

# การรายงานสรุปผลการทดสอบเจาะระบบ (Penetration Testing)

เว็บไซต์ [tcr.degitoprojects.com](http://tcr.degitoprojects.com)



PENETRATION TESTING SERVICE



- ขอบเขตงาน
- บทสรุปผู้บริหาร
- สรุปช่องทางที่ตรวจพบ
- รายละเอียดช่องทางที่ตรวจพบ

# ขอบเขตของงาน และ แผนการดำเนินโครงการ



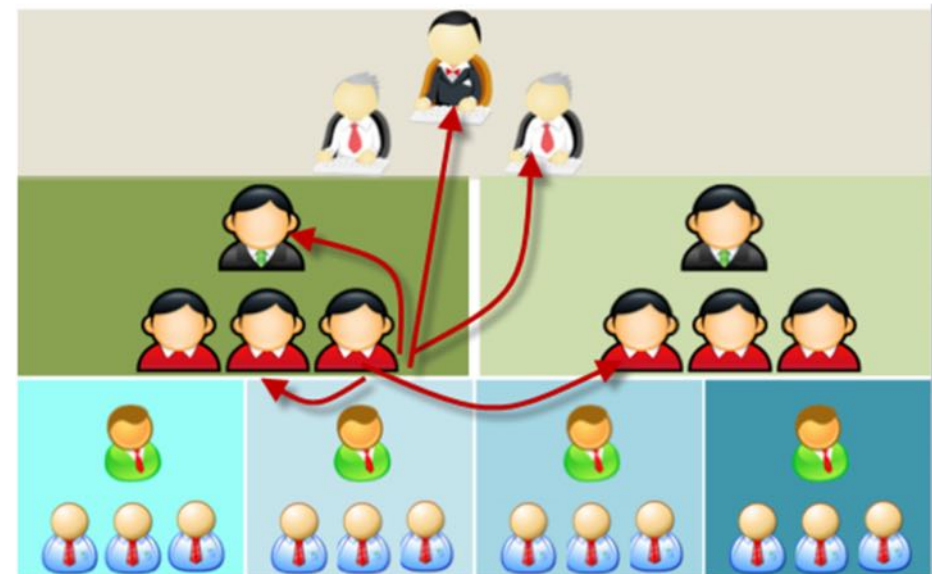
เป้าหมายที่ทำการทดสอบ	tcr.degitoprojects.com
รูปแบบในการทดสอบ	Black-box Testing
ระยะเวลาที่ทำการทดสอบ	12 พฤษภาคม 2561 – 14 พฤษภาคม 2561
นำเสนอช่องโหว่	18 พฤษภาคม 2561
ทดสอบซ้ำ	TBD

การทดสอบแบบ Black-box Testing คือ การจำลองสถานการณ์ในกรณีที่เปรียบผู้ทดสอบเสมือน Hacker จริง ๆ โดยไม่ต้องแจ้งข้อมูลใด ๆ ที่เกี่ยวกับระบบให้แก่ผู้ทดสอบทราบก่อน แจ้งเฉพาะเป้าหมายที่ต้องการจะทดสอบเท่านั้น



## Web Application Penetration Testing

- ตรวจสอบช่องโหว่ทางเทคนิค
- ตรวจสอบช่องโหว่ทาง Business Logic





Known vulnerabilities

Window Time

Snapshot in time



จากผลการทดสอบเจาะระบบเว็บไซต์ tcr.degitoprojects.com พบว่าเว็บไซต์มีช่องโหว่ที่มีความรุนแรงสูง และ สูงมาก ทำให้ผู้ไม่ประสงค์ดีสามารถควบคุมเครื่อง Server ของเว็บไซต์ และเข้าถึง Database ของทุกเว็บไซต์ที่อยู่บน Server เครื่องดังกล่าวได้ทันที โดยช่องโหว่ดังกล่าวประกอบไปด้วยรายการดังต่อไปนี้

- เว็บไซต์ไม่มีการป้องกันการเข้าถึงไฟล์ .env ทำให้ผู้ไม่ประสงค์ดีทราบถึงรหัสผ่านของ Database ที่เก็บไว้ในไฟล์ และเข้าถึง Database ของทุกเว็บไซต์ได้ทันที
- เว็บไซต์ไม่มีการตรวจสอบการอัปโหลดไฟล์ที่ดี ส่งผลให้ผู้ไม่ประสงค์ดีสามารถอัปโหลด Malicious File ขึ้นไปบนเครื่อง Server และเข้าควบคุมเครื่อง Server ได้

สำหรับวิธีการแก้ไขช่องโหว่ในภาพรวมนั้น ผู้พัฒนาควรที่จะตรวจสอบ Input จากผู้ใช้งานอย่างละเอียดและรอบคอบ อีกทั้งควรจะต้องมีทำ Hardening เครื่อง Server เพื่อลดความเสี่ยงในการตั้งค่า Server ที่ไม่ปลอดภัย และเปิดช่องให้ผู้ไม่ประสงค์ดีเข้าควบคุมเว็บไซต์และเครื่อง Server ได้ในที่สุด

# ระดับความเสี่ยง



ระดับความเสี่ยง = ผลกระทบ x โอกาสเกิด

		1-4	5-9	10-16	20-25	
ระดับความเสี่ยง		ต่ำ	ปานกลาง	สูง	สูงมาก	
โอกาสเกิด						
5	5	10	15	20	25	
4	4	8	12	16	20	
3	3	6	9	12	15	
2	2	4	6	8	10	
1	1	2	3	4	5	
		1	2	3	4	5
						ผลกระทบ

# ระดับความเสี่ยง



ระดับความเสี่ยง	รายละเอียด
สูงมาก	ความเสี่ยงในระดับสูงมาก ไม่สามารถยอมรับได้ ต้องพิจารณาหาแนวทางการแก้ไขความเสี่ยง และดำเนินการทันที
สูง	ความเสี่ยงในระดับสูง ไม่สามารถยอมรับได้ ต้องพิจารณาหาแนวทางการแก้ไขความเสี่ยง และดำเนินการแก้ไขภายในระยะเวลาที่เหมาะสม
ปานกลาง	ความเสี่ยงในระดับปานกลาง ควรพิจารณาแก้ไขความเสี่ยง แต่หากมีเหตุจำเป็นก็สามารถพิจารณายอมรับความเสี่ยงได้
ต่ำ	ความเสี่ยงในระดับที่ต่ำมาก สามารถยอมรับได้โดยไม่ต้องดำเนินการใดๆ เพิ่มเติม



# ผลกระทบ และ โอกาสเกิด



ผลกระทบ		
5	สูงมาก	มีผลกระทบรุนแรงมาก ส่งผลให้การให้บริการหยุดชะงักเป็นเวลานาน และเกิดปัญหารุนแรงกับลูกค้าหรือองค์กร ซึ่งต้องใช้เวลาและทรัพยากรสูงมากในการทำการแก้ไข
4	สูง	มีผลกระทบรุนแรง ส่งผลให้การให้บริการหยุดชะงักชั่วคราว และเกิดปัญหากับลูกค้า หรือความเชื่อมั่นต่อองค์กร ซึ่งต้องใช้เวลาและทรัพยากรมากในการทำการแก้ไข
3	ปานกลาง	มีผลกระทบในระดับปานกลาง อาจส่งผลต่อการให้บริการล่าช้า ซึ่งต้องใช้เวลาและทรัพยากรในการแก้ไข
2	ต่ำ	มีผลกระทบเล็กน้อย ซึ่งต้องใช้เวลาและทรัพยากรเล็กน้อยในการแก้ไข
1	ต่ำมาก	แทบไม่มีผลกระทบต่อการให้บริการ สามารถจัดการแก้ไขได้โดยวิธีการปฏิบัติงานปกติ

