

# 基于Firefox的Hackbar插件配置与应用

---

## 实验目的

---

通过本实验理解基于Firefox的Hackbar插件配置与应用方法，掌握渗透测试过程中如何应用Hackbar的各项功能。

## 实验环境

---

渗透主机: Kali

用户名: college

密码: 360College

工具: Firefox

目标靶机: Y-SQLi-Labs

用户名: college

密码: 360College

## 实验原理

---

Web渗透测试时，经常要和浏览器地址栏内容进行交互，比如添加或修改参数，变更URL等。有些服务器的响应包含重定向、重载、参数变化，所有的这些改变的获得需要花费大量的时间去在这些变量上尝试不同的参数，借助合适的工具，可以大大缩短这一过程的繁琐程度。

Hackbar是一个Firefox的插件，它的功能类似于地址栏，但是它里面的数据不受服务响应触发的重定向等其它变化的影响，这一功能在我们后面测试Web应用中十分有帮助。

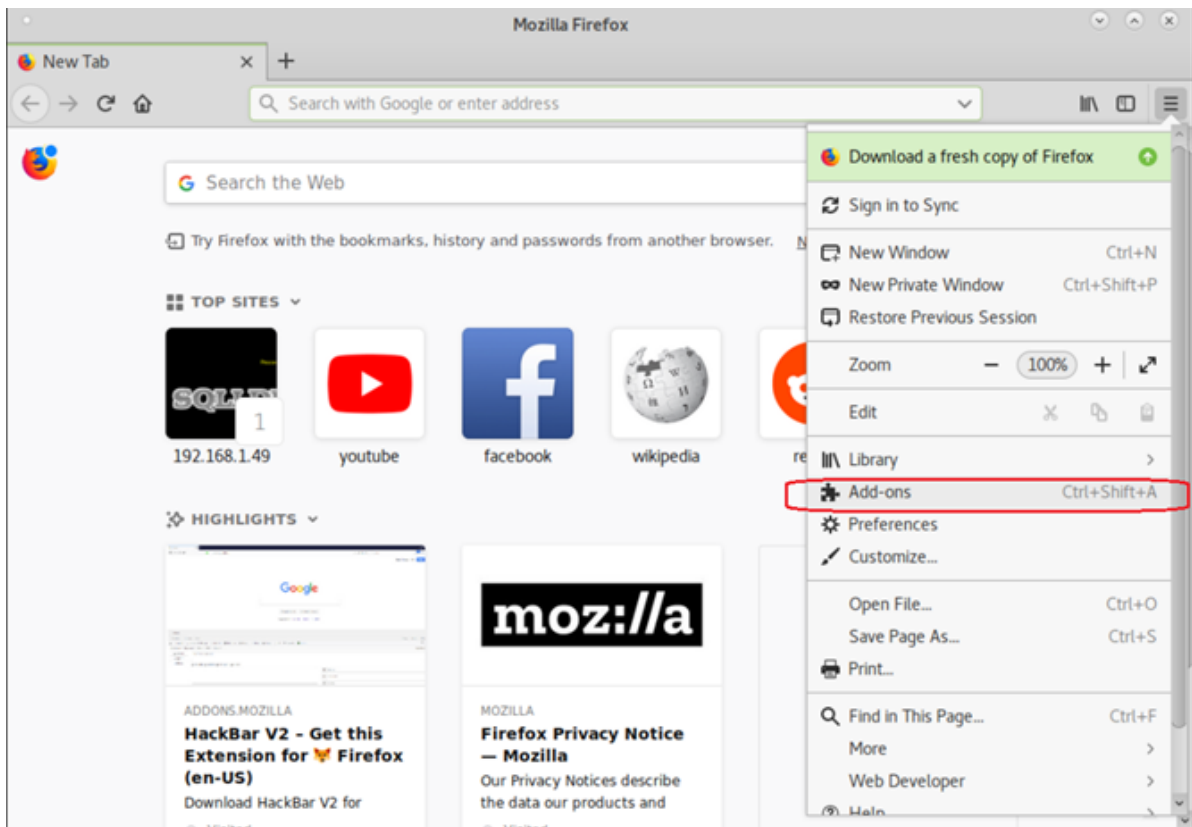
## 实验步骤

---

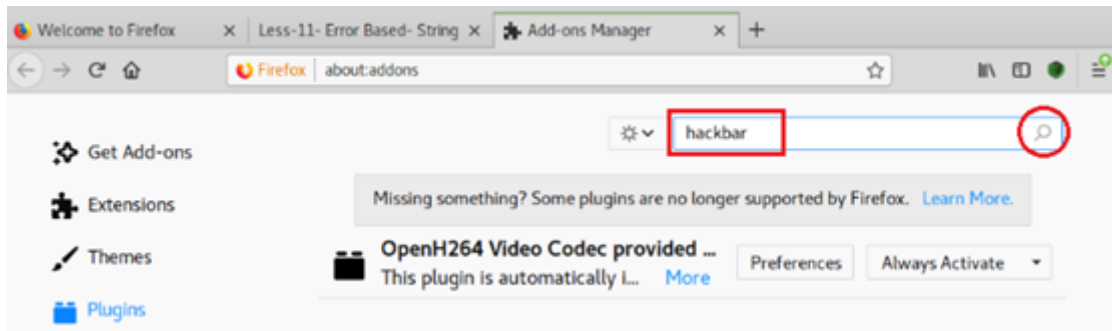
### 第一步 登录SQLI-Labs平台

### 第二步 登录Kali平台，启动firefox浏览器，并安装hackbar插件




(1) 浏览器中此路径下安装




(2) 输入关键字进行搜索



(3) 选择要安装"HackBar V2"

	<b>New Hackbar</b> A sitebar that helps pentesters to perform manual web security testing inside their browser. This addon is written in webextension and alternatives to the XUL version of original Hackbar. ★★☆☆☆ mxcx	1,891 users
