邏輯優化的灰色面
針對網頁應用的時序攻擊
（ Timing Attacks on Web ）

Ant
ant@chroot.org / yftzeng@gmail.com

2018-03-13

TAIWAN
CYBER SECURITY SUMMIT 2018
臺灣資安大會

Introduction

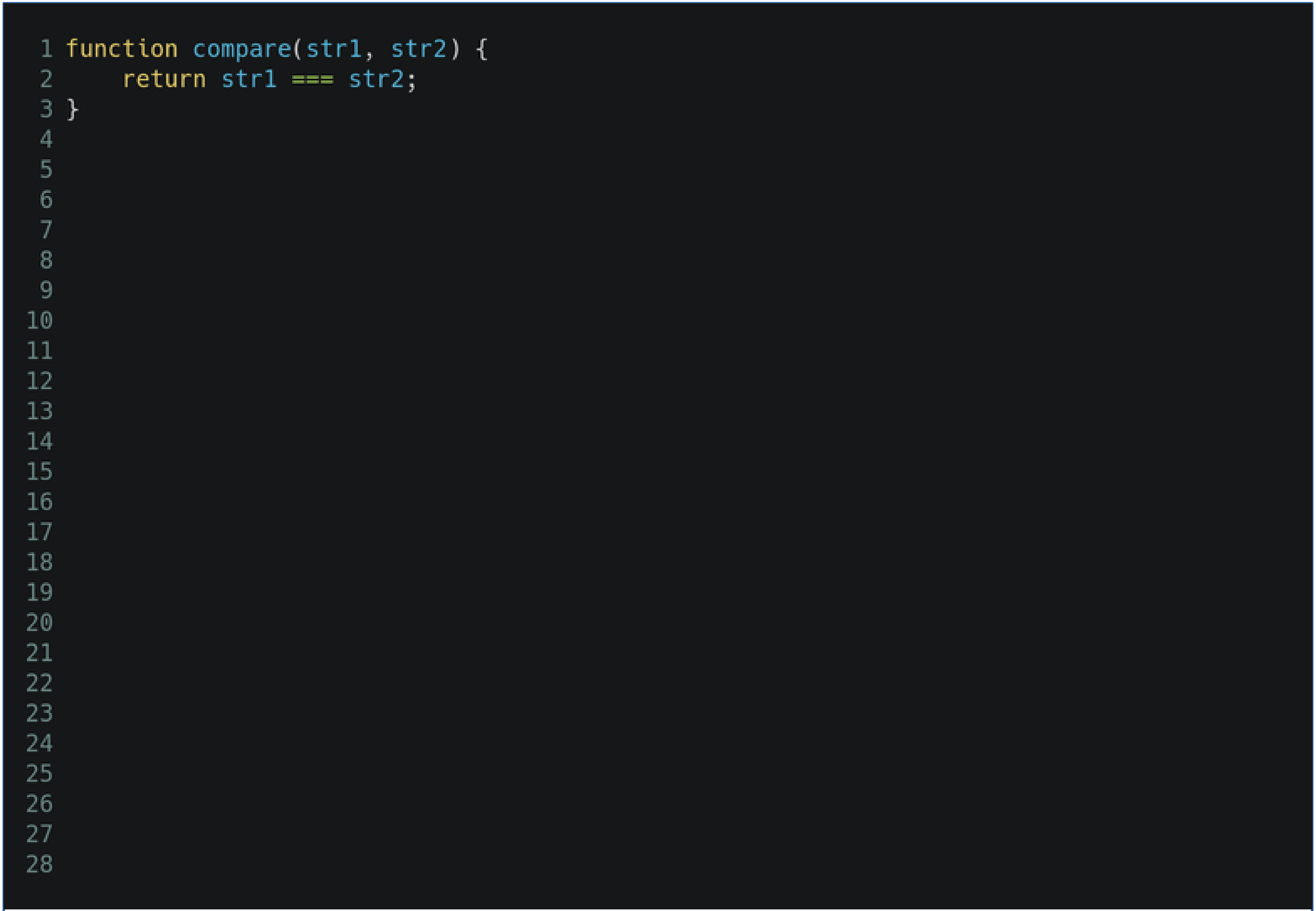
Coding • Security • Intellectual property • Startup

chroot

書亞集成
surasia

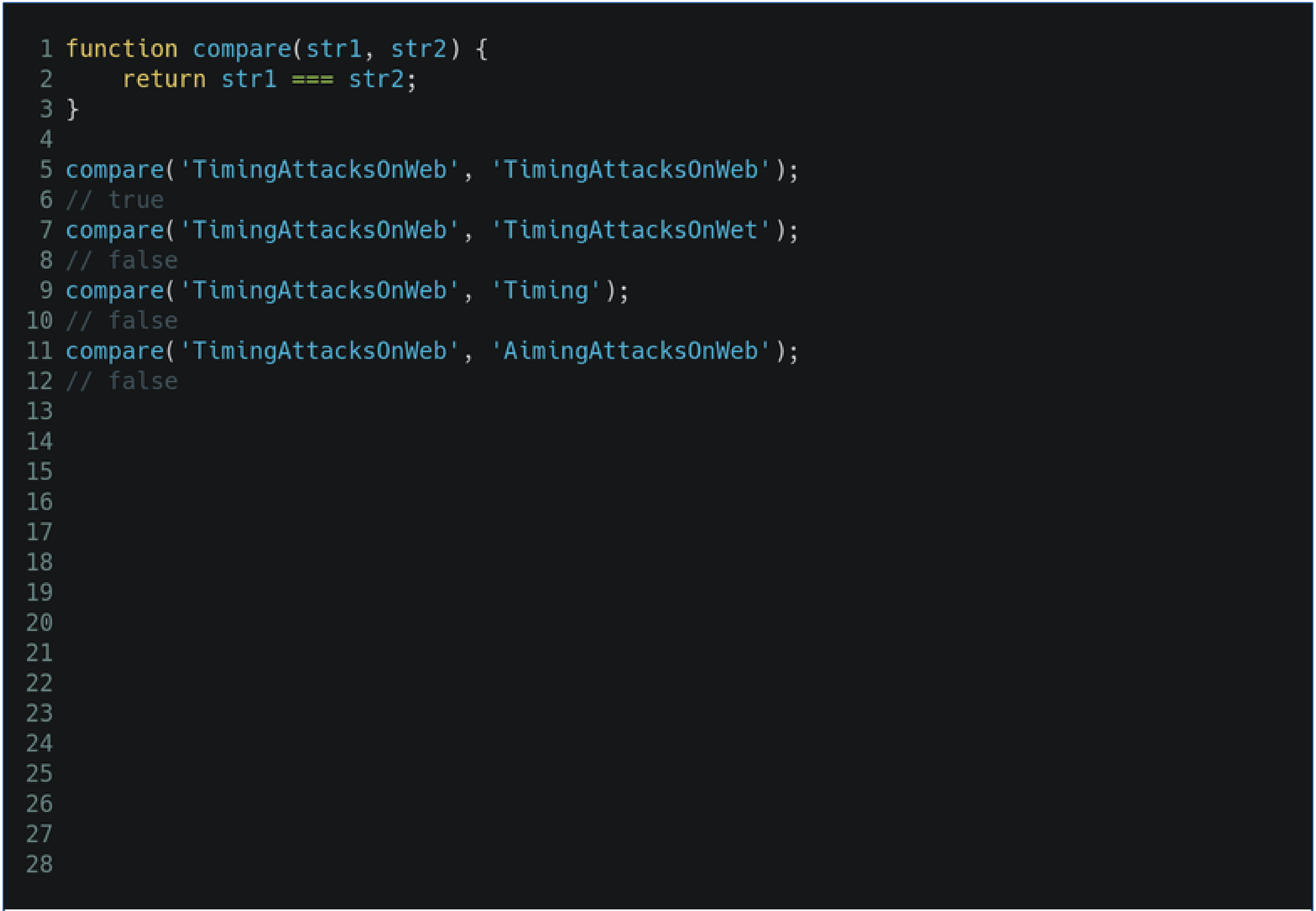
MUZiK ONLiNE

Thank @mathias for inspiring me



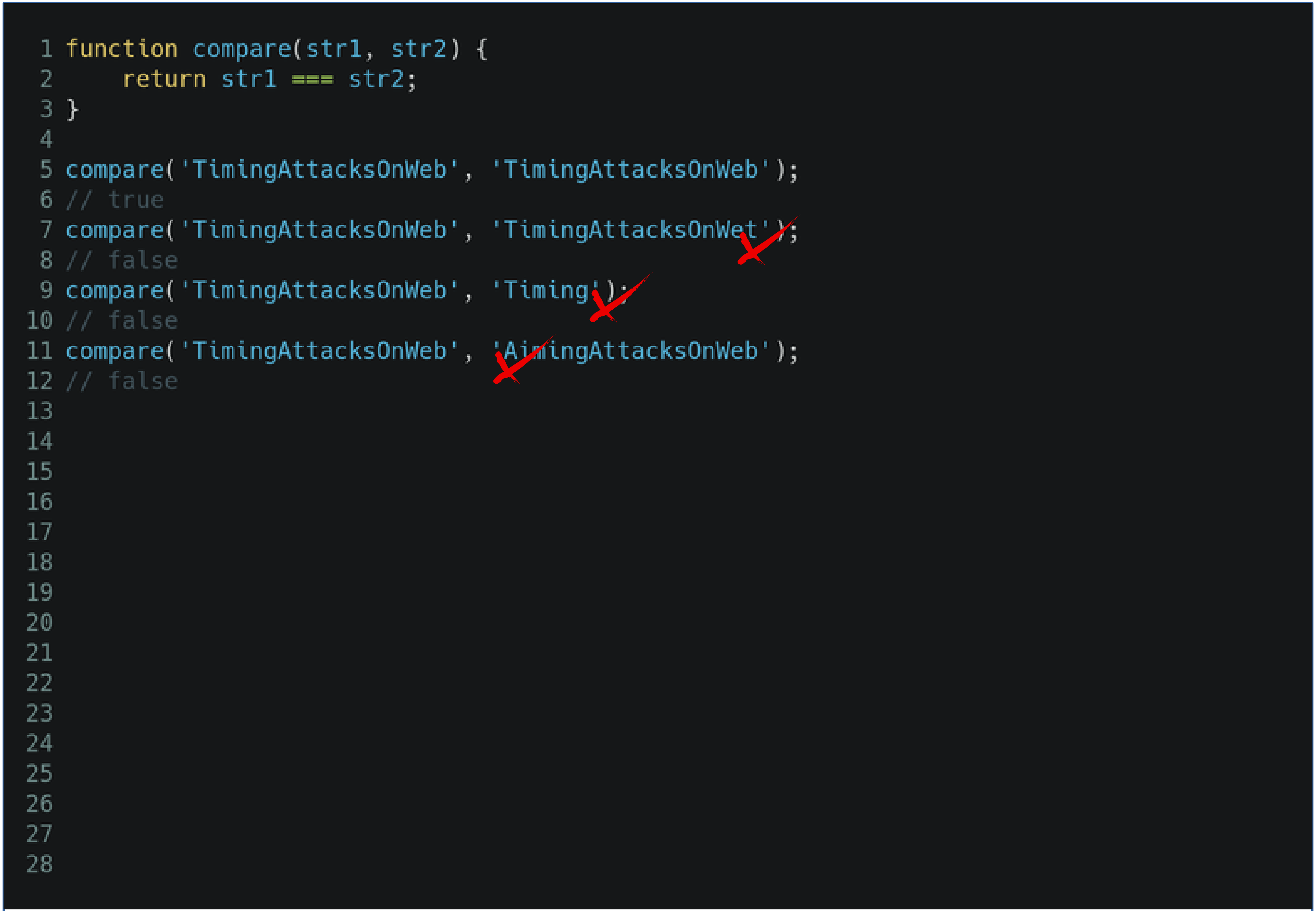
```
function compare(str1, str2) {
    return str1 === str2;
}
```

Ref: Front-End Performance The Dark Side @ ColdFront Conference 2016



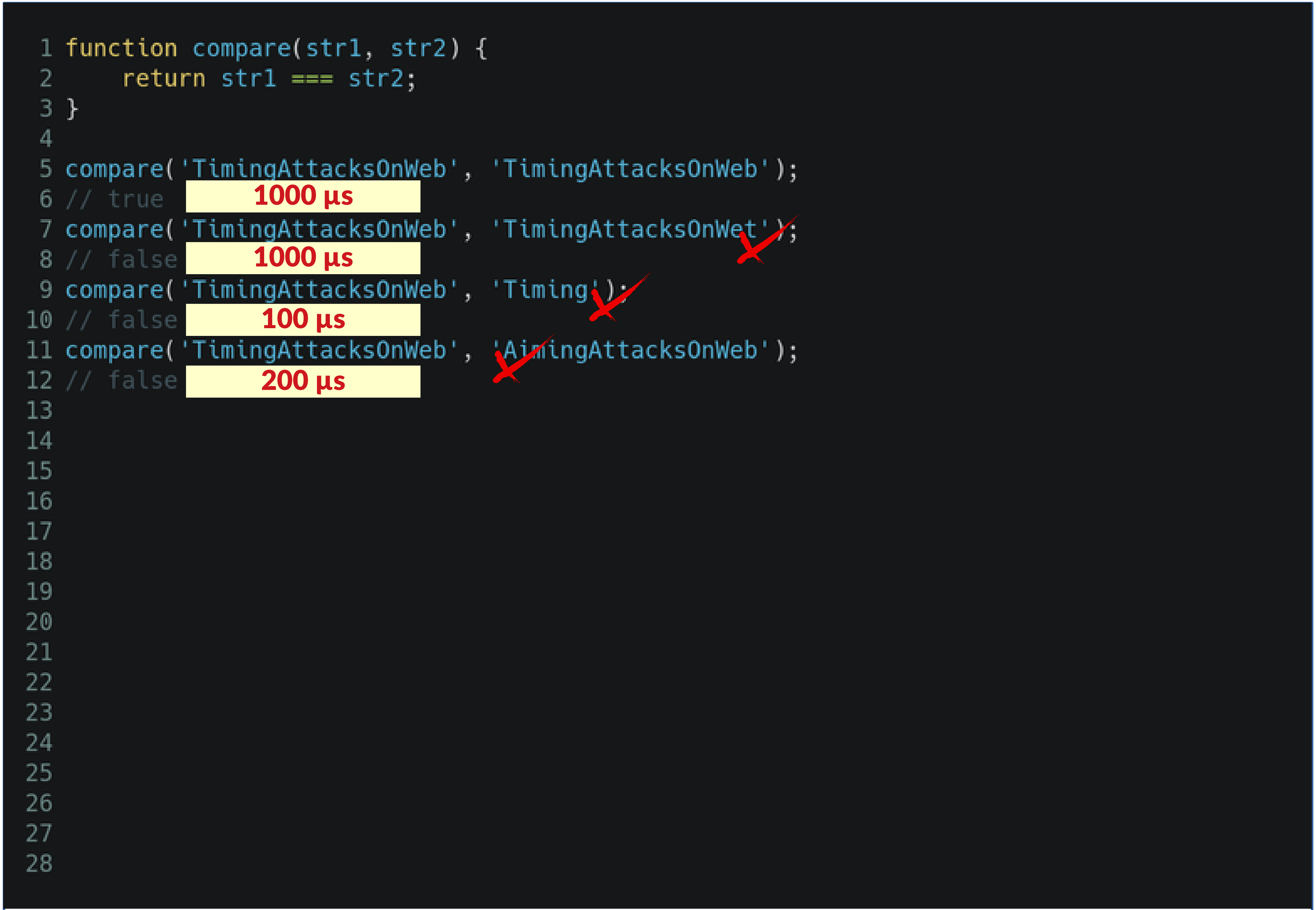
```
function compare(str1, str2) {
    return str1 === str2;
}

compare('TimingAttacksOnWeb', 'TimingAttacksOnWeb');
// true
compare('TimingAttacksOnWeb', 'TimingAttacksOnWet');
// false
compare('TimingAttacksOnWeb', 'Timing');
// false
compare('TimingAttacksOnWeb', 'AimingAttacksOnWeb');
// false
```

Ref: Front-End Performance The Dark Side @ ColdFront Conference 2016



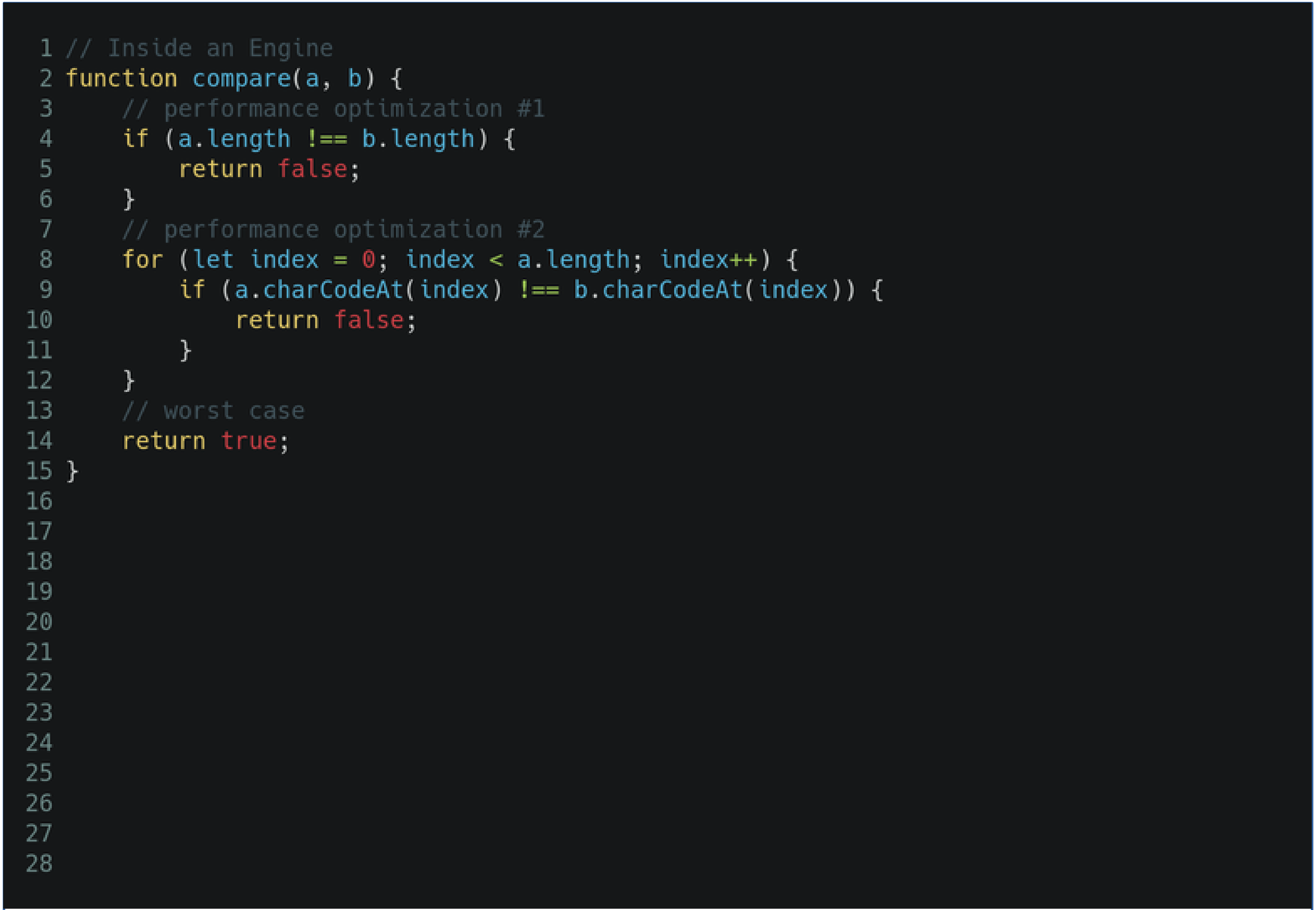
```javascript
function compare(str1, str2) {
    return str1 === str2;
}

compare('TimingAttacksOnWeb', 'TimingAttacksOnWeb');
// true
compare('TimingAttacksOnWeb', 'TimingAttacksOnWet');
// false
compare('TimingAttacksOnWeb', 'Timing');
// false
compare('TimingAttacksOnWeb', 'AimingAttacksOnWeb');
// false
```

Ref: Front-End Performance The Dark Side @ ColdFront Conference 2016



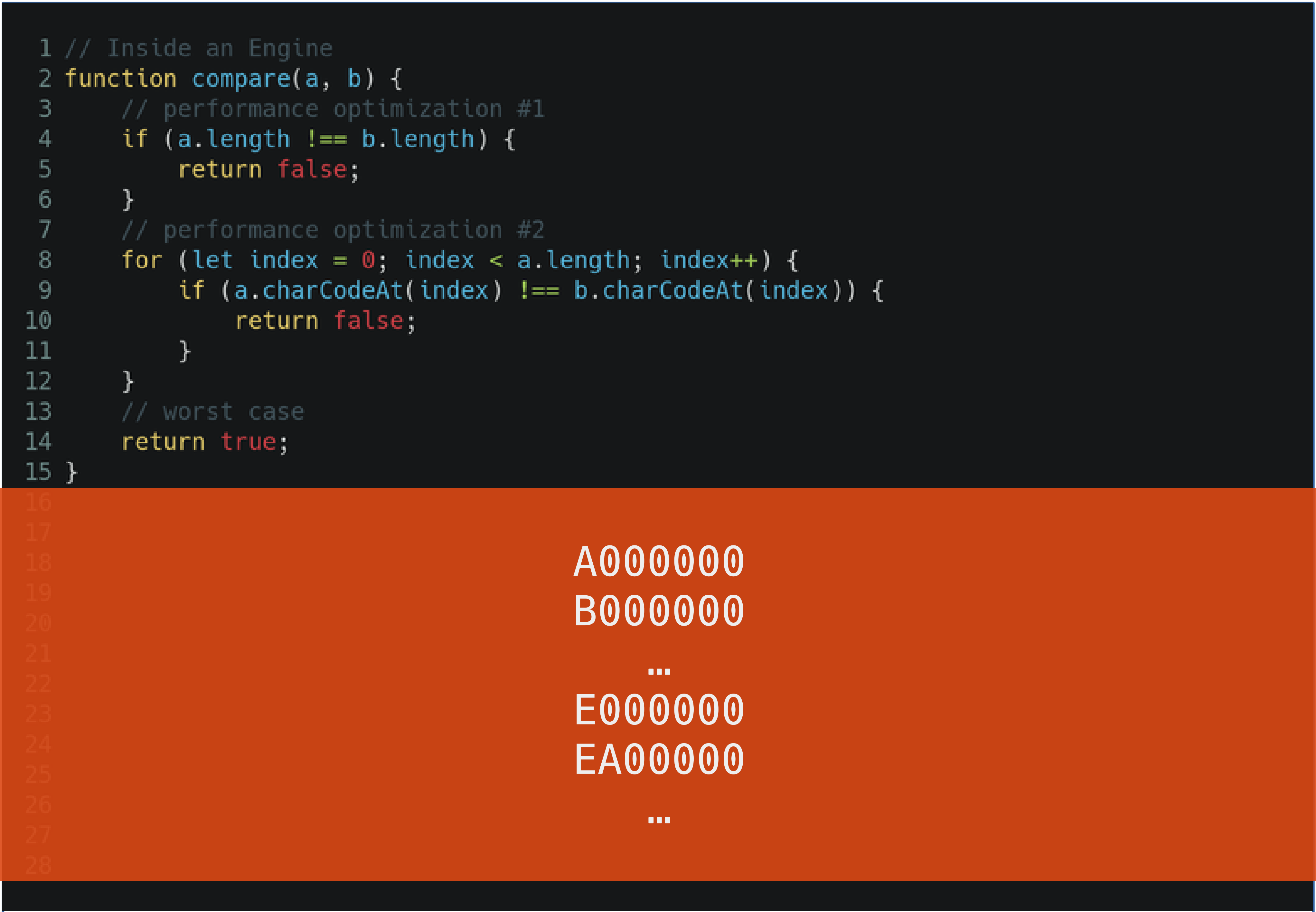
```
function compare(str1, str2) {
    return str1 === str2;
}

compare('TimingAttacksOnWeb', 'TimingAttacksOnWeb');
// true   1000 µs
compare('TimingAttacksOnWeb', 'TimingAttacksOnWet');
// false  1000 µs
compare('TimingAttacksOnWeb', 'Timing');
// false  100 µs
compare('TimingAttacksOnWeb', 'AimingAttacksOnWeb');
// false  200 µs
```

Ref: Front-End Performance The Dark Side @ ColdFront Conference 2016



```javascript
// Inside an Engine
function compare(a, b) {
    // performance optimization #1
    if (a.length !== b.length) {
        return false;
    }
    // performance optimization #2
    for (let index = 0; index < a.length; index++) {
        if (a.charCodeAt(index) !== b.charCodeAt(index)) {
            return false;
        }
    }
    // worst case
    return true;
}
```

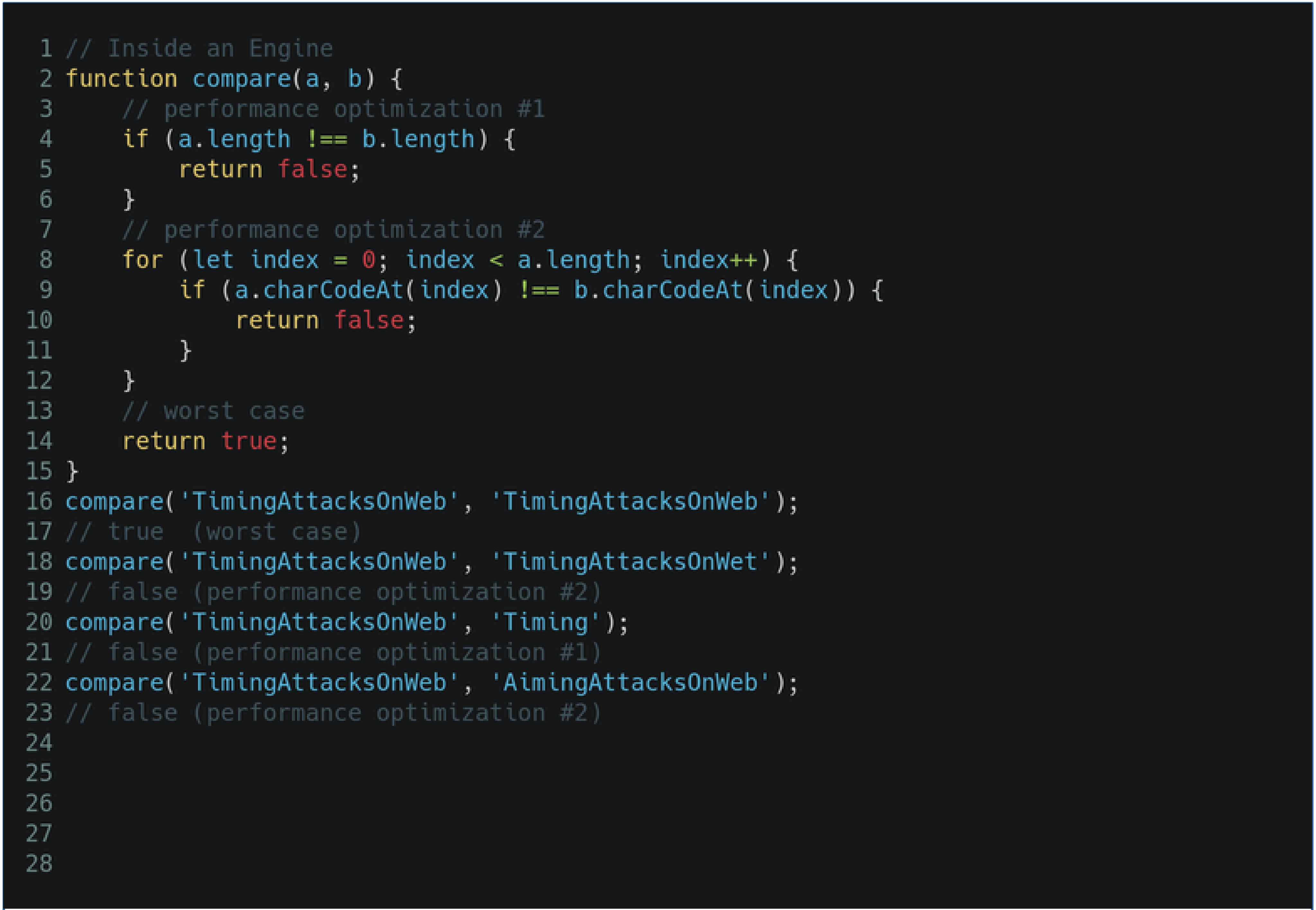
Ref: Front-End Performance The Dark Side @ ColdFront Conference 2016



```
// Inside an Engine
function compare(a, b) {
    // performance optimization #1
    if (a.length !== b.length) {
        return false;
    }
    // performance optimization #2
    for (let index = 0; index < a.length; index++) {
        if (a.charCodeAt(index) !== b.charCodeAt(index)) {
            return false;
        }
    }
    // worst case
    return true;
}
```

