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. Try the following testcases:
   * Change the value of the username parameter from "wiener" to {"$ne":""}, then send the request.
   * Change the value of the username parameter from {"$ne":""} to {"$regex":"wien.\*"}, then send the request.
   * With the username parameter set to {"$ne":""}, change the value of the password parameter from "peter" to {"$ne":""}, then send the request again.
4. Based on the responses of the above requests we will craft a Payload and will try to inject it into the username and password field as mentioned in Payload 1 and Payload 2.
5. Then, right click on the response and select Show in browser and we’ve got access to the administrator panel.

**PAYLOAD**

# {"$regex":"admin.\*"}

1. {"$ne":""}

**REMEDIATION**