โอกาสเกิด		
5	สูงมาก	Threat มีความน่าจะเป็นที่จะสร้างความเสียหายได้สูงมาก อาจเกิดขึ้นได้ทุกสัปดาห์หรือบ่อยกว่า
4	สูง	Threat มีความน่าจะเป็นที่จะสร้างความเสียหายได้สูง อาจเกิดขึ้นได้ประมาณเดือนละครั้ง
3	ปานกลาง	Threat มีความน่าจะเป็นที่จะสร้างความเสียหายได้ปานกลาง อาจเกิดขึ้นได้ประมาณปีละครั้ง
2	ต่ำ	Threat มีความน่าจะเป็นที่จะสร้างความเสียหายได้ต่ำ ในรอบหกปีอาจเกิดขึ้น 1 – 2 ครั้ง
1	ต่ำมาก	Threat มีความน่าจะเป็นที่จะสร้างความเสียหายได้ต่ำมาก ในรอบร้อยปี อาจจะได้สักครั้ง หรือแทบเป็นไปไม่ได้ที่จะเกิดขึ้น

# VA Scan vs Pentest



Scanner version: 2.10b Scan date: Sat May 12 18:18:32 2018  
Random seed: 0x6462e1bf Total time: 0 hr 16 min 18 sec 720 ms

Problems with this scan? [Click here](#) for advice.

## Crawl results - click to expand:

- <http://tcr.degitoprojects.com/> 3  
Code: 301, length: 327, declared: text/html, detected: application/xhtml+xml, charset: iso-8859-1 [ show trace + ]
- <https://tcr.degitoprojects.com/> 1 13 10 44 99 136  
Code: 302, length: 376, declared: text/html, detected: application/xhtml+xml, charset: UTF-8 [ show trace + ]

## Document type overview - click to expand:

- application/binary (13)
- application/javascript (7)
- application/xhtml+xml (11)
- image/jpeg (2)
- image/png (5)
- image/svg+xml (9)
- image/x-ms-bmp (1)
- text/css (12)
- text/plain (5)

## Issue type overview - click to expand:

- Query injection vector (1)
- Interesting file (1)
- External content embedded on a page (higher risk) (12)
- HTML form with no apparent XSRF protection (4)
- External content embedded on a page (lower risk) (5)
- SSL certificate host name mismatch (1)



View by: **OWASP Report** Patch Report **Threat Report** Print Report

**Vulnerability Scan** rename 12 May 2018 at 7:37AM (GMT+0700)  
External Host Vulnerability Report

**8** Vulnerabilities Detected

**0** HIGH Risk

**5** MED Risk

**3** LOW Risk

**28** INFO Gathered

**https://tcr.degitoprojects.c...**  
54.169.224.153  
tcr.degitoprojects.com

[Rescan URL](#)

Filter by: All (8) Level 5 (0) Level 4 (0) **Level 3 (5)** Level 2 (3) Level 1 (0) Info (28) Search for Title, Category, CVE ID or QID

**All Scan Results** 1 - 5 of 5

Web Server Uses Plain-Text Form Based Authentication	
Apple Macintosh OS X Client Apache Directory Contents Di...	
Apple MacOS X .DS_Store Directory Listing Disclosure Vuln...	
phpMyAdmin Multiple Security Vulnerabilities (PMASA-2014...	
phpMyAdmin Multiple Security Vulnerabilities (PMASA-2014...	

**Web Server Uses Plain-Text Form Based Authentication**

QID: 86728 CVE Base: 7 Port: 80  
CVSS Temporal: 6.3 Category: Web server  
CVE ID: -

**Threat:**  
The Web server uses plain-text form based authentication. A web page exists on the target host which uses an HTML login form. This data is sent from the client to the server in plain-text.



Hosts > 54.169.224.153 > Vulnerabilities 36

<input type="checkbox"/> Severity ▲	Plugin Name	Plugin Family	Count
<input type="checkbox"/> MEDIUM	Apple Mac OS X Find-By-Content .DS_Store Web Directory Listing	Web Servers	1
<input type="checkbox"/> MEDIUM	SSL Medium Strength Cipher Suites Supported	General	1
<input type="checkbox"/> INFO	Service Detection	Service detection	4

# สรุปช่องโหว่ที่ตรวจพบ



ข้อ	ช่องโหว่	ระดับความรุนแรง	ผลกระทบ	โอกาสเกิด
1	ไม่มีการป้องกันการเข้าถึงไฟล์ .env	สูงมาก	สูงมาก	สูงมาก
2	Malicious File Upload	สูง	สูงมาก	ปานกลาง
3	มีการใช้งาน phpMyAdmin ที่เป็นเวอร์ชันเก่า และมีช่องโหว่	ปานกลาง	ปานกลาง	ต่ำ
4	สามารถเข้าถึงหน้า phpMyAdmin ได้จาก Internet	ปานกลาง	ปานกลาง	ต่ำ
5	อนุญาตให้ใช้ root ในการเข้าจัดการ Database	ปานกลาง	ปานกลาง	ต่ำ
6	ไม่มีการเปิดใช้งาน HTTP Strict-Transport-Security (HSTS)	ต่ำ	ต่ำ	ต่ำ
7	มีการตั้งค่าการใช้งาน HTTPS ที่ไม่ปลอดภัย	ต่ำ	ต่ำ	ต่ำ
8	Clickjacking	ต่ำ	ต่ำ	ต่ำ
9	สามารถเข้าถึงไฟล์ .DS_Store บนเว็บไซต์ได้	ต่ำ	ต่ำ	ต่ำ
10	หน้าแสดงข้อความ Error แสดงข้อมูลที่มีความสำคัญต่อเว็บไซต์ออกมามากเกินไป	ต่ำ	ต่ำมาก	สูง

# 1. ไม่มีการป้องกันการเข้าถึงไฟล์ .env



ระดับความเสี่ยง	สูงมาก
อ้างอิง	OWASP Top 10 - 2017 A3 - Sensitive Data Exposure
จุดที่ตรวจพบ	<a href="https://tcr.degitoprojects.com/.env">https://tcr.degitoprojects.com/.env</a> <a href="https://tcr.degitoprojects.com/laravel/.env">https://tcr.degitoprojects.com/laravel/.env</a>

```
← ⓘ | https://tcr.degitoprojects.com/.env
Most Visited ▾ Offensive Security Kali Linux Kali Docs

APP_NAME=Laravel
APP_ENV=local
APP_KEY=base64: [REDACTED]
APP_DEBUG=true
APP_LOG_LEVEL=debug
APP_URL=https://tcr.degitoprojects.com

DB_CONNECTION=mysql
DB_HOST=127.0.0.1
DB_PORT=3306
DB_DATABASE=tcr
DB_USERNAME=root
DB_PASSWORD=[REDACTED]
```

```
BROADCAST_DRIVER=log
CACHE_DRIVER=file
SESSION_DRIVER=file
QUEUE_DRIVER=sync

REDIS_HOST=127.0.0.1
REDIS_PASSWORD=null
REDIS_PORT=6379

MAIL_DRIVER=smtp
MAIL_HOST=smtp.gmail.com
MAIL_PORT=587
MAIL_USERNAME=thailandpom@gmail.com
MAIL_PASSWORD=[REDACTED]
MAIL_ENCRYPTION=tls

PUSHER_APP_ID=
PUSHER_APP_KEY=
PUSHER_APP_SECRET=
PUSHER_APP_CLUSTER=mt1
```

