API (VamAPI) - SQL Injection

Pre-requisite:

1. VAmPI should be up and running.
2. Api json should be added in Postman and connected to Burp using Proxy.

What is Injection?

Attackers construct API calls that include SQL, NoSQL, LDAP, OS, or other commands that the API or the backend behind it blindly executes.

Impacted API?

API Name: Retrieve User by Username

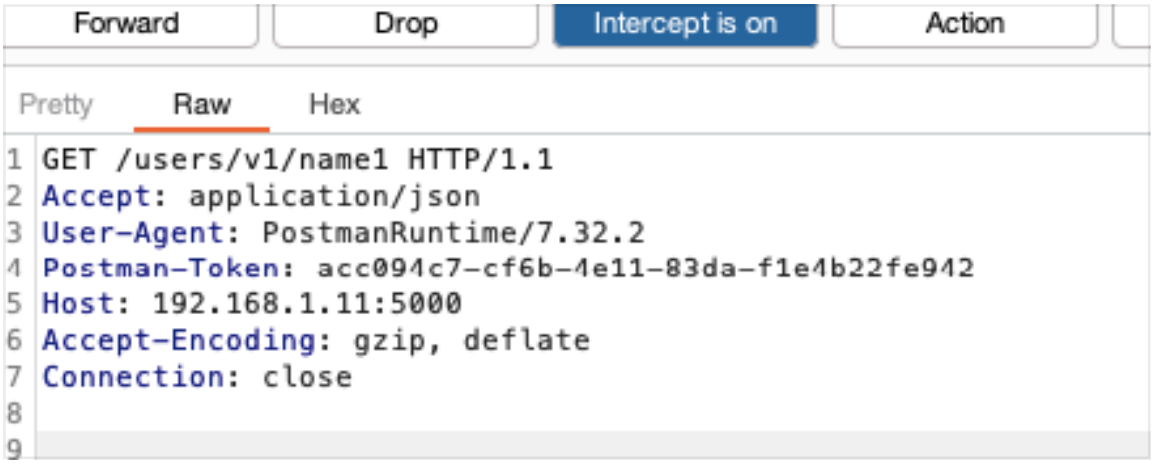
Method Type: GET

Use cases

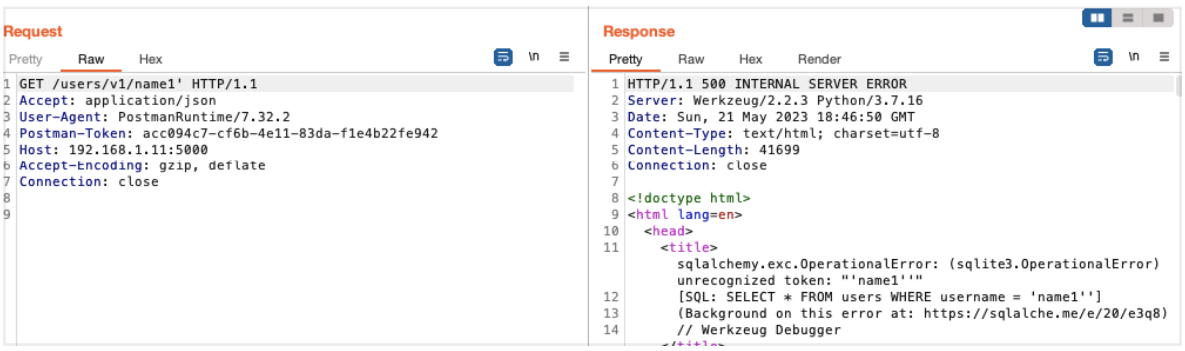
- Attackers send malicious input to be forwarded to an internal interpreter:
  - SQL
  - NoSQL
  - LDAP
  - OS commands
  - XML parsers
  - Object-Relational Mapping (ORM)

Lets Begin:

1. If we Observe the API, the username is passing in the URL. The first step we will do is to capture the request in Burp Suite.



2. As we know, now we will check if the application is throwing an error when we are sending sending special character.



3. Great..!!! This is what we were looking for, if we see the response we observe that their is an SQL Error. Which Indicates that we can try to perform an SQL Injection attack over there.

4. Now we will use SQLMAP to check if we are perform the SQL Injection. Below we can find the Screenshots of Output we got using SQLMAP.

```
┌──(kali㉿kali)-[~/Desktop/API/VAmPI]
└─$ sqlmap -u http://192.168.1.11:5000/users/v1/name1 --batch --tables
```

```
[00:32:54] [INFO] fetching tables for database: 'SQLite_masterdb'
<current>
[2 tables]
+-------+
| books |
| users |
+-------+
```

How to prevent

- Never trust your API consumers, even if they are internal.
- Strictly define all input data, such as schemas, types, and string patterns, and enforce them at runtime.
- Validate, filter, and sanitize all incoming data.
- Define, limit, and enforce API outputs to prevent data leaks

---

Thanks...!!!!!