SCENARIO

The application contains a DOM based open redirection vulnerability which redirects the user to our exploit server. We’ll try to exploit this vulnerability by forcing the user to redirect to the exploit server.

**PROCEDURE**

1. Access the application and open any blog to inspect its source code.
2. Upon inspecting we see that there is a button for going back to the home page which includes:

<a href='#' onclick='returnURL' = /url=https?:\/\/.+)/.exec(location); if(returnUrl)location.href = returnUrl[1];else location.href = "/"'>Back to Blog</a>

1. We notice that the URL parameter contains an open redirection vulnerability that allows you to change the location where the Back to blog button takes you.
2. So, according to that we will create a payload and navigate to it by injecting it into our URL which will change the URL parameter.

**PAYLOAD**

https://YOUR-LAB-ID.web-security-academy.net/post?postId=4&url=https://YOUR-EXPLOIT-SERVER-ID.exploit-server.net/

**REMEDIATION**