



Workshop 3: Performance & Security

Hay là sự thật phũ phàng mà có thể bạn đã biết

HÔM NAY TA NÓI VỀ CÁI GÌ

- Vài chuyện nhỏ về hiệu suất và bảo mật
- Tư duy như 1 hacker
- Nhìn lại & Tổng kết khóa học

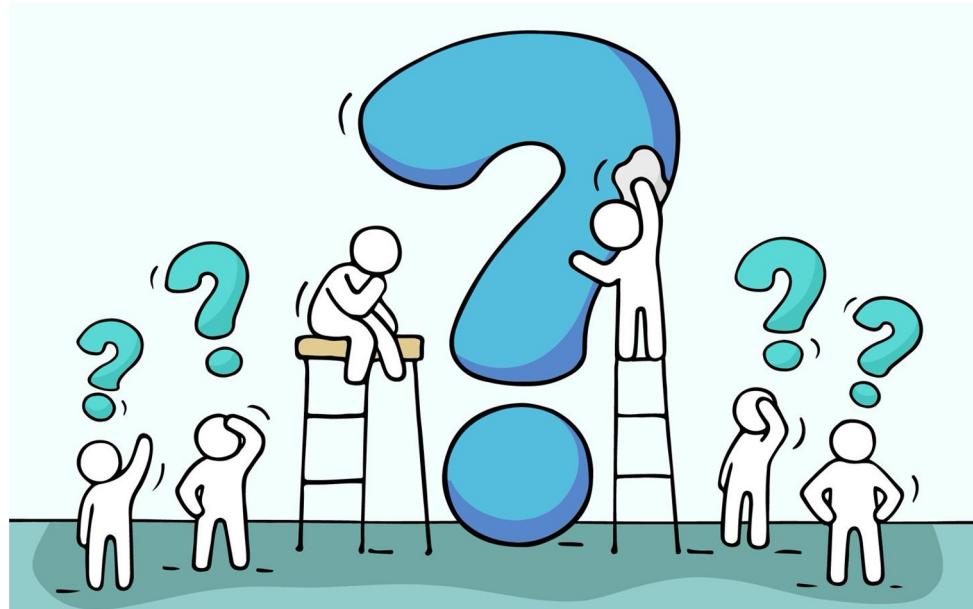


Tự vấn

- Sản phẩm bạn làm đã bao giờ bị hack, lộ thông tin hay chưa?
- Bạn đã bao giờ bị phàn nàn rằng sản phẩm này hiệu suất thấp, tốn tiền server chưa?

Câu hỏi?

1. Nếu 1 website quản lý thông tin sinh viên, bị lộ tài khoản của các sinh viên khác?
2. Nếu 1 website ngân hàng bị lộ thông tin dự thưởng của 1 số khách hàng?
3. 1 con CMS có 1 nhúm user, chạy server 4GB Ram DEV vẫn kêu yếu