	<b>HackBar V2</b> [No License, FOREVER FREE] A HackBar for new firefox (Firefox Quantum). This addon is written in webextension and alternatives to the XUL version of original Hackbar. ★★★★★ chewbaka	1,955 users
	<b>Quantum Hackbar</b> Hackbar port for the new WebExtensions API. It's redesigned and optimized to work with the new Firefox Quantum. It sits in your DevTools - Click F12 to open it. Any suggestions and/or issues are welcome :) ★★★★★ StyleShit	342 users

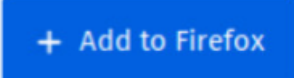
(4) 通过点击“Add to Firefox”来安装此插件



## HackBar V2

by [chewbaka](#)

[No License, FOREVER FREE] A HackBar for new firefox (Firefox Quantum). This addon is written in webextension and alternatives to the XUL version of original Hackbar.




(5) 如果显示“Remove”，表明浏览器已经安装过此插件



# HackBar V2

by [chewbaka](#)

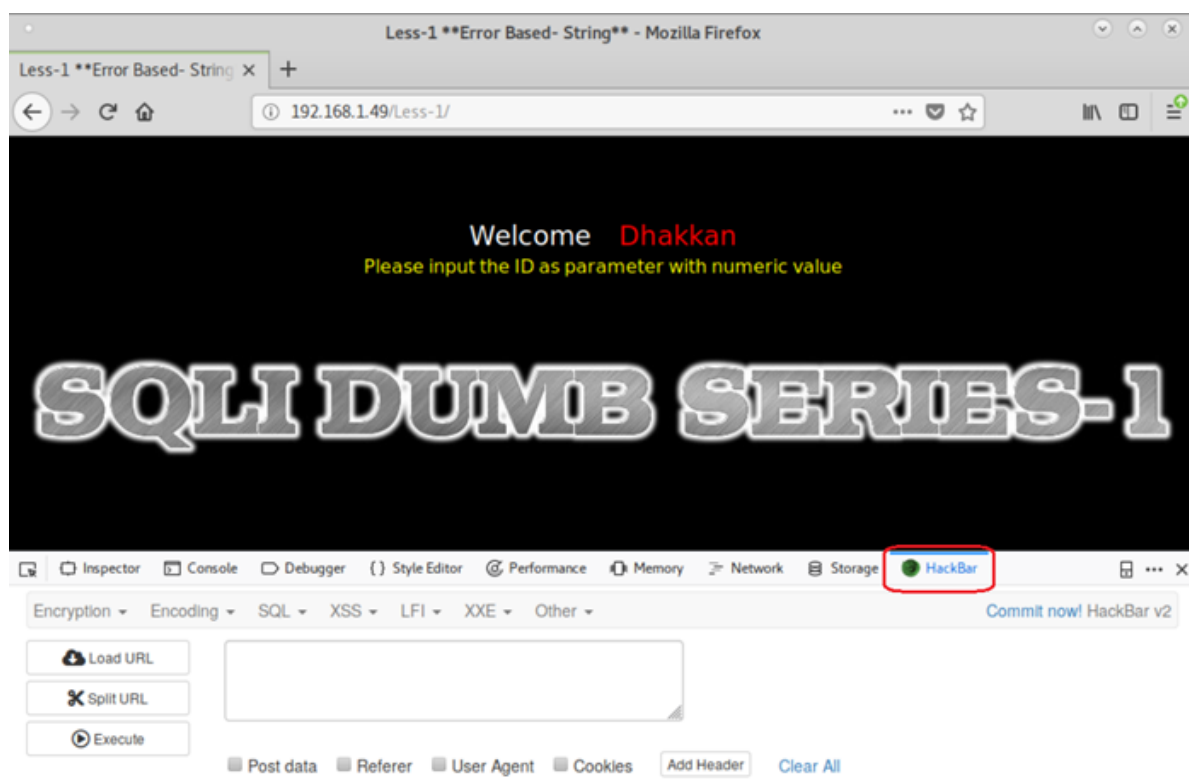
[No License, FOREVER FREE] A HackBar for new firefox (Firefox Quantum). This addon is written in webextension and alternatives to the XUL version of original Hackbar.

