XSS in Edmodo

惊鸿一瞥最是珍贵 / 2019-03-13 08:12:00 / 浏览数 1755 技术文章 翻译文章 顶(0) 踩(0)

前言

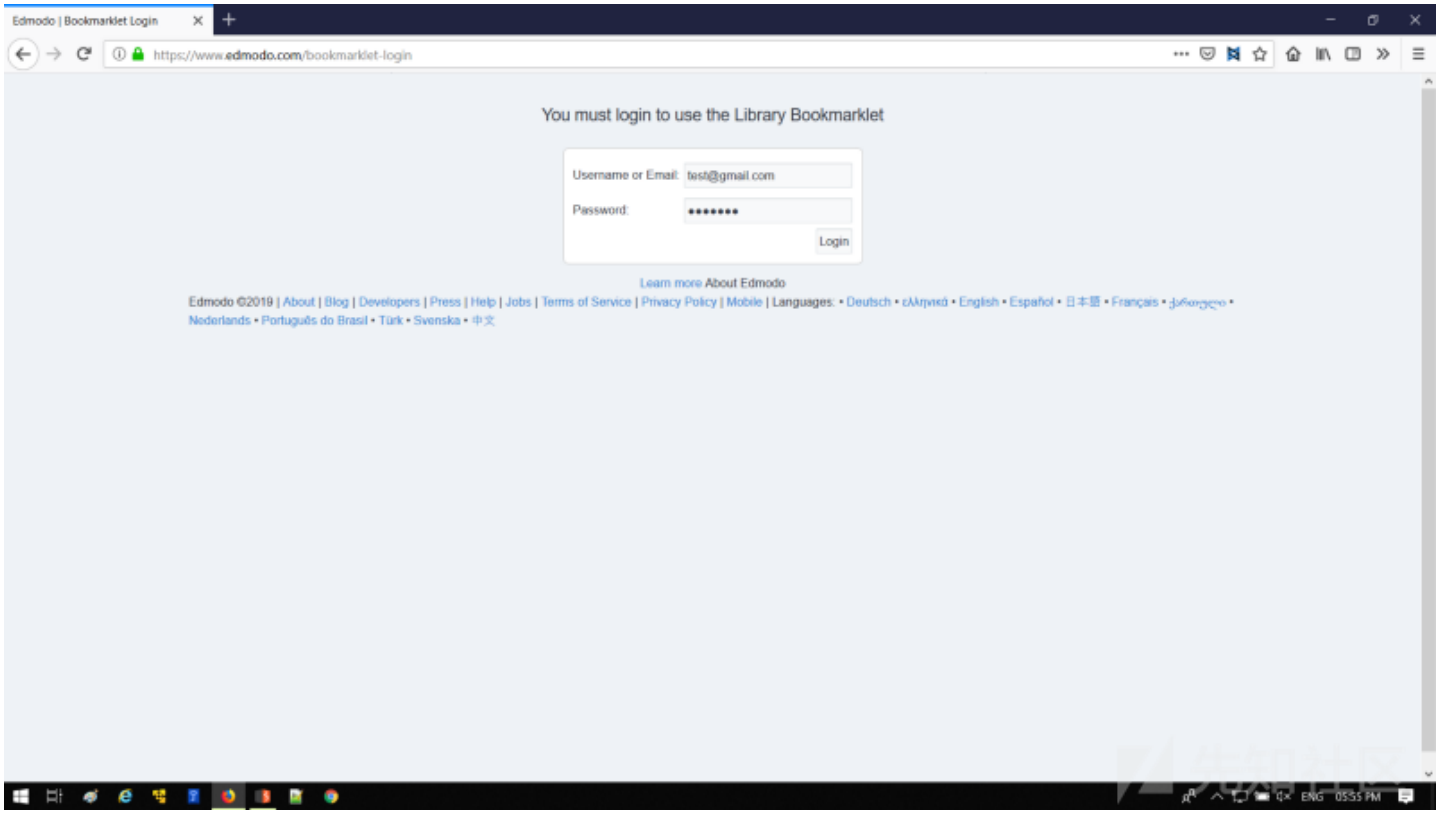
赏金猎人们，你们好！
感谢你们对Edmodo的大力支持，希望所有的同僚都能顺利拿到赏金。
接下来我要告诉大家我是如何在Edmodo中发现XSS的。
这个bug是我在一个月前发现的，在这里我要感谢Parth Shah，他的一篇关于存储型XSS的文章给了我很大的启发。
我刚刚浏览了`edmodo.com`的网站，我发现了两个或更多的URL。页面上没有任何内容，只有一个登录页面和一些过时的Edmodo布局。于是我便试图挖掘更深层次的东西。