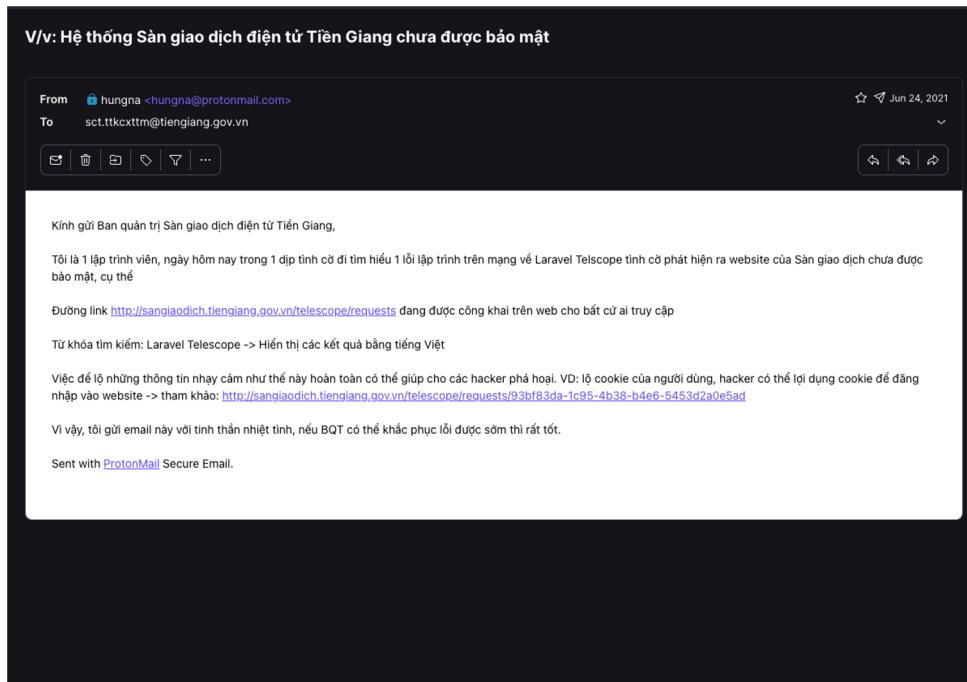
Câu chuyện bảo mật

Câu chuyện về tính
năng login và ca OT
tới 12h đêm của
team CSKH tại đây

```
[80][http-get-form] host: 192.168.100.155 login: admin password: password
[80][http-get-form] host: 192.168.100.155 login: admin password: p@ssword
[80][http-get-form] host: 192.168.100.155 login: admin password: 12345
[80][http-get-form] host: 192.168.100.155 login: admin password: 1234567890
[80][http-get-form] host: 192.168.100.155 login: admin password: Password
[80][http-get-form] host: 192.168.100.155 login: admin password: 123456
[80][http-get-form] host: 192.168.100.155 login: admin password: 1234567
[80][http-get-form] host: 192.168.100.155 login: admin password: 12345678
[80][http-get-form] host: 192.168.100.155 login: admin password: 1q2w3e4r
[80][http-get-form] host: 192.168.100.155 login: admin password: 123
[80][http-get-form] host: 192.168.100.155 login: admin password: 1
[80][http-get-form] host: 192.168.100.155 login: admin password: 12
1 of 1 target successfully completed, 12 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-07-27 15:28:24
```

