Filtern von Spam-Mails direkt auf dem Server

Von Lars Witter (Vorstand Mabi) Marburg, den 18.08.2003

Seit etwa 3 Monaten betreiben wir auf den Mabi-Mail-Servern eine Spamerkennungssoftware, der eingehende E-Mails nach verschiedenen Spam-Kriterien durchsucht und bewertet. Dieser Filter fügt in jeder als Spam erkannten Mail einige, normalerweise nicht sichtbare Zeilen im Mailheader (Kopfzeile) ein. Diese Einträge im Mailheader können durch Filterregeln, sowohl bereits auf dem Server wie auch im E-Mail-Programm, zur Aussortierung von Spam genutzt werden. Im folgenden die Beschreibung für das Anlegen von Filterregeln direkt auf dem Server
Nähere Informationen zu der Spamerkennungssoftware erhalten Sie unter: http://www.spamassassin.org/index.html

Hier mal ein Auszug aus einer als Spam erkannten und markierten E-Mail

```
X-Spam-Flag: YES
X-Spam-Status: Yes, hits=12.5 required=5.0
        tests=HTML_30_40,HTML_FONT_BIG,HTML_FONT_COLOR_RED,HTML_MESSAGE,
            MIME_HTML_NO_CHARSET,MIME_HTML_ONLY,MISSING_MIMEOLE,
            MISSING_OUTLOOK_NAME,NORMAL_HTTP_TO_IP,PENIS_ENLARGE,
            PENIS_ENLARGE2,RATWARE_EGROUPS,RCVD_IN_NJABL,
            RCVD_IN_UNCONFIRMED_DSBL
        version=2.55-hgmdevnull
X-Spam-Report:   ---- Start SpamAssassin results
 12.50 points, 5 required;
 *  4.3 -- Bulk email software fingerprint (eGroups) found in headers
 *  1.4 -- BODY: Information on getting a larger penis or breasts
 *  1.3 -- BODY: Information on getting a larger penis or breasts (2)
 *  0.9 -- BODY: Message is 30% to 40% HTML
 *  0.1 -- BODY: HTML font color is red
 *  0.1 -- BODY: HTML included in message
 *  0.3 -- BODY: FONT Size +2 and up or 3 and up
 *  0.8 -- RAW: Message text in HTML without specified charset
 *  0.7 -- URI: Uses a dotted-decimal IP address in URL
 *  0.9 -- RBL: Received via a relay in dnsbl.njabl.org
 [RBL check: found 233.81.233.219.dnsbl.njabl.org., type: 127.0.0.9]
 *  0.5 -- RBL: Received via a relay in unconfirmed.dsbl.org
 [RBL check: found 233.81.233.219.unconfirmed.dsbl.org.]
 *  0.1 -- Message only has text/html MIME parts
 *  0.5 -- Message has X-MSMail-Priority, but no X-MimeOLE
 *  0.6 -- Message looks like Outlook, but isn't
 ---- End of SpamAssassin results
X-Spam-Level: ************
X-Spam-Checker-Version: SpamAssassin 2.55-hgmdevnull (1.174.2.19-2003-05-19-exp)
```

Ist die E-Mail womöglich Spam?
Highscore der ermittelten Punkte.

Im folgenden eine Übersicht über die Bewertung der E-Mail.

Ein Spamfilter durchsucht die E-Mails nach bestimmten Kriterien wie z.b.

- Schriftgröße
- Stil (HTML-/Text-E-Mail)
- “verbotene” Worte z.b. Sex, Penis
- Absendeadresse

All diese Kriterien werden wenn sie zustimmen mit Punkten bewerten und am Ende werden alle Punkte addiert.

Wie man an diesem Auszug erkennen kann hat die E-Mail die „volle“ Punktzahl um mehr als das doppelte überschritten.

