WPSE: Fortifying Web Protocols via Browser-Side Security Monitoring

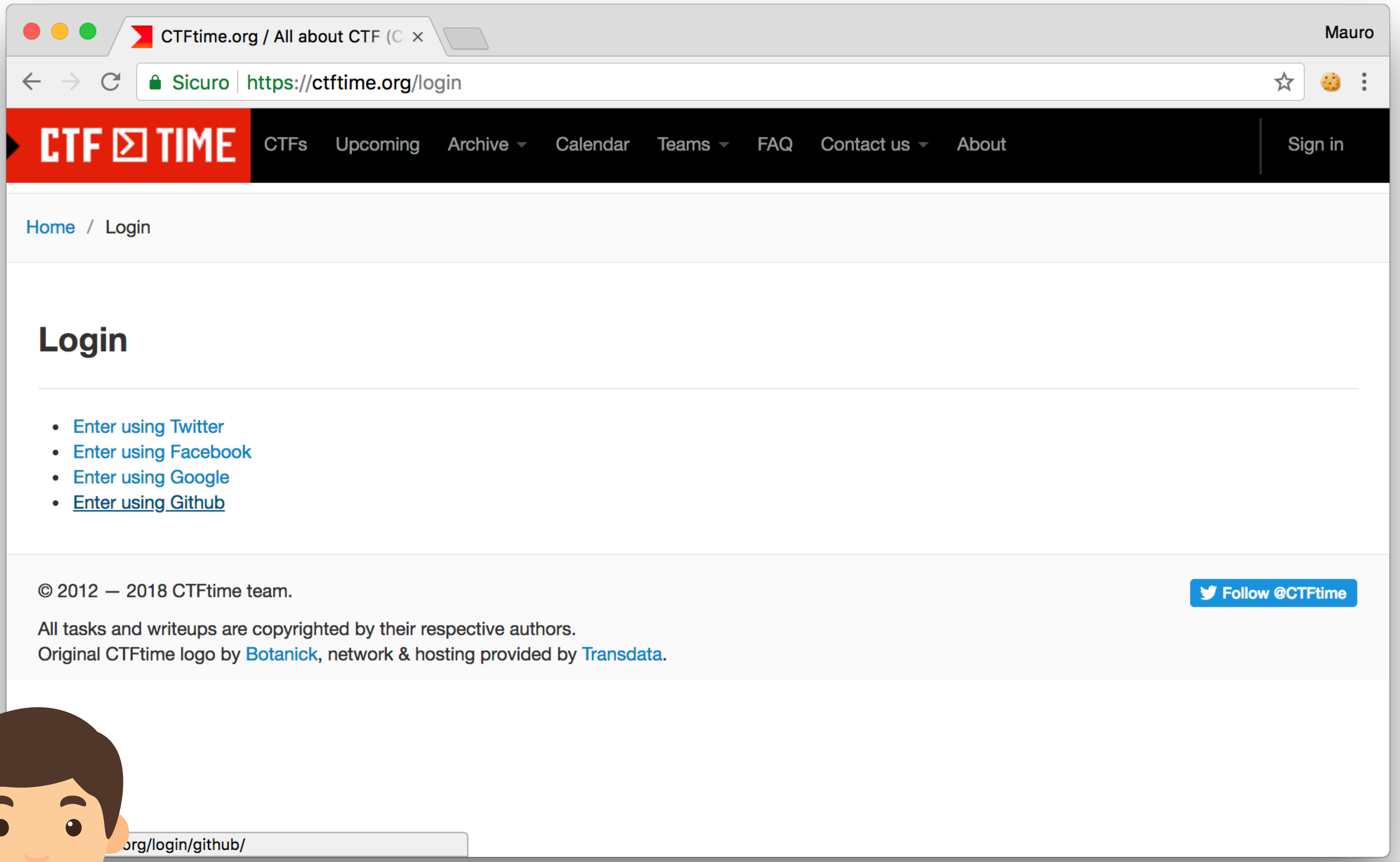
Marco Squarcina
Joint work w. Stefano Calzavara, Riccardo Focardi, Matteo Maffei,
Clara Schneidewind, Mauro Tempesta

4th OAuth Security Workshop 2019
March 21, 2019 - Stuttgart/Germany

TECHNISCHE UNIVERSITÄT WIEN

Università Ca'Foscari Venezia

Overview of a Web Protocol



CTFtime.org / All about CTF (C ×

Mauro

Sicuro | https://ctftime.org/login

CTF ⊡ TIME CTFs Upcoming Archive Calendar Teams FAQ Contact us About Sign in

Home / Login

Login

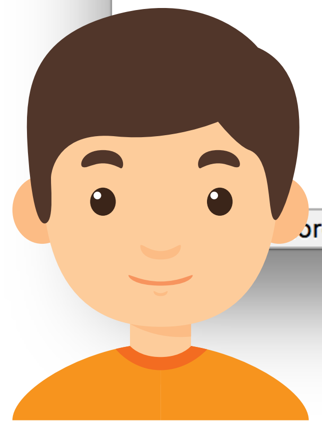
- Enter using Twitter
- Enter using Facebook
- Enter using Google
- Enter using Github

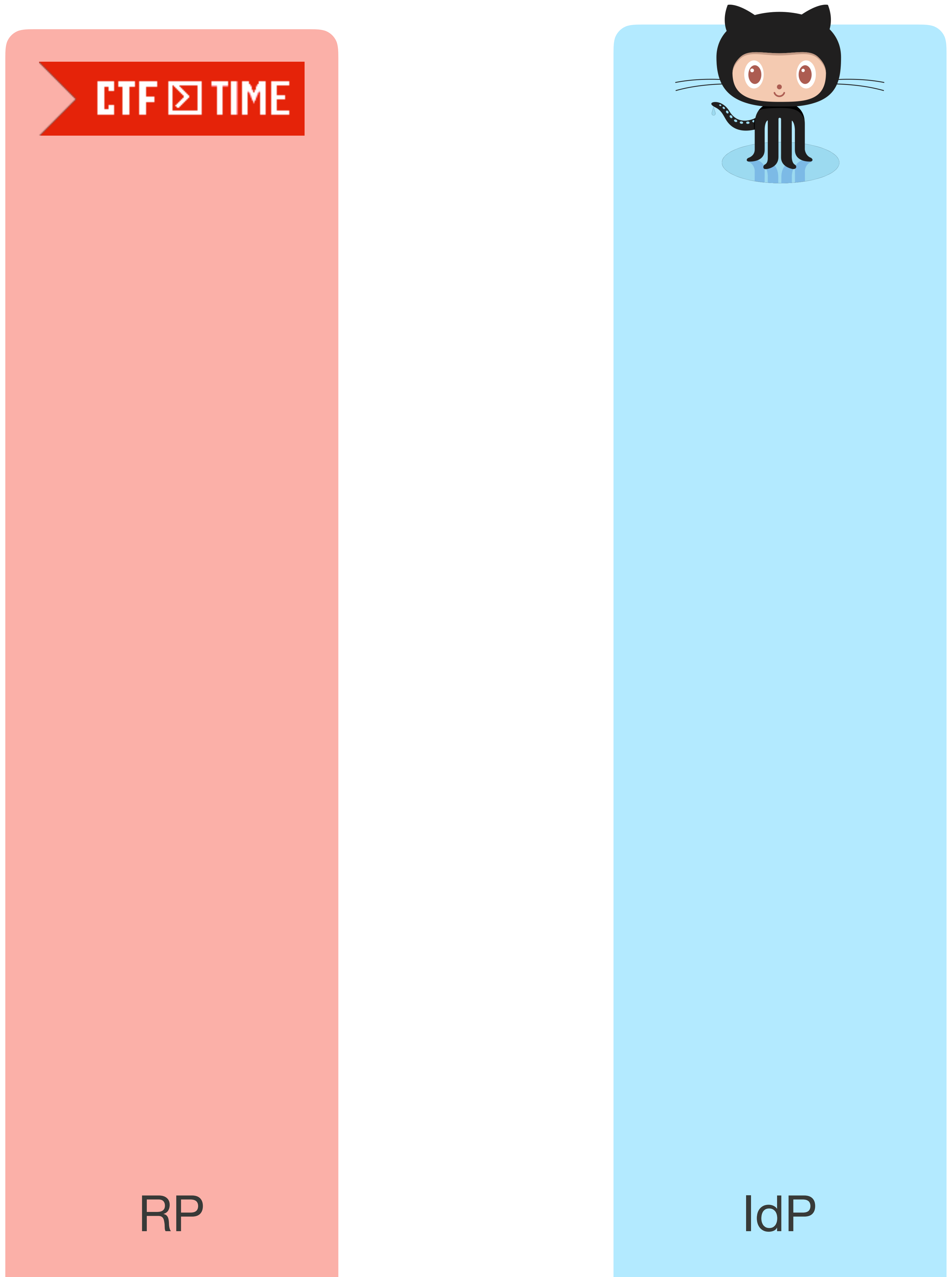
© 2012 — 2018 CTFtime team.

Follow @CTFtime

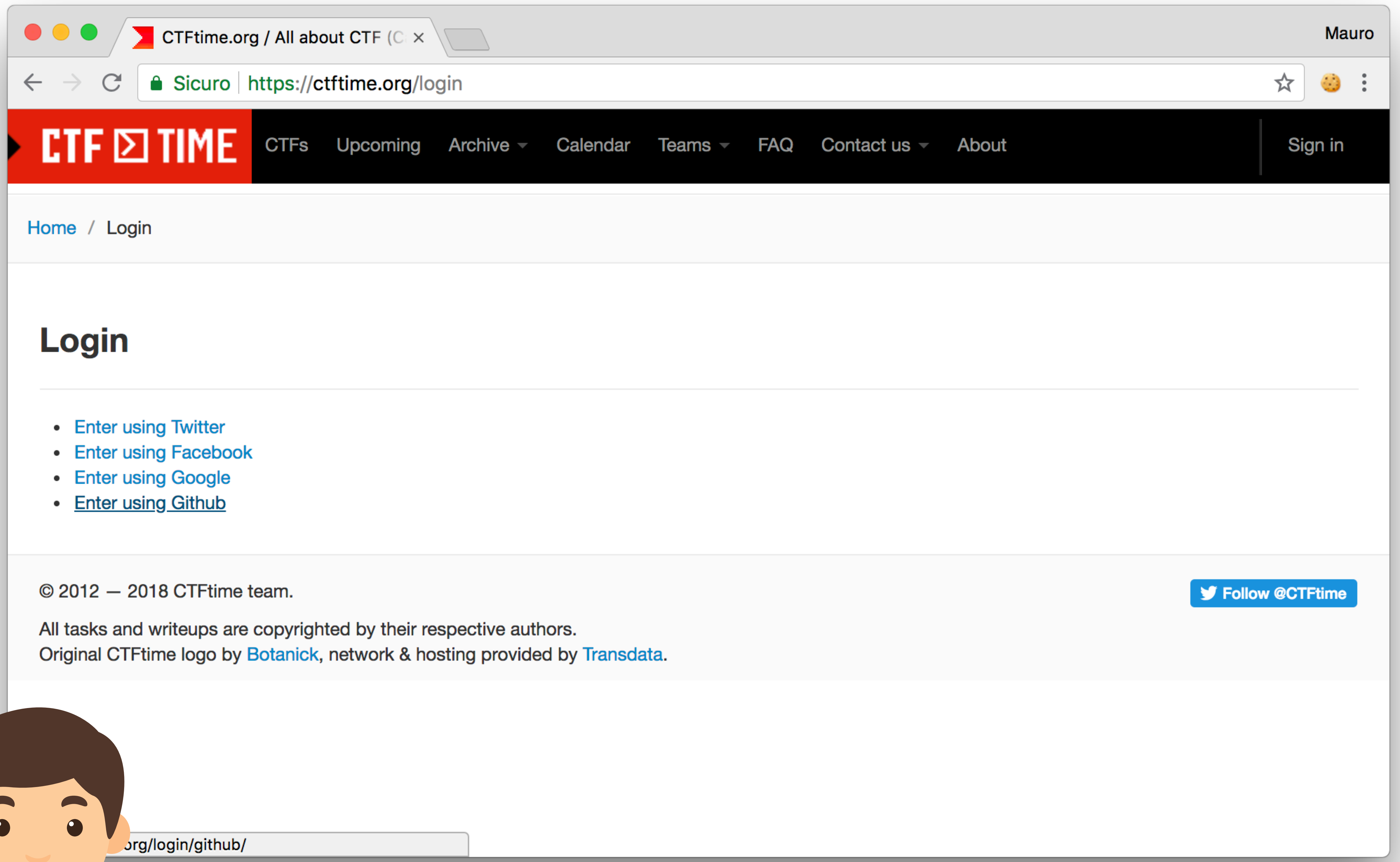
All tasks and writeups are copyrighted by their respective authors.
Original CTFtime logo by Botanick, network & hosting provided by Transdata.