# 1. ไม่มีการป้องกันการเข้าถึงไฟล์ .env



## วิธีการแก้ไข

Option 1: ป้องกันการเข้าถึงไฟล์โดยใช้ .htaccess

```
<FilesMatch "^\.env">  
    Order allow,deny  
    Deny from all  
</FilesMatch>
```

Option 2: ไม่เก็บไฟล์ .env ไว้ใน Public Folder หรือที่ ๆ สามารถ Browse เข้าถึงได้จากผู้ใช้งานทั่วไป

## 2. Malicious File Upload



ระดับความเสี่ยง	สูง
อ้างอิง	OWASP Top 10 - 2017 A6 - Security Misconfiguration
จุดที่ตรวจพบ	<a href="https://tcr.degitoprojects.com/en/สมัครงาน">https://tcr.degitoprojects.com/en/สมัครงาน</a> <a href="https://tcr.degitoprojects.com/contact/sendmailjob">https://tcr.degitoprojects.com/contact/sendmailjob</a>

เว็บไซต์: <https://tcr.degitoprojects.com/en/สมัครงาน>

วันเสาร์ที่ 28 เมษายน 2561

ณ อาคาร อาร์.เอส. ทาวเวอร์ รัชดาภิเษก ชั้น 10 MRT ศูนย์วัฒนธรรมฯ ทางออกที่ 4

สอบถามข้อมูลเพิ่มเติม ทีมสรรหาบุคลากร โทร. 02 697 5300 ต่อ 2213, 2228 และโทร. 080 088 5082  
ทุกวันจันทร์ - ศุกร์ เวลา 08.30 - 17.00 น. หรือติดต่อผ่านทางช่องทาง E-mail: recruitment@tcrbank.com

กรุณกรอกข้อมูลของท่านให้ครบถ้วนทุกช่อง เพื่อให้เจ้าหน้าที่ติดต่อกลับ

ข้อมูลส่วนตัวผู้สมัคร

ชื่อ \*

นามสกุล \*

แบบรูปถ่ายผู้สมัคร \*  No file selected.

อายุ \*

เพศ \* ☒ ชาย ☐ หญิง

วุฒิการศึกษาสูงสุด \*

แนบสำเนาวุฒิการศึกษา \*  No file selected.

ประสบการณ์ทำงาน \*

อีเมล \*

เบอร์โทรศัพท์ \*

ที่อยู่อาศัยที่สะดวกในการทำงาน \*

phpMyAdmin

Recent Favorites

1 >>>

Server: localhost » Database: tcr » Table: file\_upload

	id	career_id	filename
<input type="checkbox"/> Edit Copy Delete	68	24	5af9001414187dalia-georgia-wallpaper.jpg
<input type="checkbox"/> Edit Copy Delete	69	24	5af9001415614rose-flower-blossom-bloom-39517.jpeg
<input type="checkbox"/> Edit Copy Delete	70	25	5af935949f122uploadtest.txt
<input type="checkbox"/> Edit Copy Delete	71	25	5af93594a036auploadtest.txt
<input type="checkbox"/> Edit Copy Delete	72	25	5af93594a139cuploadtest.txt
<input type="checkbox"/> Edit Copy Delete	73	26	5af93e8f97e93testupload.php
<input type="checkbox"/> Edit Copy Delete	74	26	5af93e8f994bftestupload.php
<input type="checkbox"/> Edit Copy Delete	75	26	5af93e8f9a5b7testupload.php

ส่งข้อความถึงธนาคารไทยเครดิต เพื่อรายย่อย





## 2. Malicious File Upload



ทำการเพิ่มผู้ใช้งานลงใน  
ฐานข้อมูลทาง phpMyAdmin  
เพื่อทำการเข้าสู่ระบบ admin  
console

ธนาคารไทยเครดิต  
สงวนลิขสิทธิ์ โดย ธนาคารไทยเครดิต เพื่อรายย่อย จำกัด (มหาชน) พ.ศ.2555 - 2560.  
ออกแบบและพัฒนาโดย DEGITO

อีเมล

รหัสผ่าน

☐ จดจำฉัน

เข้าสู่ระบบ

← กลับไปหน้าหลักเว็บไซต์ | ลืมรหัสผ่าน?

Showing rows 0 - 3 (4 total, Query took 0.0002 seconds.)

SELECT \* FROM `users`

Number of rows: 25

Sort by key: None

	id	name	email	password	remember_token	role_id
<input type="checkbox"/>	3	SuperAdmin@Test	superadmin@tcr.app	\$2y\$10\$RD0lIP92mY/HbUKzCe1PugCo/sr5bpwQfLJ/DPpkCC...	lebTgrc1PLcEYo30wJmx8uDgWQImUbUKTPS2il5vUf3y4w4wb...	1
<input type="checkbox"/>	4	Admin@Test	admin@tcr.app	\$2y\$10\$Q4XAbaWWHaj8kcT3tLheQyAwis7j7pcYCsrtUDST...	J5Pi7XlmBm4W7h1px3QYYQfuhgE9XYgkePPzFFWP1QDXAsYU...	2
<input type="checkbox"/>	6	Demo@Test	demo@tcr.app	\$2y\$10\$zTMU3BvcEDxcnLKb0UxGu7RhmMhOxrmCWcOdS.Lm/P7...	HMMv52GR7g8SHXmtBwtQ7lMjABNCQTmpMQJSki8G78ulucy5r...	3
<input type="checkbox"/>	9	SuperAdmin2@Test	superadmin2@tcr.app	\$2a\$10\$dmhJHngMYV 60AisrIKlyuRV3/ePJgwmkKqJm2XfP...	SFb6gpOWswCUJ3UOkRERpY6jrJ9LCDLHbv9H1E9LtUFQXuuiQ...	1



## 2. Malicious File Upload



Dashboard of the TCR system. The URL is <https://tcr.degitoprojects.com/2561/tcr/backend/console/admin/dashboard>. The user is SUPERADMIN2@TEST.

**ยินดีต้อนรับเข้าสู่ระบบจัดการหลังบ้าน**  
เริ่มต้นจัดการหลังบ้าน.

**หน้าเว็บ:**  
สร้างหน้าเว็บ  
ดูหน้าเว็บทั้งหมด

**ข่าวสาร:**  
สร้างข่าวสาร  
ดูข่าวสารทั้งหมด  
สร้างแกล็ก  
ดูแกล็กทั้งหมด

**อัตราดอกเบี้ยเงินฝาก** + เพิ่มข้อมูล

ออมทรัพย์   0.50 - 1.80 %	ยกเลิก ลบ
ประจำ   1.50 - 1.80 %	ยกเลิก ลบ
กระแสรวรับเพิ่มค่า   0.25 - 0.75 %	ยกเลิก ลบ
ปลอดภาษี   2.50 %	ยกเลิก ลบ

**อัตราดอกเบี้ยเงินกู้** + เพิ่มข้อมูล

MLR   8.47 %	ยกเลิก ลบ
MOR   8.65 %	ยกเลิก ลบ
MRR   9.05 %	ยกเลิก ลบ
MAR   7.90 %	ยกเลิก ลบ
MGR   16.55 %	ยกเลิก ลบ

Users management page. The URL is <https://tcr.degitoprojects.com/2561/tcr/backend/console/admin/users/user>. The user is SUPERADMIN2@TEST.