 Remove

## 第三步 在firefox启用hackbar插件

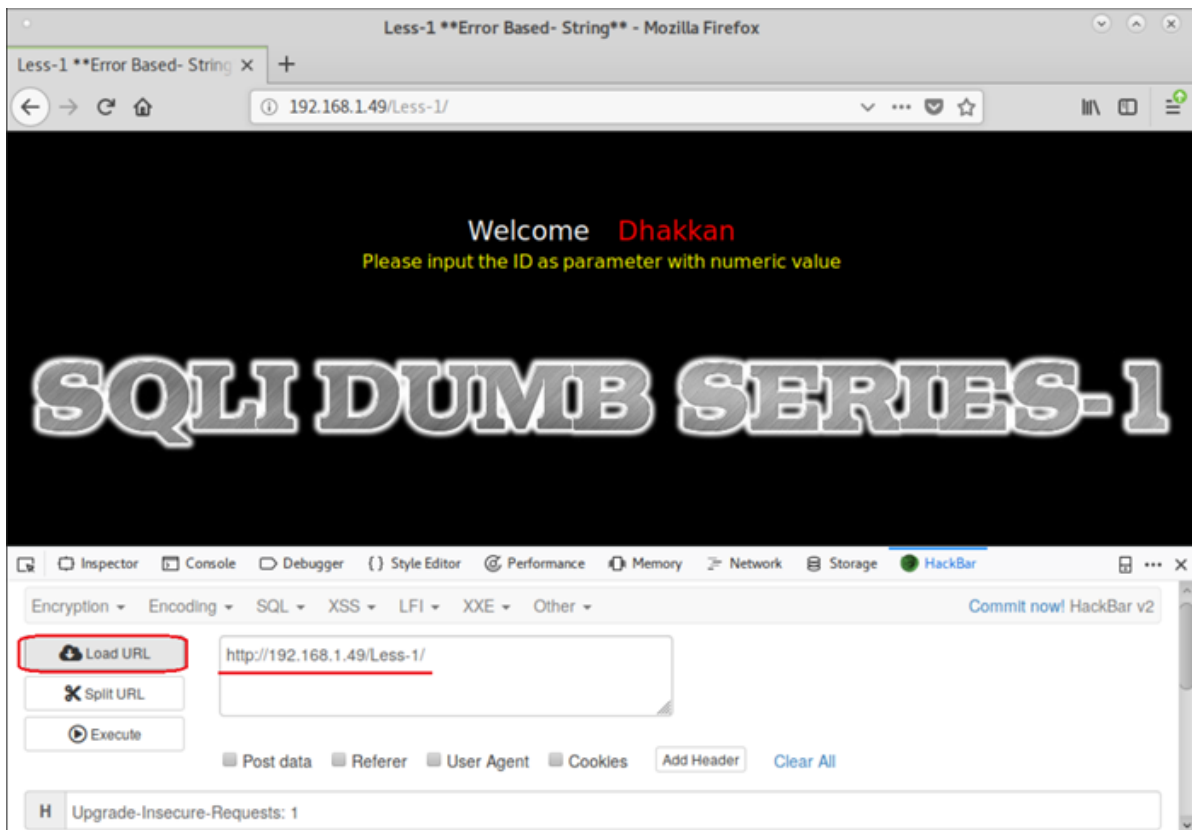
使用快捷键F12启动Hackbar，并访问如下URL：

<http://【靶机IP】/Less-1>

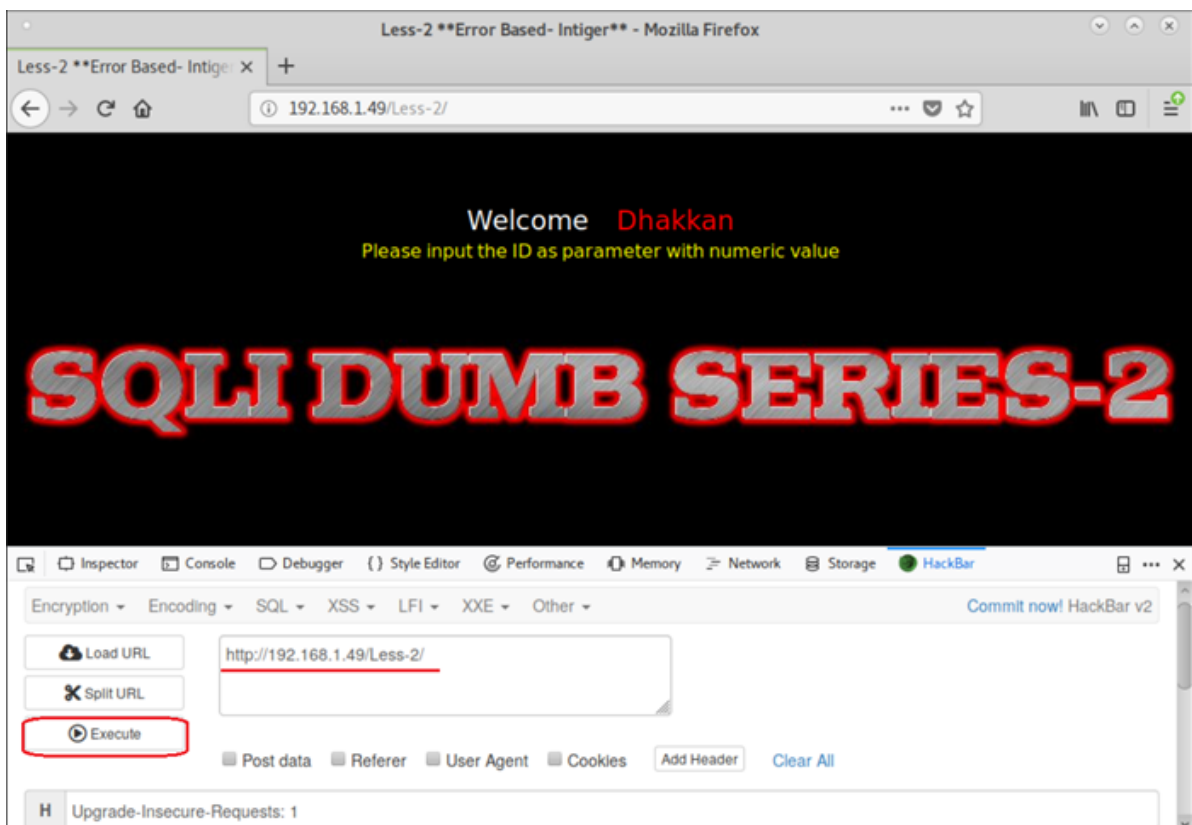