org/login/github/





Overview of a Web Protocol


CTFtime.org / All about CTF (C ×

Mauro

Sicuro | https://ctftime.org/login

CTF TIME CTFs Upcoming Archive Calendar Teams FAQ Contact us About Sign in

Home / Login

Login

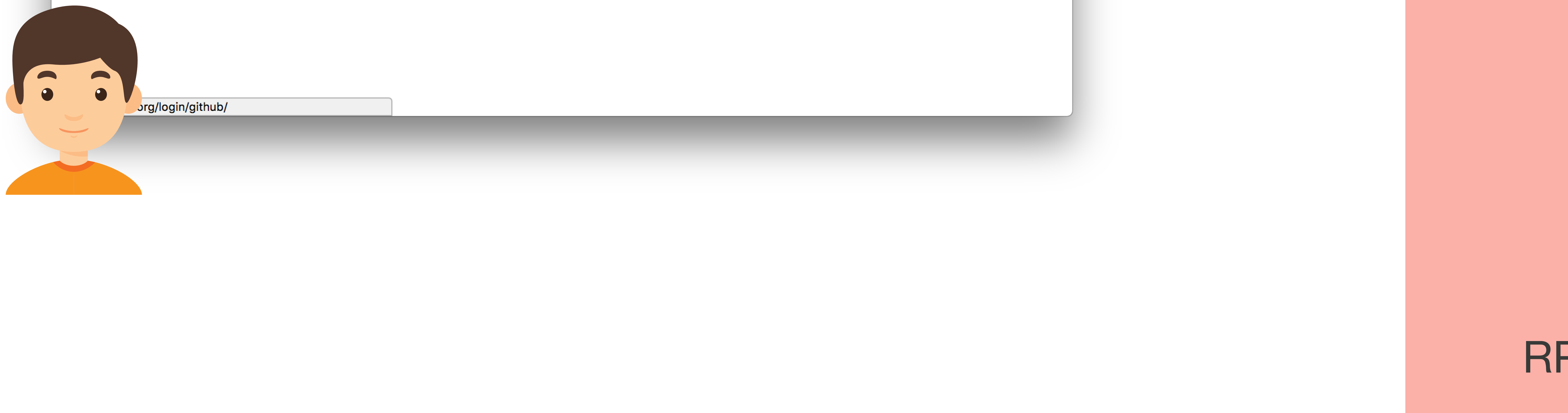
- Enter using Twitter
- Enter using Facebook
- Enter using Google
- Enter using Github

© 2012 — 2018 CTFtime team.

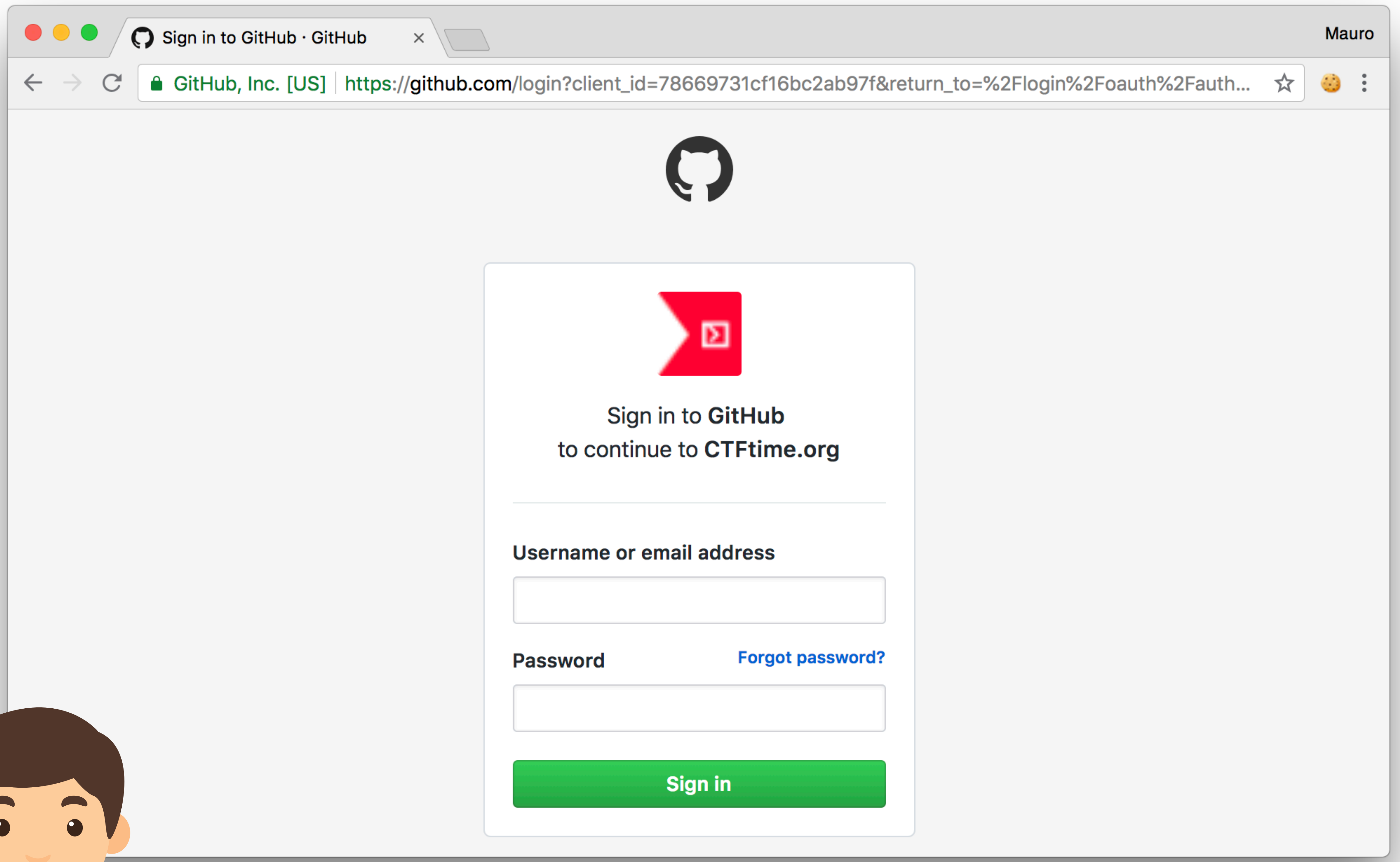
Follow @CTFtime

All tasks and writeups are copyrighted by their respective authors.
Original CTFtime logo by Botanick, network & hosting provided by Transdata.

org/login/github/



Overview of a Web Protocol

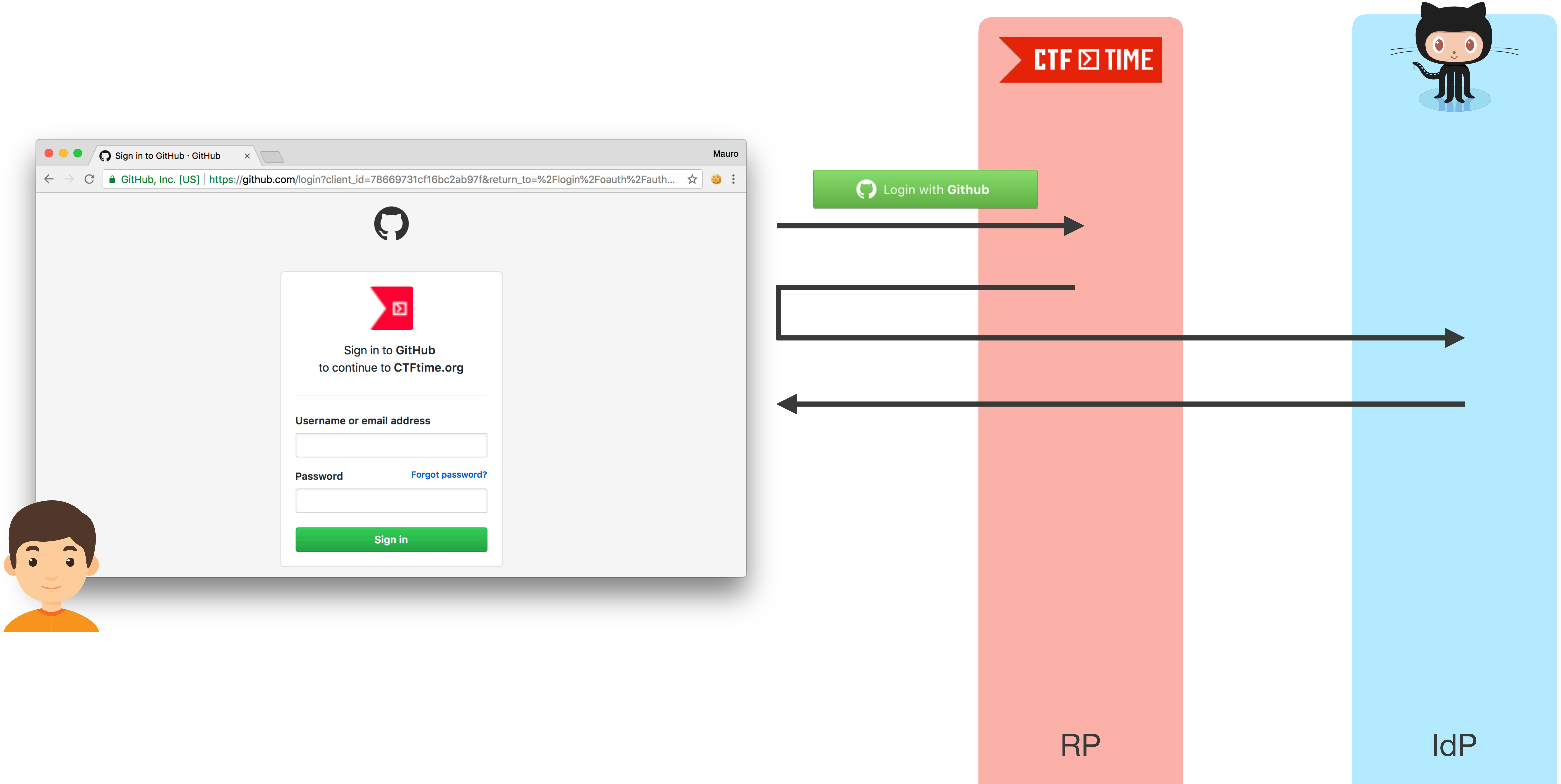

Sign in to GitHub · GitHub
Mauro
GitHub, Inc. [US] https://github.com/login?client_id=78669731cf16bc2ab97f&return_to=%2Flogin%2Foauth%2Fauth...

Sign in to **GitHub**
to continue to **CTFtime.org**

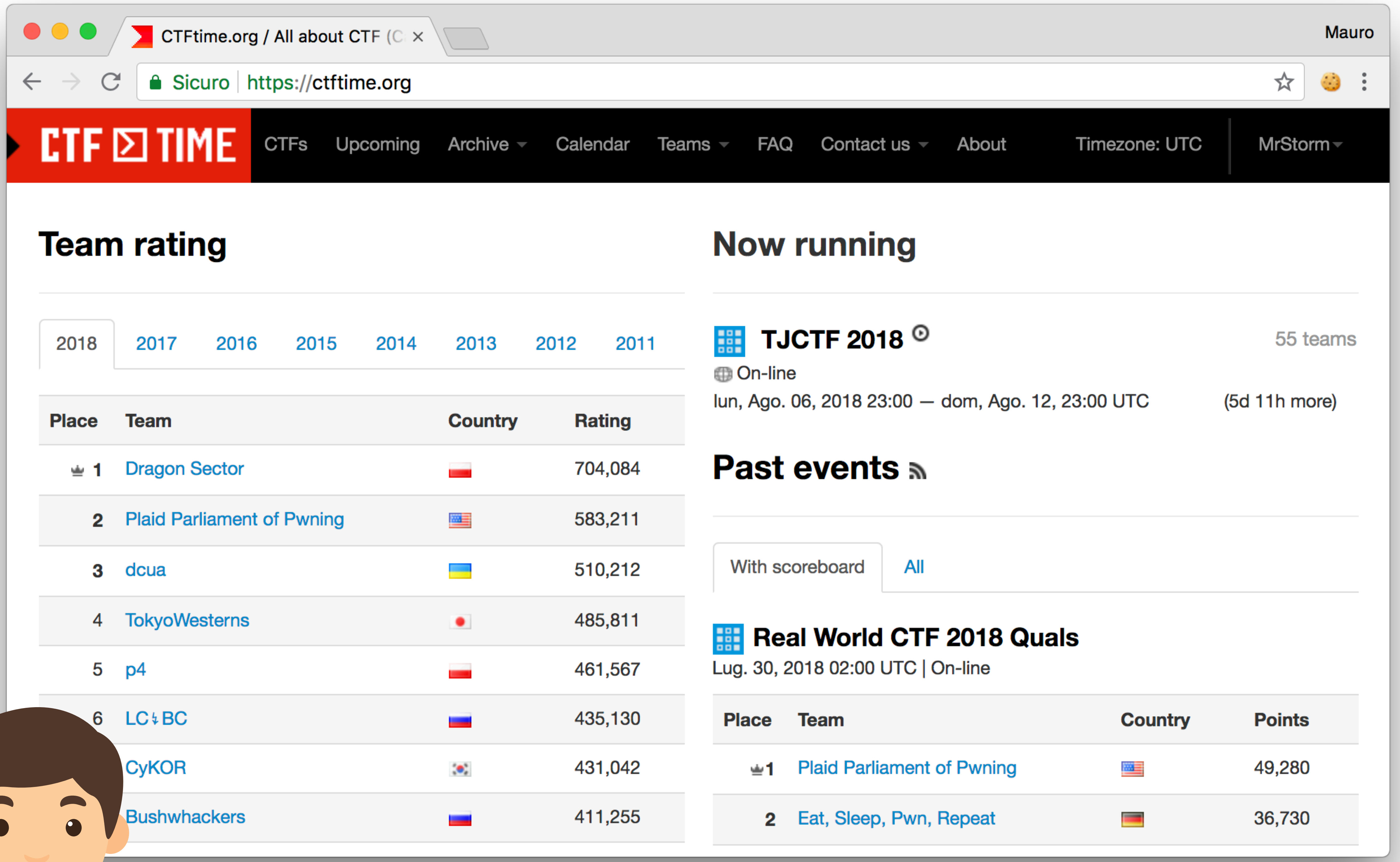
Username or email address

Password Forgot password?

