Cyber Confident Index

SEC

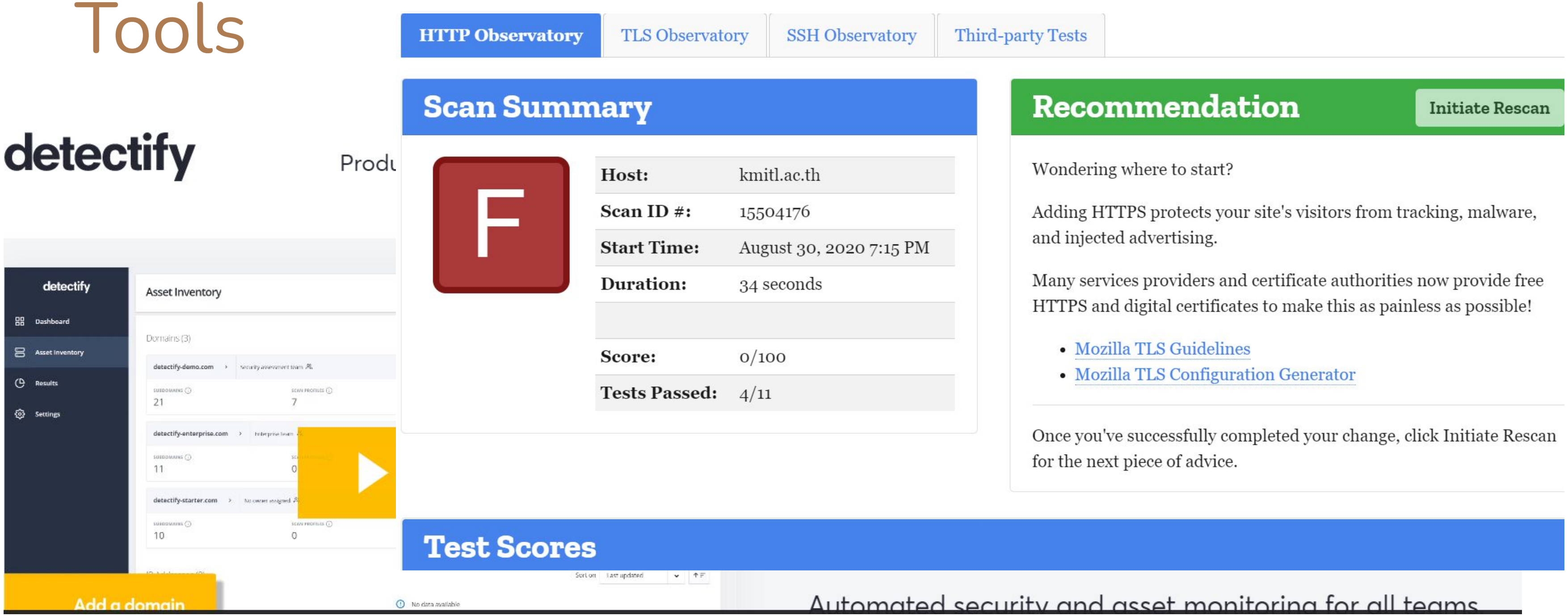
Team Members

- Pawee Tantivasdakarn (Mew)
- Soponpakorn Suttikao (Frong)
- Nattha Siriboon (Pim)

Background and Introduction

Image source https://admiralmarkets.com/th/education/articles/trading-instruments/online-trading-explained

Tools



Asset Inventory

Domains (3)

detectify-demo.com › Security assessment team
SUBDOMAINS 21 SCAN PROFILES 7

detectify-enterprise.com › Enterprise team
SUBDOMAINS 11 SCAN PROFILES 0

detectify-starter.com › No owner assigned
SUBDOMAINS 10 SCAN PROFILES 0

Scan Summary

Host:	kmitl.ac.th
Scan ID #:	15504176
Start Time:	August 30, 2020 7:15 PM
Duration:	34 seconds
Score:	0/100
Tests Passed:	4/11

Recommendation

Wondering where to start?