**USERS**

ผู้ใช้งาน > ผู้ใช้งาน

+ สร้างผู้ใช้งาน

ลำดับ	อีเมล	สิทธิ์	สร้างเมื่อ	แก้ไข	ลบ
9	superadmin2@tcr.app	System Operator	2018-03-07 02:14:05	แก้ไข	ลบ
6	demo@tcr.app	Demo	2018-03-07 08:05:05	แก้ไข	ลบ
4	admin@tcr.app	Admin	2018-03-07 02:20:27	แก้ไข	ลบ
3	superadmin@tcr.app	System Operator	2018-03-07 02:14:05	แก้ไข	ลบ

## 2. Malicious File Upload



### วิธีการแก้ไข

ตรวจสอบและจำกัดประเภทไฟล์ที่สามารถ Upload ได้ทั้งฝั่ง Front End และ Back End โดยสามารถดูวิธีการเพิ่มเติมได้ที่

- [https://www.owasp.org/index.php/Unrestricted\\_File\\_Upload](https://www.owasp.org/index.php/Unrestricted_File_Upload)

### 3.สามารถเข้าถึงหน้า phpMyAdmin ได้จาก Internet



ระดับความเสี่ยง	ปานกลาง
อ้างอิง	OWASP Top 10 - 2017 A6 - Security Misconfiguration
จุดที่ตรวจพบ	<a href="https://tcr.degitoprojects.com/phpmyadmin">https://tcr.degitoprojects.com/phpmyadmin</a>

https://tcr.degitoprojects.com/phpmyadmin/

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums Nethunter Getting Started

**phpMyAdmin**

Welcome to phpMyAdmin

Language

English

Log in

Username: root

Password:

Go

### 3.สามารถเข้าถึงหน้า phpMyAdmin ได้จาก Internet



phpMyAdmin

Recent Favorites

New

AT

atfocus

ativara

chevron

dg\_m

information\_schema

iplace

klonn

mrta

mysql

performance\_schema

phpmyadmin

redd

seta2017db

seta2018db

srabua

STAR

sys

tcr

Server: localhost

Databases SQL Status User accounts Export Import Settings Replication Variables Charsets Engines

General settings

Change password

Server connection collation: utf8mb4\_unicode\_ci

Appearance settings

Language: English

Theme: pmahomme

Font size: 82%

More settings

Database server

- Server: Localhost via UNIX socket
- Server type: MySQL
- Server version: 5.7.22-0ubuntu0.16.04.1 - (Ubuntu)
- Protocol version: 10
- User: root@localhost
- Server charset: UTF-8 Unicode (utf8)

Web server

- Apache/2.4.18 (Ubuntu)
- Database client version: libmysql - mysqlnd 5.0.12-dev - 20150407 - \$ld: b5c5906d452ec590732a93b051f3827e02749b83 \$
- PHP extension: mysqli
- PHP version: 7.0.28-0ubuntu0.16.04.1

phpMyAdmin

- Version information: 4.5.4.1deb2ubuntu2
- Documentation
- Wiki

### 3.สามารถเข้าถึงหน้า phpMyAdmin ได้จาก Internet



#### วิธีการแก้ไข

**Option 1:** จำกัดการเข้าถึง phpMyAdmin ให้เข้าถึงได้จากเฉพาะ IP Address ของผู้ดูแลระบบเท่านั้น

**Option 2:** ใช้ VPN ในการเข้าถึง phpMyAdmin

## 4. อนุญาตให้ใช้ root ในการเข้าจัดการ Database



ระดับความเสี่ยง	ปานกลาง
อ้างอิง	OWASP Top 10 - 2017 A6 - Security Misconfiguration
จุดที่ตรวจพบ	<a href="https://tcr.degitoprojects.com/phpmyadmin">https://tcr.degitoprojects.com/phpmyadmin</a>

The screenshot shows the phpMyAdmin web interface. The left sidebar lists various databases and users. The main content area displays the 'General settings' and 'Appearance settings' for the 'Server: localhost'. The 'Database server' section on the right lists the following details:

- Server: Localhost via UNIX socket
- Server type: MySQL
- Server version: 5.7.22-0ubuntu0.16.04.1 - (Ubuntu)
- Protocol version: 10
- **User: root@localhost** (highlighted with a red box)
- Server charset: UTF-8 Unicode (utf8)

The 'Web server' section on the right lists the following details:

- Apache/2.4.18 (Ubuntu)
- Database client version: libmysql - mysqlnd 5.0.12-dev - 20150407 - \$Id: b5c5906d452ec590732a93b051f3827e02749b83 \$
- PHP extension: mysqli
- PHP version: 7.0.28-0ubuntu0.16.04.1

The 'phpMyAdmin' section at the bottom lists the following details:

- Version information: 4.5.4.1deb2ubuntu2
- Documentation
- Wiki

## 4. อนุญาตให้ใช้ root ในการจัดการ Database



Screenshot of the phpMyAdmin interface showing the 'User accounts overview' page for 'Server: localhost'.

The interface includes a sidebar with a tree view of databases and a main content area with tabs for 'Databases', 'SQL', 'Status', 'User accounts', 'Export', 'Import', 'Settings', and 'Rep'. The 'User accounts' tab is active, displaying a table of user accounts.

	User name	Host name	Password	Global privileges	User group	Grant	Action
<input type="checkbox"/>	debian-sys-maint	localhost	Yes	ALL PRIVILEGES		Yes	<a href="#">Edit privileges</a> <a href="#">Export</a>
<input type="checkbox"/>	mysql.session	localhost	Yes	SUPER		No	<a href="#">Edit privileges</a> <a href="#">Export</a>
<input type="checkbox"/>	mysql.sys	localhost	Yes	USAGE		No	<a href="#">Edit privileges</a> <a href="#">Export</a>
<input type="checkbox"/>	phpmyadmin	localhost	Yes	USAGE		No	<a href="#">Edit privileges</a> <a href="#">Export</a>
<input type="checkbox"/>	root	localhost	Yes	ALL PRIVILEGES		Yes	<a href="#">Edit privileges</a> <a href="#">Export</a>

Below the table, there are controls for 'Check all' and 'With selected: Export'. A 'New' button is also present, leading to an 'Add user account' form. At the bottom, there is a 'Remove selected user accounts' button.