Sign in



Overview of a Web Protocol



CTFtime.org / All about CTF (C ×   Mauro

Sicuro | https://ctftime.org

CTF TIME | CTFs | Upcoming | Archive | Calendar | Teams | FAQ | Contact us | About | Timezone: UTC | MrStorm

Team rating

2018 | 2017 | 2016 | 2015 | 2014 | 2013 | 2012 | 2011

Place	Team	Country	Rating
1	Dragon Sector	🇵🇱	704,084
2	Plaid Parliament of Pwning	🇺🇸	583,211
3	dcua	🇺🇦	510,212
4	TokyoWesterns	🇯🇵	485,811
5	p4	🇵🇱	461,567
6	LC↯BC	🇷🇺	435,130
	CyKOR	🇰🇷	431,042
	Bushwhackers	🇷🇺	411,255

Now running

TJCTF 2018 — 55 teams

On-line

lun, Ago. 06, 2018 23:00 — dom, Ago. 12, 23:00 UTC (5d 11h more)

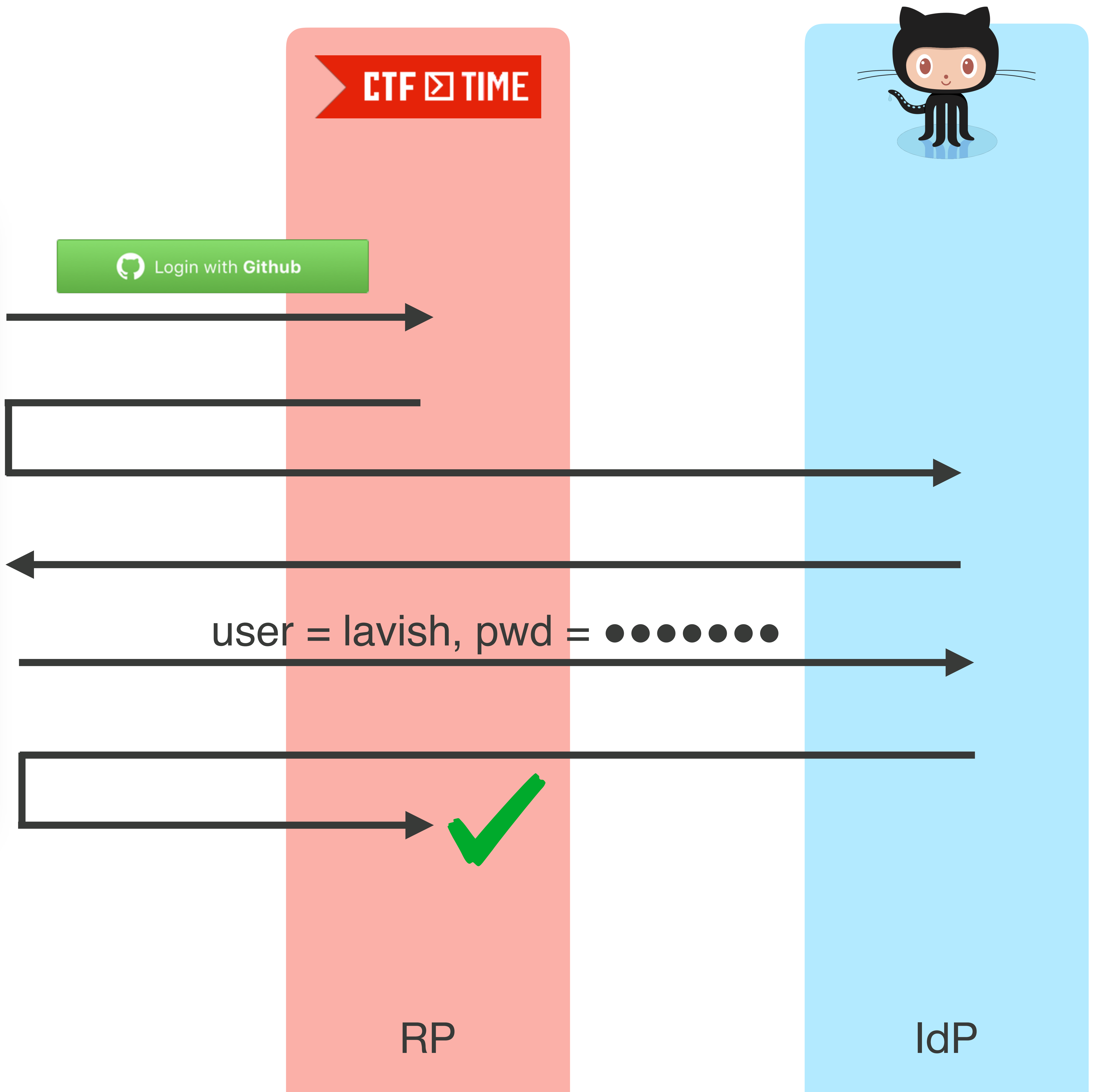
Past events

With scoreboard | All

Real World CTF 2018 Quals

Lug. 30, 2018 02:00 UTC | On-line

Place	Team	Country	Points
1	Plaid Parliament of Pwning	🇺🇸	49,280
2	Eat, Sleep, Pwn, Repeat	🇩🇪	36,730



Motivations

Designing and implementing web protocols is **HARD!**

- *Bansal et al*., Discovering Concrete Attacks on Website Authorization by Formal Analysis (**S&P '12**)
- *Wang et al.,* Signing Me onto Your Accounts through Facebook and Google: A Traffic-Guided Security Study of Commercially Deployed Single-Sign-On Web Services (**S&P'12**)
- *Sun and Beznosov,* The Devil is in the (Implementation) Details: An Empirical Analysis of OAuth SSO Systems (**CCS'12**)
- *Fett et al.,* A Comprehensive Formal Security Analysis of OAuth 2.0 (**CCS'16**)
- …

Motivations

Designing and implementing web protocols is **HARD**!

- *Bansal et al*., Discovering Concrete Attacks on Website Authorization by Formal Analysis (**S&P '12**)
- *Wang et al.,* Signing Me onto Your Accounts through Facebook and Google: A Traffic-Guided Security Study of Commercially Deployed Single-Sign-On Web Services (**S&P'12**)
- *Sun and Beznosov,* The Devil is in the (Implementation) Details: An Empirical Analysis of OAuth SSO Systems (**CCS'12**)
- *Fett et al.,* A Comprehensive Formal Security Analysis of OAuth 2.0 (**CCS'16**)
- …

WHY?

MOTIVATIONS

Designing and implementing web protocols is **HARD!**

- *Bansal et al*., Discovering Concrete Attacks on Website Authorization by Formal Analysis (**S&P '12**)
- *Wang et al.,* Signing Me onto Your Accounts through Facebook and Google: A Traffic-Guided Security Study of Commercially Deployed Single-Sign-On Web Services (**S&P'12**)
- *Sun and Beznosov,* The Devil is in the (Implementation) Details: An Empirical Analysis of OAuth SSO Systems (**CCS'12**)
- *Fett et al.,* A Comprehensive Formal Security Analysis of OAuth 2.0 (**CCS'16**)
- …

The browser is not aware of the existence of web protocols and of their semantics!

Our Proposal - WPSE

Extend the browser with a **lightweight security monitor** that enforces the compliance of the browser behaviors with respect to the web protocol specifications

Our Proposal - WPSE

Implemented as a Google Chrome **extension**

Extend the browser with a **lightweight security monitor** that enforces the compliance of the browser behaviors with respect to the web protocol specifications

Our Proposal - WPSE

Implemented as a Google Chrome **extension**

Extend the browser with a **lightweight security monitor** that enforces the compliance of the browser behaviors with respect to the web protocol specifications

Advantages

1. users of vulnerable websites are **automatically protected** against a large class of attacks
2. specifications can be **written once** and **enforced on several sites**

Challenges in Web Protocols

Compliance with the protocol flow

- Preserve the intended sequence of messages exchanged by honest participants
- Perform integrity checks on the contents of protocol messages

Secrecy of message components

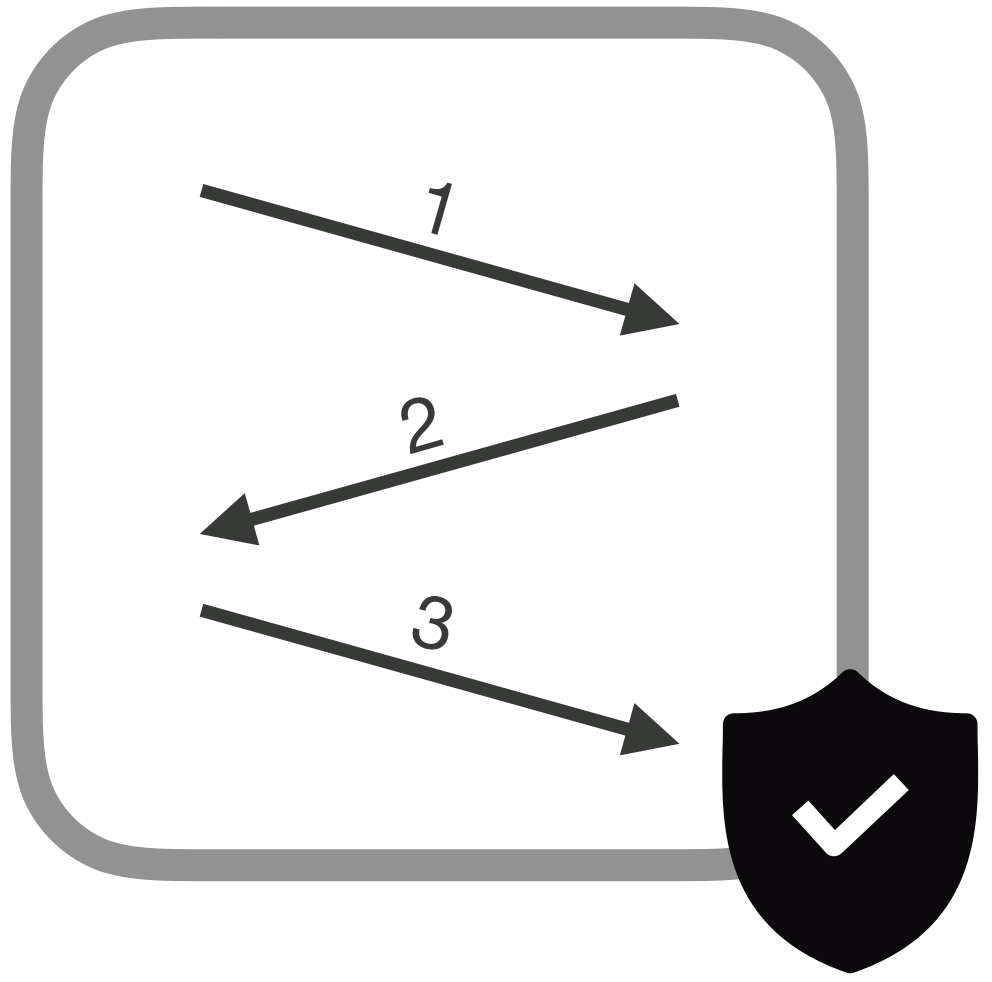
- Enforce the confidentiality of protocol secrets like tokens and credentials to avoid leaks to 3rd parties

Tackling the Challenges in WPSE

WPSE protocol specification:

- Structure and order of messages
- Desired security policies (confidentiality and integrity)

Tackling the Challenges in WPSE



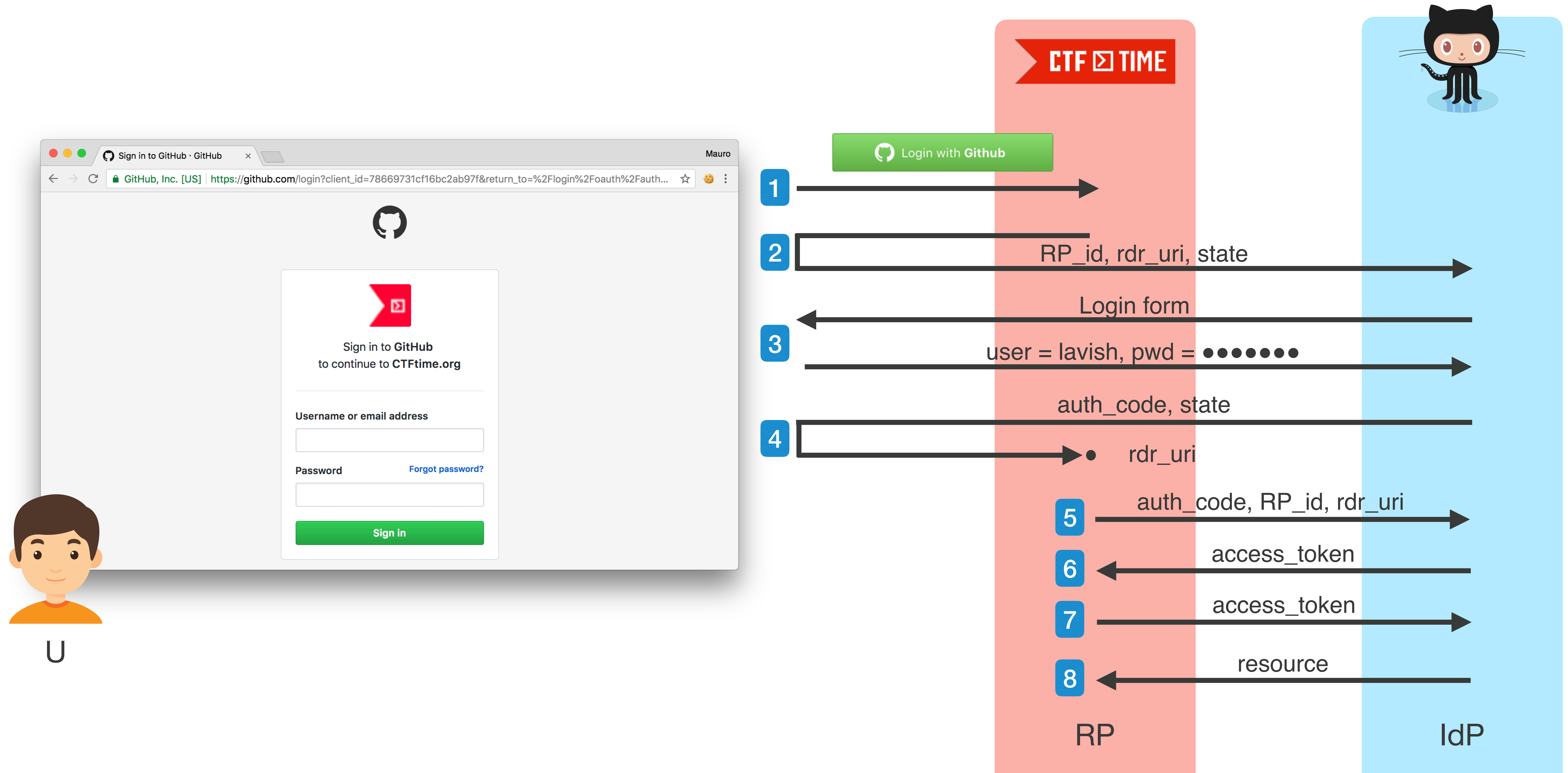
Protocol messages are **blocked** if
- not in the correct order
- integrity constraints on messages are not satisfied

Always **allow** protocol unrelated messages

Secrets in incoming messages are substituted with **random placeholders** before they enter the DOM

Placeholders in outgoing requests are replaced with secrets **only** if sent to origins entitled to learn them

Fortifying OAuth 2.0



Sign in to GitHub · GitHub
Mauro
GitHub, Inc. [US] https://github.com/login?client_id=78669731cf16bc2ab97f&return_to=%2Flogin%2Foauth%2Fauth...

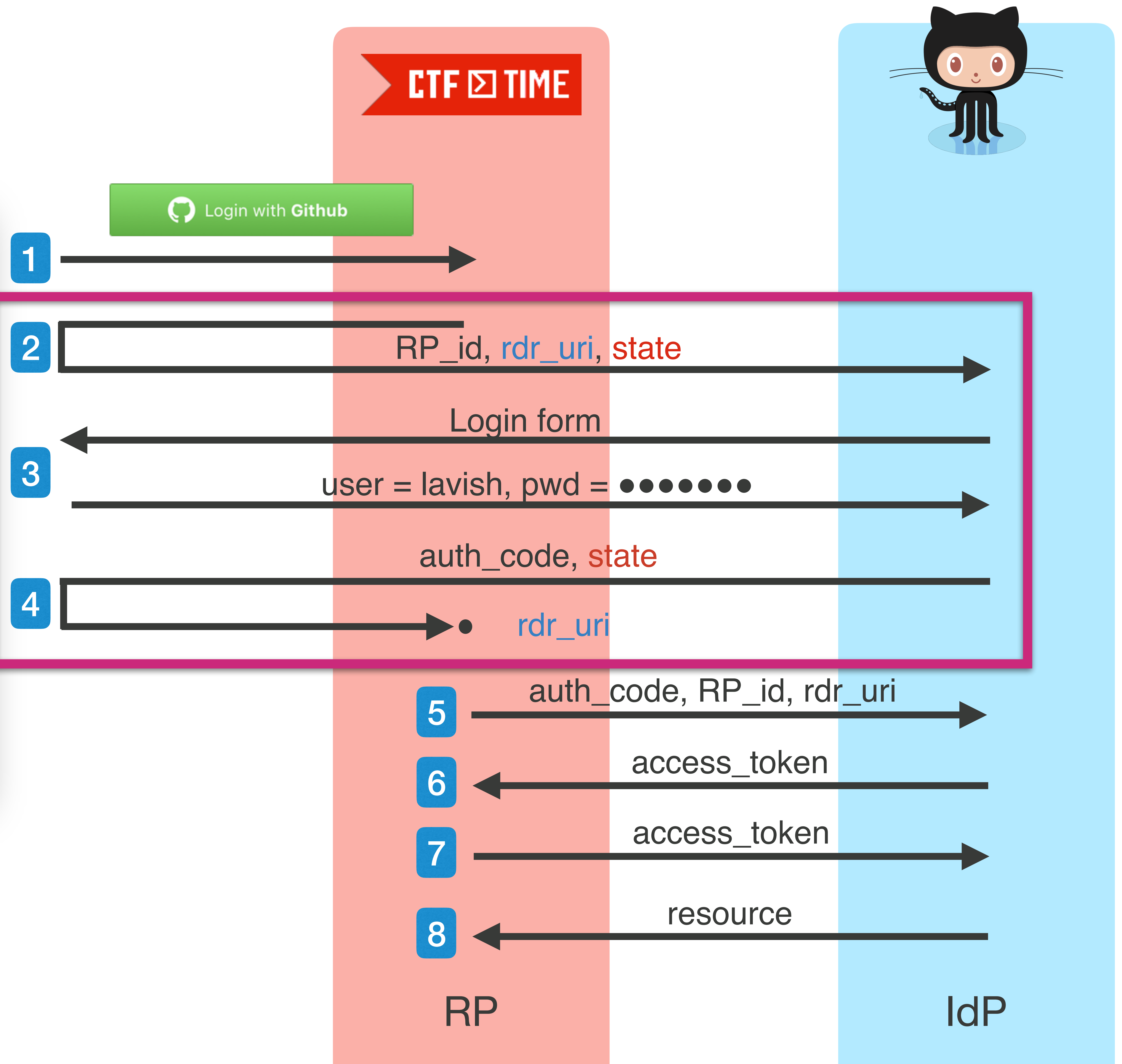
Sign in to **GitHub**
to continue to **CTFtime.org**

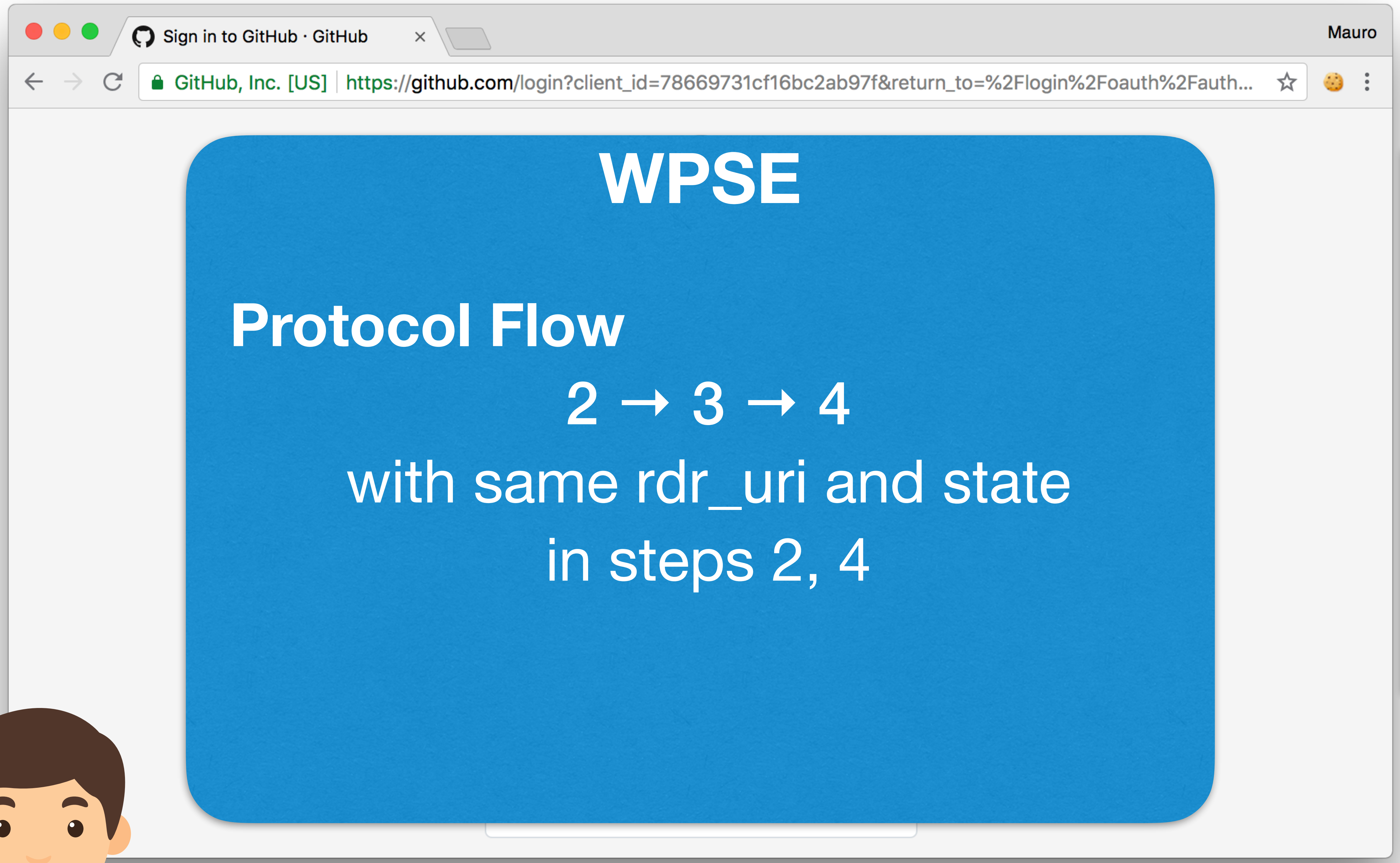
Username or email address

Password **Forgot password?**

Sign in

Fortifying OAuth 2.0




Sign in to GitHub · GitHub
Mauro
GitHub, Inc. [US] https://github.com/login?client_id=78669731cf16bc2ab97f&return_to=%2Flogin%2Foauth%2Fauth...

