# Challenge: Cursed Secret Party

## Challenge Description :

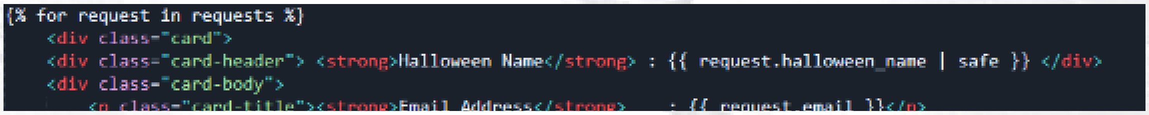
The malevolent spirits have concealed all the Halloween treats within their secret vault, and it's imperative that you decipher its enigmatic seal to reclaim the candy before the spooky night arrives.

## Context :

- Analyze this web-application, and finally get a JWT token cookie from an administrator using a XSS (Cross-site scripting) exploit to gain it.

## Flag :

- First Install the files and read the source code. You can build it in docker to get a better understanding.
- Looking at the Source code we can see a vulnerability, looking at the nunjucks library, which is being used to template the website. The Templating on this is vulnerable due to the [ | safe ] coding argument written with the [ halloween_name ] query, marks it to not be sanitized or checked in anyway.



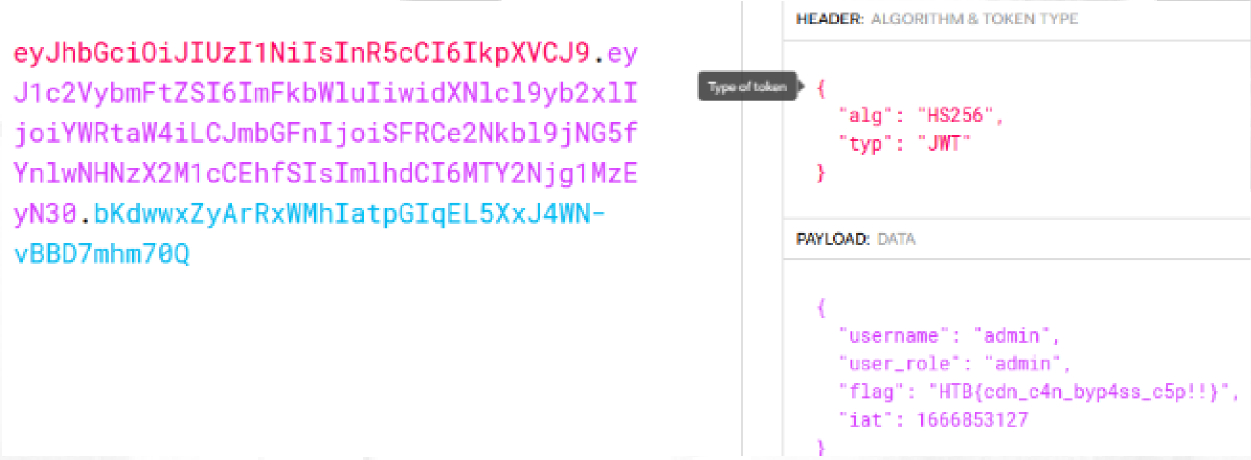
```
{% for request in requests %}
    <div class="card">
    <div class="card-header"> <strong>Halloween Name</strong> : {{ request.halloween_name | safe }} </div>
    <div class="card-body">
        <p class="card-title"><strong>Email Address</strong>    : {{ request.email }}</p>
```

- Next thing to do with this would be to try a xss payload within this, Sending one only retrieves an error, as it's expected to work.
- The only issue stopping the Request is due to CSP [ Content Security Policy ] being set.
- To bypass this I would need to upload a file to [ cdn.jsdelivr.net ] and bypass the CSP, as the script-src for the CSP is set to that domain.

```
script-src 'self' https://cdn.jsdelivr.net;
style-src 'self' https://fonts.googleapis.com;
img-src 'self';
font-src 'self' https://fonts.gstatic.com;
```

- Next i did was used a script already on the [ cdn.jsdelivr.net ] network called, [ CSP-bypass ] {Link} with the use of ngork.

- Using ngork and the CSP-bypass i was able to send a xss payload to the admins browser, get the JWT token and hopefully either login or extract the flag from the token.



```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwidXNlcl9yb2xlIjoiYWRtaW4iLCJmbGFnIjoiSFRCe2Nkbl9jNG5fYnlwNHNzX2M1cCEhfSIsImlhdCI6MTY2Njg1MzEyN30.bKdwwxZyArRxWMhIatpGIqEL5XxJ4WN-vBBD7mhm70Q
```

HEADER: ALGORITHM & TOKEN TYPE

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

PAYLOAD: DATA

```
{
  "username": "admin",
  "user_role": "admin",
  "flag": "HTB{cdn_c4n_byp4ss_c5p!!}",
  "iat": 1666853127
}
```

- The flag for this one should be : HTB{cdn_c4n_byp4ss_c5p!!}