[web] 보물

page 1,2,3 버튼을 누르면 위와 같은 각기다른 암호문 같은 것이 출력된다.

해쉬함수 같은데 해쉬는 단방향성 알고리즘이기 때문에 복호화할 방법이 없다;

```
<style>
body {background-color: white;}

.center {
  display: block;
  margin-left: auto;
  margin-right: auto;
  width: 50%;
}
</style>

<body>
<h1 align="center" style="margin-top:20px">보물</h1>
<p align="center">내 페이지 숫자 중엔 비밀이 하나 있지...그곳에 보물을 숨겨놨다. 원한다면 찾아봐라 모든 것을 그곳에 두고 왔다!</p>
<img src="treasure.jpg" class="center" style="width:300px;height:234px"></img>

<div align="center">

<form action="/" method="get" style="display:inline-block;">
    <button type="submit" value="1" name="page">Page 1</button>
</form>

<form action="/" method="get" style="display:inline-block;">
    <button type="submit" value="2" name="page">Page 2</button>
</form>

<form action="/" method="get" style="display:inline-block;">
    <button type="submit" value="3" name="page">Page 3</button>
</form>

</div>

</body>
<p align="center">
1dce4fb8a0e7be0692f72f87512c054a3dd1cfff4716a8e1a5dffbbbf757274bb479330d70bdfc3d622359ab85dd05d20a14b56798a67b8d3059233aaf7977ab</p>
```

소스코드는 위와 같다. get을 통해 데이터를 전송함을 알 수 있다.

ctf.j0n9hyun.xyz:2025/?page=1

실제로 url의 쿼리 스트링으로 1이라는 값이 전달된 것을 알 수 있다.

혹시 싶어 button에 존재하지 않는 수를 넣었더니 이번에도 해쉬값이 출력되었다. 아마도 계속 page의 value값을 바꿔가다보면 키가 나오는 형식인 것 같다.

```python
import requests

url = 'http://ctf.j0n9hyun.xyz:2025/?page='
i = 4
while True:
    page = url + str(i)
    response = requests.get(page)
    if "HackCTF" in response.text:
        print(response.text)
        break
    i += 1
```

파이썬으로 page값을 계속 증가시켜가며 페이지의 resource에 HackCTF로 시작하는 키값이 존재하는지 확인하는 코드를 작성했다.

```
<form action="/" method="get" style="display:inline-block;">
    <button type="submit" value="3" name="page">Page 3</button>
</form>

</div>

</body>
<p align="center">
HackCTF{0hhhhh_5o_g0od_try!}</p>

>>>
*** Remote Interpreter Reinitialized ***
```

조금 기다리니 키가 출력된 것을 볼 수 있었다.