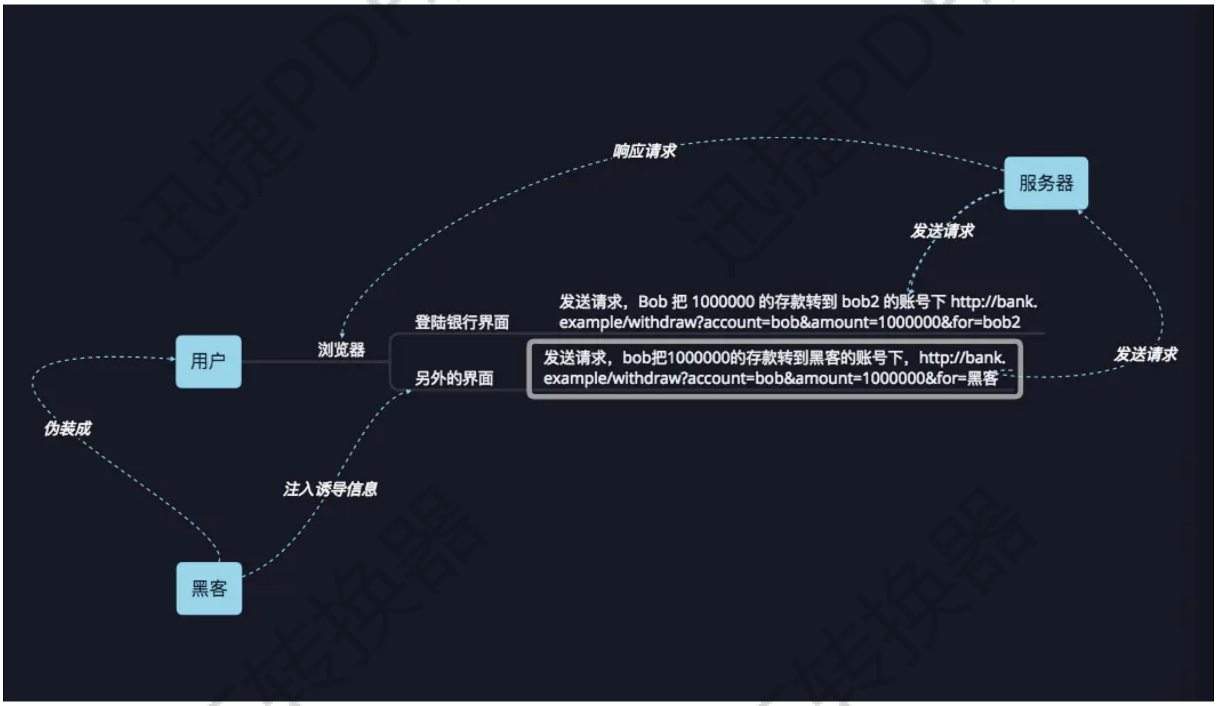
WEB 漏洞-CSRF 及 SSRF 漏洞案例讲解

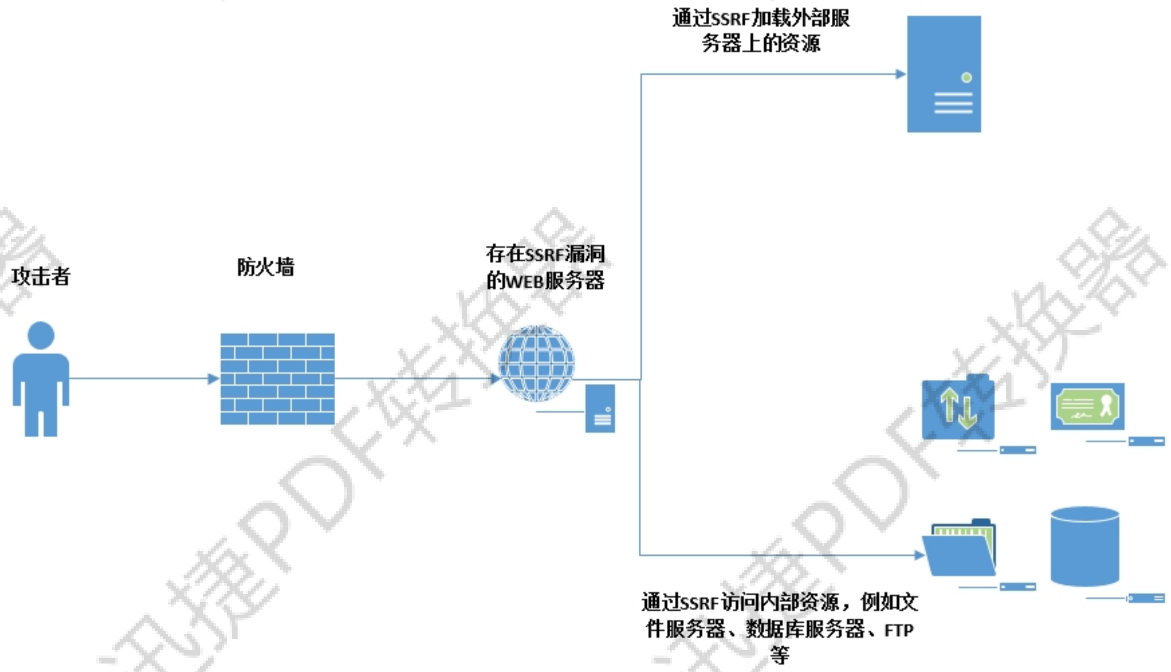