Adding HTTPS protects your site's visitors from tracking, malware, and injected advertising.

Many services providers and certificate authorities now provide free HTTPS and digital certificates to make this as painless as possible!

- Mozilla TLS Guidelines
- Mozilla TLS Configuration Generator

Once you've successfully completed your change, click Initiate Rescan for the next piece of advice.

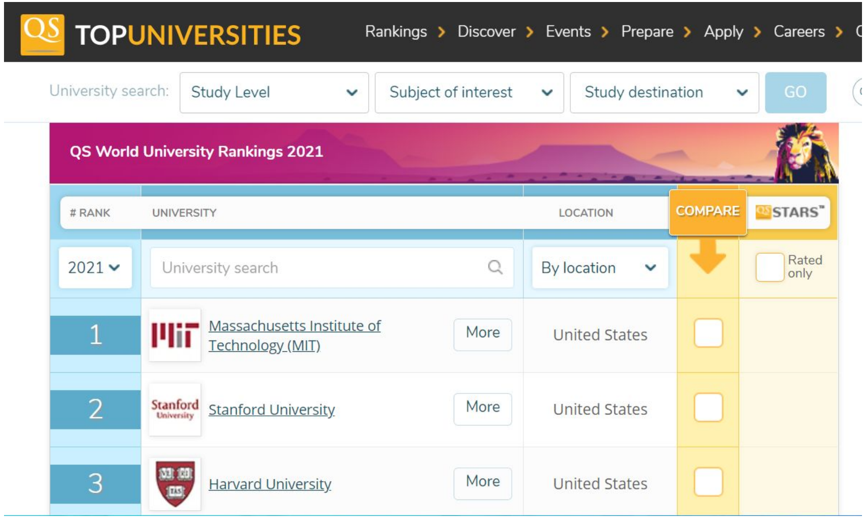
Test Scores

Sources

[1]https://detectify.com/

[2]https://observatory.mozilla.org/

Cyber Confident Index

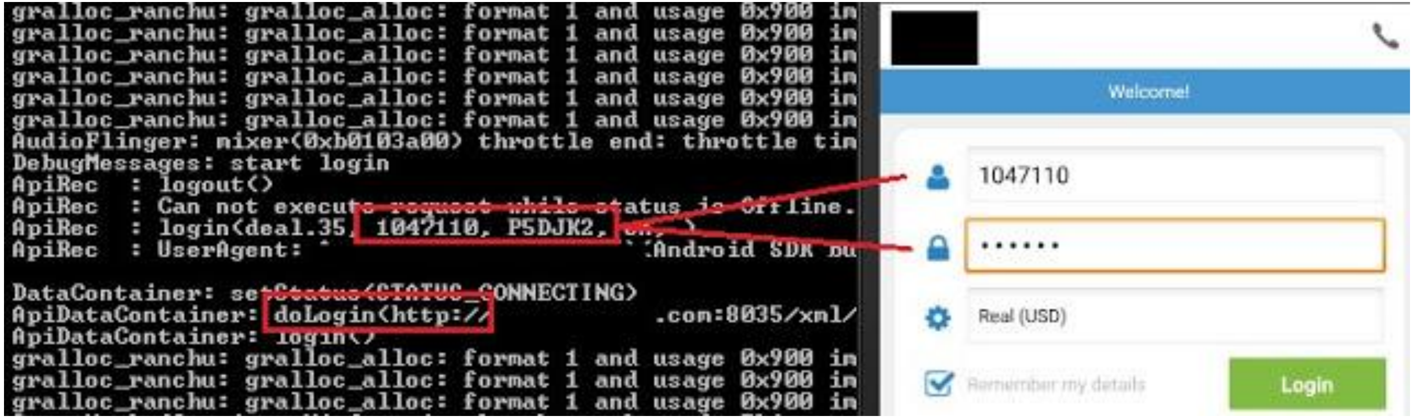


QS World University Rankings 2021

# RANK	UNIVERSITY	LOCATION
2021	University search	By location
1	Massachusetts Institute of Technology (MIT)	United States
2	Stanford University	United States
3	Harvard University	United States

