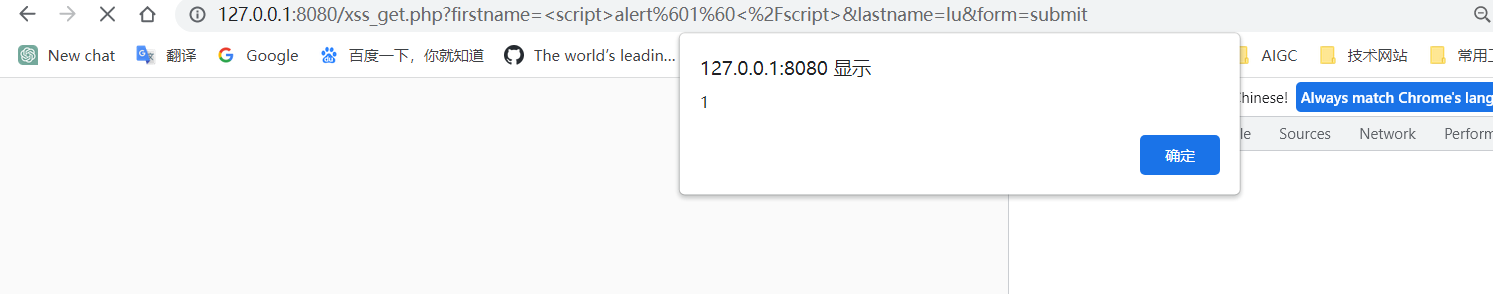
按下按钮页面显示输入框信息在welcome后面，因此可在输入框注入xss

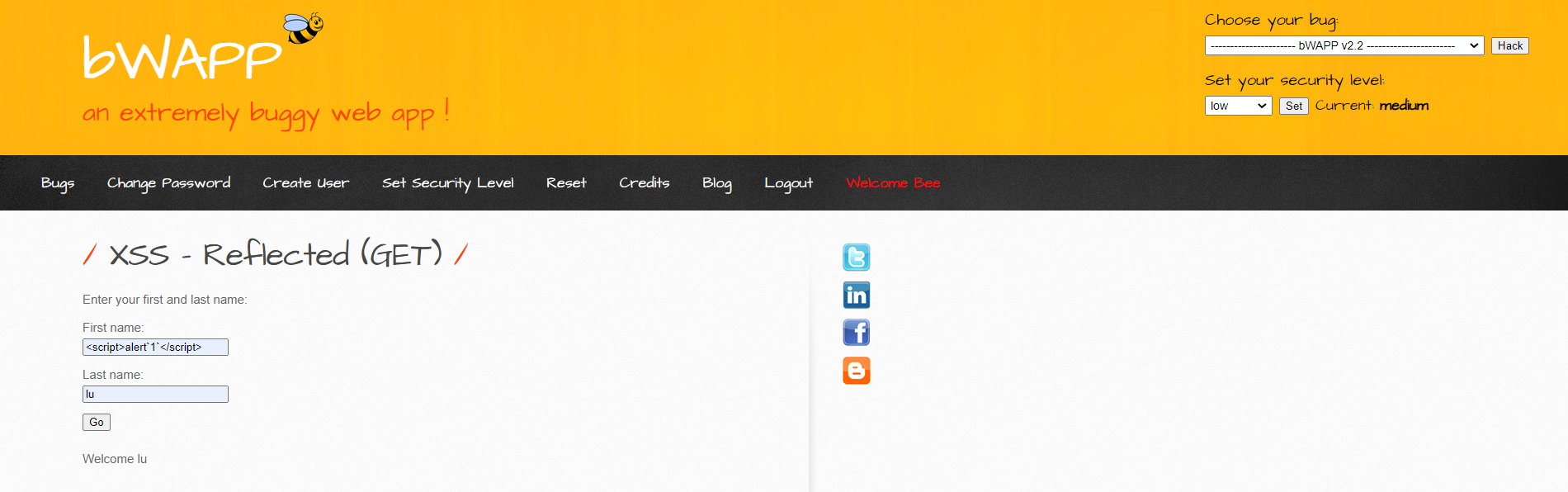
直接注入xss脚本

<script>alert`1`</script>

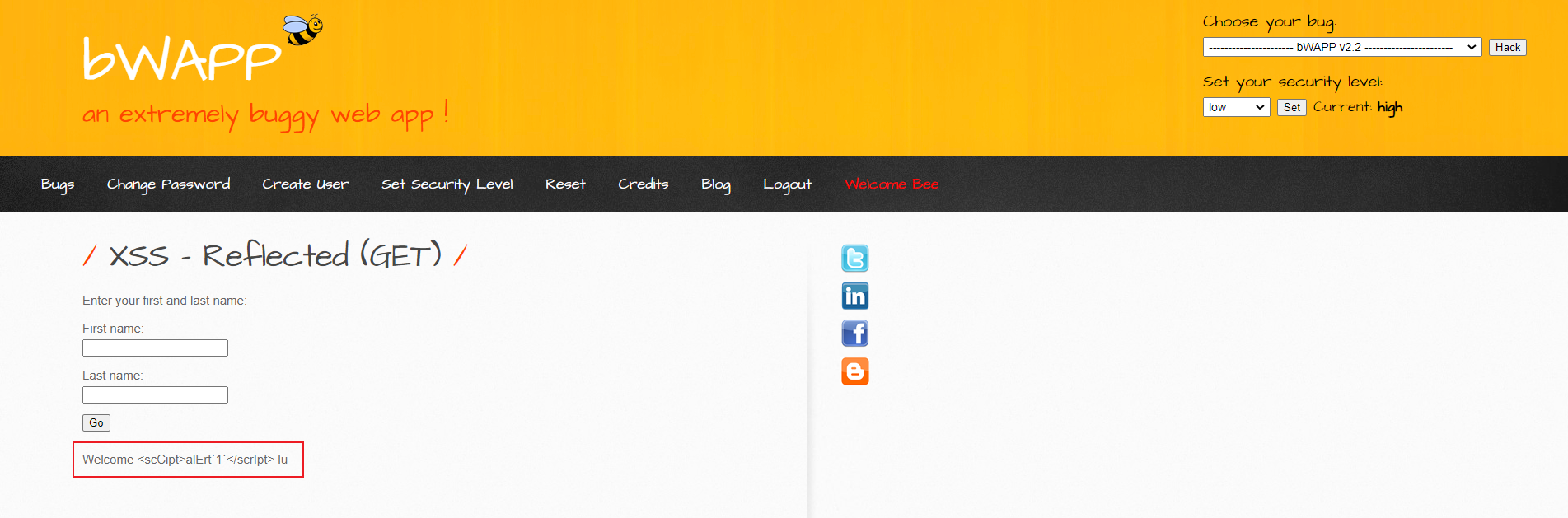
lu

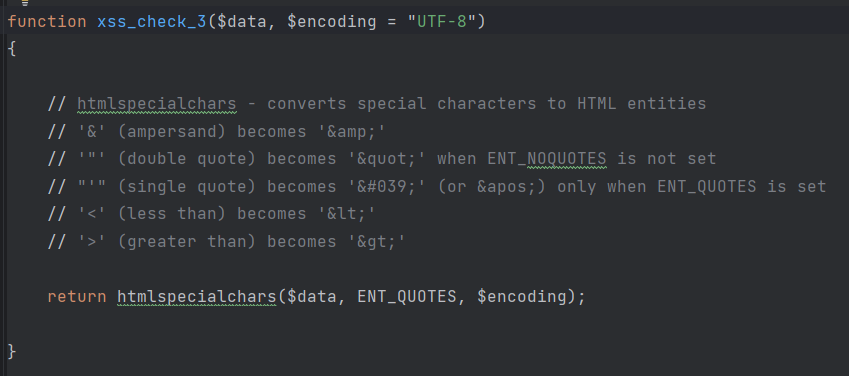
成功注入xss，无风险

