JavaScript im GIF

Kaum zu glauben aber wahr, ein "Hallo Welt" geschrieben in JavaScript in einem GIF.

Offenbar kann man beim src-Attribute des script-Tags auch ein Bild angeben, in diesem Fall ein GIF.

Der Trick an der Sache ist einen gültigen GIF-Header zu erzeugen der auch als JavaScript interprepiert werden kann.
In JavaScript wird die Kennung "GIF89a" als Variable betrachtet und in der Breitendefinition einen Kommentar begonnen "/*" der am Ende der Farbtabelle geschlossen wird "*/" und anschließend wird der Variable (GIF89a) der Wert 1 zugewiesen "=1". Das Ende des Gif-Headers ";" schließt diese Zuweisung ab, nun kann der eigentliche JavaScirpt Code folgen.
Man beachte allerdings die Größendefinition, eine Breite von $2A2F entspricht der Breite von10799 Pixel was nicht nur für ein GIF schon beträchtlich ist!

```
Address  0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f  Dump
00000000 47 49 46 38 39 61 2f 2a 64 2e 2e 2e 2e 2c 2e 2e GIF89a/*d....,..
00000010 2e 2e 2a 2f 3d 31 3b 64 6f 63 75 6d 65 6e 74 2e ..*/=1;document.
00000020 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 22 getElementById("
00000030 62 6f 78 22 29 2e 69 6e 6e 65 72 48 54 4d 4c 3d box").innerHTML=
00000040 22 48 61 6c 6c 6f 20 57 65 6c 74 22 3b          "Hallo Welt";
```

[GIF Hexdump]

Offset	Length (bytes)	Content
00	3 ($47 $49 $46)	"GIF"
03	3 ($38 $39 $61)	"87a" oder "89a"
06	2 ($2f $2a)	Breite
08	2 ($64 $2e)	Höhe
0a	1 ($2e)	Farbtabellen Infos
0b	1 ($2e)	Hintergrund Farb-Index
0c	1 ($2e)	Pixel Seitenverhältnis
0d	9 ($2c $2e $2e $2e $2e $2a $2f $3d $31)	Globale Farbtabelle / Blöcke
16	1 ($3b)	Ende
17	document.getElementById("box").innerHTML="Hallo Welt";	JavaScript-Block
4c	1 ($3b)	Ende

```
<div id="box"></div>
<script src="/media/XSS-Sicherheitsluecke.gif" type="text/javascript"></script>
```

Sicherheitslücke geschlossen:

Skript von "https://www.gocher.me/media/XSS-Sicherheitsluecke.gif (/media/XSS-Sicherheitsluecke.gif) " wurde wegen eines unerlaubten MIME-Typs ("image/gif") blockiert.
Laden fehlgeschlagen für das <script> mit der Quelle "https://www.gocher.me/media/XSS-Sicherheitsluecke.gif (/media/XSS-Sicherheitsluecke.gif) ".

Autor: Udo Schmal, veröffentlicht: 16.12.2014, letzte Änderung: 06.05.2020

© Copyright 2020 Udo Schmal (/)