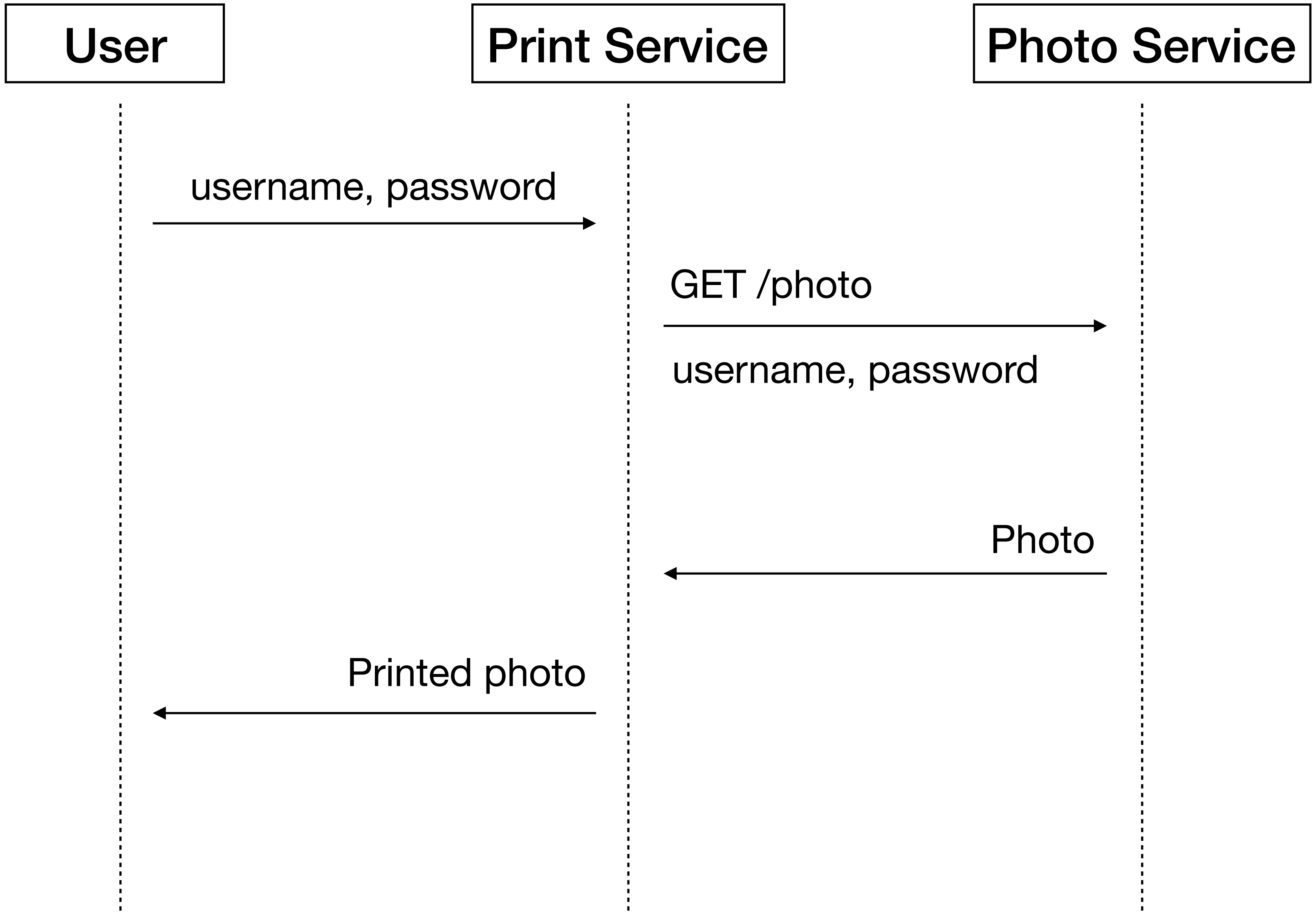
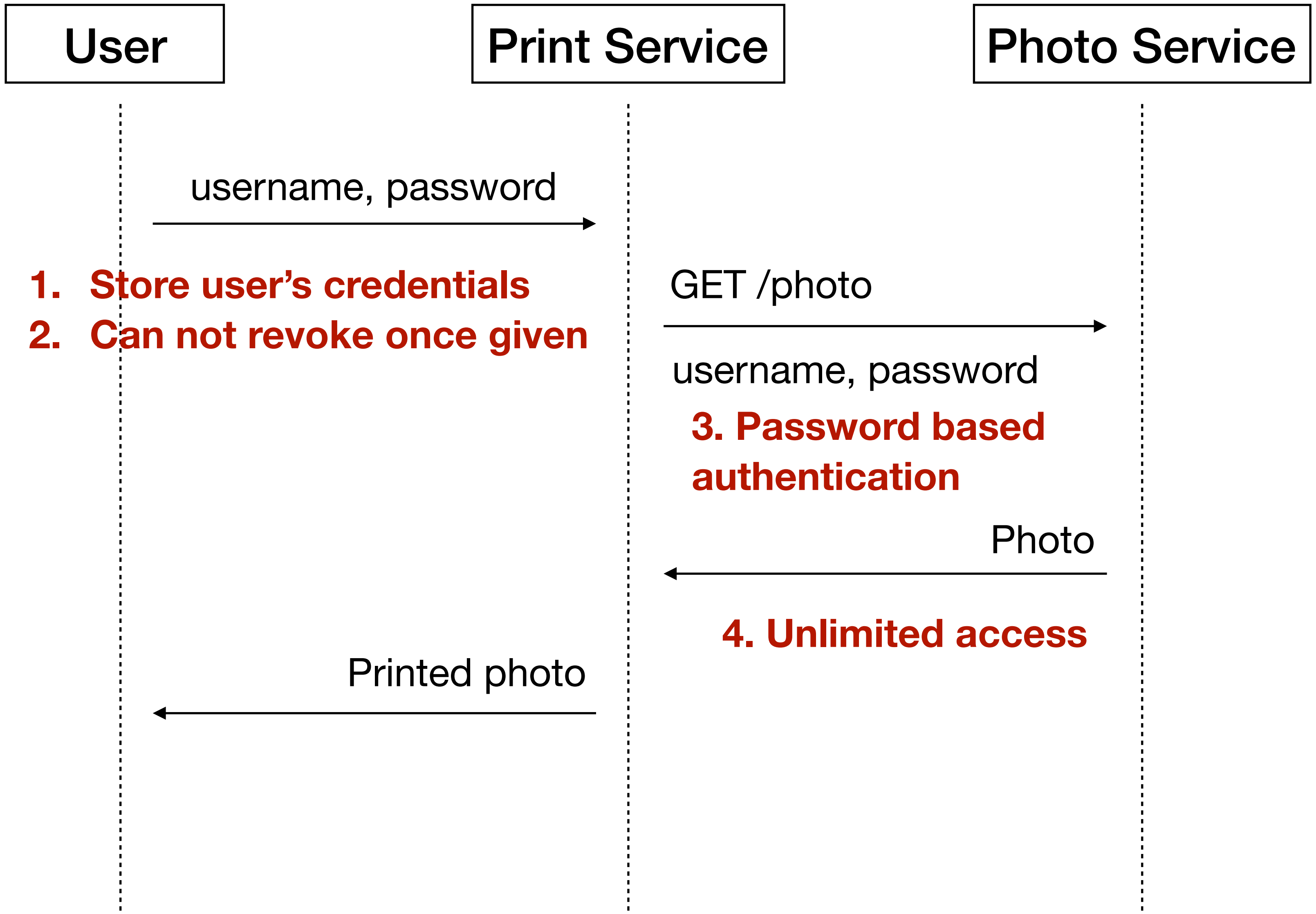
OAuth 2.0