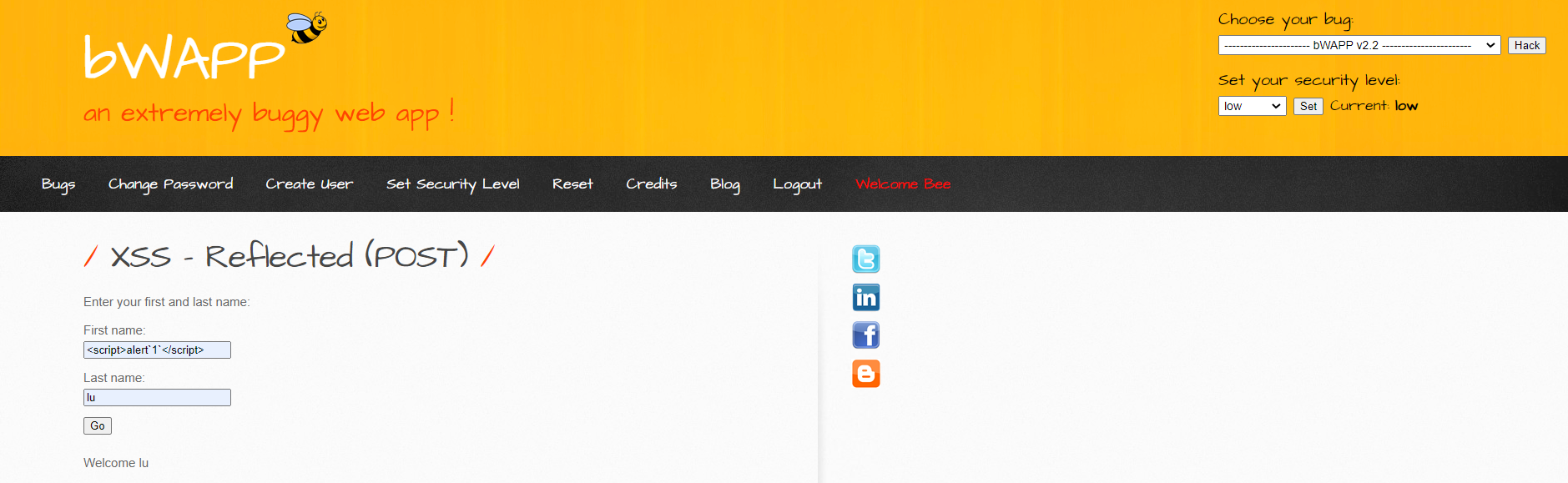
medium级别也一样

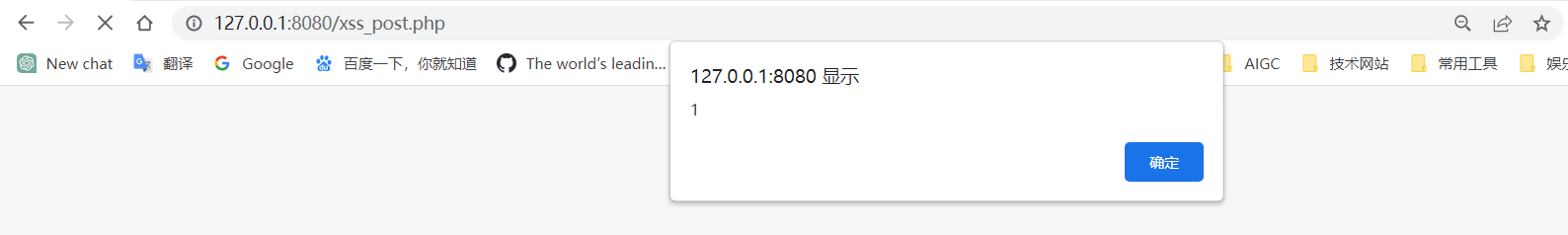
同样也能注入

high无法注入

代码审计，xss注入所需特殊符号均被实体编码，无法注入xss

post同get

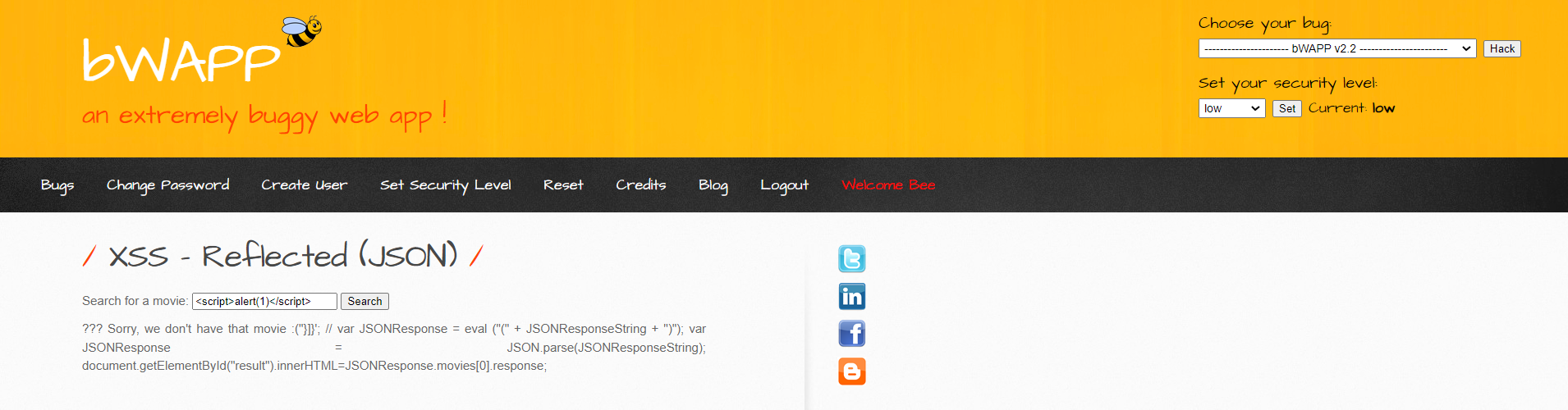
触发xss

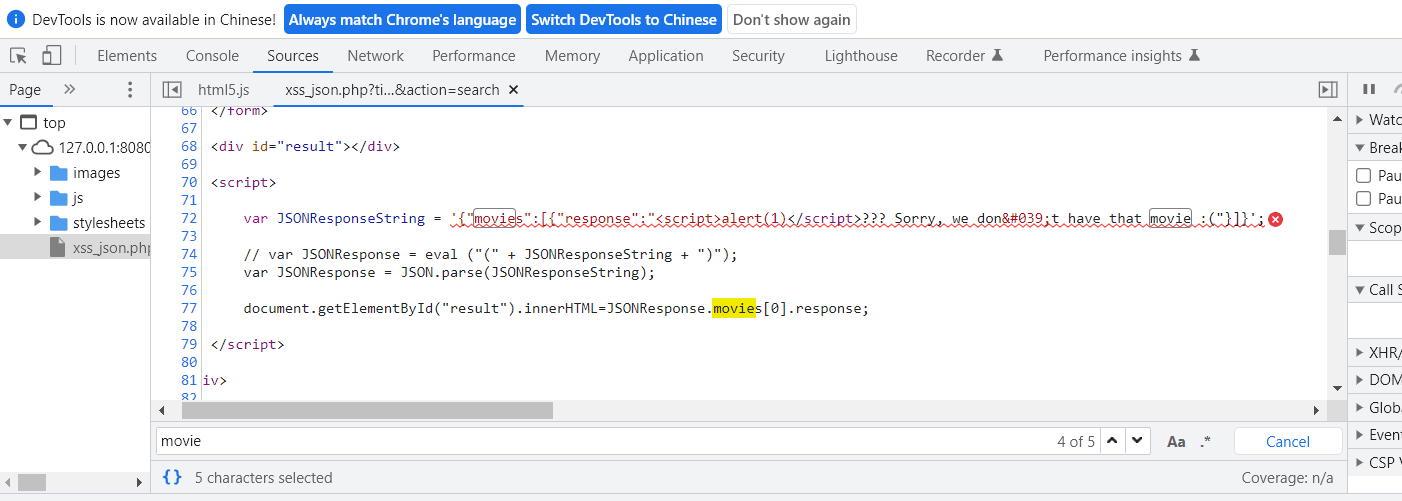
low、medium、high注入过程和注入结果同get页面

