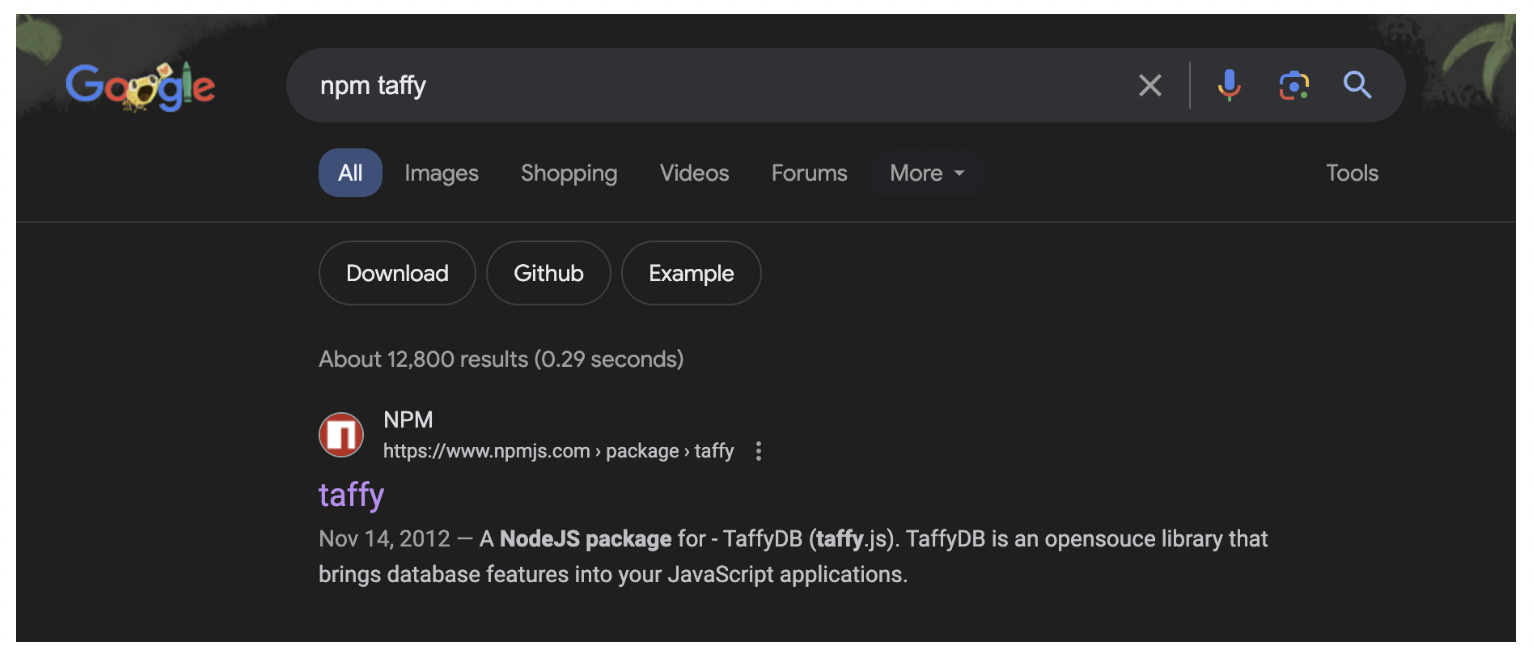
**squ1rrelCTF**

**Json Store**

Giải thử thách này bằng khai thác taffydb

taffy là 1 lựa chọn kì lạ đối với cơ sở dữ liệu, vì vậy phải có lí do để chọn nó.





Taffy bị dính lỗ hổng Internal Property Tampering. Taffy đặt 1 chỉ mục đối với data item trong cơ sở dữ liệu. Chúng ta nhận thấy chỉ mục này có thể bị giả mạo bằng cách thêm thuộc tính vào trong đầu vào của người dùng. Nếu một chỉ mục được tìm thấy trong câu truy vấn, taffyDB sẽ bỏ qua các điều kiện truy vấn khác và trả về data item có chỉ mục đó. Hơn nữa, chỉ mục có định dạng dễ đoán (ví dụ T000002R000001). Hacker có thể khai thác lỗ hổng này để truy suất bất kỳ data item nào trong DB và khai thác SQL Injection.

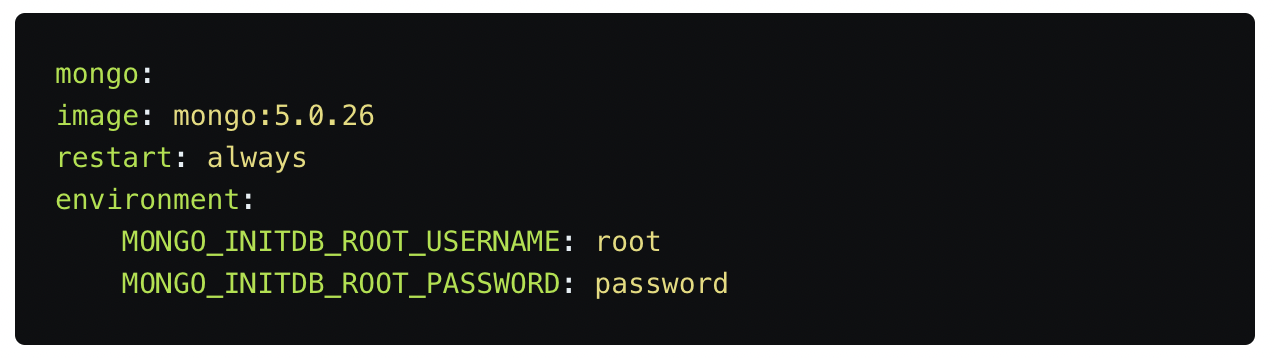
**Goosemon**

Lỗ hổng NoSQL Injection

Flag là mật khẩu của admin. Nhưng nó chặn “regex”. Bạn không thể trích xuất mật khẩu của admin bằng “regex” được.

Nhưng không có xác thực câu truy vấn. Đầu vào của bạn có thể làm câu truy vấn - ứng dụng không đảm bảo rằng req.body bao gồm các trường username và password.

Ứng dụng không dùng phiên bản mới nhất của MongoDB; thay vào đó nó dùng phiên bản 5.



Phương pháp chúng ta dùng là hàm $where, cho phép chúng ta dùng Javascript trong câu truy vấn. Hàm $where: MongoDB phiên bản 6.0 chỉnh sửa Javascript không cho phép 1 nhóm các phương thức của chuỗi và mảng, bao gồm: .contains,.substr,.includes,… Ta quyết định dùng .includes và tạo câu truy vấn sau:

Solve script của tôi:

