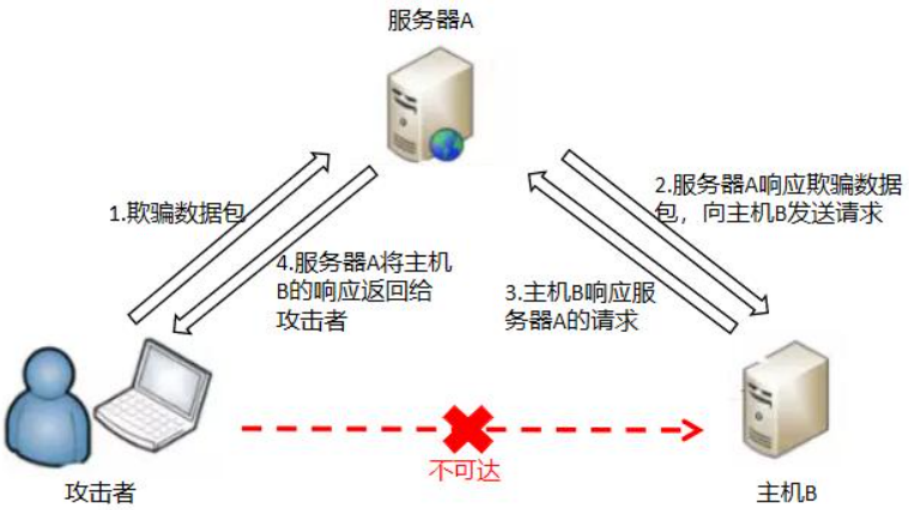
20200715信息安全实训

笔记本:	我的第一个笔记本		
创建时间:	2020/7/15 9:03	**更新时间:**	2020/7/15 17:05
作者:	820410740@qq.com		
URL:	app://desktop.dingtalk.com/web_content/chatbox.html?isFourColumnMode=false		

SSRF漏洞



https://blog.csdn.net/weixin_39190897/article/details/88226410
https://www.cnblogs.com/happystudyhuan/p/11802961.html
https://zhuanlan.zhihu.com/p/91819069

SSRF(Server-Side Request Forgery:服务器端请求伪造) 是一种由攻击者构造形成由服务端发起请求的一个安全漏洞。

SSRF 形成的原因：大都是由于服务端提供了从其他服务器应用获取数据的功能，且没有对目标地址做过滤与限制。比如从指定URL地址获取网页文本内容，加载指定地址的图片，文档，等等。

也就是说，对于为服务器提供服务的其他应用没有对访问进行限制，如果我构造好我的访问包，那我就有可能利用目标服务对他的其他服务器应用进行调用。

一般情况下，SSRF攻击的目标是从外网无法访问的内部系统。（正是因为它是由服务端发起的，所以它能够请求到与它相连而与外网隔离的内部系统）。

主要危害

攻击者利用SSRF可以实现的攻击主要有5种：

可以对外网、服务器所在内网、本地进行端口扫描，获取一些服务器的banner信息；
攻击运行在内网或本地的应用程序(比如溢出)；
对内网web应用进行指纹识别，通过访问默认文件实现；
攻击内外网的web应用，主要是使用get参数就可以实现的攻击(比如struts2，sqli等)；
利用file协议读取本地文件等。

SSRF漏洞的检测
从web功能上寻找

SSRF是由于服务器获取其他服务器的相关信息的功能中形成的。

分享:通过URL地址分享网页内容
转码服务：通过URL地址把原地址的网页内容调优使其适合手机屏幕浏览
在线翻译
图片加载与下载：通过URL地址加载或下载图片
图片、文章收藏功能
未公开的API实现以及其他调用URL的功能

1、过滤返回的信息，如果web应用是去获取某一种类型的文件。那么在把返回结果展示给用户之前先验证返回的信息是否符合标准。

2、统一错误信息，避免用户可以根据错误信息来判断远程服务器的端口状态。

3、限制请求的端口，比如80,443,8080,8090。

4、禁止不常用的协议，仅仅允许http和https请求。可以防止类似于file:///,gopher://,ftp://等引起的问题。

5、使用DNS缓存或者Host白名单的方式。
https://blog.csdn.net/qq_35983015/article/details/106959506
代码执行漏洞
https://www.jianshu.com/p/2e7363f3d3ea
https://www.cnblogs.com/lyxsalyd/p/12607769.html
https://blog.csdn.net/qq_37133717/article/details/94760485
https://www.cnblogs.com/LeeeBoom/p/12439342.html
ssrf pikachu
windows:https://www.cnblogs.com/tangjf10/p/12673947.html
https://blog.csdn.net/weixin_40412037/article/details/103998815
linux:https://blog.csdn.net/u014029795/article/details/103154810

语法

```
file_get_contents(path,include_path,context,start,max_length)
```

参数	描述
path	必需。规定要读取的文件。
include_path	可选。如果也想在 include_path 中搜寻文件的话，可以将该参数设为 "1"。
context	可选。规定文件句柄的环境。 context 是一套可以修改流的行为的选项。若使用 null，则忽略。
start	可选。规定在文件中开始读取的位置。该参数是 PHP 5.1 新加的。
max_length	可选。规定读取的字节数。该参数是 PHP 5.1 新加的。