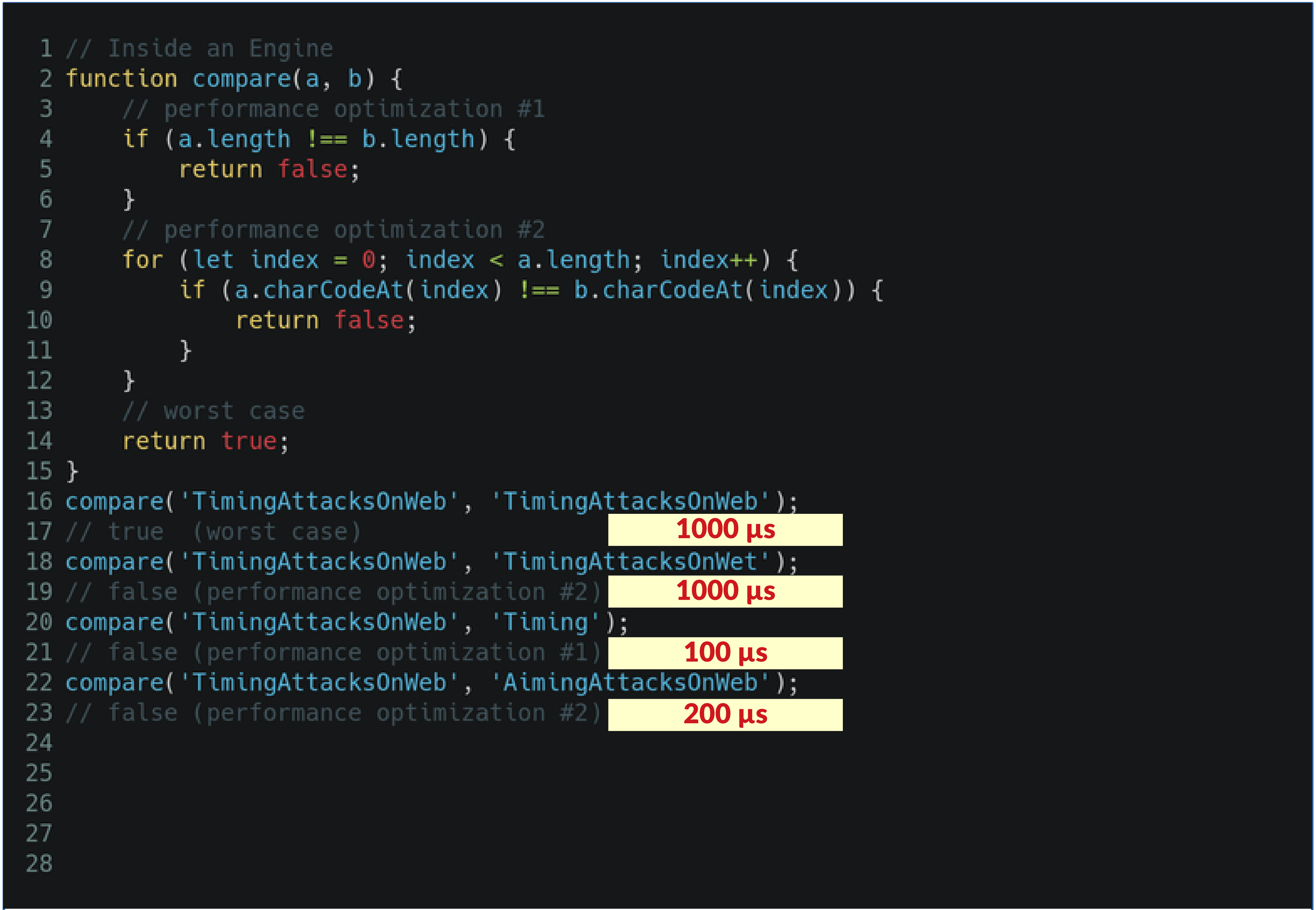
A000000
B000000
…
E000000
EA00000
…

Ref: Front-End Performance The Dark Side @ ColdFront Conference 2016



```
// Inside an Engine
function compare(a, b) {
    // performance optimization #1
    if (a.length !== b.length) {
        return false;
    }
    // performance optimization #2
    for (let index = 0; index < a.length; index++) {
        if (a.charCodeAt(index) !== b.charCodeAt(index)) {
            return false;
        }
    }
    // worst case
    return true;
}
compare('TimingAttacksOnWeb', 'TimingAttacksOnWeb');
// true  (worst case)
compare('TimingAttacksOnWeb', 'TimingAttacksOnWet');
// false (performance optimization #2)
compare('TimingAttacksOnWeb', 'Timing');
// false (performance optimization #1)
compare('TimingAttacksOnWeb', 'AimingAttacksOnWeb');
// false (performance optimization #2)
```

Ref: Front-End Performance The Dark Side @ ColdFront Conference 2016



```
// Inside an Engine
function compare(a, b) {
    // performance optimization #1
    if (a.length !== b.length) {
        return false;
    }
    // performance optimization #2
    for (let index = 0; index < a.length; index++) {
        if (a.charCodeAt(index) !== b.charCodeAt(index)) {
            return false;
        }
    }
    // worst case
    return true;
}
compare('TimingAttacksOnWeb', 'TimingAttacksOnWeb');
// true  (worst case)                      1000 µs
compare('TimingAttacksOnWeb', 'TimingAttacksOnWet');
// false (performance optimization #2)     1000 µs
compare('TimingAttacksOnWeb', 'Timing');
// false (performance optimization #1)     100 µs
compare('TimingAttacksOnWeb', 'AimingAttacksOnWeb');
// false (performance optimization #2)     200 µs
```

Ref: Front-End Performance The Dark Side @ ColdFront Conference 2016

a little bit

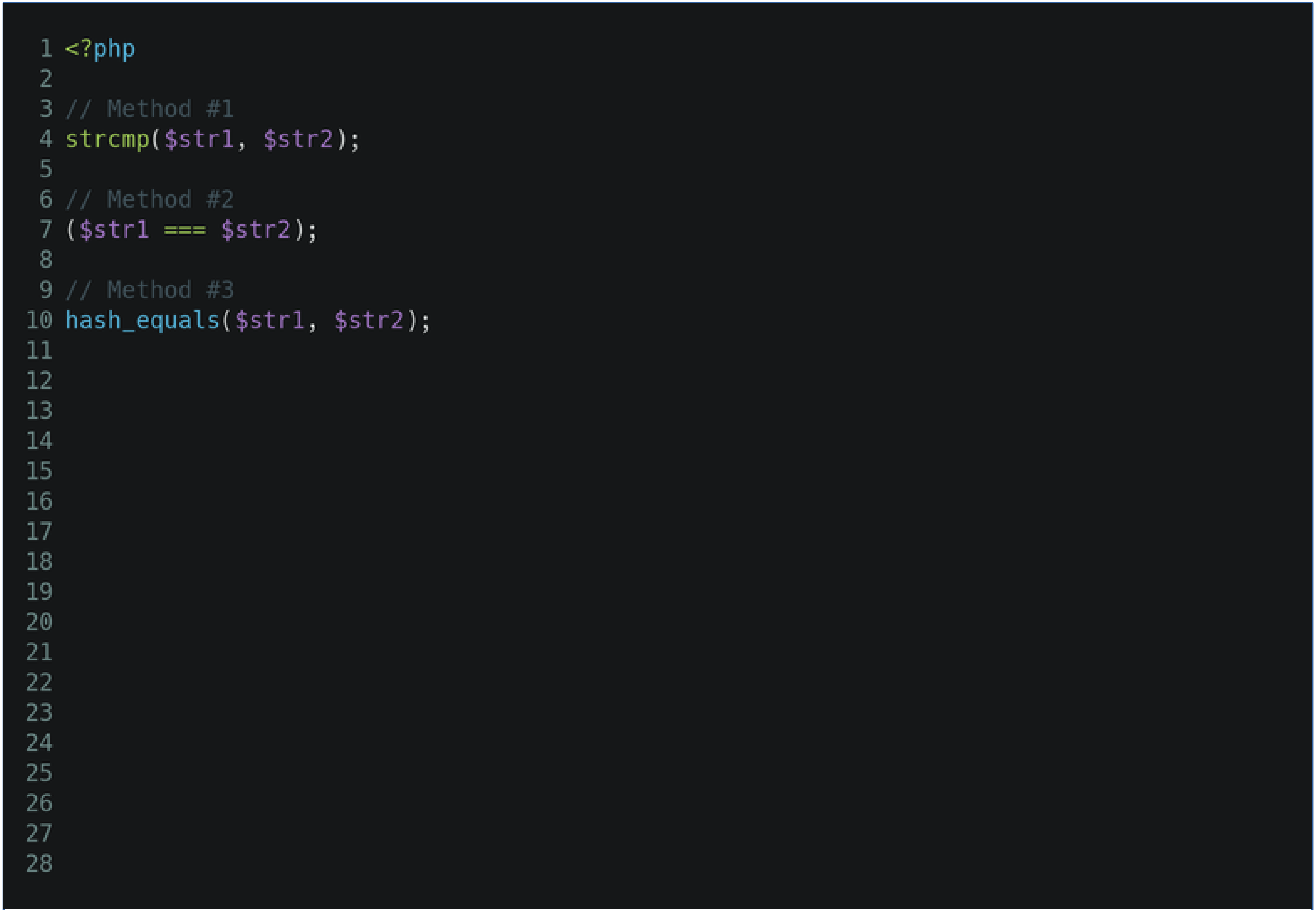
Premature optimization is the root of all evil

(過早最佳化是萬惡的根源)

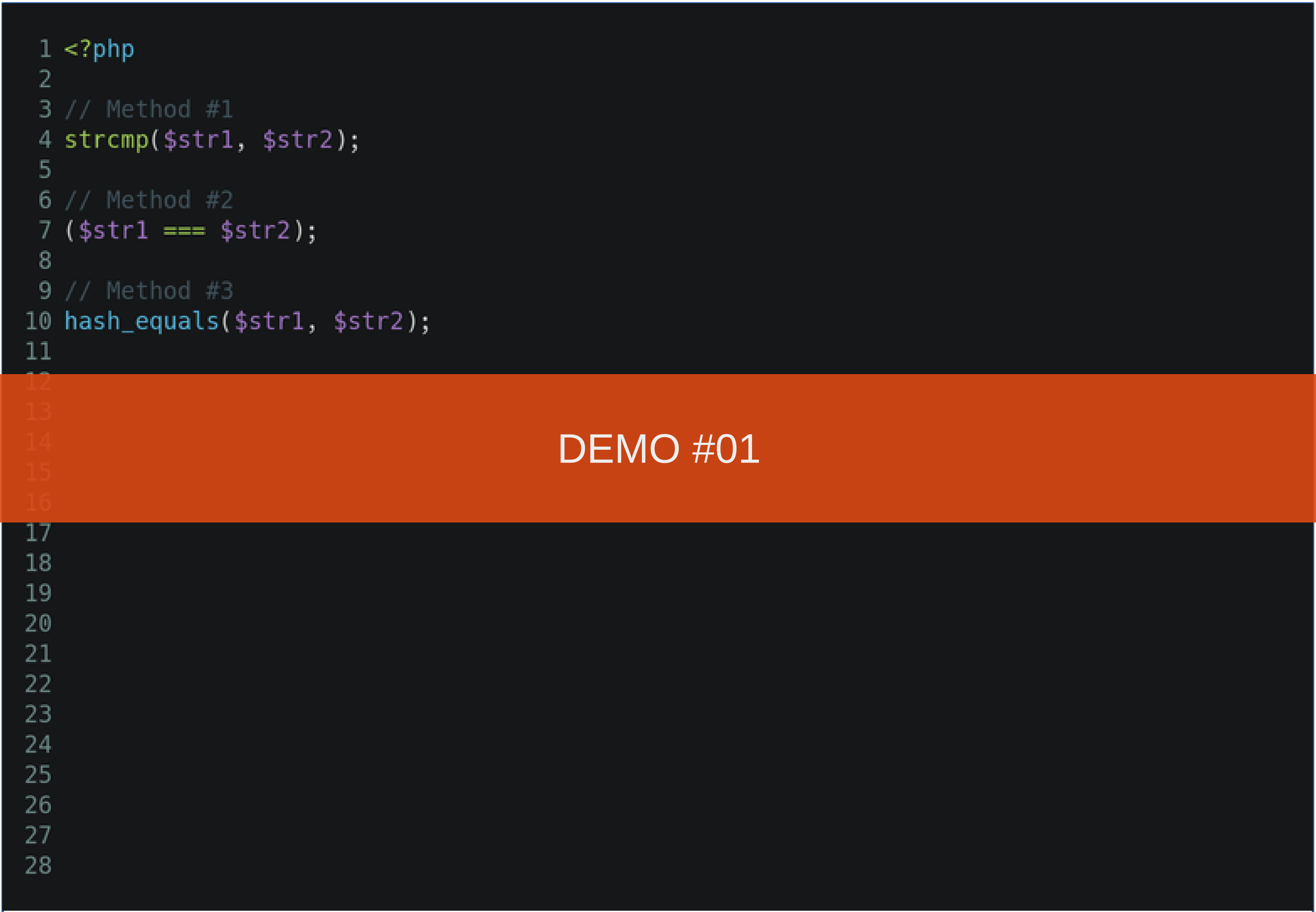
~ Donald Knuth ~

PHP

Are PHP functions safe against timing attacks ?

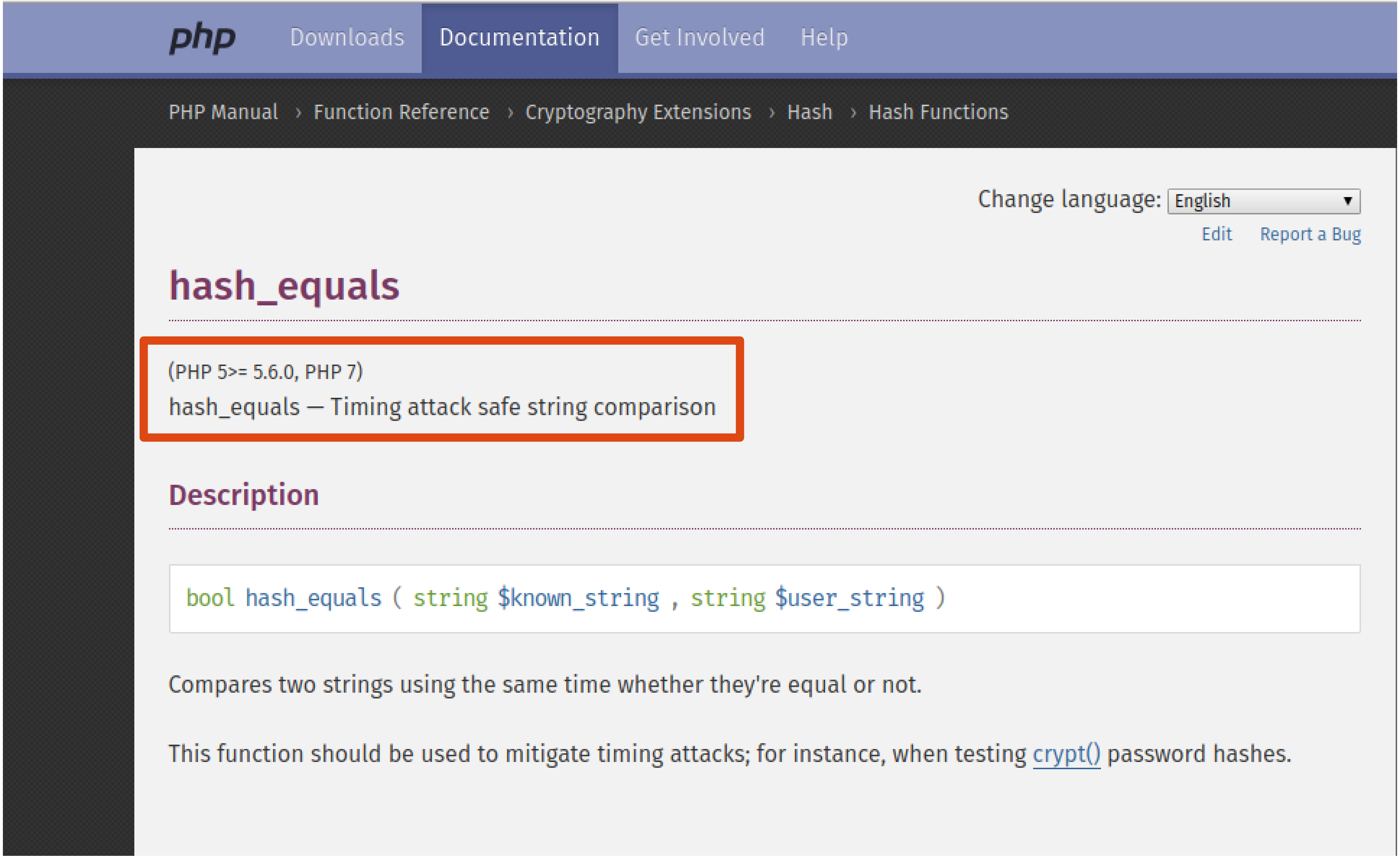


```php
<?php

// Method #1
strcmp($str1, $str2);

// Method #2
($str1 === $str2);

// Method #3
hash_equals($str1, $str2);
```



```php
<?php

// Method #1
strcmp($str1, $str2);

// Method #2
($str1 === $str2);

// Method #3
hash_equals($str1, $str2);
```

DEMO #01



PHP Manual › Function Reference › Cryptography Extensions › Hash › Hash Functions

hash_equals

(PHP 5>= 5.6.0, PHP 7)

hash_equals — Timing attack safe string comparison

Description

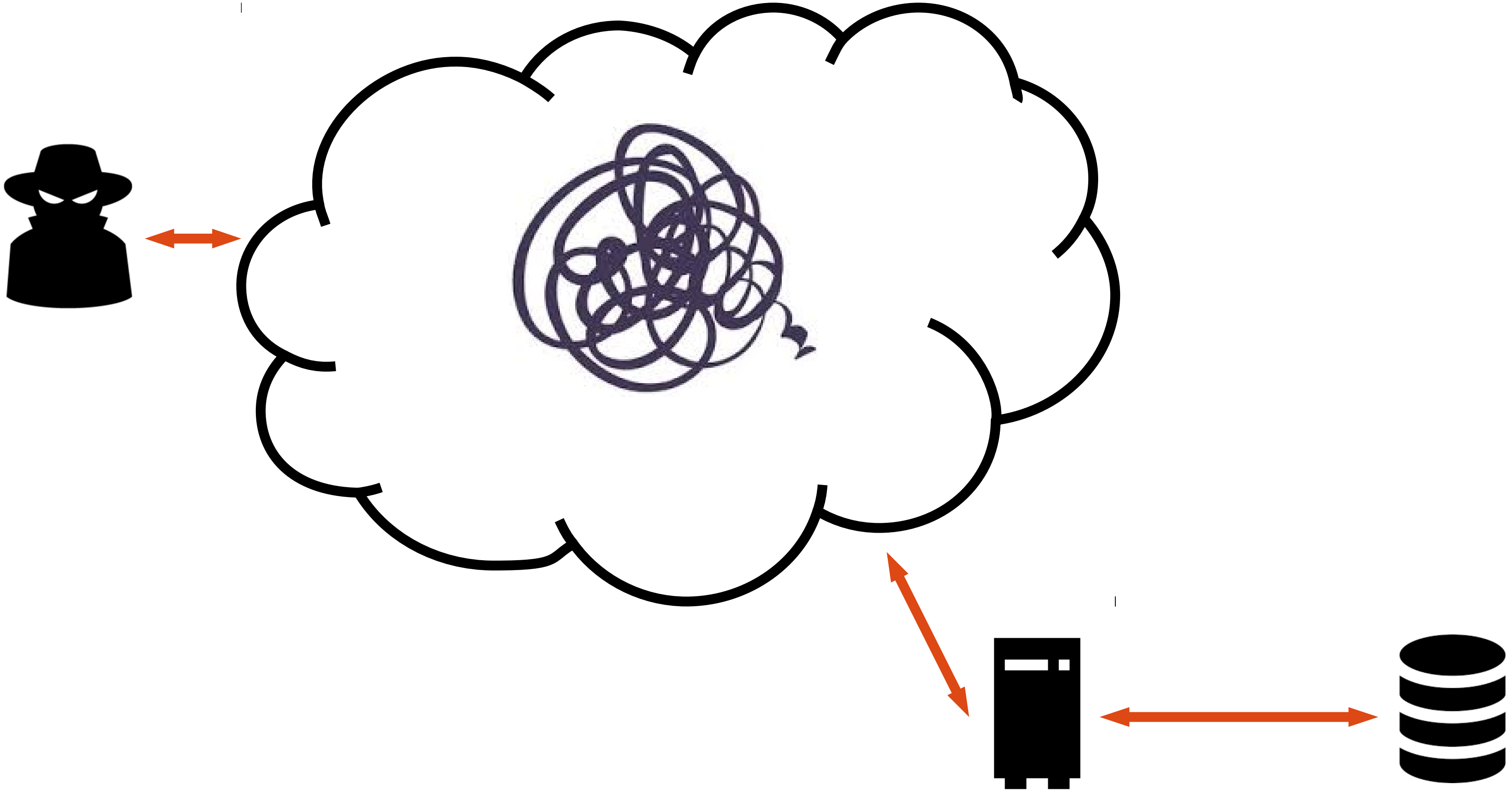
```
bool hash_equals ( string $known_string , string $user_string )
```

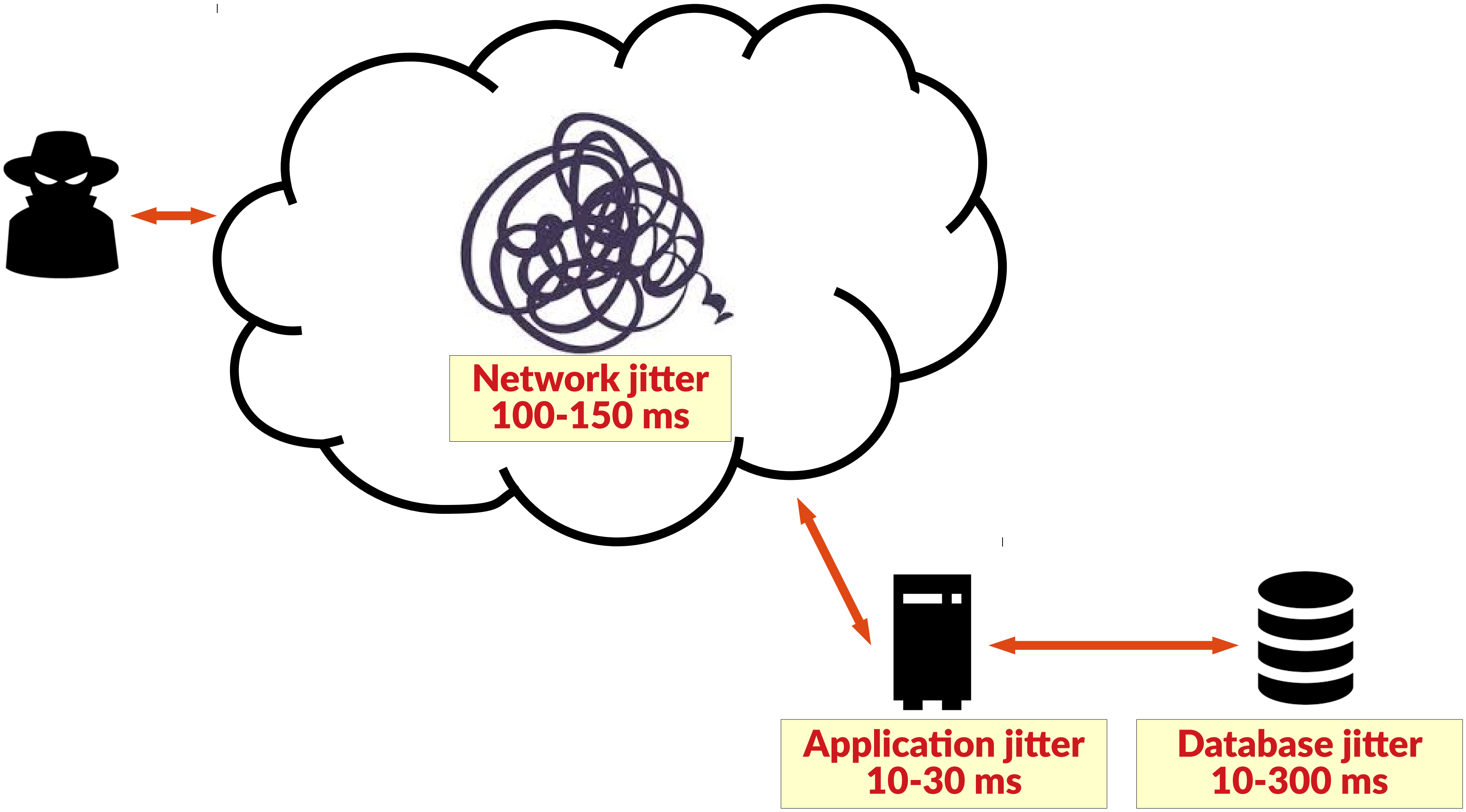
Compares two strings using the same time whether they're equal or not.

This function should be used to mitigate timing attacks; for instance, when testing crypt() password hashes.

Those work on web ideally ?

localhost





Network jitter
100-150 ms

Application jitter
10-30 ms

Database jitter
10-300 ms

Attack Shift

Timing attack against software implementation

Attack Shift

Ideal

~~Timing attack against software implementation~~

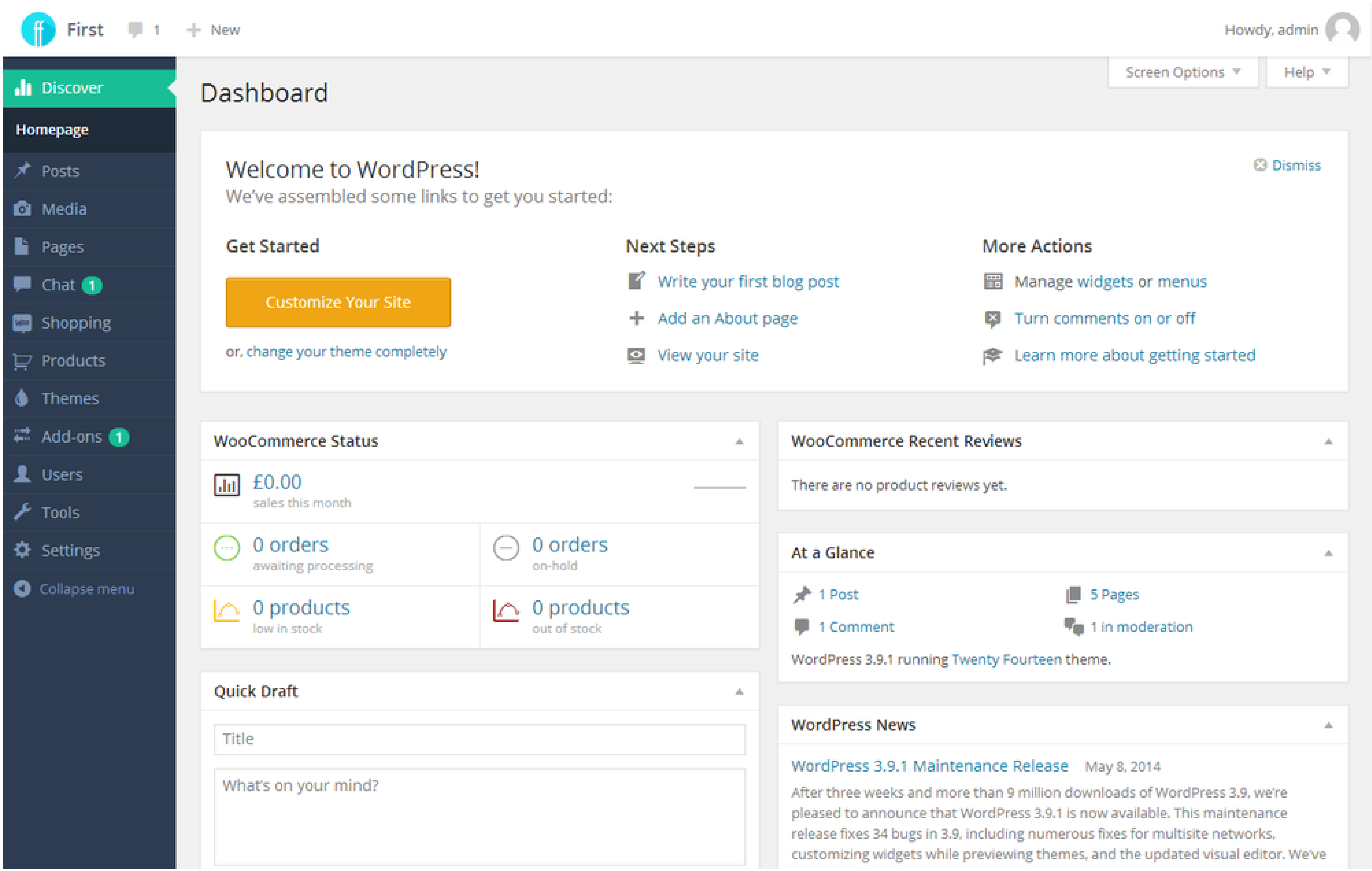
Attack Shift

Ideal

~~**Timing attack against software implementation**~~

Reality

Timing attack against business logic



Dashboard

Welcome to WordPress!