Traditional Client-Server Authentication Model



Problems



1. Store user's credentials
2. Can not revoke once given

3. Password based authentication

4. Unlimited access

Protocol Flow

```
+--------+                               +---------------+
|        |--(A)- Authorization Request ->|   Resource    |
|        |                               |     Owner     |
|        |<-(B)-- Authorization Grant ---|               |
|        |                               +---------------+
|        |
|        |        Authorization Grant &  +---------------+
|        |--(C)--- Client Credentials -->| Authorization |
| Client |                               |     Server    |
|        |<-(D)----- Access Token -------|               |
|        |                               +---------------+
|        |
|        |                               +---------------+
|        |--(E)----- Access Token ------>|    Resource   |
|        |                               |     Server    |
|        |<-(F)--- Protected Resource ---|               |
+--------+                               +---------------+
```

Roles

- `resource owner`
- `resource server`
- `client`
- `authorization server`

```
+--------+                               +---------------+
|        |--(A)- Authorization Request ->|   Resource    |
|        |                               |     Owner     |
|        |<-(B)-- Authorization Grant ---|               |
|        |                               +---------------+
|        |
|        |        Authorization Grant &  +---------------+
|        |--(C)--- Client Credentials -->| Authorization |
| Client |                               |     Server    |
|        |<-(D)----- Access Token -------|               |
|        |                               +---------------+
|        |
|        |                               +---------------+
|        |--(E)----- Access Token ------>|    Resource   |
|        |                               |     Server    |
|        |<-(F)--- Protected Resource ---|               |
+--------+                               +---------------+
+--------+                               +---------------+
|        |--(A)- Authorization Request ->|   Resource    |
|        |                               |     Owner     |
|        |<-(B)-- Authorization Grant ---|               |
|        |                               +---------------+
|        |
|        |        Authorization Grant &  +---------------+
|        |--(C)--- Client Credentials -->| Authorization |
| Client |                               |     Server    |
|        |<-(D)----- Access Token -------|               |
|        |                               +---------------+
|        |
|        |                               +---------------+
|        |--(E)----- Access Token ------>|    Resource   |
|        |                               |     Server    |
|        |<-(F)--- Protected Resource ---|               |
+--------+                               +---------------+
```

Authorization Code
Implicit
Resource Owner Password Credentials
Client Credentials

Authorization Code

Request
GET /authorize?**response_type**=code&**client_id**=s6BhdRkqt3&
redirect_uri=https%3A%2F%2Fclient%2Eexample%2Ecom%2Fcb&
scope=xxx&**state**=xxx HTTP/1.1
Host: server.example.com

Respond
HTTP/1.1 302 Found
Location:
https://client.example.com/cb?**code**=i1WsRn1uB1&
state=xxx

```
+----------+
| resource |
|   owner  |
|          |
+----------+
     ^
     |
    (B)
+----|-----+          Client Identifier      +---------------+
|         -+----(A)--- & Redirect URI ------>|               |
|  User-   |                                 | Authorization |
|  Agent  -+----(B)-- User authenticates --->|     Server    |
|          |                                 |               |
|         -+----(C)-- Authorization Code ---<|               |
+-|----|---+                                 +---------------+
  |    |                                         ^      v
 (A)  (C)                                        |      |
  |    |                                         |      |
  ^    v                                         |      |
+---------+                                      |      |
|         |>---(D)-- Client Credentials, --------'      |
|         |          Authorization Code,                |
| Client  |            & Redirect URI                   |
|         |                                             |
|         |<---(E)----- Access Token -------------------'
+---------+       (w/ Optional Refresh Token)
```

