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**