SCENARIO

This application is vulnerable to password reset poisoning. The user carlos will carelessly click on any links in emails that he receives. To solve the lab, log in to Carlos's account. We will try to get access to his account.

**PROCEDURE**

1. Open the web application and log in using the provided credentials.
2. Go to forgot password functionality of the application and try to reset our own password using the provided credentials.
3. Study all the requests properly and we see that the reset link contains a token for every password reset which could be stolen using exploit server.
4. Now if we change the requests parameters as follows:
   * Username as carlos.
   * Host header parameter as our exploit server.
5. Now we send the request and carlos will receive a request with the token number but the domain name will be ours so we can see the request made to our server on the backend using the access log.
6. Now replay the request with the token we got on the access logs and now we can reset the password.

**PAYLOAD**

https://

**REMEDIATION**

1. **Validate Email Links:** Ensure that all links sent via email are generated only from server-side configurations and not based on user input. This reduces the risk of an attacker providing malicious URLs.
2. **Token Binding to Session:** Associate password reset tokens with the user's session or IP address. This way, even if an attacker intercepts the token, it won't be valid from their session or IP.
3. **Limit Host Header Dependency:** Avoid dependence on the HTTP Host header for critical functionalities. If necessary, validate the Host header against a whitelist of allowed domains.
4. **Secondary Verification:** Before a password reset is finalized, ask the user to answer security questions or provide another form of verification.
5. **Rate Limit & Monitor Reset Requests:** Implement rate limiting on password reset requests. Too many requests in a short time frame can be an indication of an attack. Monitoring and alerting mechanisms can notify administrators of such suspicious activities.