## 4. อนุญาตให้ใช้ root ในการเข้าจัดการ Database



### วิธีการแก้ไข

- สร้าง User อื่นที่ไม่ใช่ root เพื่อใช้ในการเชื่อมต่อเว็บไซต์กับ Database หรือเพื่อใช้ในการเข้าจัดการ Database โดยจำกัดสิทธิ์เท่าที่จำเป็นที่จะต้องใช้งานให้แก่ User ดังกล่าว
- ปิดการอนุญาตให้ใช้ root ในการเข้าจัดการ Database ผ่านทาง phpMyAdmin โดยการแก้ไขไฟล์  
/etc/phpmyadmin/config.inc.php

```
$cfg['Servers'][$i]['AllowRoot'] = FALSE;
```



## 5. มีการใช้งาน phpMyAdmin ที่เป็นเวอร์ชันเก่าและมีช่องโหว่



ระดับความเสี่ยง	ปานกลาง
อ้างอิง	OWASP Top 10 - 2017 A9 - Using Components with Known Vulnerabilities
จุดที่ตรวจพบ	<a href="https://tcr.degitoprojects.com/phpmyadmin">https://tcr.degitoprojects.com/phpmyadmin</a>

### Phpmyadmin » Phpmyadmin » 4.5.4.1 : Security Vulnerabilities

Cpe Name: `cpe:/a:phpmyadmin:phpmyadmin:4.5.4.1`

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : [CVE Number Descending](#) [CVE Number Ascending](#) [CVSS Score Descending](#) [Number Of Exploits Descending](#)

[Copy Results](#) [Download Results](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	<a href="#">CVE-2018-7260</a>	<a href="#">79</a>		XSS	2018-02-21	2018-03-06	3.5	None	Remote	Medium	Single system	None	Partial	None
Cross-site scripting (XSS) vulnerability in db_central_columns.php in phpMyAdmin before 4.7.8 allows remote authenticated users to inject arbitrary web script or HTML via a crafted URL.														
2	<a href="#">CVE-2016-2562</a>	<a href="#">20</a>		+Info	2016-03-01	2016-12-02	5.8	None	Remote	Medium	Not required	Partial	Partial	None
The checkHTTP function in libraries/Config.class.php in phpMyAdmin 4.5.x before 4.5.5.1 does not verify X.509 certificates from api.github.com SSL servers, which allows man-in-the-middle attackers to spoof these servers and obtain sensitive information via a crafted certificate.														
3	<a href="#">CVE-2016-2561</a>	<a href="#">79</a>		XSS	2016-03-01	2016-12-02	3.5	None	Remote	Medium	Single system	None	Partial	None
Multiple cross-site scripting (XSS) vulnerabilities in phpMyAdmin 4.4.x before 4.4.15.5 and 4.5.x before 4.5.5.1 allow remote authenticated users to inject arbitrary web script or HTML via (1) normalization.php or (2) js/normalization.js in the database normalization page, (3) templates/database/structure/sortable_header.phtml in the database structure page, or (4) the pos parameter to db_central_columns.php in the central columns page.														
4	<a href="#">CVE-2016-2560</a>	<a href="#">79</a>		XSS	2016-03-01	2016-12-02	4.3	None	Remote	Medium	Not required	None	Partial	None
Multiple cross-site scripting (XSS) vulnerabilities in phpMyAdmin 4.0.x before 4.0.10.15, 4.4.x before 4.4.15.5, and 4.5.x before 4.5.5.1 allow remote attackers to inject arbitrary web script or HTML via (1) a crafted Host HTTP header, related to libraries/Config.class.php; (2) crafted JSON data, related to file_echo.php; (3) a crafted SQL query, related to js/functions.js; (4) the initial parameter to libraries/server_privileges.lib.php in the user accounts page; or (5) the it parameter to libraries/controllers/TableSearchController.class.php in the zoom search page.														
5	<a href="#">CVE-2016-2559</a>	<a href="#">79</a>		XSS	2016-03-01	2016-12-02	3.5	None	Remote	Medium	Single system	None	Partial	None
Cross-site scripting (XSS) vulnerability in the format function in libraries/sql-parser/src/Utils/Error.php in the SQL parser in phpMyAdmin 4.5.x before 4.5.5.1 allows remote authenticated users to inject arbitrary web script or HTML via a crafted query.														

## 5. มีการใช้งาน phpMyAdmin ที่เป็นเวอร์ชันเก่าและมีช่องโหว่



### วิธีการแก้ไข

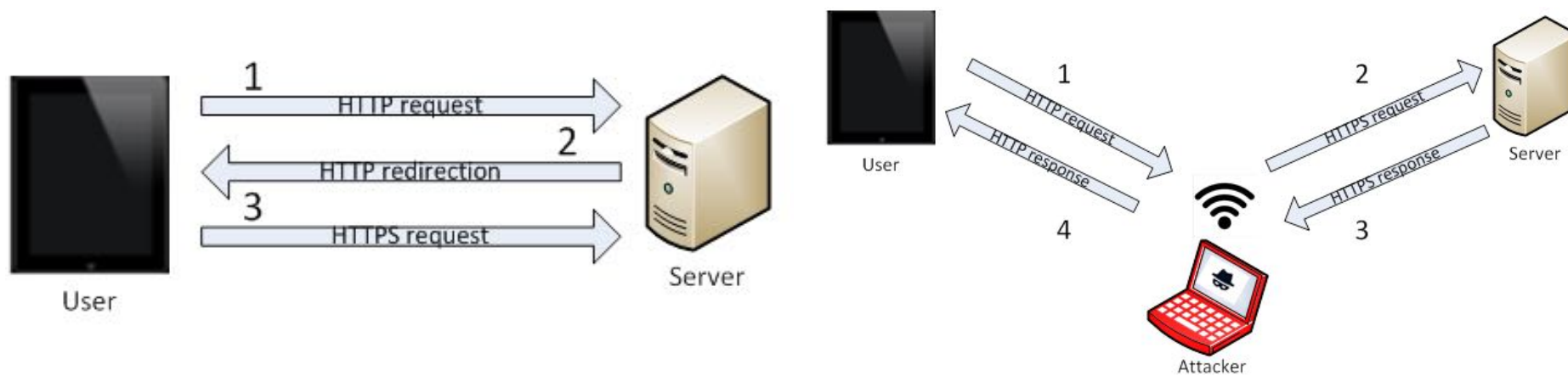
อัปเดต phpMyAdmin ให้เป็นเวอร์ชันใหม่ล่าสุด โดยสามารถดูรายละเอียดได้ที่