WPSE

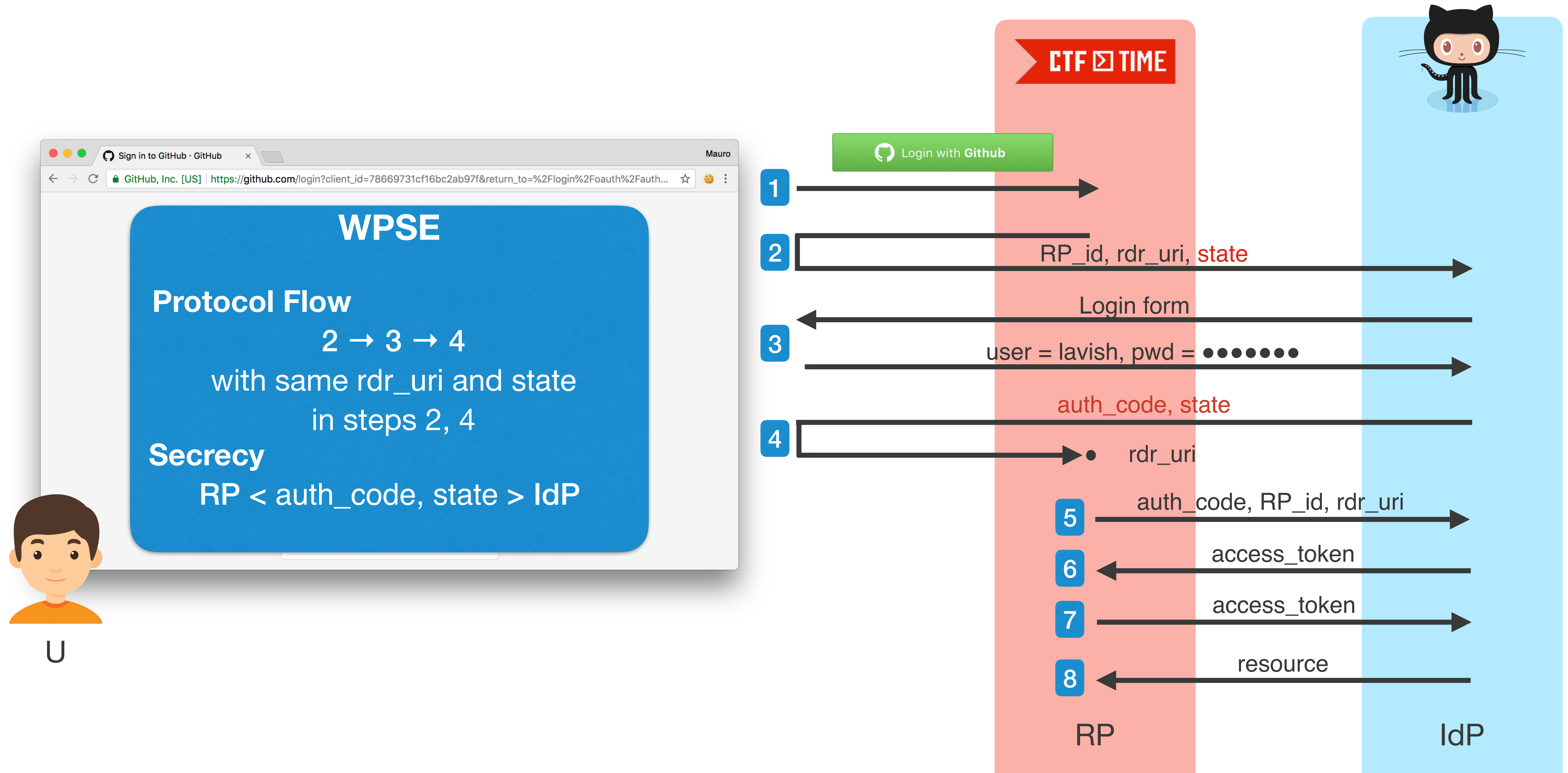
Protocol Flow

2 → 3 → 4

with same rdr_uri and state

in steps 2, 4

Fortifying OAuth 2.0



WPSE

Protocol Flow

2 → 3 → 4

with same rdr_uri and state

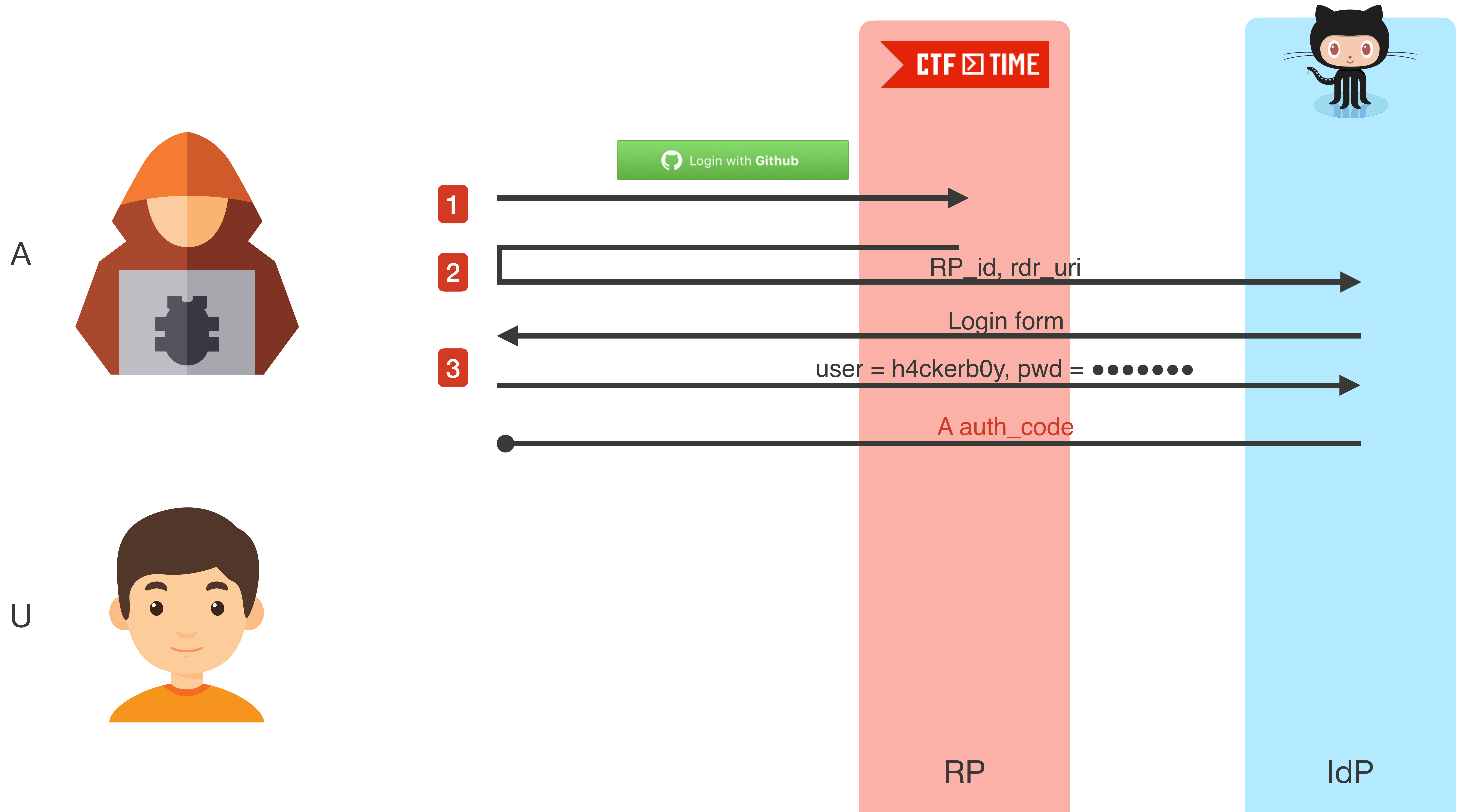
in steps 2, 4

Secrecy

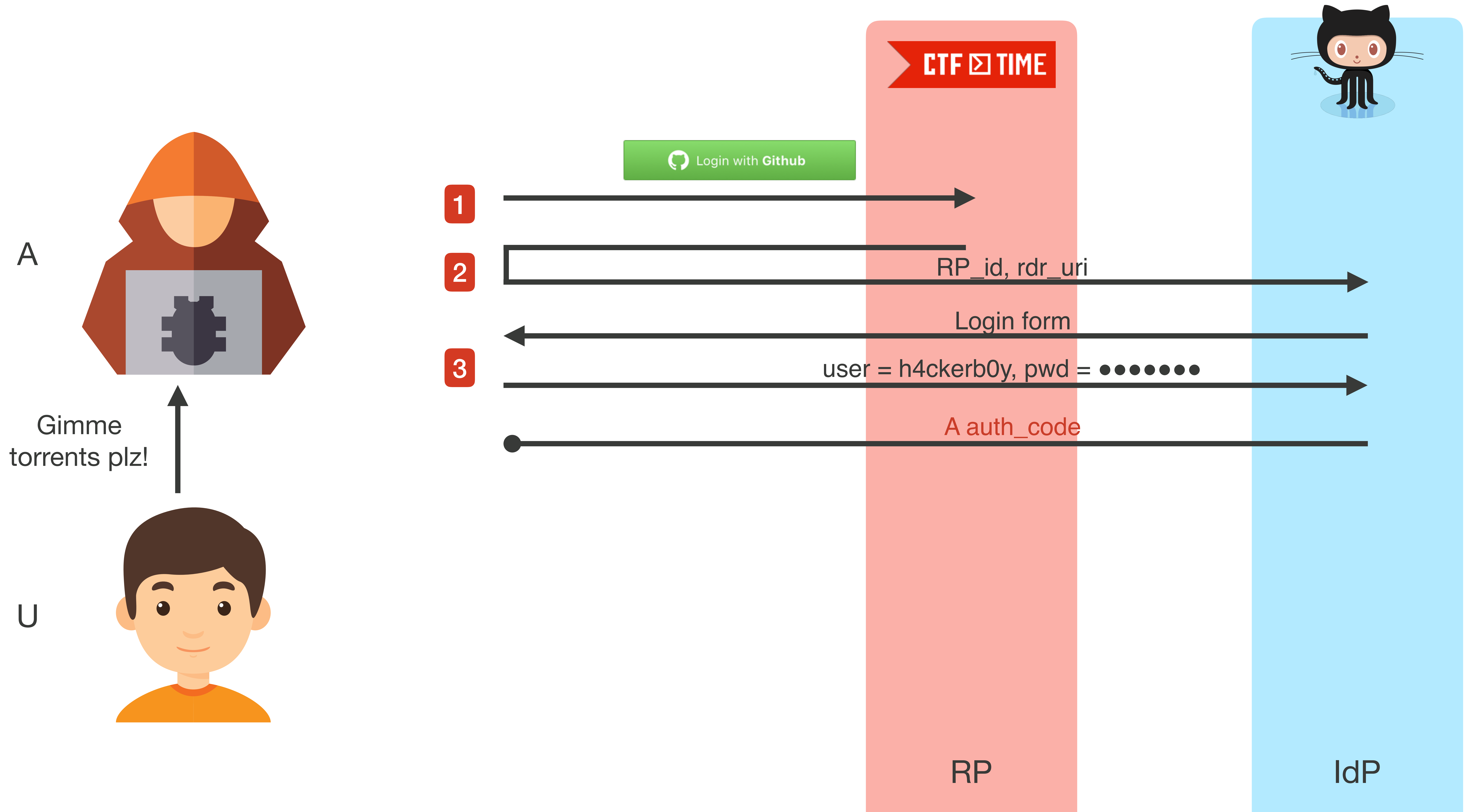
RP < auth_code, state > IdP

Sign in to GitHub · GitHub
Mauro
GitHub, Inc. [US] https://github.com/login?client_id=78669731cf16bc2ab97f&return_to=%2Flogin%2Foauth%2Fauth...
CTF TIME
Login with Github
1
2
RP_id, rdr_uri, state
Login form
3
user = lavish, pwd = ●●●●●●●
auth_code, state
4
rdr_uri
5
auth_code, RP_id, rdr_uri
6
access_token
7
access_token
8
resource
U
RP
IdP

