การรายงานสรุปผลการทดสอบเจาะระบบ (Penetration Testing)
เว็บไซต์ tcr.degitoprojects.com

ธนาคาร ไทยเครดิต เพื่อรายย่อย

PENETRATION TESTING SERVICE

วาระการประชุม

- ขอบเขตงาน
- บทสรุปผู้บริหาร
- สรุปช่องโหว่ที่ตรวจพบ
- รายละเอียดช่องโหว่ที่ตรวจพบ

ขอบเขตของงาน และ แผนการดำเนินโครงการ

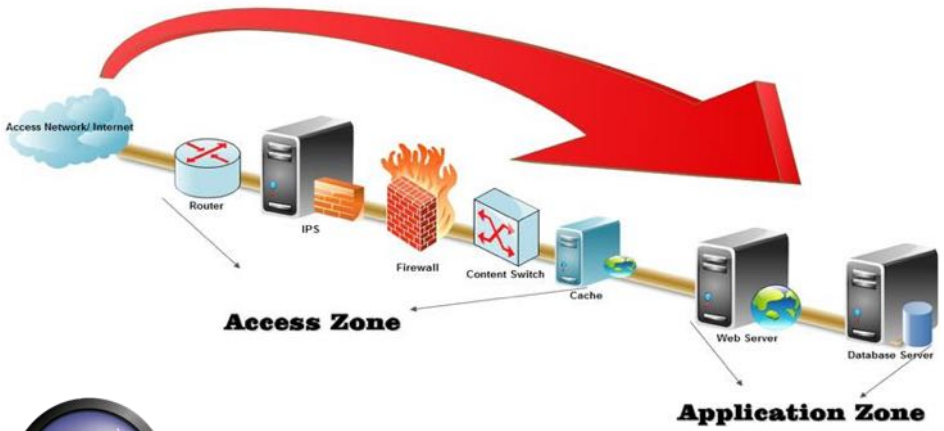
เป้าหมายที่ทำการทดสอบ	tcr.degitoprojects.com
รูปแบบในการทดสอบ	Black-box Testing
ระยะเวลาที่ทำการทดสอบ	12 พฤษภาคม 2561 – 14 พฤษภาคม 2561
นำเสนอช่องโหว่	18 พฤษภาคม 2561
ทดสอบซ้ำ	TBD

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

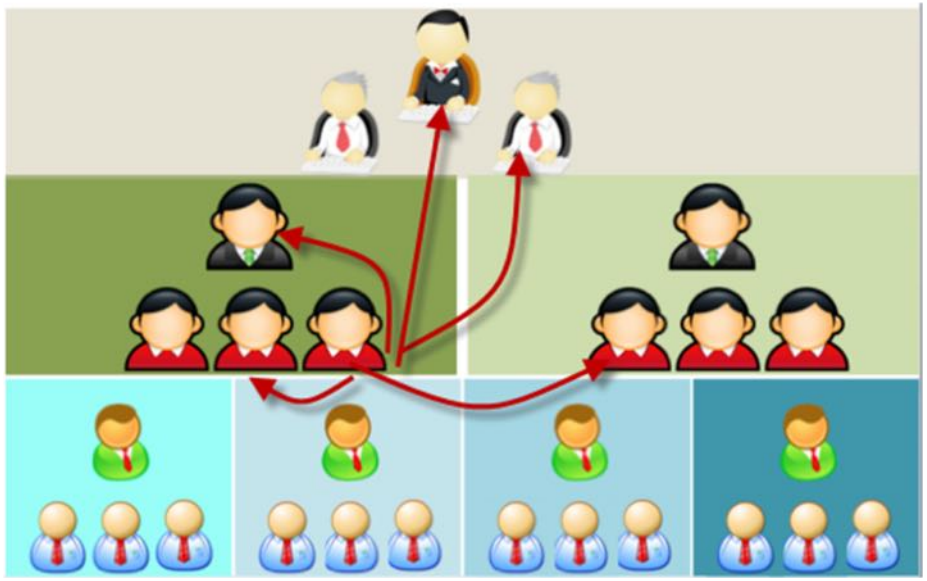
ระเบียบวิธีการทดสอบ

Web Application Penetration Testing

- ตรวจสอบช่องโหว่ทางเทคนิค
- ตรวจสอบช่องโหว่ทาง Business Logic



OWASP
Open Web Application Security Project



ข้อจำกัด

Known vulnerabilities

Window Time

Snapshot in time

บทสรุปผู้บริหาร

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

- **เว็บไซต์ไม่มีการป้องกันการเข้าถึงไฟล์ .env ทำให้ผู้ไม่ประสงค์ดีทราบถึงรหัสผ่านของ Database ที่เก็บไว้ในไฟล์ และเข้าถึง Database ของทุกเว็บไซต์ได้ทันที**
- **เว็บไซต์ไม่มีการตรวจสอบการอัพโหลดไฟล์ที่ดี ส่งผลให้ผู้ไม่ประสงค์ดีสามารถอัพโหลด 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 อาจจะเกิดได้สักครั้ง หรือแทบเป็นไปไม่ได้ที่จะเกิดขึ้น

VA Scan vs Pentest

skipfish
WEB APP SCANNER

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)

Qualys®

View by: OWASP Report | Patch Report | Threat Report — Print Report

Vulnerability Scan rename
External Host Vulnerability Report

12 May 2018 at 7:37AM (GMT+0700)

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.

Nessus™

Hosts > 54.169.224.153 > Vulnerabilities 36

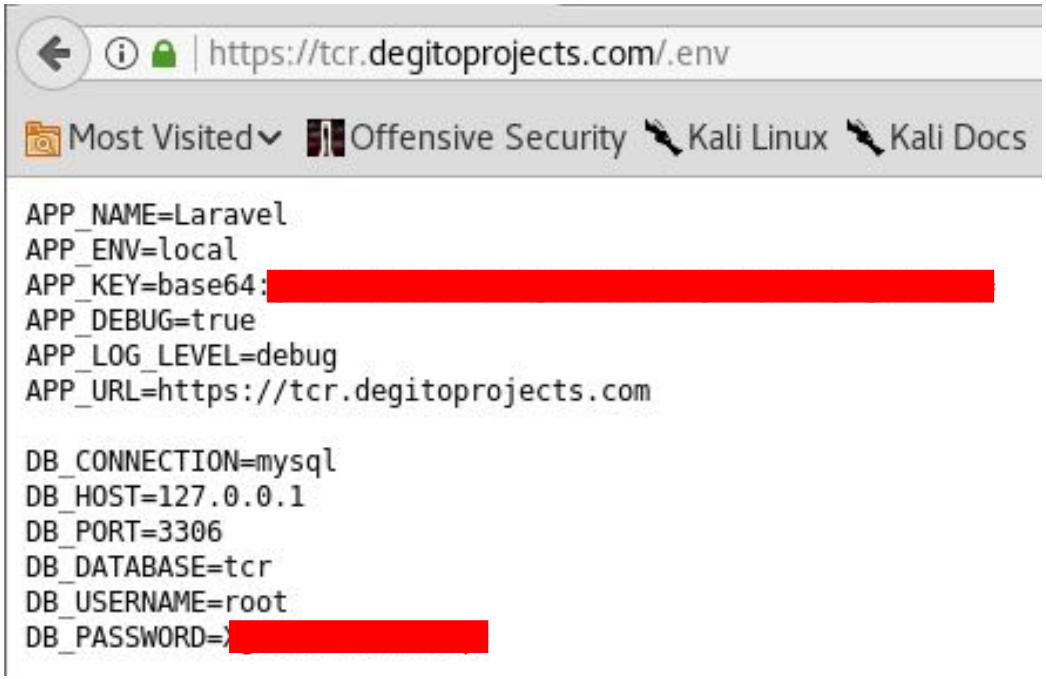
Severity	Plugin Name	Plugin Family	Count
MEDIUM	Apple Mac OS X Find-By-Content .DS_Store Web Directory Listing	Web Servers	1
MEDIUM	SSL Medium Strength Cipher Suites Supported	General	1
INFO	Service Detection	Service detection	4

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	https://tcr.degitoprojects.com/.env https://tcr.degitoprojects.com/laravel/.env