Ví dụ nhẹ về lỗi bảo mật

Thử khai thác lỗi
bảo mật với
WordPress, Laravel
bằng ...
Google.com.vn



Ví dụ nhẹ Performance

Chính nó, con server
4gb ram - 4CPU -
50GB SSD nhưng
gánh còng lưng con
CMS nhỏ với 1 ít
user

```
root@nakajima:~# top
Tasks: 46, 49 Hr: 2 running
Load average: 0.00 0.01 0.05
Uptime: 620 days(1), 23:24:23
Mem: 3474M/4,000M
Swap: 0K/0K

PID  USER  PR  NI  VIRT  RES  SHR  S% CPU% MEM% TIME+  Command
1 root      0  0  180M 3484 2188 S  0.0  0.1 48:26.19 /usr/lib/systemd/system --switched-root --system --deserialize 22
21976 root      20  0 337M 6494 4392 S  0.0  0.1 81:00.00 /usr/bin/abrt-dbus +133
21969 root      20  0 337M 6494 4392 S  0.0  0.2 81:00.00 ~ /usr/bin/abrt-dbus +133
21979 root      20  0 337M 6494 4392 S  0.0  0.2 0:00.00 ~ /usr/bin/abrt-dbus +133
21978 root      20  0 337M 6494 4392 S  0.0  0.2 0:00.00 ~ /usr/bin/abrt-dbus +133
12820 nginx     20  0 4932 2828 1228 S  0.0  0.1 9:09.17 nginx: worker process
12786 root      20  0 544M 9847 30104 S  0.0  0.6 1:05.65 php-fpm: master process (/etc/php-fpm.conf)
16338 apache    20  0 538M 3232 3504 S  0.0  1.3 2:02.25 php-fpm: pool www
16339 apache    20  0 538M 3232 3504 S  0.0  1.3 2:02.25 php-fpm: pool www
12817 apache    20  0 646M 35248 35248 S  0.0  1.4 3:43.70 php-fpm: pool www
12791 apache    20  0 558M 4888 38349 S  0.0  1.2 2:07.56 php-fpm: pool www
12787 apache    20  0 642M 7356 7116 S  0.0  1.4 2:07.56 php-fpm: pool www
12789 apache    20  0 558M 10444 40716 S  0.0  1.5 2:32.02 php-fpm: pool www
12788 apache    20  0 641M 7356 7116 S  0.0  1.4 3:26.83 php-fpm: pool www
12787 apache    20  0 642M 52236 49149 S  0.0  1.4 4:18.53 php-fpm: pool www
16337 apache    20  0 558M 10444 40716 S  0.0  1.5 2:32.02 php-fpm: pool www
1252 root       20  0 2576 988 892 S  0.0  0.0 2:10.20 /usr/libexec/postfix/master -w
16474 postfix    0  0 7260 4212 3108 S  0.0  0.1 0:08.01 pickup -l -t unix -u
12529 mysql     20  0 1936M 233M 1052 S  0.0  0.0 2:10.20 /usr/bin/python2 -s /usr/bin/fail2ban-server -s /var/run/fail2ban/fail2ban.sock -p /var/run/fail2ban/fail2ban.pid -x -b
1231 root       20  0 2014M 1413M 5532 S  0.0  35.8 23:34:24 /usr/bin/python2 -s /usr/bin/fail2ban-server -s /var/run/fail2ban/fail2ban.sock -p /var/run/fail2ban/fail2ban.pid -x -b
1230 root       20  0 2014M 1413M 5532 S  0.0  35.8 4:04:47 /bin/bash
1231 root       20  0 2014M 1413M 5532 S  0.0  35.8 23:34:24 /usr/bin/python2 -s /usr/bin/fail2ban-server -s /var/run/fail2ban/fail2ban.sock -p /var/run/fail2ban/fail2ban.pid -x -b
1262 mysql     20  0 1936M 233M 3094 S  0.0  5.0 10:26:37 /usr/sbin/mysql --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib64/mysql --log-error=/var/log/mysql
28582 mysql     20  0 1936M 233M 3094 S  0.0  5.0 19:48.91 ~ /usr/sbin/mysql --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib64/mysql --log-error=/var/log/mysql
28585 mysql     20  0 1936M 233M 3094 S  0.0  5.0 18:53:46 ~ /usr/sbin/mysql --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib64/mysql --log-error=/var/log/mysql
22259 mysql     20  0 1936M 233M 3094 S  0.0  5.0 24:56.01 ~ /usr/sbin/mysql --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib64/mysql --log-error=/var/log/mysql
22864 mysql     20  0 1936M 233M 3094 S  0.0  5.0 25:08.21 ~ /usr/sbin/mysql --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib64/mysql --log-error=/var/log/mysql
22847 mysql     20  0 1936M 233M 3094 S  0.0  5.0 31:03.09 ~ /usr/sbin/mysql --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib64/mysql --log-error=/var/log/mysql
20831 mysql     20  0 1936M 233M 3094 S  0.0  5.0 28:42.33 ~ /usr/sbin/mysql --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib64/mysql --log-error=/var/log/mysql
8828 mysql     20  0 1936M 233M 3094 S  0.0  5.0 28:19.88 ~ /usr/sbin/mysql --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib64/mysql --log-error=/var/log/mysql
1288 mysql     20  0 1936M 233M 3094 S  0.0  5.0 29:16.48 ~ /usr/sbin/mysql --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib64/mysql --log-error=/var/log/mysql
7237 mysql     20  0 1936M 233M 3094 S  0.0  5.0 29:16.48 ~ /usr/sbin/mysql --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib64/mysql --log-error=/var/log/mysql
1274 mysql     20  0 1936M 233M 3094 S  0.0  5.0 5:07.69 ~ /usr/sbin/mysql --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib64/mysql --log-error=/var/log/mysql
1273 mysql     20  0 1936M 233M 3094 S  0.0  5.0 2:34.34 ~ /usr/sbin/mysql --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib64/mysql --log-error=/var/log/mysql
1272 mysql     20  0 1936M 233M 3094 S  0.0  5.0 2:34.34 ~ /usr/sbin/mysql --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib64/mysql --log-error=/var/log/mysql
1271 mysql     20  0 1936M 233M 3094 S  0.0  5.0 27:53.39 ~ /usr/sbin/mysql --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib64/mysql --log-error=/var/log/mysql
1270 mysql     20  0 1936M 233M 3094 S  0.0  5.0 0:03.99 ~ /usr/sbin/mysql --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib64/mysql --log-error=/var/log/mysql
1269 mysql     20  0 1936M 233M 3094 S  0.0  5.0 38:53.31 ~ /usr/sbin/mysql --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib64/mysql --log-error=/var/log/mysql
1268 mysql     20  0 1936M 233M 3094 S  0.0  5.0 28:19.88 ~ /usr/sbin/mysql --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib64/mysql --log-error=/var/log/mysql
1267 mysql     20  0 1936M 233M 3094 S  0.0  5.0 35:52.06 ~ /usr/sbin/mysql --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib64/mysql --log-error=/var/log/mysql
1266 mysql     20  0 1936M 233M 3094 S  0.0  5.0 24:52.05 ~ /usr/sbin/mysql --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib64/mysql --log-error=/var/log/mysql
1265 mysql     20  0 1936M 233M 3094 S  0.0  5.0 28:19.88 ~ /usr/sbin/mysql --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib64/mysql --log-error=/var/log/mysql
1263 mysql     20  0 1936M 233M 3094 S  0.0  5.0 28:19.88 ~ /usr/sbin/mysql --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib64/mysql --log-error=/var/log/mysql
1262 mysql     20  0 1936M 233M 3094 S  0.0  5.0 28:27.57 ~ /usr/sbin/mysql --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib64/mysql --log-error=/var/log/mysql
root@nakajima:~# top
Tasks: 46, 49 Hr: 2 running
Load average: 0.00 0.01 0.05
Uptime: 620 days(1), 23:24:23
Mem: 3474M/4,000M
Swap: 0K/0K
nkjm-prod
```



