SCENARIO

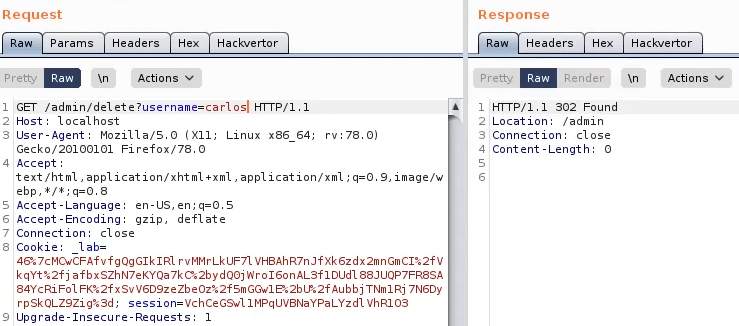
This application is vulnerable because it makes an assumption about the privilege level of the user based on the HTTP Host header. We will try to get access to the admin panel.

**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

**PROOF OF CONCEPT**

**REMEDIATION**

1. **Avoid Relying Solely on the Host Header:** The Host header should not be used to make security decisions. Attackers can easily spoof or modify the HTTP headers. Instead, use other secure methods of verifying the privilege level of a user.
2. **Authentication & Authorization:** Implement proper authentication and authorization mechanisms. Every page, especially sensitive ones like admin panels, should verify if the user is authenticated and authorized to access the content.
3. **Strong Session Management:** Utilize strong session management techniques. Make sure that session cookies are secure, HttpOnly, and set with the SameSite attribute.
4. **Referrer Check:** If an application must check the origin, it should rely on a combination of checks including the "Referer" and "Origin" headers. These headers are more reliable for checking the source of a web request, although they are not completely foolproof.
5. **Input Validation:** Validate and sanitize all incoming requests and headers. Headers like the Host header should be validated against a whitelist of allowed values.
6. **Network Configuration:** Configure the application to recognize and accept only specific Host headers. Additionally, configure network firewalls and routing rules to allow only trusted sources to access sensitive endpoints.