**PHP: Serialize**

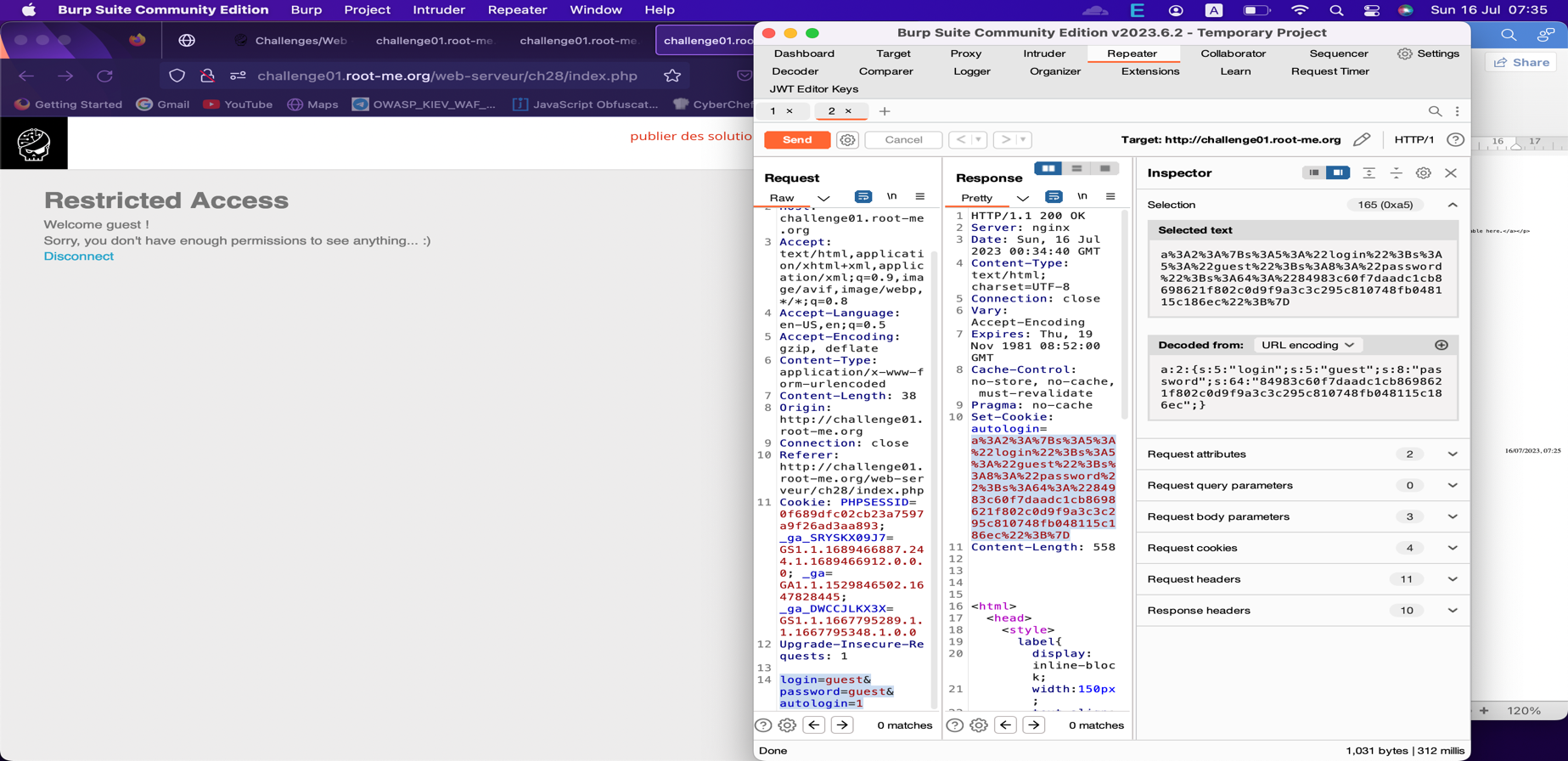
Mục tiêu: lấy được quyền truy cập của admin.

Source code:





Thử đăng nhập bằng tài khoản guest/guest và bật autologin lên.



Khi bạn disconnect hay vào main page nó sẽ tự động đăng nhập bằng cookie autologin.