Tự vấn tiếp

- Có muốn bảo vệ website mình không bị hack?
- Có muốn phần mềm mình viết ra chạy tốt, ổn định (99% uptime)?



Hacking Mindset?

Ở đây không dạy hack **Facebook**



Ảnh 1

*Hãy cho tôi biết
suy nghĩ của
bạn khi nhìn
bức ảnh này?*



Phương pháp tiếp cận

1. WordPress, Laravel các lỗi bảo mật được công khai, cứ theo đó mà check
2. Tự code an toàn -> Chưa chắc -> Cứ check theo checklist OWASP -> khả năng cao là vẫn có lỗi

SQL Server LIMIT / OFFSET SQL Injection

High taylorotwell published GHSA-4mg9-vhxq-vm7j on Apr 28, 2021

Package	Affected versions	Patched versions	Severity
<code>php laravel/framework, illuminate/database</code> (Composer)	<code>>=8.0.0, <8.40.0, >=7.0.0, <7.30.5, <6.20.26</code>	<code>6.20.26, 7.30.5, 8.40.0</code>	High

Description

Impact

Those using SQL Server with Laravel and allowing user input to be passed directly to the `limit` and `offset` functions are vulnerable to SQL injection. Other database drivers such as MySQL and Postgres are not affected by this vulnerability.

Patches

This problem has been patched on Laravel versions 6.20.26, 7.30.5, and 8.40.0.

Workarounds

You may workaround this vulnerability by ensuring that only integers are passed to the `limit` and `offset` functions, as well as the `skip` and `take` functions.

CVE ID

No known CVE

Weaknesses

No CWEs

LƯU Ý

1. Tuyệt đối không store key (aws, google) lên github, các tool hacker scan hàng ngày luôn
2. Lộ key khả năng cao mất (rất nhiều) tiền

SQL Server LIMIT / OFFSET SQL Injection

High taylorotwell published GHSA-4mg9-vhxq-vm7j on Apr 28, 2021

Package	Affected versions	Patched versions
<code>php laravel/framework, illuminate/database</code> (Composer)	<code>>=8.0.0, <8.40.0, >=7.0.0, <7.30.5, <6.20.26</code>	<code>6.20.26, 7.30.5, 8.40.0</code>

Severity
High

CVE ID
No known CVE

Weaknesses
No CWEs

Description

Impact

Those using SQL Server with Laravel and allowing user input to be passed directly to the `limit` and `offset` functions are vulnerable to SQL injection. Other database drivers such as MySQL and Postgres are not affected by this vulnerability.

Patches

This problem has been patched on Laravel versions 6.20.26, 7.30.5, and 8.40.0.

Workarounds

You may workaround this vulnerability by ensuring that only integers are passed to the `limit` and `offset` functions, as well as the `skip` and `take` functions.

OWASP Security Checklist

Level 1: low assurance levels,
completely penetration testable

Level 2: applications containing
sensitive data, recommended for
most apps

Level 3: applications performing
high-value transactions,
containing sensitive medical
data, or requiring the highest
level of trust



OWASP
Open Web Application
Security Project

HACKER MINDSET

1. Đừng chỉ nghĩ, hãy bắt tay vào làm
2. Thất bại là cơ hội, nó giúp cho ta có bài học hay
3. Bắt đầu với mục tiêu nhỏ với 1 thời gian ngắn, tập trung và phối hợp với team

THE HACK MINDSET

What we mean when we talk about hacking.



