

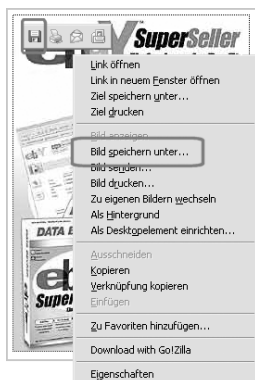
- 3** Im HTML-Code können Sie im oberen Bereich die Meta-Tags finden, mit denen der Autor Informationen für Suchmaschinen angeben kann, damit seine Webseite besser katalogisiert wird.

Je nachdem, welchen Webeditor derjenige benutzt hat und welche zusätzlichen Angaben er vornahm, erfahren Sie hier zum Beispiel seinen Namen, die Firma, für die er arbeitet, Erstellungsdatum, Webeditor, Angaben zum Jugendschutz, E-Mail-Adresse usw.

Neben den Angaben, für deren Angabe der Autor selbst die Verantwortung trägt, ist es doch erstaunlich, wie oft das Tag *name="generator"* in Webseiten vorhanden ist. Einige Editoren wie zum Beispiel MS-FrontPage setzen hier sowohl Produktname als auch Versionsnummer ein. Für Microsoft ist es so einfach festzustellen, wie verbreitet sein Produkt ist und von wem es eingesetzt wird. Sicherlich sind da auch Raubkopierer bei gewesen. Außerdem weiß so ein potenzieller Angreifer gleich, welches Betriebssystem verwendet wurde: MS-Windows. Und wenn schon FrontPage benutzt wird, dann bestimmt auch ein Outlook (Express), womit eine neue Angriffsmöglichkeit gefunden wurde.

5.5 Warum verschlüsselte Webseiten auch keinerlei Schutz bieten

Haben Sie eine eigene Homepage? Dann haben Sie gewiss viel Zeit und Mühe in die Realisierung investiert. Sie haben Grafiken und Fotos fürs Web aufbereitet, Programme per JavaScript erstellt, um dynamisch auf Benutzeraktionen reagieren zu können, und Sie haben die passenden Begleittexte geschrieben. Keine Frage: Sie wollen nicht, dass irgendjemand daherkommt und einfach alles klaut, was er bei Ihnen findet, um dann seine eigene Homepage mit Ihren Bildern zu schmücken. Denn im WWW ist es besonders einfach, Inhalte von fremden Webseiten zu kopieren: Ein Klick mit der rechten Maustaste auf das gewünschte Bild und schon kann es mit *Bild speichern unter* auf der lokalen Festplatte gespeichert werden. Bei einigen Bildern zeigt der Internet Explorer sogar eine kleine Symbolleiste im Bild an, sobald man mit der Maus auf das Bild zeigt. Über diese Symbole kann dann das Bild auch gespeichert werden. Text, der wirklich als solcher vorliegt und nicht in oder als Grafik gezeigt wird, kann ganz bequem markiert und dann mit *Bearbeiten/Kopieren* in die Zwischenablage kopiert werden, um dann in die eigene Homepage oder eine Textverarbeitung eingefügt zu werden. Und Ihre ausgeklügelten Skripte sind für jeden im HTML-Quellcode einsehbar.



Da sich nicht alle Anwender an Recht und Gesetz halten und Ihre Daten eventuell missbrauchen, kann es nichts schaden, dem einen Riegel vorzuschieben. Zahlreiche Produkte und „Insidertricks“ versprechen rasche Abhilfe: den rechten Mausklick verhindern, Markierbarkeit von Text abstellen, den ganzen HTML-Quellcode verschlüsseln usw. Doch egal, was Sie machen: Es ist zwecklos! Mit einfachsten Tricks und etwas Hacker-Kenntnis lässt sich wirklich jeder Schutzmechanismus aushebeln.

Plumpe Tricks halten keinen Hacker auf

Viele der Möglichkeiten, sich vor dem Datenklau zu schützen, beruhen auf einfachen Tricks, die gerade mal einen DAU (dümmster anzunehmender User) abhalten. Bereits etwas ambitionierte Anwender durchschauen den vergeblichen Versuch des Homepage-Besitzers sofort.

