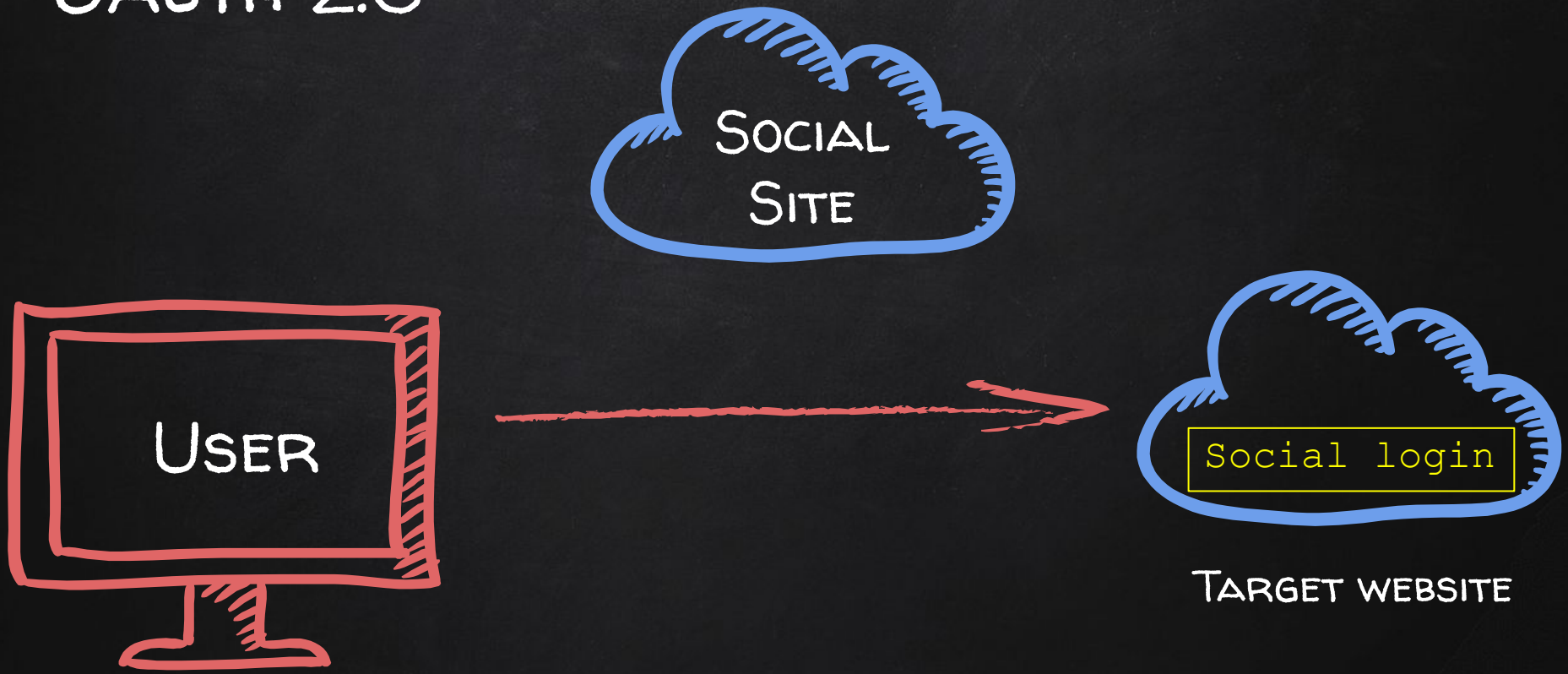
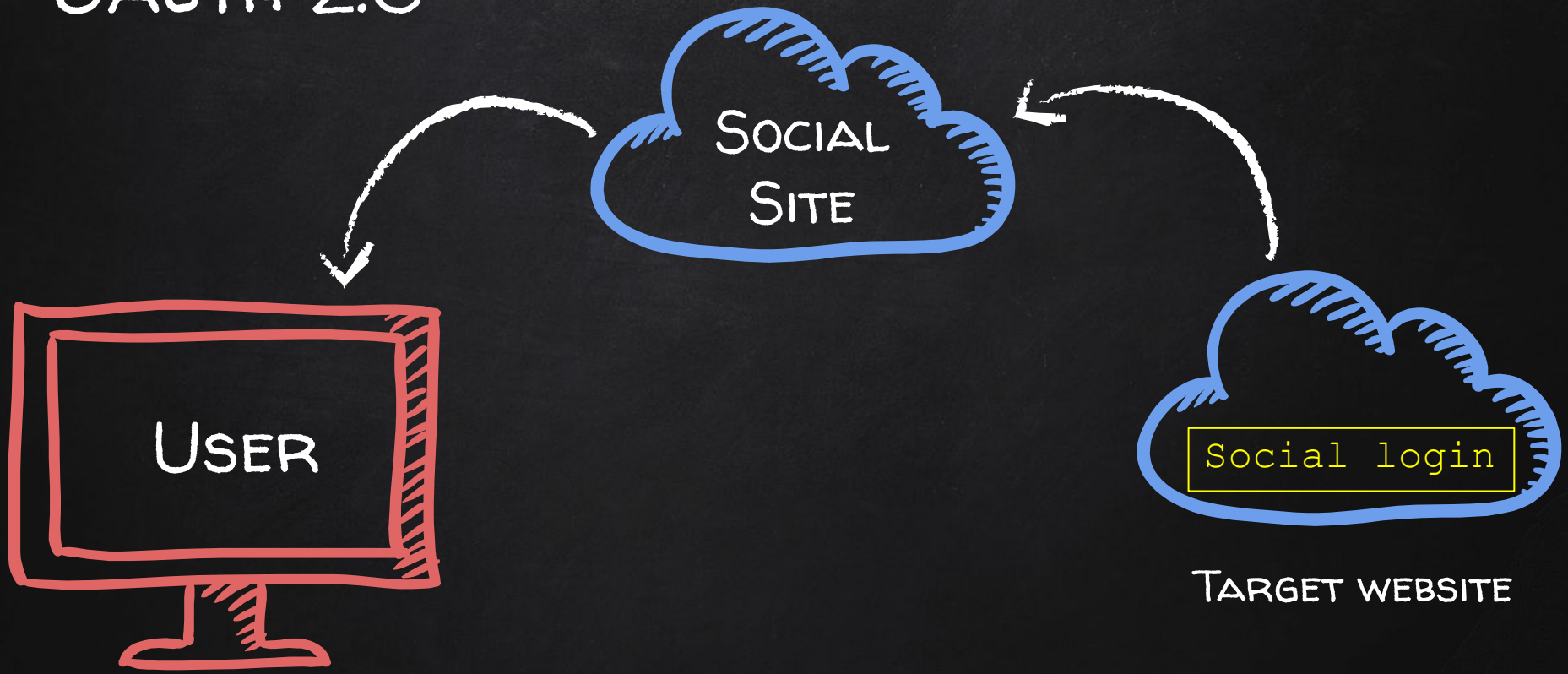
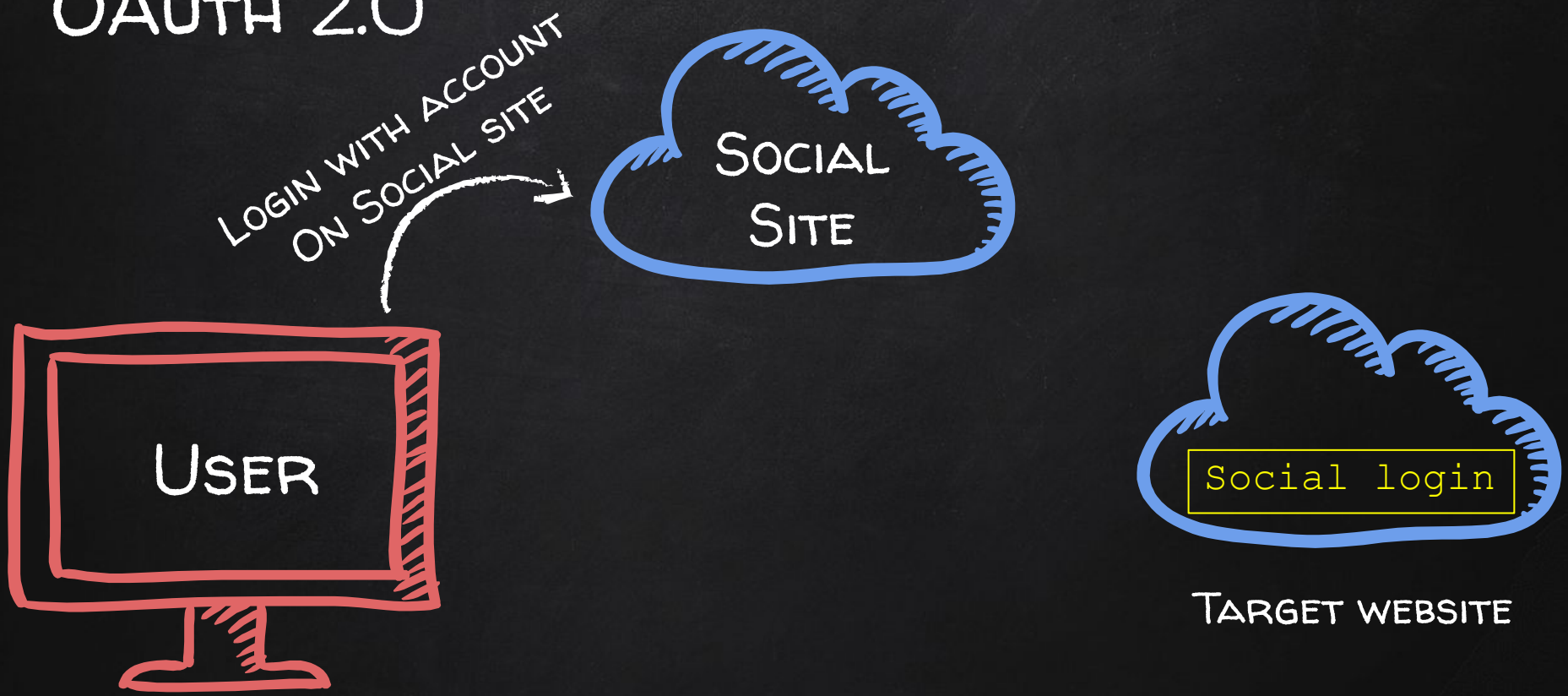
OAuth 2.0