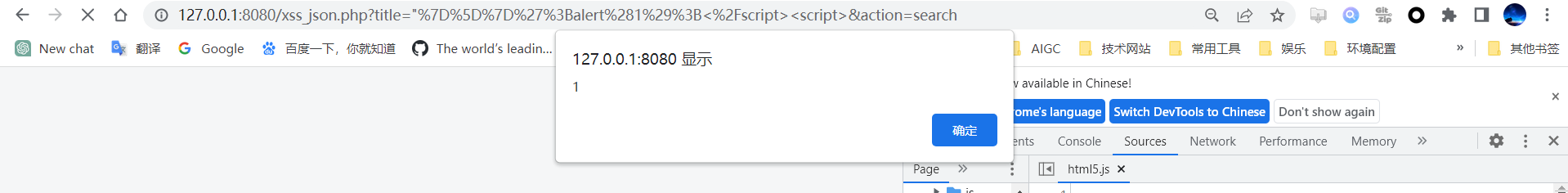
json

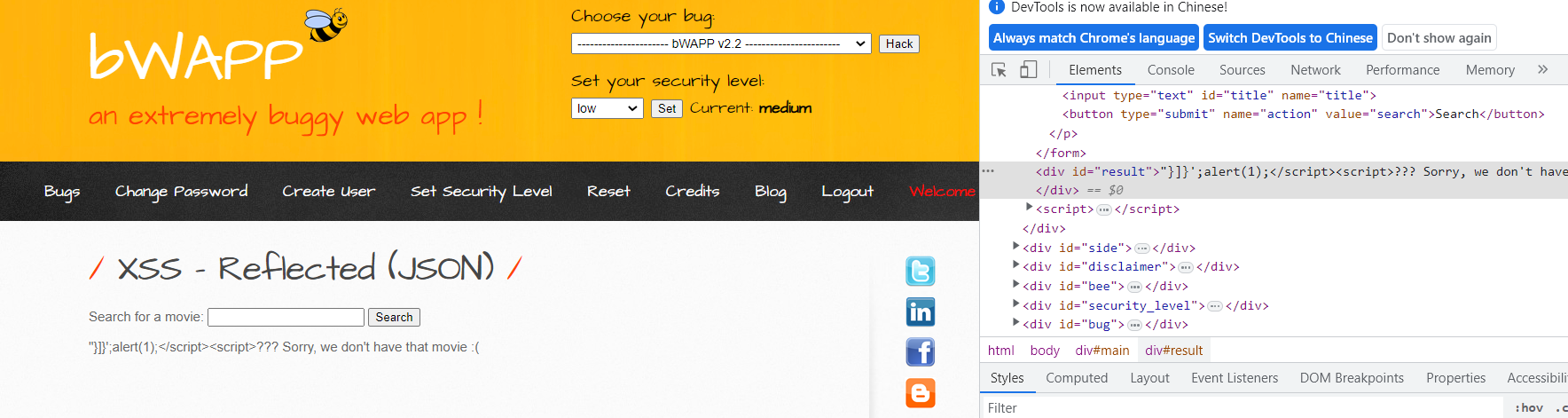
直接注入xss

<script>alert(1)</script>，出现报错

搜索源码，发现需要闭合json标签

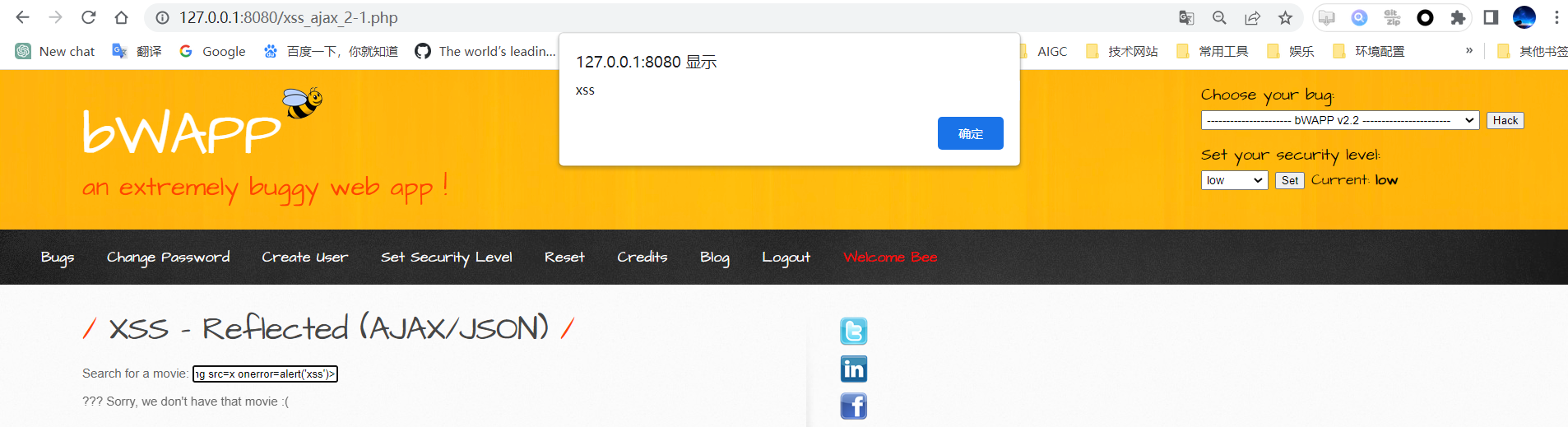
，输入"}]}';alert(1);</script><script>，闭合前面json标签和后面script标签，成功执行

