`/`**`webseite`**`/evtl. `**`Unterverzeichnis(se)`**`/.htpasswd`

- für den Homepageserver
/home/www/home/erster Buchstabe LoginID/LoginID/evtl. Unterverzeichnis(se)/.htpasswd
Beispiel: `/home/www/home/p/passembk/geheim/.htpasswd`

Zeile 4: Hier legen Sie schließlich fest, welche Benutzer Zugriff auf die geschützten Seiten haben sollen. Wenn Sie „Require valid-user“ eintragen, werden alle in der Datei .htpasswd erfassten Benutzer akzeptiert. Sie können auch einzelne Benutzer auswählen, indem Sie zuerst das Wort „user“ und dann deren Benutzernamen an Stelle von „valid-user“ durch Leerzeichen getrennt eintragen.

Zugriffsbeschränkung durch IP-Adresse bzw. Host

Neben der Zugriffsbeschränkung durch Benutzername und Passwort ist auf den WWW-Servern eine Zugriffsbeschränkung anhand von IP-Adressen möglich. So können Sie zum Beispiel den Zugriff auf Ihre WWW-Seiten nur für Rechner mit einer IP-Adresse der Ruhr-Universität Bochum oder nur für Rechner aus dem Subnetz Ihrer Einrichtung erlauben.

Ebenso wie für die Zugriffsbeschränkung durch Benutzername und Passwort müssen Sie für die Zugriffsbeschränkung durch IP-Adresse die Datei .htaccess anlegen, editieren und in das gewünschte Verzeichnis Ihrer WWW-Präsenz laden.

Hier ein Beispiel für die Einträge zur Zugriffsbeschränkung durch IP-Adresse für die Datei .htaccess (wenn Sie bereits eine Zugriffsbeschränkung durch Benutzername und Passwort eingerichtet haben, fügen Sie die Angaben bitte am Ende der Datei ein):

```
Require all denied
Require ip 134.147.128.0/24
Require ip 2a05:3e00:2:1000::/52
```

Generell gibt es für die Zugriffsbeschränkung durch IP-Adresse zwei Direktiven zur Zugriffssteuerung: **Require all denied** (verbieten) und **Require all granted** (zulassen). Durch die erste Zeile unterbinden Sie aus Sicherheitsgründen den Zugriff auf das Verzeichnis und die darin liegenden Dateien, um dann nur den in der zweiten Zeile definierten Rechnern Zugriff zu geben. In unserem Beispiel ist dies das gesamte Subnetz 134.147.128.0/24.

Neben Subnetzen können Sie auch komplette IP-Adressen verwenden. Zudem können Sie mehrere „Require“-Einträge vornehmen.

Zugriffsbeschränkung auf RUB-intern bei IPv6 und IPv4

Seit Einführung der IPv6-Adressen in großen Teilen der RUB muss für eine uniinterne Zugriffsbeschränkung mehr konfiguriert werden, als nur den IP-Bereich 134.147.0.0/16 freizugeben.

Alle Rechner der RUB, die über IPv4 ins Internet gelangen, haben eine IP-Adresse aus dem Class-B Netz 134.147.0.0/16. Dies gilt ebenfalls für externe Rechner, die sich über eine VPN-Verbindung ins Hochschulnetz verbinden.

```
Require all denied
<RequireAny>
     # Netze können in CIDR angegeben werden
     Require ip 134.147.0.0/16
     # Oder als Subnetzmaske
     Require ip 134.147.0.0 255.255.0.0
     Require ip 2a05:3e00::/44
     Require ip 10.0.0.0/8
</RequireAny>
```

Weitere Informationen über **IPv6** finden Sie unter https://noc.rub.de/web/ipv6 und über **CIDR** unter https://de.wikipedia.org/wiki/Classless_Inter-Domain_Routing.

Kombination der beiden Arten der Zugriffsbeschränkung

Eine sinnvolle Kombination von Zugriffsbeschränkung durch IP-Adresse und Benutzername / Passwort ist folgender Fall:

Sie möchten den Zugriff auf Ihre WWW-Präsenz von Ihrem Institut aus uneingeschränkt erlauben, von außerhalb aber automatisch Benutzername und Passwort abfragen, damit ausgewählte Benutzer die Informationen auch außerhalb Ihrer Einrichtung mit Benutzername und Passwort abrufen können. Legen Sie wie beschrieben die Dateien .htpasswd und .htaccess an.
Durch diesen Eintrag „**Require all denied**“ werden zunächst alle Zugriffe gesperrt. Mittels „**Require valid-user**“ in Verbindung mit der Datei .htpasswd wird ein Login-Fenster gezeigt. Werden in das Formular die richtigen Daten eingeben wird der Zugriff gewährt. Ebenfalls Zugriff OHNE Benutzerabfrage erhalten die Rechner im Adressbereich 134.147.128.0/24 und 2a05:3e00:2:1000::/52.

Beispiel für die Datei .htaccess:

```
AuthName "Name des geschützten Bereiches"
AuthType Basic
AuthUserFile /var/www/html/loginid/webseite/.htpasswd
Require all denied
Require valid-user
Require ip 134.147.128.0/24
Require ip 2a05:3e00:2:1000::/52
```

Alle Rechner in den angegebenen Netzen können die Dateien ohne Benutzereingabe anzeigen. Bei allen anderen Rechnern wird der Benutzer zur Eingabe von Benutzername und Passwort aufgefordert. Akzeptiert werden alle Benutzer/ Passwort-Kombinationen aus der Datei, die mit dem Eintrag „AuthUserFile“ bestimmt wird.

Zugriffsbeschränkung für ausgewählte Dateien

Wenn Sie nur ausgewählte Dateien mit einer Zugriffsbeschränkung belegen möchten nutzen Sie bitte folgendes Beispiel für die Datei .htaccess:

```
Require all denied
<Files "strengGeheimeStrategie.ppt">
        AuthName "Bitte anmelden"
          AuthType Basic
          AuthUserFile /var/www/html/loginid/webseite/.htpasswd
          <RequireAll>
               Require valid-user
               Require ip 134.147.128.0/24
               Require ip 2a05:3e00:2:1000::/52
          </RequireAll>
</Files>
```

Geben Sie in **Zeile 2** den Namen der zu schützenden Datei an. Alle zwischen **<FilesMatch Dateiname>** und **</Files>** eingetragenen Einstellungen gelten nur für den angegebenen Dateinamen.

Bei Fragen & Problemen

Bei Fragen und Problemen können Sie sich an unseren Helpdesk wenden: its-helpdesk@ruhr-uni-bochum.de.

IT.SERVICES | Stand: 07. Mai 2019