1. ไม่มีการป้องกันการเข้าถึงไฟล์ .env

วิธีการแก้ไข

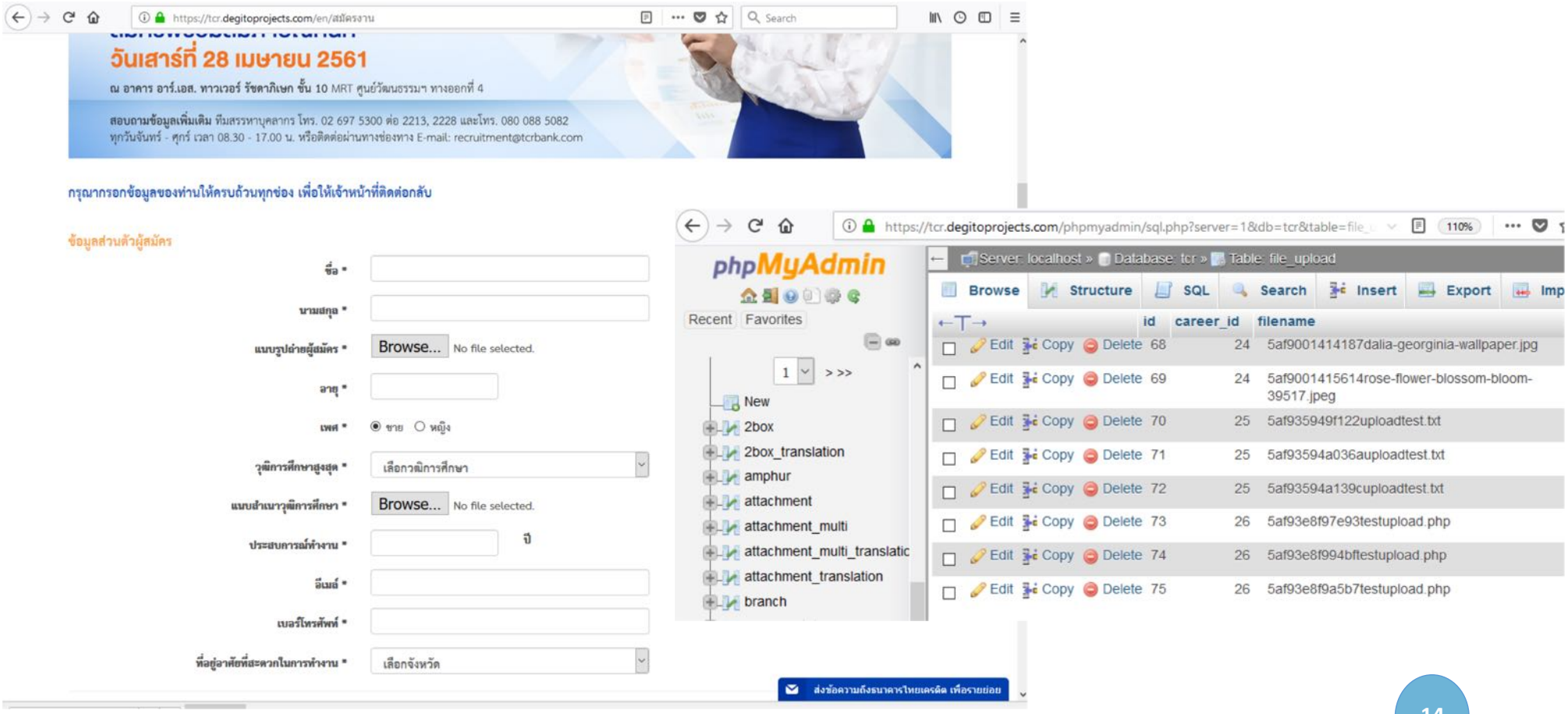
Option 1: ป้องกันการข้าถึงไฟล์โดยใช้ .htaccess

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

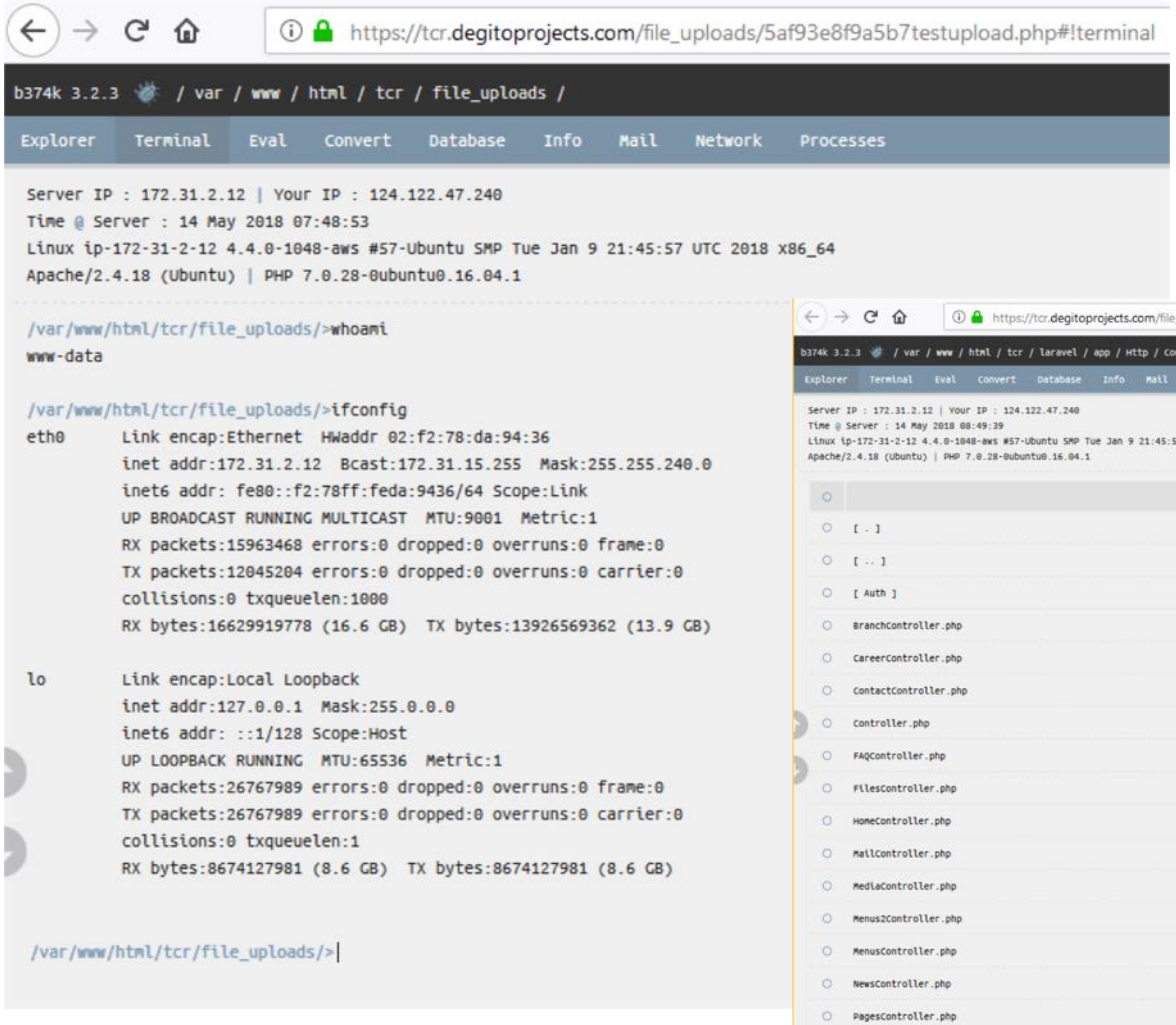
Option 2: ไม่เก็บไฟล์ .env ไว้ใน Public Folder หรือที่ ๆ สามารถ Browse เข้าถึงได้จากผู้ใช้งานทั่วไป