OAuth 2.0



OAuth 2.0

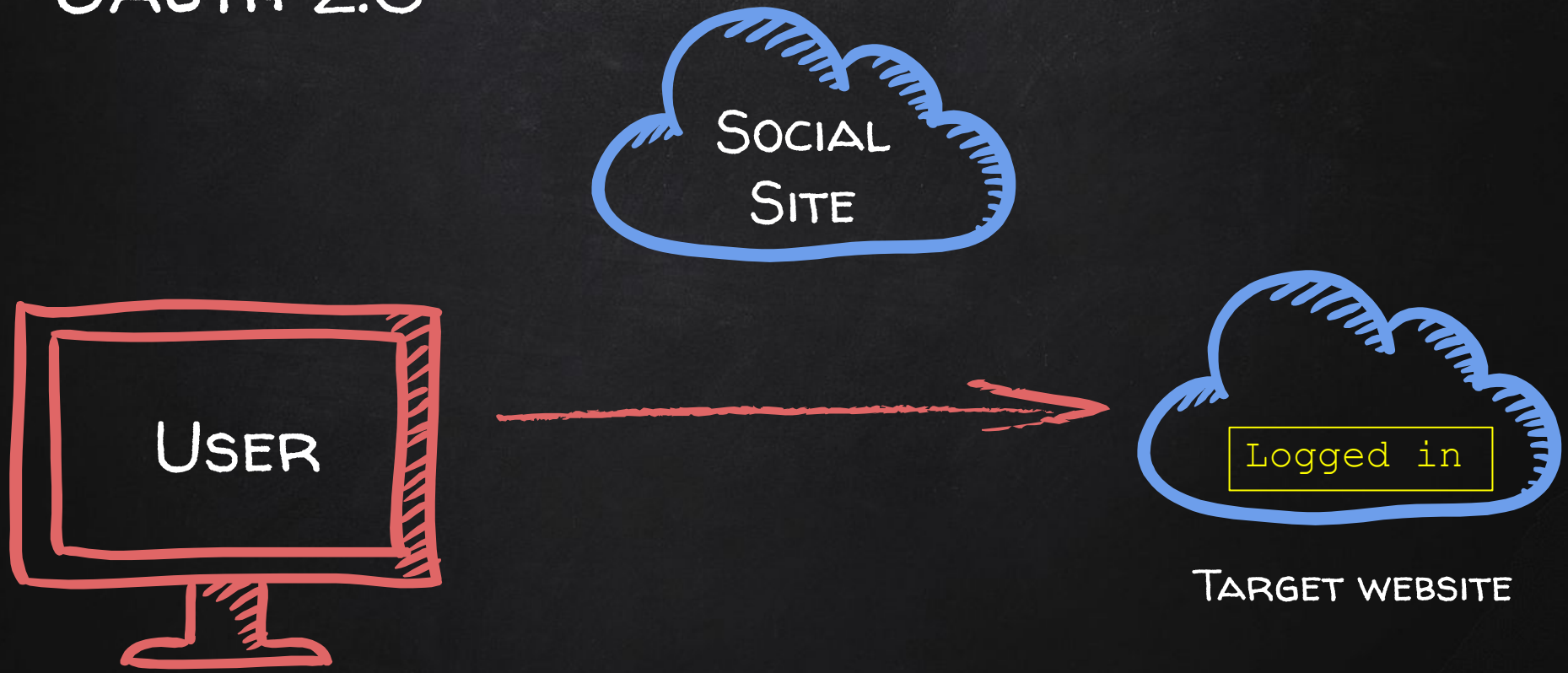

Login with account
On Social site
Social
Site
User
Social login
Target website

OAuth 2.0

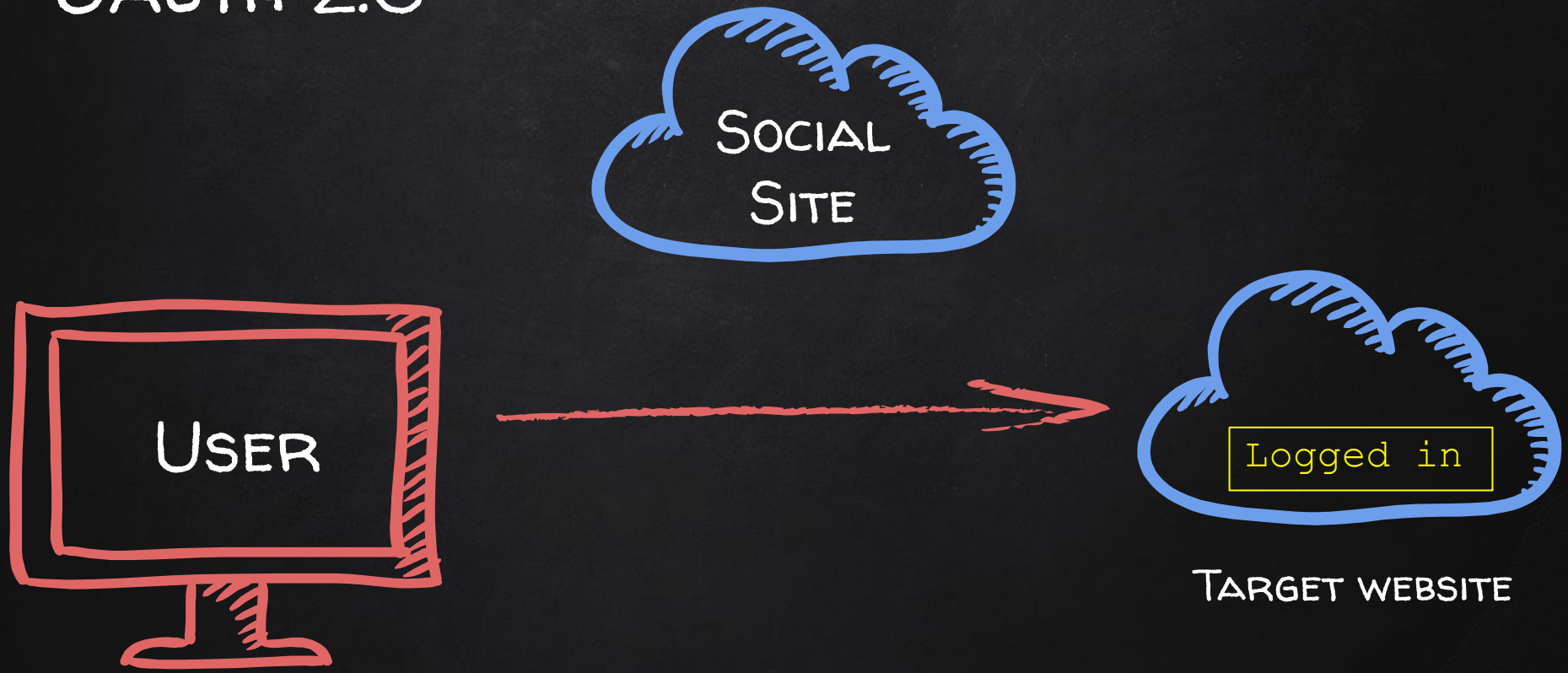
OAuth 2.0


User
Social Site
Requested Date
Access Token
Social login
Target website

OAuth 2.0



OAuth 2.0

