SCENARIO

The application contains a reflected DOM based cross site scripting vulnerability in the search box functionality but it uses a web application firewall to protect against common XSS vectors. 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. Use BurpSuite’s Repeater and send the Payload 1 and you’ll observe that it gets blocked.
3. Now open the XSS cheat sheet and copy all the possible tags and mount a brute force attack using BurpSuite’s Intruder in the search parameter enclosed within <§§> tags.
4. We can see that except <body> tag, all others threw a 404 blocked response.
5. Now put the Payload 2 in place of the search parameter.
6. In the Payload 2 use the cheat sheet again and copy all the possible events and mount a brute force attack using it.
7. Notice that only the event **onresize** there was a response code of 200 and not 400.
8. In the end, we will create a final payload 3 and will send it to the user using our exploit server to trigger the desired event.

**PAYLOAD**

1. <img src=1 onerror=print()>
2. <body%20§§=1>
3. <iframe src="https://YOUR-LAB-ID.web-security-academy.net/?search=%22%3E%3Cbody%20onresize=print()%3E" onload=this.style.width='100px'>

**PROOF OF CONCEPT**

****

**REMEDIATION**

1. **Encode User Input:** Always sanitize and encode all user inputs. Convert characters like <, >, &, " to their HTML encoded counterparts. For example, < should be encoded to &lt;.
2. **Use Secure Libraries:** Make use of security-focused libraries or frameworks that automatically escape user input, like OWASP's Java Encoder for Java applications.
3. **Content Security Policy (CSP):** Implement a strict CSP. This is a security feature provided by browsers to prevent XSS. With a proper CSP, even if an attacker manages to inject malicious scripts, the browser will not execute them.
4. **Positive Security Model:** Rather than trying to identify and block malicious inputs, identify and allow only known good inputs. This is also known as whitelisting.