## 第四步 hackbar插件的使用

(1) Load功能的使用。点击“Load URL”将当期URL加载到菜单框中：



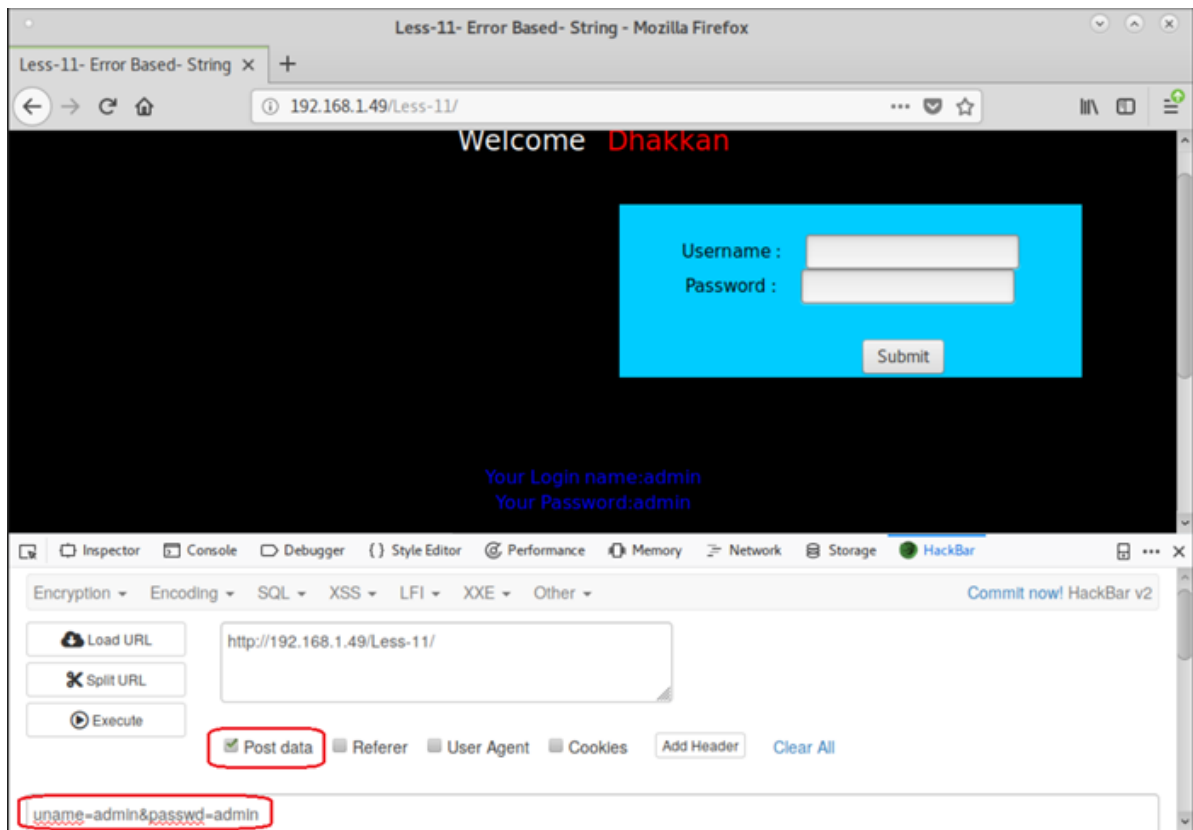
然后，将Hackbar输入框中的URL修改为http://【靶机IP】/Less-2/，并点击“Execute”按钮进行提交，此时便访问对应的web页面



