SCENARIO

The application is vulnerable to web cache poisoning because cookie isn’t included in the cache key. We will try to poison the cache with a response that executes alert(1) in the visitor's browser.

**PROCEDURE**

1. Open the web application and in the BurpSuite’s Proxy tab send the request to BurpSuite’s Repeater and study the GET request to the home URL.
2. We observe that the value from the **fehost** cookie is reflected inside a double-quoted JavaScript object in the response, try sending requests to the endpoint by using some cache busters and we see that the value is reflected in the source code of the website.
3. Replace the value of the **fehost** parameter in the cookie with the payload to trigger an alert.
4. Send the malicious request and keep replaying the request until we see our exploit server URL being reflected in the response and **X-Cache: hit** in the headers.

**PAYLOAD**

"-alert(1)-"qwertyuiop

**REMEDIATION**