链滴

【XSS】alert(1) to win 第三题

作者：zjhch123
原文链接：https://ld246.com/article/1467220745190
来源网站：链滴

题目很有意思
<pre><code class="highlight-chroma"><span class="highlight
cl">function escape(s) {
  var url = 'javascr
pt:console.log(' + JSON.stringify(s) + ')';
  console.log(url);

  var a = documen
.createElement('a');
  a.href = url;
  document.body.
ppendChild(a);
  a.click();
}
</code></pre>
意思就是我的输入被 JSON.stringify()函数转义。比如我输入”实际上是\”，输入\实际上是\\。
br>
所以这里需要对该函数进行绕过。
在第二题中，题目：
<pre><code class="highlight-chroma"><span class="highlight
cl">function escape(s) {
  s = JSON.stringif
(s);
  return '<scrip
>console.log(' + s + ');</script>';
}
</code></pre>
可以使用闭合 <code><script></code> 标签的方式绕过。我输入
<code></script><script>alert(1)//</code>
即可过关。
可是第三题不能这么使用，因为不存在 <code><script></code> 标签。
所以首先想办法的是绕过 <code>log()</code> 函数。
我们可以发现题目中是创建了一个 <code><a></code>，且给 <code><a></code> 的
<code>href</code> 属性进行赋值，并在将 <code><a></code> 添加到浏览器上。这就
以想到浏览器会对部分代码进行 URL 转义。比如说双引号 <code>” </code> 对应的是 <code>%2
</code>,空格 对应的是 <code>%20</code>...这里我们可以使用 %22 来让浏览器帮我们渲染出
个双引号从而逃过 <code>log()</code> 函数。
输入
<code>%22);alert(1)//</code>
成功过关