细节

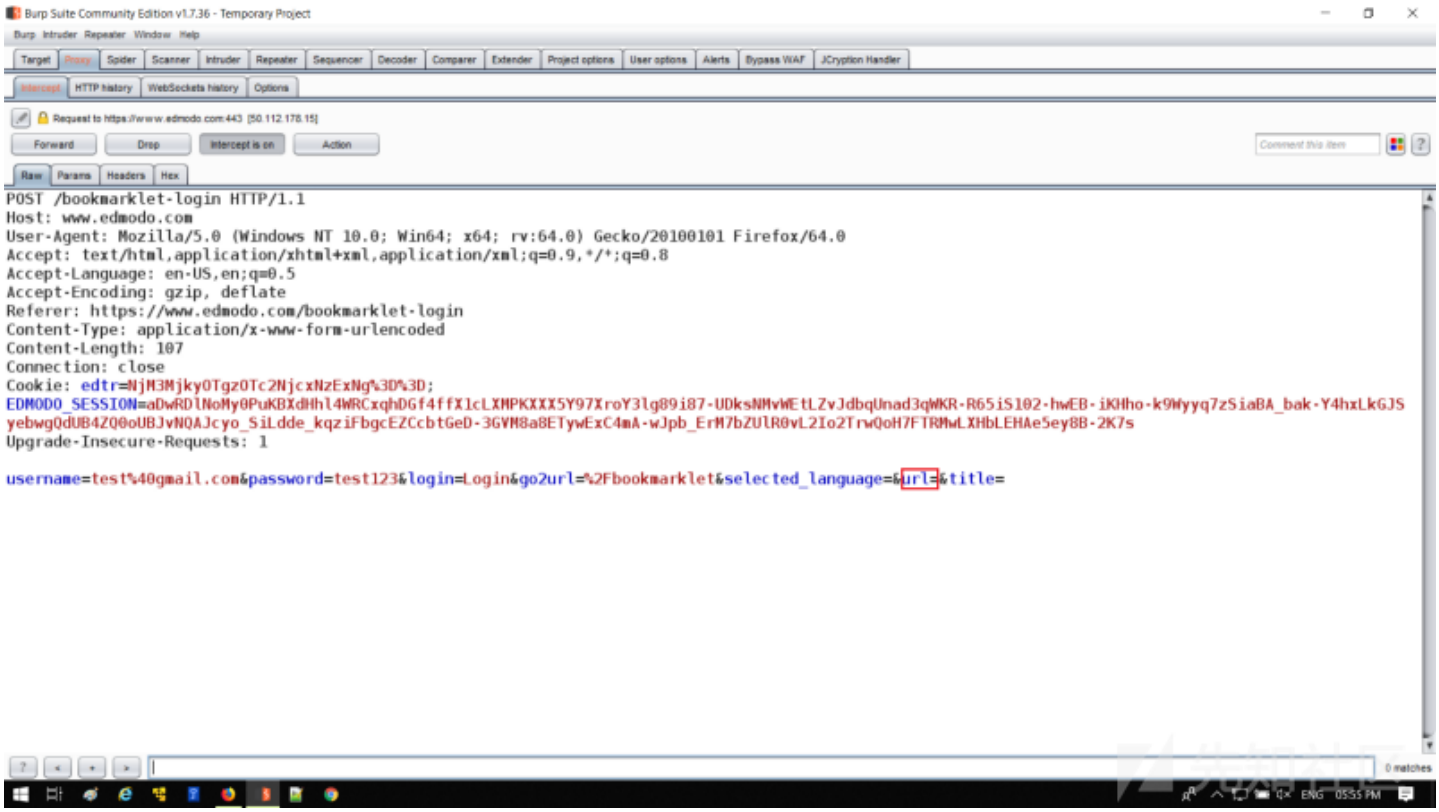
思索了一段时间后，我决定捕获该页面的登录请求。
目标URL:

```
https://www.edmodo.com/bookmarklet-login
```