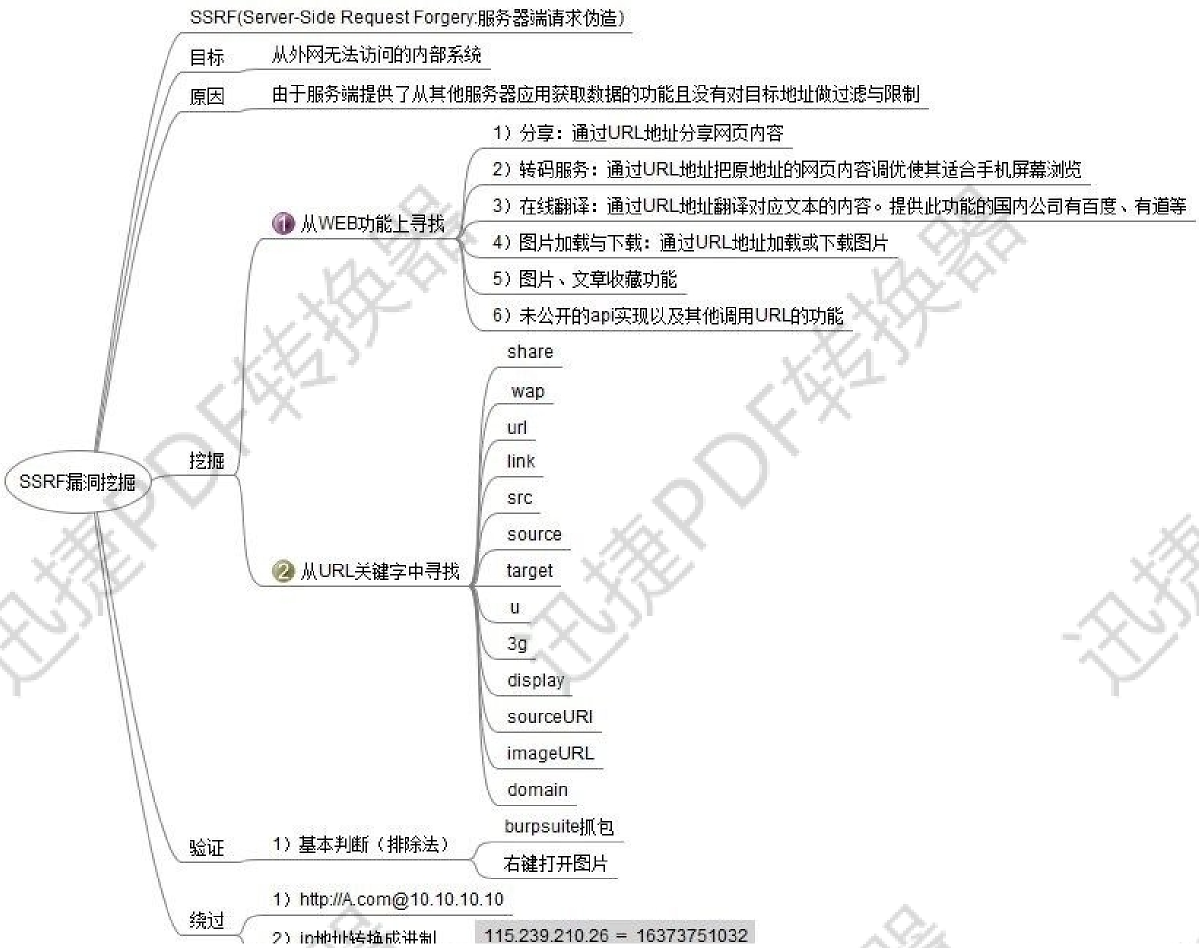
发送请求，Bob 把 1000000 的存款转到 bob2 的账号下 http://bank.example/withdraw?account=bob&amount=1000000&for=bob2

