Json 劫持

一、漏洞简介

Json 劫持攻击又为”JSON Hijacking”，攻击过程有点类似于 csrf，只不过 csrf 只管发送 http 请求，但是 json-hijack 的目的是获取敏感数据。 一些 web 应用会把一些敏感数据以 json 的形式返回到前端，如果仅仅通过 cookie 来判断请求是否合法，那么就可以利用类似 csrf 的手段，向目标服务器发送请求，以获得敏感数据。

二、漏洞危害

1. 可能导致用户权限被盗用。
2. 可对劫持页进行网站钓鱼。

三、修复方案

1. 验证 HTTP Referer 头信息。
2. 在请求中添加 csrfToken 并在后端进行验证。
3. 严格过滤 callback 函数名及 JSON 里数据的输出。