- <https://www.phpmyadmin.net/downloads/>

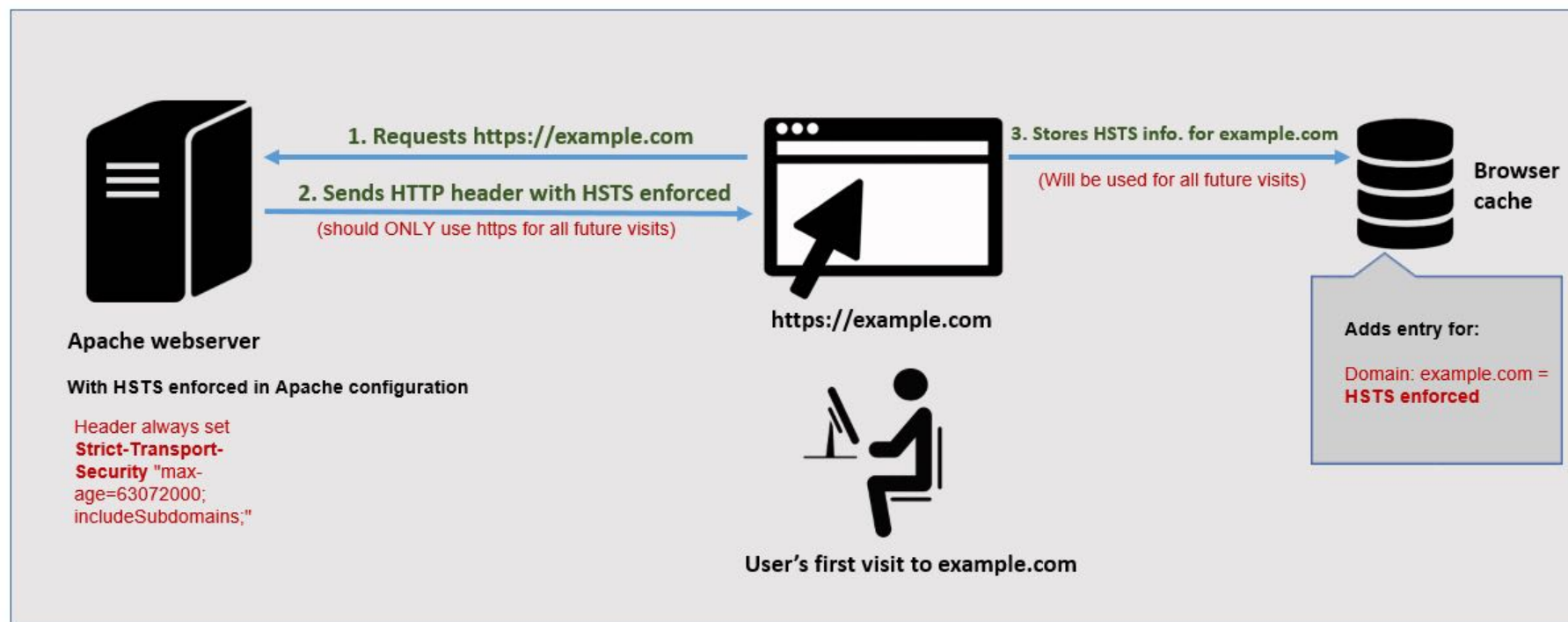
## 6. ไม่มีการเปิดใช้งาน HTTP Strict-Transport-Security (HSTS)



ระดับความเสี่ยง	ต่ำ
อ้างอิง	OWASP Top 10 - 2017 A6 - Security Misconfiguration
จุดที่ตรวจพบ	<a href="https://tcr.degitoprojects.com/">https://tcr.degitoprojects.com/</a>



## 6. ไม่มีการเปิดใช้งาน HTTP Strict-Transport-Security (HSTS)



Web server with HTTP Strict Transport Security (HSTS) enforced

## 6. ไม่มีการเปิดใช้งาน HTTP Strict-Transport-Security (HSTS)



Request		Response		
Raw	Headers	Hex	HTML	Render
<pre>HTTP/1.1 302 Found Date: Sun, 13 May 2018 09:08:11 GMT Server: Apache/2.4.18 (Ubuntu) Vary: Accept-Language Cache-Control: no-cache, private Location: https://tcr.degitoprojects.com/en Set-Cookie: XSRF-TOKEN=eyJpdiI6ImVzcmZJVnJwTDNiVGRNWEFnR1 ST2wwblpQXC84ZzZpQnNTUUE9PSIsIm1hYyI6IjBkZjFi 11:08:11 GMT; Max-Age=7200; path=/ Set-Cookie: laravel_session=eyJpdiI6ImcwaWs5NmVwZlRVRGIwS tKUytadWY2ZHVCtL3J6TzVZMGJqdz09IiwibWFjIjoiaZ Content-Length: 376 Connection: close Content-Type: text/html; charset=UTF-8</pre>				

Request		Response		
Raw	Headers	Hex	HTML	Render
<pre>HTTP/1.1 200 OK Date: Sun, 13 May 2018 09:08:12 GMT Server: Apache/2.4.18 (Ubuntu) Cache-Control: no-cache, private Set-Cookie: XSRF-TOKEN=eyJpdiI6IlBGa1pCZTFmcml6bly2cGl0 yQnFDRlRtbVJlUnhDZzVnPT0iLCJtYWMiOiIzMzdHNj 11:08:12 GMT; Max-Age=7200; path=/ Set-Cookie: laravel_session=eyJpdiI6ImpBXC9VMXRnMkk4Wll 5QZFBZdFwvVGsybkdvU05rWVhTZz09IiwibWFjIjoiaZ Vary: Accept-Encoding Content-Length: 172397 Connection: close Content-Type: text/html; charset=UTF-8</pre>				



## 6. ไม่มีการเปิดใช้งาน HTTP Strict-Transport-Security (HSTS)



### วิธีการแก้ไข

เปิดใช้งาน Strict-Transport-Security Header

```
# Optionally load the headers module:  
LoadModule headers_module modules/mod_headers.so  
  
<VirtualHost *:443>  
    Header always set Strict-Transport-Security "max-age=63072000; includeSubdomains;"  
</VirtualHost>
```

## 7. มีการตั้งค่าการใช้งาน HTTPS ที่ไม่ปลอดภัย



ระดับความเสี่ยง	ต่ำ
อ้างอิง	OWASP Top 10 - 2017 A6 - Security Misconfiguration
จุดที่ตรวจพบ	<a href="https://tcr.degitoprojects.com/">https://tcr.degitoprojects.com/</a>



### Protocols

TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

For TLS 1.3 tests, we currently support draft version 18.

TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)	ECDH secp256r1 (eq. 3072 bits RSA) FS	WEAK	112
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)	DH 2048 bits FS	WEAK	112
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)		WEAK	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)		WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)		WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)		WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)		WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)		WEAK	256
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)		WEAK	112

## 7. มีการตั้งค่าการใช้งาน HTTPS ที่ไม่ปลอดภัย



### วิธีการแก้ไข

- ปิดการสนับสนุน TLSv1.0 โดยการแก้ไขไฟล์ ssl.conf ที่ Parameter SSLProtocol

```
SSLProtocol TLSv1.2 TLSv1.3
```

- ปิดการสนับสนุน Cipher Suite ที่ไม่มีความปลอดภัย โดยการแก้ไขไฟล์ ssl.conf ที่ Parameter SSLCipherSuite