发送请求，bob把1000000的存款转到黑客的账号下，http://bank.example/withdraw?account=bob&amount=1000000&for=黑客

#CSRF 漏洞解释，原理等
#CSRF 漏洞检测，案例，防御等

#防御方案
1、当用户发送重要的请求时需要输入原始密码
2、设置随机 Token
3、检验 referer 来源，请求时判断请求链接是否为当前管理员正在使用的页面（管理员在编辑文章，黑客发来恶意的修改密码链接，因为修改密码页面管理员并没有在操作，所以攻击失败）
4、设置验证码
5、限制请求方式只能为 POST


通过SSRF加载外部服务器上的资源
攻击者
防火墙
存在SSRF漏洞的WEB服务器
通过SSRF访问内部资源，例如文件服务器、数据库服务器、FTP等



SSRF漏洞挖掘

- SSRF(Server-Side Request Forgery:服务器端请求伪造)
- 目标
  - 从外网无法访问的内部系统
- 原因
  - 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
- 挖掘
  - ① 从WEB功能上寻找
    - 1）分享：通过URL地址分享网页内容
    - 2）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
    - 3）在线翻译：通过URL地址翻译对应文本的内容。提供此功能的国内公司有百度、有道等
    - 4）图片加载与下载：通过URL地址加载或下载图片
    - 5）图片、文章收藏功能
    - 6）未公开的api实现以及其他调用URL的功能
  - ② 从URL关键字中寻找
    - share
    - wap
    - url
    - link
    - src
    - source
    - target
    - u
    - 3g
    - display
    - sourceURl
    - imageURL
    - domain
- 验证
  - 1）基本判断（排除法）
    - burpsuite抓包
    - 右键打开图片
- 绕过
  - 1）http://A.com@10.10.10.10
  - 2）ip地址转换成进制
    - 115.239.210.26 = 16373751032

