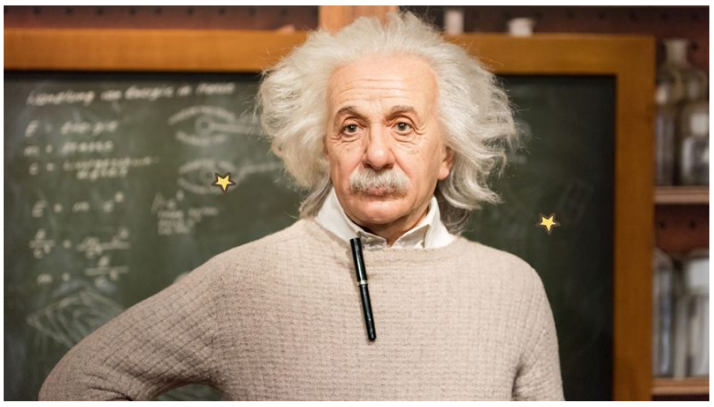
HEALTHKATHON 2022 - PENTEST STUDENT

Reja Revaldy F

SOAL 1

We cannot solve our problems with the same thinking we used when we created them.

ALBERT EINSTEIN



Diberikan sebuah website yang berisikan gambar albert einstein saya mencoba melakukan cek kepada header dengan menggunakan command curl dan saya mendapatkan beberapa petunjuk yang saya duga adalah flag

```
< HTTP/1.1 200 OK
< Date: Sat, 17 Sep 2022 04:33:30 GMT
< Server: Apache/2.4.54 (Debian)
< X-Powered-By: PHP/7.4.30
< Set-Cookie: wrapper=Q1BKU3t9
< Allow-Siri-Google-Cortana-Search-Clients: 1
< Anti-HPKP-Suicide: ignoreAfter=6000000
< Content-Meaning: none; flag-part-number=last part-content=%y?y=,#};
< Browser-Restrict: openInNewTab=false; noRefererFromHere=1;
< Check-CDN-Revocation-List: 1; ignoreIfError;
< Connection: keep-alive
< Flag-First-Part-Is-Here: encoding=...+base64; part1=545756734e486b30626d6b3d;
< Flag-Parts-Connector: char=_; charCode=95; hexCharCode=0x5f;
< Flag-Security-Policy: ecnryption=none,
< Task: category=easy; encoding=true; justString=false; isThisHelp=true; flagPart2=733370656e75
68; flagPart4=6d336c346d70347531; totalPart=e
< X-Bug-Bounty: openRedirects=false; logoutCSRF=false; selfXSS=false;
< X-Content-Config: blink-origin-in-addressbar, disable-addressbar-copy-paste, disable-javascri
pt-history-api
< X-Do-Not-Link-From-These-Sites: /blacklist.txt
< X-FRAME-Restrict: minhsize:100px; minvsize:100px; readable
< X-Frame-Options: SAMEORIGIN
< X-Header: meaning=none;
< X-If-You-Read-This-Join-Tomsk-State-University: additional-points=5; url=http://www.fpmk.tsu.
ru/node/474;
< X-Ignore-CSP-Whitelists: 1
< X-Mouse-Disable-Click-After-Page: 3 secodns
< X-Nikita-Please-Add-This-Header: False
< X-Order-To-KFC: order=coffee; order=fried-potato; transport=SASHA
< X-Papper-Compatibility: disallow
< X-ShellShock-vector: (){:}; echo "Want flag?"; python -c "part3="68347421"; print part3.decod
e("hex")"
< X-Super-Hero-Status: False
< X-Window-Restrictions: disallow-from-window-open
< X-XXX-Movie: url=goo.gl/0kGizJ
< Y-Toilet-Papper-Compatibility: allow
< content-security-policy: real-strict-dynamic
< strict-transport-security: max-age=31536000000000000
< x-xss-protection: -1; mode=ignoreheader
< Vary: Accept-Encoding
< Content-Length: 283
```

di header saya mendapatkan 4 part flag yang di encode dengan hex, setelah saya decode ternyata masih perlu part terakhir untuk mendapatkan flag

```
λ ~/Cybersecurity/bpjs/soal1{done}/pentest.student.1337hackathon.id:81/ cat style.css
@import "custom.77.css";

.hero {
    text-align: center;
    text-transform: uppercase;
    color: red;
}
```

lalu setelah saya mencoba untuk mencari part yang lain saya membuka file style.css dan di file tersebut melakukan import terhadap file custom.77.css

```
λ ~/Cybersecurity/bpjs/soal1{done}/pentest.student.1337hackathon.id:81/ cat custom.77.css
.quote {
    font-family: Helvetica, Arial, sans-serif;
    text-align: center;
    color: #4CAF50;
    /* readme: RGVjb2RlIHBhcnQ1IGJ5IHVzaW5nIHRoZSBYT1IgZnVuY3Rpb24gd2l0aCBjdXN0b20gY3NzIG51bWJlci4= */
}
```

di file custom.77.css terdapat text yang di encode base64, lalu saya langsung saja melakukan decode dan menemukan clue selanjutnya

```
λ ~/Cybersecurity/bpjs/soal1{done}/pentest.student.1337hackathon.id:81/ ls
custom.77.css  index.html  pict.jpg  style.css
λ ~/Cybersecurity/bpjs/soal1{done}/pentest.student.1337hackathon.id:81/ echo "RGVjb2RlIHBhcnQ1IGJ5IHVzaW5nIHRoZSBYT1IgZnVuY3Rpb24gd2l0aCBjdXN0b20gY3NzIG51bWJlci4=" | base64 --decode
Decode part5 by using the XOR function with custom css number.
```

part ke 5 atau part terakhir di encode dengan menggunakan function xor dengan key css custom number yang berada di file name css “77”

```
< Content-Meaning: none; flag-part-number=last part-content=%y?y=,#};
```

disini saya menduga ini adalah flag terakhir yang di encode dengan function xor menggunakan key 77, jadi langsung saja saya kumpulkan part dari flag tersebut dan menjalankannya di python agar lebih mudah di decode

```python
import base64

def decrypt(encrypted: bytes, key: bytes):
    result = []

    for i in range(len(encrypted)):
        result.append(encrypted[i] ^ key[i % len(key)])

    return bytes(result)

encrypted = b"%y?y=,#"
key = bytes([77, ])

part1 = base64.b64decode(bytes.fromhex('545756734e486b30626d6b3d').decode('utf-8')).decode('utf-8')
part2 = bytes.fromhex('733370656e7568').decode('utf-8')
part3 = bytes.fromhex('68347421').decode('utf-8')
part4 = bytes.fromhex('6d336c346d70347531').decode('utf-8')
part5 = decrypt(encrypted, key).decode('utf-8')

flag = f"{part1}_{part2}_{part3}_{part4}_{part5}"

print(f"BPJS{{{flag}}}")


>> BPJS{Mel4y4ni_s3penuh_h4t!_m3l4mp4u1_h4r4pan}
```

FLAG = BPJS{Mel4y4ni_s3penuh_h4t!_m3l4mp4u1_h4r4pan}