Das Problem bei allen Varianten der Verheimlichung ist, dass die zu knackende Webseite bereits beim Anwender angekommen ist, denn der Browser soll sie ja darstellen. Außerdem greifen die meisten Tricks auf JavaScript-Funktionen zurück oder sind nur für bestimmte Browserversionen geeignet.

JavaScript-Schutzmechanismen aushebeln

Zu den beliebtesten Tricks gehört eindeutig der Versuch, per JavaScript den Rechtsklick abzufangen, sodass der Betrachter nicht direkt über das Kontextmenü ein Bild speichern oder den Quellcode betrachten kann. Dies können Sie auf verschiedene Arten umgehen.

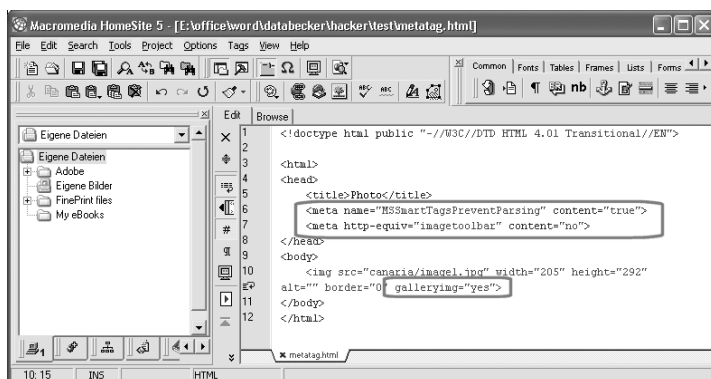


- 1 Geht es Ihnen um einen Blick in den Quellcode, benutzen Sie einfach die gleiche Funktion aus dem Menü *Ansicht/Quelltext*, und schon wird Ihnen der HTML-Code präsentiert, da die Menüfunktionen nicht abgefangen werden können.
- 2 Wollen Sie ein Bild speichern, dann haben Sie im Internet Explorer ab Version 6 meistens Glück: Bei größeren Bildern, die nicht im Hintergrund (auch einer Tabelle) liegen, erscheint eine kleine Symbolleiste im Bild, sobald Sie einen Moment mit der Maus auf dem Bild verweilen. Das lässt sich zwar mit einem Meta-Tag seitens des Anbieters verhindern, doch das wissen bisher nur die wenigsten. Klicken Sie einfach auf das Diskettensymbol, um die Grafik zu speichern. Die Anzeige der Bildsymbolleiste können Sie über *Extras/Internetoptionen* auf der Registerkarte *Erweitert* mit der Option *Bildsymbolleiste aktivieren* steuern.



INFO Meta-Tag für Bildsymbolleiste

Microsoft hat auch die Smart Tags im Internet Explorer 6 eingeführt. Damit ist es möglich, dass in einer Webseite automatisch zusätzliche Links durch den Browser eingefügt werden, die der Ersteller der Seite nie vorgesehen hat. Mit der Angabe `<meta name="MSSmartTagsPreventParsing" content="true">` im `<head>`-Bereich einer Webseite verhindern Sie dieses bisher noch nicht übliche Feature für Ihre eigenen Webseiten. Mit `<meta http-equiv="imagetoolbar" content="no">` unterdrücken Sie die generelle Anzeige der Bildsymbolleisten. Wenn Sie wollen, können Sie für einzelne Bilder mit dem Attribut `galleryimg="yes"` bei jeder Grafik einzeln die Bildsymbolleiste aktivieren oder auch abstellen.

