SCENARIO

The application possesses a NoSQL Injection Vulnerability and is powered by a MongoDB NoSQL database. We will try to exploit the vulnerability in order to gain administrator privileges using MongoDB operators.

**PROCEDURE**

1. Open the web application and navigate to the user login page.
2. Login using the given credentials.
3. Send GET /user/lookup?user=wiener request form the Proxy tab to BurpSuite’s Repeater.
4. First, we will inject Payload 1 in order to get the length of the administrator’s account’s password in URL encoded form.
5. Forward the request to the Intruder as we need to mount a brute force attack on the password’s characters one by one.
6. Now in order to mount a brute force attack place Payload 2 in place of the user parameter and go for Cluster Bomb attack and in Payload 1 for the attack select 0-7 and a-z for Payload 2.
7. After the attack is completed, sort by descending order on the length of the content and note down the password.

**PAYLOAD**

1. administrator' && this.password.length == 8|| 'a'=='b
2. administrator' && this.password[§0§]=='§a§

**REMEDIATION**