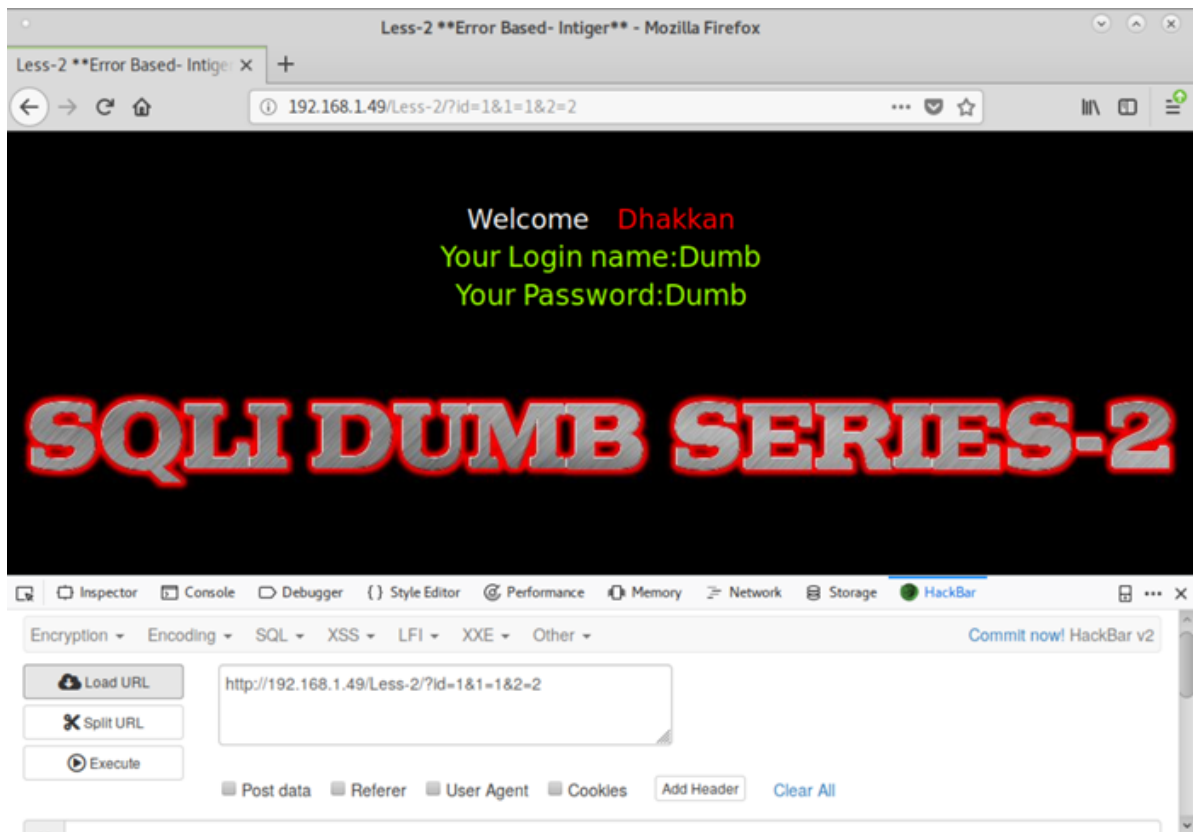
(2) Post功能的使用。在浏览器地址栏中输入http://【靶机IP】/Less-11/，选择访问SQLi-Labs的Less-11，紧接着在hackbar中点击“Load URL”按钮，并勾选“Post data”选项启用Post功能，并在Post数据输入框中填写如下的Post数据：

