

Projektowanie Bezpiecznych Aplikacji, projekt

Przemysław Samsel 25.05.21 r.

Projekt własnego systemu do zarządzania Lamami na posterunkach.

Adres repozytorium (znajdują się na nim dokumenty OpenAPI, diagramy etc.):
<https://github.com/PrzemyslawSamsel/pbaLlamaVille>

Generowanie tokena:

1. Należy wykonać zapytanie pod endpoint: <adres_url>:8000/token

Credentials: llamaoperator : llamasAre1heB3st

POST

localhost:8000/token

Send

Params

Authorization

Headers (8)

Body

Pre-request Script

Tests

Settings

Cookies

☐ none

☐ form-data

☒ x-www-form-urlencoded

☐ raw

☐ binary

☐ GraphQL

	KEY	VALUE	DESCRIPTION	...	Bulk Edit
<input checked="" type="checkbox"/>	password	llamasAre1heB3st			
<input checked="" type="checkbox"/>	username	llamaoperator			
	Key	Value	Description		

Otrzymamy odpowiedź :

```
Body  Cookies  Headers (4)  Test Results  200 OK  642 ms  414 B  Save Response ✓  
Pretty  Raw  Preview  Visualize  JSON  ⌵  
1  {  
2    "access_token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.  
    eyJzY29wZSI6WyJsbGFTYWJ2aWxsZV9yZXNvdXJjZSJdLCJqdGkiOiJjYWVjMWI4Ni1jODdkLTExZWlTYTZkYi0xZTAwM2ExNG  
    E3NzYiLCJjbGllbnRfaWQiOiJsbGFTYW9wZXJhdG9yIiwiaXNwIjoxNjIzODgwMjY2fQ.  
    5nJ8I3zY2fkMx9WeRvfgZhjCHQF4Nqi-szRHVwv7skw",  
3    "token_type": "bearer"  
4  }
```

Generowanie HMAC:

<https://www.devglan.com/online-tools/hmac-sha256-online>

Mając przykładowy request dodania lamy:

```
{
  "llama": {
    "name": "Gonzo",
    "age": 15,
    "breed": "wikunia",
    "color": "white",
    "coat": "podrozny"
  }
}
```

Zamieniamy go przy pomocy Pythona na zwykły string:

```
$> Python3
....
>>> rq = {
...     "name": "Gonzo",
...     "age": 15,
...     "breed": "wikunia",
...     "color": "white",
...     "coat": "podrozny"
... }
>>> str(rq)
"{'name': 'Gonzo', 'age': 15, 'breed': 'wikunia', 'color': 'white', 'coat': 'podrozny'}"
```

Następnie kopiujemy zawartość “zserializowanego” słownika i wrzucamy na wyżej wymienioną stronę:

Wartość skrótu będzie następująca:

```
dca5bd6206d2536c63184ec2a2df8a1dbaaf215d46e2a513311d94cb44e4e304
```

Enter Plain Text to Compute Hash

```
{'name': 'Gonzo', 'age': 15, 'breed': 'wikunia', 'color': 'white', 'coat': 'podrozny'}
```

Enter the Secret Key

secret123456

Select Cryptographic Hash Function

SHA-256

Output Text Format:
☒ Plain Text
☐ Base64

Compute Hash

Hashed Output:

dca5bd6206d2536c63184ec2a2df8a1dbaaf215d46e2a513311d94cb44e4e304

1. Struktura systemu oraz przepływy (flow diagrams)





