小白兔WR

主页

随笔

所有文章/ 好友们/ 关于我

RPO攻击初体验

2018-04-02

文章目录

上周参加了CTF比赛，虽然结果一般般，但还是学到了不少东西，比[illegible]击。RPO(Relative Path Overwrite) 攻击又称为相对路径覆盖攻击，[illegible]器和网络服务器的反应与服务器的 Web 缓存技术和配置差异，利用[illegible]加载的css/js的相对路径来加载其他文件，最终浏览器将服务器返回[illegible]css/js的文件当做css/js来解析，从而导致XSS，信息泄露等漏洞产生[illegible]击在网络上资料较少，如果不是参加比赛还真不会去了解这种攻击技术，所以这里分享给大家。

了解RPO

如果让我来解释RPO，大概就是利用css、js的相对路劲分析漏洞进行的攻击，
原理：
1.在Url中使用%2f来代替/
2.Url在浏览器分析时，会把%2f解码为/，然后就正常返回页面
3.但是css/js在解析时，不会进行解码，所以就出现了目录覆盖的情况
4.产生这种漏洞的最大原因是CSS/js解析器的一个特性：浏览器在解析CSS/js样式时，会忽略非法的部分，直到找到正确的开始然后进行解析一直到结束。所以当我们植入CSS/js代码，欺骗CSS/js解析器忽略之前不合法的语法内容，从而加载我们注入的CSS/js内容。
5.一般来说，在phpinfo框架中出现这种情况的可能性比较大