

攻防世界WEB进阶之NewsCenter

原创

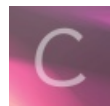
置顶 [harry_c](#) 于 2019-07-28 15:18:47 发布 3464 收藏 2

分类专栏: [攻防世界](#) 文章标签: [攻防世界](#) [NewsCenter](#) [web](#) [安全](#) [进阶](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/harry_c/article/details/97614941

版权



[攻防世界](#) 专栏收录该内容

29 篇文章 2 订阅

订阅专栏

攻防世界WEB进阶之NewsCenter

第一步: [描述](#)

第二步: [操作](#)

第三步: [答案](#)

难度系数: 1星

题目来源: XCTF 4th-QCTF-2018

题目描述: 暂无

第一步: 描述

本题题目没有描述, 所以直接开启场景, 映入眼帘的是一个搜索框, 所以我们应该自然想到可能存在着sql注入等问题, 首先使用bp进行抓取搜索时候的包。

Hacker News

OVERVIEW

Search news

search
<script>alert('Harry')</script>

Request to http://111.198.29.45:39704

POST / HTTP/1.1
Host: 111.198.29.45:39704
Content-Length: 50
Cache-Control: max-age=0
Origin: http://111.198.29.45:39704
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://111.198.29.45:39704/
Accept-Language: zh-CN,zh;q=0.9
Connection: close

search=%3Cscript%3Ealert%26Hary%29%3C%2Fscript%3E

https://blog.csdn.net/harry_c

第二步: 操作