medium和high应该都使用html实体编码，没有报错信息

Cross-Site Scripting - Reflected (AJAX/JSON)

low&medium

<img src=x onerror=alert('xss')>

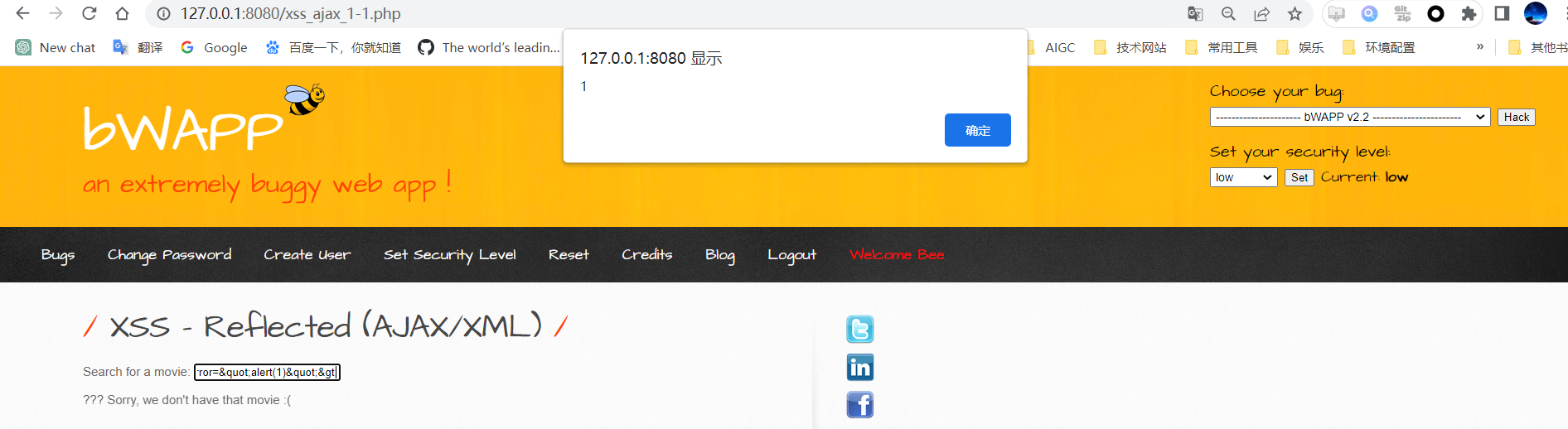
high



Cross-Site Scripting - Reflected (AJAX/XML)

low&medium

&lt;img src=0 onerror=&quot;alert(1)&quot;&gt;

