**PHP - Unserialize Pop Chain**

Bài này thật sự rất hay. Và mình đã tự làm nó, cảm thấy rất vui và hạnh phúc. Cùng khai thác nó nào.

Source code:

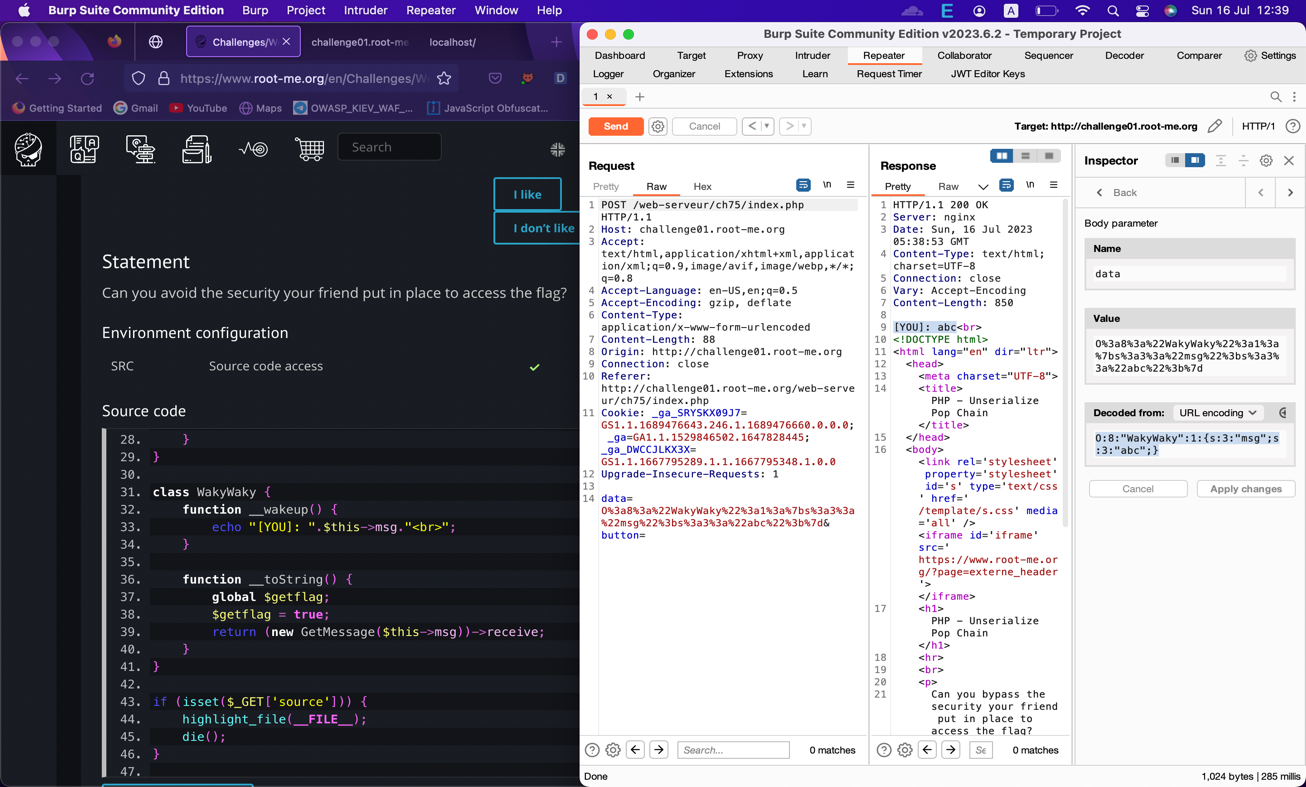




Biến POST["data"] được unserialize, mình sẽ xem code xử lí dữ liệu này như thế nào.

Để có được flag, $getflag phải bằng true. Để bằng true, mình phải tạo 1 đối tượng WakyWaky trước. Vả lại, magic method như \_\_wakeup sẽ được thực thi khi đối tượng này được deserialize.

Test magic method \_\_wakeup:



Method \_\_toString chỉ thực thi khi echo 1 đối tượng, nó sẽ chuyển đối tượng đó thành chuỗi.

Mình sẽ khởi tạo 1 đối tượng là WakyWaky(1) trước có msg cũng là 1 đối tượng WakyWaky(2).

function \_\_wakeup() {

echo "[YOU]: ".$this->msg."<br>";

}

Khi đó $this->msg cũng là 1 đối tượng, khi echo 1 đối tượng thì method \_\_toString được thực thi.

Như vậy, $getflag sẽ bằng true và trả về 1 đối tượng là (new GetMessage($this->msg))->receive

echo (new GetMessage($this->msg))->receive

Khi new GetMessage($this->msg) thì method \_\_construct được thực thi với $receive sẽ là thuộc tính msg của thằng WakyWaky 2.

$GetMessage->receive= WakyWaky(2)->msg

echo WakyWaky(2)->msg

Cái echo này không quan trọng, chủ yếu là mình muốn set $getflag=true. Như vậy WakyWaky(2)->msg phải là 1 đối tượng GetMessage có thuộc tính receive là "HelloBooooooy".

Nếu bạn quan sát kĩ sẽ thấy lớp GetMessage rất thú vị:

function \_\_construct($receive) {

if ($receive === "HelloBooooooy") {

die("[FRIEND]: Ahahah you get fooled by my security my friend!<br>");

} else {

$this->receive = $receive;

}

}

function \_\_destruct() {

global $getflag;

if ($this->receive !== "HelloBooooooy") {

die("[FRIEND]: Hm.. you don't seem to be the friend I was waiting for..<br>");

} else {

if ($getflag) {

include("flag.php");

echo "[FRIEND]: Oh ! Hi! Let me show you my secret: ".$FLAG . "<br>";

}

}

}

Ở construct, receive mà là HelloBoy thì nó xuất ra … và dừng thực thi code ở dưới luôn (kể cả \_\_destruct). Nhưng để lấy được flag ở \_\_destruct thì receive phải là HelloBoy.

Rất là mâu thuẫn, hầu như không lấy được flag luôn. Đây chính là điểm hay của bài này. Cách làm là bạn phải làm sao để set cho thuộc tính receive là HelloBoy nhưng phải bỏ qua được thằng \_\_construct là thành công. Rất đơn giản.

O:10:"GetMessage":1:{s:7:"receive";s:13:"HelloBooooooy";}

Nhờ đó mà bạn cũng hiểu được cách hoạt động của payload này, nó sẽ không chạy \_\_construct nhưng vẫn có thuộc tính là "HelloBooooooy".

Sau một hồi phân tích tỉ mỉ thì đây là payload cuối cùng:

O:8:"WakyWaky":1:{s:3:"msg";O:8:"WakyWaky":1:{s:3:"msg";O:10:"GetMessage":1:{s:7:"receive";s:13:"HelloBooooooy";}}}

**Flag: uns3r14liz3\_p0p\_ch41n\_r0cks**

Để làm được bài này, mình cũng phải chạy thử code ở localhost.