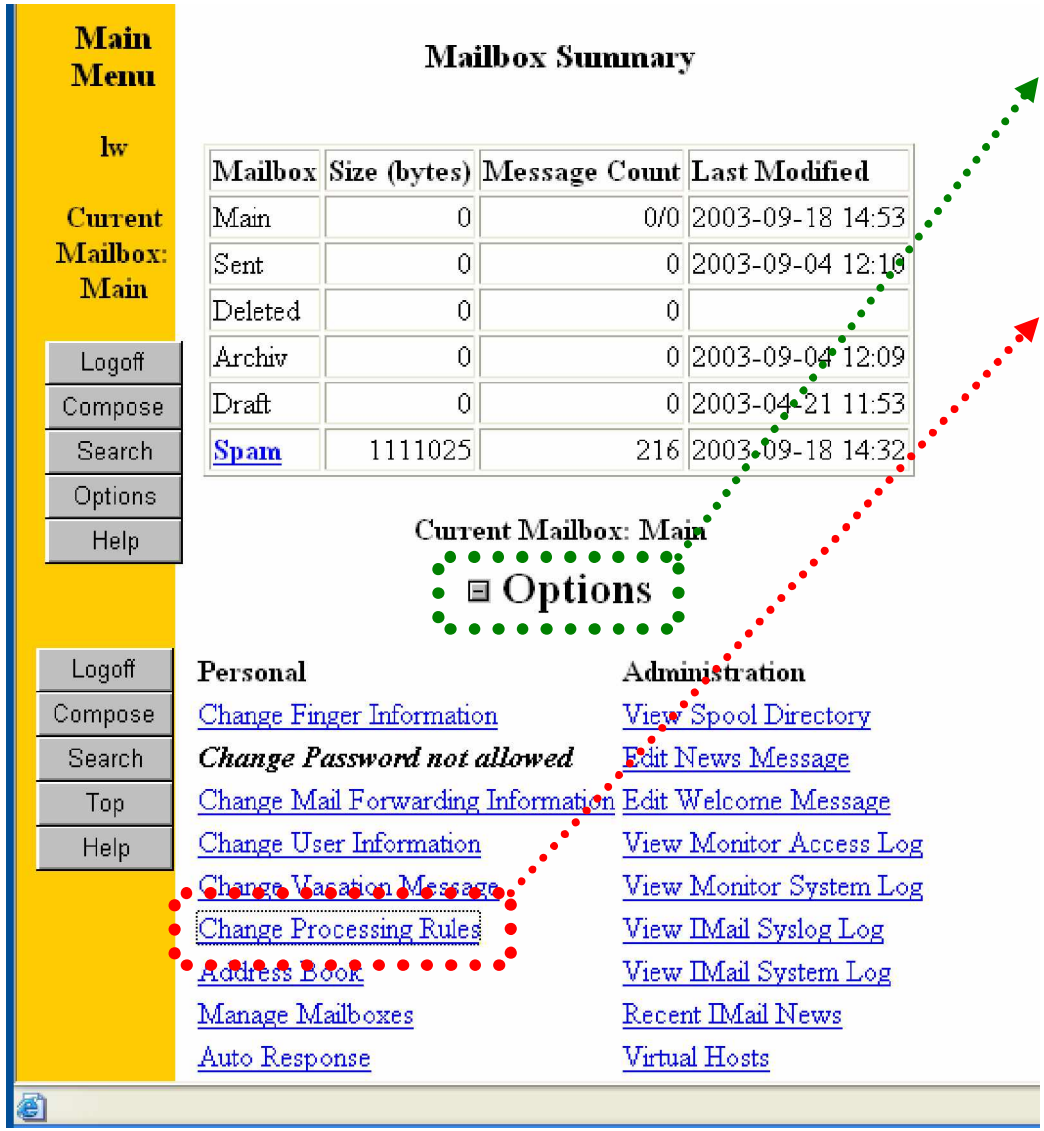
Mit „volle“ Punktzahl ist die Punktzahl gemeint die man angeben kann, ab wann eine Mail als Spam erkannt wird.

