**natas34**

Bạn dùng thông tin đăng nhập sau: natas33: APwWDD3fRAf6226sgBOBaSptGwvXwQhG

Đây là code PHP của challenge:



Mục tiêu ở đây là upload file sẽ được thực thi ở phía máy chủ nếu md5 checksum bằng giá trị sau: adeafbadbabec0dedabada55ba55d00d.

Tất nhiên, MD5 cũng bị dính lỗ hổng collision, nó sẽ vô ích nếu cố gắng tìm collision cho đoạn mã trên. Ngay cả khi về mặt lí thuyết là có thể, nó sẽ mất vài năm và file của bạn sẽ lớn hơn 4096 bytes bị giới hạn trong code.

Tuy nhiên, chúng ta kiểm soát được 2 tham số là filename và uploaded file (file content). Trong đoạn code sau bạn có thể thấy filename được đặt ở phía máy khách với session\_id:



Sau một vài nghiên cứu, tôi đã xem qua tài liệu sau: “It’s a PHP unserialization vulnerability Jim, but not as we know it” bởi Sam Thomas. Về cơ bản anh ấy giải thích cách khai thác phar:// và .phar archive trong php để unserialize dữ liệu

Cái thú vị về những file phar (PHP archive) là chúng chứa metadata trong định dạng serialize. Nếu 1 thao tác tập tin được thực hiện trên 1 file phar đang có qua giao thức phar:// thì meta data đã được serialized sẽ được unserialized. Điều đó đồng nghĩa với việc 1 đối tượng trong metadata được tải trong phạm vi của ứng dụng.

Cùng tổng kết nó lại nào:

* Chúng ta có thể đăng tải bất cứ loại file nào chúng ta muốn
* Chúng ta kiểm soát được tham số filename
* md5\_file() có thể đọc Phar stream

Vì vậy, nếu chúng ta dựng 1 Phar archive với dữ liệu đã serialized, cố gắng mở nó bằng phar stream wrapper, chúng ta có thể thực thi code.

Tôi giải nó với hai bước. Đầu tiên, tôi đăng tải 1 file php để đọc mật khẩu của natas34.



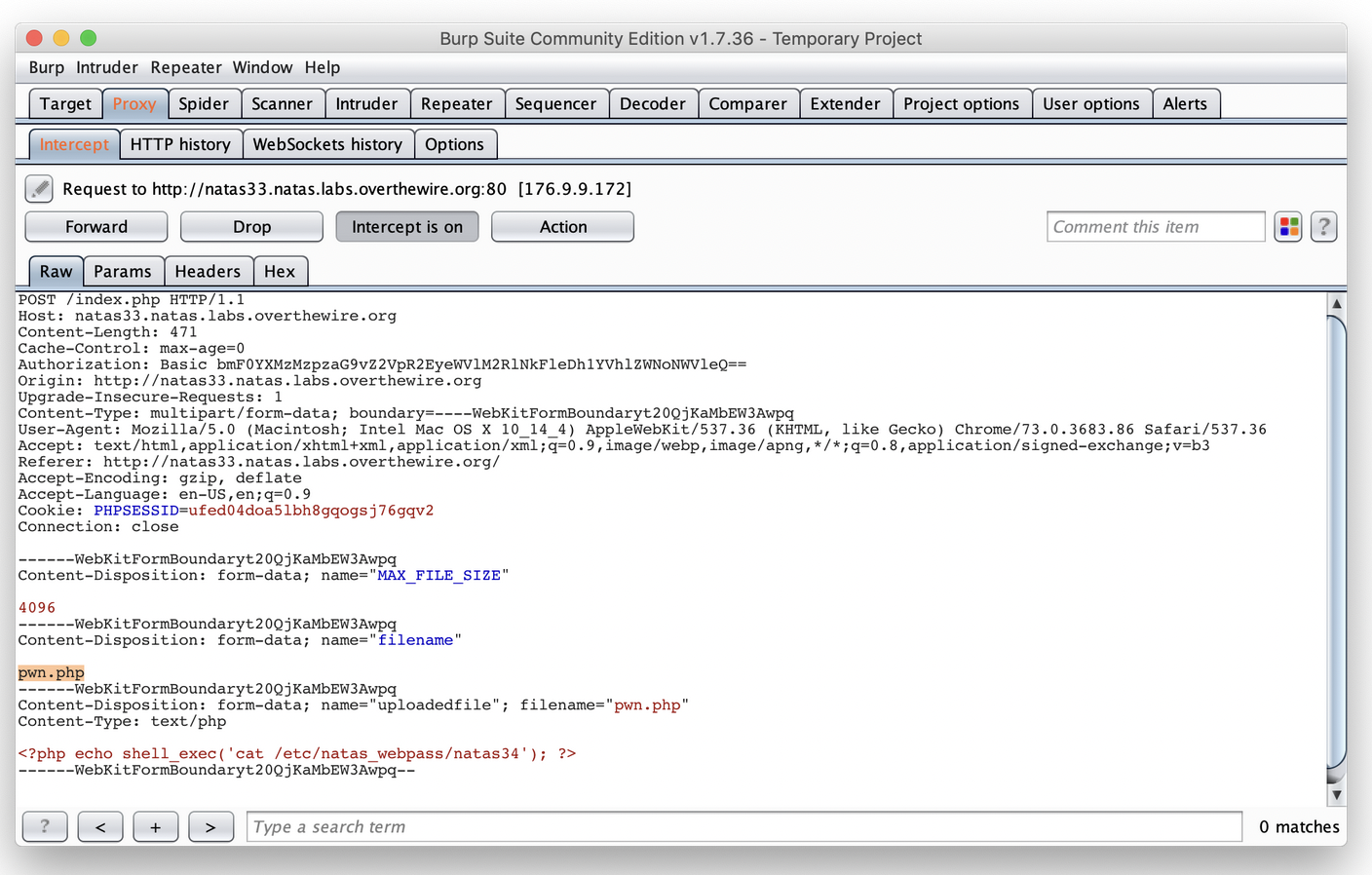
Tôi chặn yêu cầu và đổi tên file là pwn.php. Sau đó tôi dựng 1 php archive như sau:



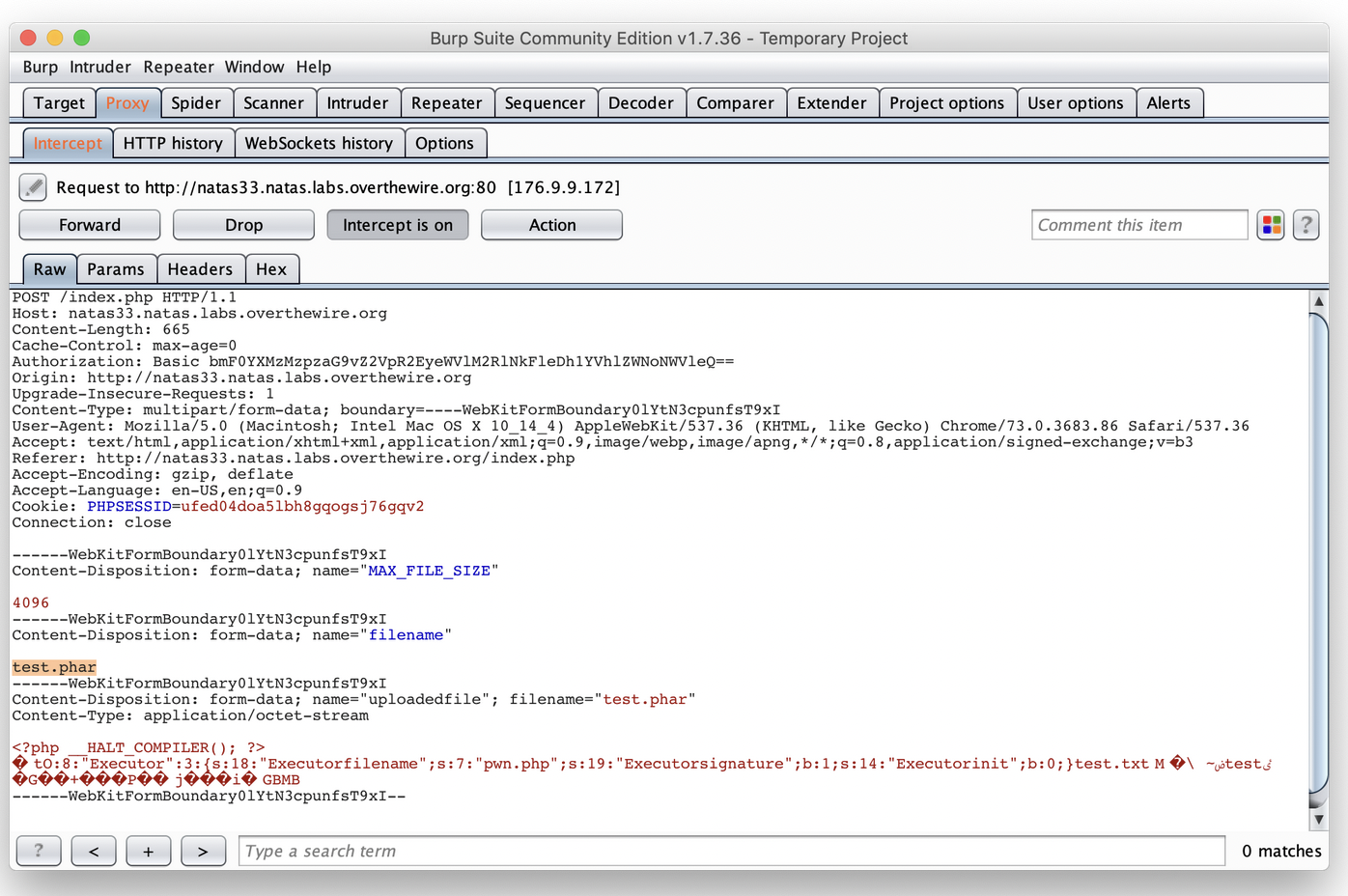
Trong code này, tôi đổi thuộc tính filename là pwn.php và signature bằng true. Bằng việc làm cho phép so sánh md5 luôn trả về true, hàm passthru() sẽ thực thi đuọc pwn.php.