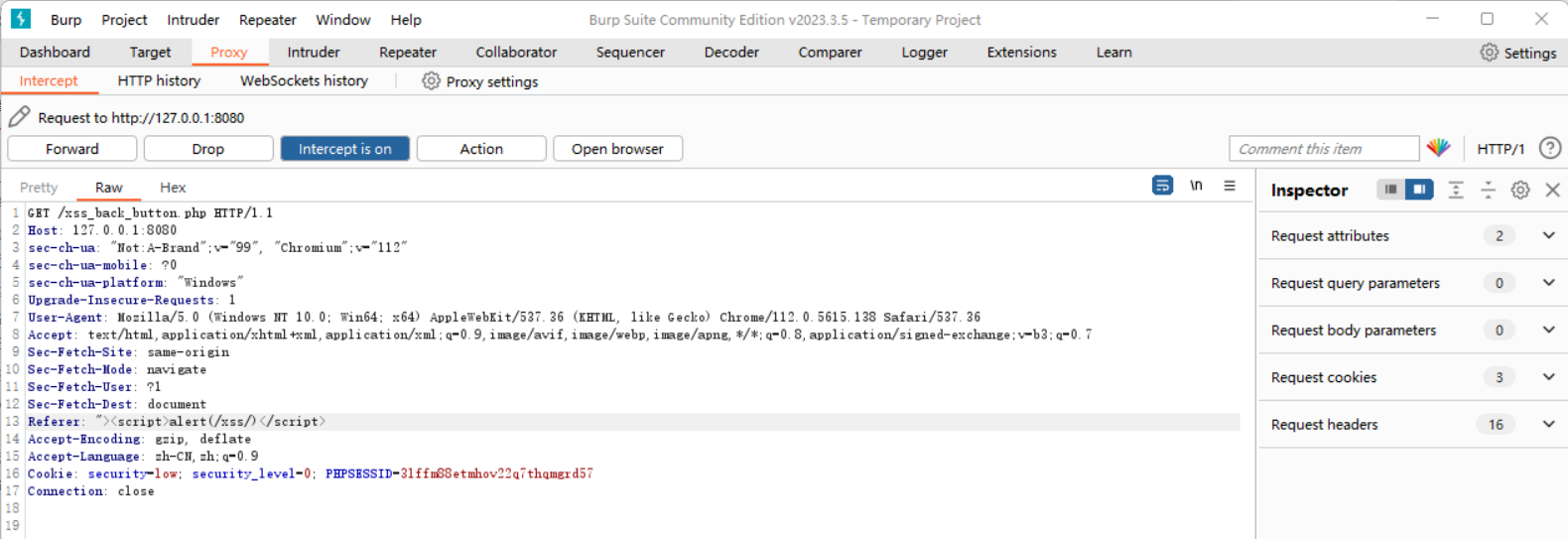
high过滤了

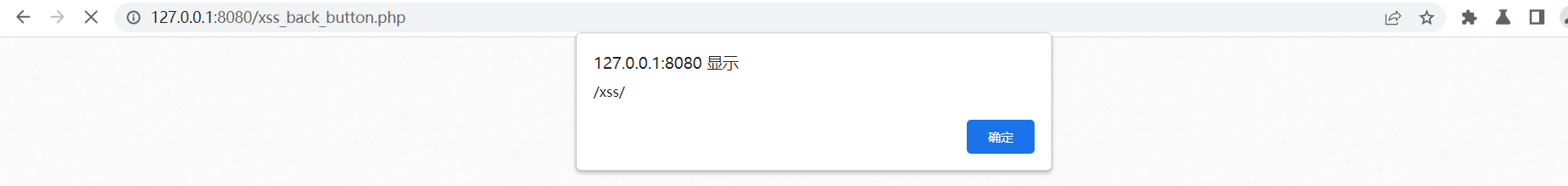


XSS - Reflected (Back Button)