Eine E-Mail, die 4.9 Points erreicht wird nicht als Spam erkannt, erst ab 5 Punkten ist sie laut unserer (und der von Spamassassin) Definition Müll.

Genauere Informationen können unter o.g. Adresse nachgelesen werden.

So, dann wollen wir mal eine Filterregel anlegen.

Der Start, wie gewohnt **mail.mabi.de** im Browser öffnen und Anmeldedaten eingeben – danach erscheint dieses Fenster

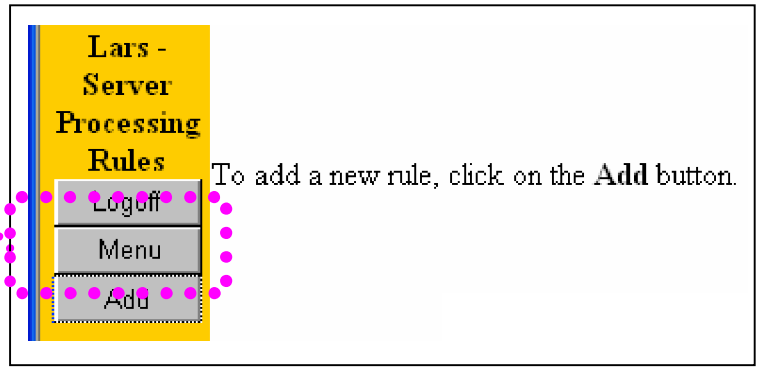


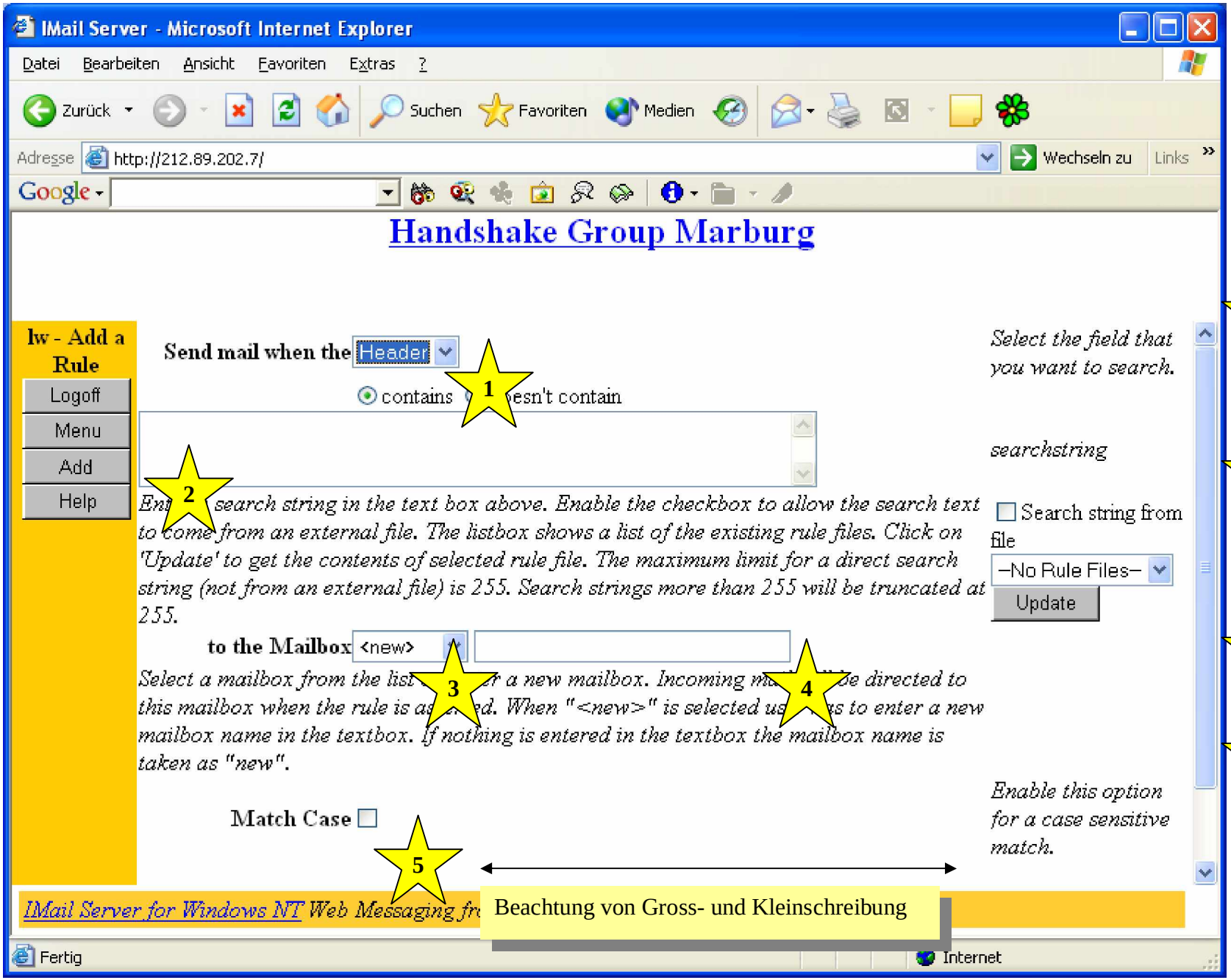
Eventuell hier - falls ein „+“ vor „Options“ steht - anklicken um die Optionen anzuzeigen