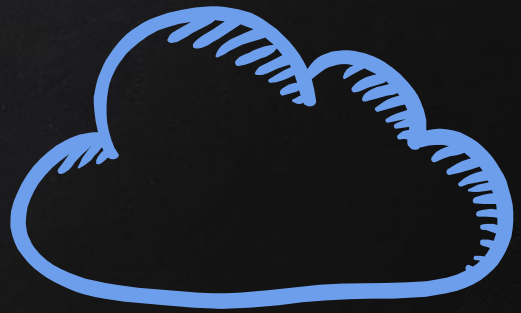


Cross Site Request Forgery

CSRF

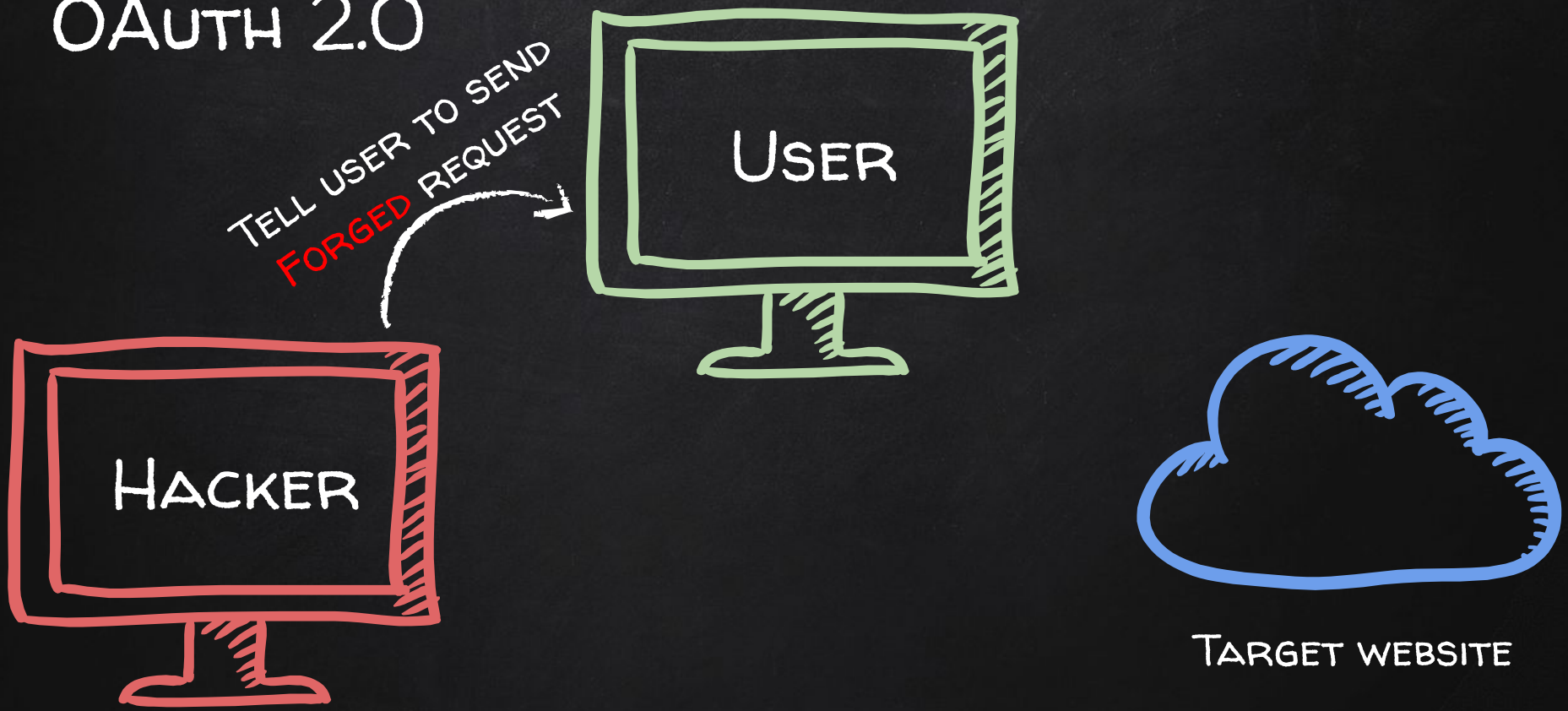
- Requests are not validated at the server side.
- Server does not check if the user generated the request.
- Requests can be forged and sent to users to make them do things they don't intend to do such as changing their password.