2. Malicious File Upload

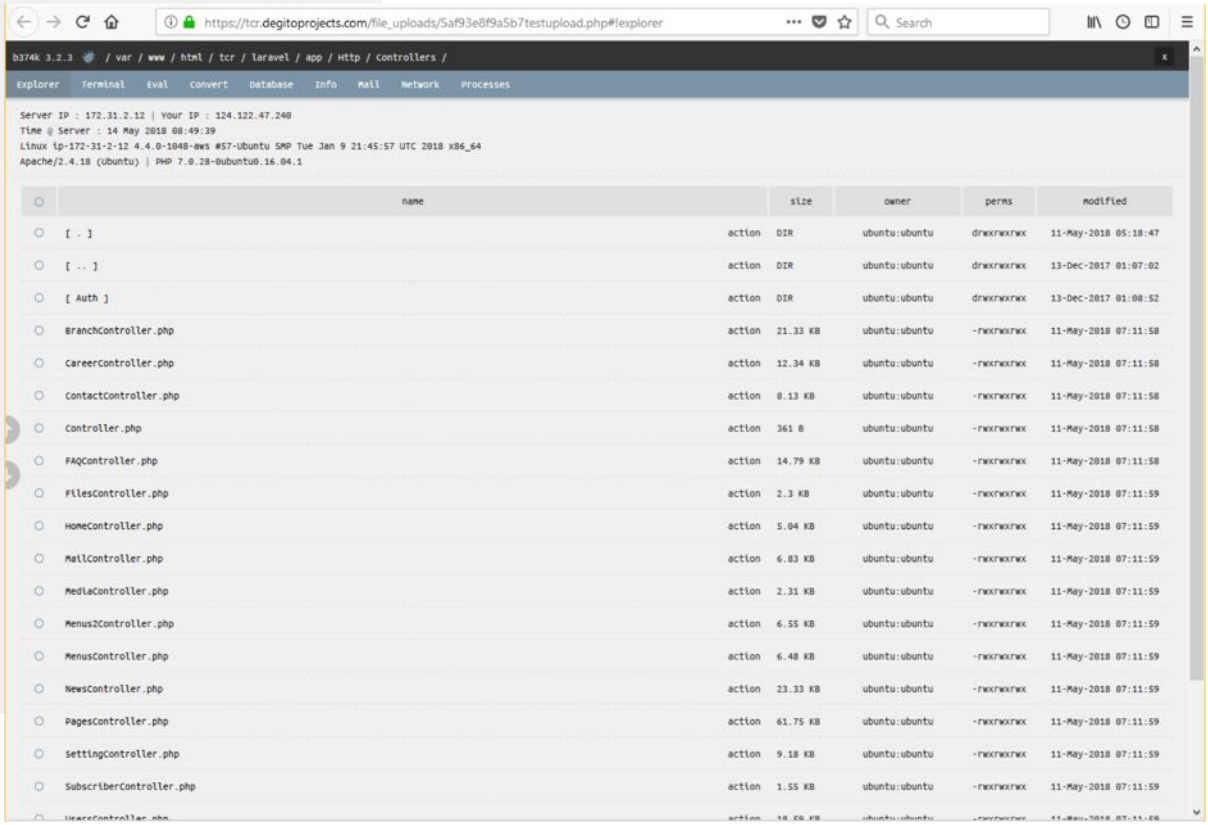
ระดับความเสี่ยง	สูง
อ้างอิง	OWASP Top 10 - 2017 A6 - Security Misconfiguration
จุดที่ตรวจพบ	https://tcr.degitoprojects.com/en/สมัครงาน https://tcr.degitoprojects.com/contact/sendmailjob



2. Malicious File Upload

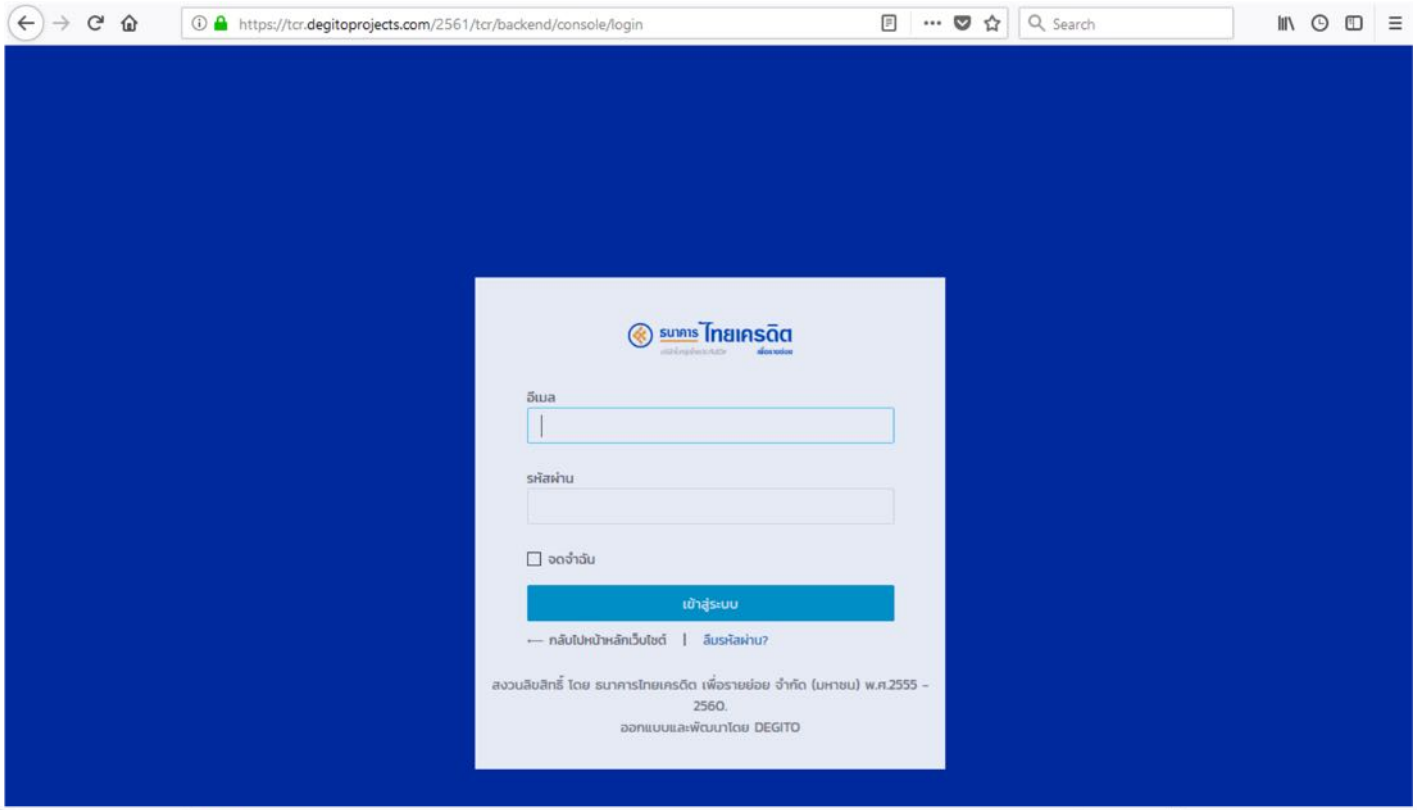


ทำการหาข้อมูลเพิ่มเติมบนเครื่องเซิฟเวอร์จึงพบ path ไปสู่หน้า admin console

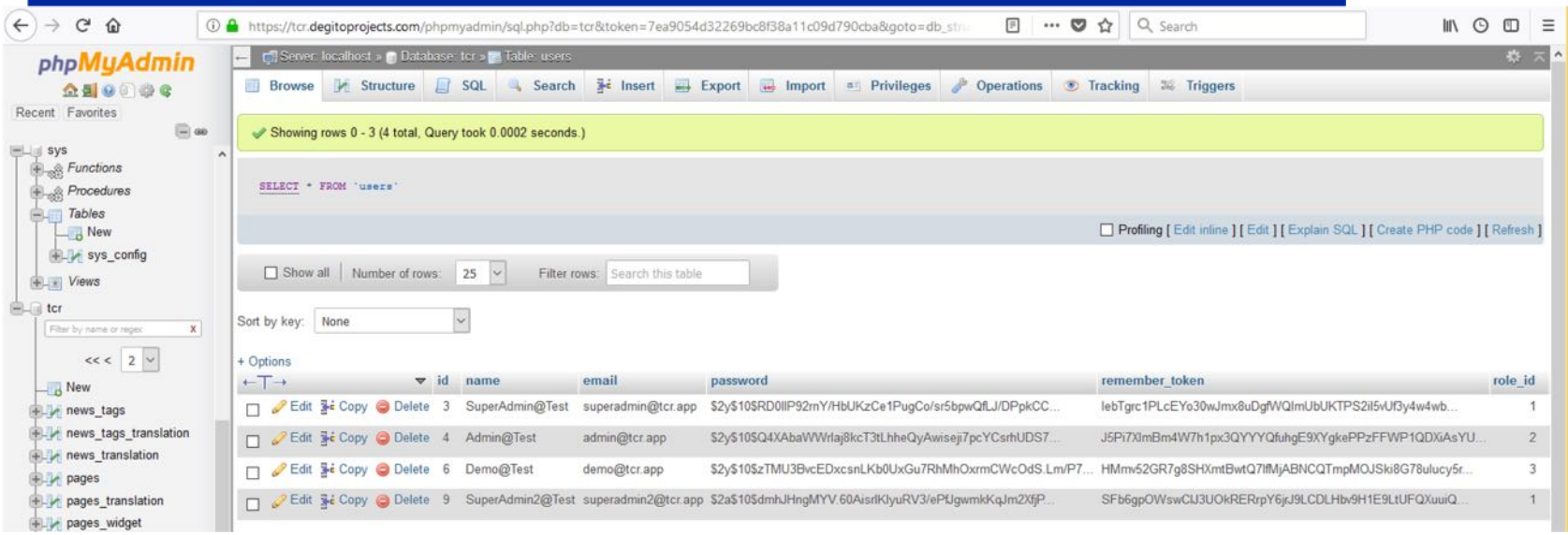



```
return redirect('/2561/tcr/backend/console/admin/menus/menu')->withErrors([
    'success' => 'สร้างเมนูไอเท็มเรียบร้อยแล้ว.',
]);
```