Authorization Code

```
Request
POST /token HTTP/1.1
Host: server.example.com
Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW
Content-Type: application/x-www-form-urlencoded

grant_type=authorization_code&client_id=s6BhdRkqt3&
code=i1WsRn1uB1&
redirect_uri=https%3A%2F%2Fclient%2Eexample%2Ecom%2Fcb

Response
HTTP/1.1 200 OK
Content-Type: application/json
Cache-Control: no-store

{
    "access_token":"SlAV32hkKG",
    "token_type":"example",
    "expires_in":3600,
    "refresh_token":"8xLOxBtZp8",
    "example_parameter":"example_value"
}
```

```
+----------+
| resource |
|   owner  |
|          |
+----------+
     ^
     |
    (B)
+----|-----+          Client Identifier      +---------------+
|         -+----(A)--- & Redirect URI ------>|               |
|  User-   |                                 | Authorization |
|  Agent  -+----(B)-- User authenticates --->|     Server    |
|          |                                 |               |
|         -+----(C)-- Authorization Code ---<|               |
+-|----|---+                                 +---------------+
  |    |                                         ^      v
 (A)  (C)                                        |      |
  |    |                                         |      |
  ^    v                                         |      |
+---------+                                      |      |
|         |>---(D)-- Client Credentials, --------'      |
|         |          Authorization Code,                |
| Client  |           & Redirect URI                    |
|         |                                             |
|         |<---(E)----- Access Token -------------------'
+---------+       (w/ Optional Refresh Token)
```

Implicit Grant

```
Request
GET /authorize?response_type=token&client_id=s6BhdRkqt3&
    redirect_uri=https%3A%2F%2Fclient%2Eexample%2Ecom%2Fcb HTTP/1.1
Host: server.example.com

Response
HTTP/1.1 302 Found
Location: http://example.com/rd#access_token=FJQbwq9&
          token_type=example&expires_in=3600
```

```
+----------+
| Resource |
|  Owner   |
|          |
+----------+
     ^
     |
    (B)
+----|-----+          Client Identifier     +---------------+
|         -+----(A)--- & Redirect URI ----->|               |
|  User-   |                                | Authorization |
|  Agent  -|----(B)-- User authenticates -->|     Server    |
|          |                                |               |
|          |<---(C)---- Redirect URI ------<|               |
|          |          with Access Token     +---------------+
|          |            in Fragment
|          |                                +---------------+
|          |----(D)---- Redirect URI ------>|   Web Server  |
|          |          without Fragment      |  with Client  |
|          |                                |   Resource    |
|     (F)  |<---(E)------- Script ---------<|               |
|          |                                +---------------+
+-|--------+
  |    |
 (A)  (G) Access Token
  |    |
  ^    v
+---------+
|         |
|  Client |
|         |
+---------+
```

Resource Owner Password Credentials

Request

```
POST /token HTTP/1.1
Host: server.example.com
Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW
Content-Type: application/x-www-form-urlencoded

grant_type=password&client_id=s6BhdRkqt3&
username=johndoe&password=A3ddj3w
```

Response

```
HTTP/1.1 200 OK
Content-Type: application/json
Cache-Control: no-store

{
   "access_token":"SlAV32hkKG",
   "token_type":"example",
   "expires_in":3600,
   "refresh_token":"8xLOxBtZp8",
   "example_parameter":"example_value"
}
```

