Upload mit Virenprüfung

Dieses HowTo ist zwar auf den Upload über HTML Formulare spezialisiert, doch nach dem Bearbeiten dieses HowTos solltet ihr außerdem in der Lage sein auch Ordner nach Viren zu prüfen.

Als Voraussetzung benötigt ihr die Blibliothek php5-clamavlib. Wenn ihr über eine aktuelle Debian Distribution verfügt, könnt ihr das Paket mit einem Paketmanager installieren. Abhängigkeiten wie der eigentliche Virenscanner ClamAV werden dann automatisch gelöst.

Hier z.B. die Installation auf einem aktuellen Ubuntu:

sudo apt-get install php5-clamavlib
Paketlisten werden gelesen... Fertig
Abhängigkeitsbaum wird aufgebaut
Reading state information... Fertig
Die folgenden zusätzlichen Pakete werden installiert:
libclamav1 libgmp3c2
Vorgeschlagene Pakete:
clamav-freshclam
Die folgenden NEUEN Pakete werden installiert:
libclamav1 libgmp3c2 php5-clamavlib
0 aktualisiert, 3 neu installiert, 0 zu entfernen und 0 nicht aktualisiert.
Es müssen 714kB Archive geholt werden.
Nach dem Auspacken werden 1315kB Plattenplatz zusätzlich benutzt.
Möchten Sie fortfahren [J/n]=]

Nach der Installation startet ihr am besten den Server neu

Quellcode

```
1. /etc/init.d/apache2 restart
```

Wenn die Installation erfolgreich war stehen euch in PHP neue Funktionen zur Verfügung.
Da wären z.B. cl_info, cl_scanfile, cl_scanbuff, cl_setlimits, cl_scanfile_ex, cl_scanbuff_ex, cl_pretcode, clam_scan_buffer, clam_scan_file, clam_get_version.

Da die Funktion einen String zurück gibt, verwendet ihr am besten clam_get_version() um die korrekte Installation sicherzustellen.

Inhaltsverzeichnis

Upload Formular

Im nächsten Schritt erstellen wir das Upload Formular.

Bis auf die Zeilen 4 und 5 sollte das Script klar sein. Die Zeilen 4 und 5 werden später erläutert.

Quellcode

```
1. <?php
2. if(isset($_POST)) {
3. 
4. cl_setlimits(5, 1000, 200, 0, 10485760);
5. if($clamav = cl_scanfile($_FILES['datei']['tmp_name']))
6. die('Virus gefunden: '.$clamav.'<br />ClamAV version: '.clam_get_version());
```

```
7. else {
8. move_uploaded_file($_FILES['datei']['tmp_name'], $_FILES['datei']['name']);
9. echo "Datei erfolgreich hochgeladen";
10. }
11. }
12. }
13. ?>
14. <html>
15. <head>
16. <title>Datei Upload mit automatischer Virenprüfung</title>
17. </head>
19. <body>
20. <form method="post" enctype="multipart/form-data">
23. <input type="file" name="datei" />
24. <input type="submit" />
26. </form>
27. </body>
28. </html>
```

Alles anzeigen

Der Konstruktur von cl_setlimits sieht im Einzelnen wie folgt aus: cl_setlimits($maxreclevel, $maxfiles, $maxratio, $archivememlim, $maxfilesize)

- $maxreclevel: Maximaler Rekursionslevel (beim Scannen von Ordnern)
- $maxfiles: Maximale Anzahl an Dateien die gescannt werden sollen
- $maxratio: Maximale Kompressionsstufe
- $archivememlim: Begrenze die Speichernutzung für bzip2 (true/false)
- $maxfilesize: Nur die ersten * Bytes von Dateien werden gescannt.

Weblinks

- howtoforge.com/scan_viruses_with_php_clamavlib
- clamav.net/doc/0.88.4/html/node41.html