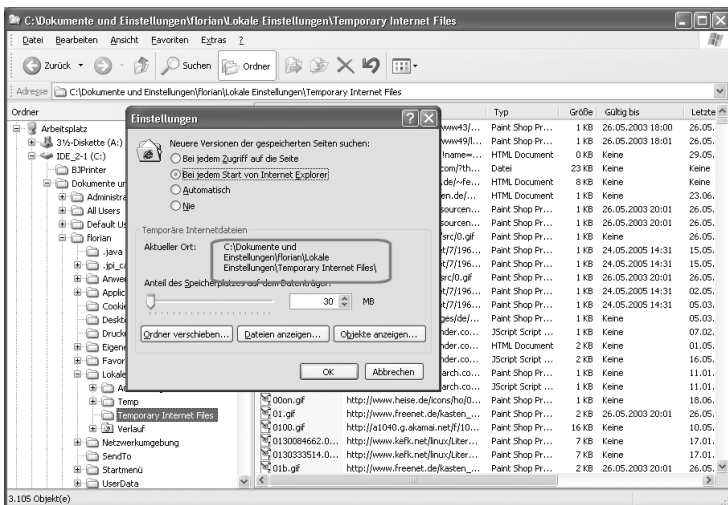


- 3 Schalten Sie JavaScript einfach zeitweilig aus. Im Menü *Extras/Internetoptionen* können Sie auf der Registerkarte *Sicherheit* über die Schaltfläche *Stufe anpassen* die Option *Active Scripting/Deaktivieren* wählen.

Dann funktioniert die Seite zwar eventuell nicht mehr komplett, doch auch das Abfangen des Rechtsklicks klappt nicht mehr und Sie können die Bilder nach einem Reload der Seite (F5) wie gewohnt per Rechtsklick und *Bild speichern unter* sichern.



- 4** Der Internet Explorer speichert normalerweise automatisch alle Webseiten und deren Inhalt für eine gewisse Zeit in einem temporären Verzeichnis auf der Festplatte – dem Cache. Welcher Ordner das bei Ihnen ist, können Sie im IE über *Extras/Internetoptionen* auf der Registerkarte *Allgemein* durch Anklicken der Schaltfläche *Einstellungen* erfahren. Schauen Sie doch einfach mal in das Verzeichnis, was dort alles an Bildern etc. zu finden ist. Aber Vorsicht: Hier herrscht ein heilloses Chaos und das Verzeichnis kann viele Dateien enthalten, sodass es eine Weile dauert, bis im Explorer alles angezeigt wird.

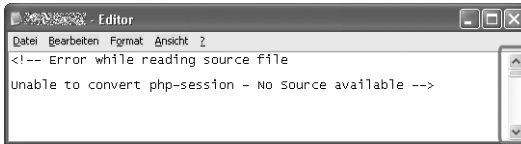


- 5 Haben Sie keine Lust, im Cache-Ordner zu suchen, speichern Sie einfach die komplette Webseite über *Datei/Speichern unter* ab. Im angegebenen Ordner wird dann eine Datei mit der Webseite und ein Unterordner mit allen weiteren Dateien (Bilder etc.) angelegt. Jetzt können Sie die einzelnen Dateien leichter finden und den Quellcode mit einem Editor öffnen.

INFO Fehlermeldungen im Quellcode

Ein einfacher, aber manchmal wirksamer Trick, neugierige Menschen von einem Blick in den Quellcode abzuhalten, ist, diesen mit vielen Leerzeilen am Anfang auszustatten.

Beliebt sind auch in HTML-Kommentaren eingebettete Pseudo-Fehlermeldungen, die dem Betrachter bei einem flüchtigen Blick vorgaukeln sollen, dass es nichts zu sehen gibt. Dabei weist die Bildlaufleiste am rechten Fensterrand schon den Weg zum Ziel: einfach abwärts scrollen, bis der Quellcode sichtbar wird.