We've assembled some links to get you started:

Get Started

or, change your theme completely

Next Steps

- Write your first blog post
- Add an About page
- View your site

More Actions

- Manage widgets or menus
- Turn comments on or off
- Learn more about getting started

WooCommerce Status

£0.00 sales this month

0 orders awaiting processing

0 orders on-hold

0 products low in stock

0 products out of stock

WooCommerce Recent Reviews

There are no product reviews yet.

At a Glance

1 Post

5 Pages

1 Comment

1 in moderation

WordPress 3.9.1 running Twenty Fourteen theme.

Quick Draft

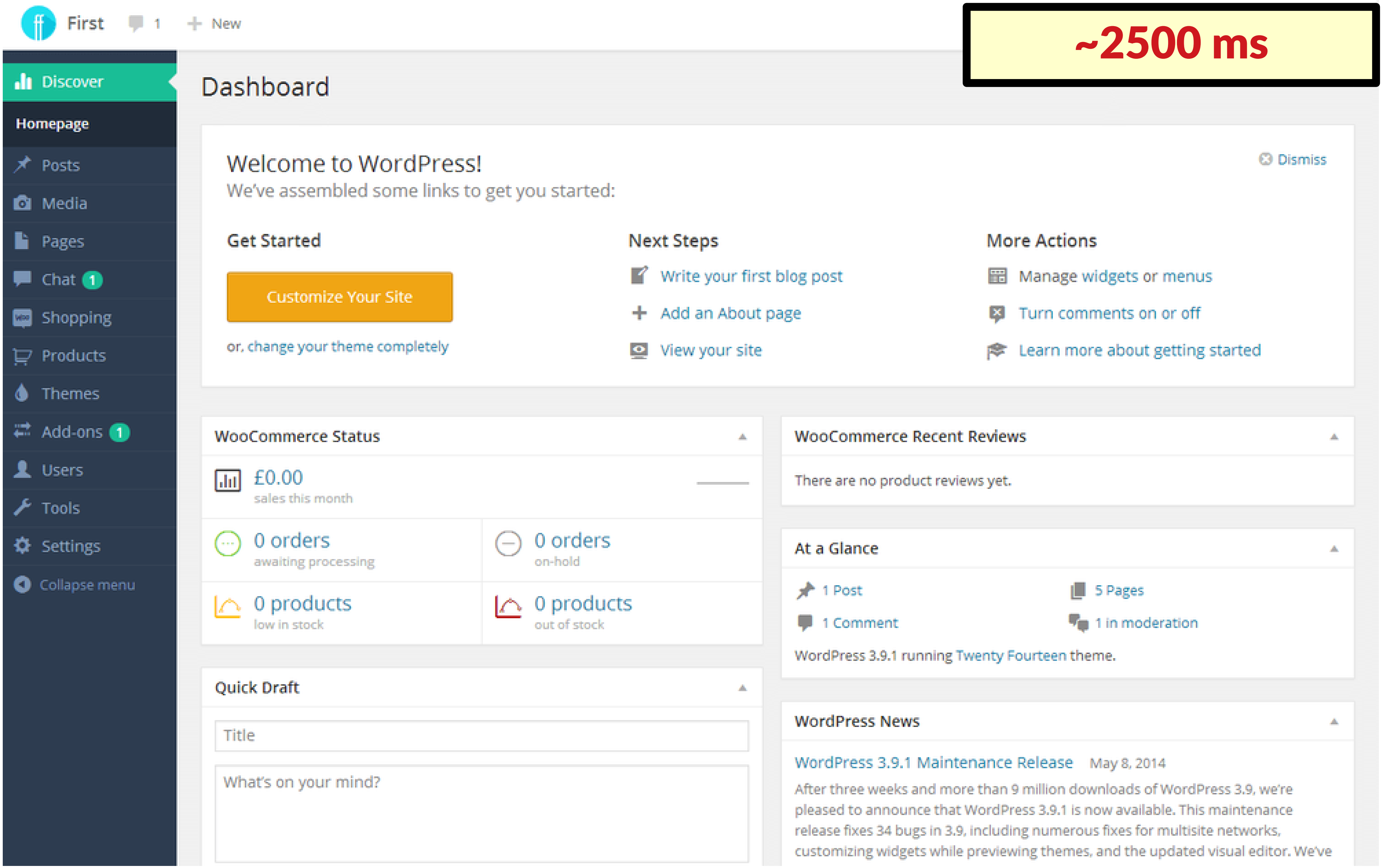
Title

What's on your mind?

WordPress News

WordPress 3.9.1 Maintenance Release May 8, 2014

After three weeks and more than 9 million downloads of WordPress 3.9, we're pleased to announce that WordPress 3.9.1 is now available. This maintenance release fixes 34 bugs in 3.9, including numerous fixes for multisite networks, customizing widgets while previewing themes, and the updated visual editor. We've



~2500 ms

Dashboard

Welcome to WordPress!

We've assembled some links to get you started:

Dismiss

Get Started

Customize Your Site

or, change your theme completely

Next Steps

- Write your first blog post
- Add an About page
- View your site

More Actions

- Manage widgets or menus
- Turn comments on or off
- Learn more about getting started

WooCommerce Status

£0.00 sales this month

0 orders awaiting processing

0 orders on-hold

0 products low in stock

0 products out of stock

WooCommerce Recent Reviews

There are no product reviews yet.

At a Glance

1 Post

5 Pages

1 Comment

1 in moderation

WordPress 3.9.1 running Twenty Fourteen theme.

Quick Draft

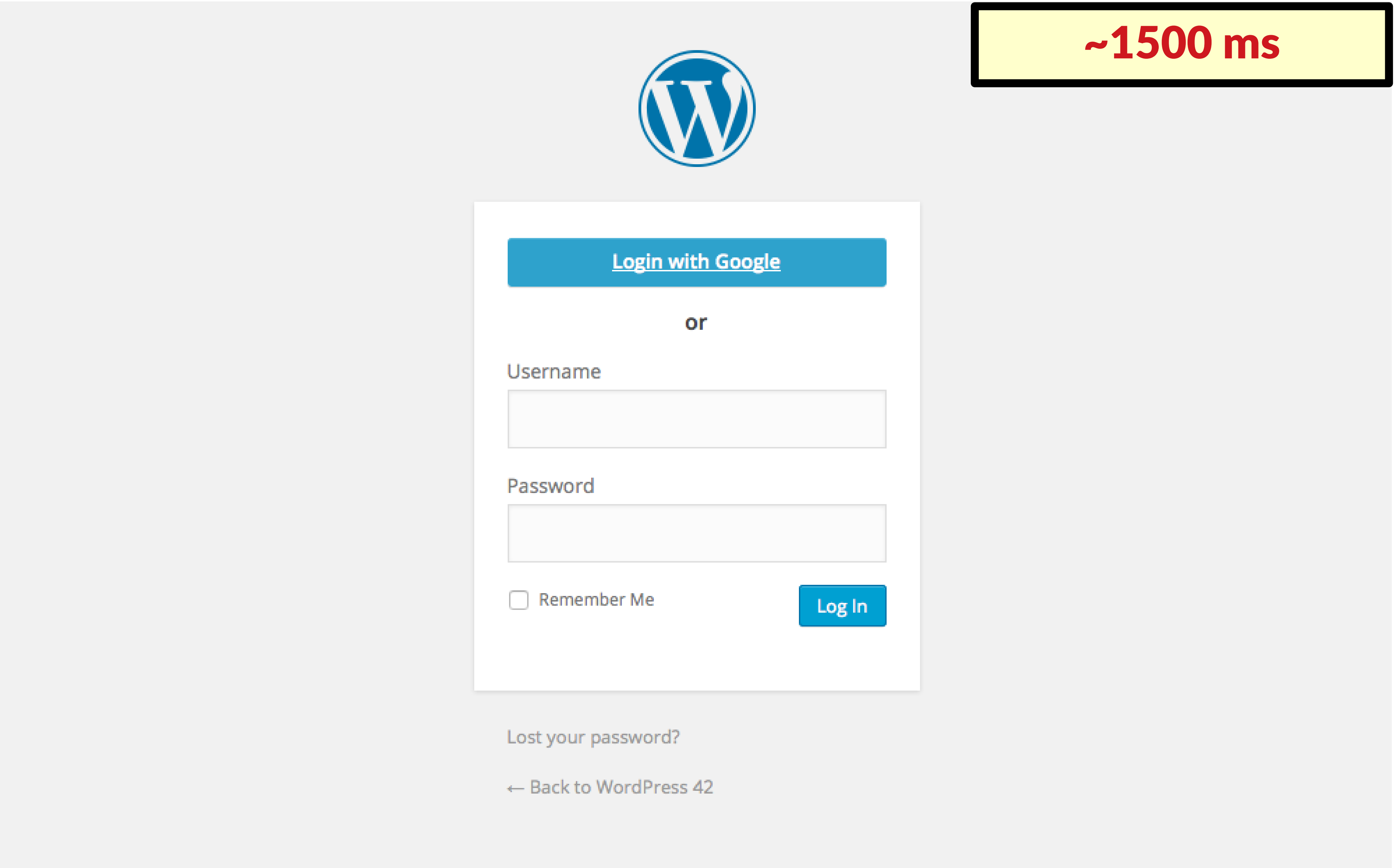
Title

What's on your mind?

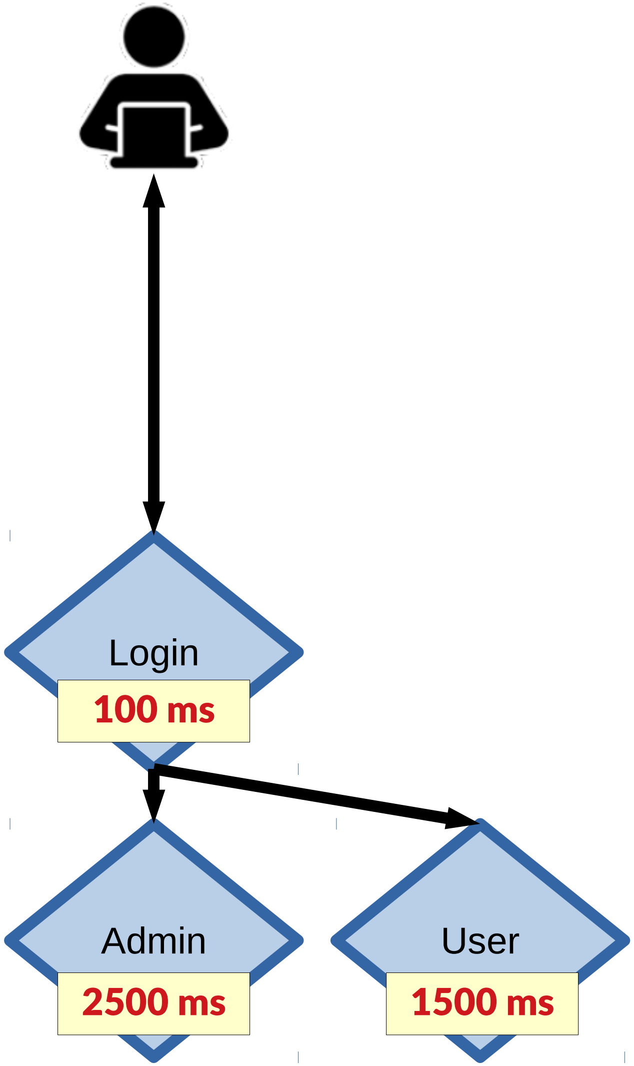
WordPress News

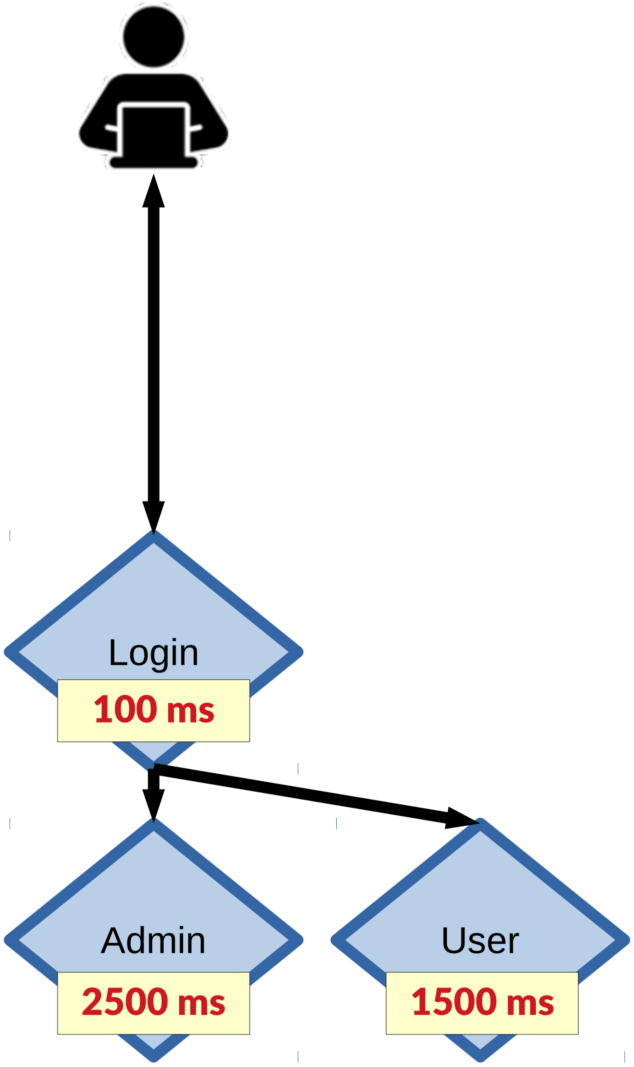
WordPress 3.9.1 Maintenance Release May 8, 2014

After three weeks and more than 9 million downloads of WordPress 3.9, we're pleased to announce that WordPress 3.9.1 is now available. This maintenance release fixes 34 bugs in 3.9, including numerous fixes for multisite networks, customizing widgets while previewing themes, and the updated visual editor. We've

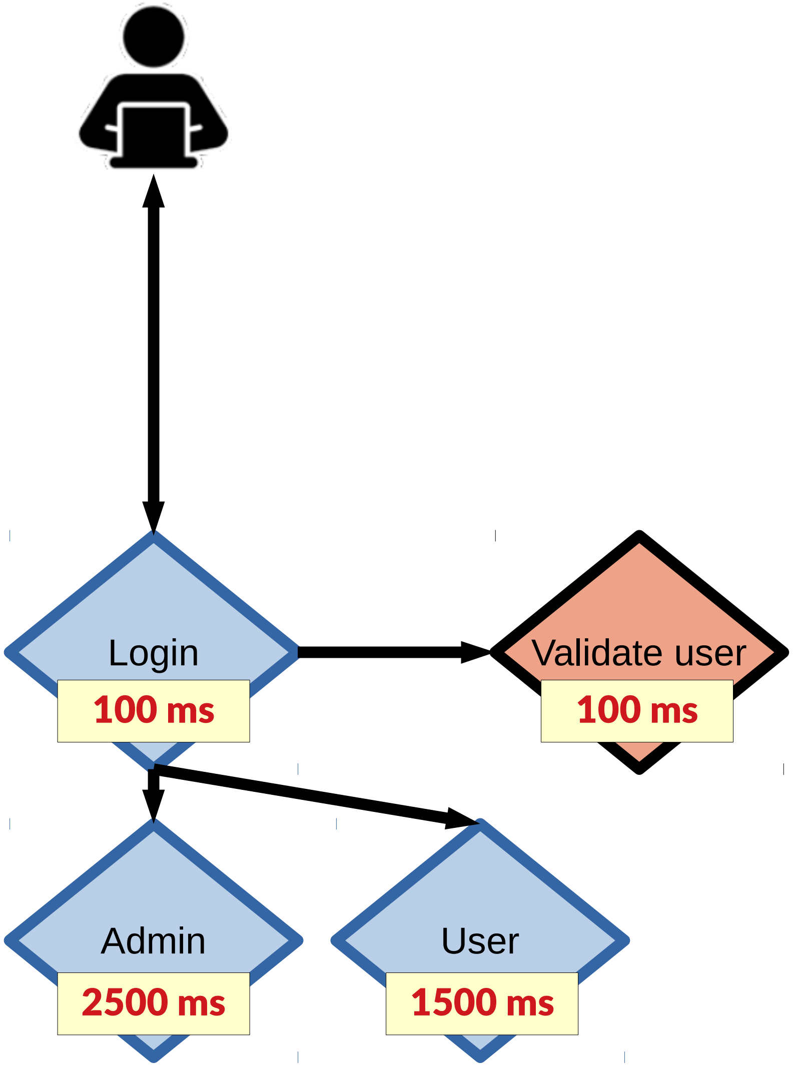

Login with Google
or
Username
Password
□ Remember Me
Log In
Lost your password?
← Back to WordPress 42

~1500 ms

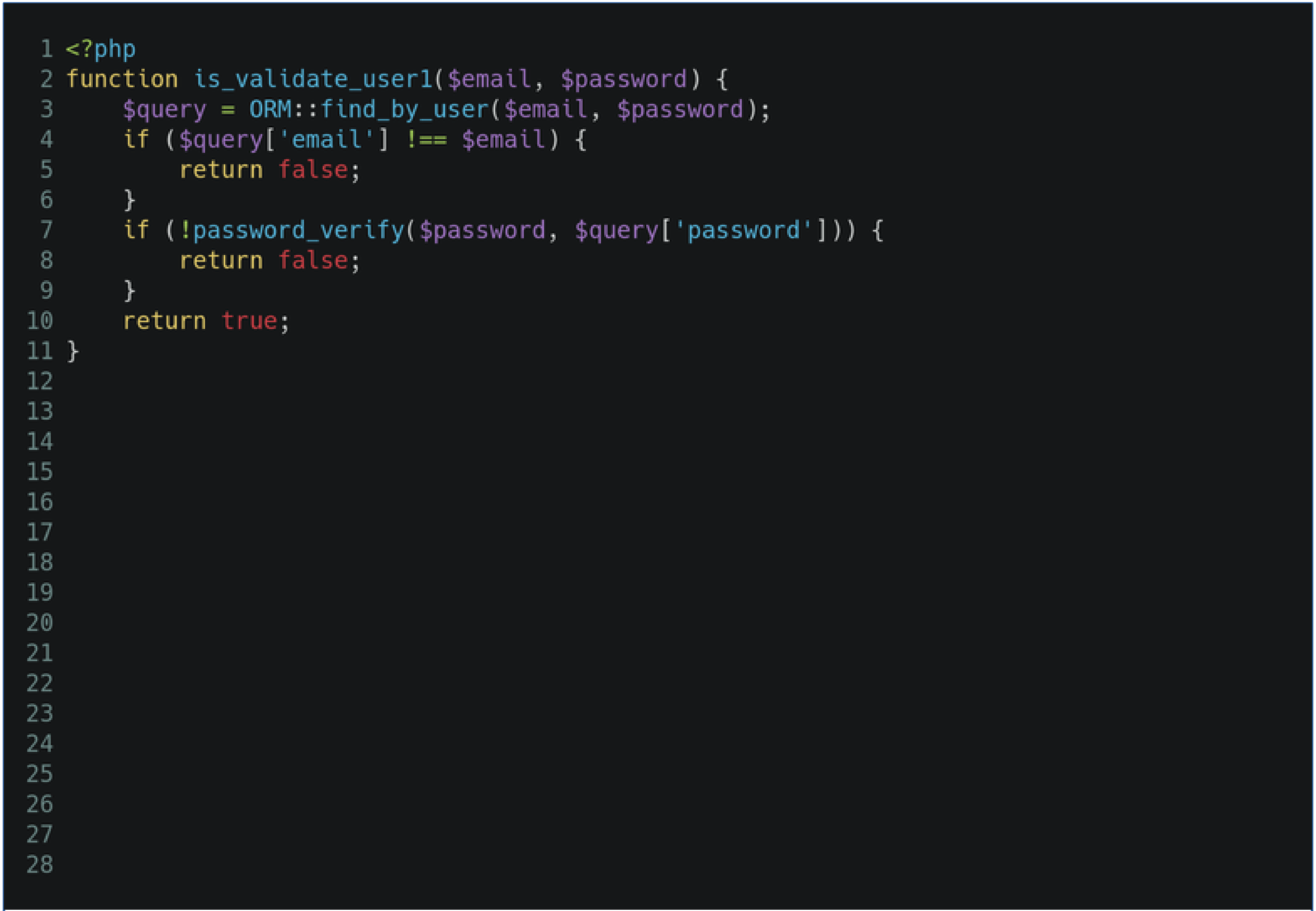

Login
100 ms
Admin
2500 ms
User
1500 ms



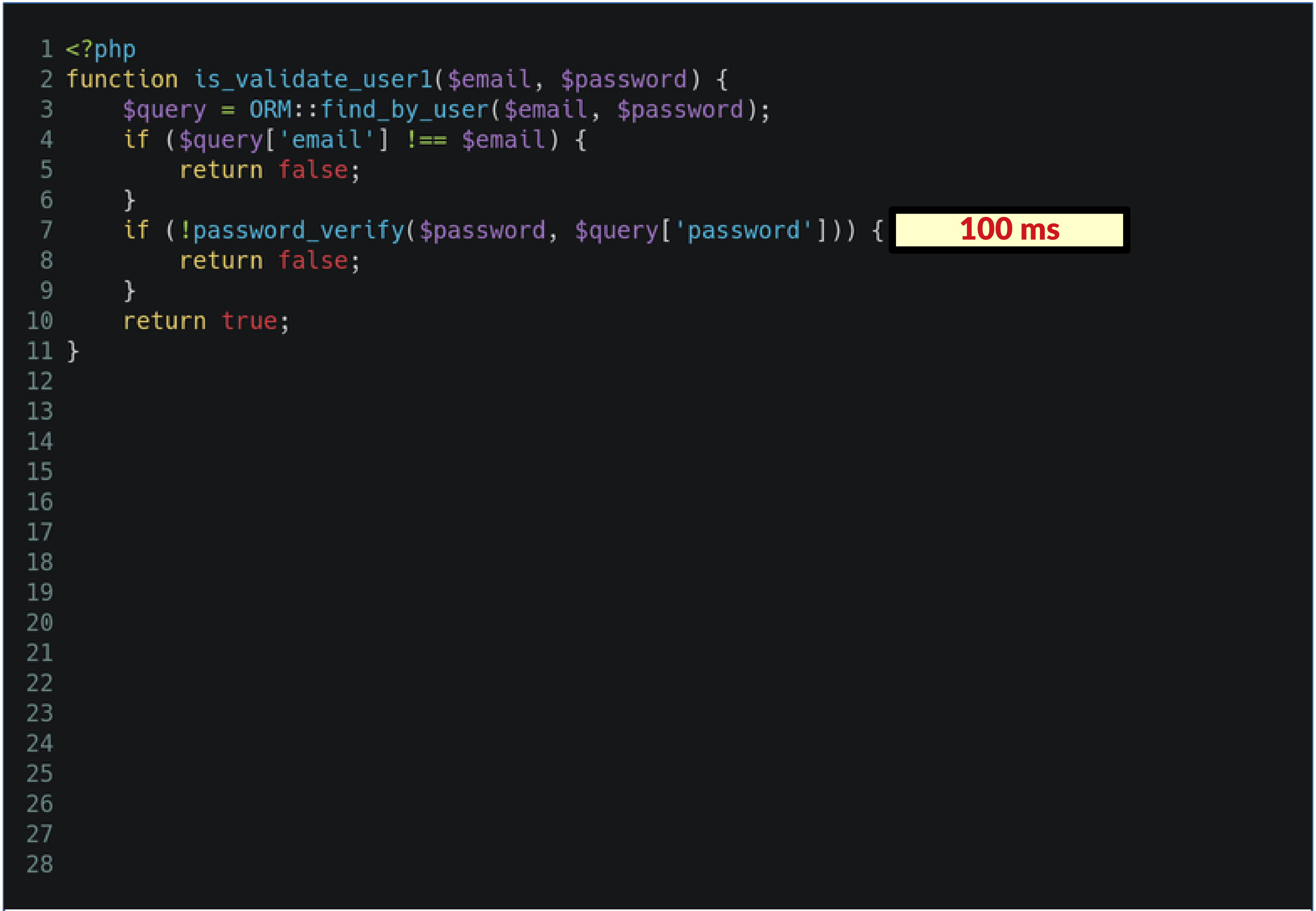
~1000 ms



~1000 ms

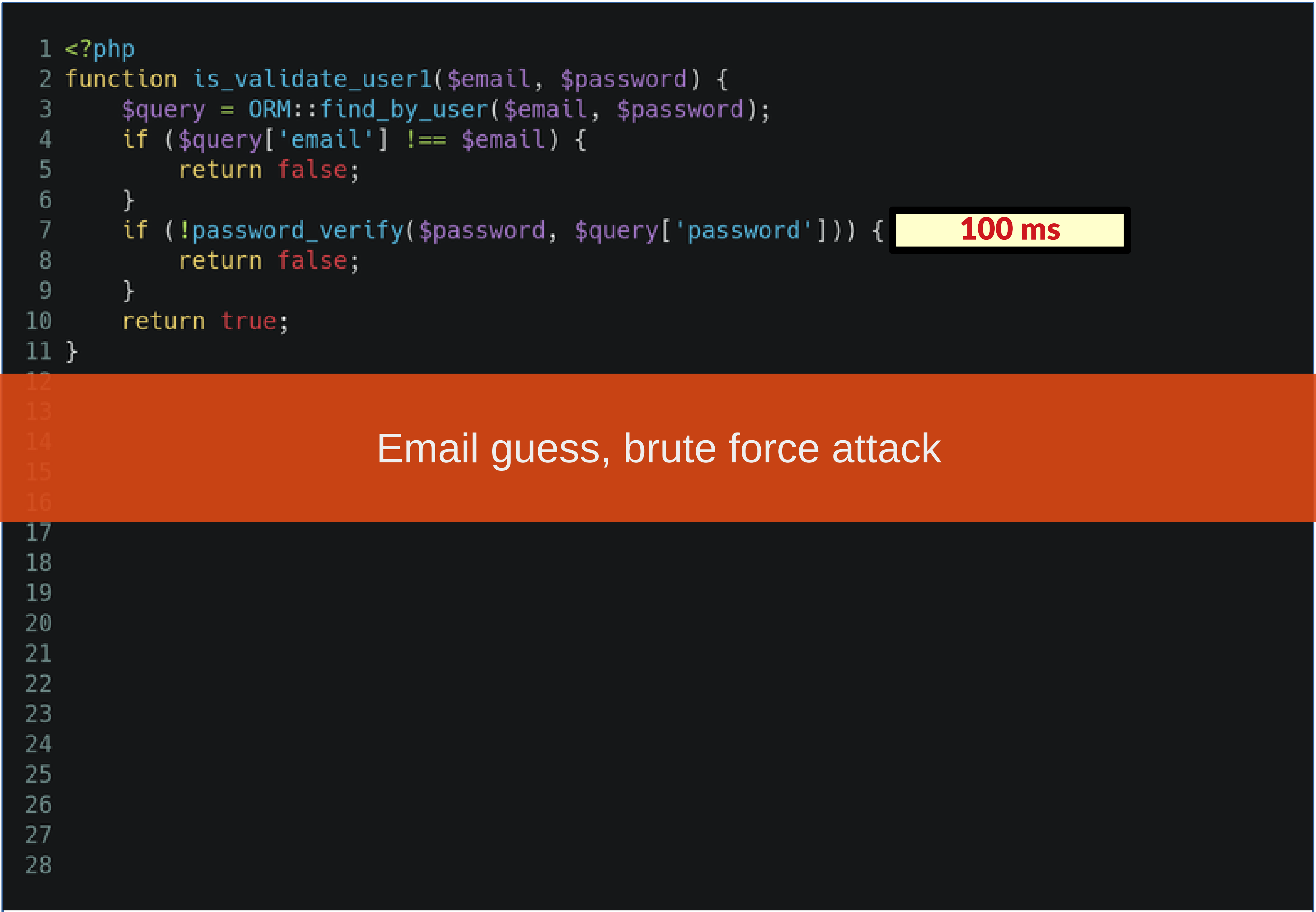


```php
<?php
function is_validate_user1($email, $password) {
    $query = ORM::find_by_user($email, $password);
    if ($query['email'] !== $email) {
        return false;
    }
    if (!password_verify($password, $query['password'])) {
        return false;
    }
    return true;
}
```



```php
<?php
function is_validate_user1($email, $password) {
    $query = ORM::find_by_user($email, $password);
    if ($query['email'] !== $email) {
        return false;
    }
    if (!password_verify($password, $query['password'])) {
        return false;
    }
    return true;
}
```