$data = unserialize($\_COOKIE['autologin']);

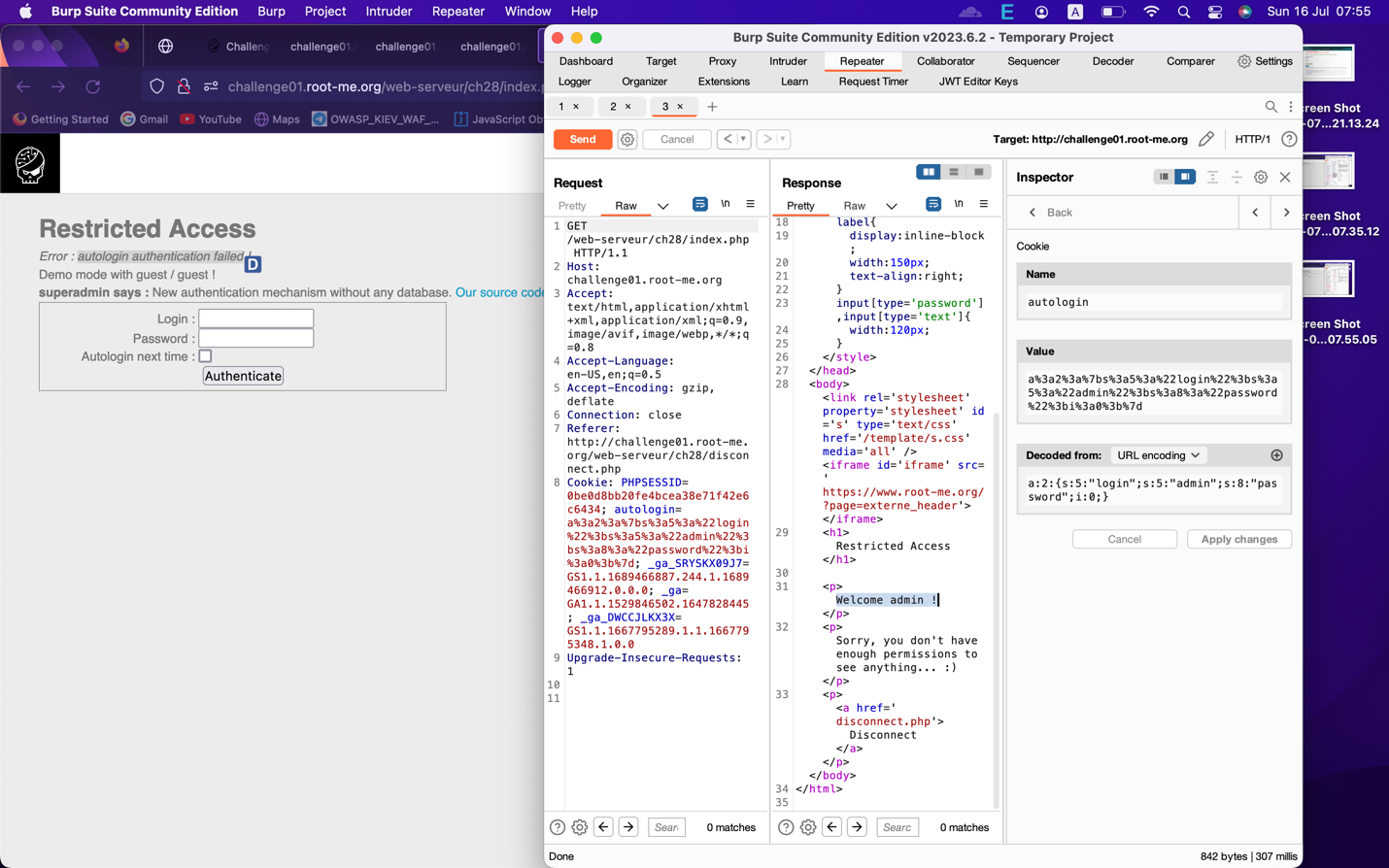
Login và mật khẩu sẽ được lưu trong mảng data. Mật khẩu được hash sha256.

Khi mình thấy “==”, mình nghĩ ngay đến type juggling.

Lúc đầu, mình cho login là admin, mật khẩu là 1 magic hash.

