Ein Lösungsansatz zur Verwundbarkeit von Internet Explorer aufgrund gefälschter URLs

Problem

Internet Explorer ist durch gefälschte URLs verwundbar. Es ist möglich optional einen Benutzernamen in einer URL durch @-Zeichen mit anzugeben, wie z.B.:

http://benutzername@www.meineseite.de

Falls der Benutzername %01 beinhaltet und wenn man mit der Maus auf dieser URL steht, wird diese Adresse auf der Status-Zeile nur bis zum @-Zeichen dargestellt. Die eigentliche Web-Adresse bleibt dem Benutzer verborgen. Dadurch entsteht die Gefahr, damit den Benutzern durch absichtlich falsch konzipierten URLs wichtige Daten geklaut werden können.

Sie können über diese Verwundbarkeit auf [1], [2], [3] mehr Informationen finden.

Lösung (aktualisiert am 23.12.2003)

Die hier beschriebene Lösung ist kein Patch. Es wird also keine Änderungen an Internet Explorer vorgenommen oder keine externe Plug-Ins installiert.

Der Workaround basiert auf die Nutzung der durch die PICSRules (s. [4]) definierten Filtern. PICSRules beschreiben Regeln für die Filterung der URLs, die entweder blockiert oder freigeschaltet werden. PICS ist die Kurzform von "Platform for Internet Content Selection" und wurde von W3C als Spezifikation standardisiert (s. [5]).

Zuerst brauchen wir die Filterregeln zu schreiben, um die gefälschten URLs zu blockieren:

workaround.prf

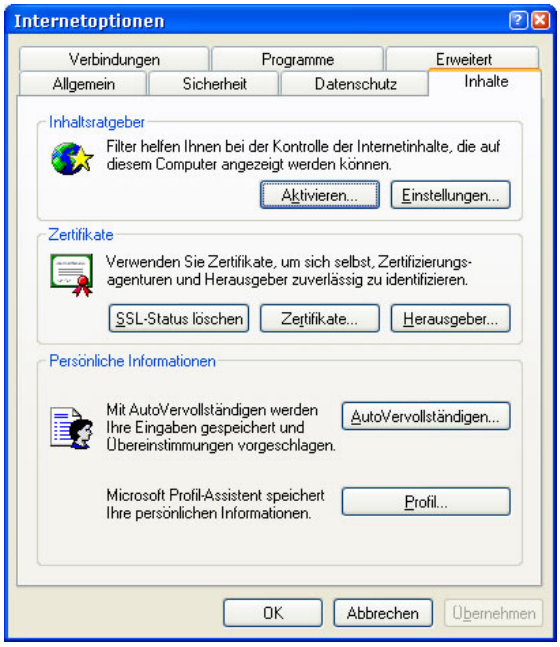
```
(PicsRule-1.1
 (
  Policy (RejectByURL ("http://*%01@*"))
  Policy (AcceptByURL ("*://*/*"))
 )
)
```

Diese Datei kann mit jedem beliebigen Text-Editor erstellt werden. Sie können sie aber auch von [7] herunterladen. Speichern Sie sie als *workoaround.prf*. Es gibt kein vordefiniertes Verzeichnis, die Datei zu speichern aber wir brauchen sie unten nochmal.

Die erste Policy-Zeile blockiert die gefälschten URLs, die zweite läßt die restlichen passieren.

Der nächste Schritt ist die Aktivierung des **Inhaltsratgebers** im Internet Explorer. Sie können den wie folgt aktivieren.

