SCENARIO

This application is vulnerable because it makes an assumption about the privilege level of the user based on the HTTP Host header. We will try to get access to the admin panel.

**PROCEDURE**

1. Go to the web application and using BurpSuite send the request for homepage to the Repeater.
2. Try changing the Host header to anything other than the original value and we see that we can still access the homepage.
3. Now try to access the admin panel by appending Payload 1 to the URL and we see that admin panel can only be accessed by local users.
4. In order to fool the server in assuming that we are trying to access the page from the local network we will replace the Host header’s value with Payload 2.
5. Now send the request to access the admin page and we get access to it.

**PAYLOAD**

1. /admin
2. localhost

**REMEDIATION**