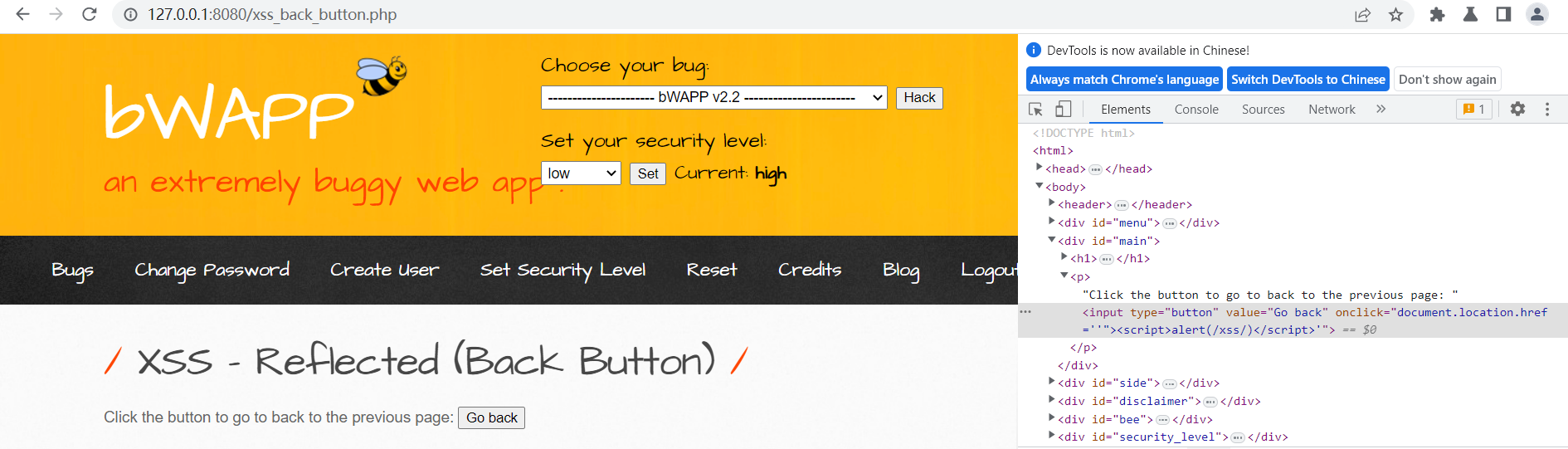
low&medium

"><script>alert(/xss/)</script>

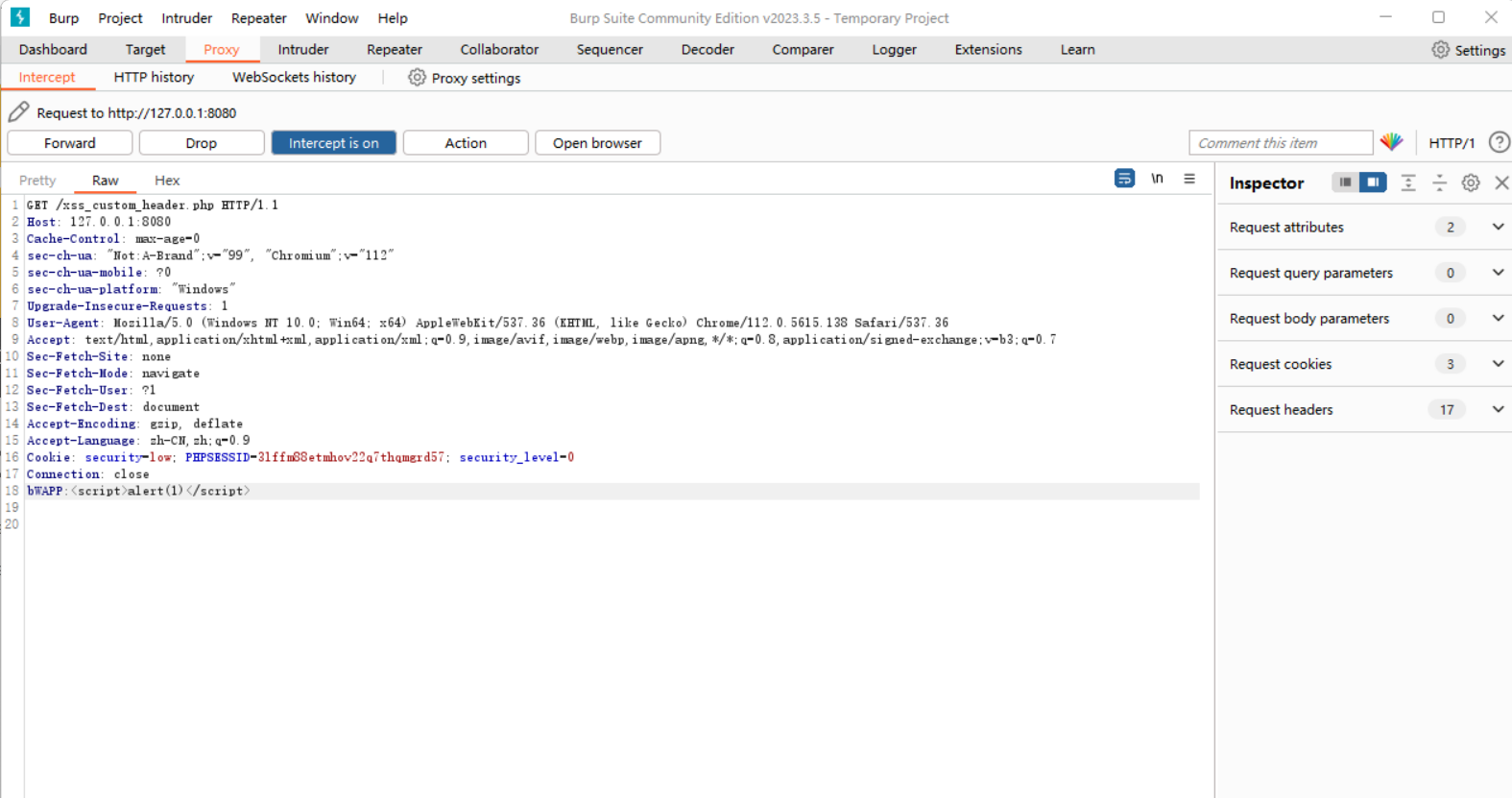


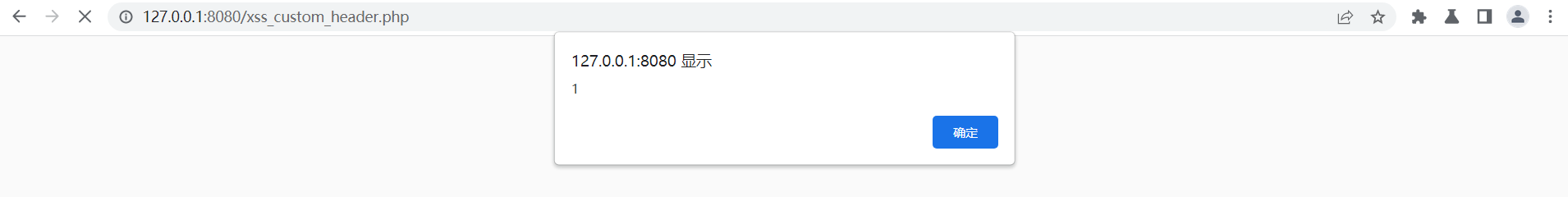
high

无法直接闭合



# ****XSS - Reflected (Custom Header)****

成功注入xss

Medium

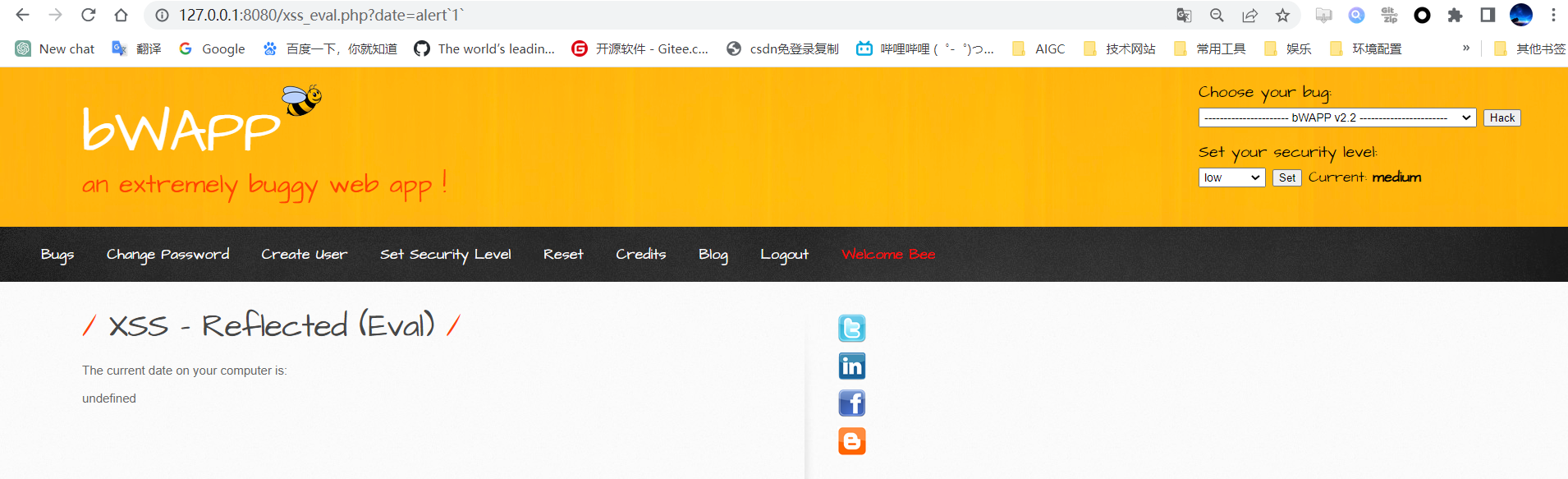
由于采用了addslashes()函数转义单引号等字符, 但是仍可以xss注入

High

将所有关键字转换为HTML实体, 安全:

## ****XSS - Reflected (Eval)****

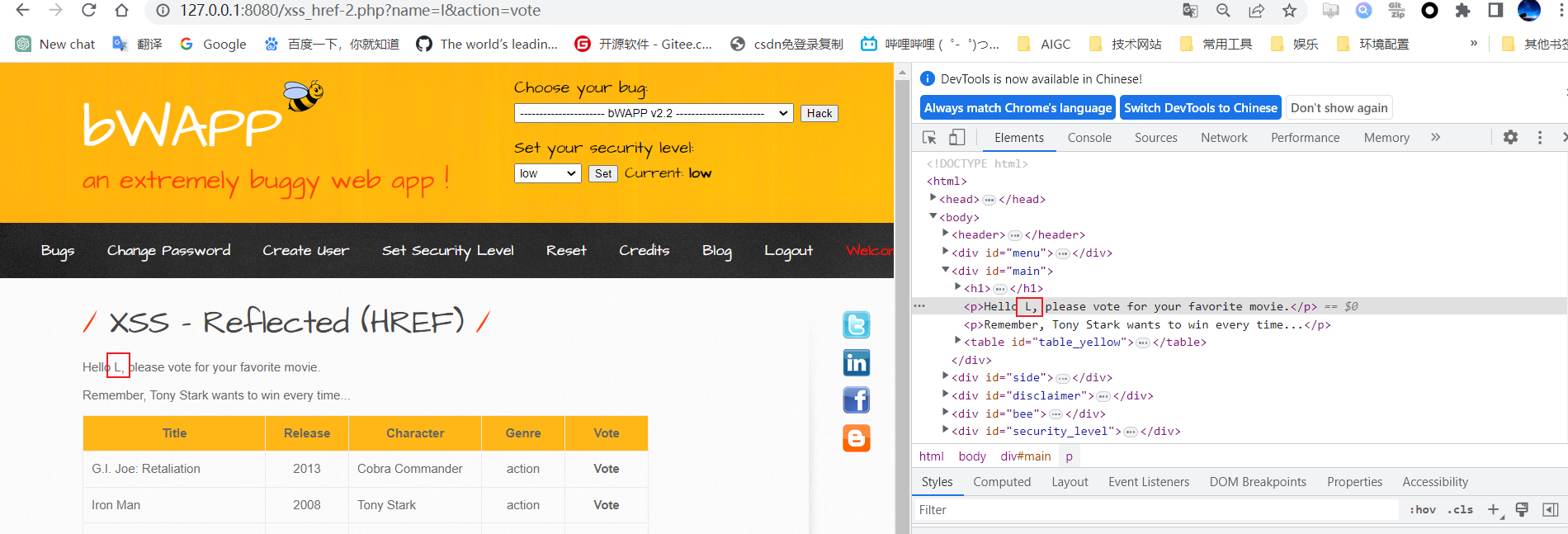
****low&medium****

high

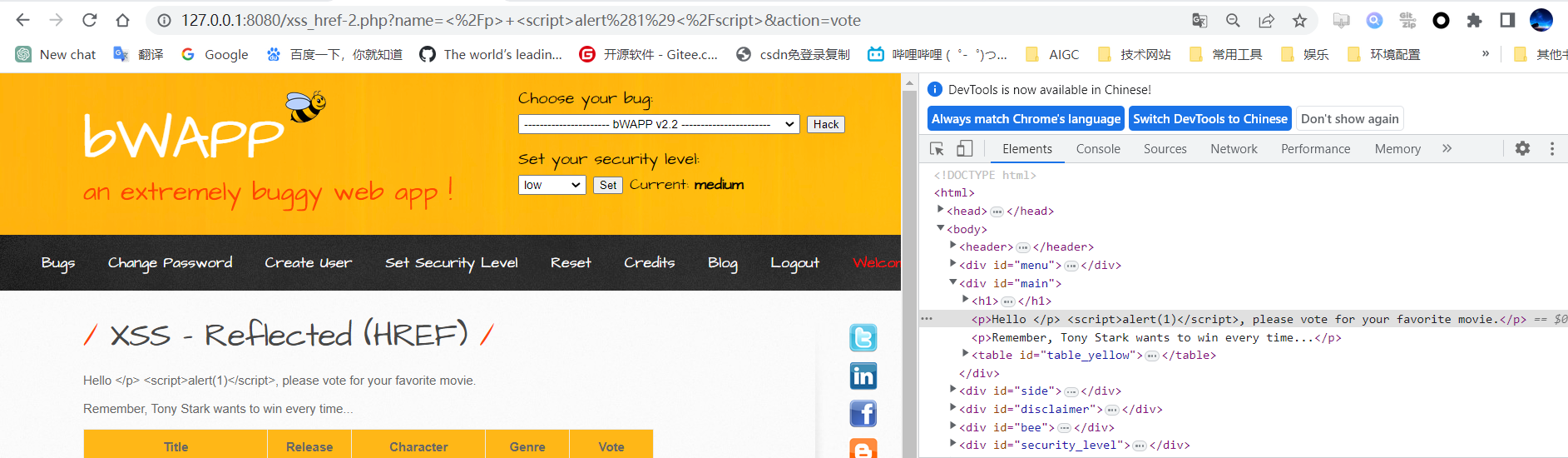
源码中使用了htmlspecialchars()函数来进行过滤

XSS - Reflected (HREF)

low

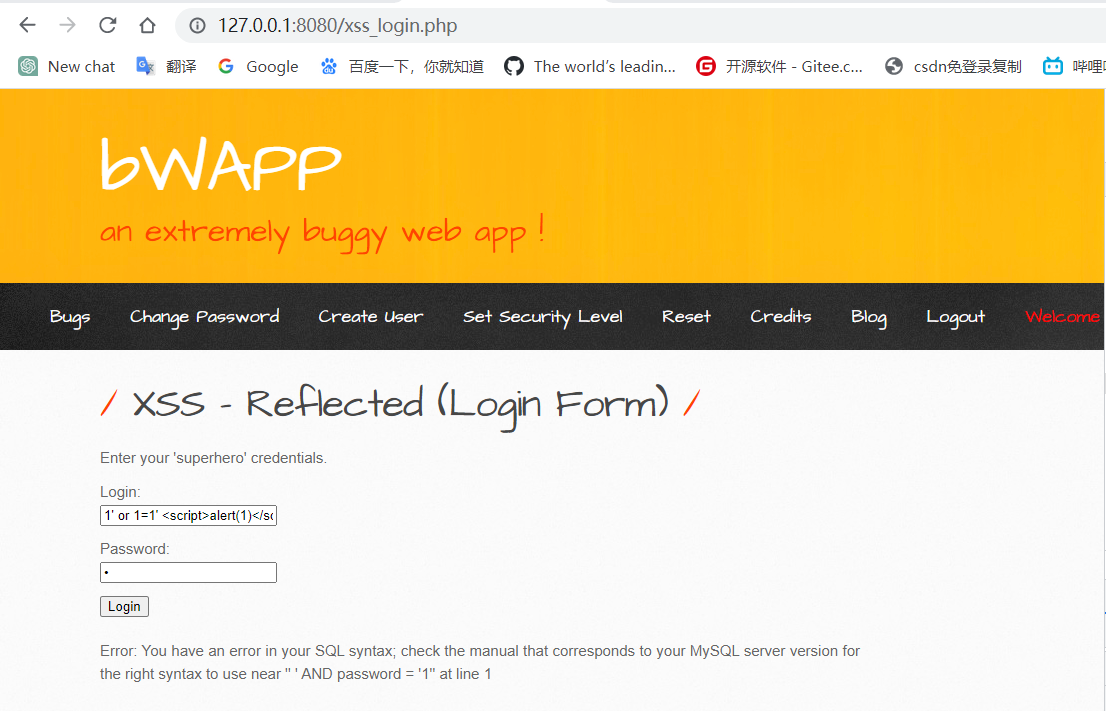
medium&high

源码中使用了urlencode()函数来进行过滤。



XSS - Reflected (Login Form)