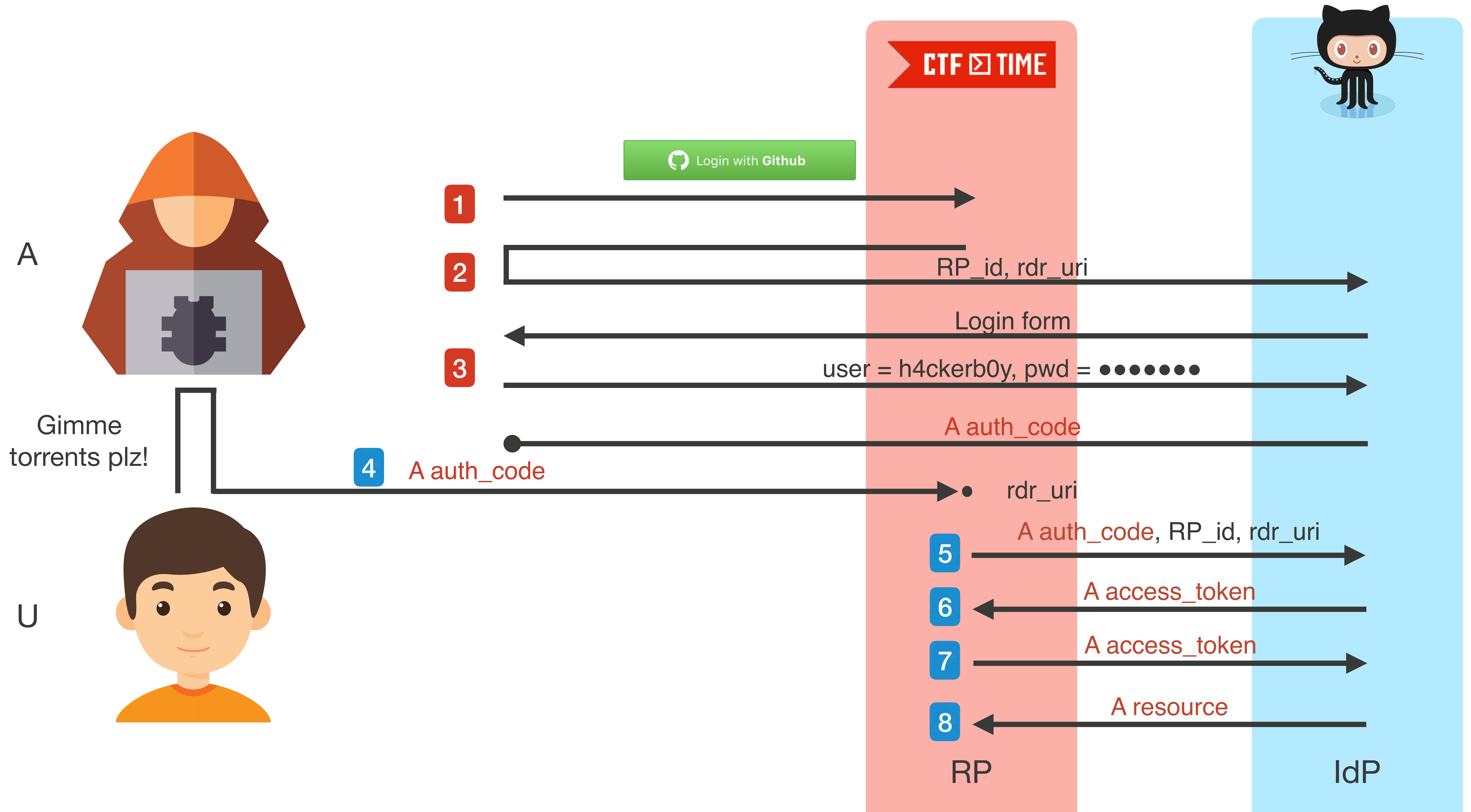
Session Swapping [SB12]



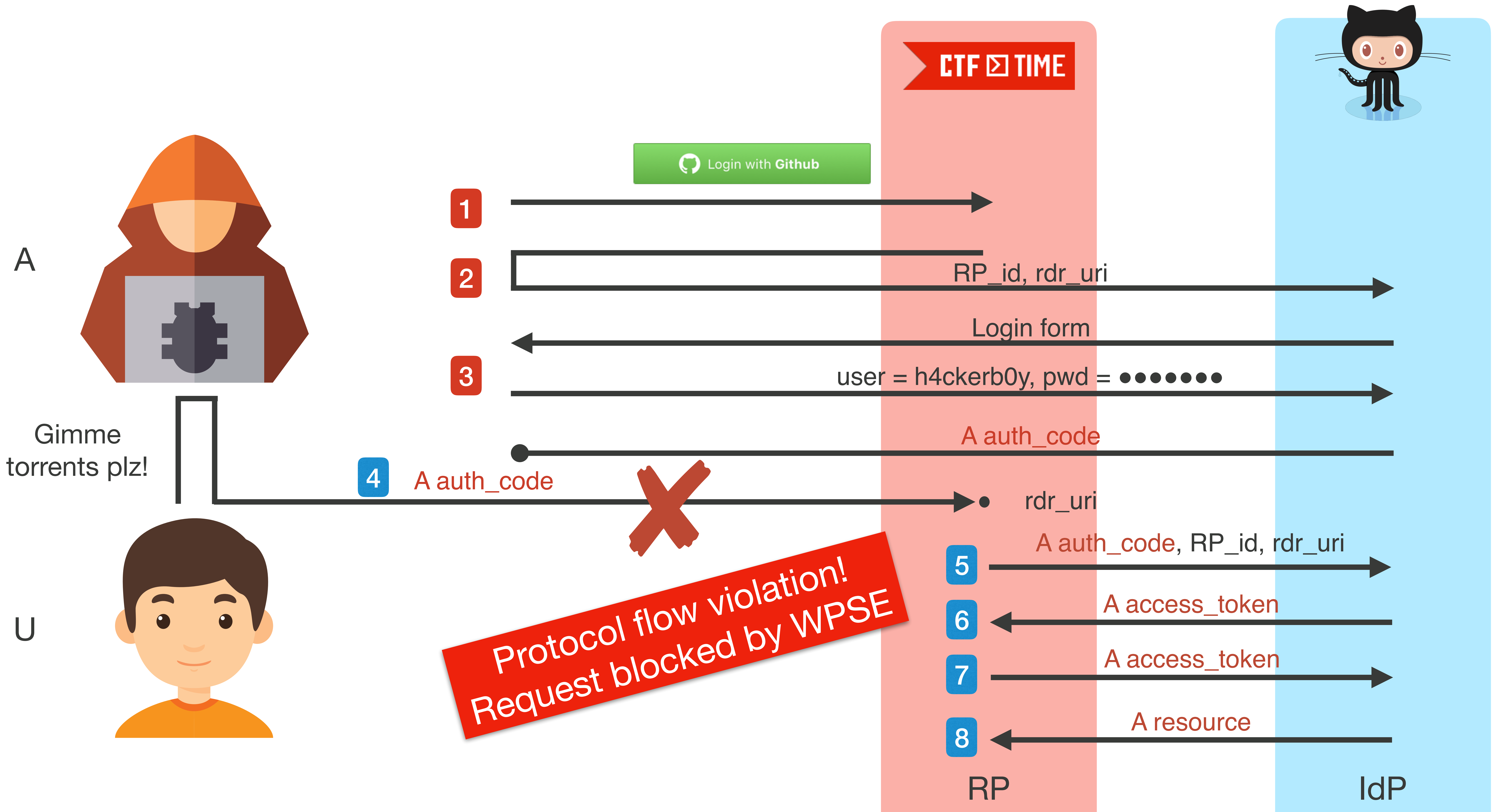
Session Swapping [SB12]



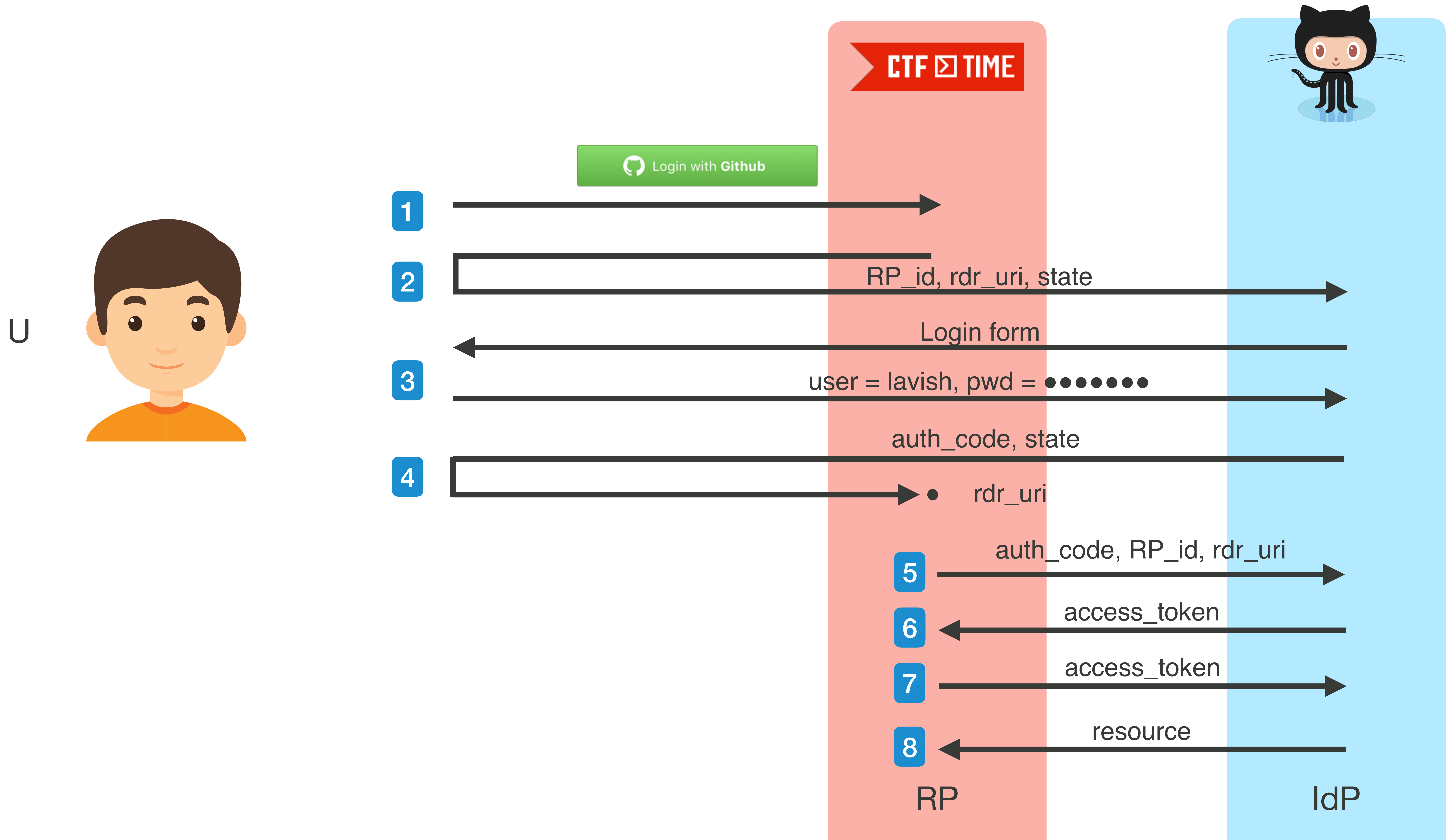
Session Swapping [SB12]



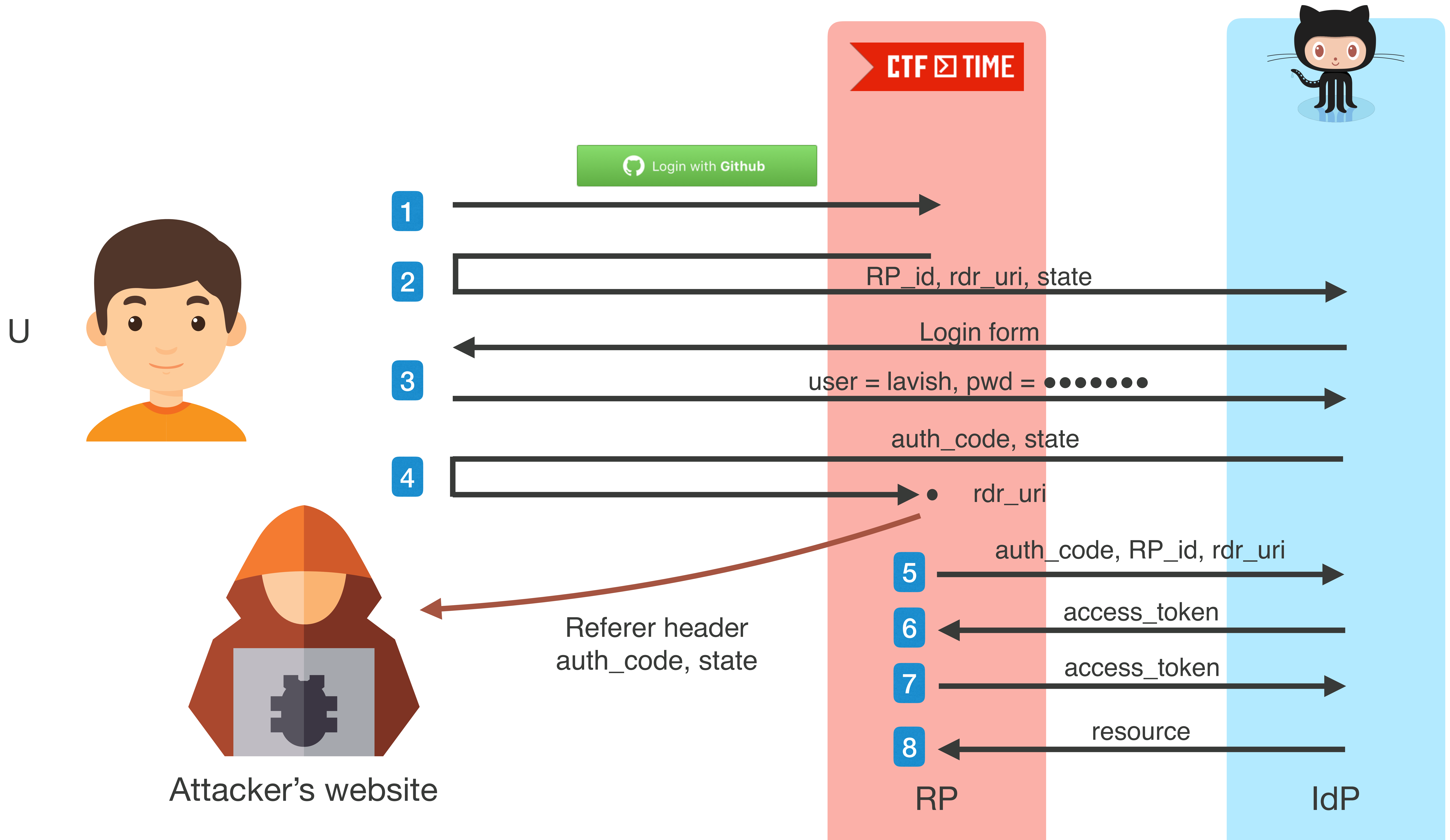
Session Swapping [SB12]



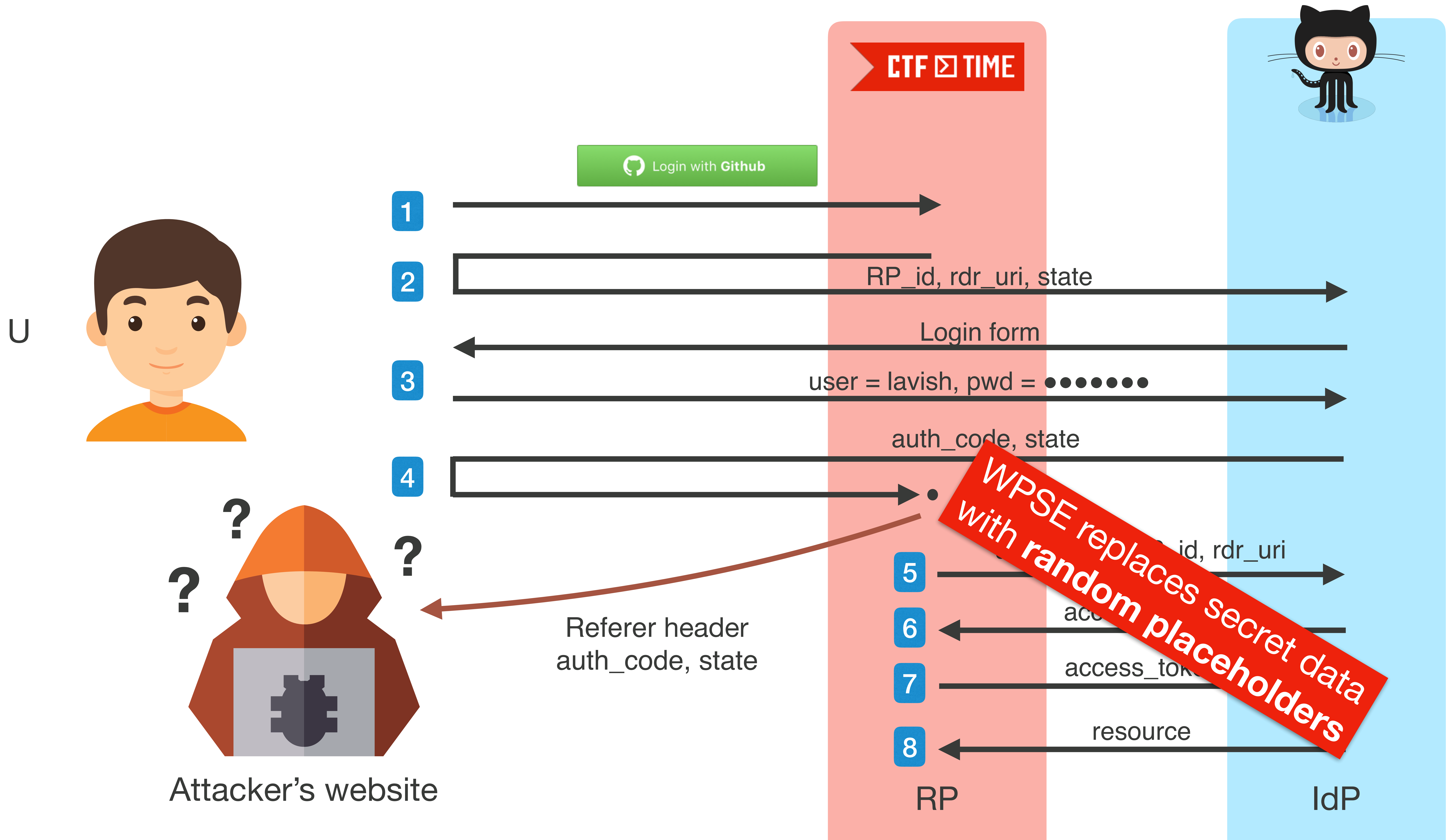
State Leak Attack [FKS16]



State Leak Attack [FKS16]



State Leak Attack [FKS16]



Experimental Evaluation

- Manual investigation of 30 RPs for each IdP from Alexa top 100K
- Analyzed both **authorization code mode** and **implicit mode** of OAuth 2.0

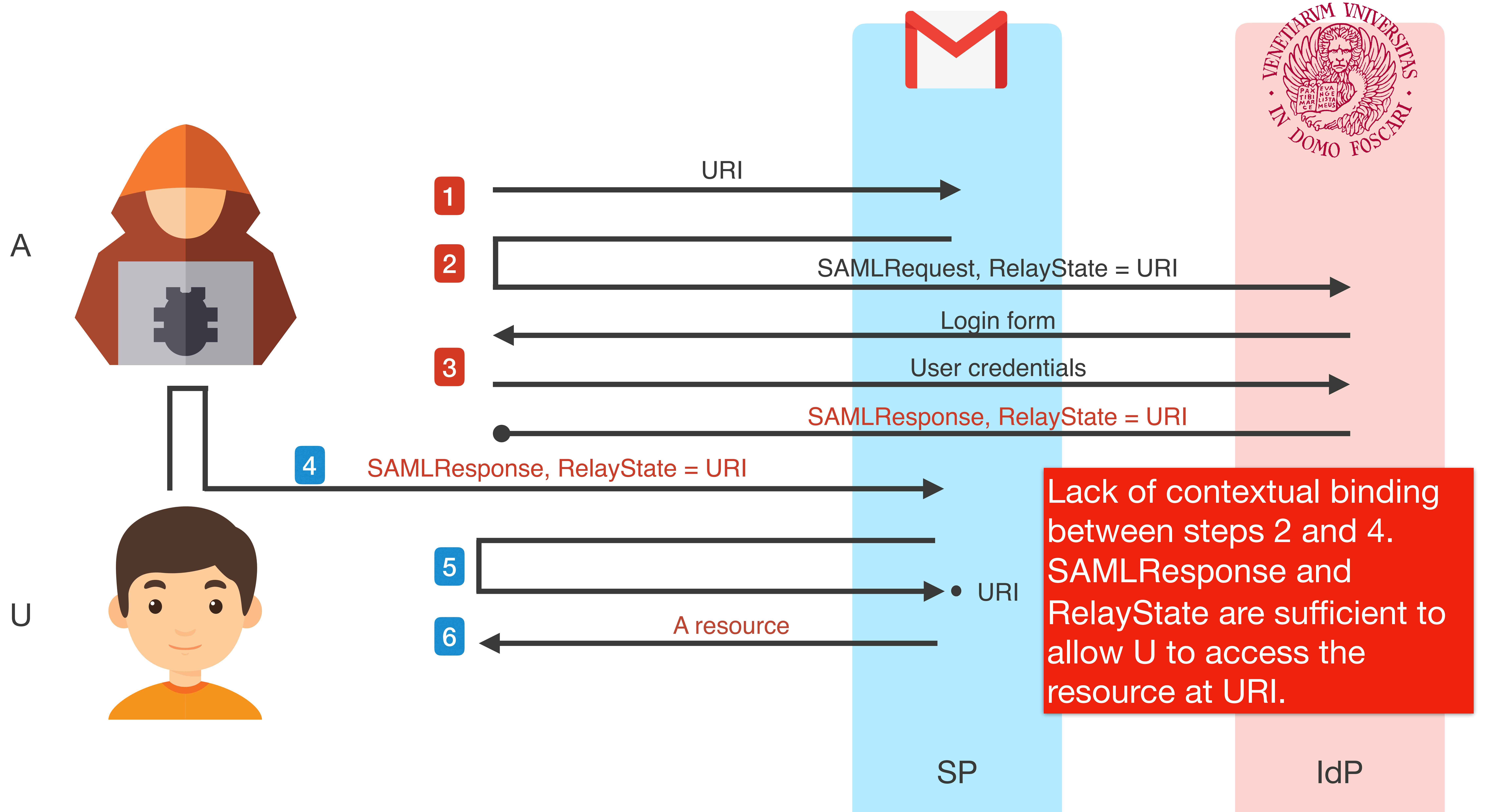
Security

- Leakage of sensitive data due to **tracking/ads libraries** (4 RPs)
- Lack or misuse of the **state parameter** (55 RPs)

Compatibility

Problems due to **security critical deviations** in the **protocol flow** (7 RPs), e.g. auth code is sent twice, second time over HTTP

Attacking Google Implementation of SAML 2.0



A
U
1
URI
2
SAMLRequest, RelayState = URI
Login form
3
User credentials
SAMLResponse, RelayState = URI
4
SAMLResponse, RelayState = URI
5
URI
6
A resource
SP
IdP
VENETIARVM UNIVERSITAS IN DOMO FOSCARI

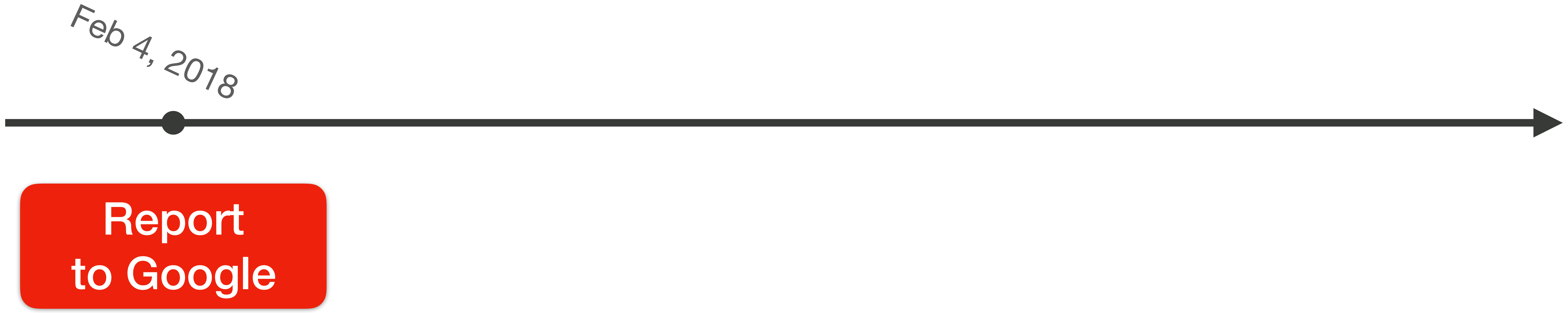
Lack of contextual binding between steps 2 and 4. SAMLResponse and RelayState are sufficient to allow U to access the resource at URI.