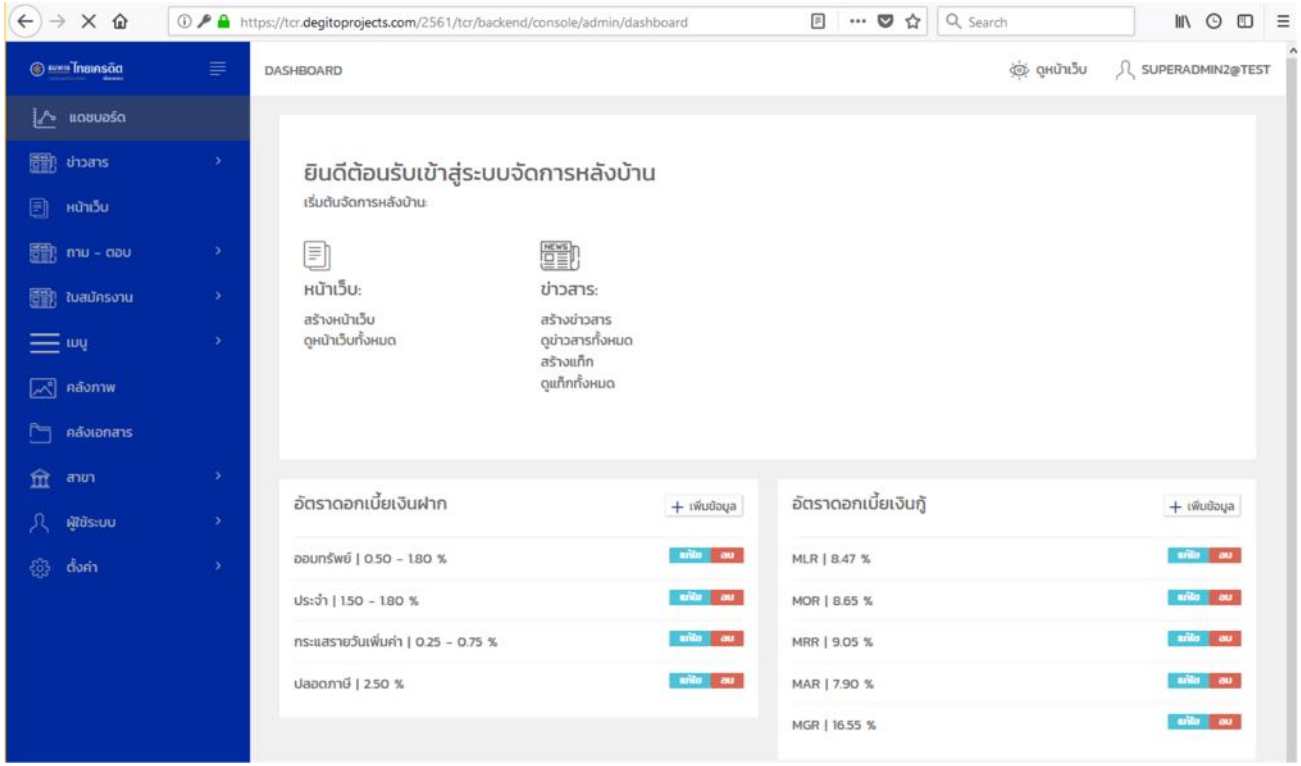
2. Malicious File Upload

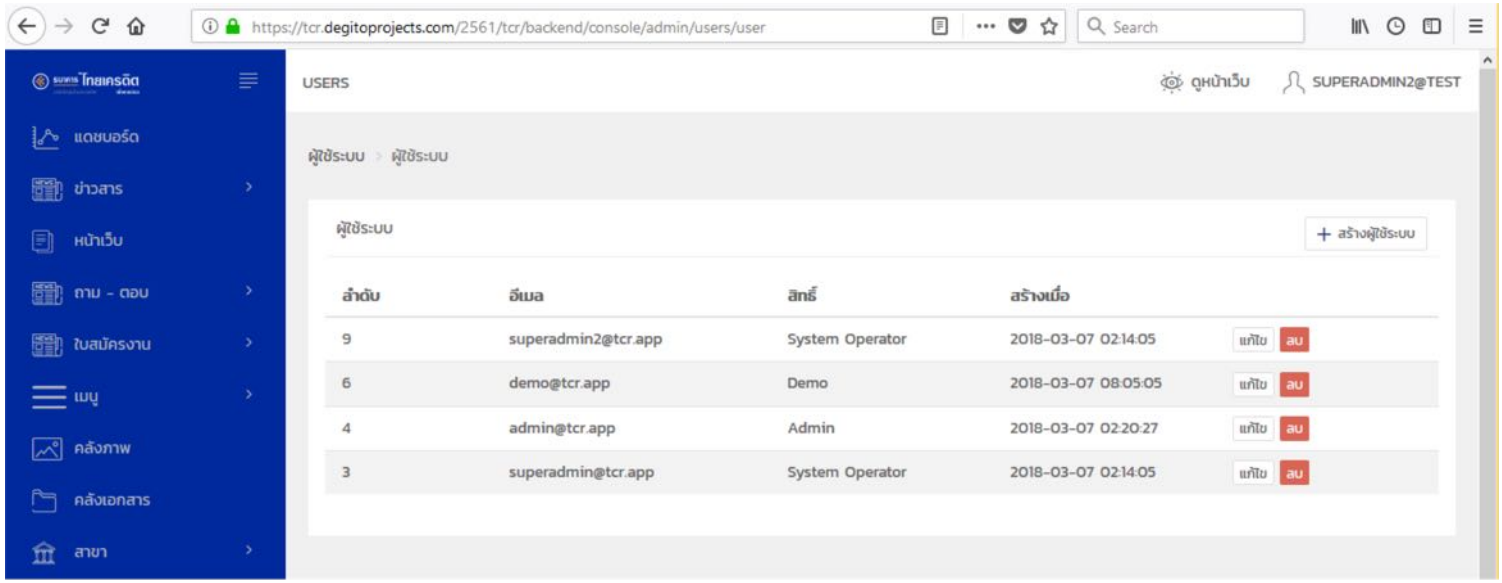


ทำการเพิ่มผู้ใช้งานลงไปในฐานข้อมูลทาง phpMyAdmin เพื่อทำการเข้าสู่ระบบ admin console