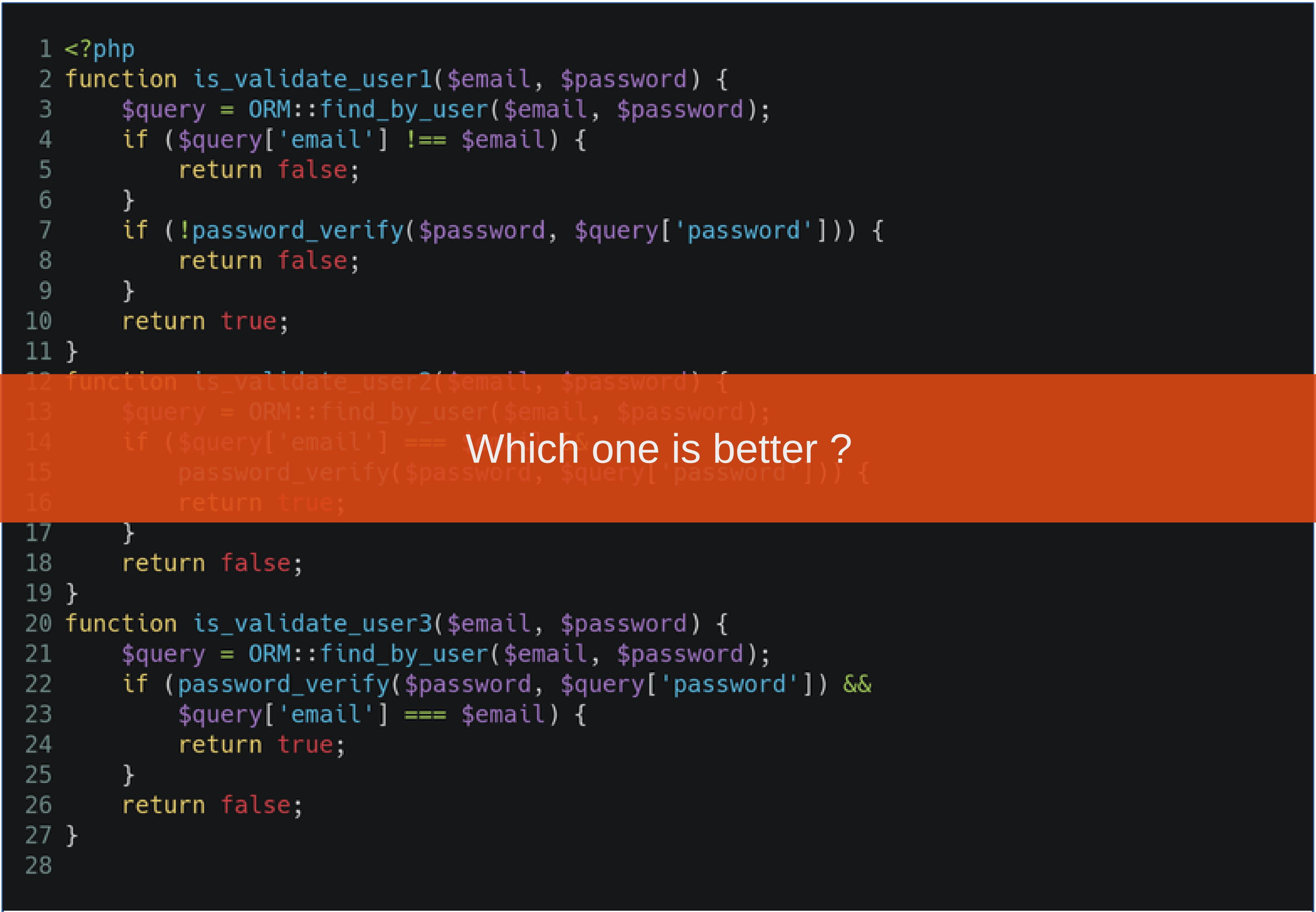
100 ms



```php
<?php
function is_validate_user1($email, $password) {
    $query = ORM::find_by_user($email, $password);
    if ($query['email'] !== $email) {
        return false;
    }
    if (!password_verify($password, $query['password'])) {
        return false;
    }
    return true;
}
```

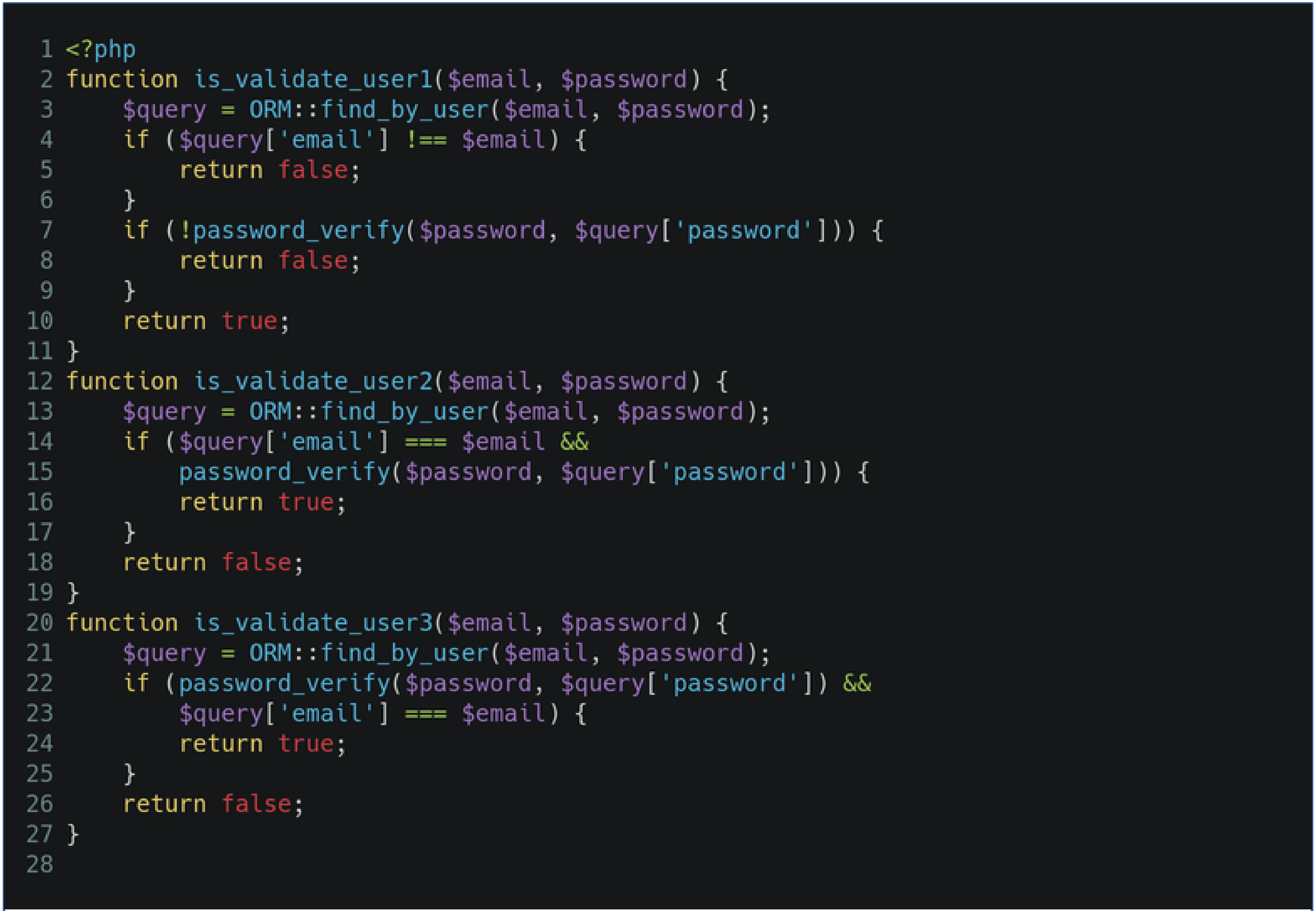
100 ms

Email guess, brute force attack

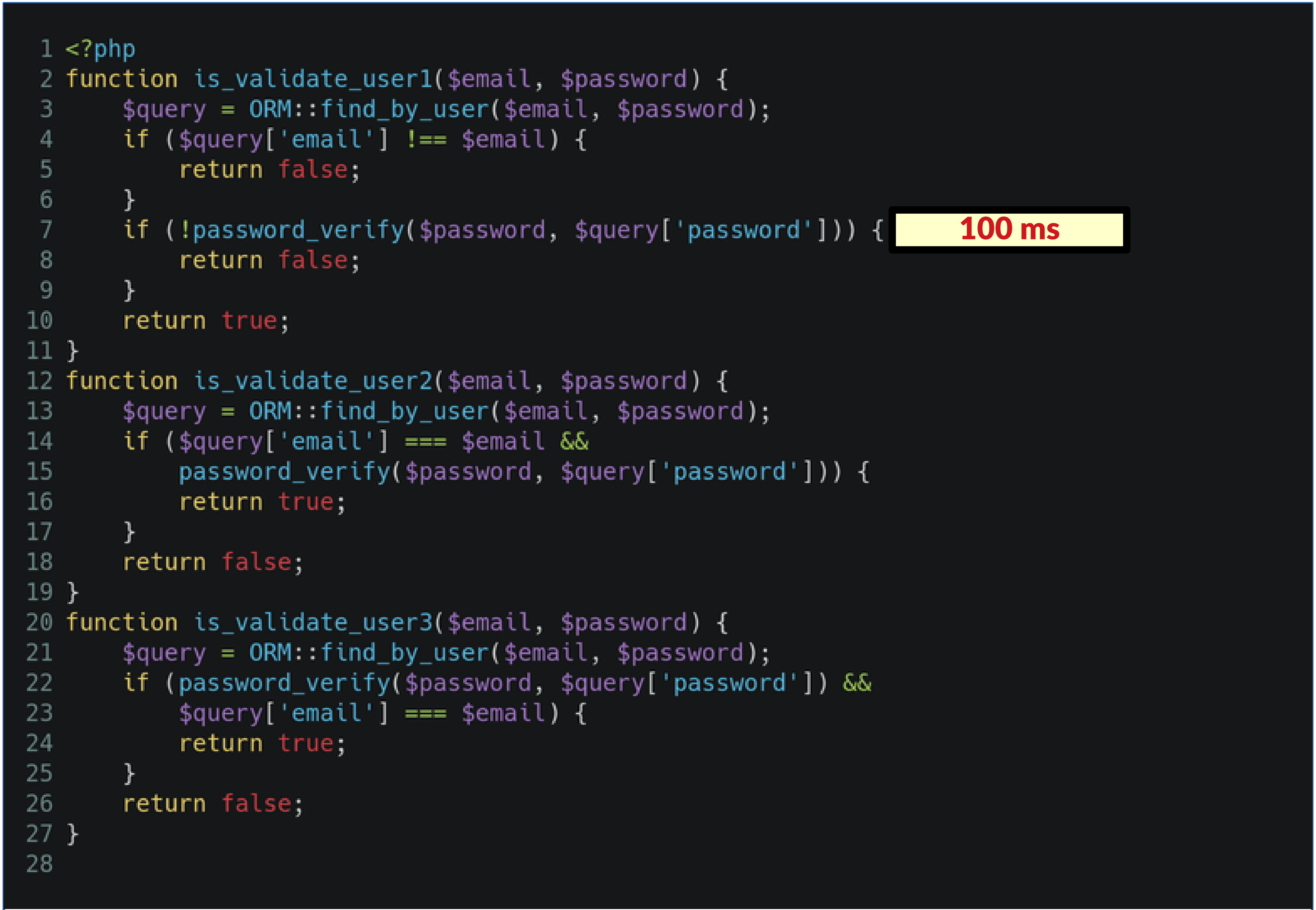


```php
<?php
function is_validate_user1($email, $password) {
    $query = ORM::find_by_user($email, $password);
    if ($query['email'] !== $email) {
        return false;
    }
    if (!password_verify($password, $query['password'])) {
        return false;
    }
    return true;
}
function is_validate_user2($email, $password) {
    $query = ORM::find_by_user($email, $password);
    if ($query['email'] === $email &&
        password_verify($password, $query['password'])) {
        return true;
    }
    return false;
}
function is_validate_user3($email, $password) {
    $query = ORM::find_by_user($email, $password);
    if (password_verify($password, $query['password']) &&
        $query['email'] === $email) {
        return true;
    }
    return false;
}

```

Which one is better ?

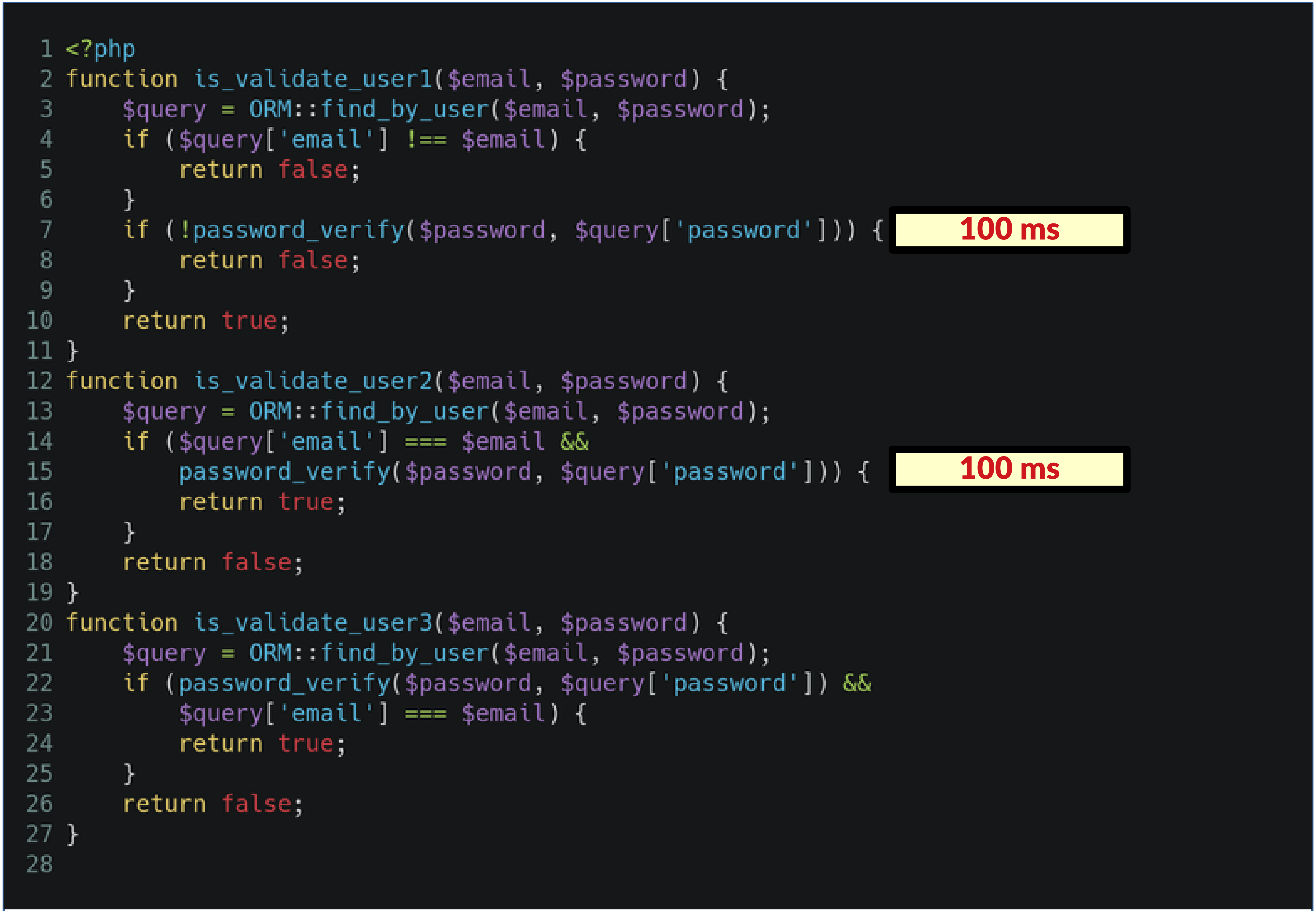


```php
<?php
function is_validate_user1($email, $password) {
    $query = ORM::find_by_user($email, $password);
    if ($query['email'] !== $email) {
        return false;
    }
    if (!password_verify($password, $query['password'])) {
        return false;
    }
    return true;
}
function is_validate_user2($email, $password) {
    $query = ORM::find_by_user($email, $password);
    if ($query['email'] === $email &&
        password_verify($password, $query['password'])) {
        return true;
    }
    return false;
}
function is_validate_user3($email, $password) {
    $query = ORM::find_by_user($email, $password);
    if (password_verify($password, $query['password']) &&
        $query['email'] === $email) {
        return true;
    }
    return false;
}

```



```php
<?php
function is_validate_user1($email, $password) {
    $query = ORM::find_by_user($email, $password);
    if ($query['email'] !== $email) {
        return false;
    }
    if (!password_verify($password, $query['password'])) {
        return false;
    }
    return true;
}
function is_validate_user2($email, $password) {
    $query = ORM::find_by_user($email, $password);
    if ($query['email'] === $email &&
        password_verify($password, $query['password'])) {
        return true;
    }
    return false;
}
function is_validate_user3($email, $password) {
    $query = ORM::find_by_user($email, $password);
    if (password_verify($password, $query['password']) &&
        $query['email'] === $email) {
        return true;
    }
    return false;
}
```

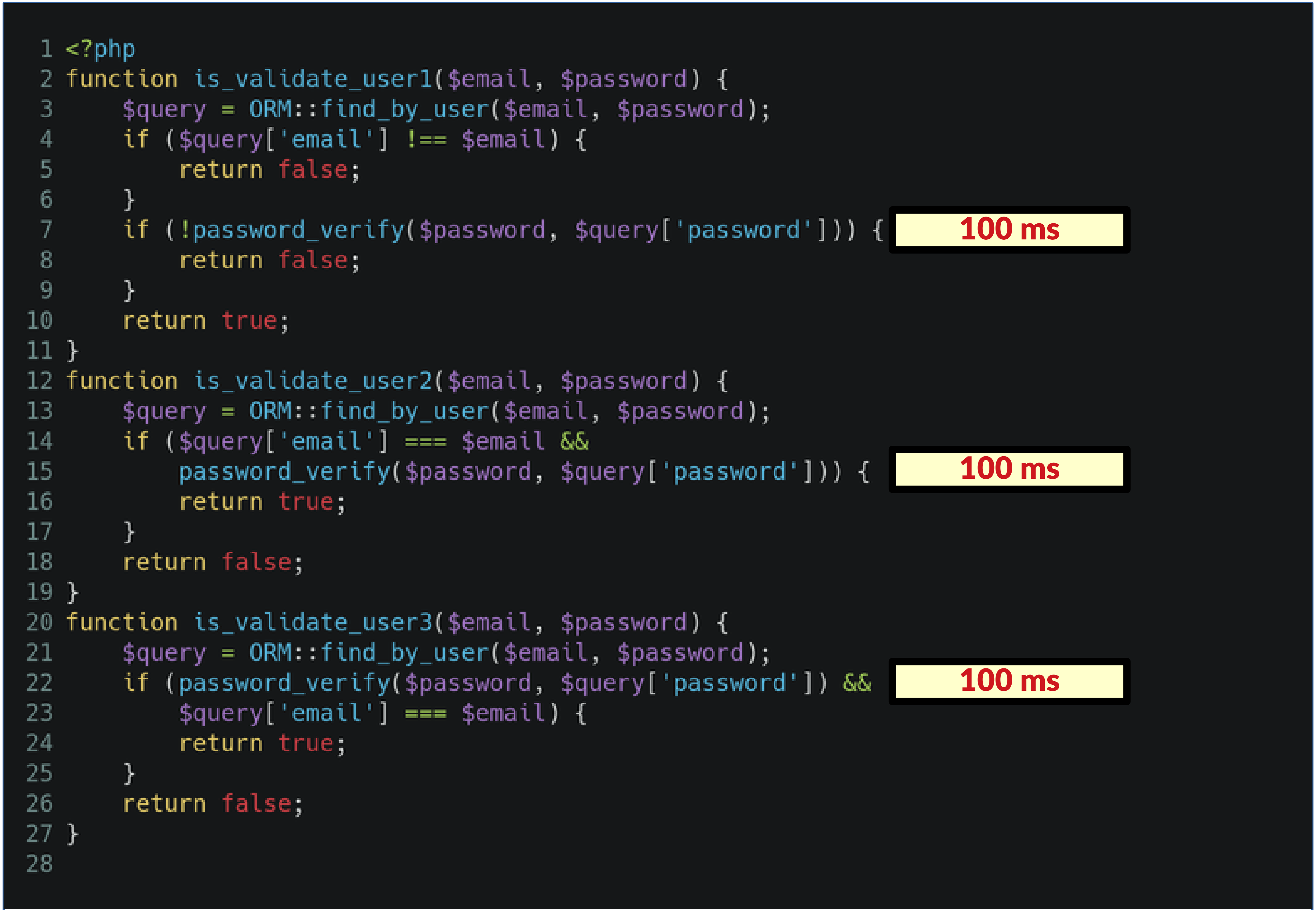
100 ms



```php
<?php
function is_validate_user1($email, $password) {
    $query = ORM::find_by_user($email, $password);
    if ($query['email'] !== $email) {
        return false;
    }
    if (!password_verify($password, $query['password'])) {
        return false;
    }
    return true;
}
function is_validate_user2($email, $password) {
    $query = ORM::find_by_user($email, $password);
    if ($query['email'] === $email &&
        password_verify($password, $query['password'])) {
        return true;
    }
    return false;
}
function is_validate_user3($email, $password) {
    $query = ORM::find_by_user($email, $password);
    if (password_verify($password, $query['password']) &&
        $query['email'] === $email) {
        return true;
    }
    return false;
}

```

100 ms

100 ms



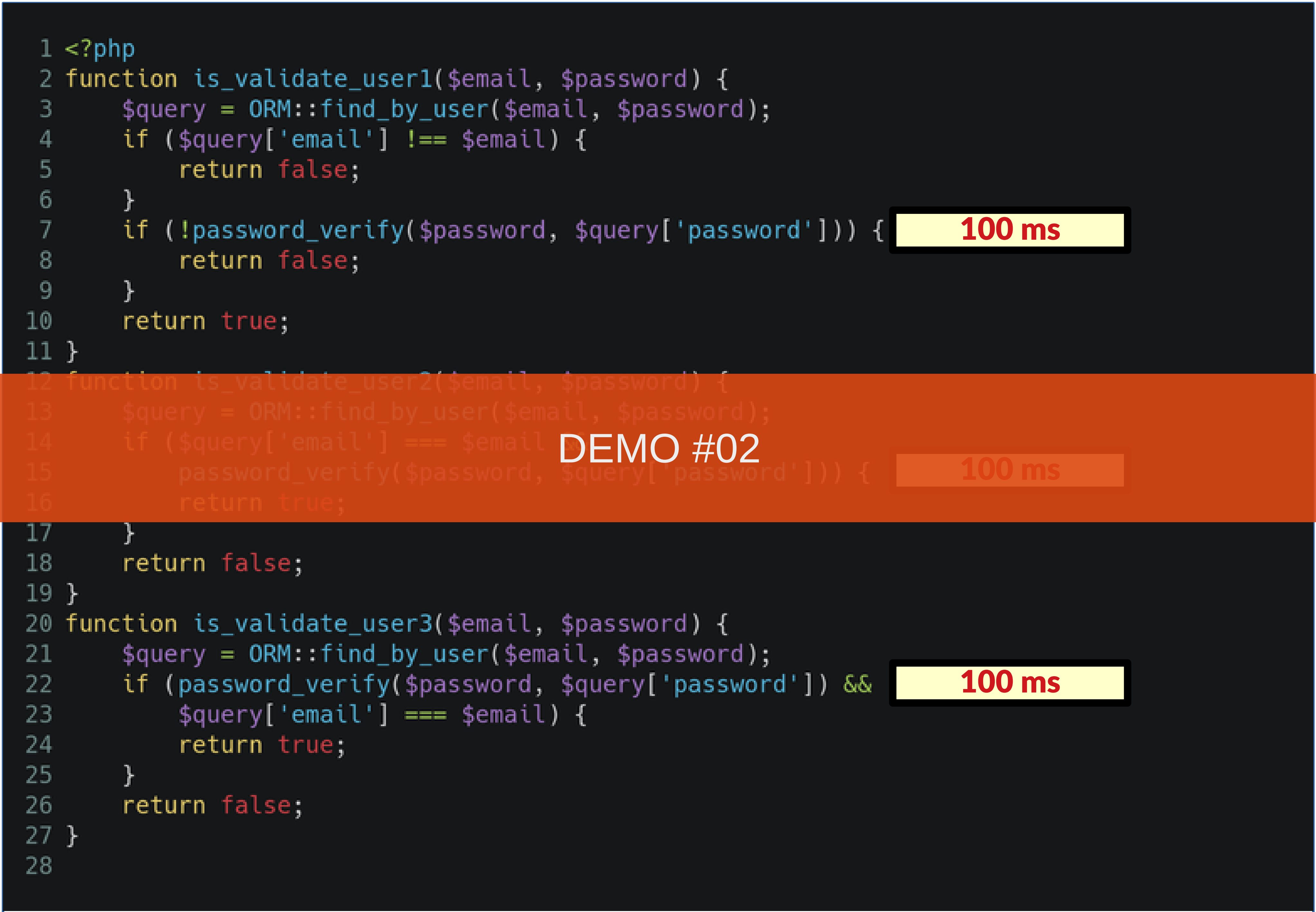
```php
<?php
function is_validate_user1($email, $password) {
    $query = ORM::find_by_user($email, $password);
    if ($query['email'] !== $email) {
        return false;
    }
    if (!password_verify($password, $query['password'])) {
        return false;
    }
    return true;
}
function is_validate_user2($email, $password) {
    $query = ORM::find_by_user($email, $password);
    if ($query['email'] === $email &&
        password_verify($password, $query['password'])) {
        return true;
    }
    return false;
}
function is_validate_user3($email, $password) {
    $query = ORM::find_by_user($email, $password);
    if (password_verify($password, $query['password']) &&
        $query['email'] === $email) {
        return true;
    }
    return false;
}