OAuth 2.0



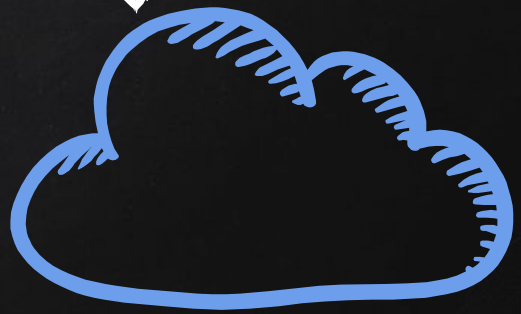
Target website

OAuth 2.0


Tell user to send
Forged request
User
Hacker
Target website

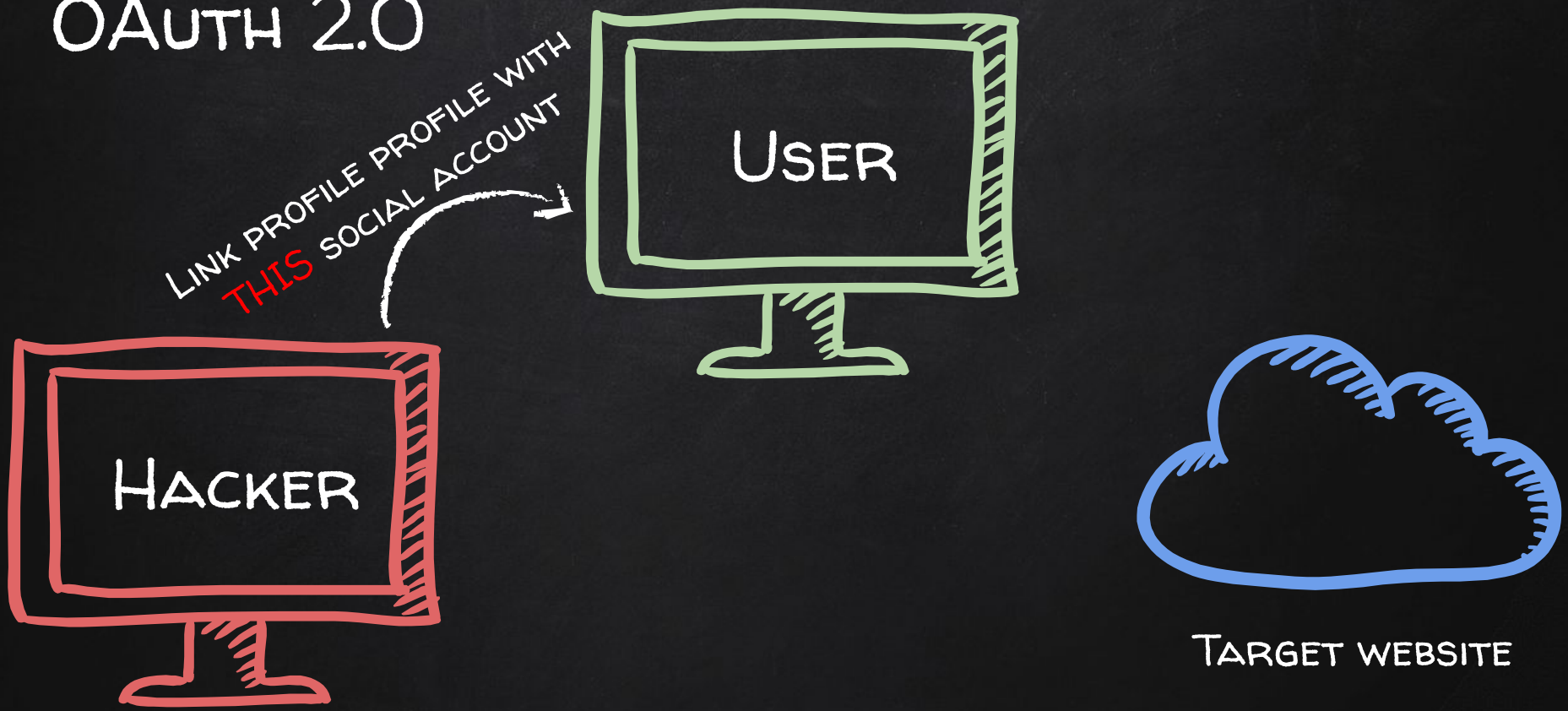
OAuth 2.0

Forged Request



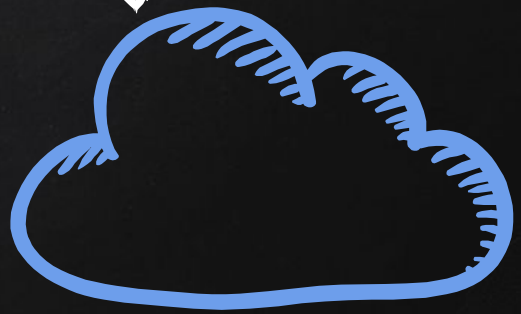
Target website

OAuth 2.0


