Slack plugin pre podporu vedenia záverečných prác

Weiwei Chen

Školiteľ: RNDr. Richard Ostertág, PhD.

Problematika

- Zosúladiť pravidelné týždenné stretávanie vedúceho práce so študentami je niekedy ťažké. Preto môže byť zaujímavé prejsť na stretávanie sa v „elektronickej podobe“ cez komunikačnú platformu Slack.
- Prehľad práce
  - 1) Slack App – Komunikácia medzi Slackom a Slack aplikaciou
  - 2) Webové stránky – Manažovanie systému a zobrazovanie reporty

Slack

- Prvé spustenie Slacku bolo v auguste 2013.
- Komunikačná platforma
- Messenger
- Kanály (súkromný a verejný)
- Multiplatformový softvér (Win, MacOS, Linux, IOS, Andriod, Web)

Slack API

Web APIs

- Posielanie a odoslanie správ, ...

Events APIs

- Notifikácie udalosti

Real-Time konverzácia

OAuth access token

- URL Handshake

Správy v formáte JSON


```
{
    "token": "YOUR_TOKEN_HERE",
    "team_id":"TPSGXX6X2",
    "api_app_id":"APWXEVX7",
    "event":{
        "client_msg_id": "37fe19d9-8eaa-418d-90x8-fa3ce001c63x"
        "type": "message",
        "text": "hi",
        "user": "UPX2012XA",
        "ts": "1573676189.015010",
        "team": "TPSXXX6H2",
        "channel": "DPYMLX898",
        "event_ts": "153676259.0150010",
        "channel_type": "im"
    },
    "type": "event_callback",
    "event_id": "EvQh112XUA0",
    "event_time": 1573654189,
    "authed_users":[
        "UQ9RBLGB7"
    ]

}
```

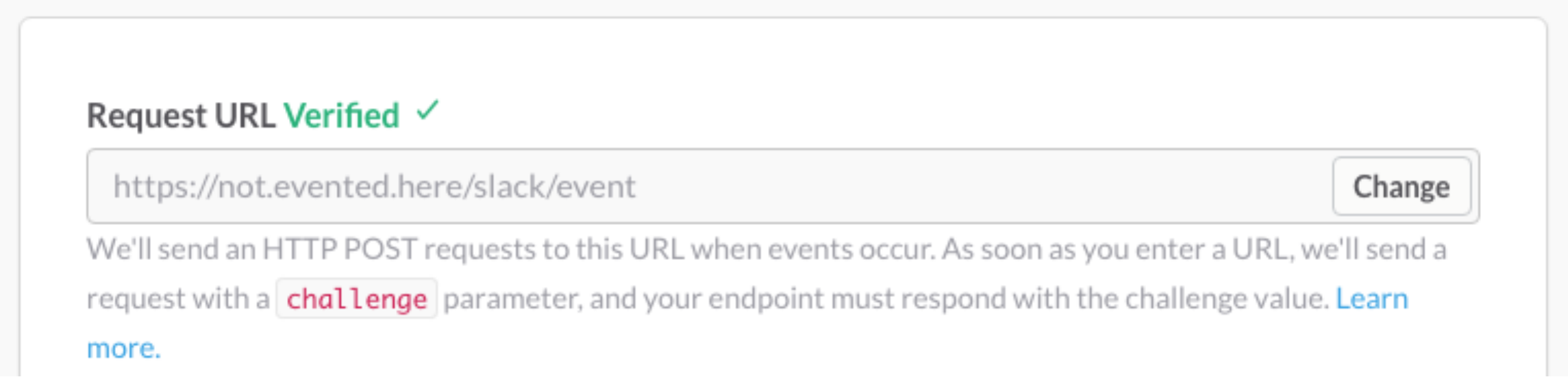
URL Handshake

From Slack to application:

```
HTTP 200 OK Content-type: application/x-www-form-urlencoded
challenge=3eZbrw1aBm2rZgRNFdxV2595E9CY3gmdALWMmHkvFXO7tYXAYM8P
```

Expected from application:

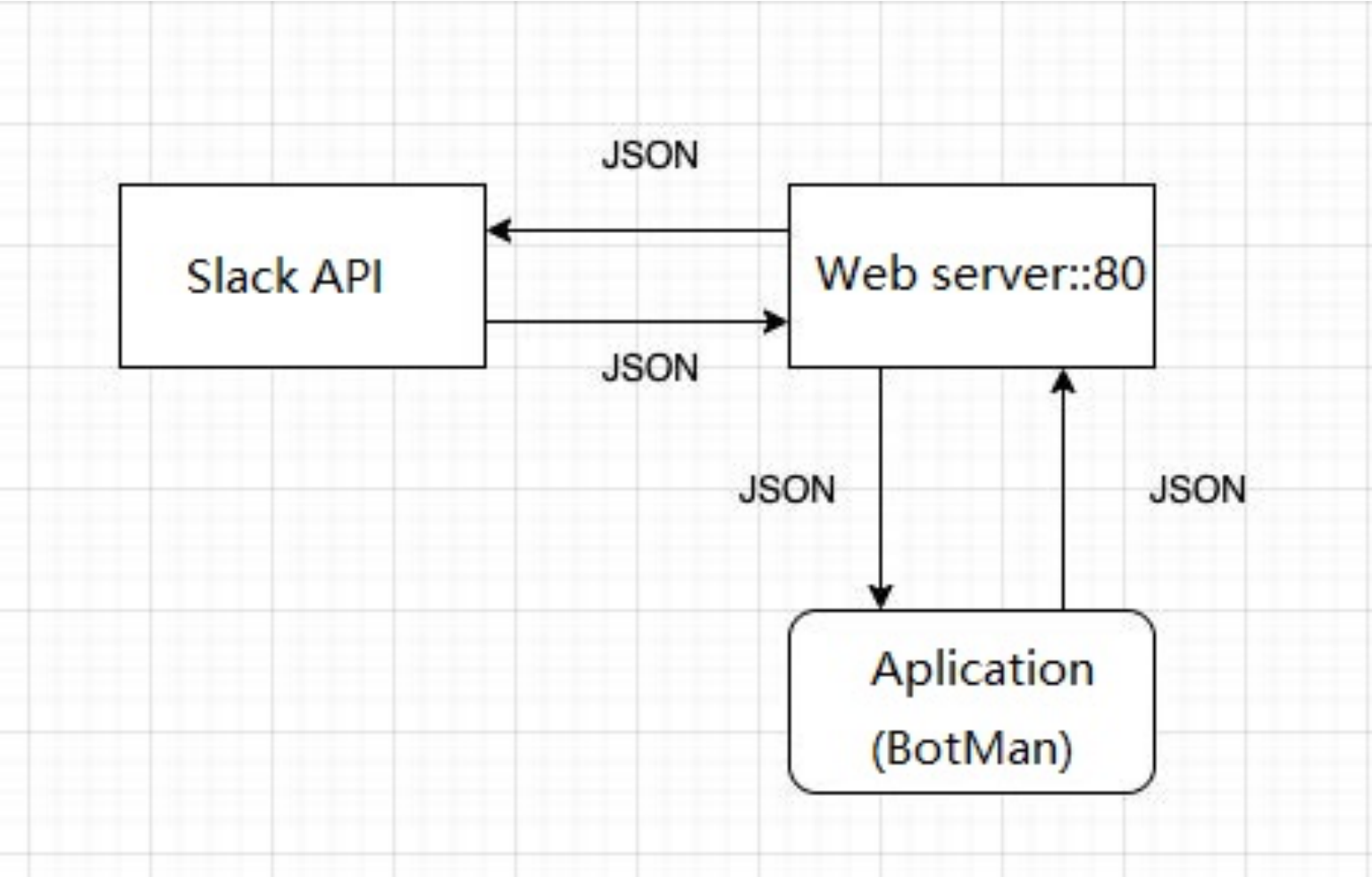
```
HTTP 200 OK Content-type: application/json
{"challenge":"3eZbrw1aBm2rZgRNFdxV2595E9CY3gmdALWMmHkvFXO7tYXAYM8P"}
```