2. Malicious File Upload





2. Malicious File Upload

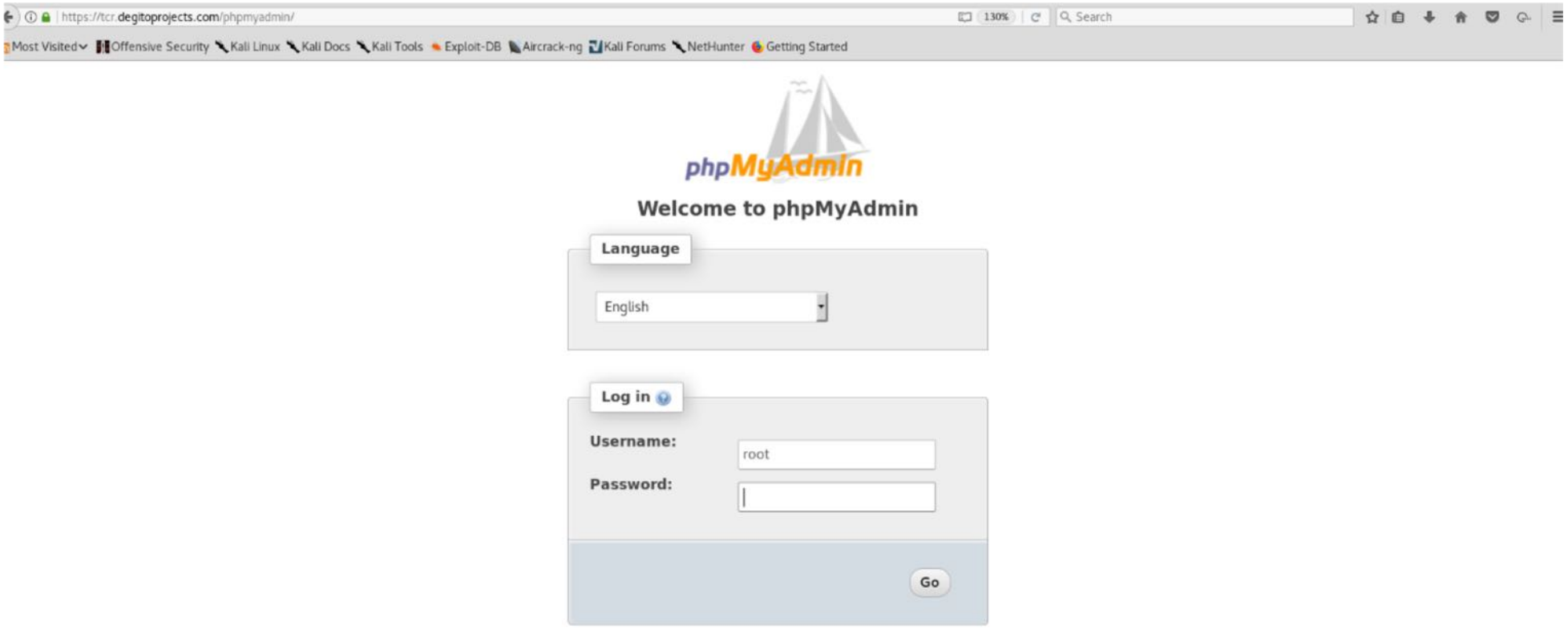
<u>วิธีการแก้ไข</u>

ตรวจสอบและจำกัดประเภทไฟล์ที่สามารถ Upload ได้ทั้งฝั่ง Front End และ Back End โดยสามารถดูวิธีการเพิ่มเติมได้ที่

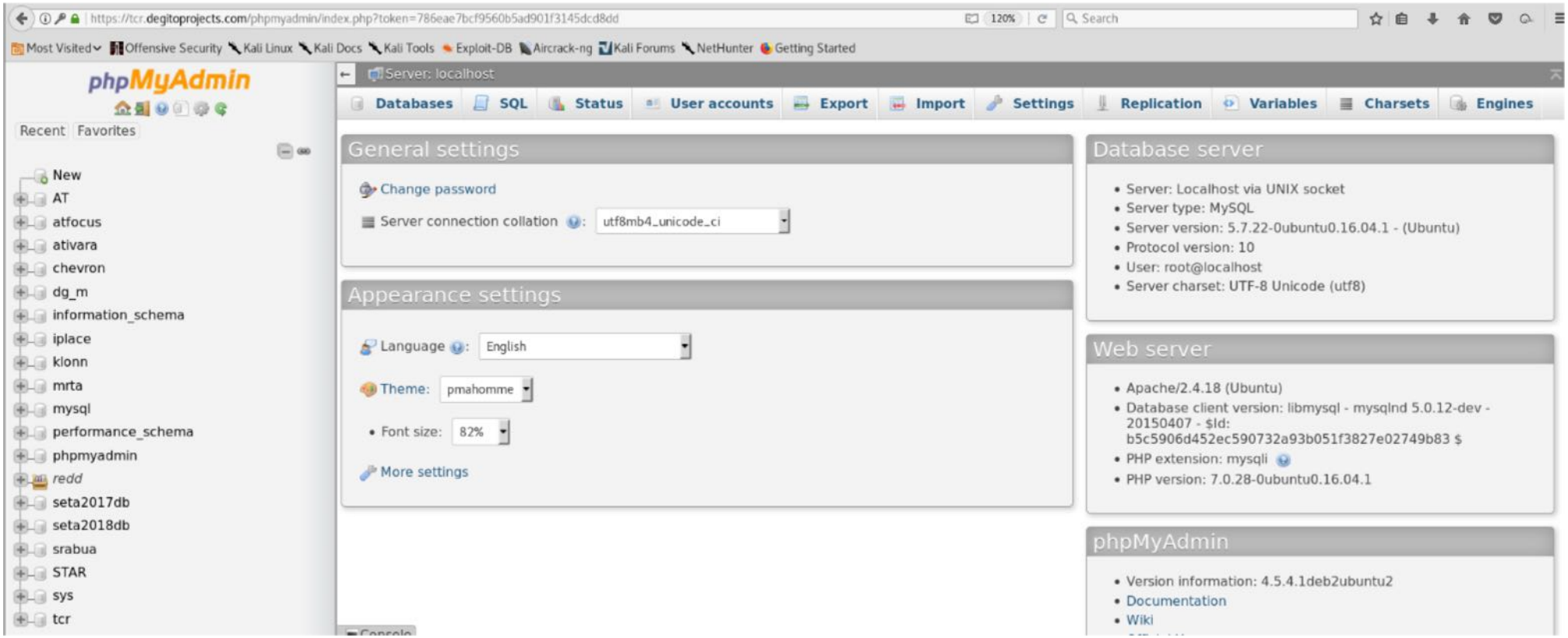
- https://www.owasp.org/index.php/Unrestricted_File_Upload

3.สามารถเข้าถึงหน้า phpMyAdmin ได้จาก Internet

ระดับความเสี่ยง	ปานกลาง
อ้างอิง	OWASP Top 10 - 2017 A6 - Security Misconfiguration
จุดที่ตรวจพบ	https://tcr.degitoprojects.com/phpmyadmin



3.สามารถเข้าถึงหน้า phpMyAdmin ได้จาก Internet



3.สามารถเข้าถึงหน้า phpMyAdmin ได้จาก Internet

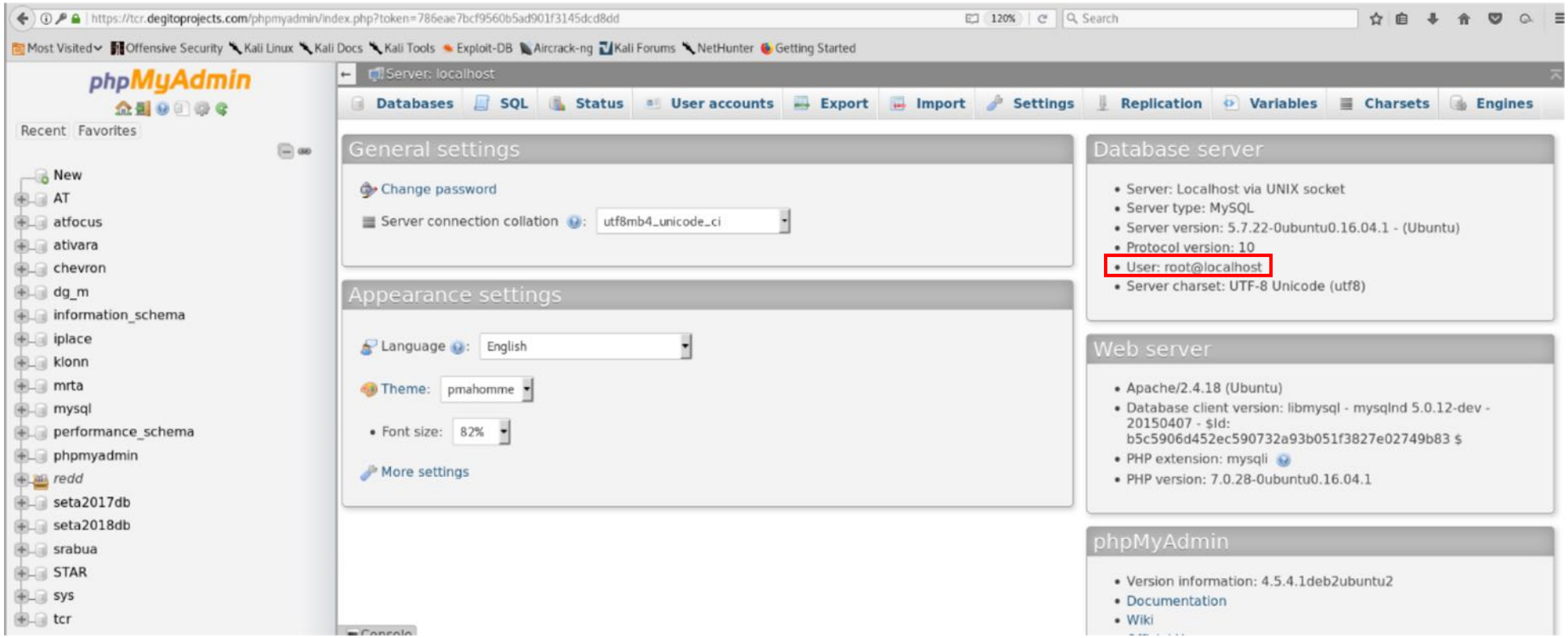
วิธีการแก้ไข

Option 1: จำกัดการเข้าถึง phpMyAdmin ให้เข้าถึงได้จากเฉพาะ IP Address ของผู้ดูแลระบบเท่านั้น

