**SCENARIO**

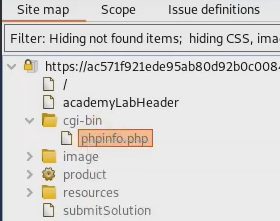
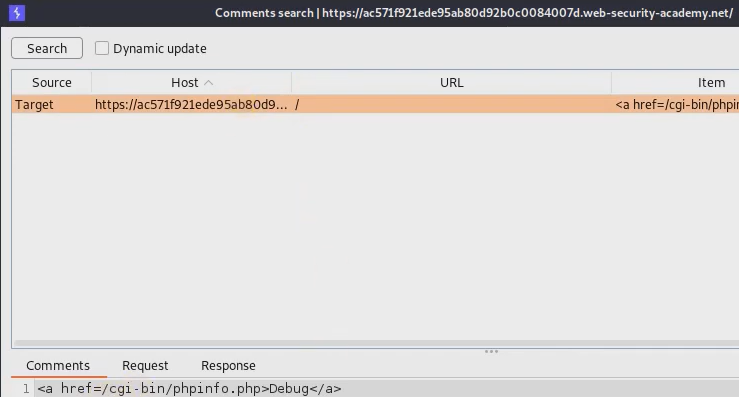
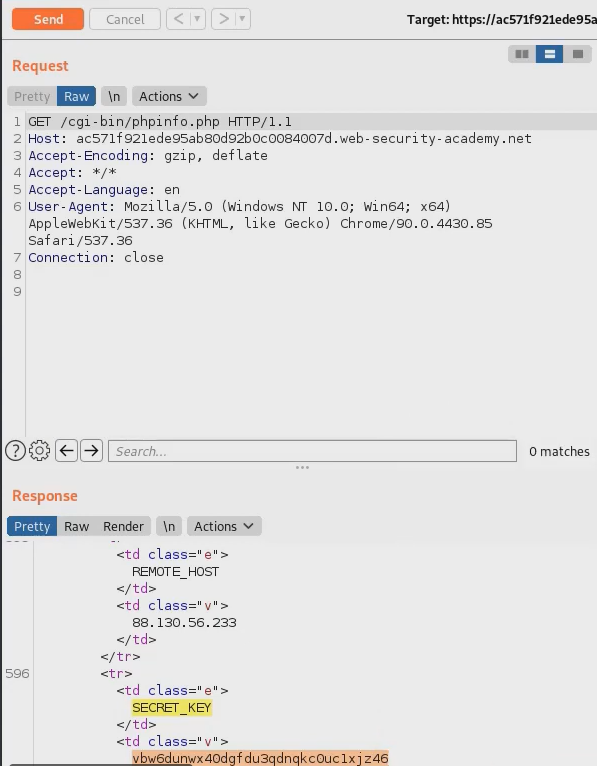
The application has a debug page that unwarily provides internal and potentially sensitive application data, including environment variables.

**PROCEDURE**

1. While routing through Burp, navigate to the main page.
2. Discover the "Debug" link through content discovery or by scanning HTML comments.
3. Requesting this debug page divulges several debugging details, among which we spot the SECRET\_KEY environment variable.

**PAYLOAD**

GET request to /cgi-bin/phpinfo.php

******PROOF OF CONCEPT  
  
  
  
REMEDIATION**

1. **Limit Debug Information:** Avoid revealing detailed debug information publicly, especially in a production environment.
2. **Access Controls:** Implement strict access controls for any route that might provide sensitive application details.
3. **Secure Environment Variables:** Always protect and encrypt critical environment variables, ensuring they aren't leaked.