SCENARIO

The application contains a stored cross site scripting vulnerability in the comment box functionality. We will try to trigger an alert message by injecting a payload into the search box.

**PROCEDURE**

1. Go to the vulnerable application and comment something with all the fields filled.
2. Check out the response/source and you’ll find that the application puts the website into a href HTML tag unsafely.
3. We don’t even need to break out of that tag because we can simply execute JavaScript into that tag by using the given payload.

**PAYLOAD**

javascript:alert(“HACKED!”)

**REMEDIATION**