SCENARIO

The application contains a reflected cross site scripting vulnerability in the search box functionality but it uses a web application firewall to protect against common XSS vectors by blocking all HTML tags except custom ones. We will try to trigger an alert message by injecting a payload into the search box.

**PROCEDURE**

1. Go to the vulnerable application and try searching for anything.
2. As we’re already told that we need to exploit the vulnerability by triggering an alert.
3. We’ll create a payload and then we will send it to the target using our exploit server containing a custom tag with on-focus event handler that fires alert function as soon as the page loads.

**PAYLOAD**

1. <script>

location = 'https://YOUR-LAB-ID.web-security-academy.net/?search=%3Cxss+id%3Dx+onfocus%3Dalert%28document.cookie%29%20tabindex=1%3E#x';

</script>

**REMEDIATION**