#SSRF 漏洞解释，原理等

#SSRF 漏洞检测，案例，防御等

各个协议调用探针：http,file,dict,ftp,gopher 等

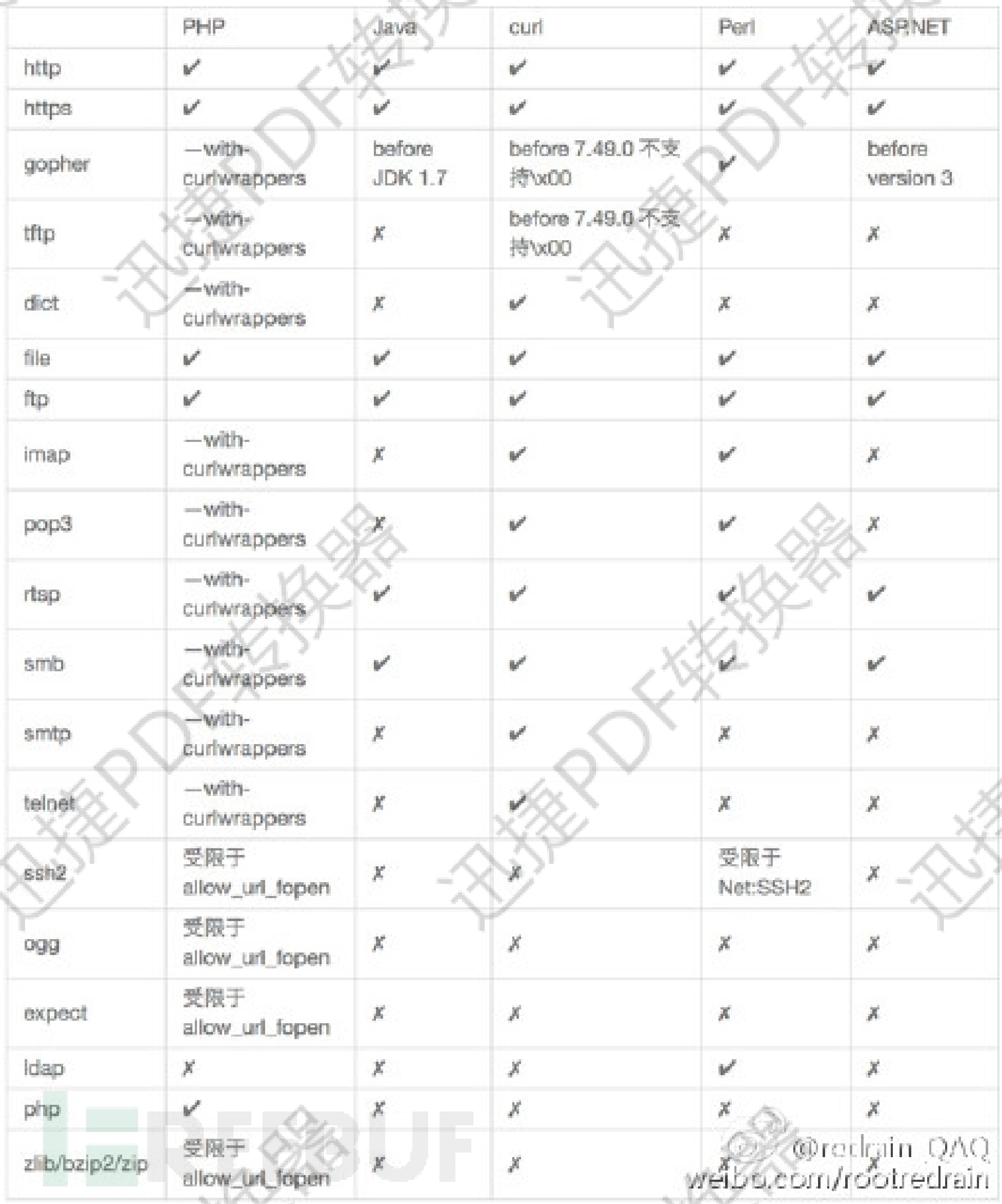
漏洞攻击：端口扫描，指纹识别，漏洞利用，内网探针等

http://192.168.64.144/phpmyadmin/

file:///D:/www.txt

dict://192.168.64.144:3306/info

ftp://192.168.64.144:21



	PHP	Java	curl	Perl	ASP.NET
http	✔	✔	✔	✔	✔
https	✔	✔	✔	✔	✔
gopher	—with-curlwrappers	before JDK 1.7	before 7.49.0 不支持\x00	✔	before version 3
tftp	—with-curlwrappers	✗	before 7.49.0 不支持\x00	✗	✗
dict	—with-curlwrappers	✗	✔	✗	✗
file	✔	✔	✔	✔	✔
ftp	✔	✔	✔	✔	✔
imap	—with-curlwrappers	✗	✔	✔	✗
pop3	—with-curlwrappers	✗	✔	✔	✗
rtsp	—with-curlwrappers	✔	✔	✔	✔
smb	—with-curlwrappers	✔	✔	✔	✔
smtp	—with-curlwrappers	✗	✔	✗	✗
telnet	—with-curlwrappers	✗	✔	✗	✗
ssh2	受限于 allow_url_fopen	✗	✗	受限于 Net:SSH2	✗
ogg	受限于 allow_url_fopen	✗	✗	✗	✗
expect	受限于 allow_url_fopen	✗	✗	✗	✗
ldap	✗	✗	✗	✔	✗
php	✔	✗	✗	✗	✗
zlib/bzip2/zip	受限于 allow_url_fopen	✗	✗	✗	✗

演示案例：

✧ Pikachu_CSRF 案例及 Burp 检测

✧ Pikachu_CSRF 防御 Token 测试测试

✧ SSRF_PHP,JAVA 漏洞代码协议运用

✧ SSRF_漏洞代码结合某漏洞利用测试

✧ SSRF 实战_图片加载翻译转码等应用说明

涉及资源：

https://pan.baidu.com/s/1bp96ECJ

https://www.t00ls.net/articles-41070.html

```
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<form action="" method="POST">
请输入图片地址：<input type='text' name='url'>
<input type='submit' value="提交">
</form>

<?php
/*
$url=$_POST['url'];
$img                                                                              =
file_get_contents('http://192.168.64.144:8080/?search==%00{.exec|cmd.exe%20/c%20net%20user%20t
est1234%201234%20/add.}');
echo $url;
echo $img;
//header("Content-Type: image/jpeg;text/html; charset=utf-8");
//echo $img;
//$file=fopen('x.png','w+');
//fwrite($file,$img);
//fclose($file);
*/
?>

<?php
$_POST['url'];
$ch = curl_init();
```

```
curl_setopt($ch, CURLOPT_URL, $_POST['url']);
curl_setopt($ch, CURLOPT_HEADER, false);
curl_exec($ch);
curl_close($ch);
?>
```