Nun folgt man diesem Link

Hier werden dann die entsprechenden Filter gesetzt oder geändert.

Im neu erscheinenden Dialog auf diese Schaltfläche klicken





Beachtung von Gross- und Kleinschreibung

Auf dieser Seite kann nach allem was eine E-Mail hergibt gefiltert und sortiert werden.

Wir wollen Spam filtern, den der Spamassassin als Müll erkannt hat.

1 Hier wird **Header** ausgewählt, da das zu suchende Kriterium sich im Email-Header befindet.

2 Eingabe des Kriteriums: **X-Spam-Flag: YES** (So werden Spam-Mail markiert)

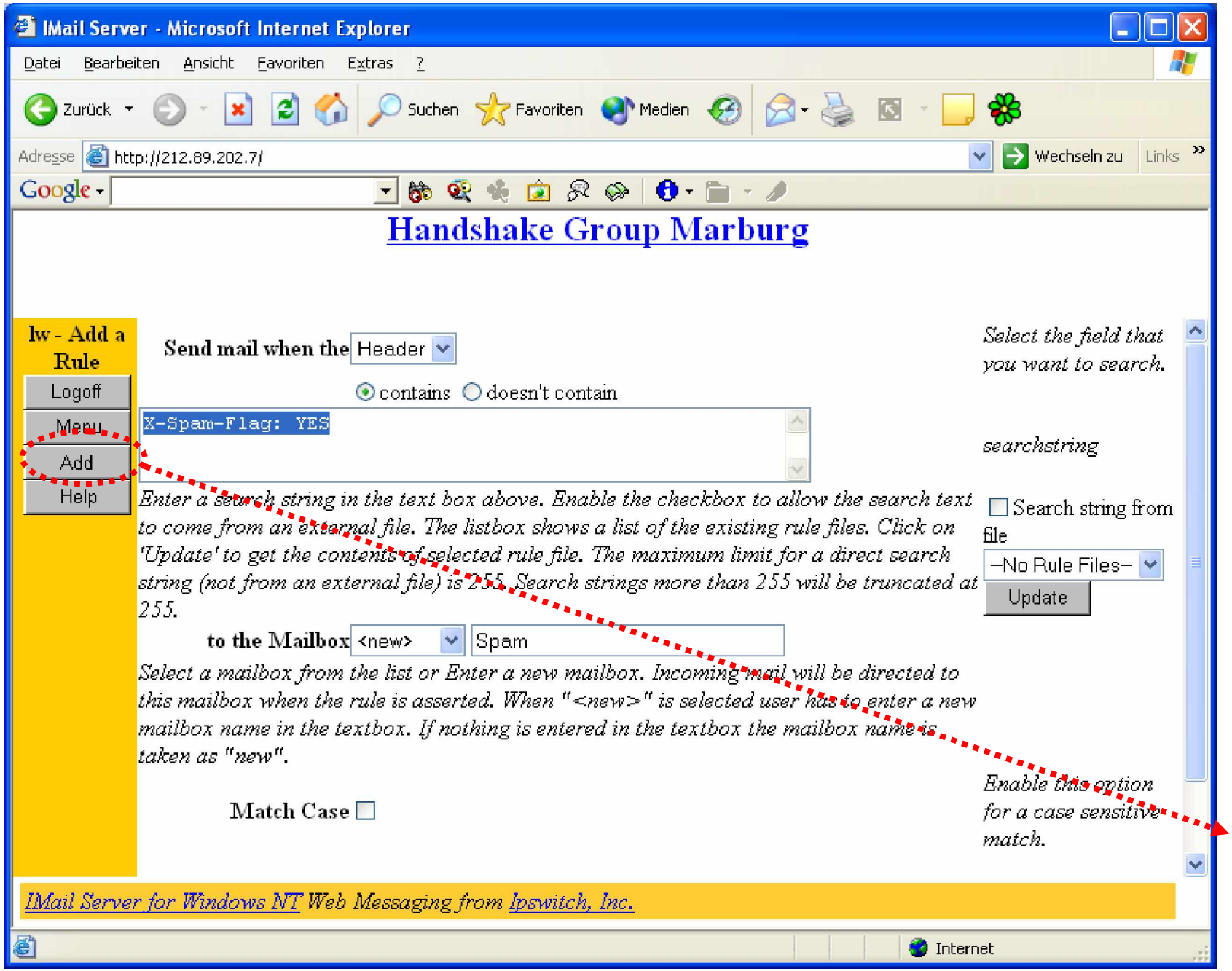
3 Hier stehen mehrere Möglichkeiten zur Auswahl

<new>: legt einen neuen Ordner mit dem unter 4 angegebenen Namen

4

<delete>: löscht Spam-Mails sofort!

Danach folgt eine Liste der bereits vorhandenen Ordner



Vollständig ausgefüllt sieht die Filterregel so aus.