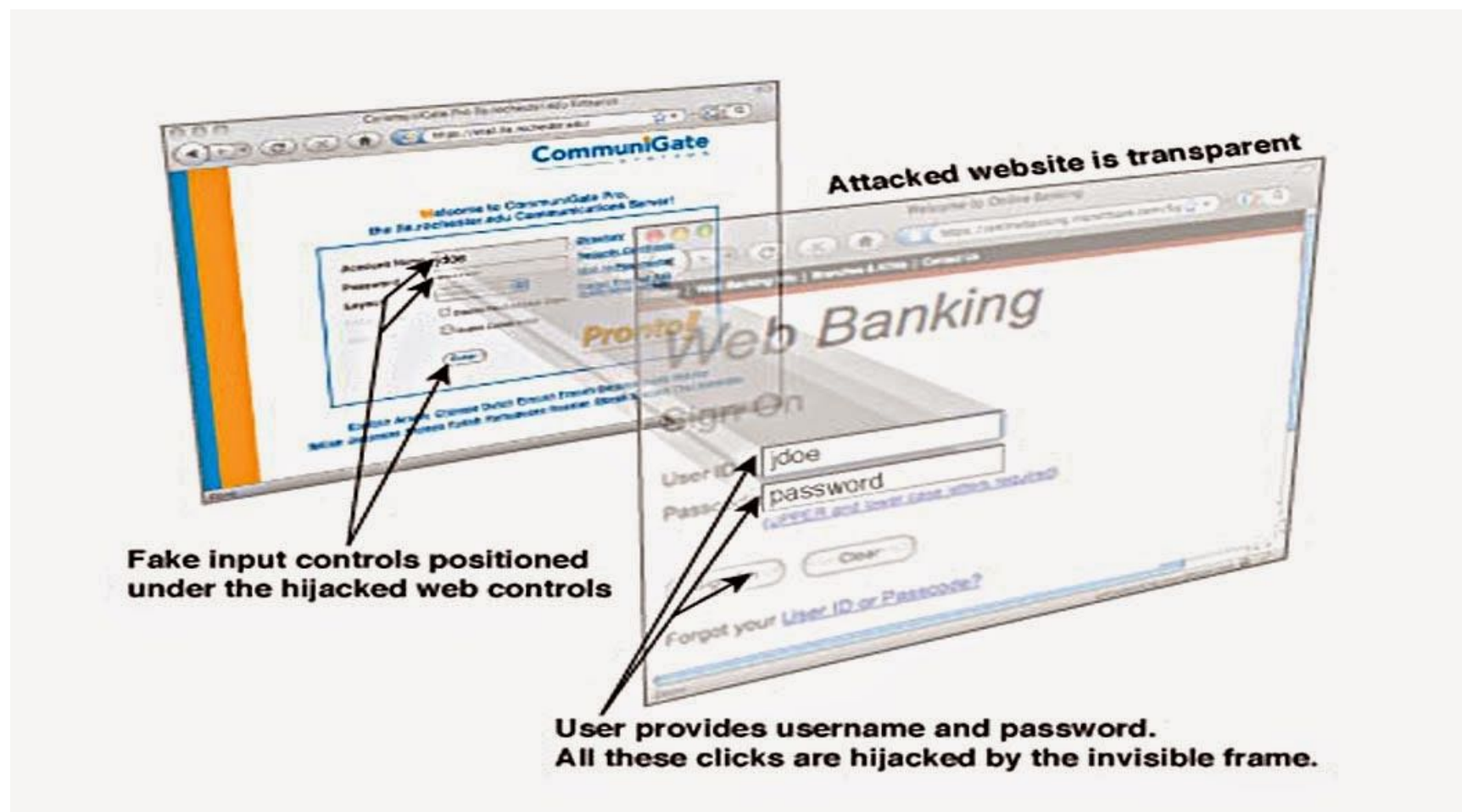
```
SSLCipherSuite <List ของ Cipher suite ปัจจุบัน> !ECDHE-RSA-DES-CBC3-SHA !EDH-RSA-DES-CBC3-SHA  
!AES128-GCM-SHA256 !AES256-GCM-SHA384 !AES128-SHA256 !AES256-SHA256 !AES128-SHA  
!AES256-SHA !DES-CBC3-SHA
```



## 8. Clickjacking



ระดับความเสี่ยง	ต่ำ
อ้างอิง	OWASP Top 10 - 2017 A6 - Security Misconfiguration
จุดที่ตรวจพบ	<a href="https://tcr.degitoprojects.com/">https://tcr.degitoprojects.com/</a>



## 8. Clickjacking



Response เมื่อ Request ไปยัง <https://tcr.degitoprojects.com/en>

Request		Response		
Raw	Headers	Hex	HTML	Render
<pre>HTTP/1.1 200 OK Date: Mon, 14 May 2018 15:35:14 GMT Server: Apache/2.4.18 (Ubuntu) Cache-Control: no-cache, private Set-Cookie: XSRF-TOKEN=eyJpdiI6IlE5TlVVaEc3amNWbWNWNGc2 KZ1wvUkdCblhxYzQ2aDJkZ0E9PSIsIm1hYyI6IjJhMm 17:35:14 GMT; Max-Age=7200; path=/ Set-Cookie: laravel_session=eyJpdiI6IkZKVFAwdWNGSGhkbXB 8zb1VKRWJzcEFBcGd1Z09HQVNcLzZadz09IiwibWFjI Vary: Accept-Encoding Content-Length: 172397 Connection: close Content-Type: text/html; charset=UTF-8</pre>				

## 8. Clickjacking



Response เมื่อ Request ไปยัง <https://tcr.degitoprojects.com/2561/tcr/backend/console/login>

Request	Response
Raw	Headers
Hex	HTML
Render	

```
HTTP/1.1 200 OK
Date: Mon, 14 May 2018 15:38:06 GMT
Server: Apache/2.4.18 (Ubuntu)
Cache-Control: no-cache, private
Set-Cookie:
XSRF-TOKEN=eyJpdiI6InBEd3FxUVRGb2g5STlU
3b1pBVEVkmZnkwVmRGc9PSIsIm1hYyI6ImQyYm'
17:38:06 GMT; Max-Age=7200; path=/
Set-Cookie:
laravel_session=eyJpdiI6IkE5Zis1Nk54bk0
ZoTVZnUldjaWk5eElwQU5NcmhRPT0iLCJtYWMiO
Vary: Accept-Encoding
Content-Length: 6222
Connection: close
Content-Type: text/html; charset=UTF-8
```

## 8. Clickjacking



### วิธีการแก้ไข

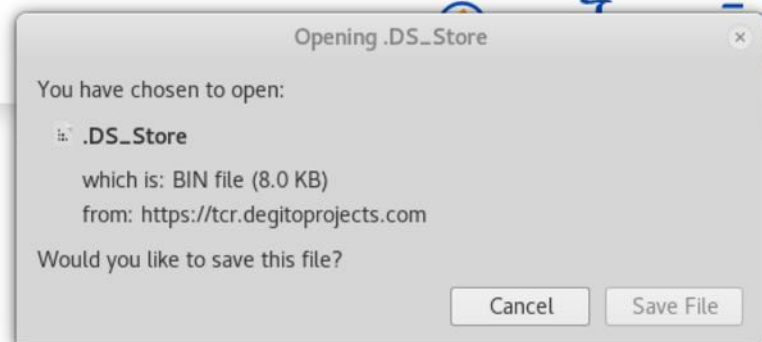
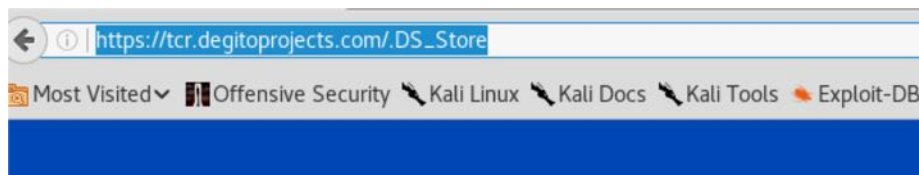
ตั้งค่าเพื่อใช้งาน X-Frame-Options Header โดยแก้ไขไฟล์ httpd.conf

Header always append **X-Frame-Options SAMEORIGIN**;