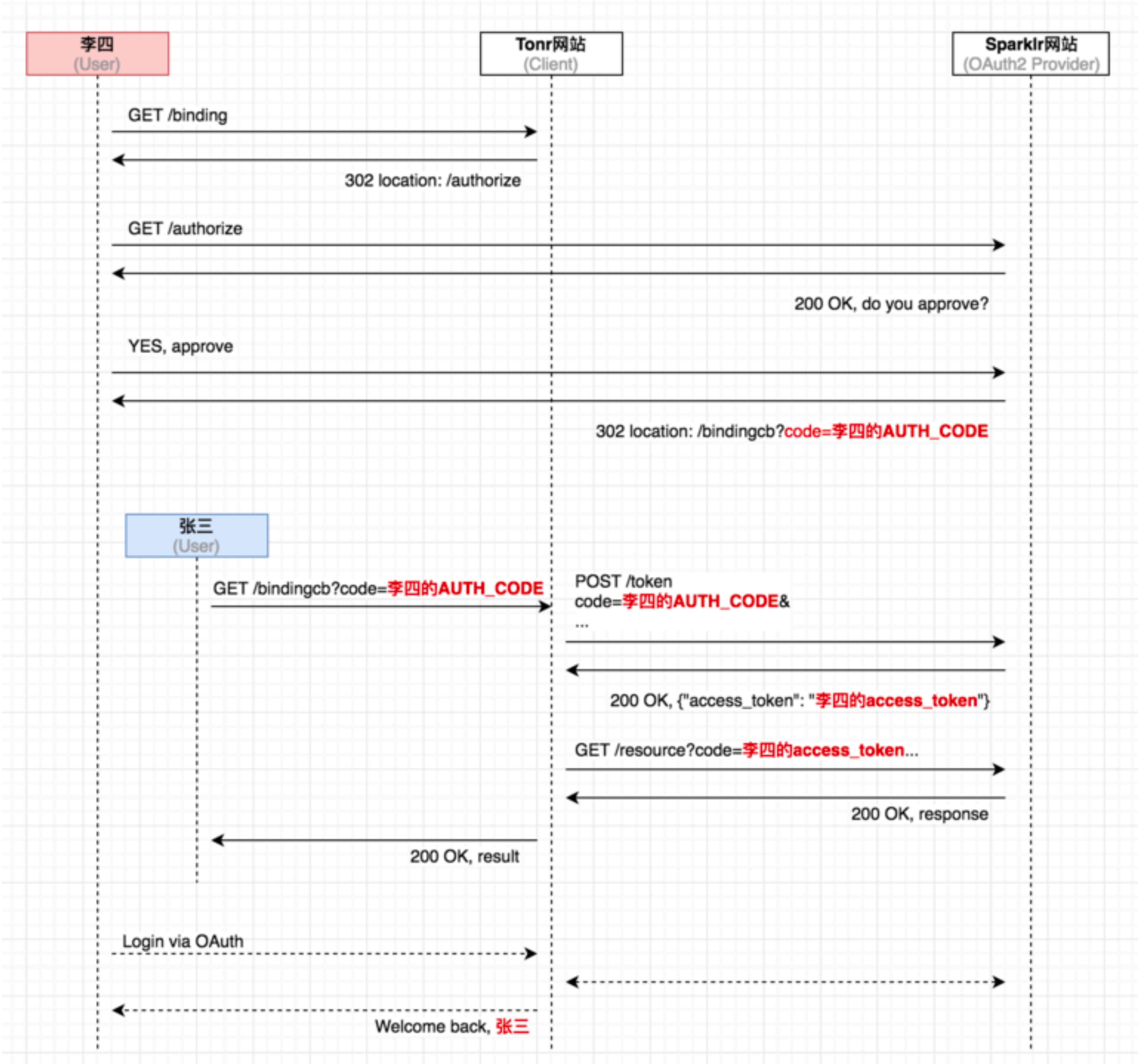
```
+----------+
| Resource |
|  Owner   |
|          |
+----------+
     v
     |
    (A) Password Credentials
     |
     v
+---------+                                  +---------------+
|         |          Client Credentials      |               |
|         |>--(B)---- & Resource Owner ----->|               |
| Client  |         Password Credentials     | Authorization |
|         |                                  |     Server    |
|         |<--(C)---- Access Token ---------<|               |
|         |    (w/ Optional Refresh Token)   |               |
+---------+                                  +---------------+
```