我打开这个URL，看到天蓝色背景的登录屏幕。我尝试了SQL，XSS输入，但都没有任何反应。然后，我尝试深入应用程序并检查请求的每个参数。当我登录的时候。



显示有一个名为URL的参数正在传递请求。

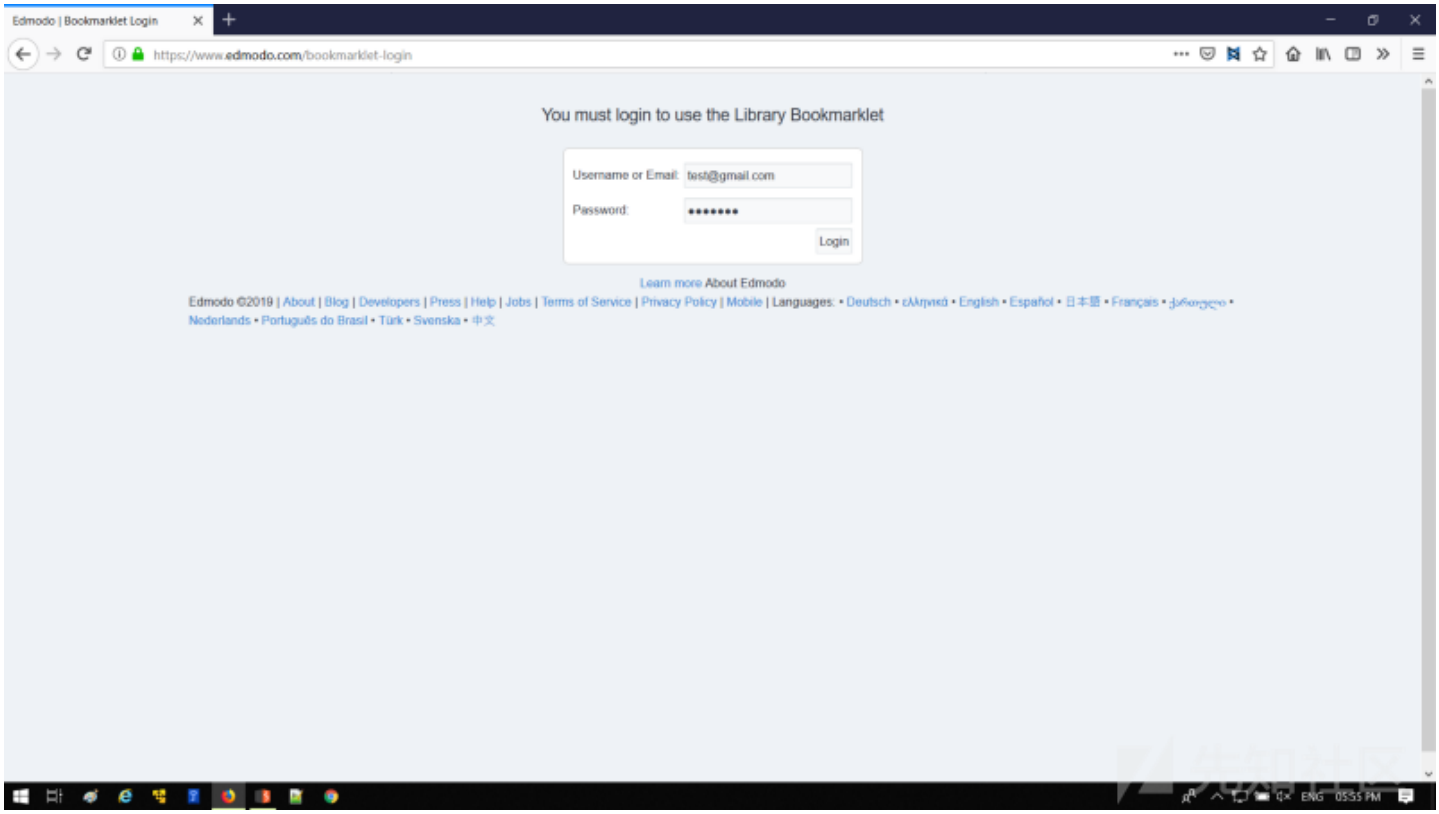


当URL参数传递请求时，我陷入沉思！