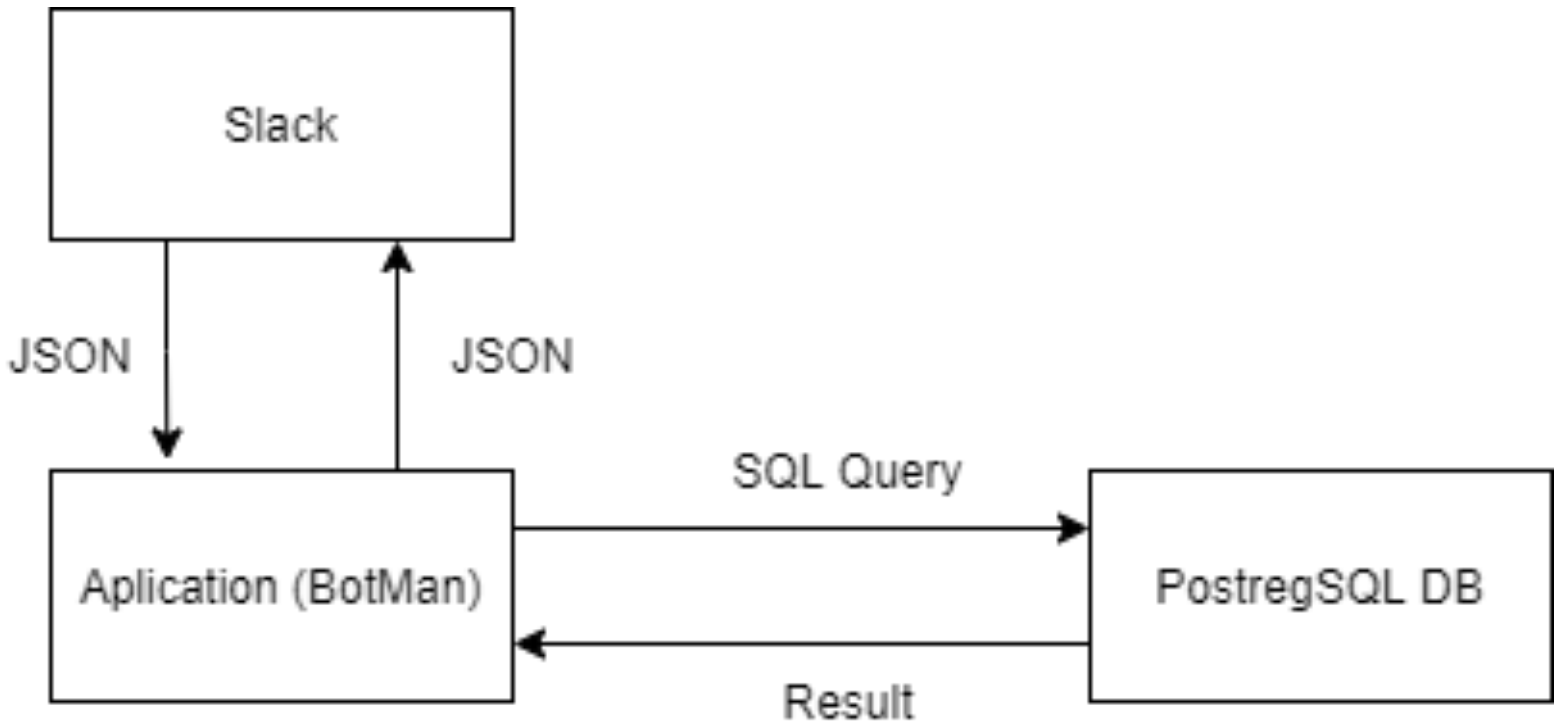


Slack App

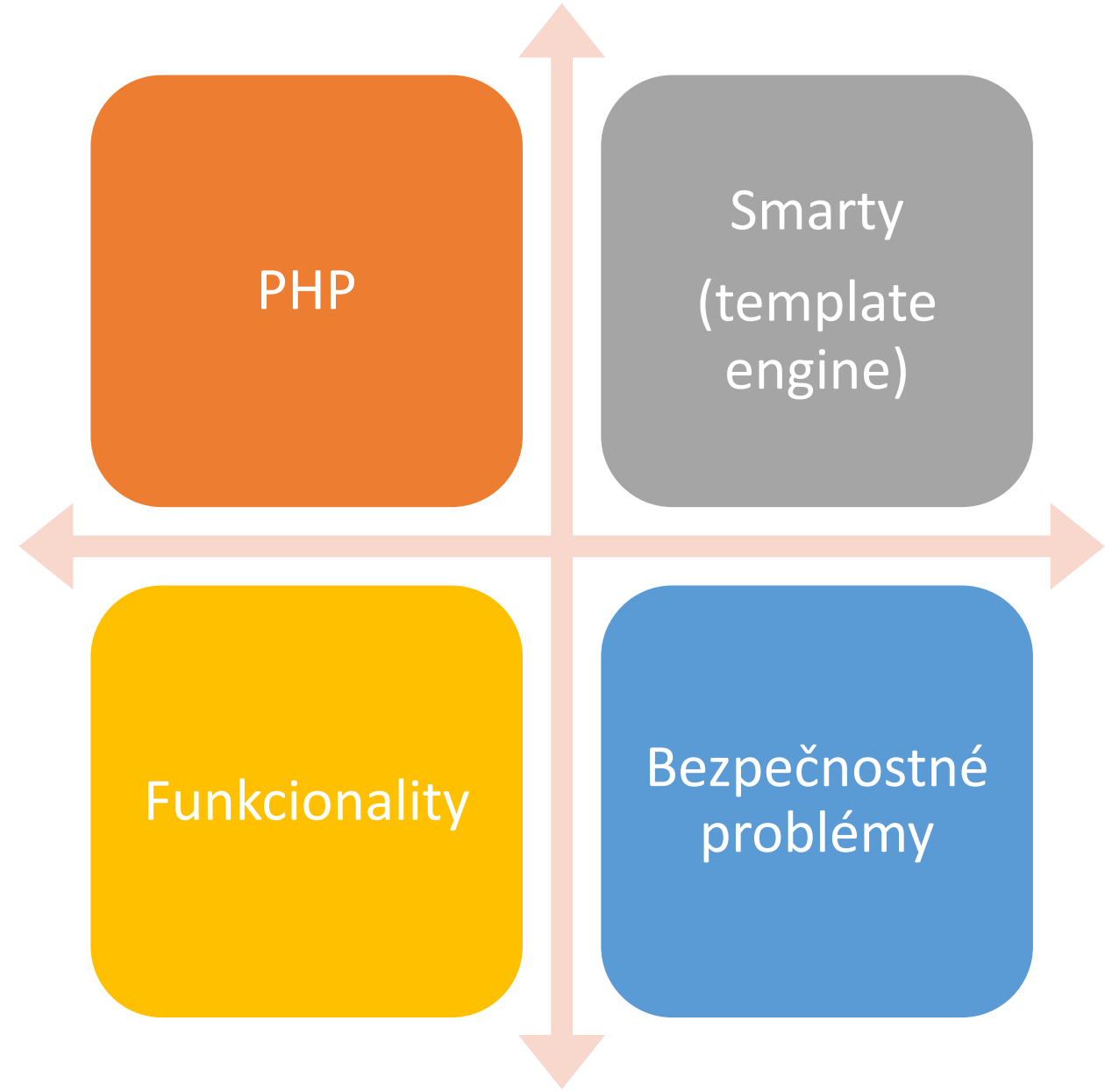
- Bot - Bot user
- BotMan (PHP Framework)
- Funkcionality
  - Základné otázky (robil som, budem robiť, mám problém)
  - Automatické posielanie správ (Cron job alebo Task Scheduler)
  - Periodické reporty
  - Úprava odpovedaných otázok
  - Oneskorenie siete (Network delay)
- Ukladanie informácie do DB
- Bezpečnosť (OAuth token)

