详细分析过程：

首先fuzz了一下字符，发现过滤了<>、#、1、alert、on，同时只放行第一个双引号。

但是留下了atob，首先使用大小写混写绕过对on的限制，用第一个双引号截断value。

用反引号绕过对单引号的过滤，用base64编码alert(1)，然后解码。

由于eval被过滤了，所以使用setInterval周期执行里面的js代码。

最后本地测试了下：



还需要一个空格才可以正常执行。

于是去乌云知识库翻之前的各种题解，然后看到有个alert(1)in”aaa”的姿势，就使用HTML编码手动补充一个”，然后用in绕过。

PAYLOAD:

[http://218.245.4.113:8080/web05/df1014aa2d59e1a02bba52955f797c7d/xss.php?xss="Onfocus=](http://218.245.4.113:8080/web05/df1014aa2d59e1a02bba52955f797c7d/xss.php?xss=%22Onfocus=setInterval(atob(%60YWxlcnQoMSk=%60))in%26quot)[setInterval(atob(`YWxlcnQoMSk=`))in%26quot](http://218.245.4.113:8080/web05/df1014aa2d59e1a02bba52955f797c7d/xss.php?xss=%22Onfocus=setInterval(atob(%60YWxlcnQoMSk=%60))in%26quot)

