

Aplikacje webowe

Bezpieczeństwo systemów komputerowych
semestr zimowy, 2020/21

Wstęp

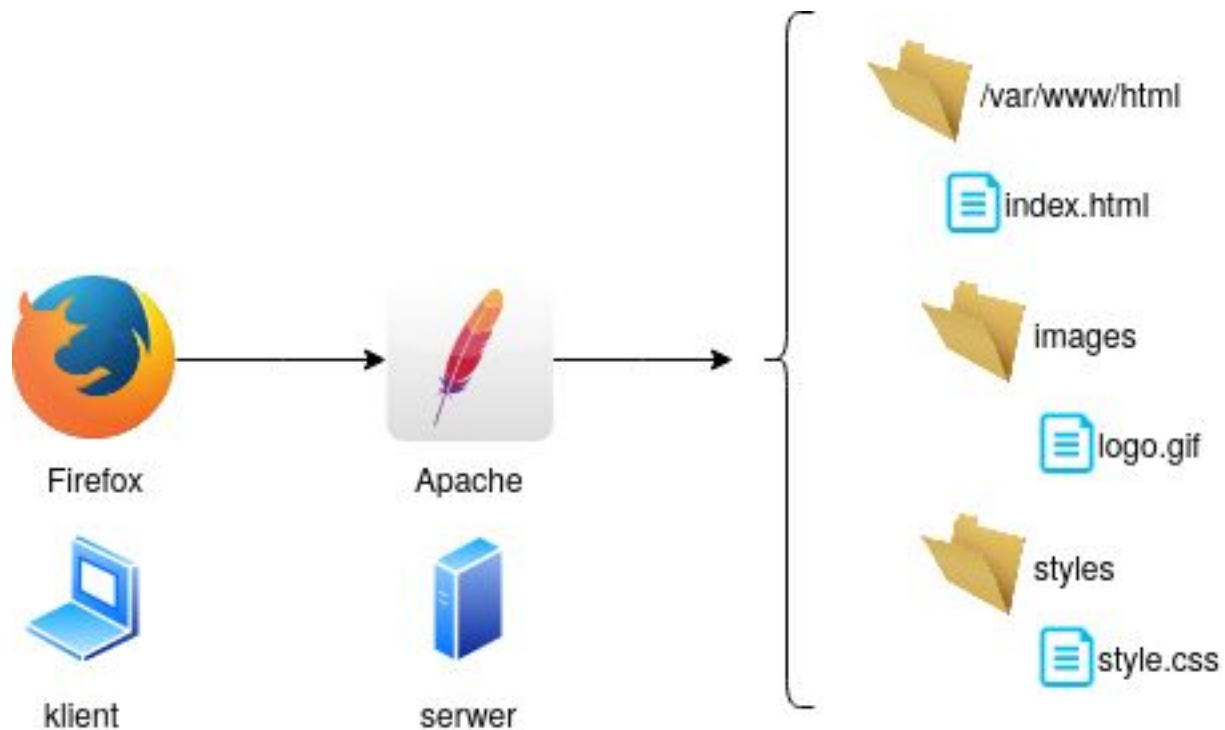
- Co będzie na zajęciach
 - co może pójść nie tak
 - techniki ataku
- Czego nie będzie na zajęciach
 - metodyk audytu i testów penetracyjnych aplikacji webowych

Formuła zajęć

Jakie będą zadania?

Co to jest flaga?

Część I - serwer WWW i pliki



Część I - serwer WWW i pliki

<http://bsk2020.kazet.cc:8001/>

Pliki na serwerze

- .git/, .svn/ ...
- /server-status/, /server-info/ ...
- .bash_history ...
- (wyprzedzając materiał) /health/, /admin/ ...

Część I - serwer WWW i pliki

<http://bsk2020.kazet.cc:8021/>

Dobra lista: <https://github.com/maurosoria/dirsearch/blob/master/db/dicc.txt>

Narzędzie: <https://github.com/maurosoria/dirsearch>

Jakie jest kryterium czy lista jest dobra.

Część I - serwer WWW i pliki

<http://bsk2020.kazet.cc:8002/>

(a tu już trochę trudniej)