uname=admin&passwd=admin

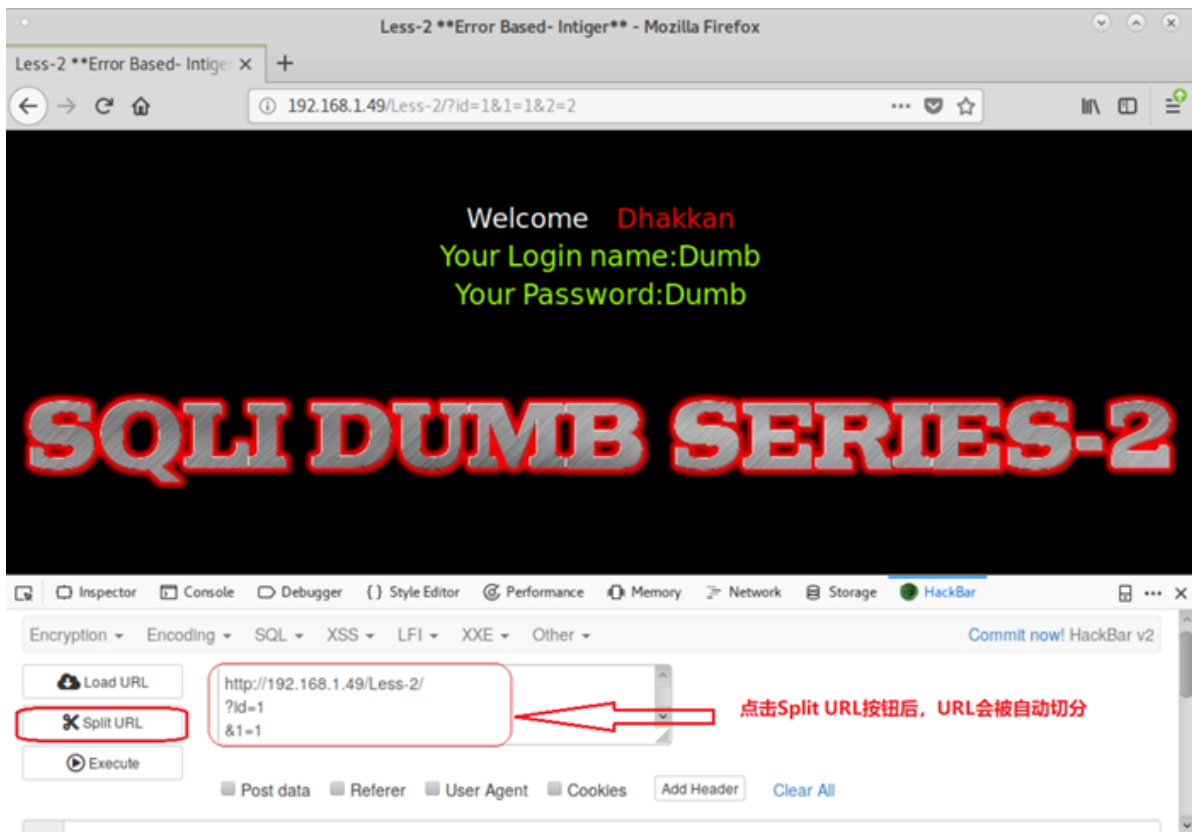
输入完毕，点击“Execute”按钮，访问成功。



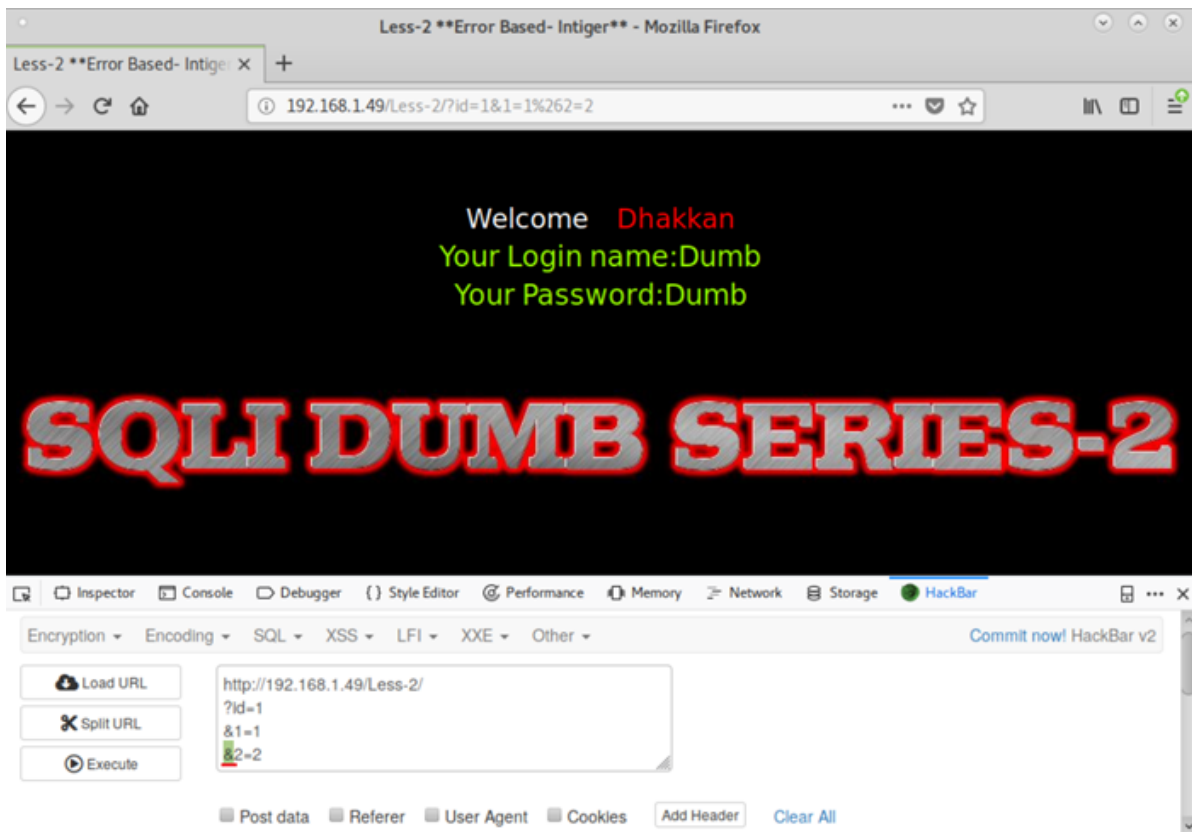
(3) Split功能的使用。选择访问SQLi-Labs的Less-2，输入URL的参数如图所示时对应的Web界面



