

jwt-cracker – Simple HS256 JWT Token Brute Force Cracker

Simple HS256 JWT token brute force cracker.

Effective only to crack JWT tokens with weak secrets. **Recommendation:** Use strong long secrets or RS256 tokens.

Install

With npm:

```
[crayon-6a9d5fe28e6db108226971/]
```

Usage

From command line:

```
[crayon-6a9d5fe28e6e1787558844/]
```

Where:

- **token:** the full HS256 JWT token string to crack
- **alphabet:** the alphabet to use for the brute force (default: «abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789»)
- **maxLength:** the max length of the string generated during the brute force (default: 12)

Requirements

This script requires Node.js version 6.0.0 or higher

Example

Cracking the default jwt.io example:

[crayon-6a9d5fe28e6e3366604953/]

Encoded

PASTE A TOKEN HERE

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0Ij0nRydwV9.TJVA950rM7E2cBab30RMHrHDcEfxjoYZgeFONFh7HgQ

Decoded

EDIT THE PAYLOAD AND SECRET (ONLY HS256 SUPPORTED)

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

```
{
  "sub": "1234567890",
  "name": "John Doe",
  "admin": true
}
```

VERIFY SIGNATURE

HMACSHA256(
 base64UrlEncode(header) + "." +
 base64UrlEncode(payload),

secret

) ☐ secret base64 encoded

It takes about 2 hours in a Macbook Pro (2.5GHz quad-core Intel Core i7).

Contributing

Everyone is very welcome to contribute to this project. You can contribute just by submitting bugs or suggesting improvements by [opening an issue on GitHub](#).

License

Licensed under [MIT License](#). © Luciano Mammino.