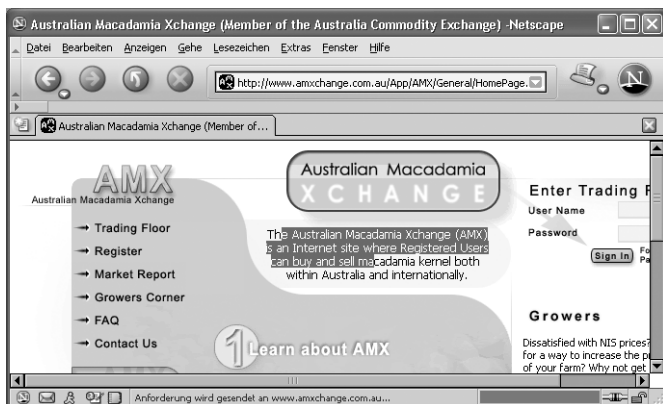


Sicherheit nur im Internet Explorer vorhanden

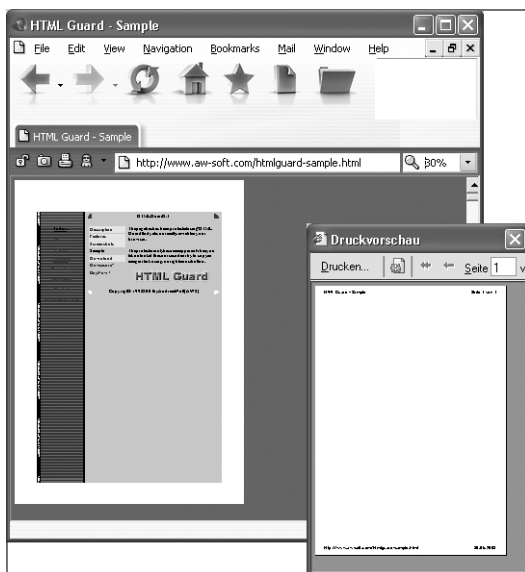
Da der Internet Explorer die größte Verbreitung bei den Anwendern besitzt, sind die meisten Kopierschutzmechanismen auf diesen Browser zugeschnitten.

Dazu gehört auch die Möglichkeit, per JavaScript dafür zu sorgen, dass die Webseite beim Ausdruck weiß wird oder nichts markiert werden kann. Natürlich hält das keinen Hacker wirklich auf:

- 1 Schalten Sie wieder JavaScript kurzzeitig ab: im Menü *Extras/Internetoptionen* auf der Registerkarte *Sicherheit* über die Schaltfläche *Stufe anpassen* die Option *Active Scripting/Deaktivieren* wählen.
- 2 Den Trick, dass Sie nichts markieren können, beherrscht nur der IE ab Version 4. Benutzen Sie einfach einen älteren Browser oder einen anderen wie zum Beispiel Netscape (<http://www.netscape.de>) oder Opera (<http://www.opera.com>), um die Seite zu betrachten und den Text zu markieren.



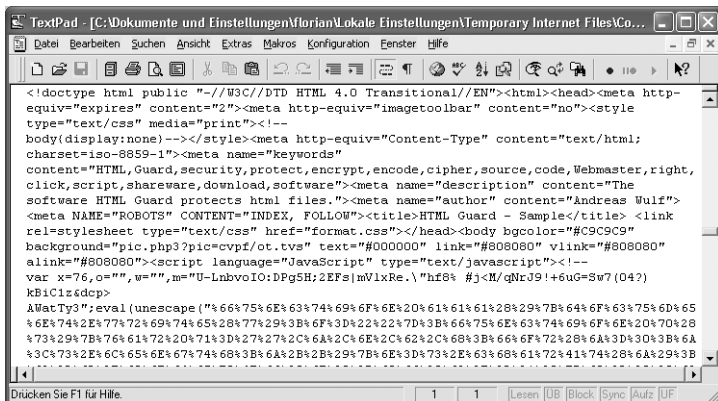
- 3** Wenn Sie beim Ausdruck oder in der Druckvorschau nur ein leeres Blatt zu sehen bekommen (Internet Explorer ab Version 5), dann können Sie wie im vorherigen Schritt auf einen anderen Browser ausweichen, um die Seite dort zu drucken.



Während der IE eine leere Seite in der Druckvorschau darstellt, zeigt Opera alles richtig an (<http://www.aw-soft.com/htmlguard-sample.html>).