Anegdota: pewien warszawski *Software House*

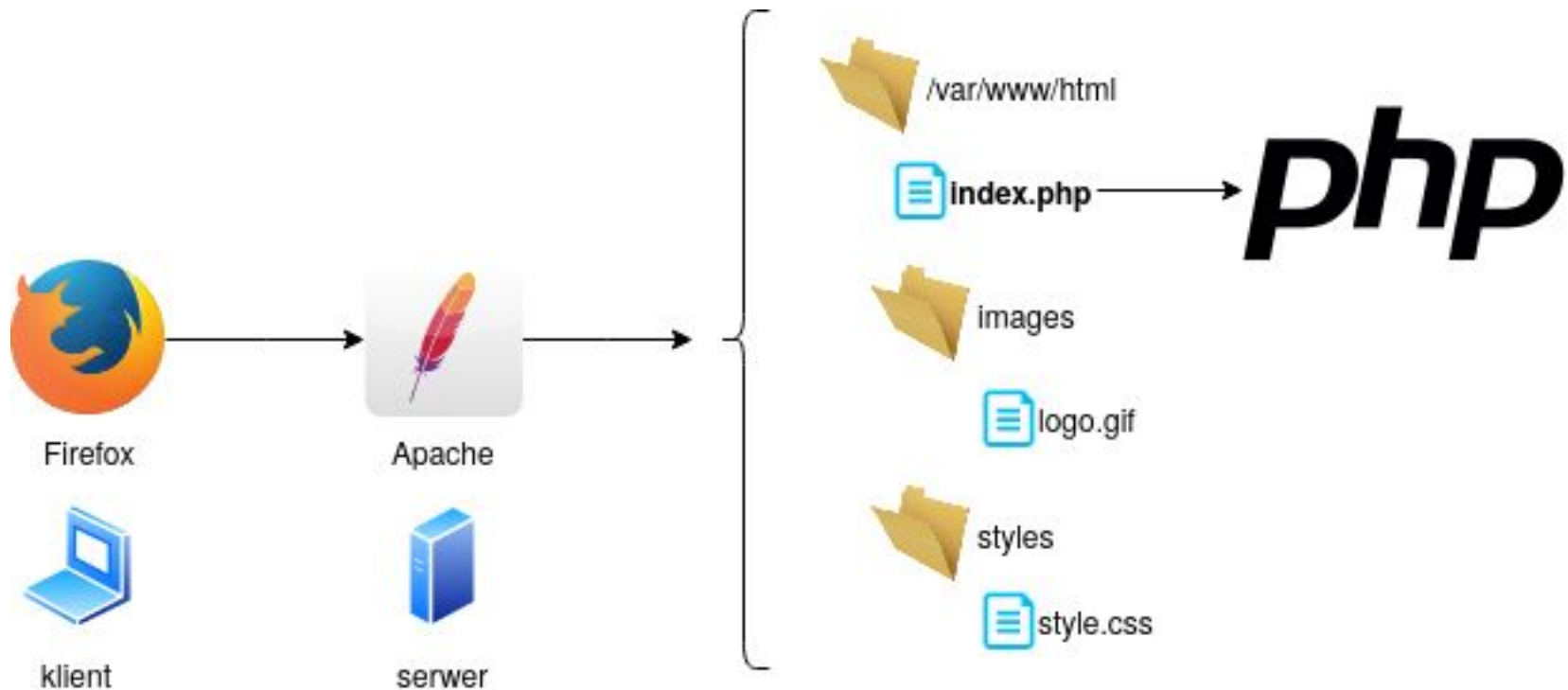
Co robić, jak żyć?

- jeśli udostępniać repozytorium Gita - to świadomie
- ogólnie: nie wrzucać sekretów
 - skanery: entropia / regexy

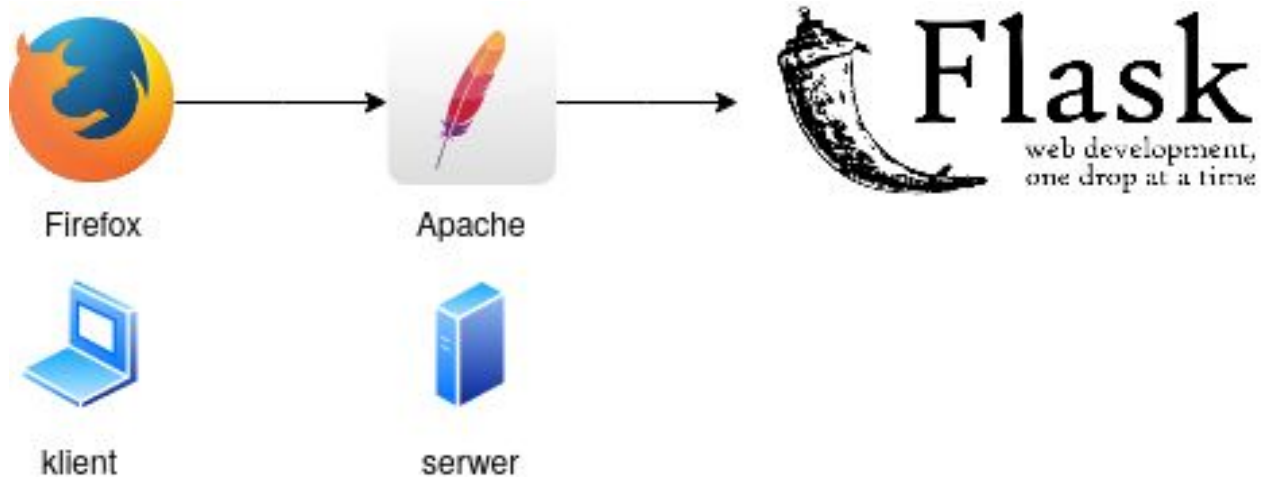
Zabezpieczenia po stronie klienta

<http://bsk2020.kazet.cc:8003/>

Część II - serwer WWW i aplikacja webowa



Część II - serwer WWW i aplikacja webowa



Zadanie 17 (wybaczcie dziwną kolejność)

<http://bsk2020.kazet.cc:8017/>

Zadanie 4

...

```
if (isset($_GET['id'])) {  
    echo(file_get_contents("content/" . $_GET["id"]));  
} else {  
    echo(file_get_contents("content/index"));  
}
```

...

<http://bsk2020.kazet.cc:8004/>

Zadanie 5

...

```
if (isset($_GET['id'])) {  
    echo(file_get_contents("content/" .  
        str_replace(' ../', '', $_GET['id'])));  
} else {  
    echo(file_get_contents("content/index"));  
}
```

...

<http://bsk2020.kazet.cc:8005/>