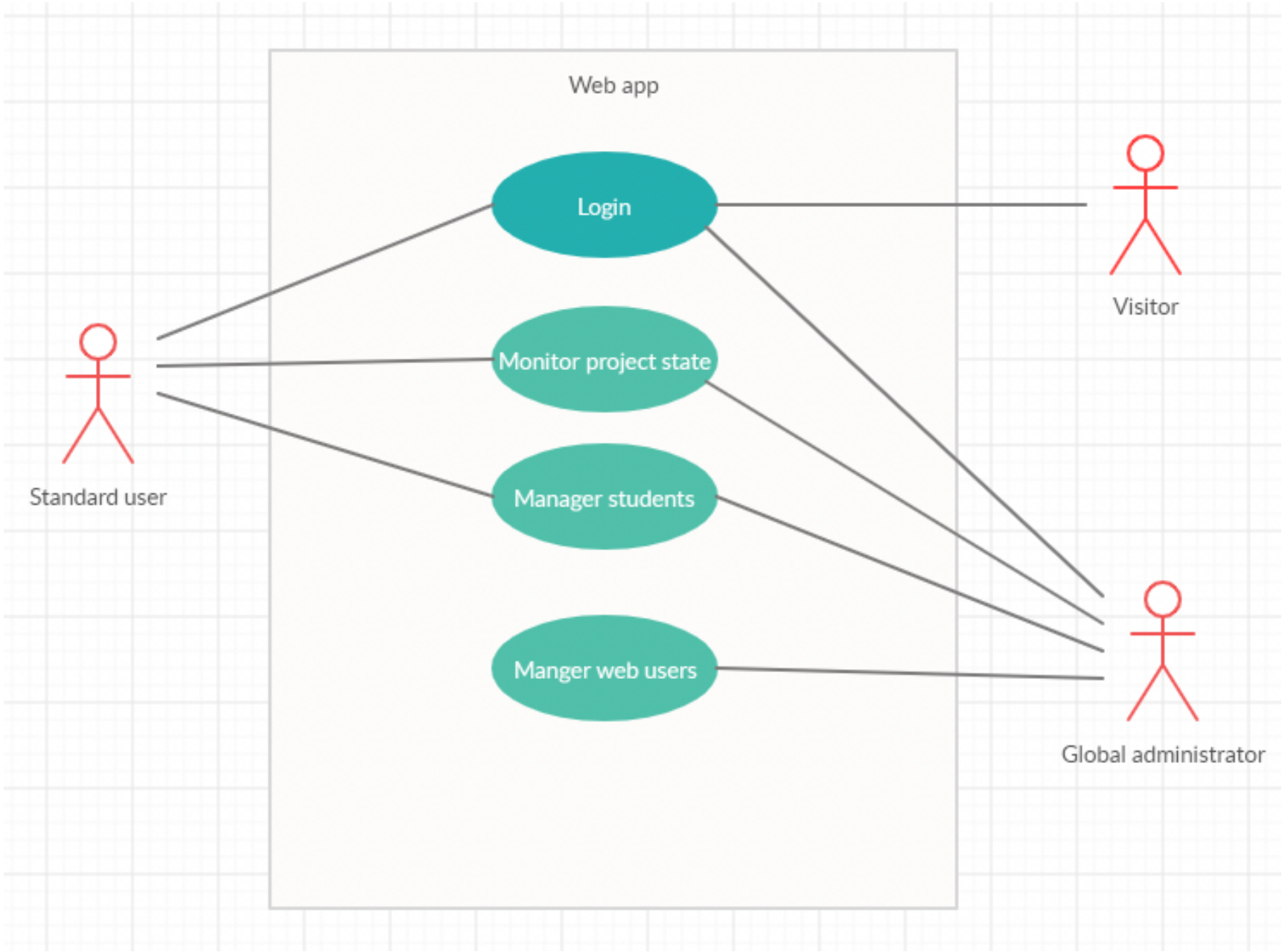
Komunikácia medzi Slackom API a aplikáciou




Slack
JSON
JSON
SQL Query
Aplication (BotMan)
PostregSQL DB
Result

Webové stránky




Web app
Login
Monitor project state
Manager students
Manger web users
Standard user
Visitor
Global administrator

Bezpečnosť webovej stránky

- Injection – JS, SQL, ...
  - Kontrola vstupných dát na strane klienta aj na strane servera
- Hijaking – MITM, Session fixed, ...
  - HTTPS
  - Aktualizácia session identifikátor po prihlásenia
- Heslo – Slabé heslo, únik databázy
  - salt

MS bot Framework

- MS Teams
- Skype
- Pripadne iné platformy, napr. Facebook Messenger, HipChat, Telegram, ...

Otázky

- **Strana 30:**
- *Pre riešenie toho útoku server po niekoľkých neúspešných pokusoch prihlásenie môže používateľovi zamietnuť prihlásenie do systému na určitý čas, aby útočník nemohol preťažiť server a rýchlo testovať heslo podľa slovníku.*
- Implementuje Vaše riešenie niečo takéto? Ak nie, viete nám povedať, ako by ste niečo takéto implementovali?
- **Súbor web\temp.php a commands\help\index.php:**
- Kde vo Vašej aplikácii používate tieto časti programu a aký je ich účel?

Otázky

- **1)** Skúste vybrať a popišať jednu časť vašej implementácie, ku ktorej ste museli najdlhšie hľadať správne riešenie a ktorou by ste sa chceli pochváliť.
- **2)** Skúste vysvetliť, prečo ste zvolili jednosmernú HTTP komunikáciu a nie obojsmernú cez WebSocket?

Zdroje

- https://api.slack.com/com
- https://botman.io/2.0/welcome
- https://www.smarty.net/docs/en/
- https://docs.microsoft.com/en-us/azure/bot-service/

Ďakujem za pozornosť.