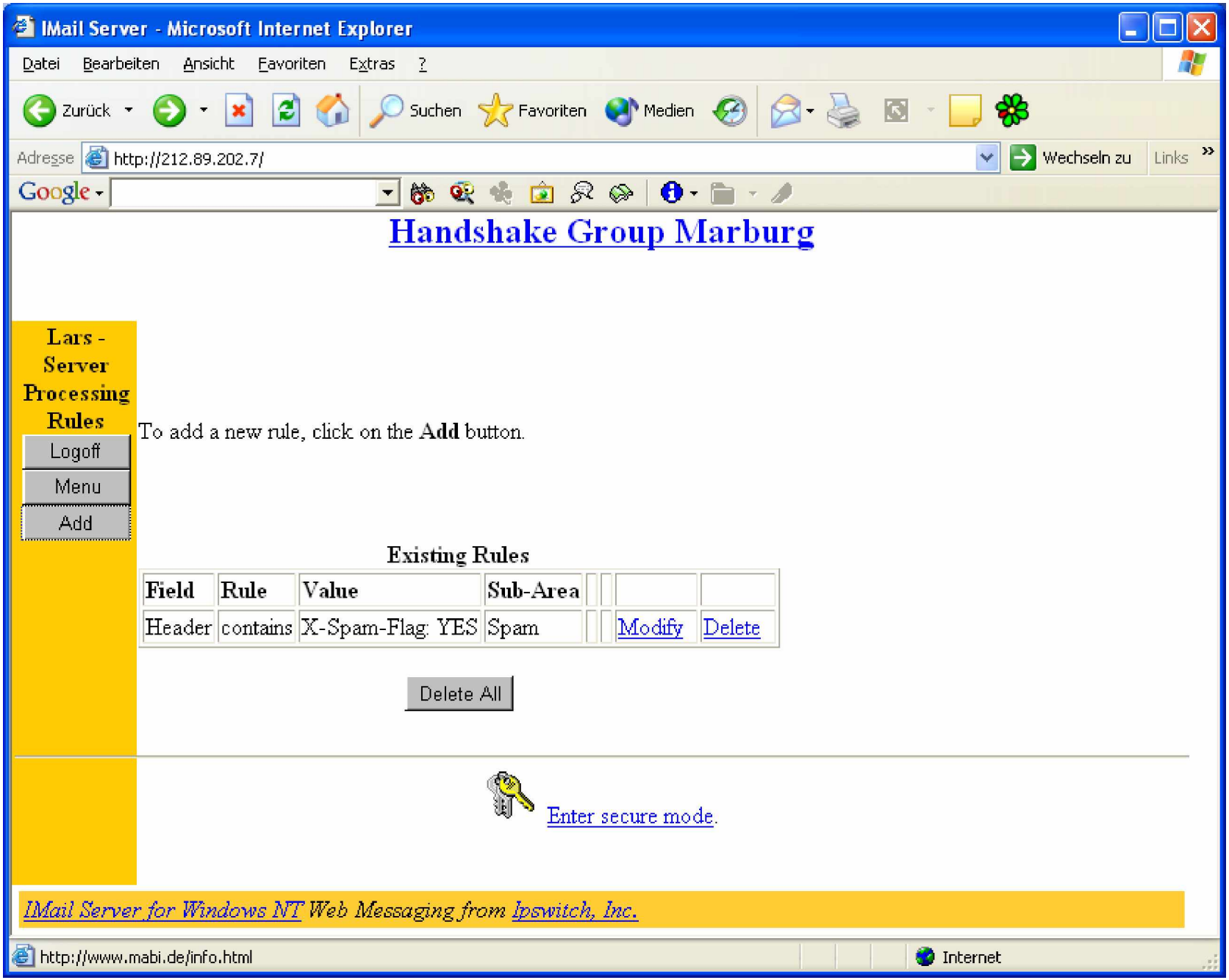
Erklärung:

Es wird nach einem Kriterium im Header (Nachrichten-kopzeilen) gesucht die mit „**X-Spam-Flag: YES**“ übereinstimmt.

Sollte eine Mail gefunden werden, so erstelle (falls noch nicht geschehen einen neuen Ordner namens „Spam“) bzw. verschiebe die Mail in den Ordner.

Beachte aber nicht die tatsächliche Schreibweise.
Ein „x-spam-flag: yes“ würde genauso gefiltert werden.

Jetzt noch links auf **ADD** und fertig.



Wenn alles klar gegangen ist müsste das folgende Fenster so aussehen.

Mit „**Modify**“ kann man die Regel ändern und mit „**Delete**“ wieder löschen.

Probieren Sie bitte das Filtern zu Beginn mit dem Verschieben in einen neuen Ordner und prüfen Sie immer wieder ob wichtige Mails versehentlich als Spam markiert wurden und dadurch in dem Spam-Ordner gelandet sind.

Beachten Sie bitte diese Mails verbrauchen ebenfalls Speicherplatz in Ihrer Mailbox!

Die Mails aus dem Extra-Ordner können nicht mit einem POP3-Client abgeholt werden – Dazu müssen Sie in Ihren Email-Client ein IMAP-Konto einrichten oder die Spam-Mails über das Webinterface löschen.

Nach einer positiven Testphase können Sie dann die Regel so ändern, dass die Mails direkt gelöscht werden.

Hilfe zum Einrichten der verschiedenen Kontenarten in Ihrem E-Mail-Client (E-Mail-Programm) entnehmen Sie bitte Ihrem jeweiligen E-Mailprogramm