Nó báo lỗi: autologin authentication failed

Mình thử mật khẩu là số 0.



Mình đăng nhập được tài khoản admin nhưng không xem được flag. Tài khoản admin là 1 user bình thường.

Đọc code mới thấy muốn xem được trang admin.inc.php phải là superadmin. Cũng cách đó thử lại thì sai thông tin đăng nhập.

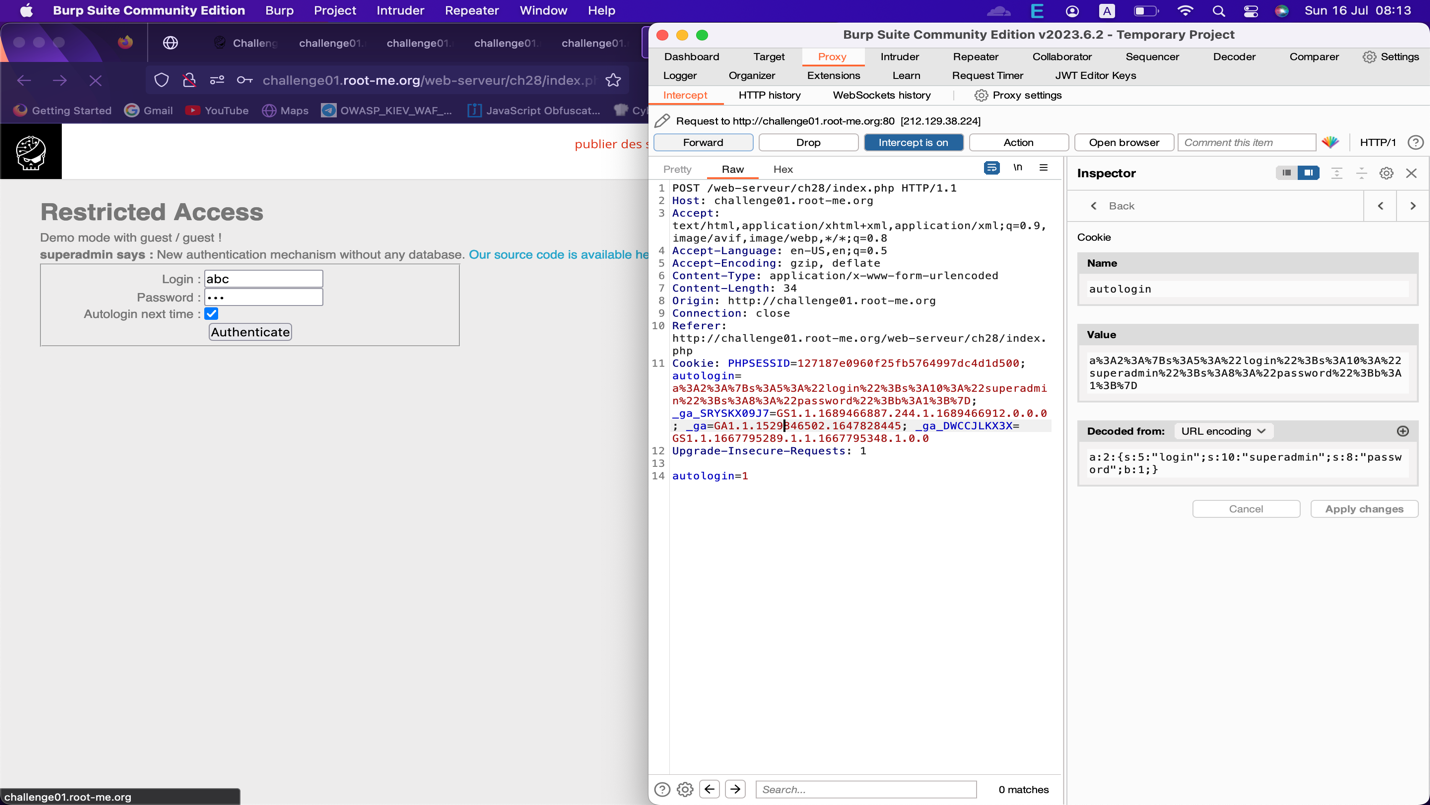
Mình mới thấy sai sai. Magic method =’0’ nhưng ai lại để mật khẩu là 0 cơ chứ.