New Attack Against Google SAML 2.0

- Similar to the **session swapping** attack presented before
- **Login CSRF** against Google Suite applications (Drive, Gmail, Keep, …)

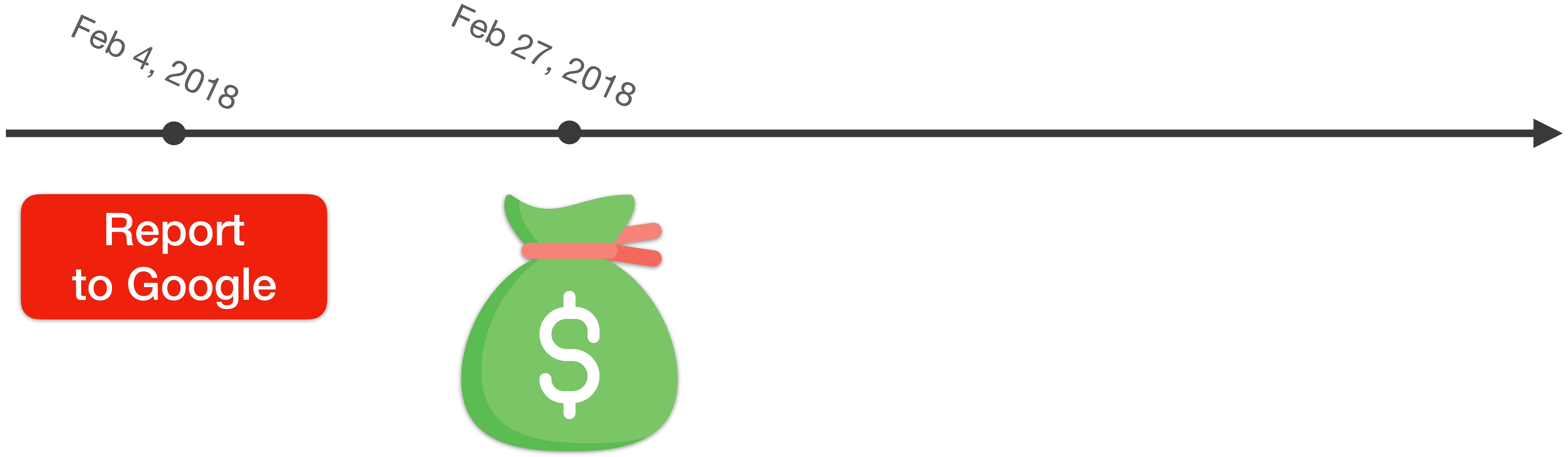
New Attack Against Google SAML 2.0

- Similar to the **session swapping** attack presented before
- **Login CSRF** against Google Suite applications (Drive, Gmail, Keep, …)



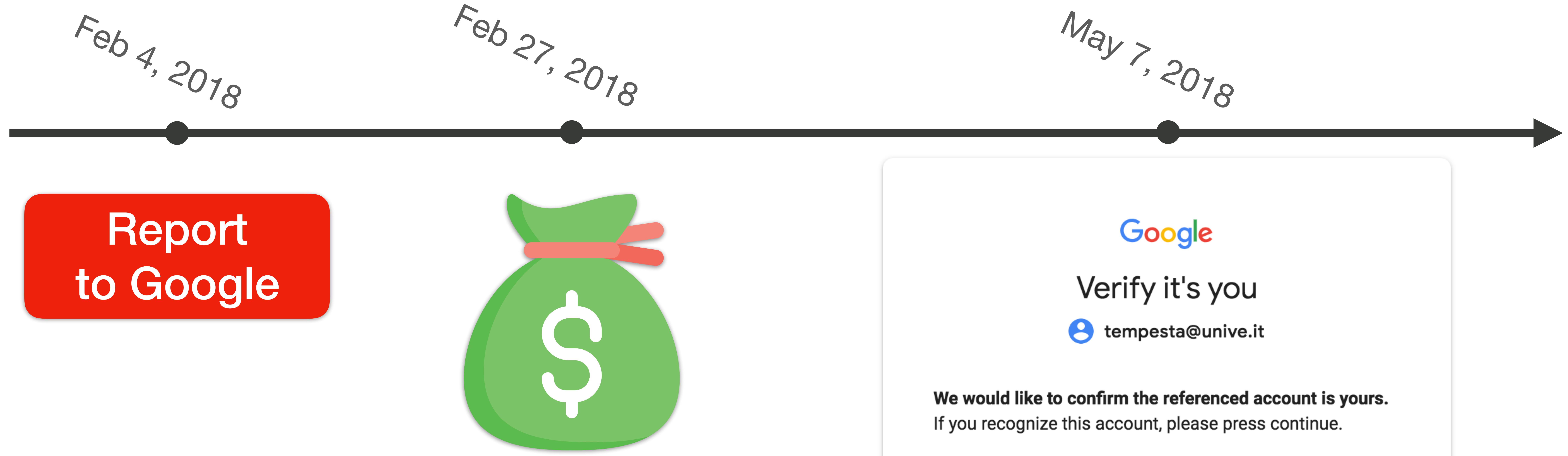
New Attack Against Google SAML 2.0

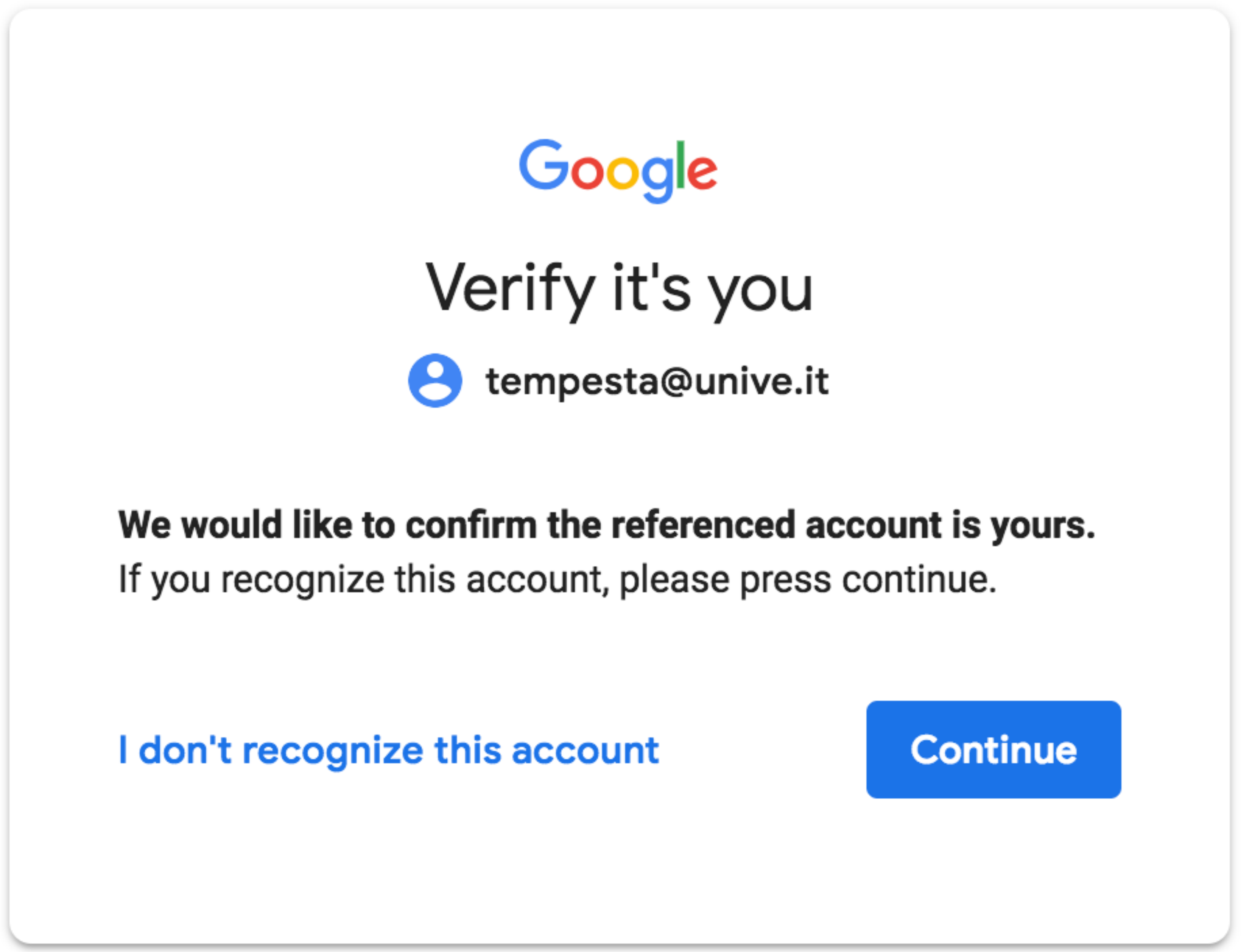
- Similar to the **session swapping** attack presented before
- **Login CSRF** against Google Suite applications (Drive, Gmail, Keep, …)



New Attack Against Google SAML 2.0

- Similar to the **session swapping** attack presented before
- **Login CSRF** against Google Suite applications (Drive, Gmail, Keep, …)




Google

Verify it's you

tempesta@unive.it

We would like to confirm the referenced account is yours.
If you recognize this account, please press continue.

I don't recognize this account — Continue

New Attack Against Google SAML 2.0

- Similar to the **session swapping** attack presented before
- **Login CSRF** against Google Suite applications (Drive, Gmail, Keep, …)

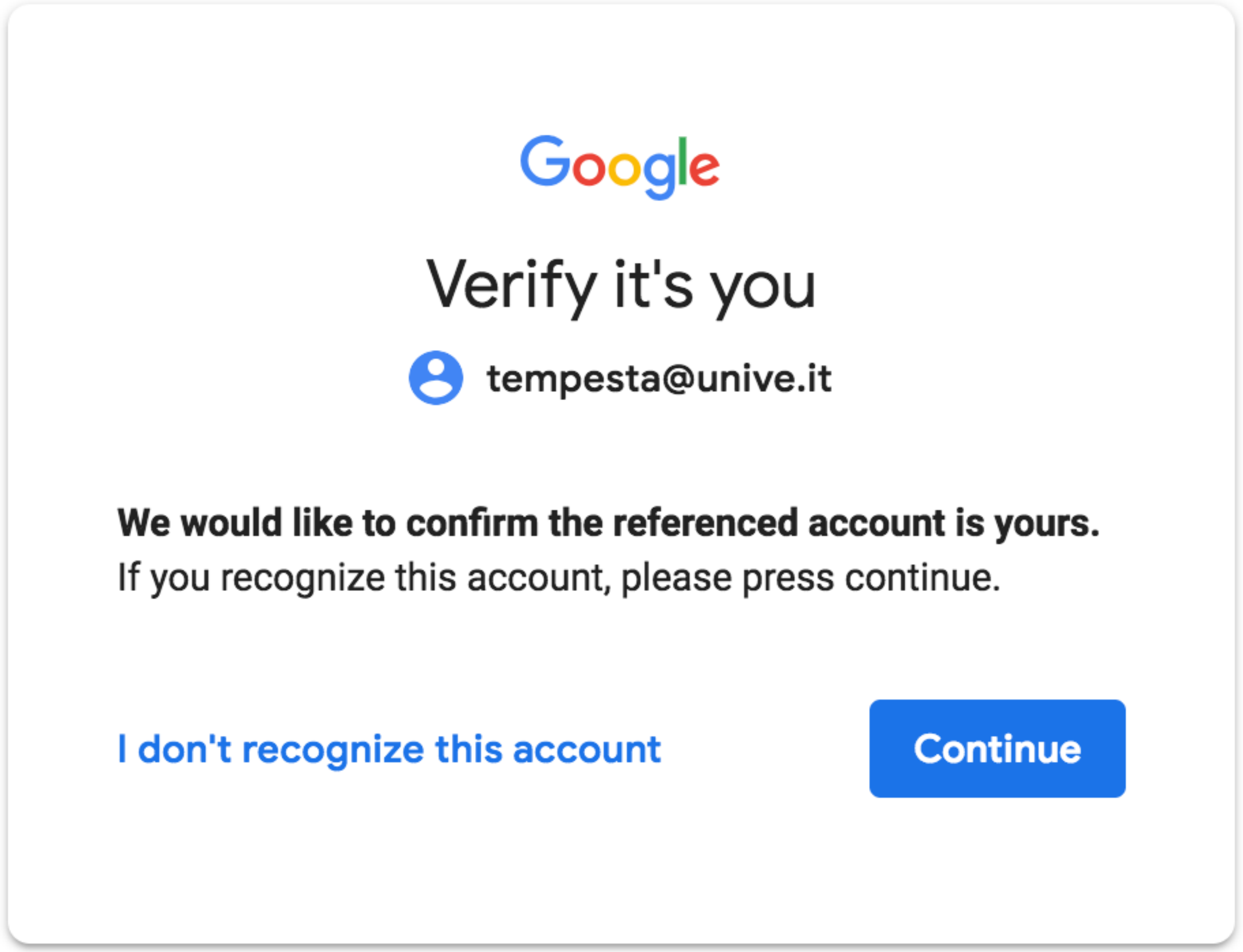
Feb 4, 2018

Feb 27, 2018

May 7, 2018

And now?

Report to Google



Google

Verify it's you

tempesta@unive.it

We would like to confirm the referenced account is yours.
If you recognize this account, please press continue.

Summing Up

Lightweight policies on the client-side suffice to enforce **provable security** guarantees in web protocols

SUMMING UP

Lightweight policies on the client-side suffice to enforce **provable security** guarantees in web protocols

- Support for additional protocols e.g., **e-payments**
- **Automatic** techniques to **synthesize WPSE policies** from protocol specifications / browser traffic
- Embed WPSE into real **browsers**

Thank You!

Q&A

@blueminimal

marco.squarcina@tuwien.ac.at

https://sites.google.com/site/wpseproject/