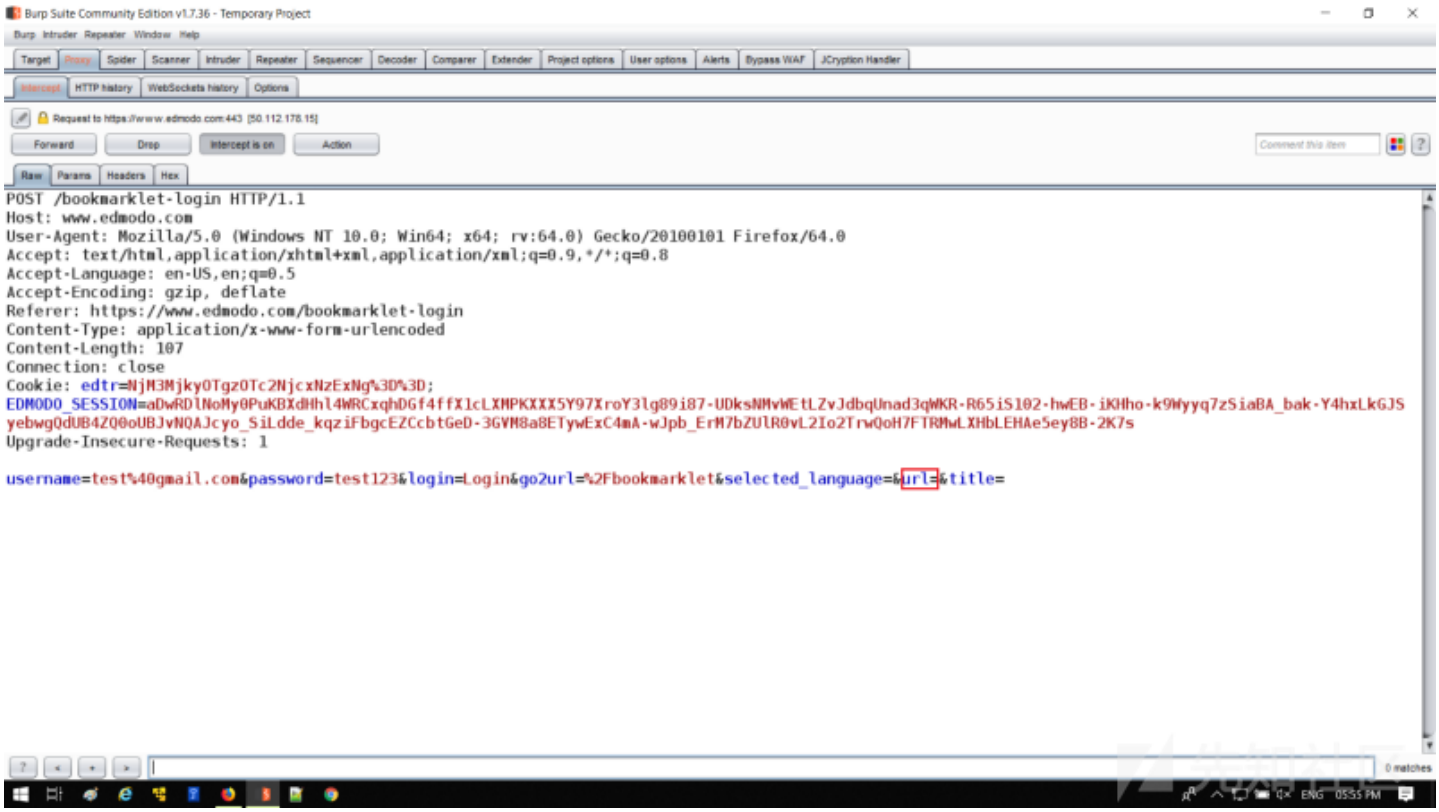
现在，我要试着输入一些字符串，比如"Test
Example"。然后显示响应，我发现没有用于过滤输入的验证或过滤器。然后我尝试了经过精心设计的payload。我发现payload破坏了响应端的输入标签。它接受所有特殊字
payload，而不会给出任何错误。