## 9. สามารถเข้าถึงไฟล์ .DS\_Store บนเว็บไซต์ได้



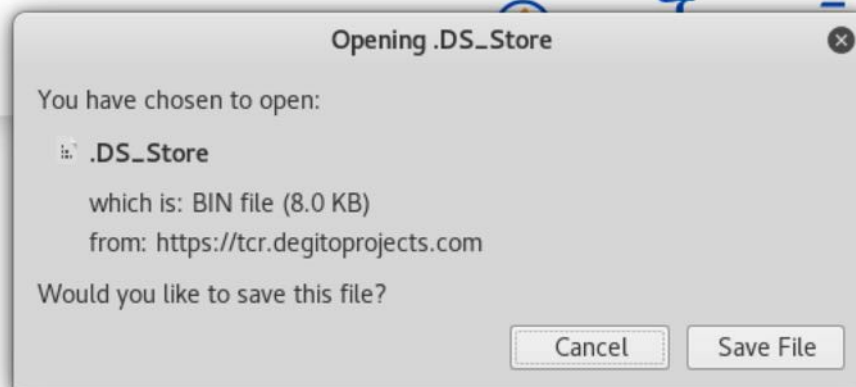
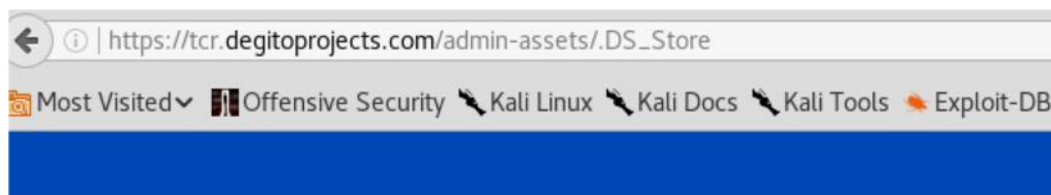
ระดับความเสี่ยง	ต่ำ
อ้างอิง	OWASP Top 10 - 2017 A3 - Sensitive Data Exposure
จุดที่ตรวจพบ	<a href="https://tcr.degitoprojects.com/.DS_Store">https://tcr.degitoprojects.com/.DS_Store</a> <a href="https://tcr.degitoprojects.com/admin-asset/.DS_Store">https://tcr.degitoprojects.com/admin-asset/.DS_Store</a>



```
root@Demon:~/Downloads/fdb_1.0/fdb# ./fdb.pl -type ds --filename '/root/Downloads/DS_Store.oct
et-stream' --base_url http://tcr.degitoprojects.com/ --verbose
URL: http://tcr.degitoprojects.com/.idea
URL: http://tcr.degitoprojects.com/.idea
URL: http://tcr.degitoprojects.com/.idea
URL: http://tcr.degitoprojects.com/.idea
URL: http://tcr.degitoprojects.com/.idea
URL: http://tcr.degitoprojects.com/.sass-cache
URL: http://tcr.degitoprojects.com/.well-known
URL: http://tcr.degitoprojects.com/admin-assets
URL: http://tcr.degitoprojects.com/admin-assets
URL: http://tcr.degitoprojects.com/admin-assets
URL: http://tcr.degitoprojects.com/admin-assets
URL: http://tcr.degitoprojects.com/admin-assets
URL: http://tcr.degitoprojects.com/css
URL: http://tcr.degitoprojects.com/css
URL: http://tcr.degitoprojects.com/css
URL: http://tcr.degitoprojects.com/css
URL: http://tcr.degitoprojects.com/dependencies
URL: http://tcr.degitoprojects.com/dependencies
URL: http://tcr.degitoprojects.com/dependencies
URL: http://tcr.degitoprojects.com/dependencies
URL: http://tcr.degitoprojects.com/dependencies
URL: http://tcr.degitoprojects.com/js
URL: http://tcr.degitoprojects.com/js
URL: http://tcr.degitoprojects.com/js
URL: http://tcr.degitoprojects.com/js
```



## 9. สามารถเข้าถึงไฟล์ .DS\_Store บนเว็บไซต์ได้



```
root@Demon:~/Downloads/fdb_1.0/fdb# ./fdb.pl -type ds --filename '/root/Downloads/DS_Store(1)
--base_url http://tcr.degitoprojects.com/admin-assets --verbose
URL: http://tcr.degitoprojects.com/admin-assets/data
URL: http://tcr.degitoprojects.com/admin-assets/data
URL: http://tcr.degitoprojects.com/admin-assets/fonts
URL: http://tcr.degitoprojects.com/admin-assets/fonts
URL: http://tcr.degitoprojects.com/admin-assets/icon-font
URL: http://tcr.degitoprojects.com/admin-assets/icon-font
URL: http://tcr.degitoprojects.com/admin-assets/icon-font
URL: http://tcr.degitoprojects.com/admin-assets/images
URL: http://tcr.degitoprojects.com/admin-assets/images
URL: http://tcr.degitoprojects.com/admin-assets/images
URL: http://tcr.degitoprojects.com/admin-assets/scripts
URL: http://tcr.degitoprojects.com/admin-assets/scripts
URL: http://tcr.degitoprojects.com/admin-assets/scripts
URL: http://tcr.degitoprojects.com/admin-assets/styles
URL: http://tcr.degitoprojects.com/admin-assets/styles
URL: http://tcr.degitoprojects.com/admin-assets/vendor
URL: http://tcr.degitoprojects.com/admin-assets/vendor
URL: http://tcr.degitoprojects.com/admin-assets/vendor
URL: http://tcr.degitoprojects.com/admin-assets/vendor
```

## 9. สามารถเข้าถึงไฟล์ .DS\_Store บนเว็บไซต์ได้



### วิธีการแก้ไข

ลบไฟล์ .DS\_Store ทุกไฟล์ที่มีอยู่บนเว็บไซต์

## 10. หน้าแสดงข้อความ Error แสดงข้อมูลที่มีความสำคัญต่อเว็บไซต์ออกมามากเกินไป



ระดับความเสี่ยง	ต่ำ
อ้างอิง	OWASP Top 10 - 2017 A3 - Sensitive Data Exposure
จุดที่ตรวจพบ	<a href="https://tcr.degitoprojects.com/">https://tcr.degitoprojects.com/</a>

```
(3/3) ErrorException
Undefined variable: errors (View: /var/www/html/tcr/laravel/resources/views/template/layout/home.blade.php) (View: /var/www/html/tcr/laravel/resources/views/template/layout/home.blade.php)

in d3abc6060f834c82a95ebcf70782169d5c6e7cf2.php line 339

at CompilerEngine->handleViewException(object(ErrorException), 1)
in PhpEngine.php line 44

at PhpEngine->evaluatePath('/var/www/html/tcr/laravel/storage/framework/views/157f70e2dbcfd934f0db20f39506603d52cc.php', array('__env' => object(Factory), 'app' => object(Application), 'exception' => object(NotFoundHttpException)))
in CompilerEngine.php line 59

at CompilerEngine->get('/var/www/html/tcr/laravel/resources/views/errors/404.blade.php', array('__env' => object(Factory), 'app' => object(Application), 'exception' => object(NotFoundHttpException)))
in View.php line 137

at View->getContents()
in View.php line 120

at View->renderContents()
in View.php line 85

at View->render()
in Response.php line 38
```



## 10. หน้าแสดงข้อความ Error แสดงข้อมูลที่มีความสำคัญต่อเว็บไซต์ออกมามากเกินไป



### วิธีการแก้ไข

- ปิด Debug Mode ของ Laravel Framework โดยการแก้ไข Parameter APP\_DEBUG ในไฟล์ .env

```
APP_DEBUG=false;
```

- แสดงหน้า Custom Error Page แทนการแสดงข้อความ Errorr ออกมาโดยตรง โดยสามารถดูวิธีการได้ที่
  - <https://laravel.com/docs/5.6/errors#custom-http-error-pages>