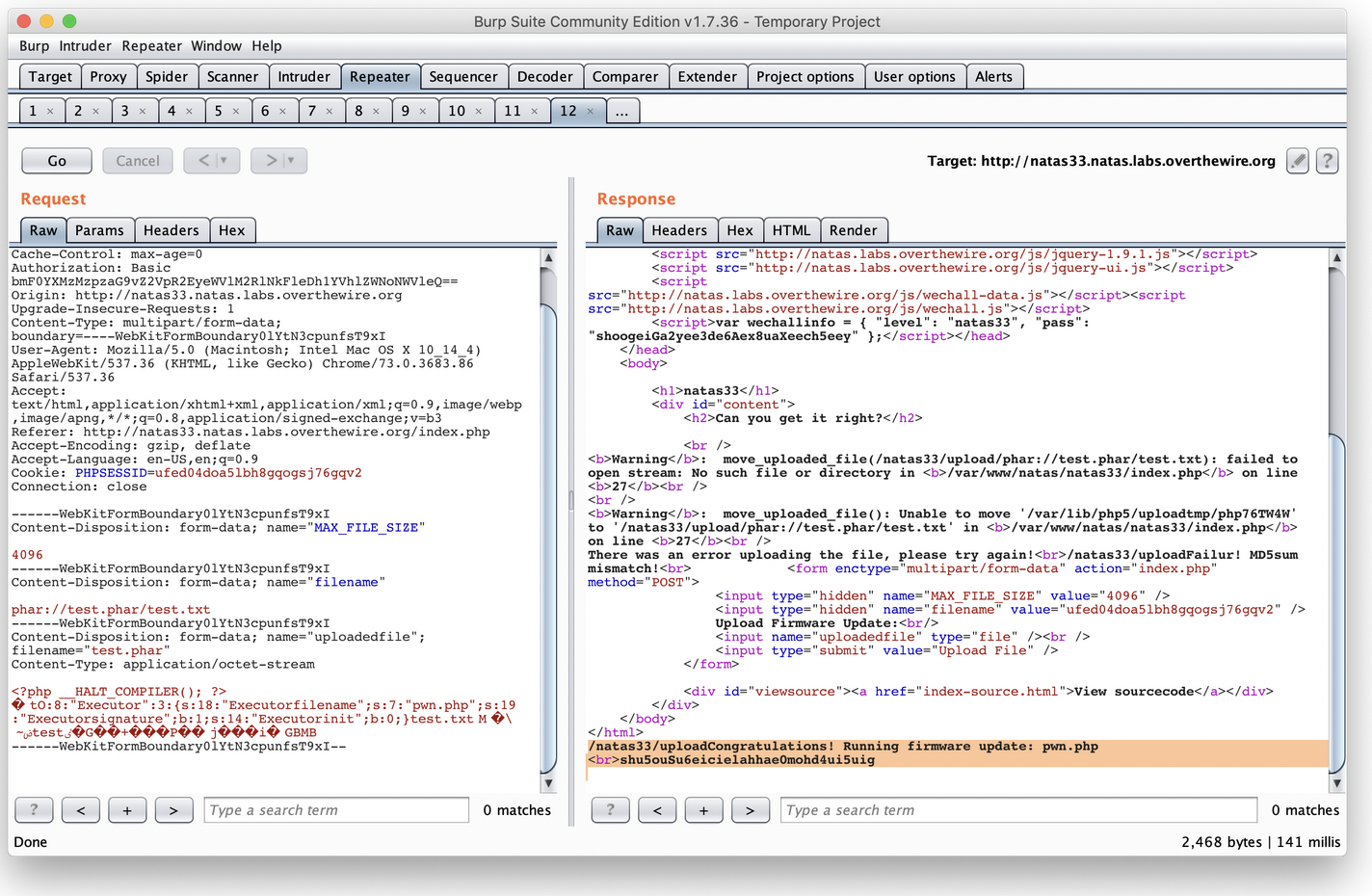
Đầu tiên, đăng tải file php và đổi tên nó trong Burp:



Sau đó upload Phar archive và đổi tên nó:



Cuối cùng, gửi yêu cầu trước đến Burp Repeater và điều chỉnh filename là phar://test.phar/test.txt để buộc hàm md5\_file() thông dịch Phar archive.



Thành công!