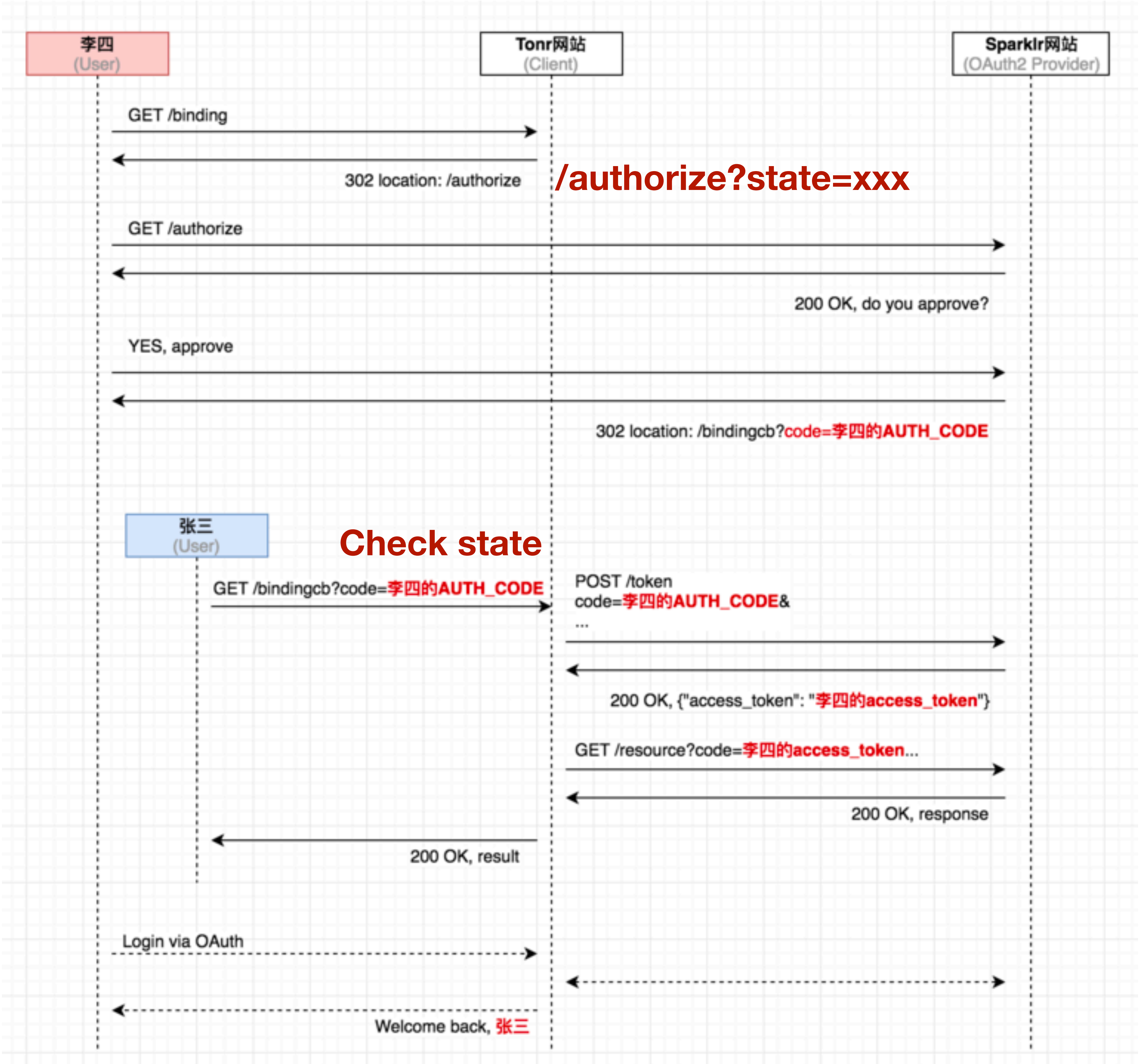
Client Credentials

```
+---------+                                  +---------------+
|         |                                  |               |
|         |>--(A)--- Client Credentials ---->| Authorization |
| Client  |                                  |     Server    |
|         |<--(B)---- Access Token ---------<|               |
|         |    (w/ Optional Refresh Token)   |               |
+---------+                                  +---------------+
```