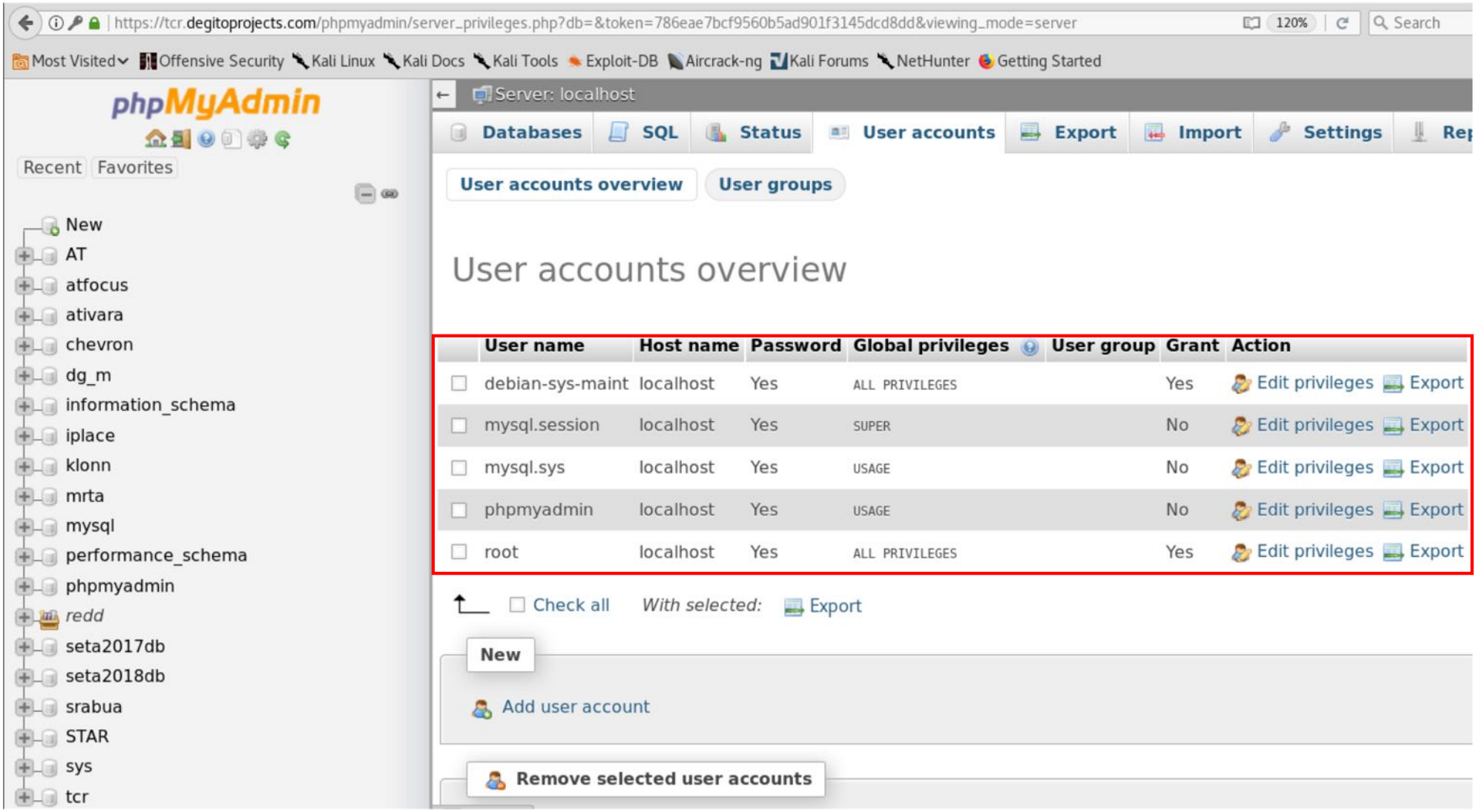
Option 2: ใช้ VPN ในการเข้าถึง phpMyAdmin

4. อนุญาตให้ใช้ root ในการเข้าจัดการ Database

ระดับความเสี่ยง	ปานกลาง
อ้างอิง	OWASP Top 10 - 2017 A6 - Security Misconfiguration
จุดที่ตรวจพบ	https://tcr.degitoprojects.com/phpmyadmin



4. อนุญาตให้ใช้ root ในการเข้าจัดการ Database



4. อนุญาตให้ใช้ root ในการเข้าจัดการ Database

<u>วิธีการแก้ไข</u>

- 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 ที่เป็นเวอร์ชั่นเก่าและมีช่องโหว่

ระดับความเสี่ยง	ปานกลาง
อ้างอิง	OWASP Top 10 - 2017 A9 - Using Components with Known Vulnerabilities
จุดที่ตรวจพบ	https://tcr.degitoprojects.com/phpmyadmin

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	CVE-2018-7260	79		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	CVE-2016-2562	20		+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	CVE-2016-2561	79		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	CVE-2016-2560	79		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	CVE-2016-2559	79		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