Link profile profile with
THIS social account
User
Hacker
Target website

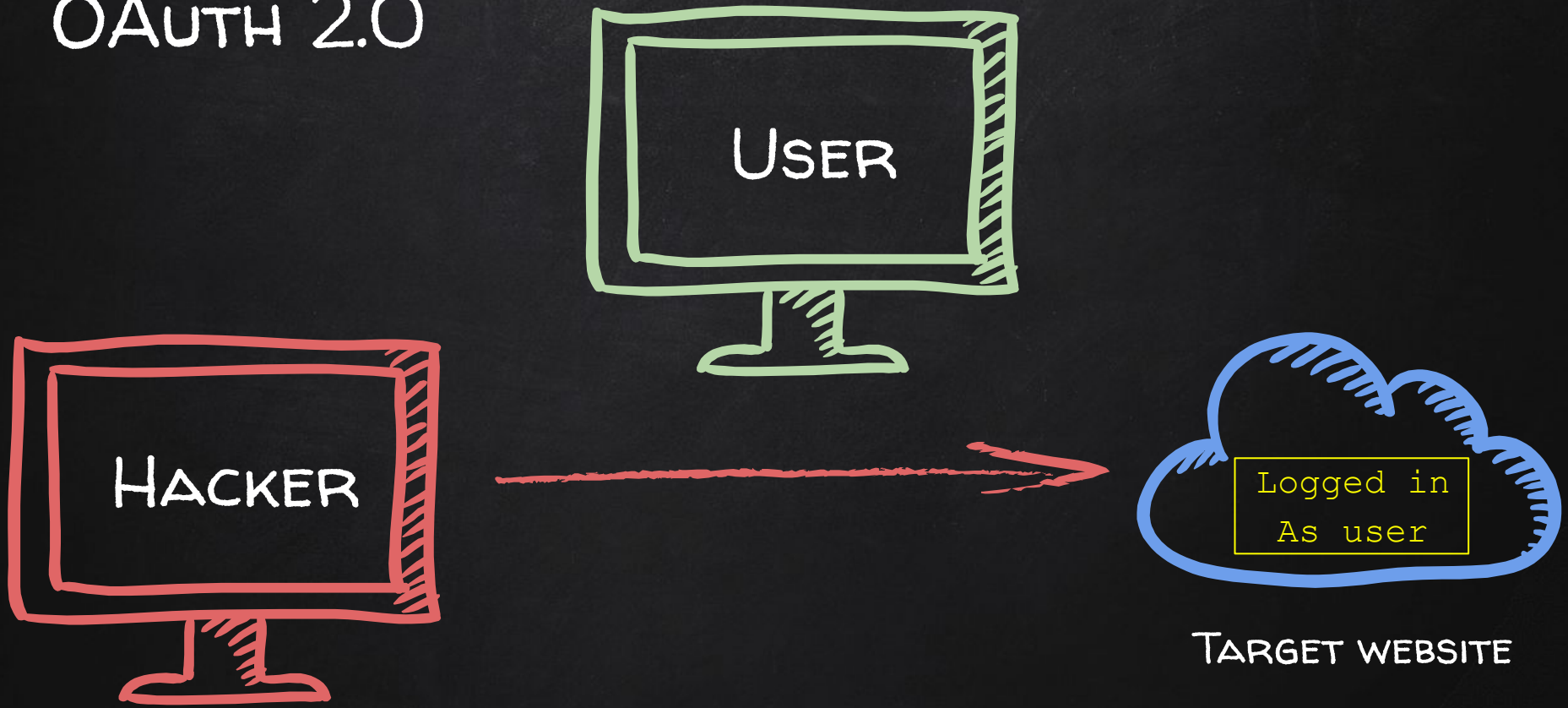
OAuth 2.0

Forged Request

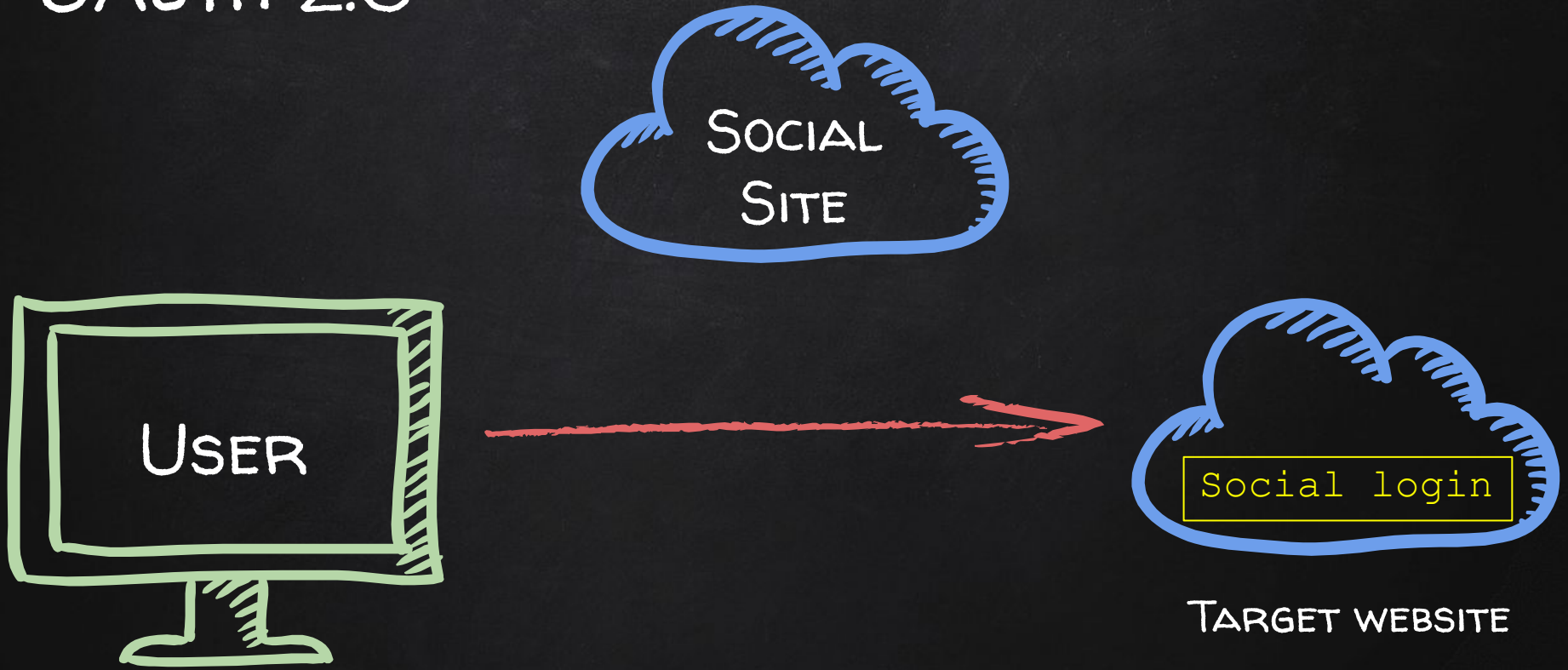


Target website

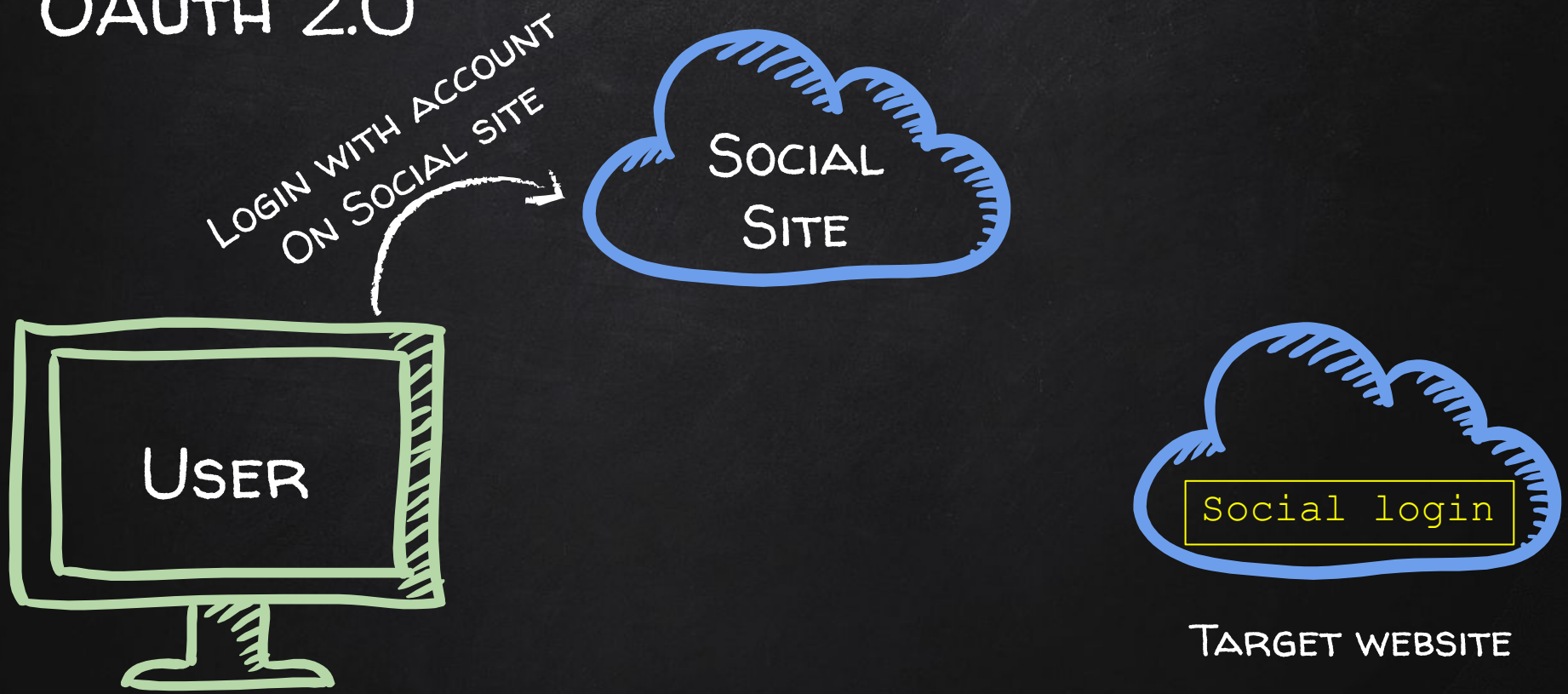
OAuth 2.0



OAuth 2.0