1. Wählen Sie das Menü **Extras** -> **Internetoptionen**
2. Wählen Sie den Bereich **Inhalte**
3. Klicken Sie aufs Button **Aktivieren**

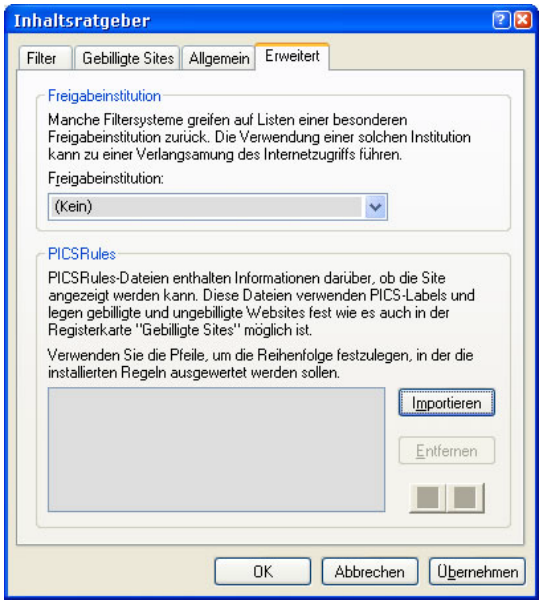


4. Sie bekommen dann das Fenster von **Inhaltsratgeber**. Nachdem Klicken auf **OK** werden Sie gebeten, um ein Supervisor-Kennwort einzugeben. Sie sollten das Kennwort gut bewahren, weil es immer dann gefragt wird, falls Sie entweder die Einstellungen ändern wollen oder entscheiden sollen, was mit einer durch die Filterregeln blockierten Seite geschehen soll.

5. Es ist auch zu raten, einen Erinnerungssatz anzugeben, falls Sie das Kennwort vielleicht vergessen sollten. Dann klicken Sie auf **OK**.

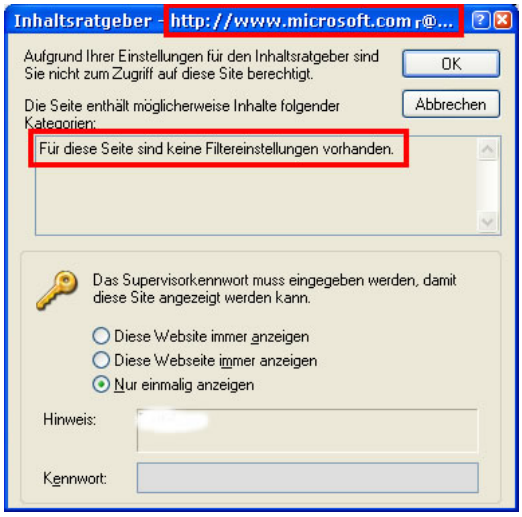
Jetzt können wir die Regel-Datei (*workaround.prf*) in Internet Explorer einlesen:

1. Wählen Sie das Menü **Extras** -> **Internetoptionen**
2. Wählen Sie den Bereich **Inhalte**
3. Klicken Sie aufs Button **Einstellungen**
4. Sie werden nach Ihrem Supervisor-Kennwort gefragt. Nach der Eingabe bekommen Sie das Fenster von Inhaltsratgeber.



5. Wählen Sie den Bereich **Erweitert** und klicken Sie aufs Button **Importieren**
6. Wählen Sie die Regel-Datei (workaround.prf) aus und klicken sie auf **OK**

Nach diesen Schritten sollte Internet Explorer in der Lage sein, die manipulierten URLs zu blockieren. Falls so eine URL aufgerufen wird, werden Sie gefragt, was damit geschehen soll:



Die Funktionsweise dieses Workarounds können Sie auf [3], [6] oder [8] testen. Auf [8] wird demonstriert, wie leicht eine ebay-Login-Seite nachgeahmt werden kann.

References

[1]. http://www.securityfocus.com/archive/1/346948
[2]. http://www.heise.de/security/news/meldung/42768
[3]. http://security.openwares.org
[4]. http://www.w3.org/TR/REC-PICSRules
[5]. http://www.w3.org/PICS/
[6]. http://www.heise.de/security/dienste/browsercheck/demos/ie/e5_18.shtml
[7]. http://www.ornek.de/security/workaround.prf
[8]. http://es-de-we.net/fake.htm