使用万能密码： 1' or 1=1' 加入XSS的Payload ，导致在mysql\_error()函数报错时，执行html语句  
Payload: 1' or 1=1' <script>alert(1)</script>  
报错信息：Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' <script>alert(1)</script>' AND password = 'bug'' at line 1



Medium

源码中使用了addslashes()函数来进行过滤，因为有转义，所以该函数无效。

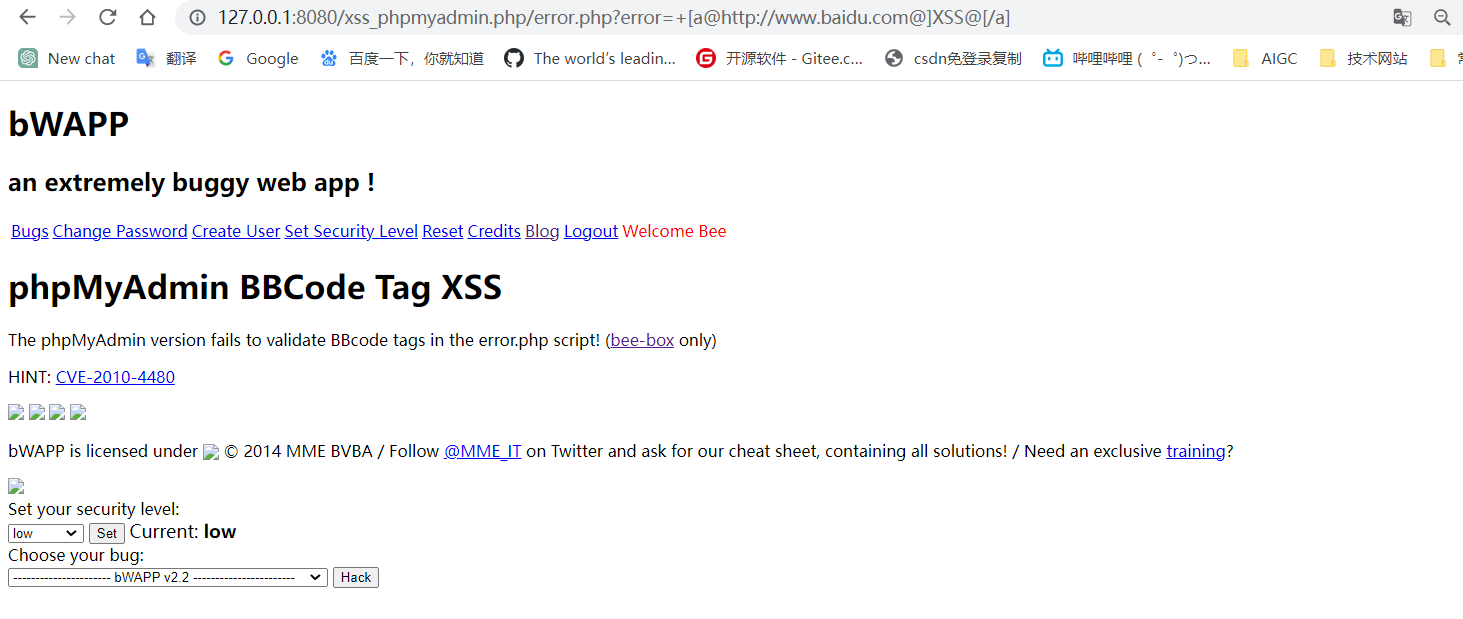
High

源码中使用了htmlspecialchars()函数来进行过滤。

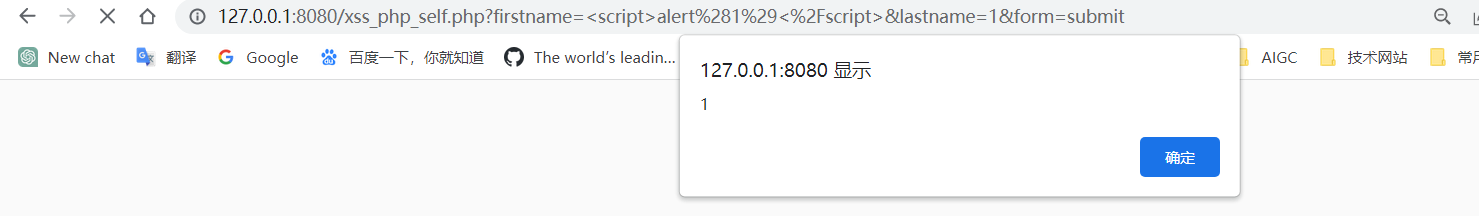
## phpMyAdmin BBCode Tag XSS

/error.php?error=+[[a@http](mailto:a@http)://www.baidu.com@]XSS@[/a]

失败

XSS - Reflected (PHP\_SELF)



Medium

源码中使用了addslashes()函数来进行过滤。

High

源码中使用了htmlspecialchars()函数来进行过滤。

XSS - Reflected (Referer)

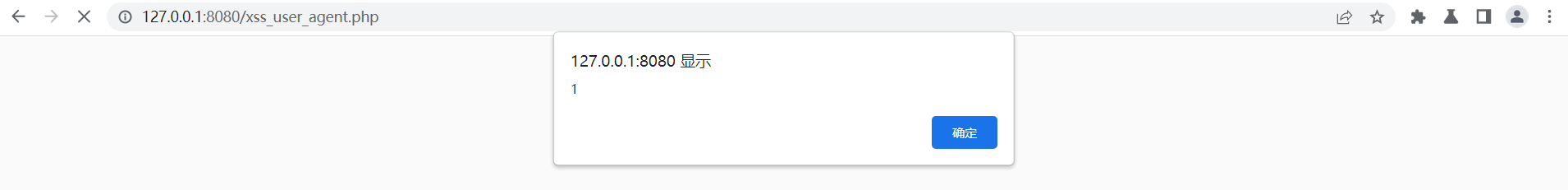
直接在Referer里加入XSS的Payload



XSS - Reflected (User-Agent)

直接在 User-Agent 里加入 XSS的Payload



XSS - Stored (Change Secret)