OAuth 2.0

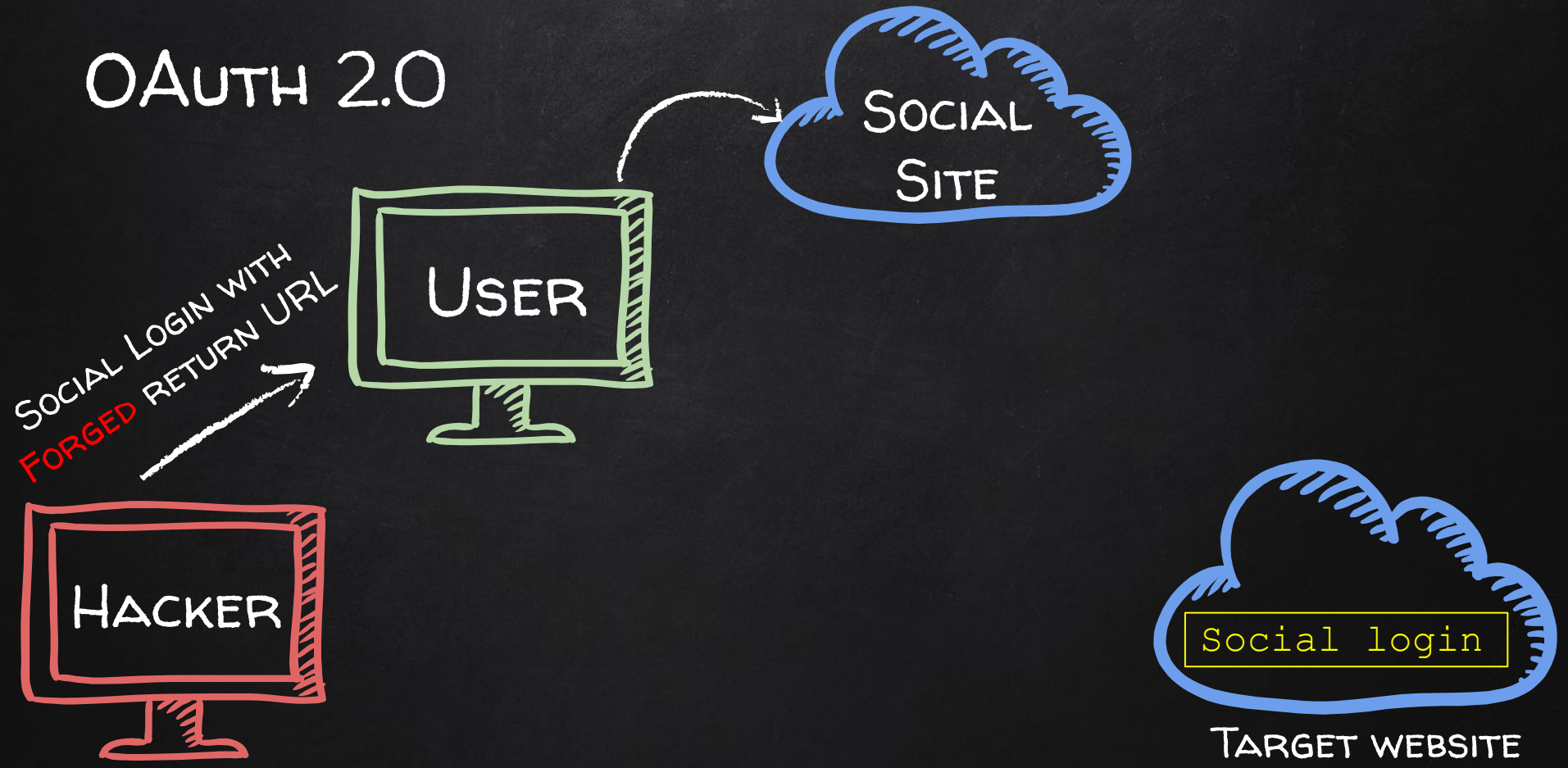

Login with account
On Social site
Social
Site
User
Social login
Target website

OAuth 2.0

OAuth 2.0


Social Site
Requested Date
User
Access Token
Social login
Target website

OAuth 2.0

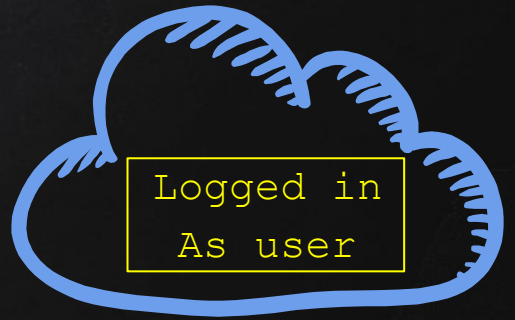

Social Site
User
Social Login with
Forged return URL
Hacker
Social login
Target website

OAuth 2.0


Social Site
User
Social Login with
Forged return URL
Access Token
Hacker's
server
Hacker
Access Token
Social login
Target website

OAuth 2.0

Access Token



Target website