```

100 ms

100 ms

100 ms

DEMO #02

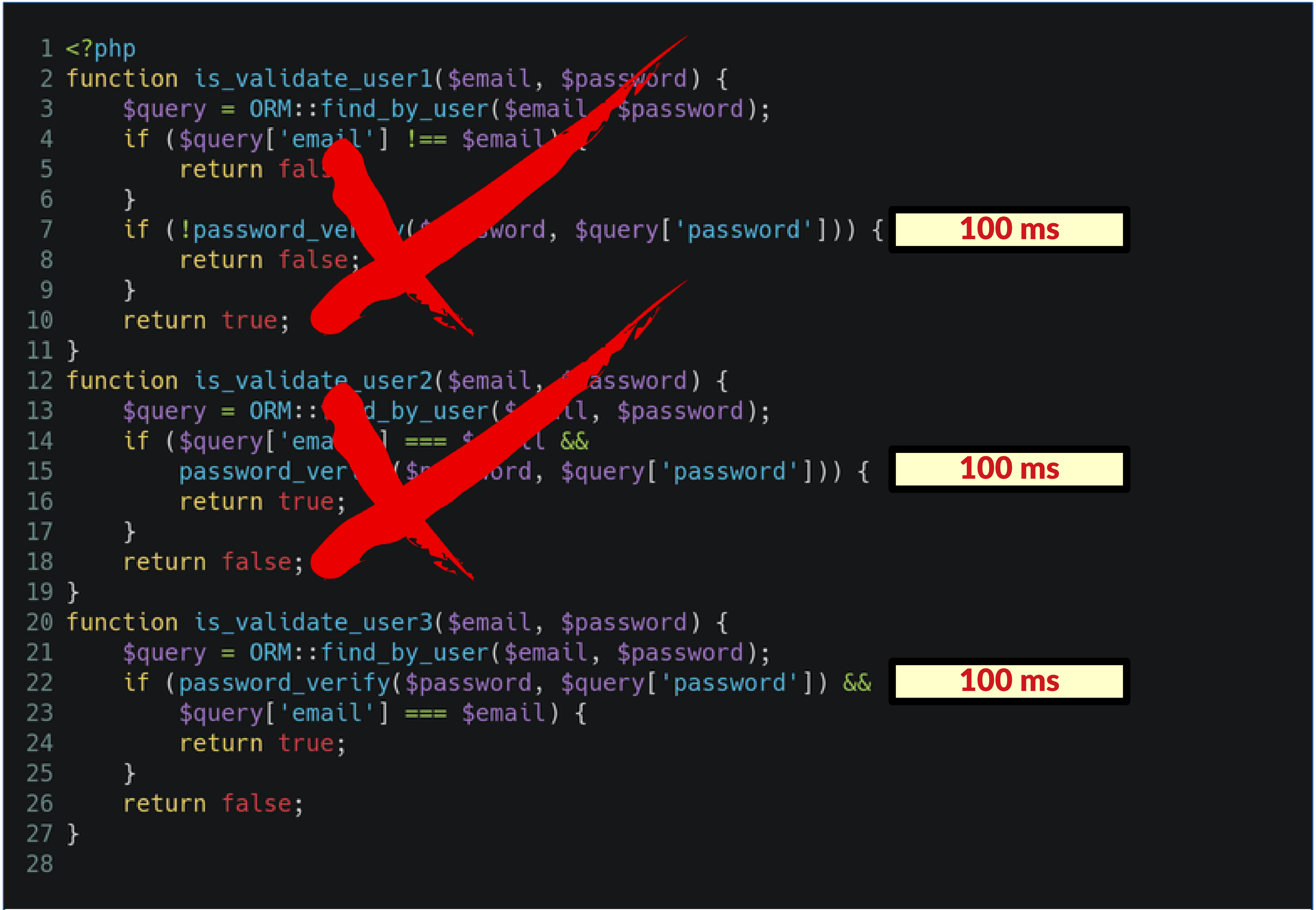


```php
<?php
function is_validate_user1($email, $password) {
    $query = ORM::find_by_user($email, $password);
    if ($query['email'] !== $email) {
        return false;
    }
    if (!password_verify($password, $query['password'])) {
        return false;
    }
    return true;
}
function is_validate_user2($email, $password) {
    $query = ORM::find_by_user($email, $password);
    if ($query['email'] === $email &&
        password_verify($password, $query['password'])) {
        return true;
    }
    return false;
}
function is_validate_user3($email, $password) {
    $query = ORM::find_by_user($email, $password);
    if (password_verify($password, $query['password']) &&
        $query['email'] === $email) {
        return true;
    }
    return false;
}

```

100 ms

100 ms

100 ms

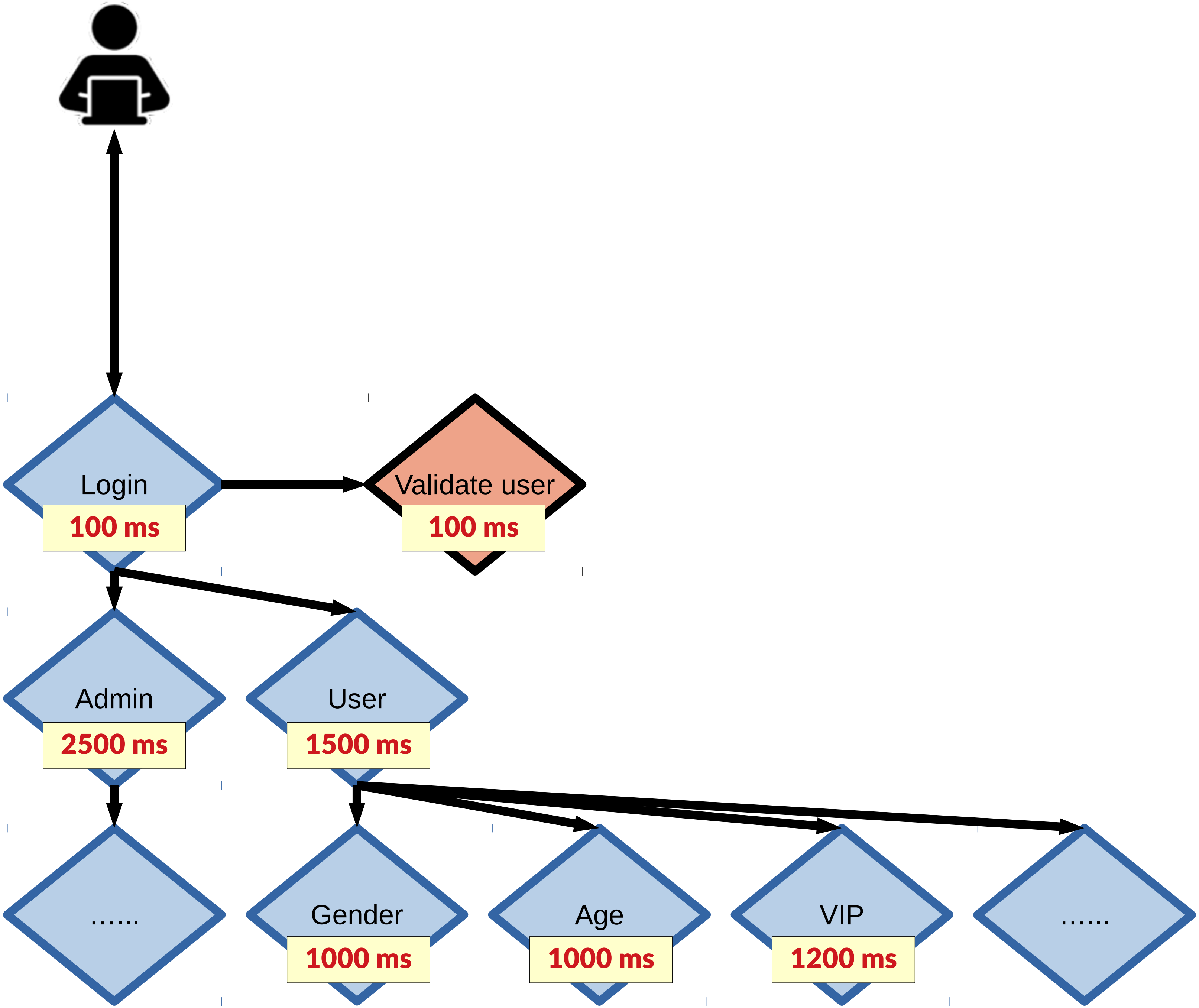


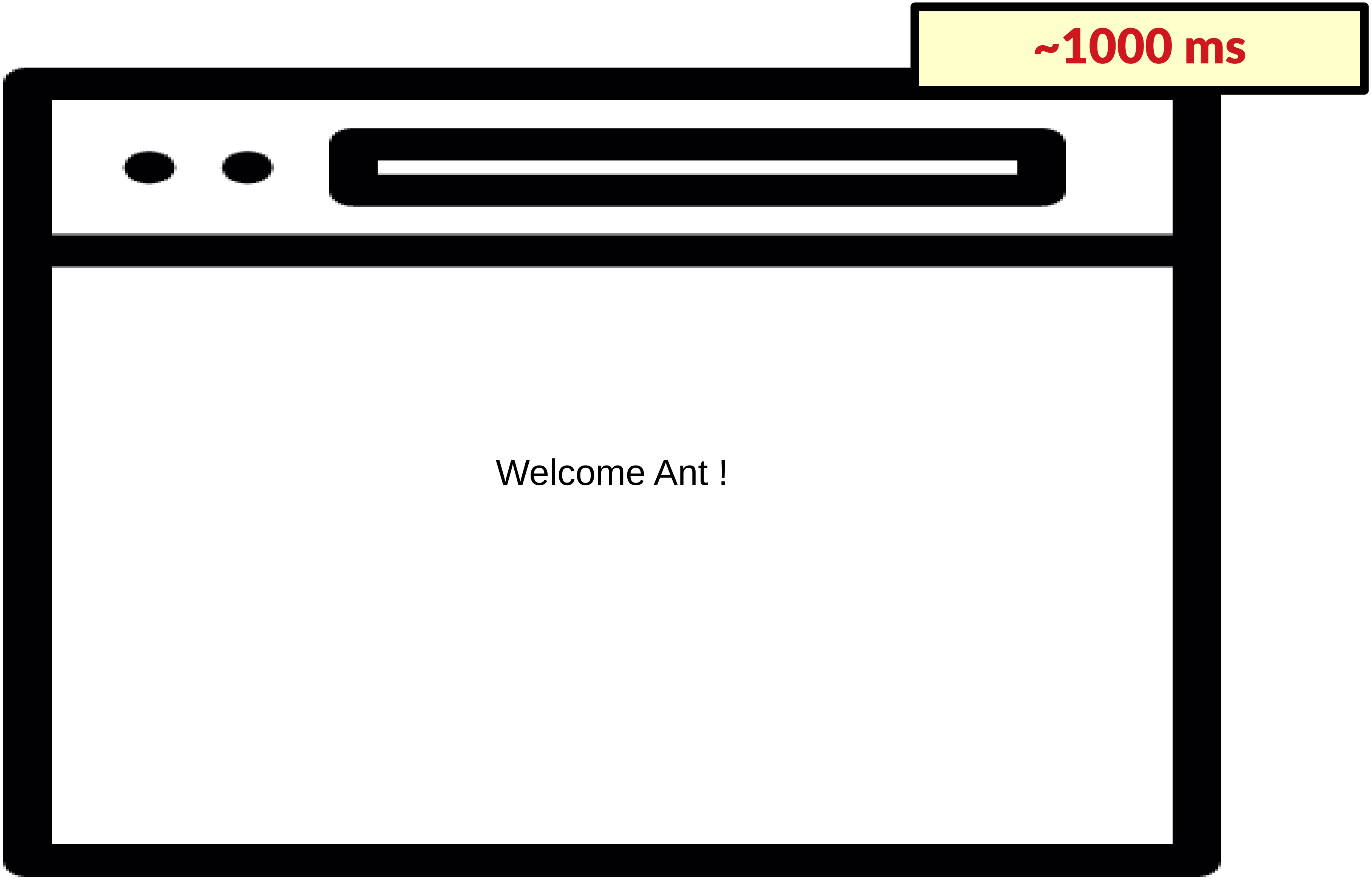
```php
<?php
function is_validate_user1($email, $password) {
    $query = ORM::find_by_user($email, $password);
    if ($query['email'] !== $email) {
        return false;
    }
    if (!password_verify($password, $query['password'])) {
        return false;
    }
    return true;
}
function is_validate_user2($email, $password) {
    $query = ORM::find_by_user($email, $password);
    if ($query['email'] === $email &&
        password_verify($password, $query['password'])) {
        return true;
    }
    return false;
}
function is_validate_user3($email, $password) {
    $query = ORM::find_by_user($email, $password);
    if (password_verify($password, $query['password']) &&
        $query['email'] === $email) {
        return true;
    }
    return false;
}
```

100 ms

100 ms

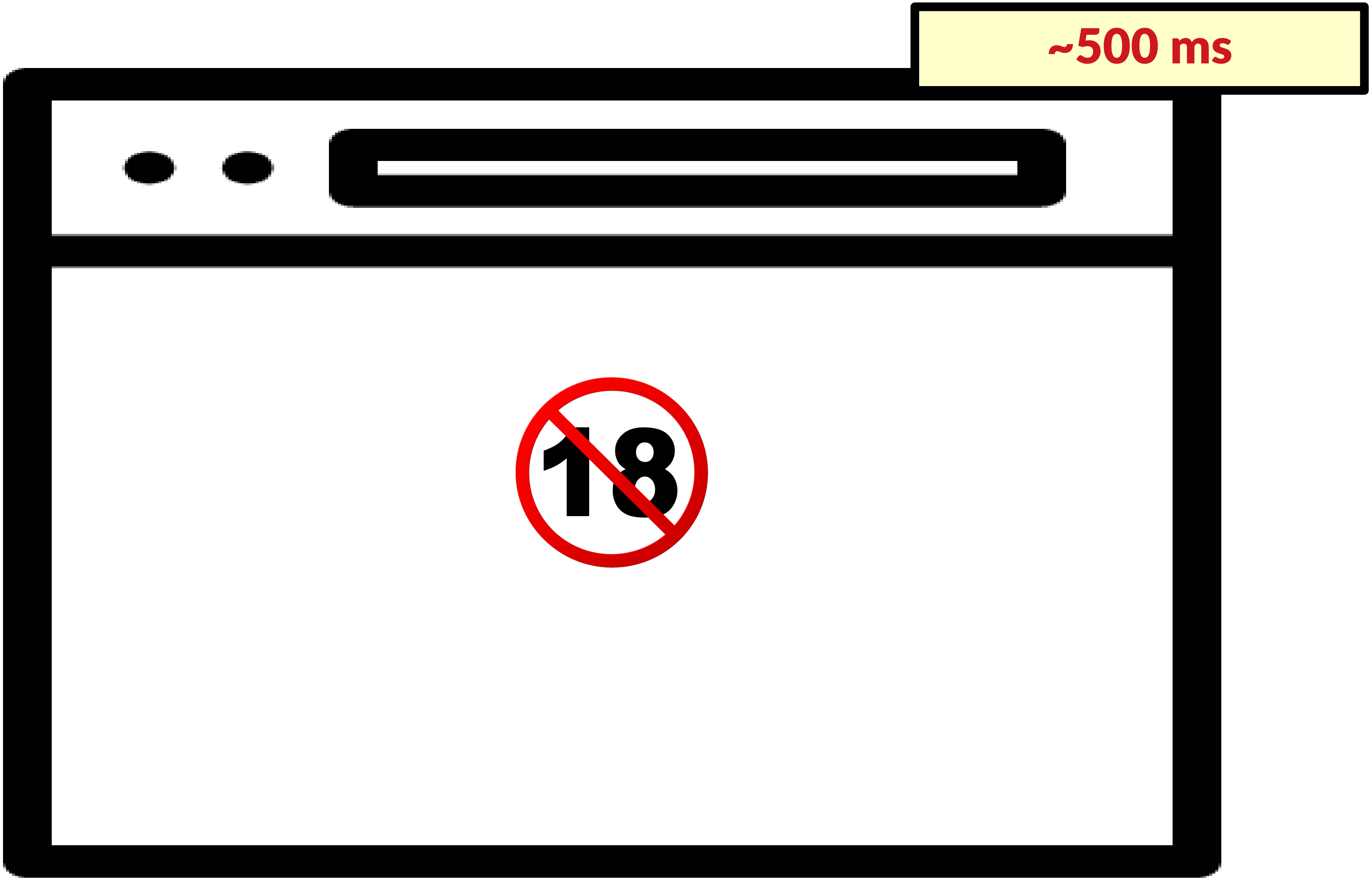
100 ms


Login
100 ms
Validate user
100 ms
Admin
2500 ms
User
1500 ms
……
Gender
1000 ms
Age
1000 ms
VIP
1200 ms
……



~1000 ms

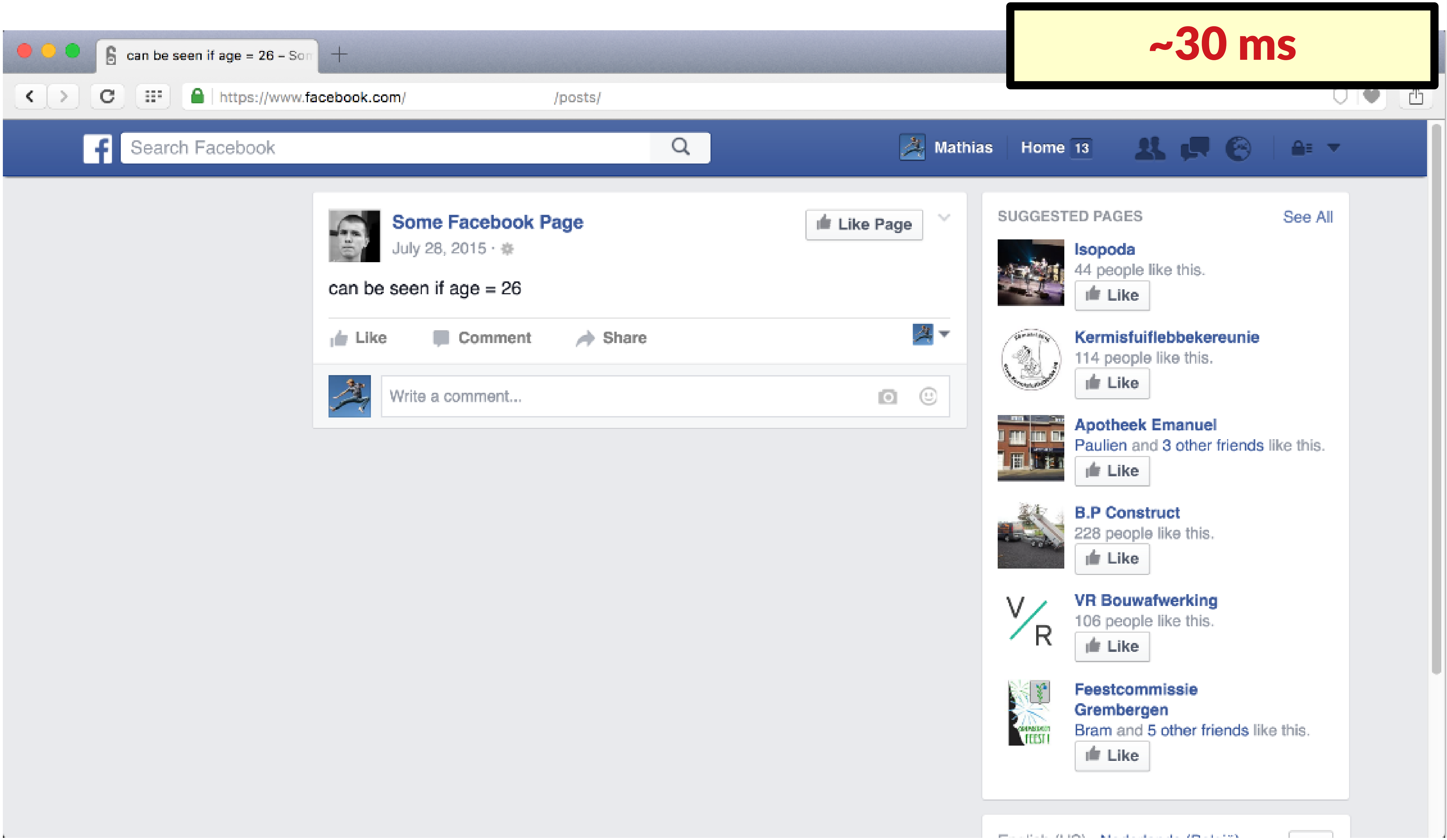
Welcome Ant !



~500 ms

old

~30 ms



can be seen if age = 26 – Son

https://www.facebook.com/ /posts/

Search Facebook

Mathias Home 13

Some Facebook Page

July 28, 2015 ·

Like Page

can be seen if age = 26

Like Comment Share

Write a comment...

SUGGESTED PAGES See All

Isopoda
44 people like this.
Like

Kermisfuiflebbekereunie
114 people like this.
Like

Apotheek Emanuel
Paulien and 3 other friends like this.
Like

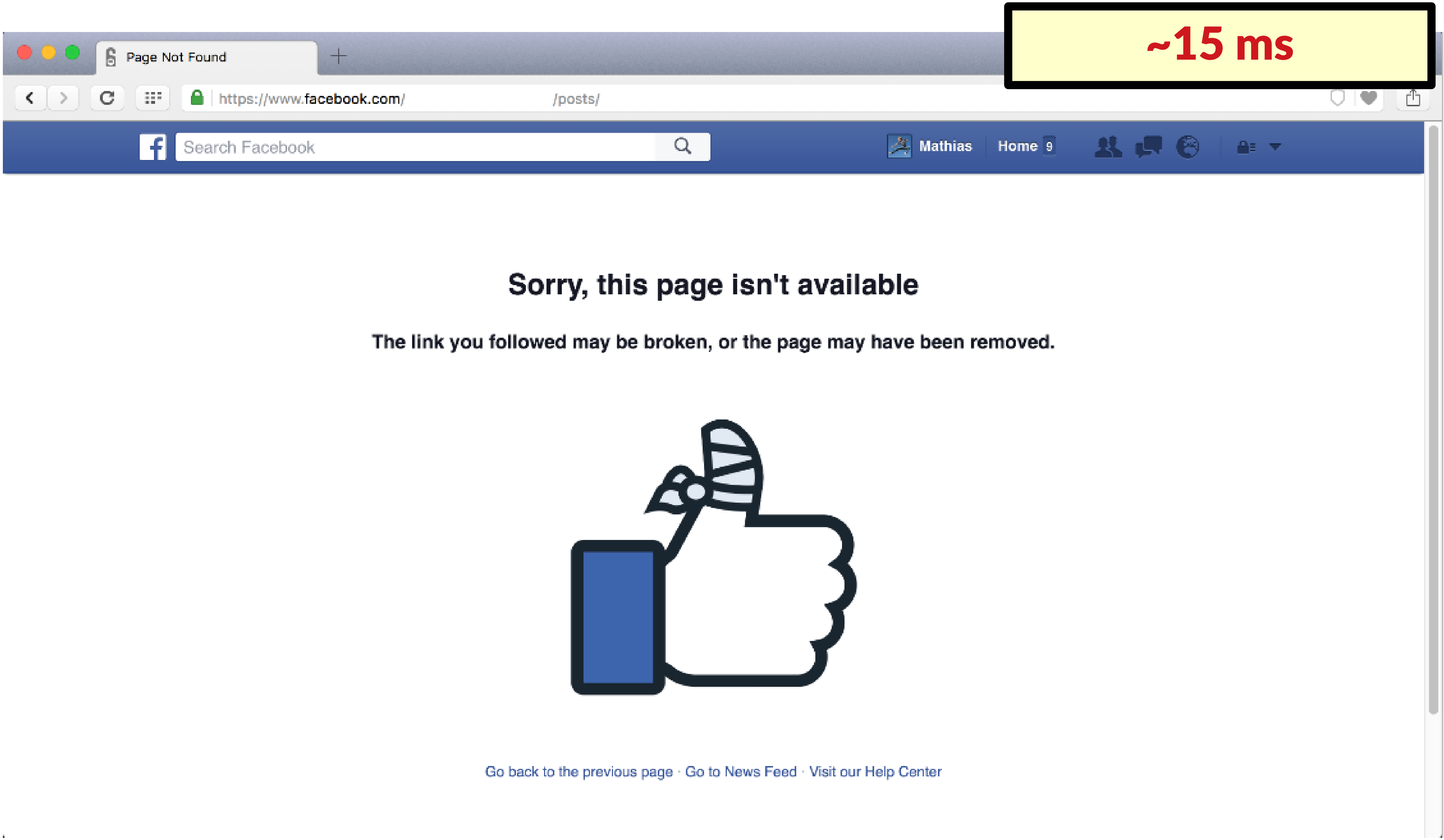
B.P Construct
228 people like this.
Like

VR Bouwafwerking
106 people like this.
Like

Feestcommissie Grembergen
Bram and 5 other friends like this.
Like

Ref: Front-End Performance The Dark Side @ ColdFront Conference 2016 (p52)

~15 ms

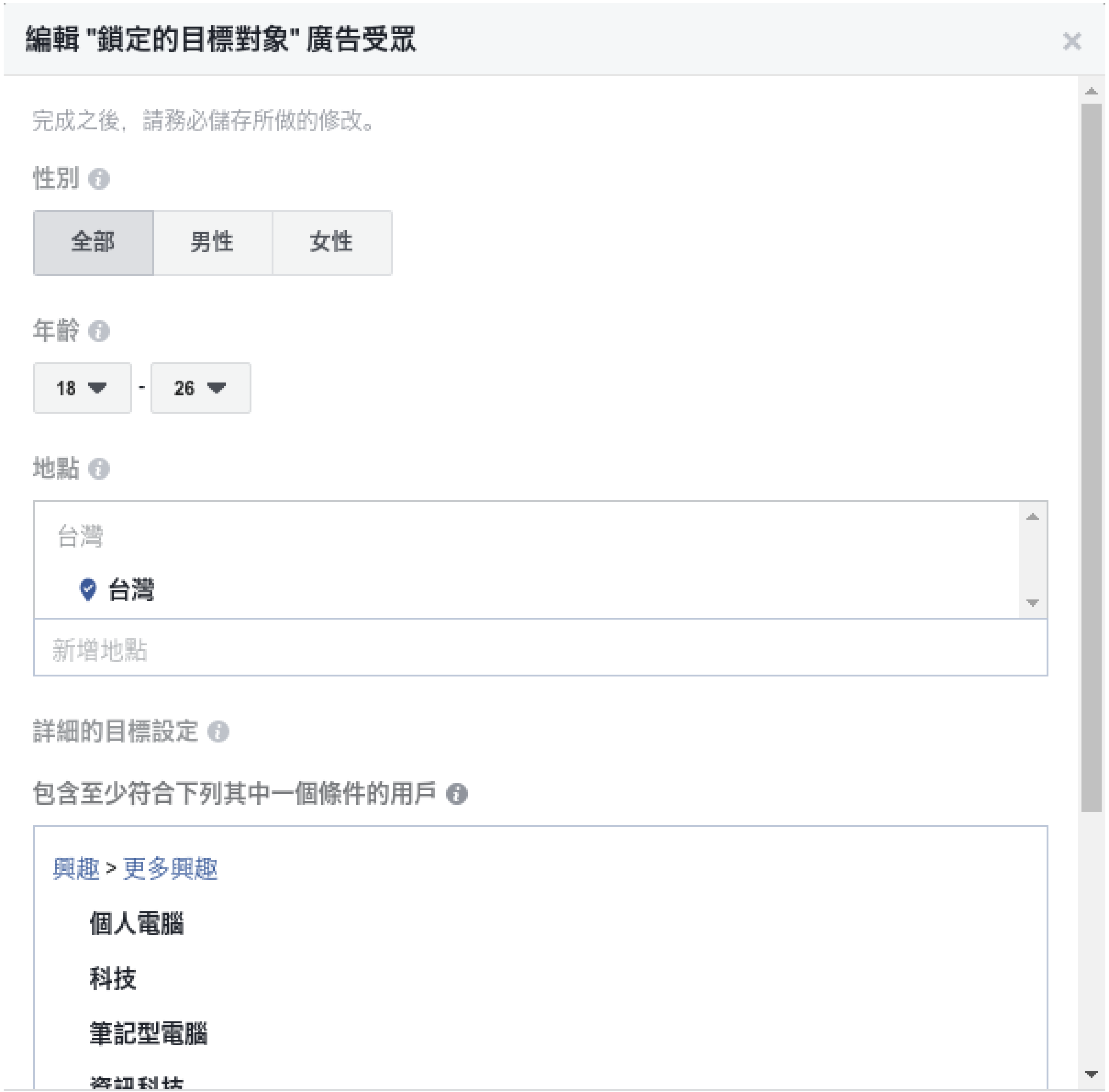


Sorry, this page isn't available

The link you followed may be broken, or the page may have been removed.