Verschlüsselte Webseiten knacken

Mit harten Bandagen kämpft, wer seine Webseiten nur verschlüsselt zum Betrachter überträgt. Dann kann dieser zwar einen Blick auf den Quellcode werfen, doch er wird nichts Sinnvolles zu sehen bekommen, denn der größte Teil der Seite enthält nur kryptische Zeichen.



```
<!doctype html public "-//W3C//DTD HTML 4.0 Transitional//EN"><html><head><meta http-  
equiv="expires" content="2"><meta http-equiv="imageToolbar" content="no"><style  
type="text/css" media="print"><!--  
body{display:none}--></style><meta http-equiv="Content-Type" content="text/html;  
charset=iso-8859-1"><meta name="keywords"  
content="HTML,Guard,security,protect,encrypt,encode,cipher,source,code,Webmaster,right,  
click,script,shareware,download,software"><meta name="description" content="The  
software HTML Guard protects HTML files.><meta name="author" content="Andreas Wulf">  
<meta NAME="ROBOTS" CONTENT="INDEX, FOLLOW"><title>HTML Guard - Sample</title> <link  
rel="stylesheet" type="text/css" href="format.css"></head><body bgcolor="#C9C9C9"  
background="pic.php?pic=evpf/ot.tvs" text="#000000" link="#808080" vlink="#808080"  
alink="#808080"><script language="JavaScript" type="text/javascript"><!--  
var x=76,o="",w="",m="U-LnbvoIO:DPg5H;2EFs!mVlXRe.\`hf6# #j<N/qNrJ9!+6uG=3w7(047)  
kB1C1z6dcp>  
AWatT3":eval(unescape("%66%75%6E%63%74%69%6F%6E%20%61%61%61%28%29%7B%64%6F%63%75%6D%65  
%6E%74%2E%77%72%69%74%65%28%77%29%3B%6F%3D%22%22%7D%3B%66%75%6E%63%74%69%6F%6E%64%20%70%28  
%73%29%7B%76%61%72%20%71%3D%27%2%2C%6A%2C%6E%2C%62%2C%68%3B%66%6F%72%28%6A%3D%30%3B%6A  
%3C%73%2E%6C%65%6E%67%74%68%3B%6A%2B%2B%29%7B%6E%3D%73%2E%63%68%61%72%41%74%28%6A%29%3B
```

Ein Blick in den Quellcode der Webseite <http://www.aw-soft.com/htmlguard-sample.html> hilft nicht weiter.

Auf den ersten Blick scheint man hier nicht weiterzukommen. Am Anfang täuschen viele Leerzeilen darüber hinweg, dass weiter unten doch noch Quellcode vorhanden ist. Bei näherer Analyse fällt dann auf, dass zwischen den vielen scheinbar unsinnigen Zeichen ein paar wenige JavaScript-Befehle stehen. Und hier setzt der Hacker sein Wissen über die JavaScript-Programmierung an und knackt die Seite in wenigen Minuten.



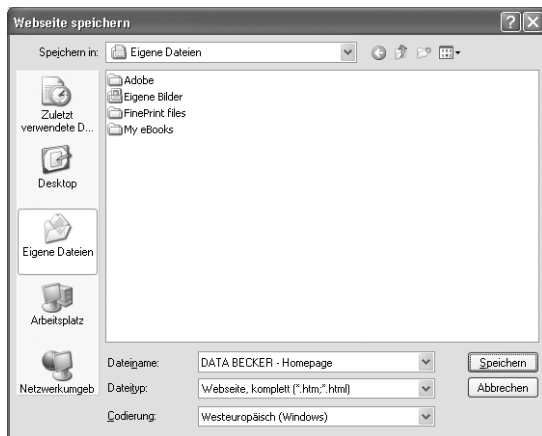
So funktioniert die Geheimniskrämerei

Die meisten Verschlüsselungen sind im Prinzip sehr einfach: Die Ausgangswebseite wird von einem Programm (z. B. HTML Guard <http://www.aw-soft.com/html-guard.html> oder HTML-Protect <http://www.8ung.at/start/download/content/html-protect.htm>) eingelesen und dann werden alle Zeichen nach einem relativ einfachen Verfahren kodiert. Die so ermittelten Zeichen speichert man in einer neuen Webseite (die dann auch im Netz publiziert wird) zusammen mit einer JavaScript-Routine, die den Code entschlüsselt und die HTML-Anweisungen zur Laufzeit in den Hauptteil der Webseite schreibt. Derartige Webseiten sind eigentlich im Alltag unbrauchbar, denn sie zwingen den Betrachter dazu, JavaScript zu aktivieren, weil er sonst gar nichts zu sehen bekommt, da die Dekodierung ja nicht funktionieren kann. Außerdem können verschlüsselte Webseiten nicht von Suchmaschinen katalogisiert werden, weshalb sie im Web nicht zu finden sind.