具体步骤

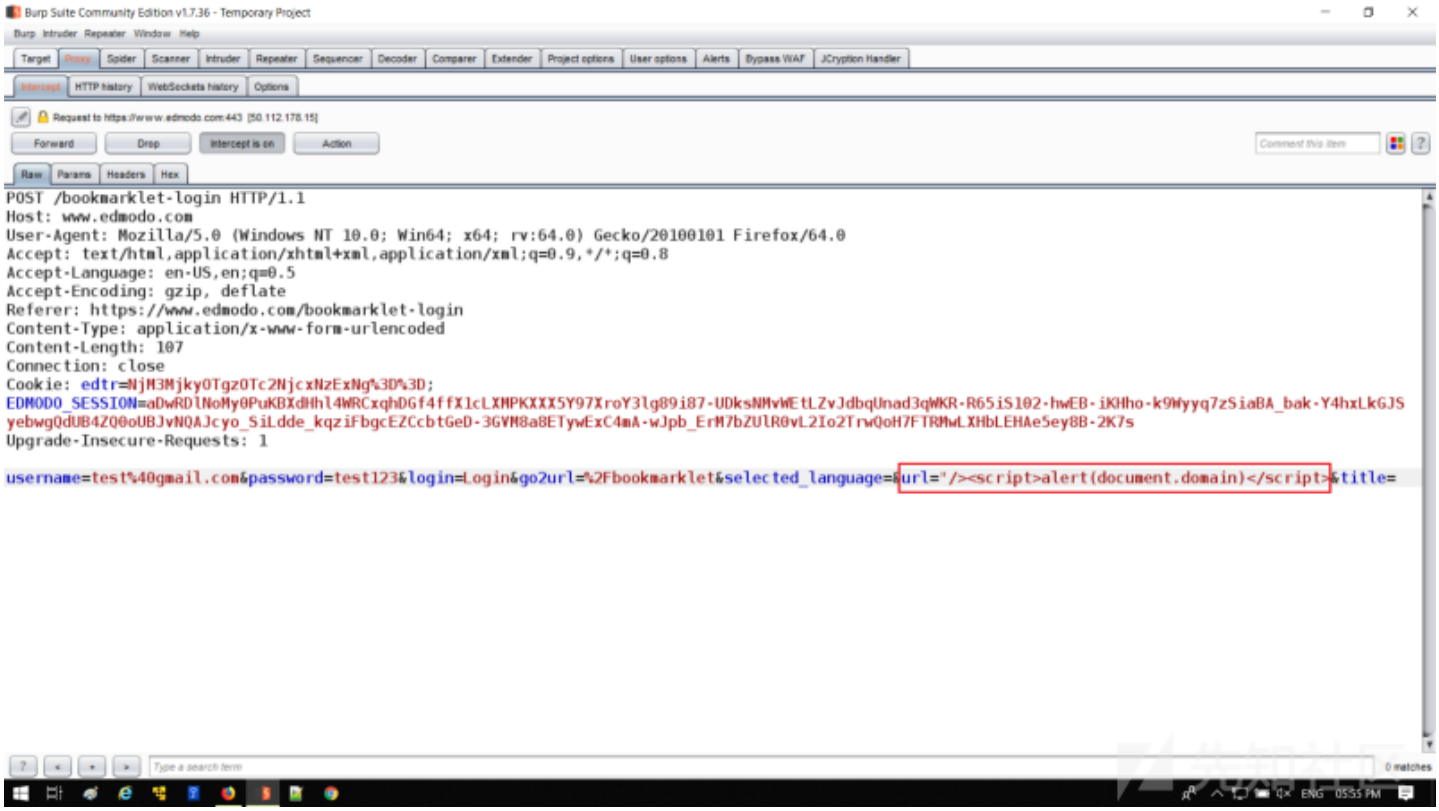
步骤1：打开`https://www.edmodo.com/bookmarklet-login`。输入用户名和密码。