Go back to the previous page · Go to News Feed · Visit our Help Center

Ref: Front-End Performance The Dark Side @ ColdFront Conference 2016 (p54)



編輯 "鎖定的目標對象" 廣告受眾

完成之後，請務必儲存所做的修改。

性別

[✓ 全部] 男性 女性

年齡

18 - 26

地點

台灣

台灣

新增地點

詳細的目標設定

包含至少符合下列其中一個條件的用戶

興趣 > 更多興趣

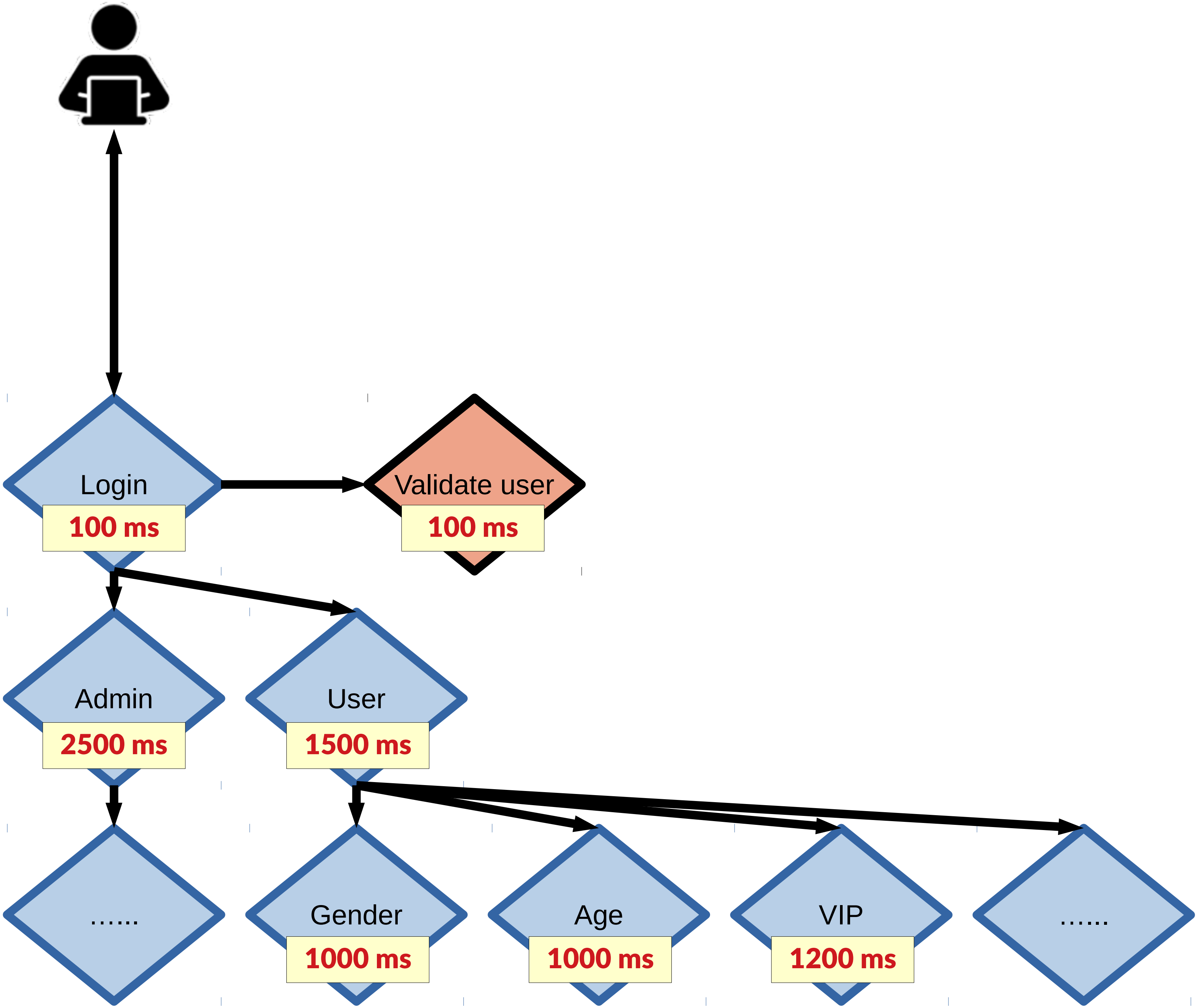
個人電腦

科技

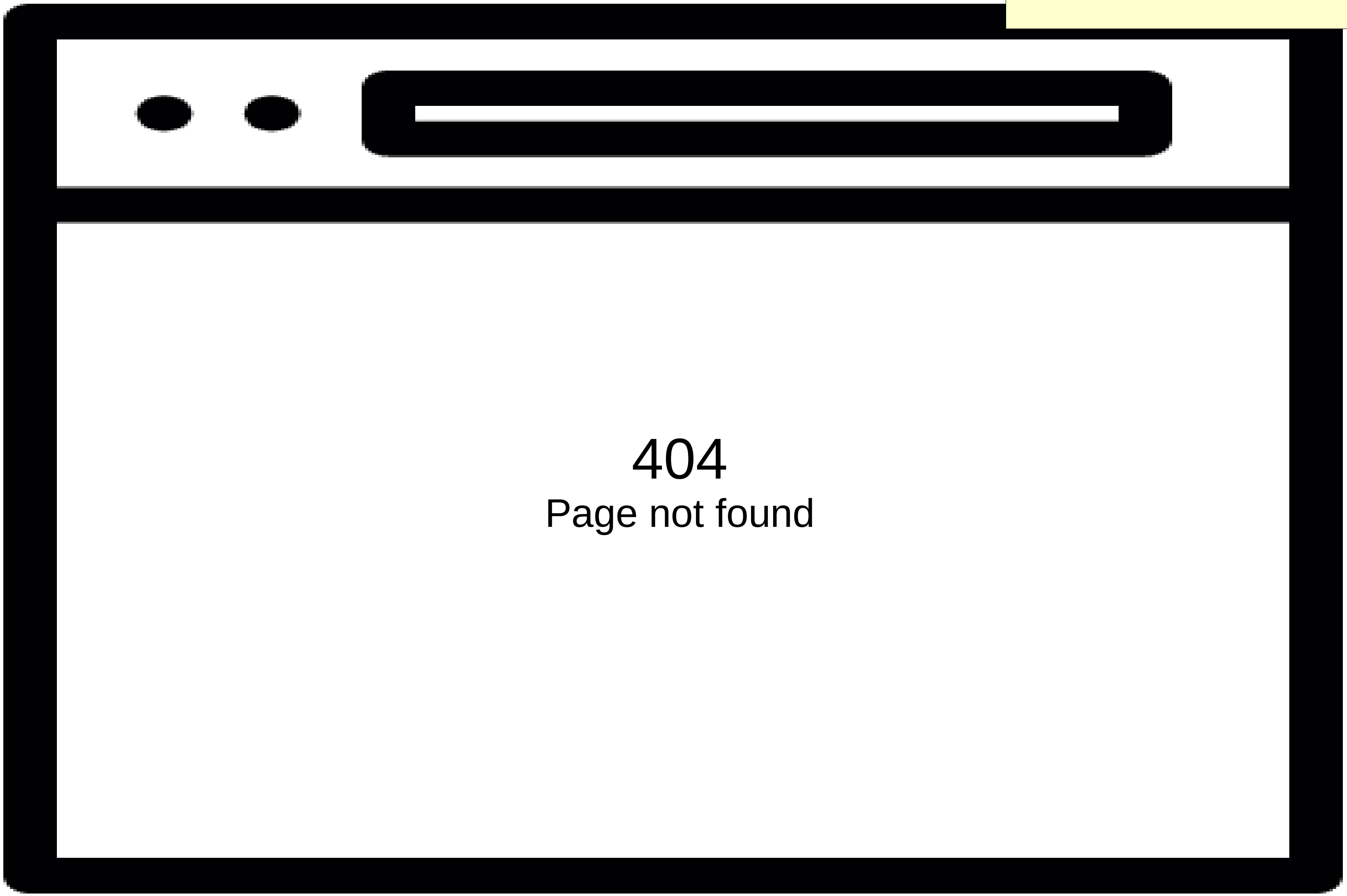
筆記型電腦

資訊科技

Ref: Front-End Performance The Dark Side @ ColdFront Conference 2016 (p50)

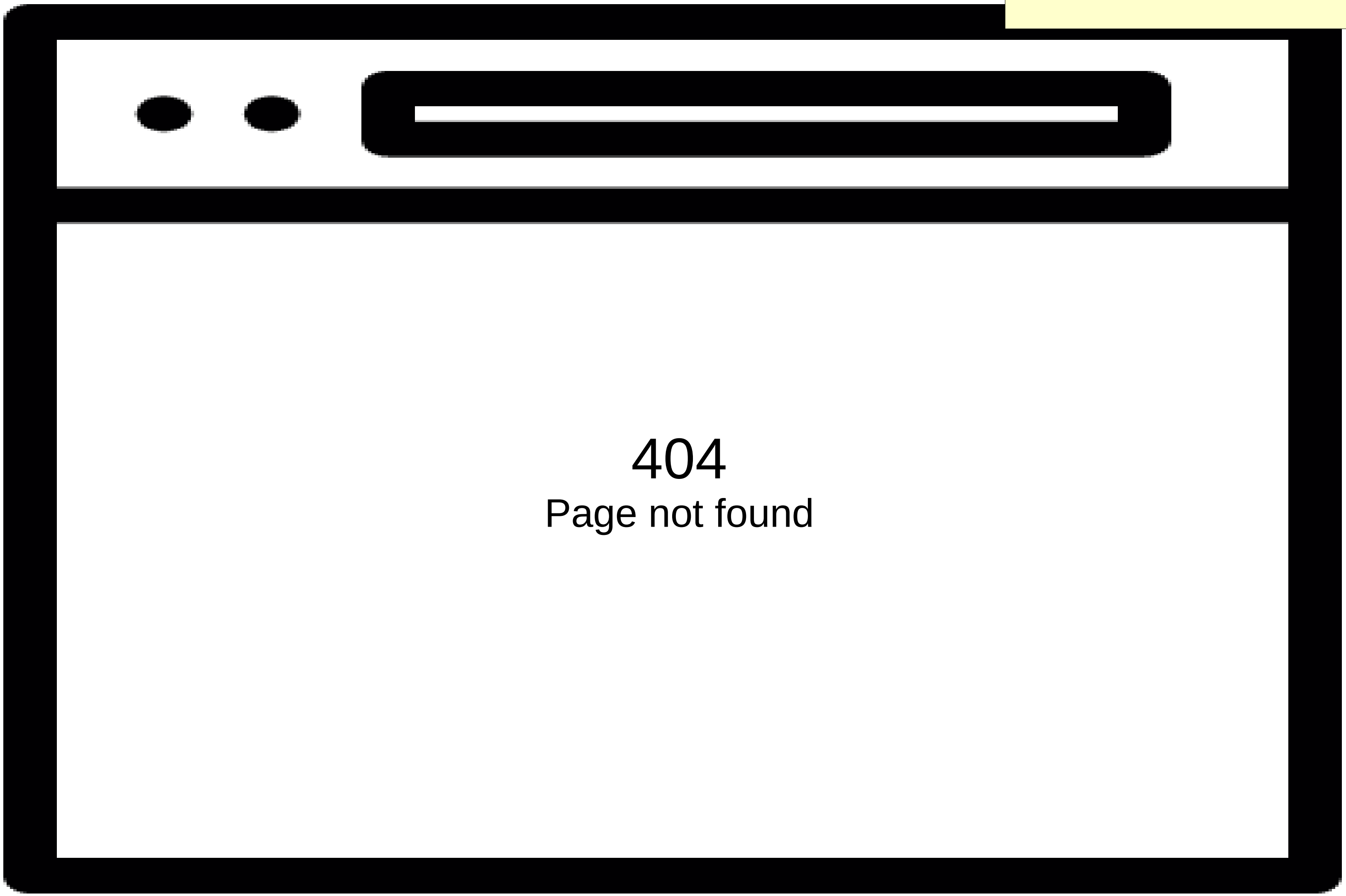

Login
100 ms
Validate user
100 ms
Admin
2500 ms
User
1500 ms
……
Gender
1000 ms
Age
1000 ms
VIP
1200 ms
……

~200 ms



404

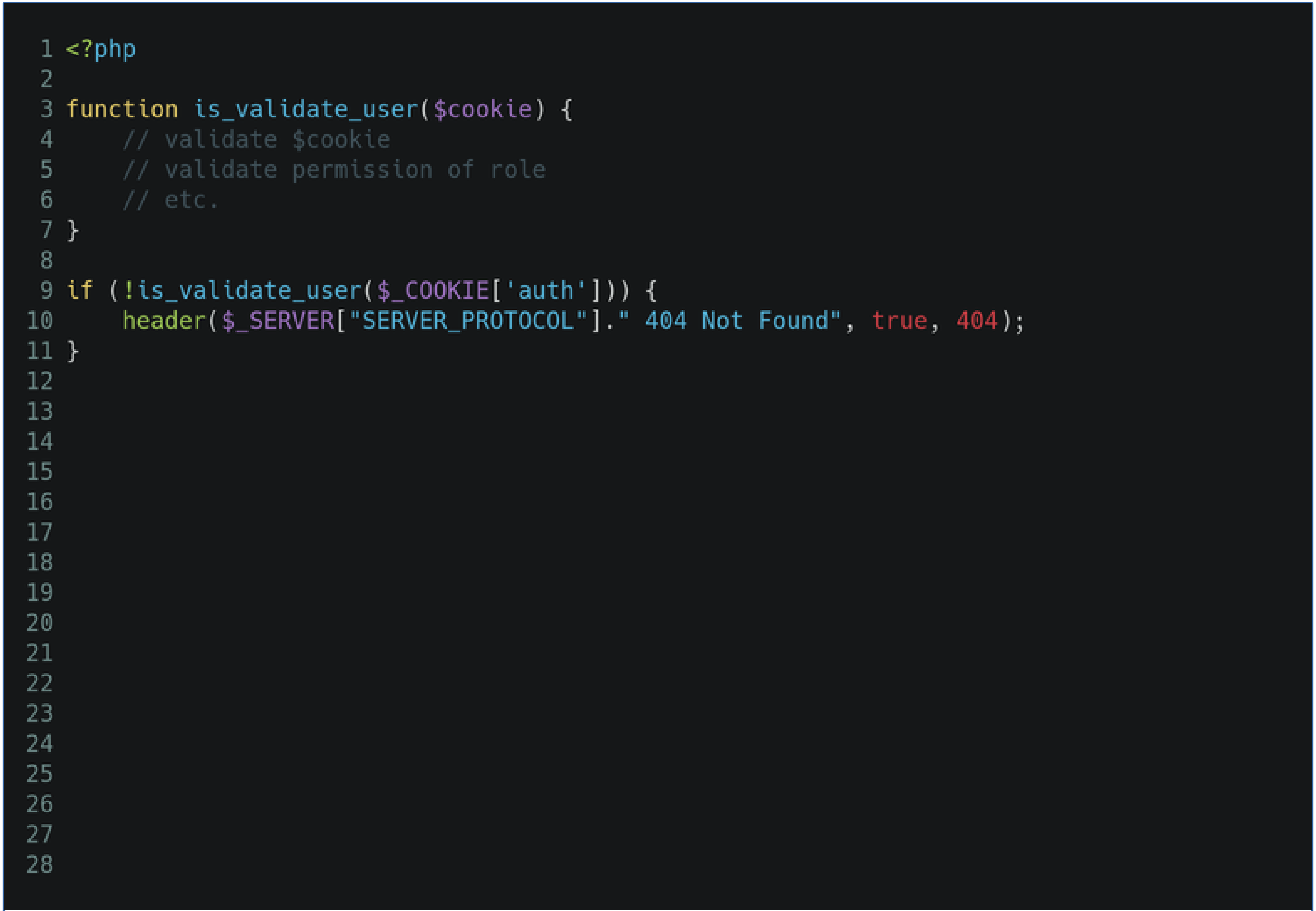
Page not found



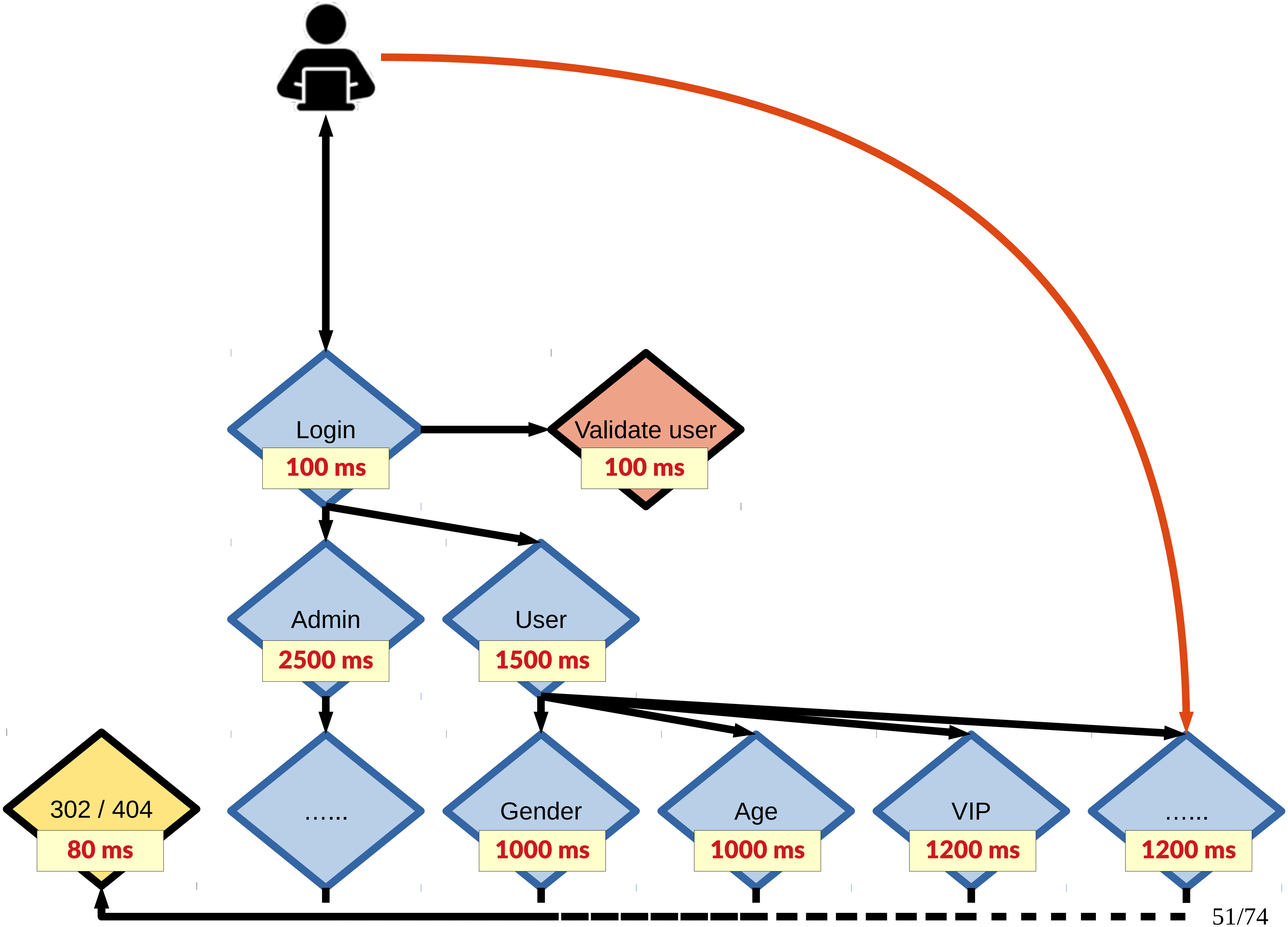
404

Page not found

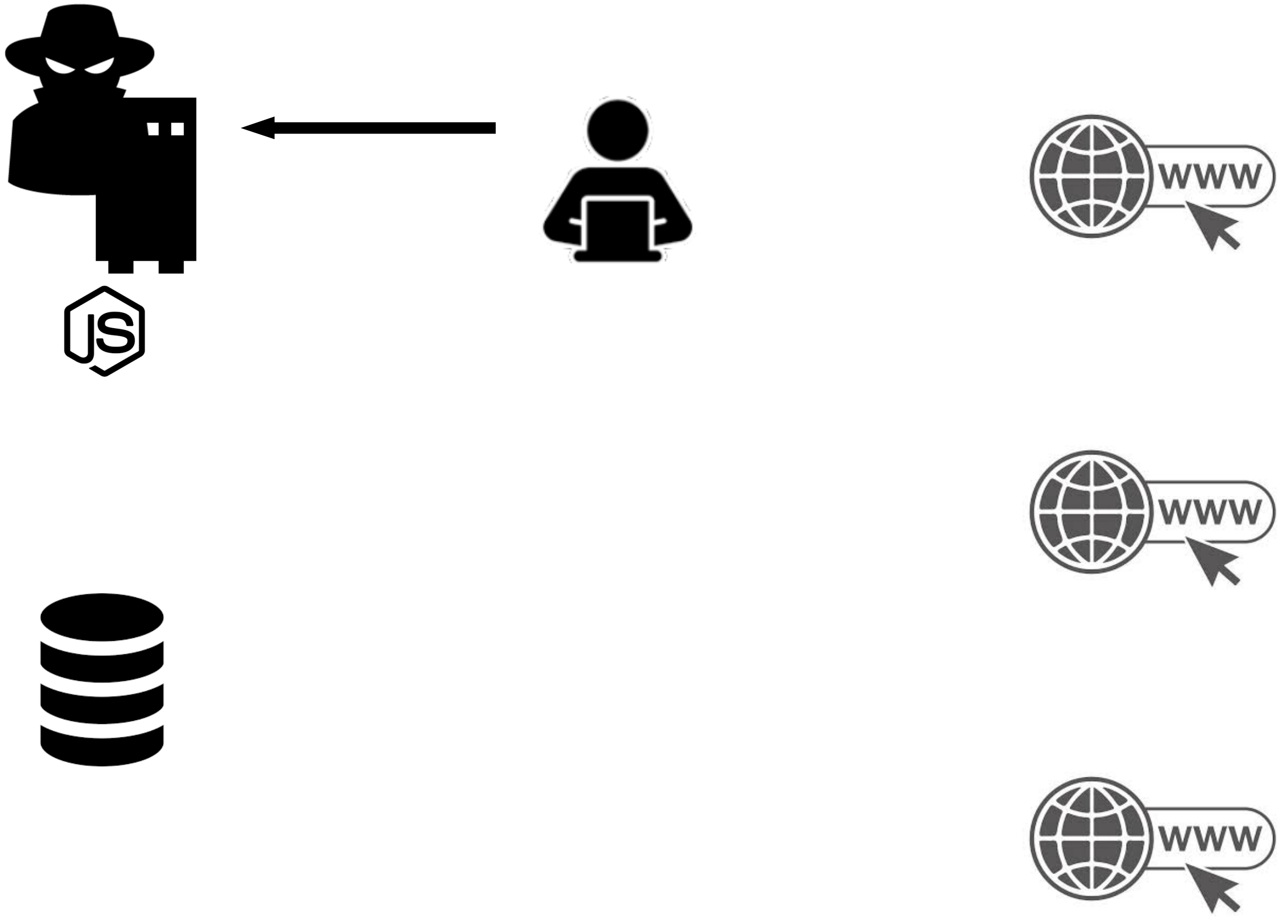
~80 ms

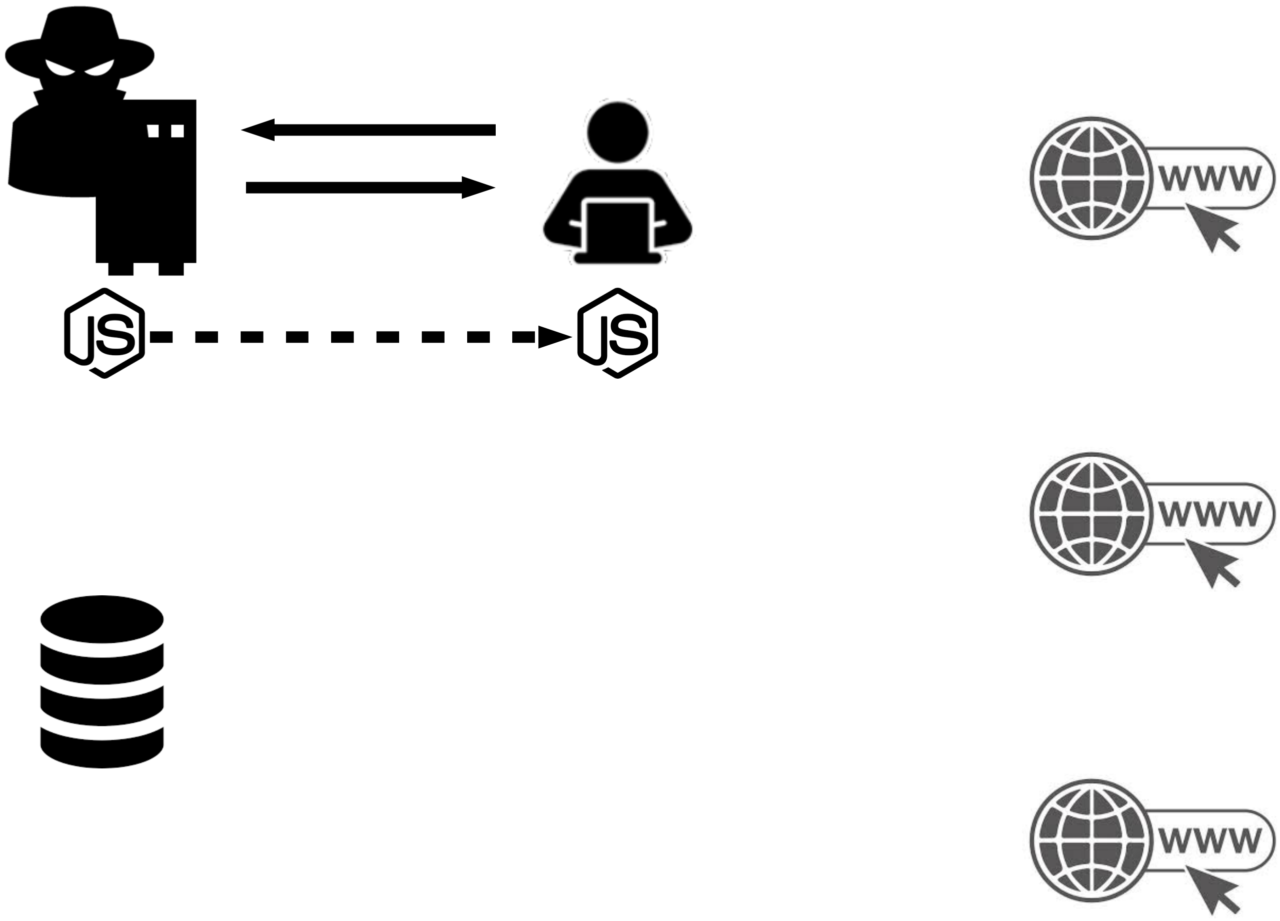


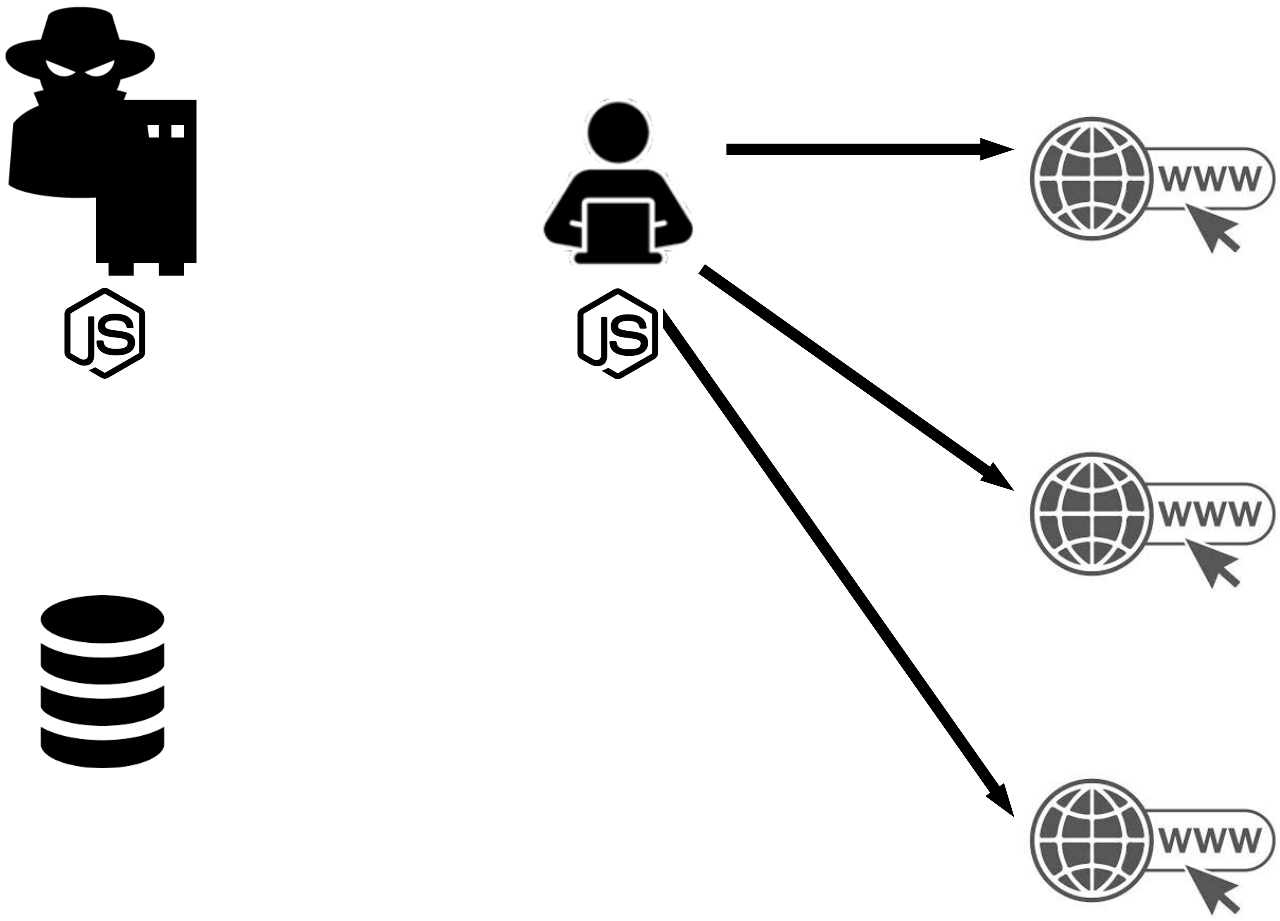
```php
<?php

function is_validate_user($cookie) {
    // validate $cookie
    // validate permission of role
    // etc.
}

if (!is_validate_user($_COOKIE['auth'])) {
    header($_SERVER["SERVER_PROTOCOL"]." 404 Not Found", true, 404);
}
```