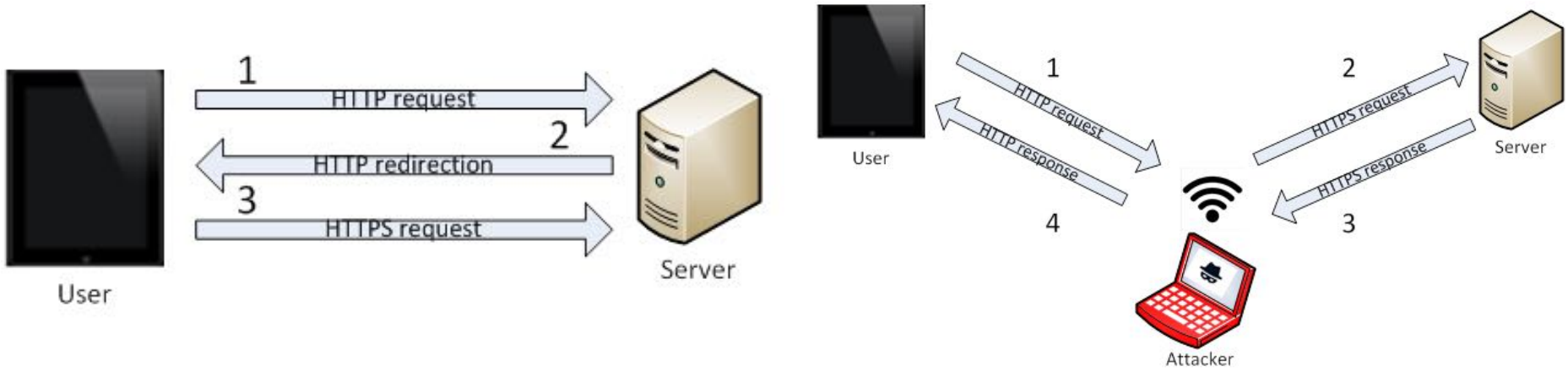
วิธีการแก้ไข

อัพเดท phpMyAdmin ให้เป็นเวอร์ชันใหม่ล่าสุด โดยสามารถดูรายละเอียดได้ที่

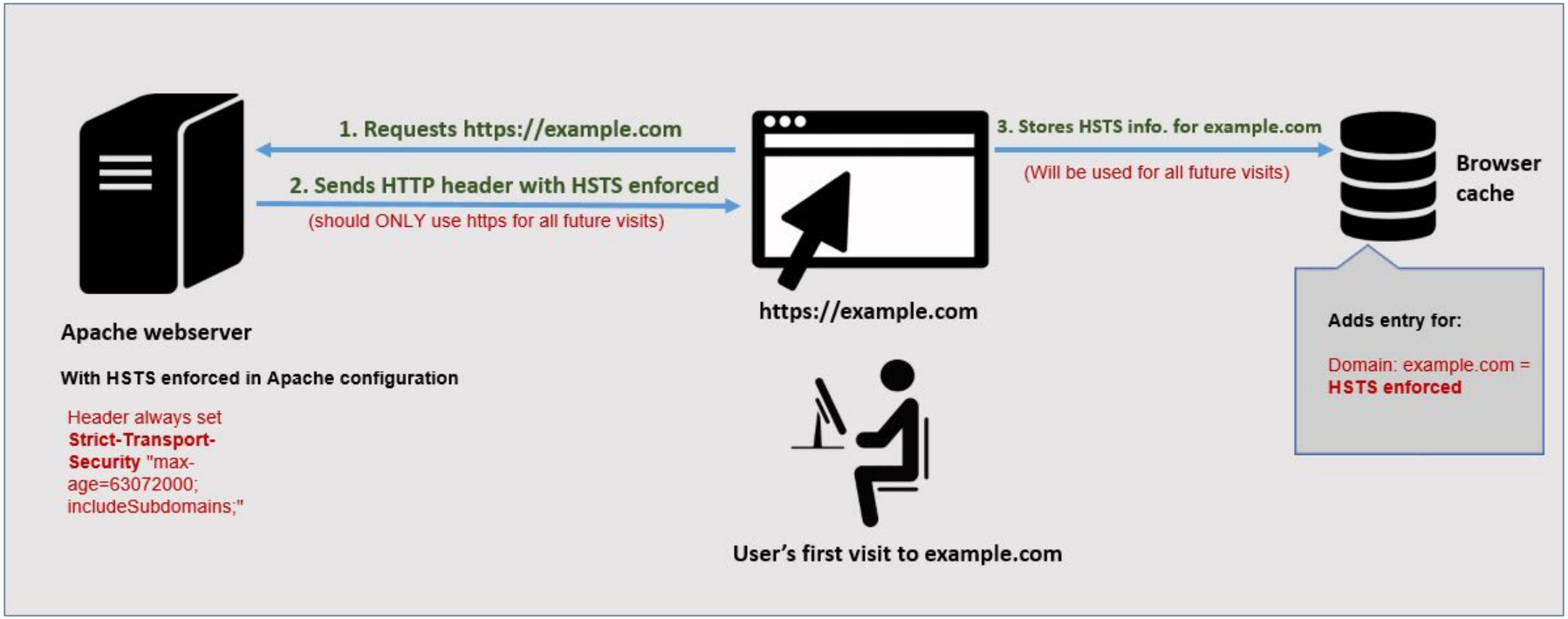
- https://www.phpmyadmin.net/downloads/

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

ระดับความเสี่ยง	ต่ำ
อ้างอิง	OWASP Top 10 - 2017 A6 - Security Misconfiguration
จุดที่ตรวจพบ	https://tcr.degitoprojects.com/



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

```
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
ST2wwb1pQXC84ZzZpQnNTUUE9PSIsIm1hYyI6IjBkZjFi
11:08:11 GMT; Max-Age=7200; path=/
Set-Cookie:
laravel_session=eyJpdiI6ImcwaWs5NmVwZlRVRGIwS
tKUytadWY2ZHVcL3J6TzVZMGJqdz09IiwibWFjIjoiNzF
Content-Length: 376
Connection: close
Content-Type: text/html; charset=UTF-8
```

Request | Response

Raw | Headers | Hex | HTML | Render

```
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
yQnFDR1RtbVJ1UnhDZzVnPT0iLCJtYWMiOiIzMzdhNj
11:08:12 GMT; Max-Age=7200; path=/
Set-Cookie:
laravel_session=eyJpdiI6ImpBXC9VMXRnMkk4Wll
5QZFBZdFwvVGsybkdvU05rWVhTZz09IiwibWFjIjoiZ
Vary: Accept-Encoding
Content-Length: 172397
Connection: close
Content-Type: text/html; charset=UTF-8
```

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	https://tcr.degitoprojects.com/

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

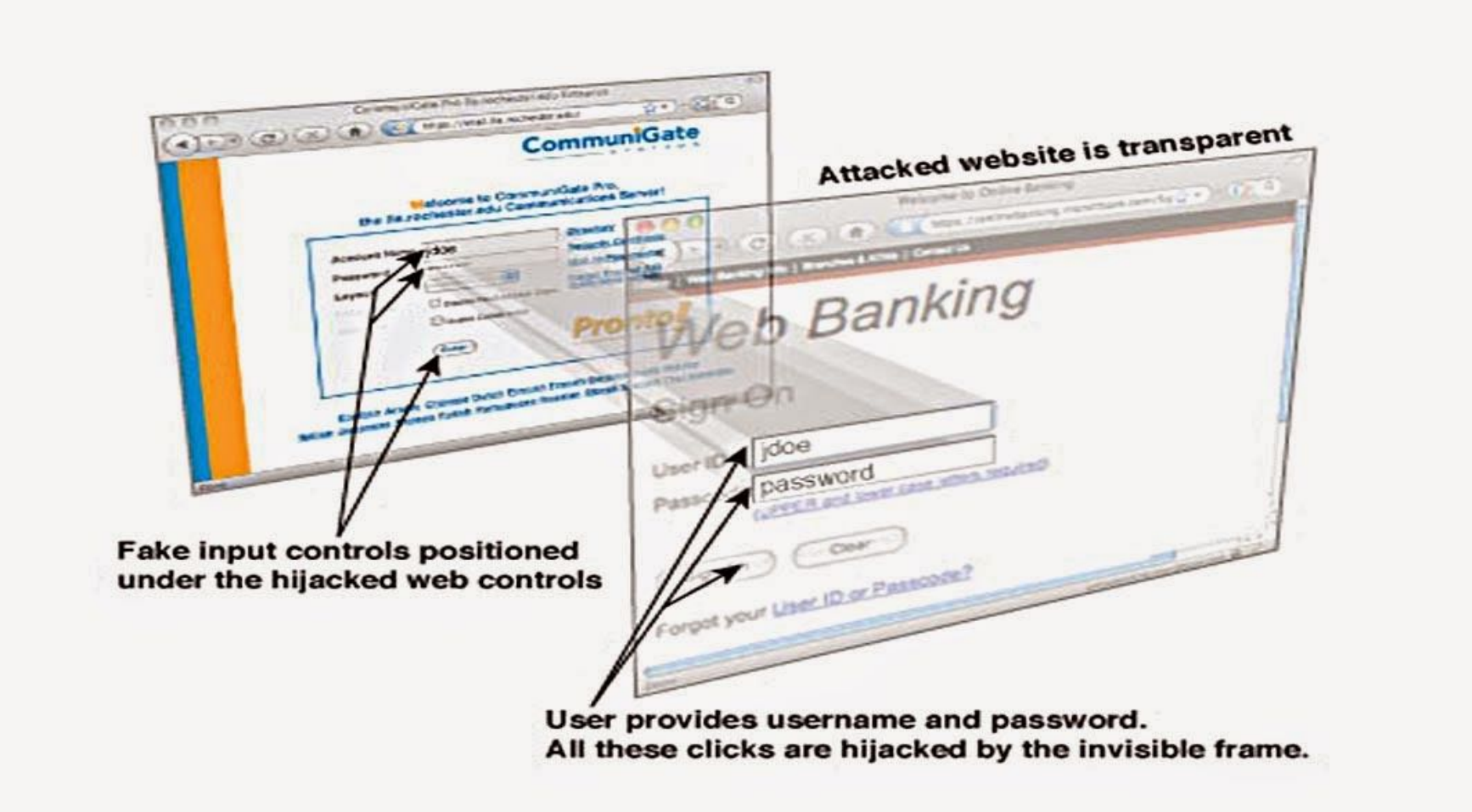
```
SSLProtocol TLSv1.2 TLSv1.3
```

- 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	https://tcr.degitoprojects.com/



8. Clickjacking

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

Request | Response

Raw | Headers | Hex | HTML | Render

```
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
```

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
3b1pBVEVkMzNkWmVmRGc9PSIsIm1hYyI6ImQyYm
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