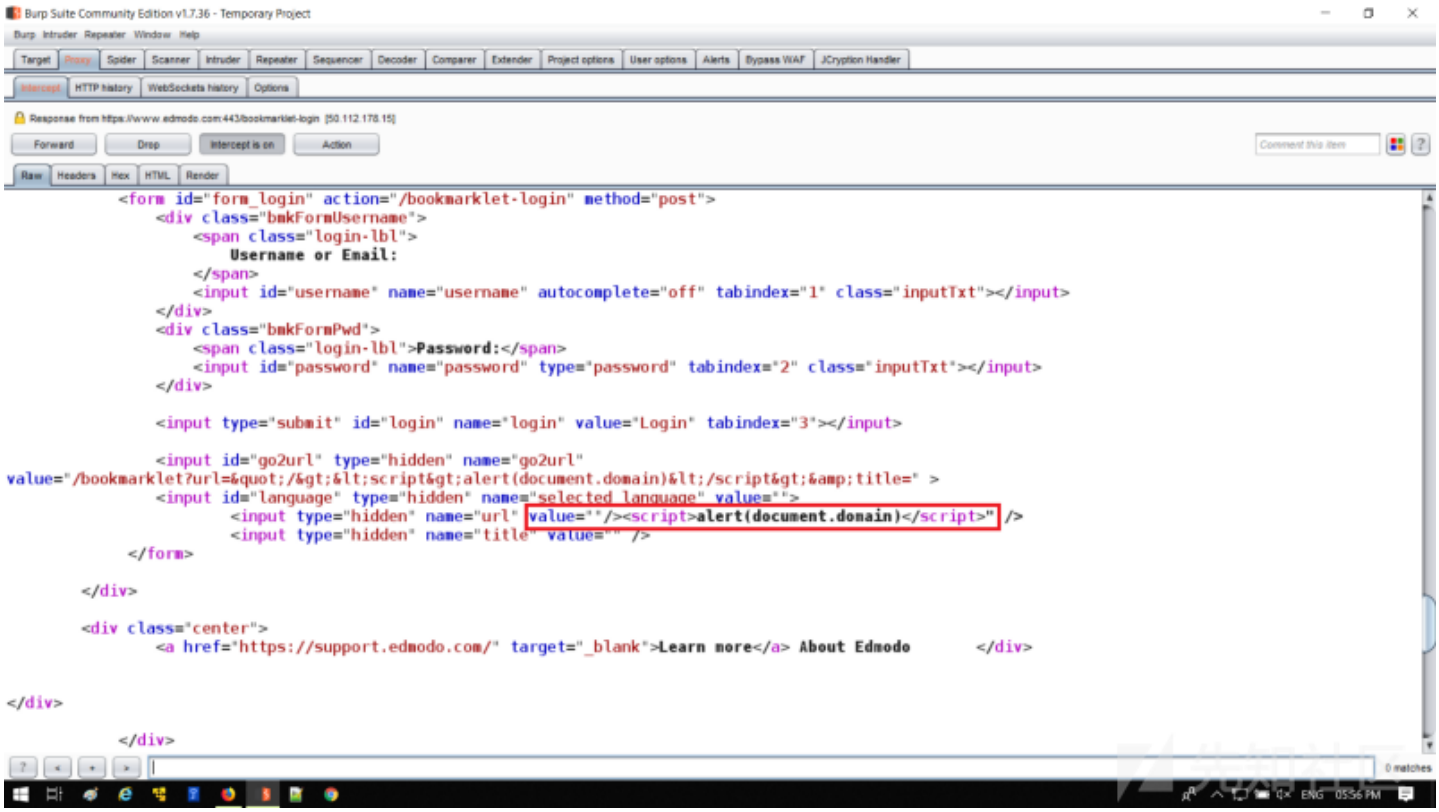
步骤2：拦截请求。注意在请求中传递的`url`参数。



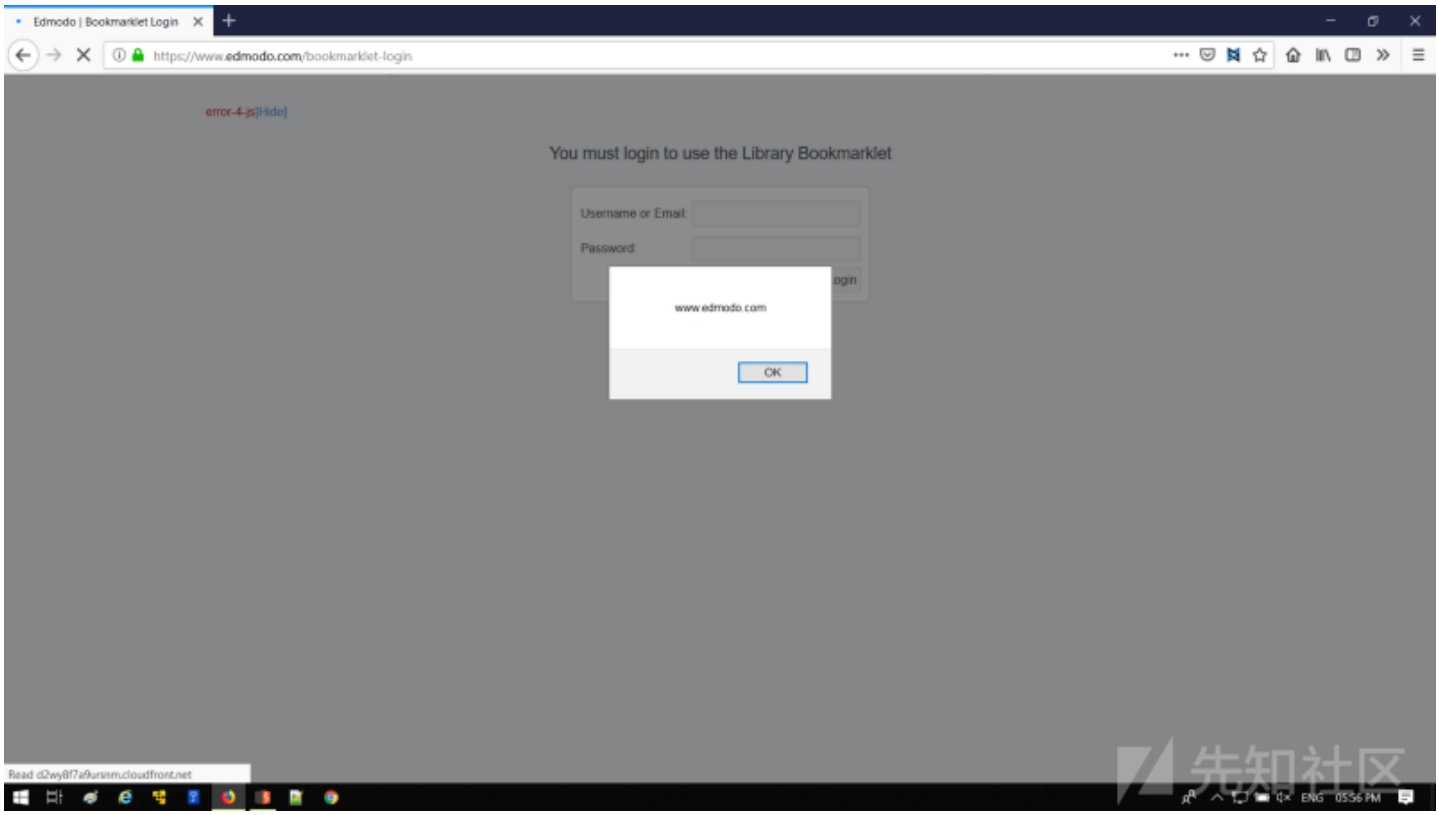
步骤3：put `url =“/> <script >alert■document.domain■</ script`。



步骤4：检查响应



步骤5：payload成功执行！



感悟

永不放弃是挖洞人员的第一奥义。
我非常高兴，因为这是我发现的第一个bug，Edmodo确认后给我发放了奖励。

时间线

2019年1月9日：发送报告

2019年1月10日：验证bug。

2019年1月10日：成功验证bug。

2019年1月11日：Edmodo发送奖励

2019年1月20日：收到奖励

总结

深入研究Web应用程序。
检查传入请求的每个参数。
永远不要放弃，不放弃深层次的研究
一定要多练习，熟能生巧嘛~

参考

https://medium.com/@parthshah14031998/how-i-stumbled-upon-a-stored-xss-my-first-bug-bounty-story-2793300d82bb

■■■https://medium.com/@valakeyur/xss-in-edmodo-within-5-minute-my-first-bug-bounty-889e3da6167d

上一篇：某php一处疑似官方后门导致get... 下一篇：VPN扩展功能的隐私安全问题
1. 0 条回复

- 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板