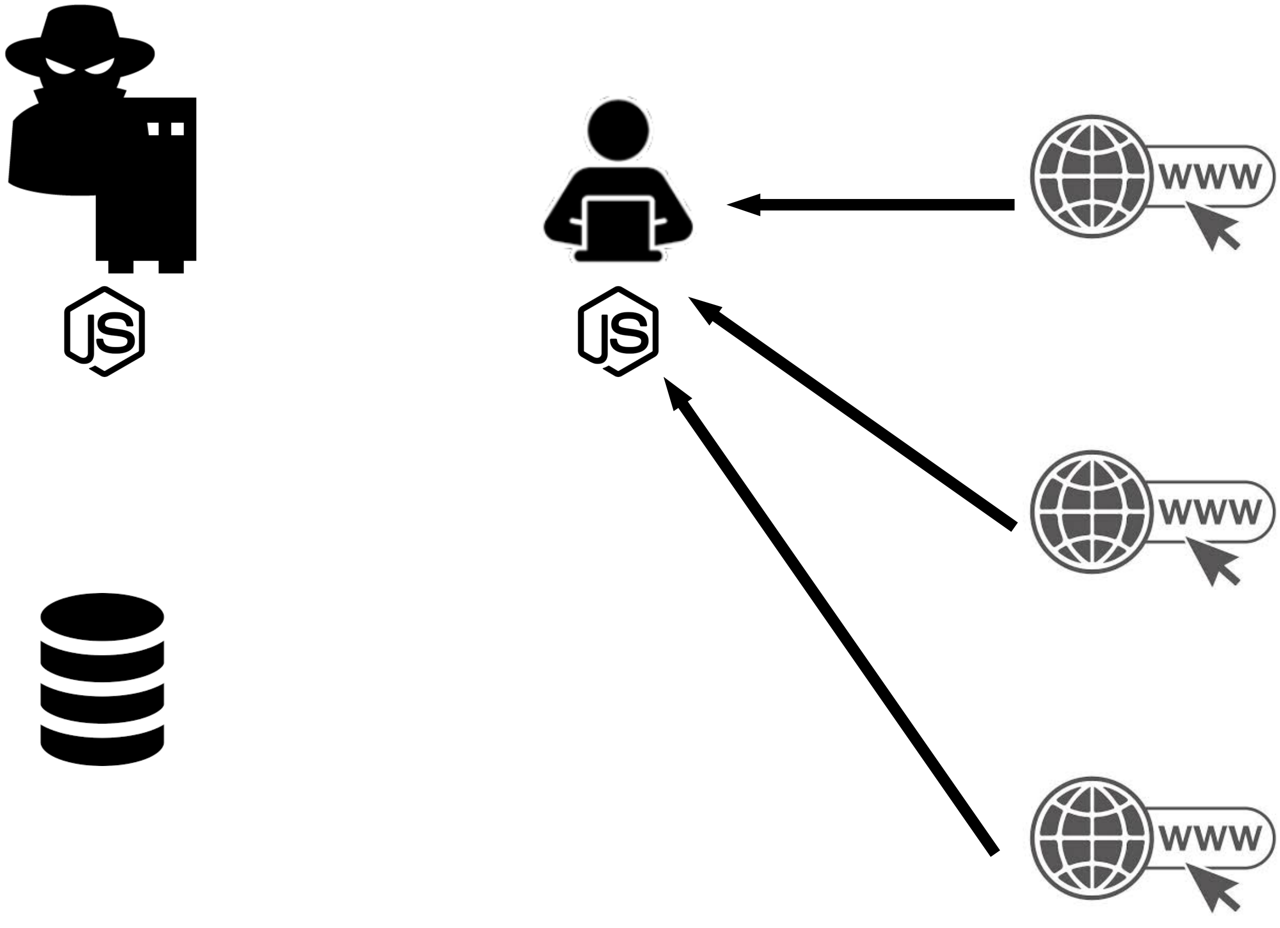

Login
100 ms
Validate user
100 ms
Admin
2500 ms
User
1500 ms
302 / 404
80 ms
……
Gender
1000 ms
Age
1000 ms
VIP
1200 ms
……
1200 ms

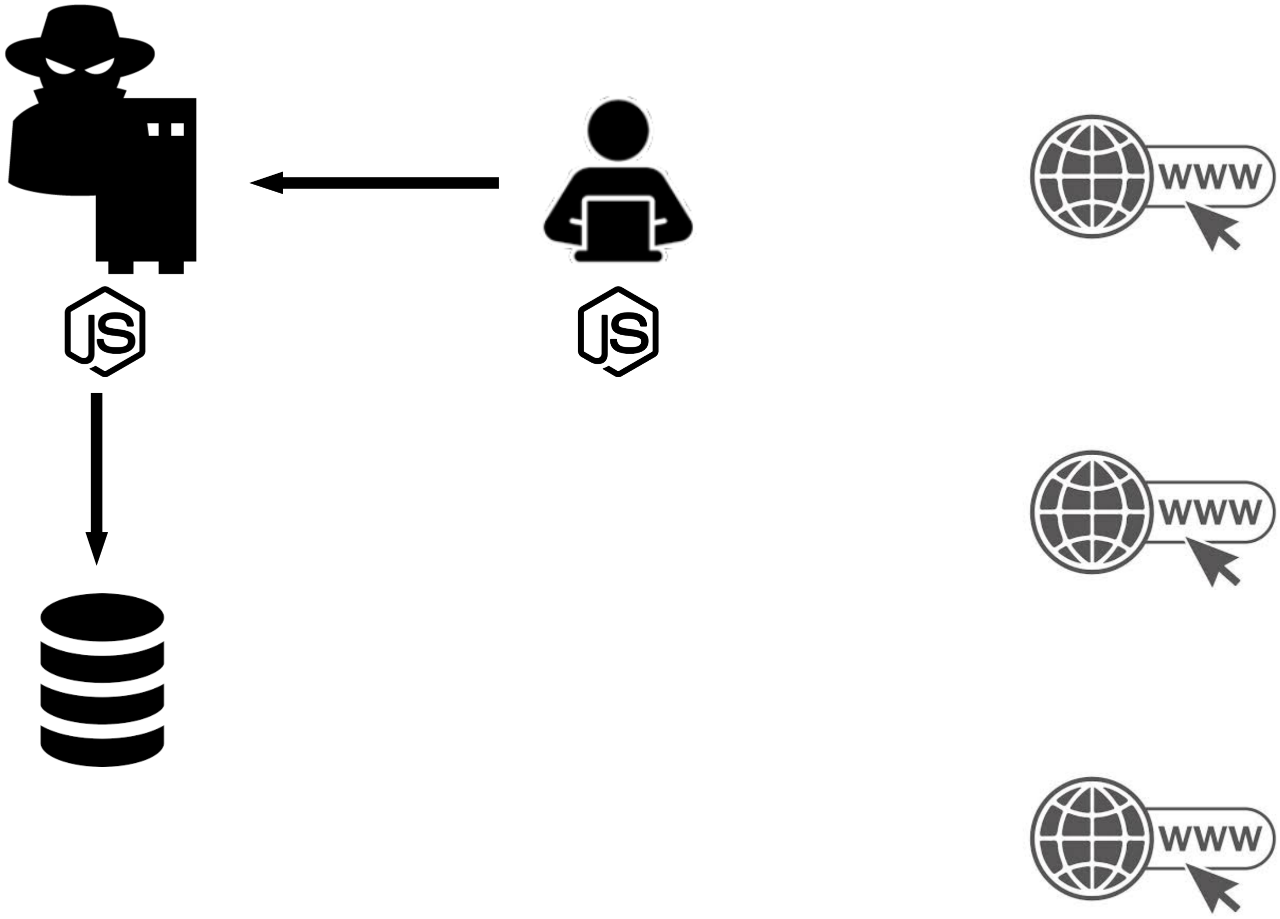
www
www
www

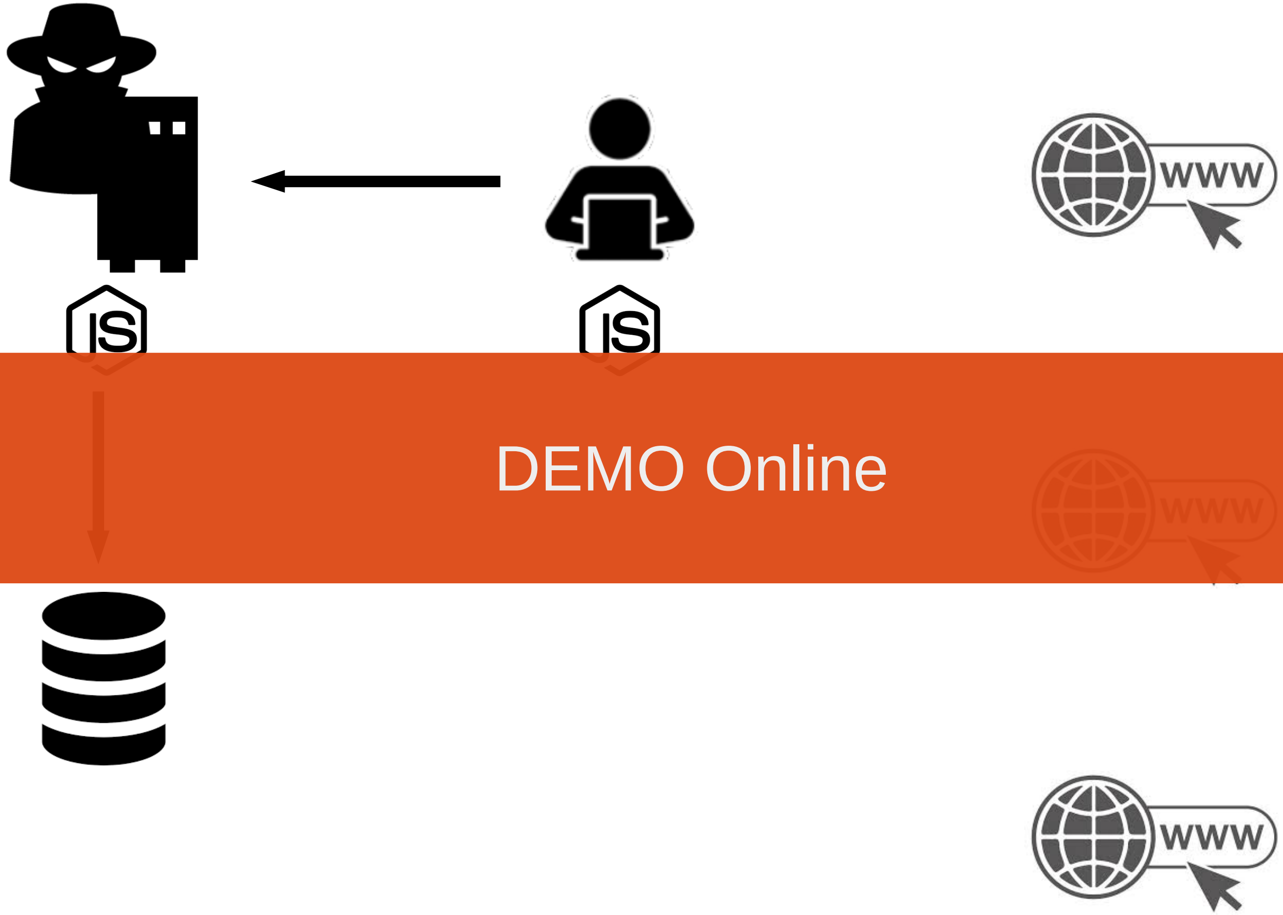

JS
www
www
www


JS
JS
www
www
www

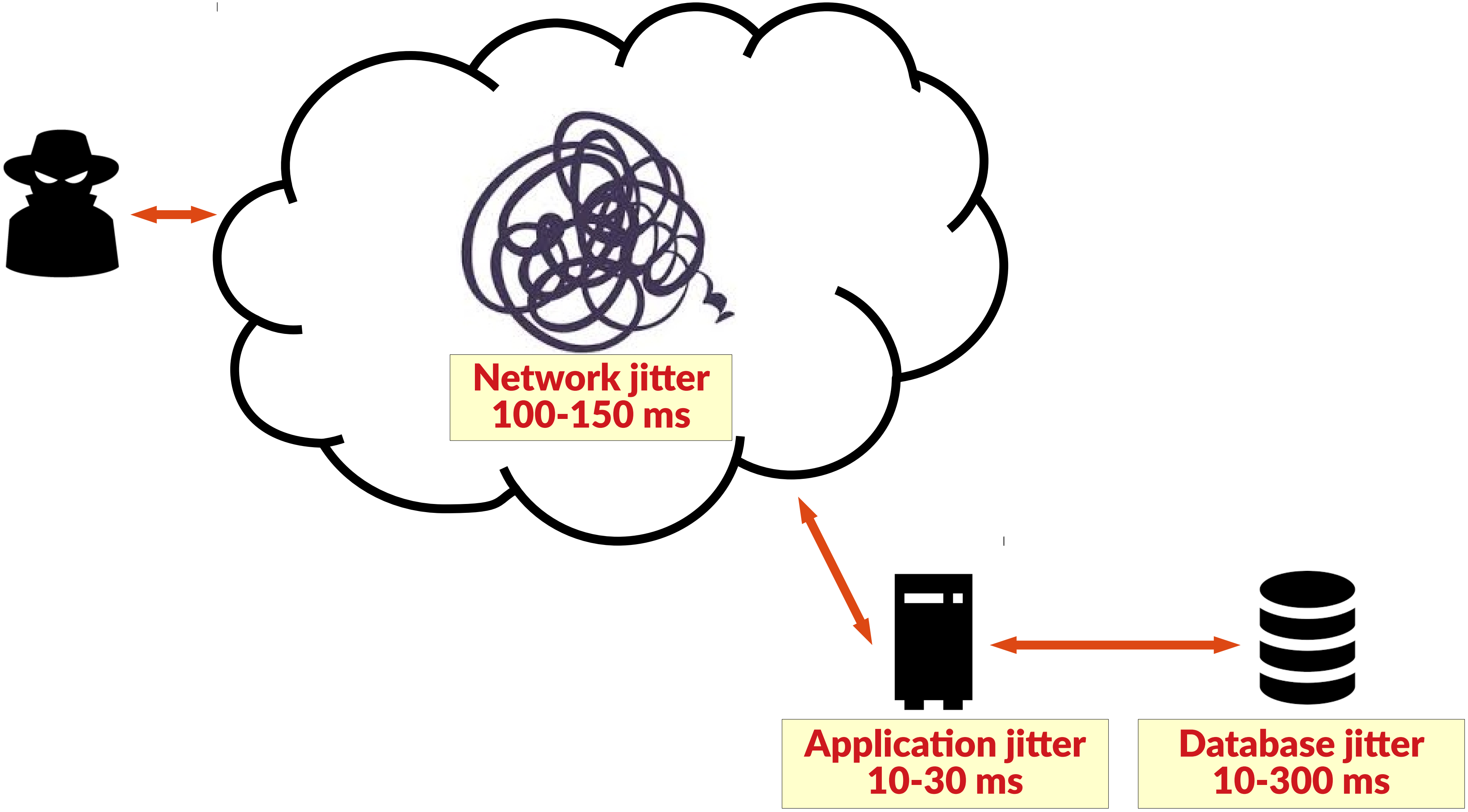

www
www
www


JS
JS
www
www
www


JS
JS
www
www
www



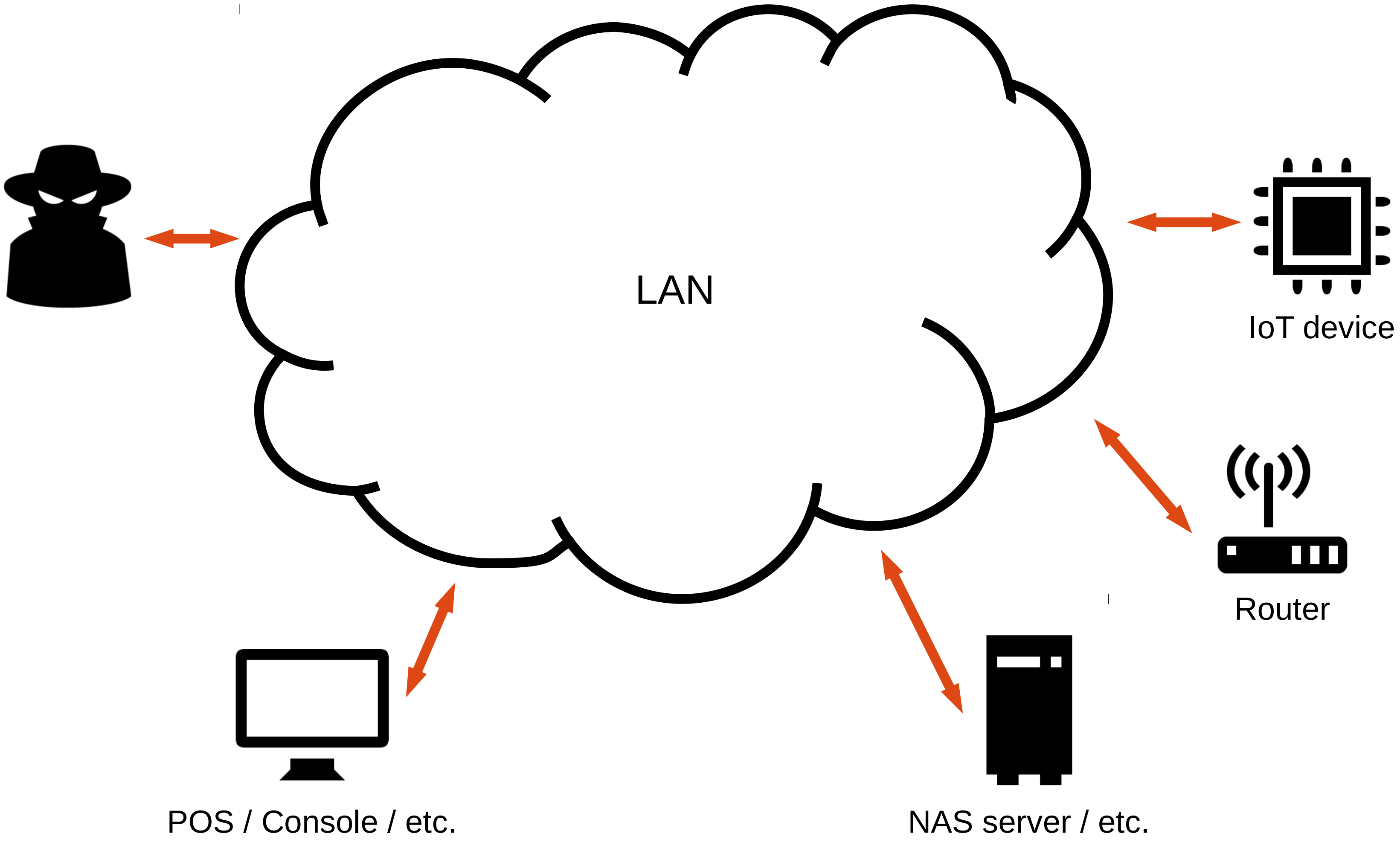
DEMO Online

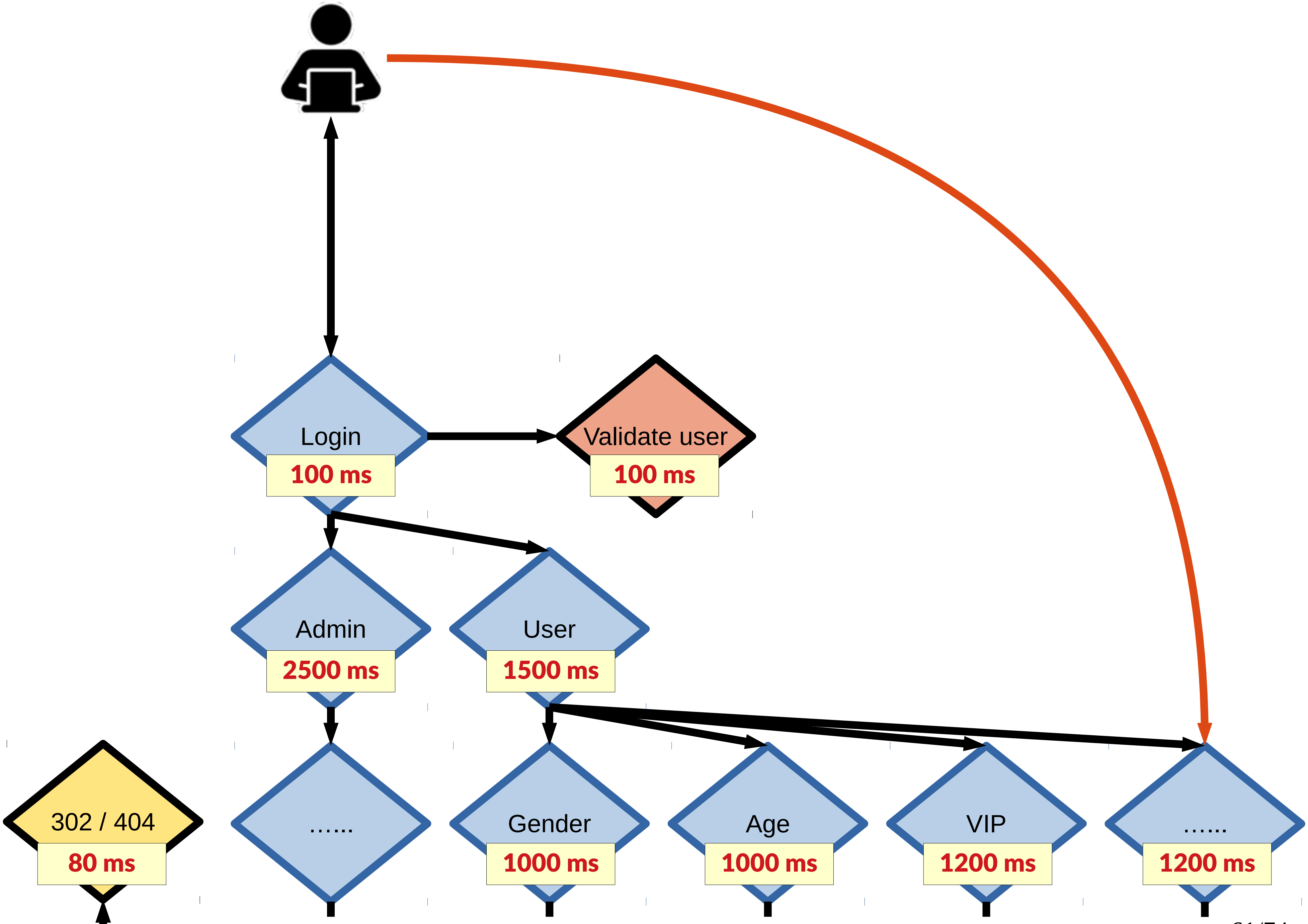


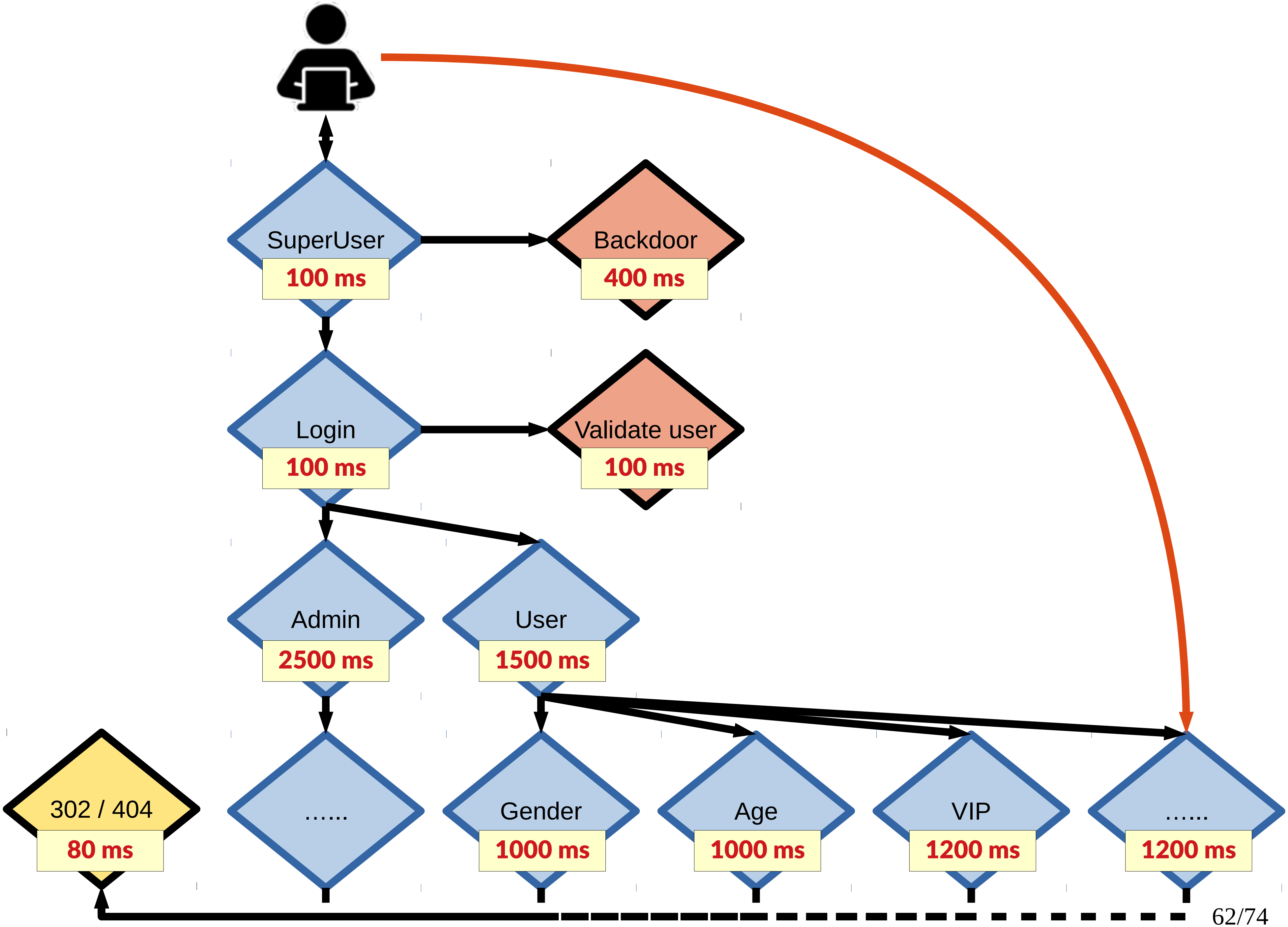
Network jitter
100-150 ms

Application jitter
10-30 ms

Database jitter
10-300 ms


LAN
IoT device
Router
POS / Console / etc.
NAS server / etc.