Don't over think it,
just try it.



Use "failures" as
opportunities to learn.



Keep the goal small,
the team tight and
the timeline short.

Hacker đỉnh cấp

1. FFmpeg, QEMU, Xen
2. TinyC, TinyGL, TinyEMU
3. QuickJS: a small but complete Javascript engine.
4. BPG (Better Portable Graphics)
5. NNCP (lossless data compressor)
6. Bellard's formula for calculating single digits of PI
7. JSLinux: Run Linux or other Operating Systems in your browser!



Fabrice Bellard

Vì sao cần tối ưu performance?

1. Vì tiền 💰, cả nghĩa đen,
lẫn nghĩa bóng 😊
(Hoặc: tôi thích thì tôi
làm 😎)
2. Output: request, user,
ccu, response time /
success
3. Input Resources: Time,
CPU, RAM, Disk I/O,
Network bandwidth

$$\text{Performance} = \frac{\text{Output Result}}{\text{Input Resources}}$$

Bài toán kinh tế

1. Web kiếm được 100\$, tiền server hết 1000\$
2. Target khách hàng 1 triệu, web đáp ứng tối đa 1000
3. Web load lâu quá, user dỗi
4. Vì tiền lương / thưởng



Một năm qua làm như trâu,
thường em đâu sếp...

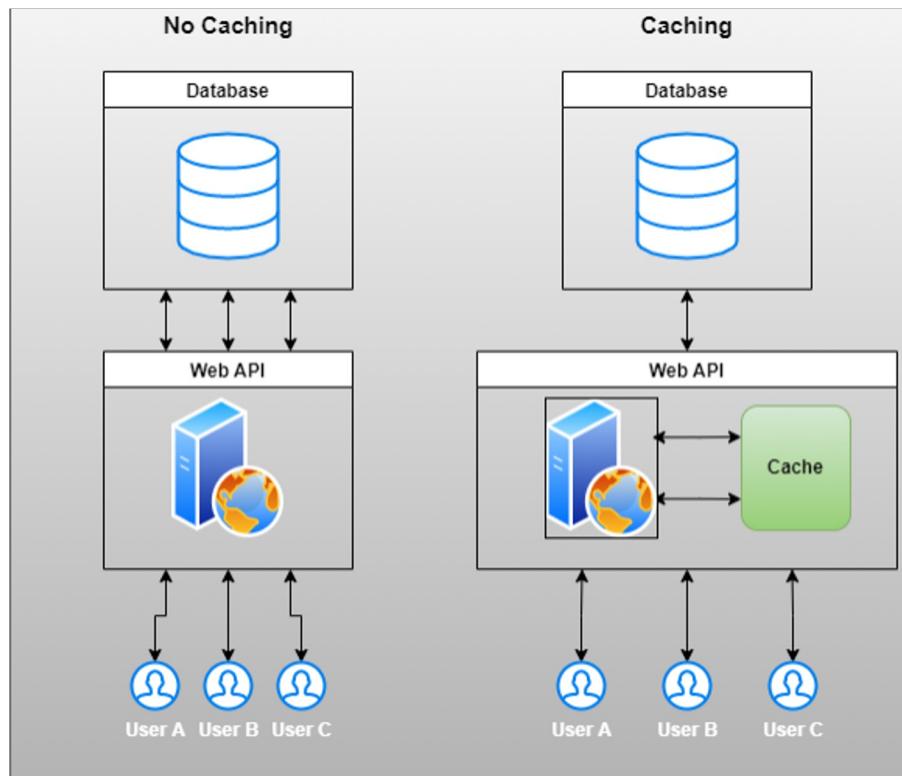
Performance mindset

- **Performance Optimization** nói tới cả 1 quá trình từ khi thiết kế, triển khai tới vận hành, feedback,...
- Có **mindset** về **performance** khác với việc thực hiện tối ưu performance ngay từ đầu.



Ví dụ: Implement Caching

- Có **mindset** về **caching** tức là biết data ở đâu có thể cache, và dùng nó thì có thể giảm được tài nguyên gì.
- **Implement caching** ngay từ khi mới bắt đầu code -> làm phát sinh nhiều vấn đề liên quan tới logic business, sai lệch dữ liệu....