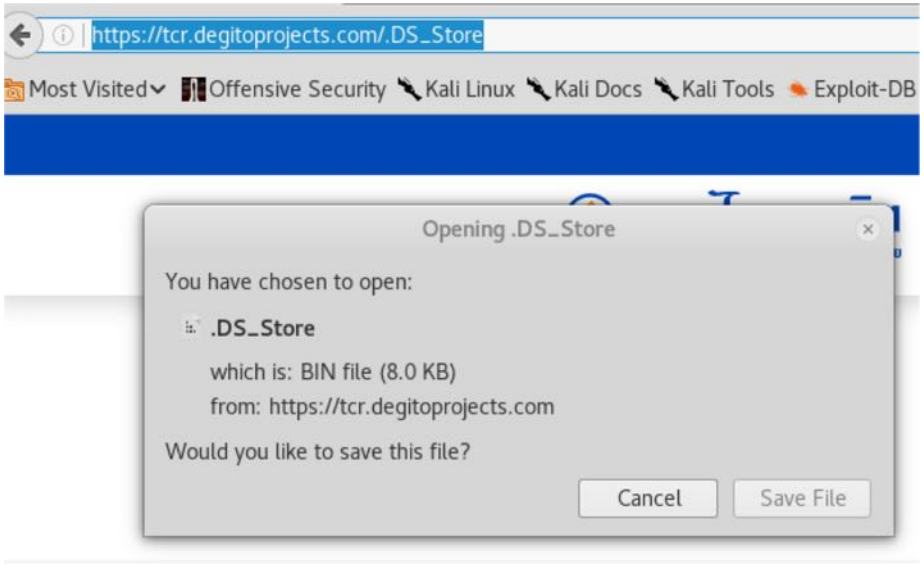
<u>วิธีการแก้ไข</u>

ตั้งค่าเพื่อใช้งาน X-Frame-Options Header โดยแก้ไขไฟล์ httpd.conf

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

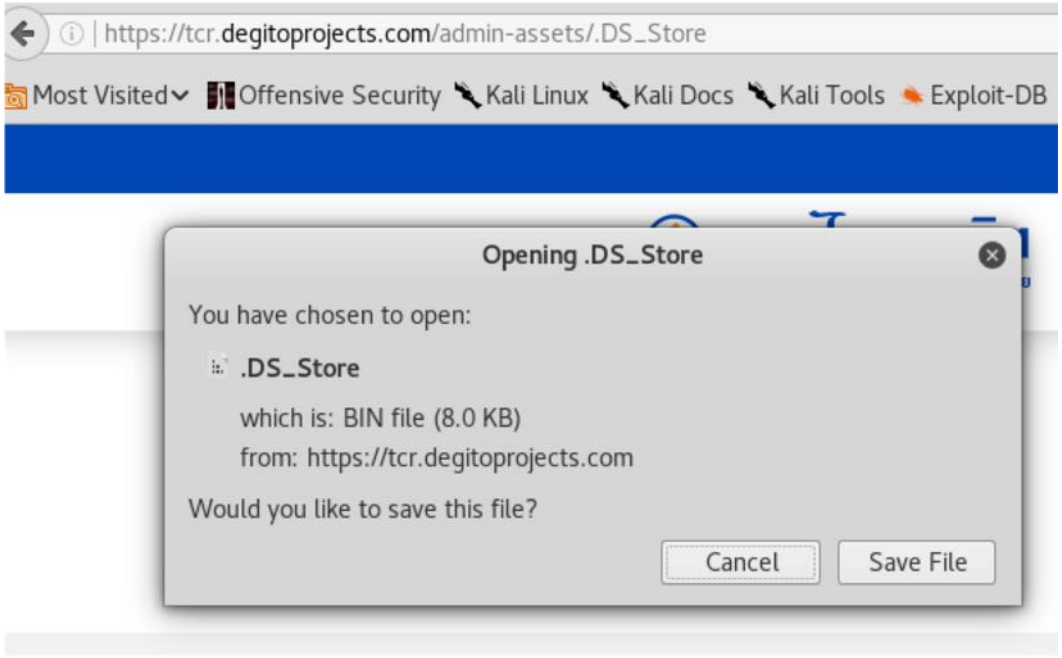
9. สามารถเข้าถึงไฟล์ .DS_Store บนเว็บไซต์ได้

ระดับความเสี่ยง	ต่ำ
อ้างอิง	OWASP Top 10 - 2017 A3 - Sensitive Data Exposure
จุดที่ตรวจพบ	https://tcr.degitoprojects.com/.DS_Store https://tcr.degitoprojects.com/admin-asset/.DS_Store




```
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
```

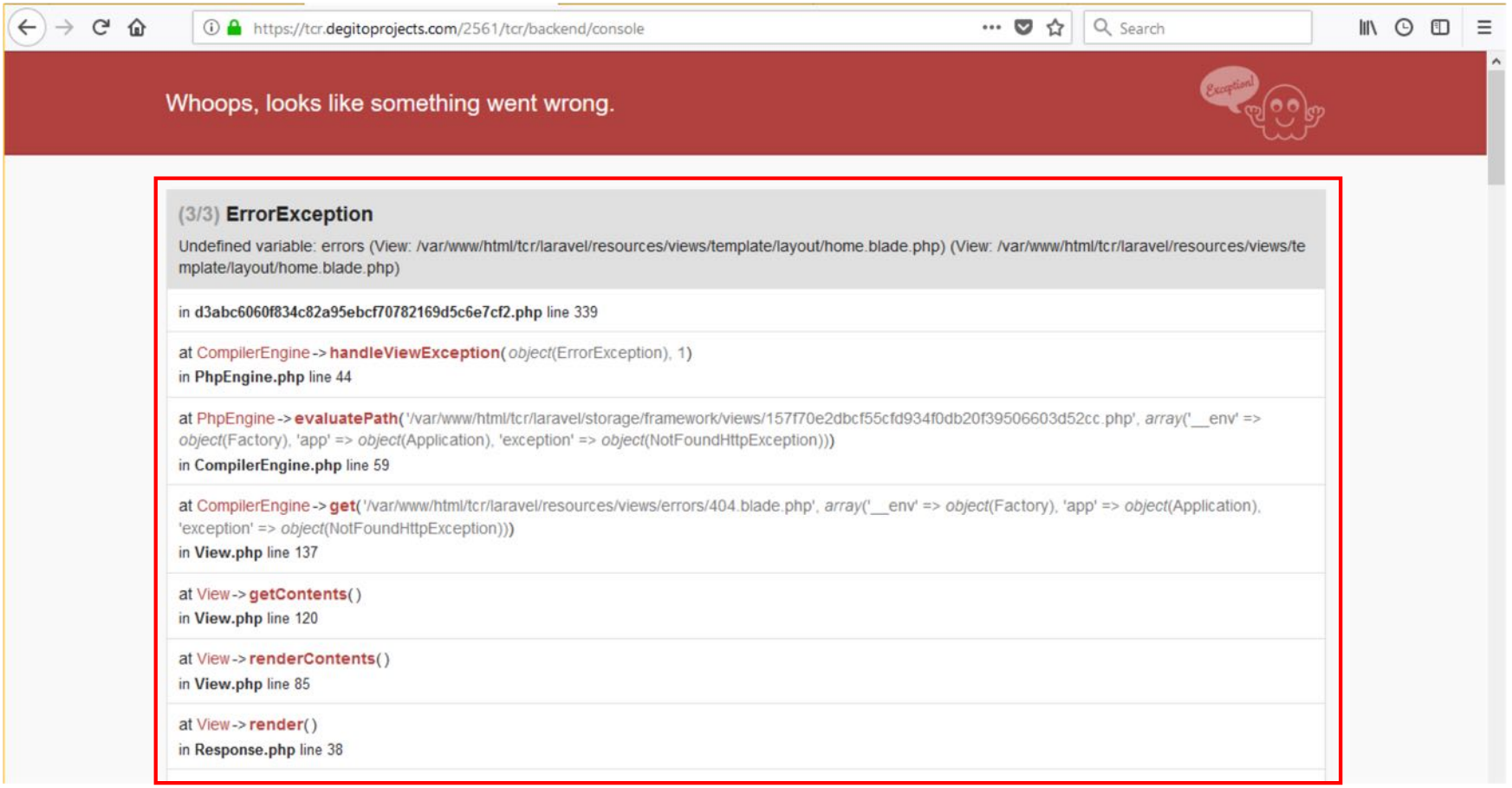
9. สามารถเข้าถึงไฟล์ .DS_Store บนเว็บไซต์ได้

วิธีการแก้ไข

ลบไฟล์ .DS_Store ทุกไฟล์ที่มีอยู่บนเว็บไซต์

10. หน้าแสดงข้อความ Error แสดงข้อมูลที่มีความสำคัญต่อเว็บไซต์ออกมามากเกินไป

ระดับความเสี่ยง	ต่ำ
อ้างอิง	OWASP Top 10 - 2017 A3 - Sensitive Data Exposure
จุดที่ตรวจพบ	https://tcr.degitoprojects.com/



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

THANK YOU