Sources
[1]https://www.investors.com/news/best-online-brokers/website-security-brokerage-accounts-best-brokers-raise-bar/
[2]https://www.topuniversities.com/university-rankings/world-university-rankings/2021

“62% of the apps sent sensitive data to log files, and 67% stored it unencrypted. Physical access to the device is required to extract this data.”



```
gralloc_ranchu: gralloc_alloc: format 1 and usage 0x900 im
gralloc_ranchu: gralloc_alloc: format 1 and usage 0x900 im
gralloc_ranchu: gralloc_alloc: format 1 and usage 0x900 im
gralloc_ranchu: gralloc_alloc: format 1 and usage 0x900 im
gralloc_ranchu: gralloc_alloc: format 1 and usage 0x900 im
gralloc_ranchu: gralloc_alloc: format 1 and usage 0x900 im
AudioFlinger: mixer(0xb0103a00) throttle end: throttle tim
DebugMessages: start login
ApiRec   : logout()
ApiRec   : Can not execute request while status is Offline.
ApiRec   : login(deal.35, 1047110, P5DJK2, en,  )
ApiRec   : UserAgent: `                ` (Android SDK bu

DataContainer: setStatus(STATUS_CONNECTING)
ApiDataContainer: doLogin(http://               .com:8035/xml/
ApiDataContainer: login()
gralloc_ranchu: gralloc_alloc: format 1 and usage 0x900 im
gralloc_ranchu: gralloc_alloc: format 1 and usage 0x900 im
gralloc_ranchu: gralloc_alloc: format 1 and usage 0x900 im
```

[redacted]

1047110

••••••

Real (USD)

☑ Remember my details

Source: https://ioactive.com/are-you-trading-securely-insights-into/

Objectives

1. **To build a system that could do an automated penetration test.**

2. **To reduce the cost of the penetration test which is usually costly. Our system is on-demand and lower cost, so the firm could do this kind of test more often and benefit the user.**

3. **To automate the penetration test process.**

4. **To identify the vulnerability of the security system.**

5. **To create an index ranking system and overall stat on how well the security system the brokers have implemented.**

Scope

1. **Automate the penetration test from the outsider perspective or “black box” with the given IP, or endpoint, or IP with the port.**

2. **Report the gap of the security system to its owner. Each report will be auto-generated.**