Ví dụ: Request ban đầu có latency 500ms

- Tối ưu DB giúp giảm 300ms
- Sử dụng caching giúp giảm thêm 100ms
- Sử dụng redis pipeline giúp giảm thêm 20ms
- Bỏ logging giúp giảm 5ms
- Optimize thêm đoạn code foreach loop giúp giảm 5ms



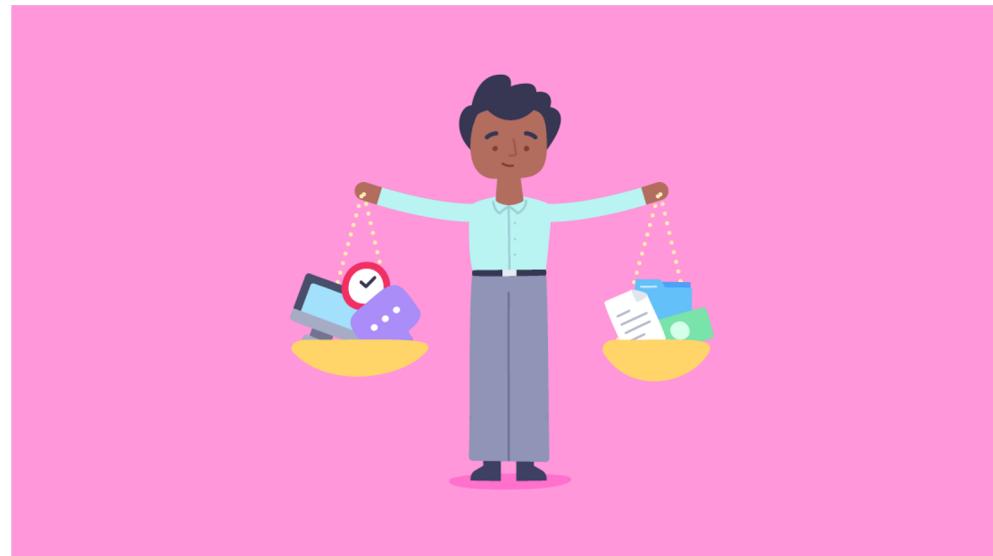
5 Quy trình thực hiện

- Chọn thang đo performance và thiết lập target về performance
- Phân tích performance tĩnh: solution, code, database, architecture
- Benchmarking
- Monitoring / Profiling
- Phân tích performance động khi có sự cố



2 Phương pháp tiếp cận

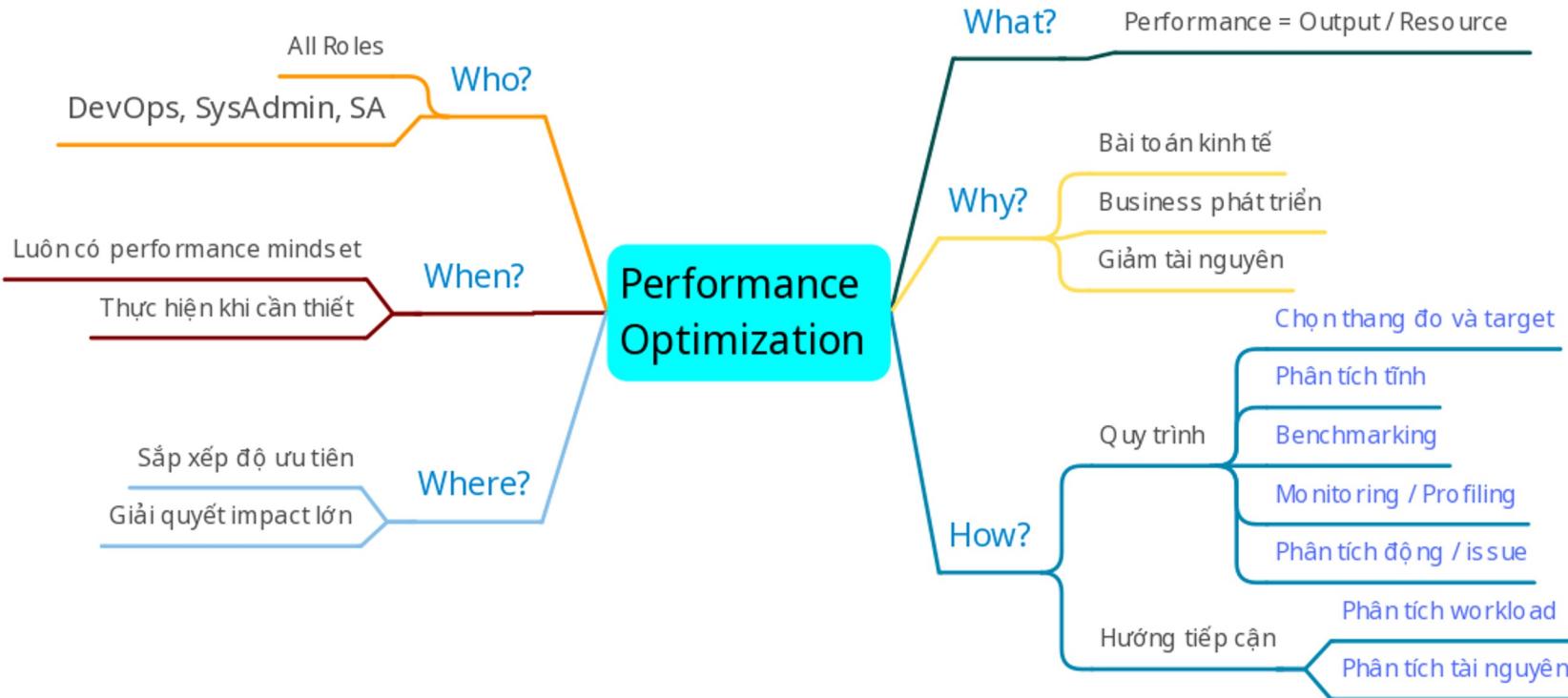
- **Phân tích workload:** Đặt target về workload (tải) của hệ thống và xem application có đáp ứng được không.
- **Phân tích tài nguyên:** Theo dõi mức độ sử dụng tài nguyên (CPU, RAM, disk, network,...) trong các trường hợp khác nhau.



