Tips für Webmaster

Email injection - Spam über Kontaktformulare verhindern.

Spam ist sicherlich eines der schlimmsten Probleme dem Ottoemailverbraucher gegenübersteht. Umfangreiche Spamfilter beseitigen leider nur die Symptome, aber es gilt die Ursachen zu eliminieren. Und die sind immer öfter Kontaktformulare auf harmlosen Webseiten.

Zu einer guten Website gehört natürlich auch die Möglichkeit den Betreiber zu kontaktieren. Dies kann über die Post erfolgen, geht aber meist viel schneller duch die Angabe einer Emailadresse oder eines Kontaktformulars.
Die Angabe einer Emailadresse ist natürlich schon mal ein gefundenes Fressen für Spammer.
Kontaktformulare sind da schon praktischer. Sie verbergen die eigene Adresse und bieten zudem noch meist den psychologischen Vorteil dass der Webseitenbesucher schon mal weiß er alles schreiben muß, und sich nicht selbst einen ganzen Text mit Form und Struktur ausdenken muss.

Dieses Formular wir dann meist über die recht nützliche, aber auch gefährliche PHP-Funktion mail() abgeschickt.

Das Kontaktformular der Firma xyz schaut folgendermaßen aus:
Code

Die Funktion mail() ist folgendermaßen aufgebaut:

```
 <?php
if (!isset($_POST["senden"])){  // Formular wurde noch nicht abgeschic
kt, zeige Formular
? >
<form method="POST" action="<?=$_SERVER['PHP_SELF'];?>">
Von: <input type="text" name="Absender">
Betreff : <input type="text" name="Betreff">
Nachricht :
<textarea name="Nachricht" rows="50" cols="30" lines="20"></textarea>
<input type="submit" name="senden" value="Abschicken">
</form>
<?
}else{
$from=$_POST['Absender'];
if (mail("info@xyz.de",$_POST['Betreff'],$_POST['Nachricht'],"From: $f
rom")){    // Nachricht senden
echo "Danke für Ihre Nachricht, wir werden sie gleich bearbeiten"; //
zeige Erfolgsnachricht falls alles geklappt hat.
```

```
}else{
echo "Leider lief was falsch. Ihre Nachricht konnte nicht abgeschickt
werden"; // zeige Fehlermeldung falls was schief lief
}
}
?>
```

Im Formular der Firma xyz wurden die Headers dazu verwendet um das Formular mit der Email-Adresse des Besuchers abzuschicken.

Die Kommunikation mit dem Mailserver sieht nun folgendermaßen aus

```
To: info@xyz.de
Subject: Hallo
From: sender@example.xxx
Hallo
Meine Nachricht
Ciao
```

Wenn nun aber ein böser Spammer dieses Formular verschickt und als seine Adresse info@xyz.de Bcc: info@adresse1.xxx, info@adresse2.xxx, info@adresse3.xxx angibt so wird aus der Kommunikation:

```
To: info@xyz.de
Subject: Hallo
From: info@xzy.de
Bcc: info@adresse1.xxx, info@adresse2.xxx, info@adresse3.xxx
Hallo
Ich sende gerade über das Formular der
Firma xyz Spam an info@adresse1 und
an info@adresse2 und an info@adresse3
Ciao
```

Das ist nun ein ziemliches Problem für die Firma xyz. erstens steigt ihr Traffic auf dem Server, 2. bekommt sie sicherlich Beschwerden von erbosten Spamempfängern und 3., wenn es ganz schlimm kommt, landet ihre Adresse in öffentlichen Blacklisten und wird von allen Mailservern, die diese benutzen, abgelehnt.

Deshalb ist es wichtig Kontaktformulare abzusichern.

Unser verbessertes Skript fügt in Zeile 13 folgendes ein:

```
$from=$_POST['Absender'];
if (strpos($from,"
") || strpos($from,"
")) die("No spamming please");
```

Nun stirbt das Skript mir der Meldung: "No spamming please", falls in der Mailadresse ein Zeichen für eine neue Zeile oder ein einfaches Anführungszeichen vorkommt. Nicht gerade schön, aber wirkungsvoll.

Linktipps vom Suleitec Support Team:

Versendet Ihre Webseite heimlich Spam ?

Eindeutige ID: #1032
Verfasser: Thomas Andergassen
Letzte Änderung: 2009-06-23 20:48