然后点击“Split URL”按钮，输入框中的URL会被切分（按照不同的动态参数），再次执行“Execute”，Web界面响应结果与上面一致

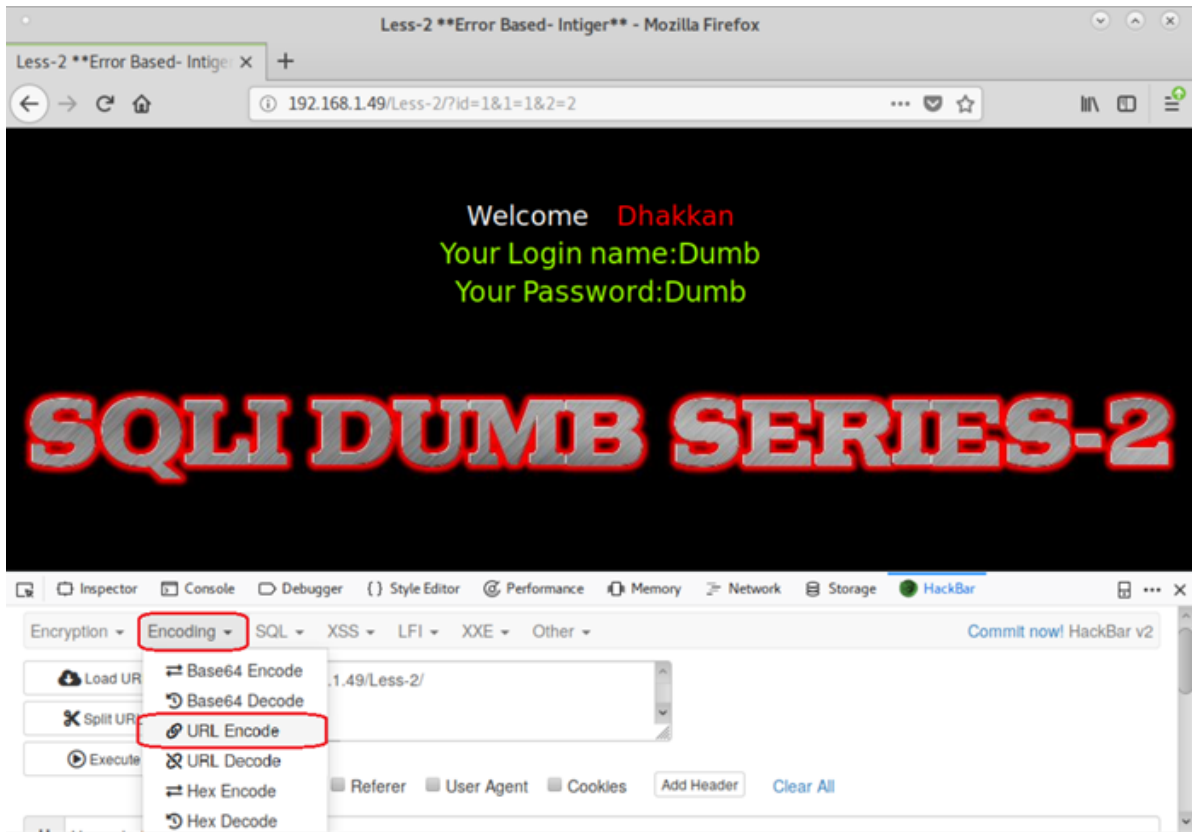


(4) 编码功能的使用。接着上一个场景，在hackbar输入框中选中第二个“&”符号：

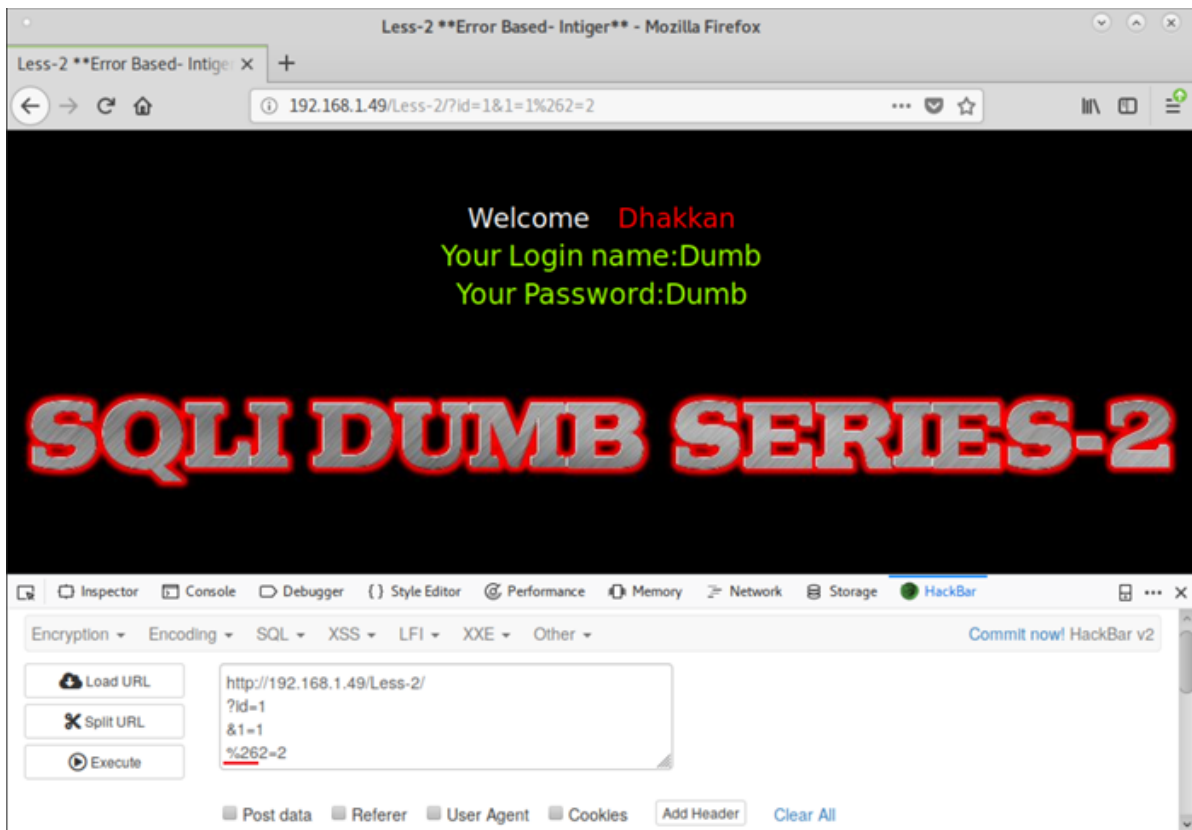


然后点击hackbar菜单项“Encoding”中的“URL Encode”，对“&”符号进行URL编码：





此时“&”符号被编码成了“%26”，再次点击“Execute”提交，Web界面显示结果相同。



## 思考与总结

通过本次实验，成功实现了利用Firefox的插件Hackbar各种功能对目标网站进行了操作，大家要熟练了解和使用Hackbar的其他功能，更加高效的在web渗透中进行使用。



