



Übungsaufgaben:

- 1) Informieren Sie sich die unter der URL

`http://www.karzauninkat.com/Goldhtml/goldhtml.htm`

über die schlimmsten Fehler bei der Gestaltung von HTML-Seiten.

- 2) Unter der URL

`http://www.drweb.de/php/php_kurs.shtml`

finden Sie einen kleinen PHP-Kurs von Jochen Stärk. Laden Sie sich das Archiv (in ein Unterverzeichnis Ihres Homeverzeichnis auf dem IT-Cluster) herunter, entpacken Sie es mit dem Kommando `unzip phptutorial.zip`, und arbeiten Sie den Kurs durch!

Praktikumsaufgaben:

Datenbankanbindung des Websystems (MySQL/PHP):

- a) • Überprüfen Sie die Installation und den Status des Datenbank-Managementsystems MySQL unter Verwendung des Kommandos **rmysql**.
- Überprüfen Sie die korrekte Installation des PHP4-Moduls im Webserver *apache*. Beachten Sie dabei auch die Mime-Type-Zuordnungen.

Hinweis: Für die weitere erfolgreiche Teilnahme an den Übungen ist es erforderlich, eMail in zertifizierter Form versenden zu können; nicht unterzeichnete eMails können nicht bewertet werden. Die *folgenden Aufgaben* sind daher von *jeder* an den Übungen teilnehmenden *Person* (und nicht für jede Gruppe) durchzuführen!

X.509 (S/MIME) Zertifikate (**Bonuspunkte!**):

- b) Schaffen Sie die Voraussetzungen für S/MIME-unterzeichnete und -verschlüsselte eMail:

- Beantragen Sie ein (kostenloses TC Express) X.509 Zertifikat unter der URL
`http://www.trustcenter.de/`
- Besorgen Sie sich mit Hilfe der Suchfunktion des Trustcenters oder unter der URL
`http://www.math.uni-wuppertal.de/~fpf/`
den öffentlichen Schlüssel von P. Feuerstein.
- Schicken Sie ihm (an die Adresse `fpf@math.uni-wuppertal.de`) eine verschlüsselte (encrypted) *und* unterzeichnete (signed) eMail.
- Konfigurieren Sie den Webserver *apache* auf ihrer VMware Linux Installation derart, daß Dateien mit der Extension *.der* durch den Webserver dem Mime-Type *application/x-x509-email-cert* zugeordnet werden. Ändern Sie zu diesem Zweck die entsprechende Datei im Verzeichnis `/etc/httpd/`.
- Ergänzen Sie jeweils Ihre persönliche Homepage auf Ihrer Website um einen Link auf Ihren öffentlichen Schlüssel und um den zugehörigen Fingerprint (MD5).

Pretty Good Privacy (PGP) (*Bonuspunkte!*):

c) Schaffen Sie die Voraussetzungen für die PGP-Verschlüsselung von Dateien:

- Erzeugen Sie sich ein RSA Schlüsselpaar (der Länge 1024 Bit) zum Verschlüsseln und Entschlüsseln von Dateien.
- Extrahieren Sie Ihren öffentlichen Schlüssel in eine ASCII-Datei, um ihn bei Bedarf weitergeben zu können.
- Besorgen Sie sich die öffentlichen Schlüssel von H.-J. Buhl und P. Feuerstein von deren Homepages und fügen Sie diese Schlüssel Ihrem öffentlichen Schlüsselring zu.

Information:

Unter folgenden URLs finden sie neue Informationen über Sicherheitslücken und Datenschutz-Probleme:

<http://www.heise.de/newsticker/data/dab-06.01.04-000/>

<http://www.heise.de/newsticker/data/dab-07.01.04-000/>

Ende der Bearbeitungszeit: 20. Januar 2004