3. **All reports must be encrypted.**

4. **The penetration test should be able to scale and secure.**

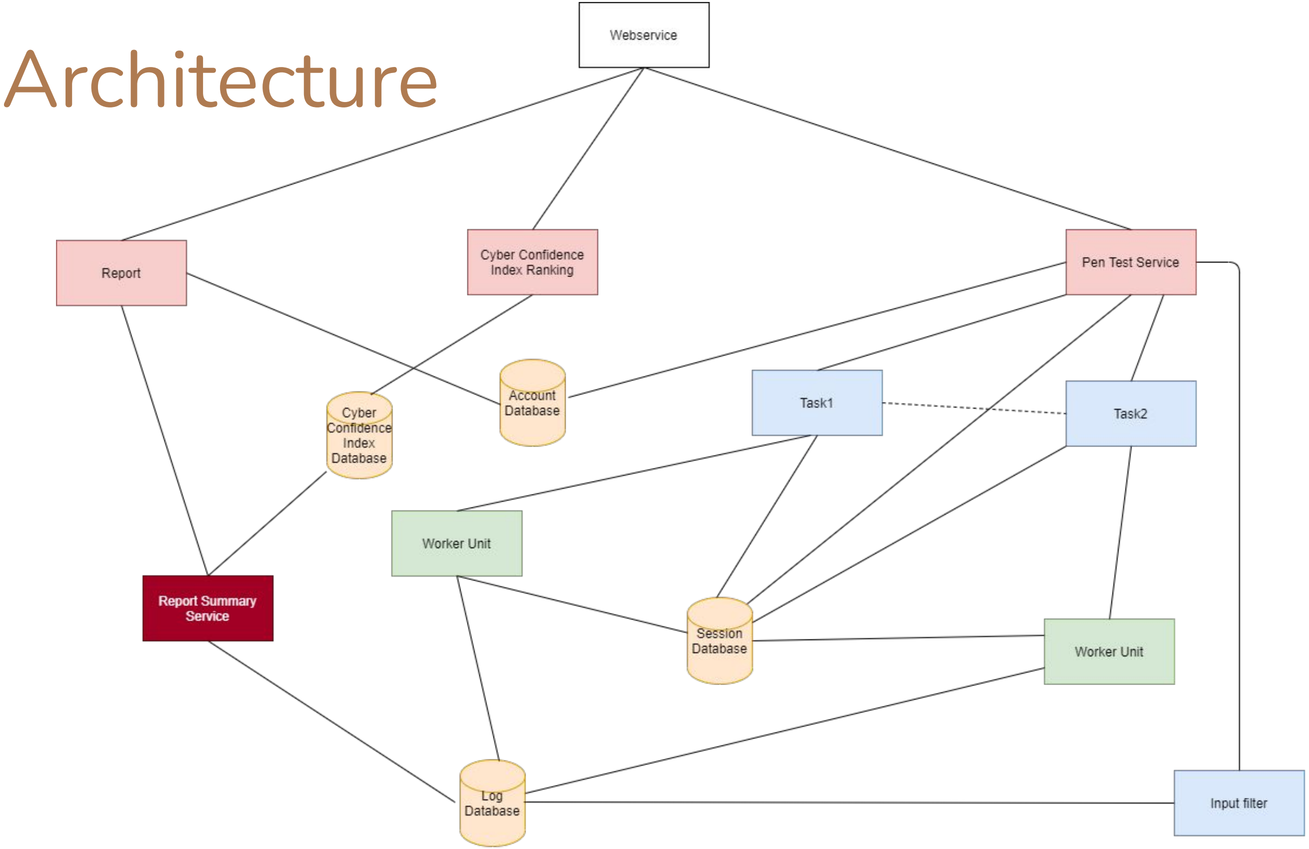
5. **Show the overall stat of the brokers’ security system to the consumers.**

What we focus

1.) Injection
2.) Broken Authentication
3.) Sensitive Data Exposure
4.) XML External Entities (XXE)
5.) Cross-Site Scription XSS
6.) Using Compensation with known vulnerabilities

Source: https://owasp.org/www-project-top-ten/

System Architecture



Materials and Tools

1. **Nmap**
2. **DNSMap**
3. **Enum4linux**
4. **Searchsploit**
5. **CVE**
6. **SQLMap**
7. **Hydra**
8. **Dirb**
9. **XSSsniper**

Methodology

1. **Research and analyze the strength of each tool.**
2. **Design the system by integrating those tools.**
3. **Design the System Architecture and Database.**
4. **Test the designed model and collect information.**
5. **Deploy the designed model and penetrate the customer's security system.**
6. **Identify the vulnerabilities.**
7. **Collect all the log files and send feedback to the company.**
8. **Visualize the succession rate of penetrating the security system to the consumers.**

Expected outcomes

1. **Client companies gain insight knowledge about their system vulnerabilities through our report.**

2. **The general public can gauge the trustworthiness of our client companies.**

3. **Reduce the chance of attacks.**

4. **Consumers have a good experience with trading**

Timeline

https://docs.google.com/spreadsheets/d/1b-lXyBjpqEvtcjRba_S_k7NpXrpeYszqQ1k4zzNjluE/edit?usp=sharing

Responsibility

- **Frong**

  Core feature and Website GUI

- **Pim**

  Core feature and Microservice

- **Mew**

  Core feature and Backend + API

Q&A