Writeup - Kendrick Lan’s Desktop

---

1. AzisMissing

- Examine os códigos *javascripts* presentes na aplicação ao acessar ela;
- A flag está presente na atribuição da varíavel `cyberwar`.

```
541b7135666e28b2773121860dc698b7d0aa139eb11cf29cda1a6fe83e9f079e
```

2. JaSON

- Acesse a rota `/api/auth/login`;
- Decodifique o *token* JWT na resposta da requisição.

```
b053e86ed56c00ff78bab833b0211f22a1d5b21291da6d3f48381ecaa1ccb537
```

3. LittleDetail

- Acesse a rota `/api/users/list` utilizando o *token* JWT obtido no passo anterior;
- Obtenha a flag na resposta da requisição.

```
56765c6961530b48b2b75fc9b67e44eb58dc1ed2f7f16b8d5a0ecb87e763206b
```

4. DataInside

- Utilize alguma das credênciais obtidas ao acessar o endpoint da flag anterior e acesse a aplicação;
- Navegue até a rota `/evidences`;
- Note que o mecânismo de buscar evidências está vulnerável a ataques de SQLi
- Utilize técnicas de SQLi para explorar o banco de dados que a aplicação se comunica e obtenha a flag.
    - Como exemplo, utilizando o seguinte *payload* o atacante seria capaz de obter a flag

```
"" UNION SELECT NULL, flag, NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL FROM flag
_tb; -- -
```

```
3ffc8408ca6de1a19ad48c6c2ba0289e53901708c8a316977a95da5106abe719
```

5. NoComments

- Acesse a funciondalide de *download* de arquivos ZIP de evidências;
- Note que o parâmetro `files` está vulnerável a ataques de *path tranversal;*
- Através desta vulnerabilidade, obtenha o código fonte da aplicação. O mesmo pode ser alcançado através da rota `../index.js`;
- Examine o código e você encontrará a quinta flag comentada no código.

```
39e31bc69e1f95fdfa0ebbc56e369a8ffa520fc661b39ef998599069f339852a
```