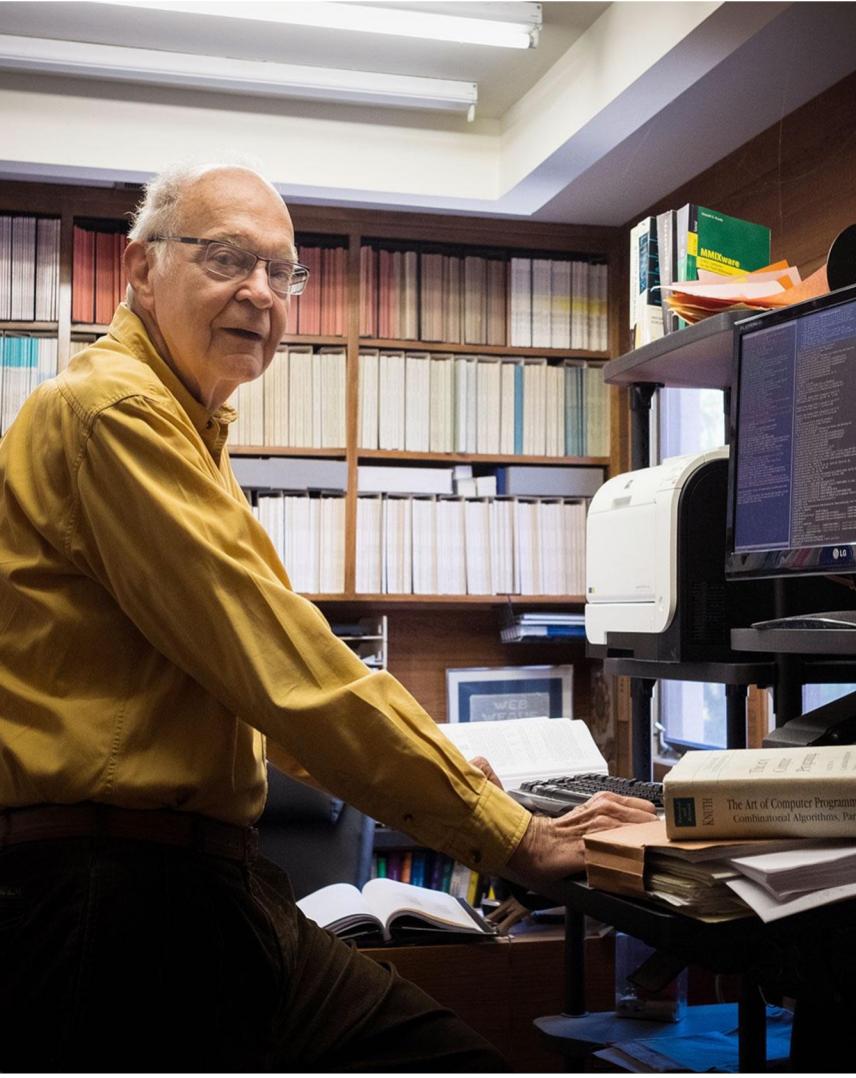


Optimize Performance?