Login
100 ms
Validate user
100 ms
Admin
2500 ms
User
1500 ms
302 / 404
80 ms
……
Gender
1000 ms
Age
1000 ms
VIP
1200 ms
……
1200 ms



SuperUser
100 ms

Backdoor
400 ms

Login
100 ms

Validate user
100 ms

Admin
2500 ms

User
1500 ms

302 / 404
80 ms

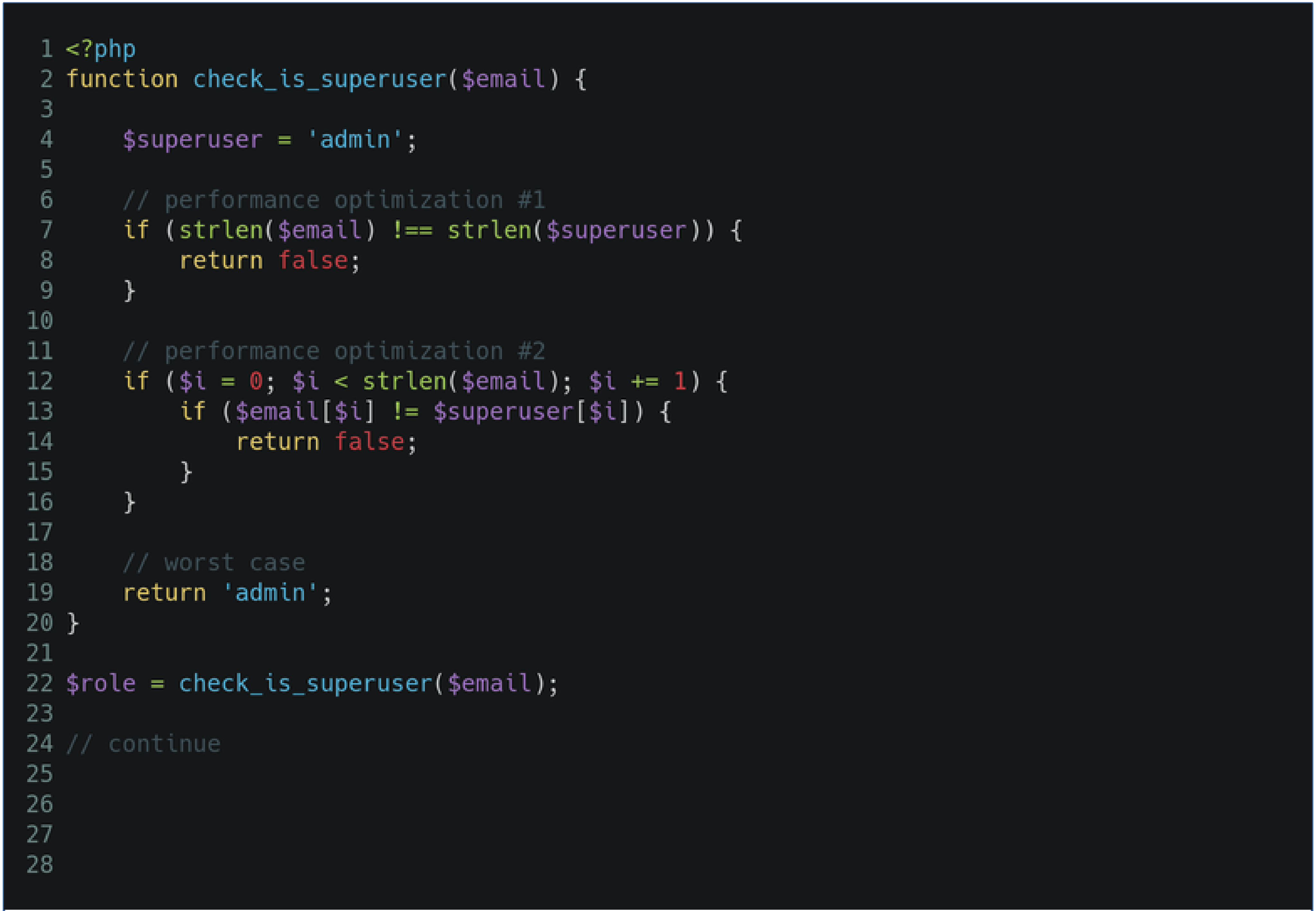
……

Gender
1000 ms

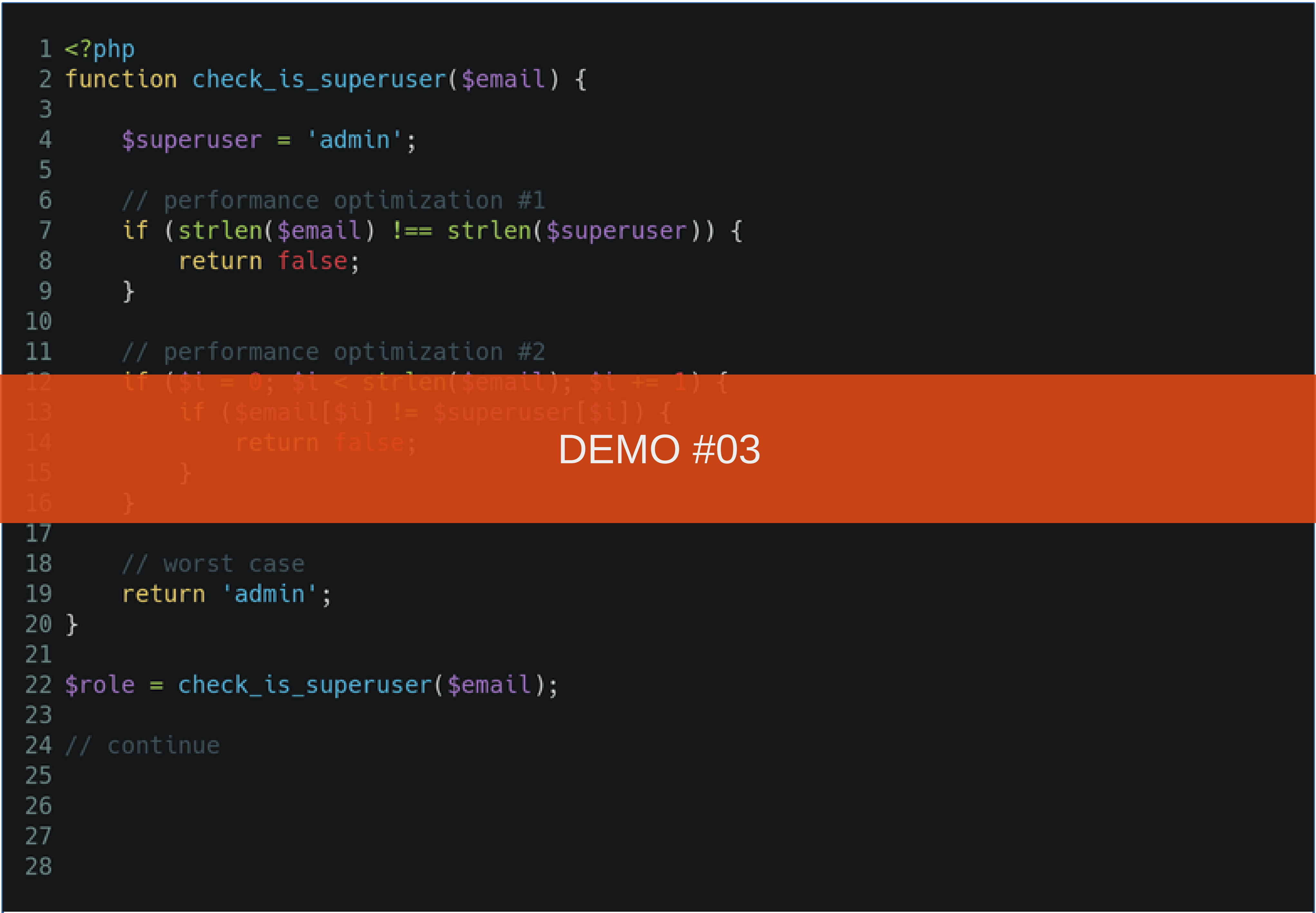
Age
1000 ms

VIP
1200 ms

……
1200 ms

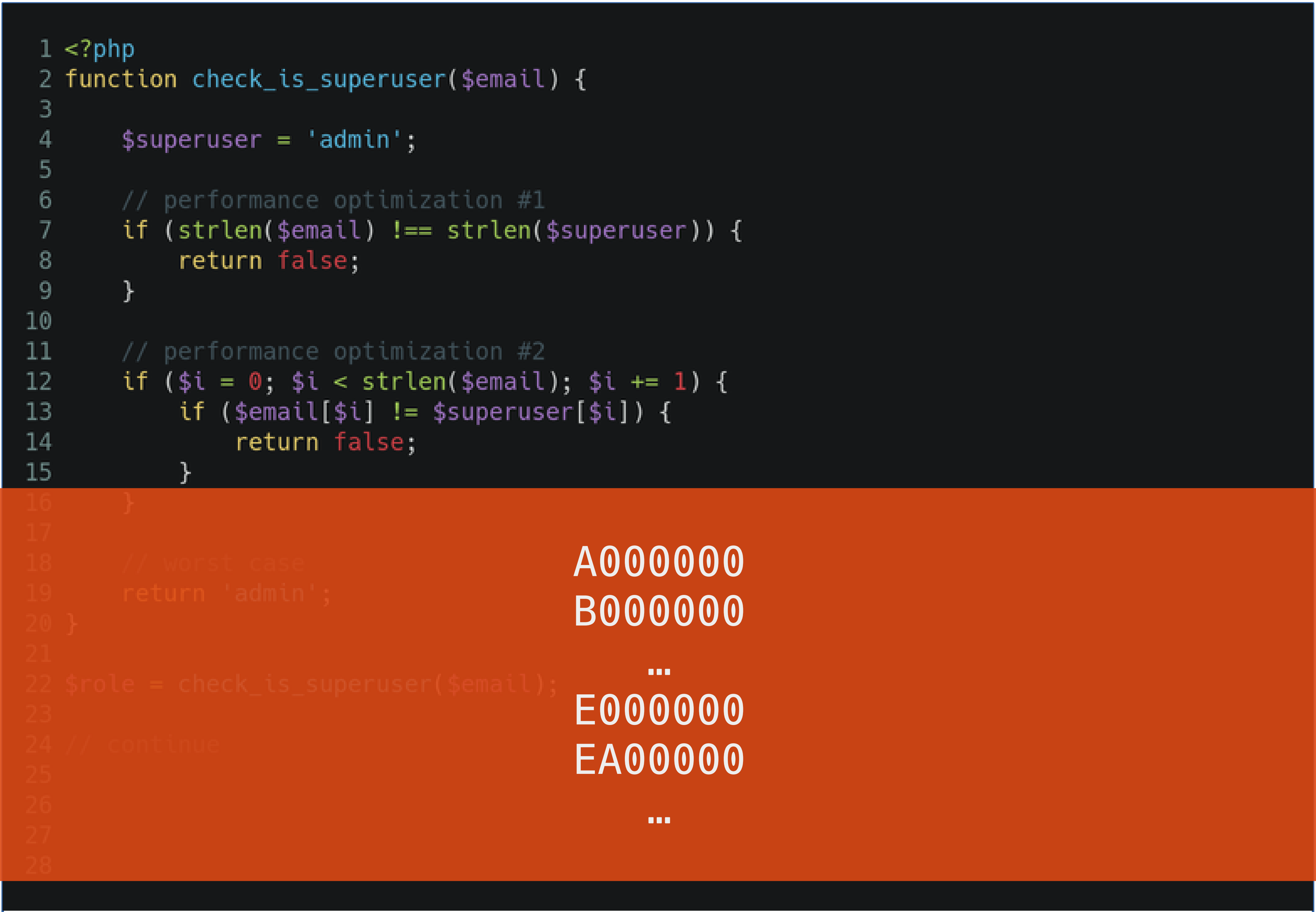


```php
<?php
function check_is_superuser($email) {

    $superuser = 'admin';

    // performance optimization #1
    if (strlen($email) !== strlen($superuser)) {
        return false;
    }

    // performance optimization #2
    if ($i = 0; $i < strlen($email); $i += 1) {
        if ($email[$i] != $superuser[$i]) {
            return false;
        }
    }

    // worst case
    return 'admin';
}

$role = check_is_superuser($email);

// continue
```



```php
<?php
function check_is_superuser($email) {

    $superuser = 'admin';

    // performance optimization #1
    if (strlen($email) !== strlen($superuser)) {
        return false;
    }

    // performance optimization #2
    if ($i = 0; $i < strlen($email); $i += 1) {
        if ($email[$i] != $superuser[$i]) {
            return false;
        }
    }

    // worst case
    return 'admin';
}

$role = check_is_superuser($email);

// continue
```

DEMO #03



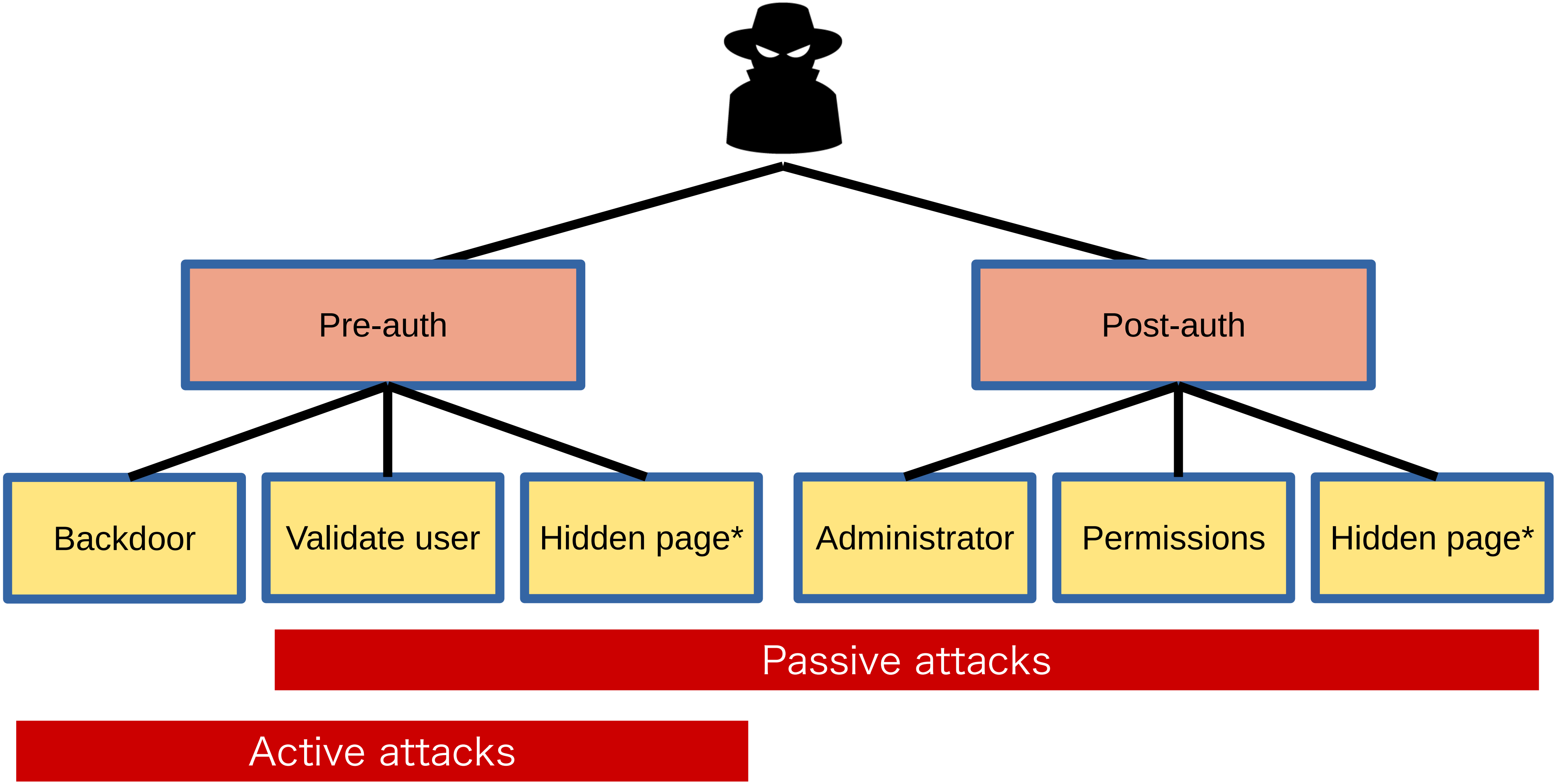
```php
<?php
function check_is_superuser($email) {

    $superuser = 'admin';

    // performance optimization #1
    if (strlen($email) !== strlen($superuser)) {
        return false;
    }

    // performance optimization #2
    if ($i = 0; $i < strlen($email); $i += 1) {
        if ($email[$i] != $superuser[$i]) {
            return false;
        }
    }

    // worst case
    return 'admin';
}

$role = check_is_superuser($email);

// continue
```

A000000
B000000
…
E000000
EA00000
…

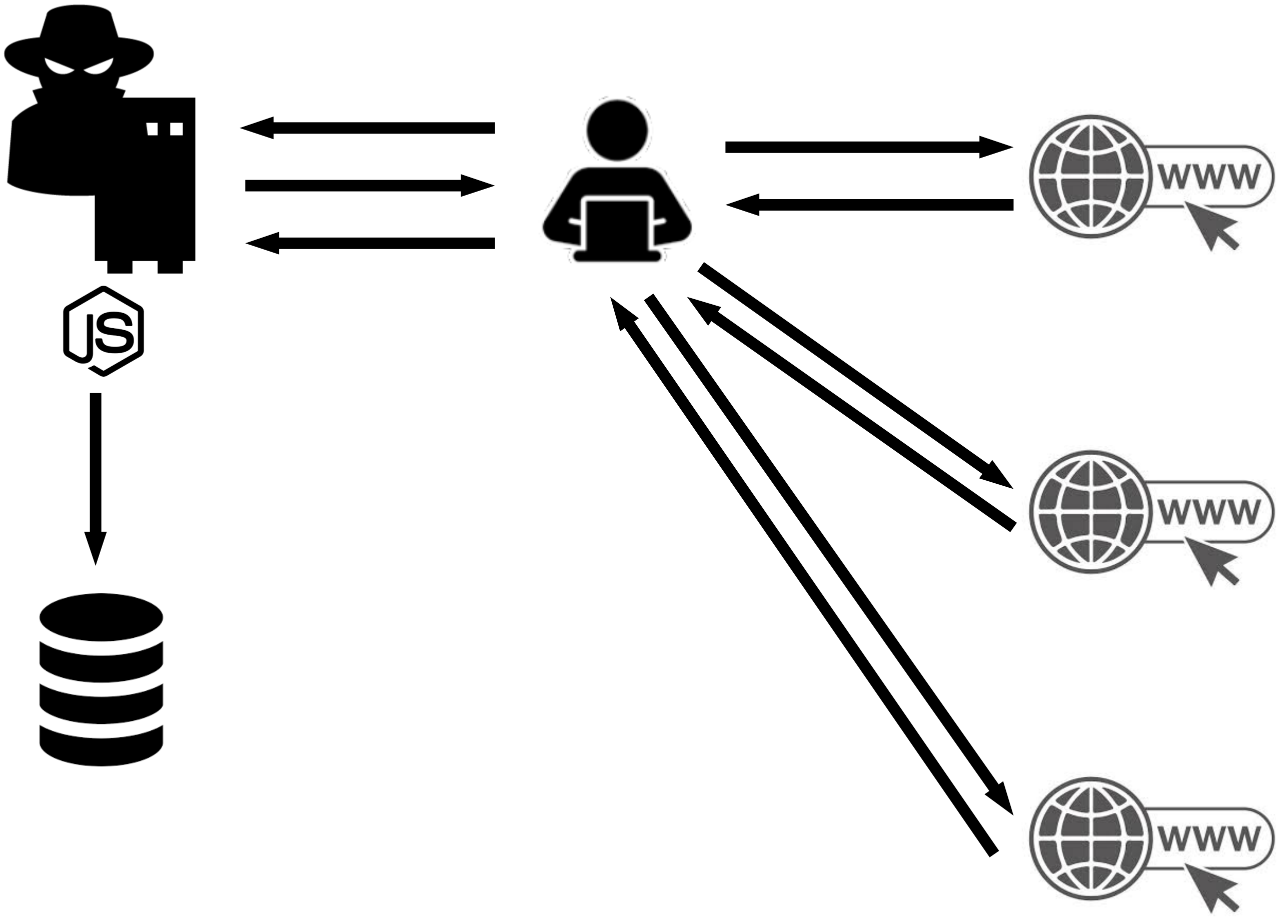
最佳化就像迴旋鏢，何時不小心回來打到你，可能也不知道

~ Ant ~

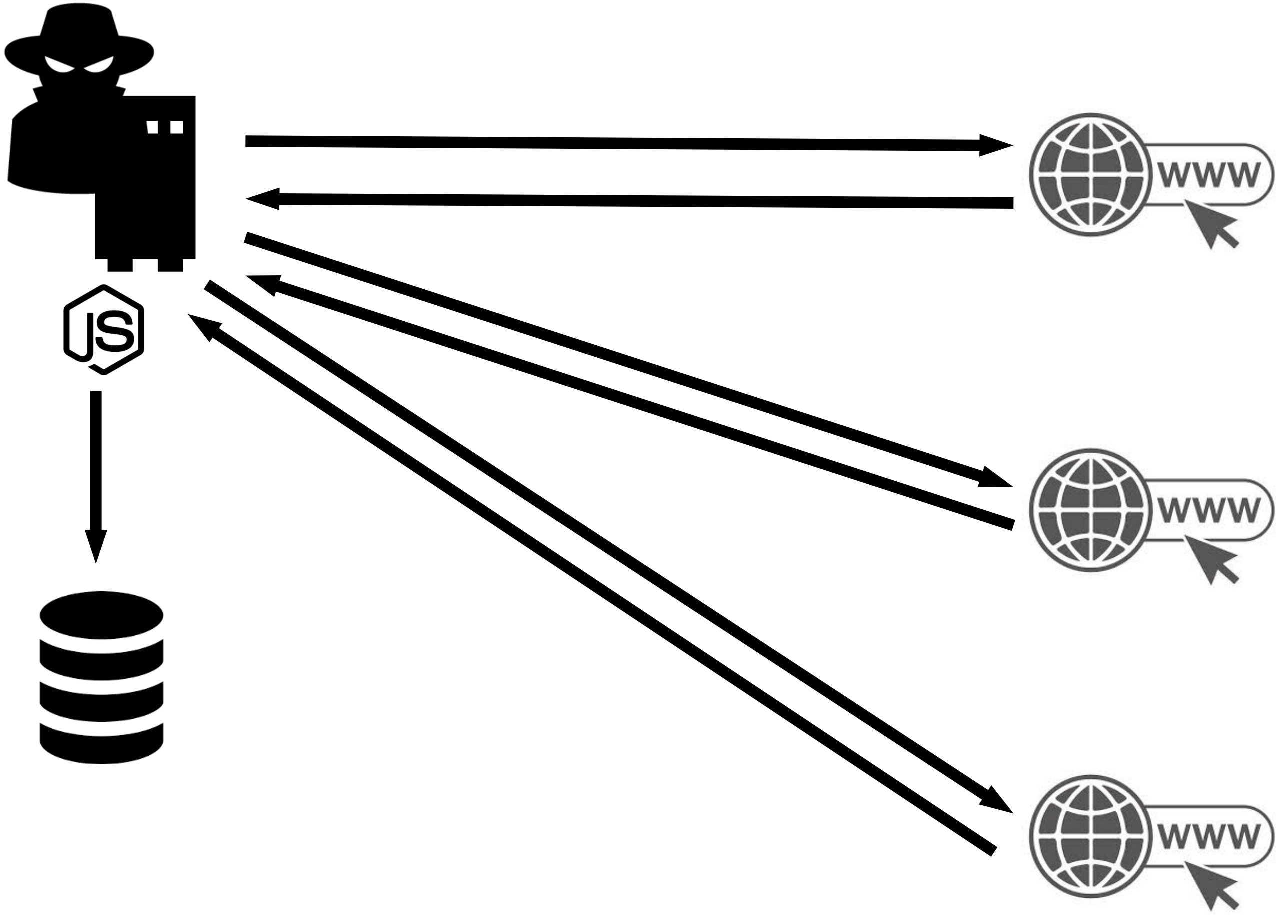
Attack Modes



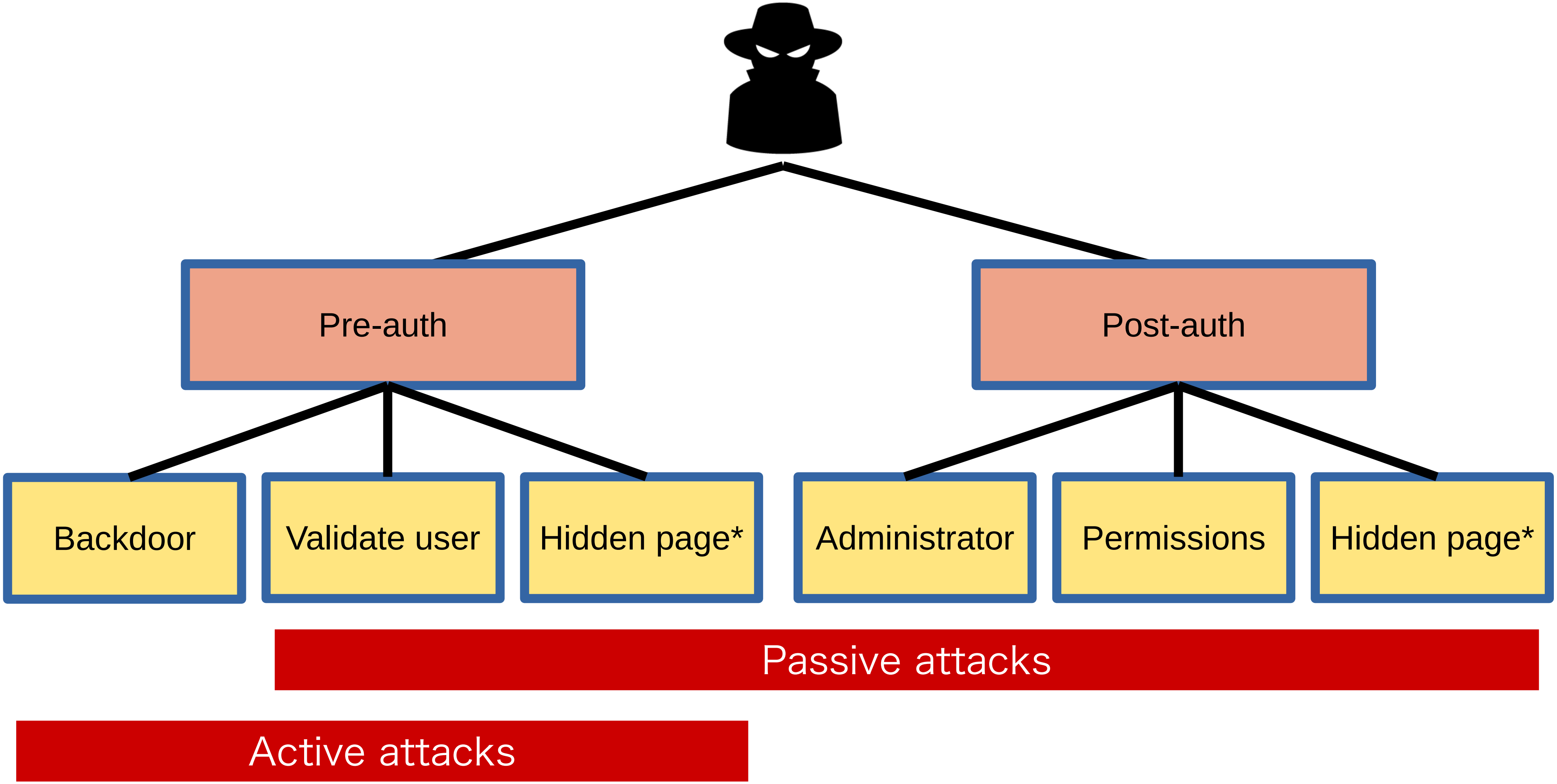
Passive attacks



Active attacks



Attack Modes



Pre-auth

Post-auth

Backdoor

Validate user

Hidden page*

Administrator

Permissions

Hidden page*

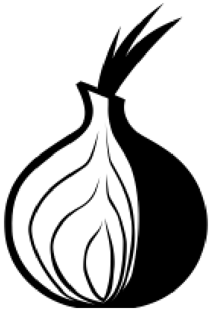
Passive attacks

Active attacks

password hash function ?

password hash function ?

DEMO #04



安全就像洋蔥，一片一片地剝開，總有一片會讓人流淚

~ Ant ~

ant@chroot.org / yftzeng@gmail.com

https://www.facebook.com/yftzeng.tw

https://twitter.com/yftzeng