Mình đọc lại code nhiều lần nhưng chỉ thấy có type juggling mới có thể đăng nhập được tài khoản admin.

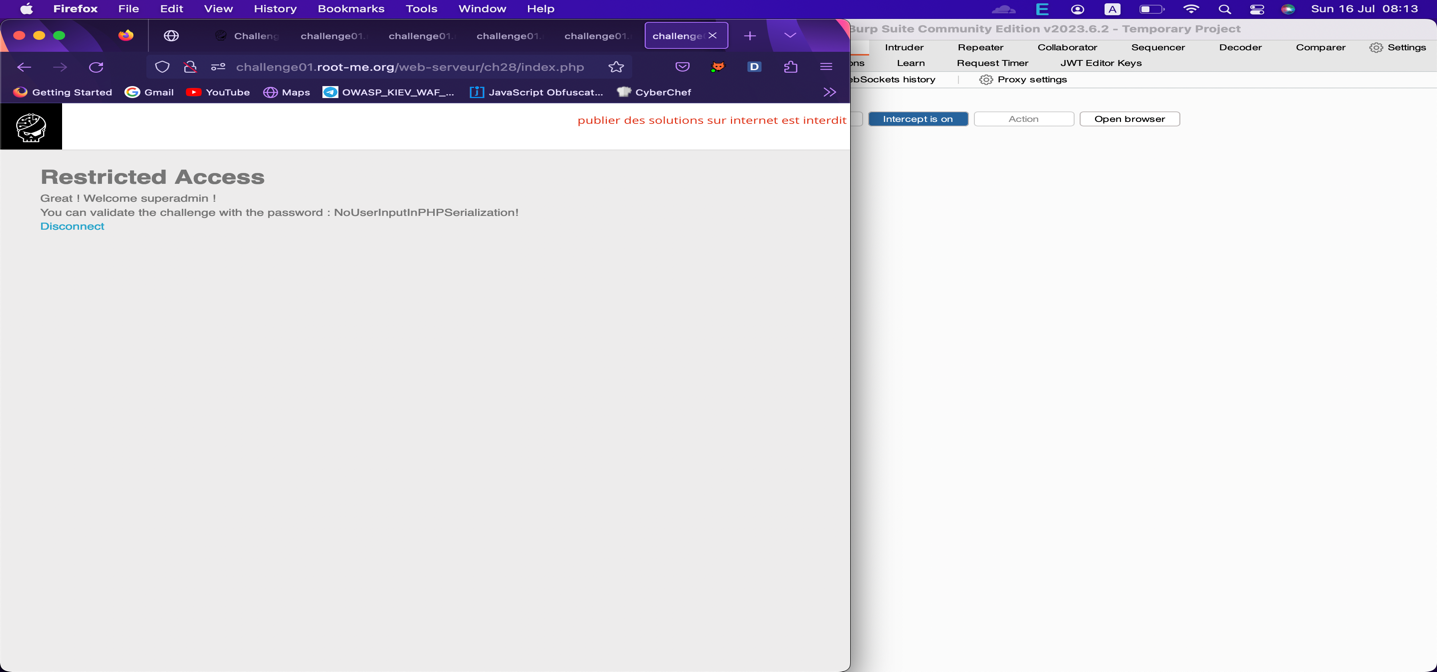
Cuối cùng, mình mới nghĩ ra sao không để mật khẩu là luôn đúng (bool=1).

Vì cookie tự động thêm autologin cũ vào nên rất khó xem được phản hồi chính xác. Kiểu như mình đã chỉnh sửa autologin rồi nhưng trang web hình như không load kịp nên vẫn hiện ra phản hồi cũ làm cho mình rất khó theo dõi hành vi của ứng dụng. Nên để chắc chắn hơn, mình nghĩ bạn nên chặn yêu cầu và chỉnh sửa nó sẽ dễ hơn. Let’s go.

Tốt nhất là bạn nên sửa autologin ở trang đăng nhập nha. Trang disconnect hay main page không được đâu. Muốn vào trang đó, bạn phải xóa autologin ở cookie đi và set lại nó ở trang đăng nhập mới thành công.



Và đây là thành quả:



**Flag: NoUserInputInPHPSerialization**