Tối ưu **kết quả đầu ra** dựa trên **nguồn lực đầu vào** hữu hạn!



5W-1H Performance Mindset



**“Optimize code sớm là
nguồn gốc mọi tội ác” -
Donald Knuth**

- Code của bạn sẽ được đọc, được nâng cấp và bảo trì bởi nhiều người khác.
- Dev giỏi sẽ biết cách viết code chạy nhanh, biết cách optimize code
- Dev xuất sắc sẽ biết khi nào cần phải optimize code, khi nào không

You complete
me!

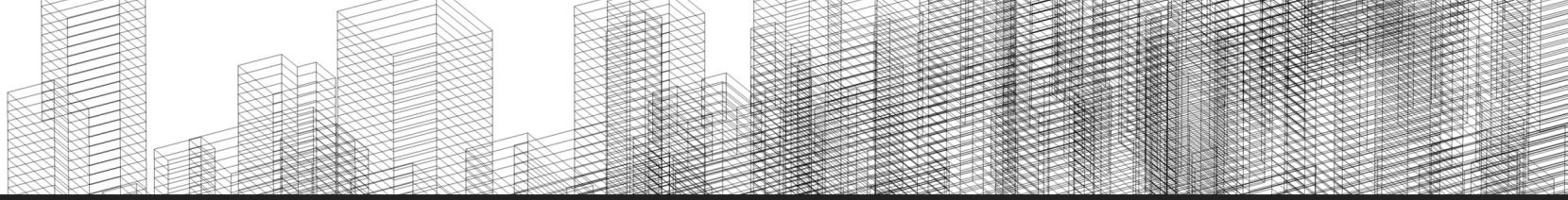
*Người tốt - Kẻ
xấu luôn tồn
tại*

*Thành ai là do
bạn chọn*



Bonus

- Theo bạn vì sao team anh Khoa luôn thắng trong 3 lần game?
- Bạn học được gì từ điều đó?



"LỜI CHƯA NÓI"

Khoá học này tập trung vào những chỉ dẫn mang tính định hướng cho việc phát triển sự nghiệp lâu dài của DEV.

Bởi mang tính định hướng lâu dài, nên có những nguyên lý cơ bản, đơn giản và mang tính nền tảng, giúp DEV nâng cao trình độ 1 cách bền vững theo thời gian...!

CodeBase Universal

- Codebase & Packager
- Operations, Monitoring, SEO
- Performance & Security
- Skill and Level UP

Góc chia sẻ

Complete me!

- Hãy cho mình biết về cảm nghĩ của bạn sau khoá học này?
- Bạn thích hay không thích?
- Nó có giúp ích cho bạn trong chặng đường sắp tới không?

**Think Big, Start Small,
Move Fast**



6 Nguyên lý

- Project approach
- Test first
- ROI driven
- Data driven
- Systemic thinking
- Triangle feedbacks



5 Yếu tố

- OOP
- SDLC
- Packager
- Maintainer
- Collection



6 kỹ thuật

- Quản lý Scope
- Unit & Auto Test
- Ghi log
- Phân tích log
- Theo dõi | Giám sát
- Sử dụng công cụ



6 Checklist SEO for DEV

- Ping
- Robots, RSS, Sitemap
- URL for SEO
- Title & Meta Description
- Media Optimize
- Speed Optimize



Hard Skills

Learnable and presentable skills,
knowledge and qualification

- Language knowledge
- Degrees, apprenticeships, certificates
- Accounting
- Typing techniques
- Machine operations
- Programming languages
- Software knowledge
- etc.

Soft Skills

Character traits, personal, inter-personal skills

- Communication skills
- Flexibility
- Self-reflection, Self-discipline
- Teamwork
- Time management
- Empathy
- Ability to take criticism
- Etc.

Hard skills can be proven, whereas soft skills are harder to prove.



Thanks & Welcome!