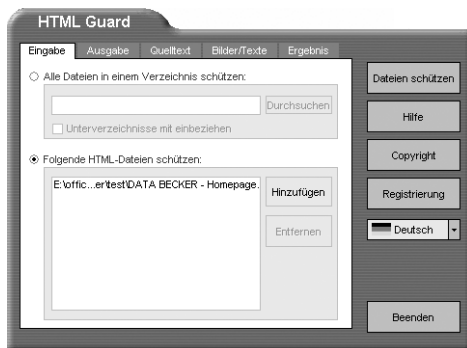
Erstellen Sie verschlüsselte Seiten

Wenn Sie das selbst einmal ausprobieren wollen, dann besorgen Sie sich doch die kostenlose Demo von HTML Guard und verschlüsseln eine eigene Webseite, die Sie zuvor erstellt haben oder aus dem Internet speichern:

- 1 Speichern Sie im Internet Explorer eine beliebige Webseite mit *Datei/Speichern unter* ab. Achten Sie darauf, dass Sie bei *Dateityp Webseite, komplett* aktiviert haben, damit alle Inhalte der Seite gesichert werden.



- 2 Starten Sie HTML Guard und wählen Sie auf der Registerkarte *Eingabe* die HTML-Datei der gespeicherten Seite aus.



- 3 Auf der Registerkarte *Ausgabe* wählen Sie, wo die verschlüsselte Datei gespeichert werden soll und ob Sie ein Backup wünschen.



- 4 Bei *Quelltext* aktivieren Sie die Option *Quelltext verschlüsseln*, damit der HTML-Code verschlüsselt wird. Mit *Quelltext 'quetschen'* wird der Quelltext schwerer zu lesen, da dann alle Zeilenumbrüche entfernt werden. Wenn Sie wollen, können Sie auch noch Leerzeilen einfügen, damit der Quelltext nicht sofort sichtbar ist.



- 5 Auf der Registerkarte *Bilder/Texte* können Sie weitere Einstellungen aktivieren, um Einblicke in den Quelltext weiter zu erschweren.



- Nachdem Sie auf *Dateien schützen* geklickt haben, wird die Datei verschlüsselt etc. und Sie können *Beenden* anklicken, um das Programm zu verlassen. Kontrollieren Sie die Webseite im Browser und überprüfen Sie, wie Sie die einzelnen Schutzmechanismen umgehen können.

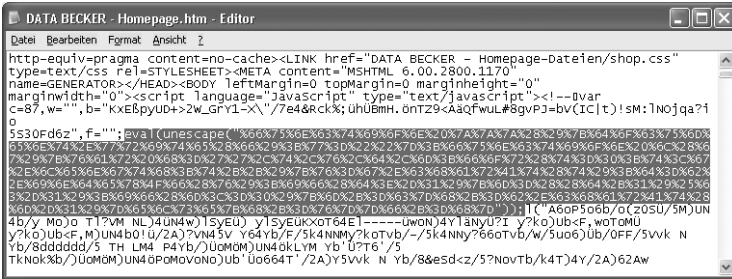
Knacken Sie Ihre eigene Webseite

Um eine Webseite zu entschlüsseln, macht sich der Hacker gar nicht die Mühe, sich die Zähne am Code auszubeißen, sondern er überlässt das Entschlüsseln der eingebauten Funktion und manipuliert dann die Ausgabe, sodass er alles zu sehen bekommt. Wenn Sie selbst eine Webseite verschlüsselt haben, dann können Sie das auch bei sich selbst testen:

- Öffnen Sie den Quellcode in einem Editor (z. B. *Start/Programme/Zubehör/Editor*). Im Windows-Editor müssen Sie beim Öffnen als Dateityp *Alle Dateien* einstellen, um die HTML-Datei auswählen zu können.
- Der besseren Übersicht wegen aktivieren Sie *Format/Zeilenumbruch*.
- Irgendwo im Code steht immer so etwas wie

```
eval(unescape("..."));
```

Finden Sie diese Stelle und suchen Sie dann weiter nach zwei sich schließenden runden Klammern, gefolgt von einem Semikolon.



```

http-equiv=pragma content=no-cache><LINK href="DATA BECKER - Homepage-Dateien/shop.css"
type=text/css rel=STYLESHEET><META content="MSHTML 6.00.2800.1170"
name=GENERATOR></HEAD><BODY leftMargin=0 topMargin=0 marginHeight="0"
marginWidth="0"><script language="JavaScript" type="text"><!--divar
c=87,w="",b="kx&E&pyUD->2w_gfY1-X\`/7e4&Rck&;uh0Mh.0ntZ9<AaqfWul#8gvPJ=bv(IC|T)!sm:lNojqaf1
0
5S30Fd62",f="";eval(unescape('%06%75%0E%63%74%09%96%F%0E%20%87%A%7A%82%28%9%7B%64%0F%66%3%75%0D%
8%3%0E%7%02%0E%77%72%98%74%06%32%8%66%2D%82%B77%93D%22%82%7D%03%06%37%3%0E%63%74%09%96%F%0E%20%87%A%
7A%82%28%9%7B%64%0F%66%3%75%0D%8%3%0E%7%02%0E%77%72%98%74%06%32%8%66%2D%82%B77%93D%22%82%7D%03%06%37%
7%02%9E%7B%6E1%72%20%0E%83%0E%78%2C%74%32C%76%2C%64%2C%66%3B%66%6F%72%82%74%3D%03%83%87%4%3C%67
%2E%6%3E%65%6E%74%74%0E%83%87%4%2B%2B%29%7B%76%3D%67%2E%63%68%61%72%41%3%74%28%74%28%3%8%64%3D%63%
2E%69%6E%64%65%78%4F%66%28%76%29%3B%69%66%28%64%3E%2D%31%32%9%7B%66%3D%32%8%28%3%8%64%32%83%1%32%9%2%
B%2D%31%32%8%3B%69%66%28%6E%83C%3D%3C%3D%32%9%7B%66%2B%3D%68%2B%3D%63%7D%68%2B%3D%63%36%63%37%24%41%74%32%
%0D%2%31%32%9%2D%66%3C%7%3%87%7D%66%3B%3D%68%7D%))1(C"ADop906bD(4205U/5M)UN
4b/y moJo T1?VM NLJ4UN4W)lSyEU) y1SyEUx0t64E1-----uW0N)4Y1anyU?I y7ko)ub<F,w0t0MU
y7k0)ub<F,M)UN4b0i(ü/2A)7vN45v Y64Yb/F/5k4NNM?k0tVb/-/5k4NNY?660tVb/w/5u06)Üb/0FF/5vVk N
Yb/8ddd/5 TH LM4 P4Yb/)Ü0M0M)UN46kLYM Yb'U?T6'/5
TKNoK&0/)Ü0M0M)UN49P0M0v0N0)Üb'Ü0664T'/2A)Y5VvK N Yb/8&e&sdz/5?NovTb(k4T)4Y/2A)62Aw

```

- Ändern Sie diese JavaScript-Anweisung so um, dass vor *unescape* der Befehl *alert* (sticht und am Ende eine weitere Klammer hinzukommt:


```
eval(alert(unescape("...")));
```
- Speichern Sie die Datei ab, ohne den Editor zu schließen, und öffnen Sie die Webseite im Browser (*Datei/Öffnen* oder Doppelklick auf den Dateinamen im Explorer). Sie bekommen ein Dialogfeld angezeigt, das einen oder mehrere JavaScript-Befehle enthält.