Threats

CSRF on Authorization response

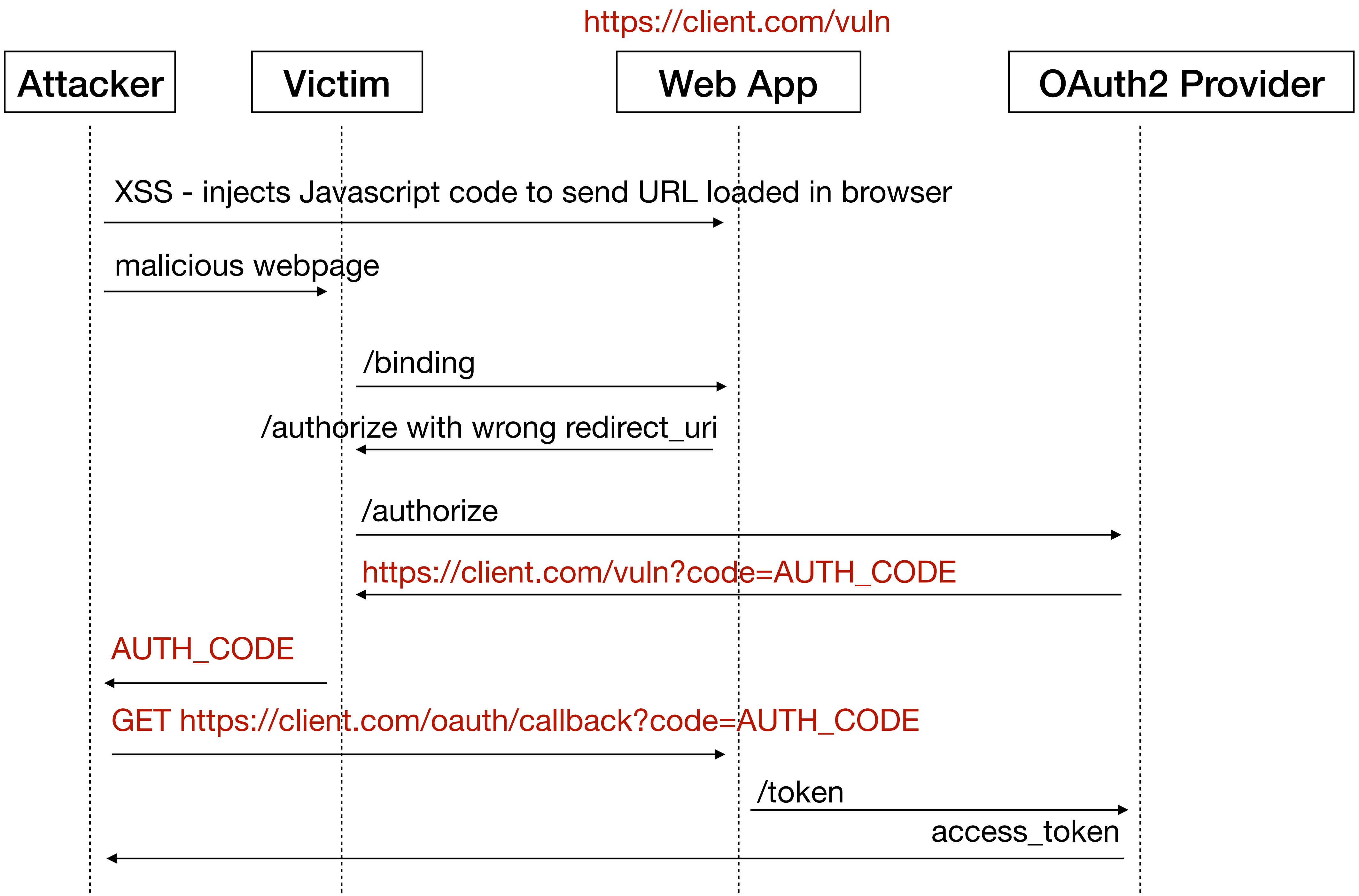




/authorize?state=xxx

Check state

‘redirect_uri’ Attack



https://client.com/vuln

Attacker

Victim

Web App

OAuth2 Provider

XSS - injects Javascript code to send URL loaded in browser

malicious webpage

/binding

/authorize with wrong redirect_uri

/authorize

https://client.com/vuln?code=AUTH_CODE

AUTH_CODE

GET https://client.com/oauth/callback?code=AUTH_CODE

/token

access_token

- whitelist ‘redirect_uri’
- **exact** matches