



**Department of Computer Science;  
Faculty of Science, Khon Kaen  
University**

## Nikto 2

จัดทำโดย

นายพงษ์ไท ศิริปี	563020218-3
นายธีระพัฒน์ ธีระนุกูล	563020212-5
นายพีระศักดิ์ บุญเจริญสุข	563020223-0
นาย หัสติล คงโนนกกอก	563020237-9
นางสาวขวัญข้าว เสี่ยงเลิศ	563020200-2
นางสาวพรรณราย กองทอง	563020770-1

Group ID 14

322376Information and Communication

Technology Security

## โปรแกรม Nikto 2

### คุณสมบัติ

Nikto เป็นโปรแกรมภาษา perl ใช้ในการตรวจสอบไฟล์ ,พาท ที่ไม่ปลอดภัยในระบบ สแกนหาช่องโหว่เว็บไซต์ และอาจเป็นภัยร้ายเมื่อแฮกเกอร์นำไปใช้ในการแฮกเว็บ เช่นกัน สามารถใช้เช็คความปลอดภัยของระบบเว็บได้ดี เป็นอันดับต้น ๆ ของโปรแกรมตรวจสอบ Security website

### จุดเด่นของโปรแกรม

- การสนับสนุนปลั๊กอิน (มาตรฐาน PERL)
- สำหรับการตรวจสอบซอฟต์แวร์เซิร์ฟเวอร์ที่ล้ำสมัย
- การสนับสนุนพรีอ็อกซี (มีการตรวจสอบ)
- การตรวจสอบโฮสต์ (ขั้นพื้นฐาน)

### วิธีการใช้งานโปรแกรม Nikto 2

1. โหลดโปรแกรมที่ <https://cirt.net/Nikto2>

CIRT.net  
Suspicion Breeds Confidence

Nikto DAVTest CMS Explorer Other Code Default Passwords About

Home » Nikto

with **netsparker**  
web application security scanner  
DOWNLOAD

**HELP WANTED**  
PENETRATION TESTERS  
SUNERA sunera.com/careers

## Nikto2

Install: Run from a git repo - <https://github.com/sullo/nikto>  
Download: Latest GitHub Release (zip)  
Stable Release: Version 2.1.5 bz2 or gz | Changelog

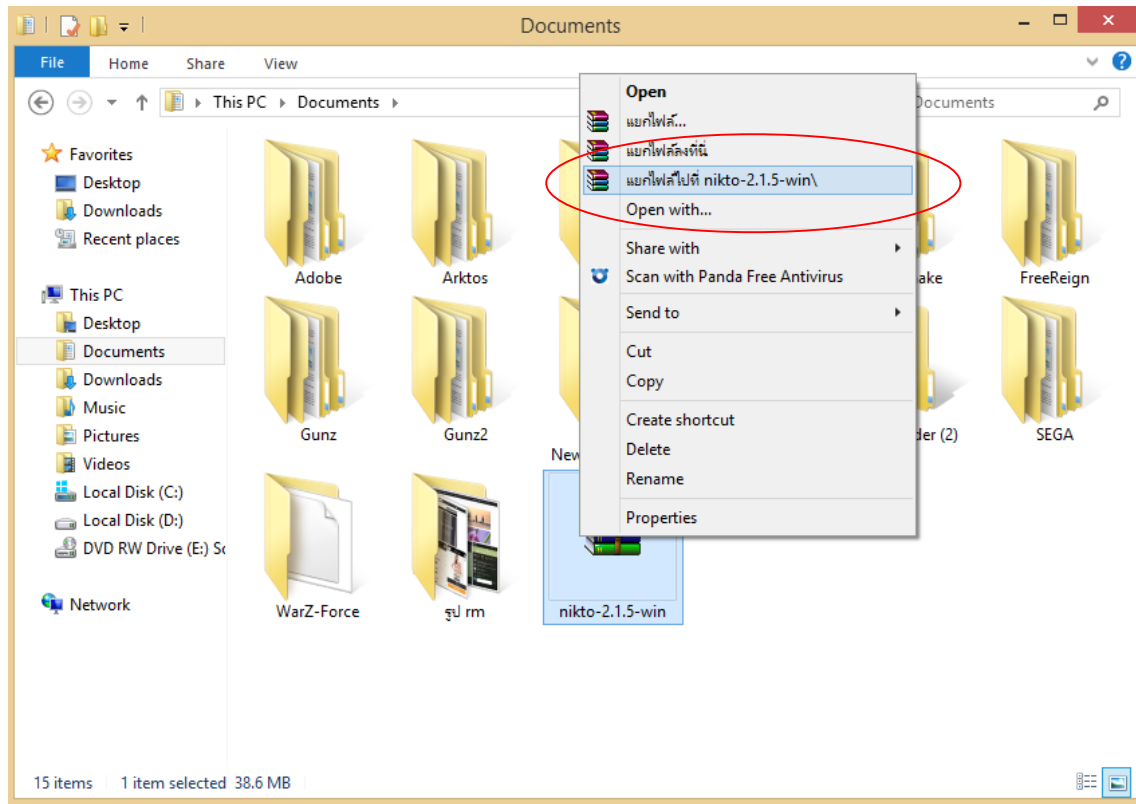
Nikto is sponsored by Netsparker, a false positive free web application security scanner.  
[Click here](#) to download a demo of Netsparker, or [click here](#) to apply for a free trial of Netsparker Cloud online scanner.

Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated.

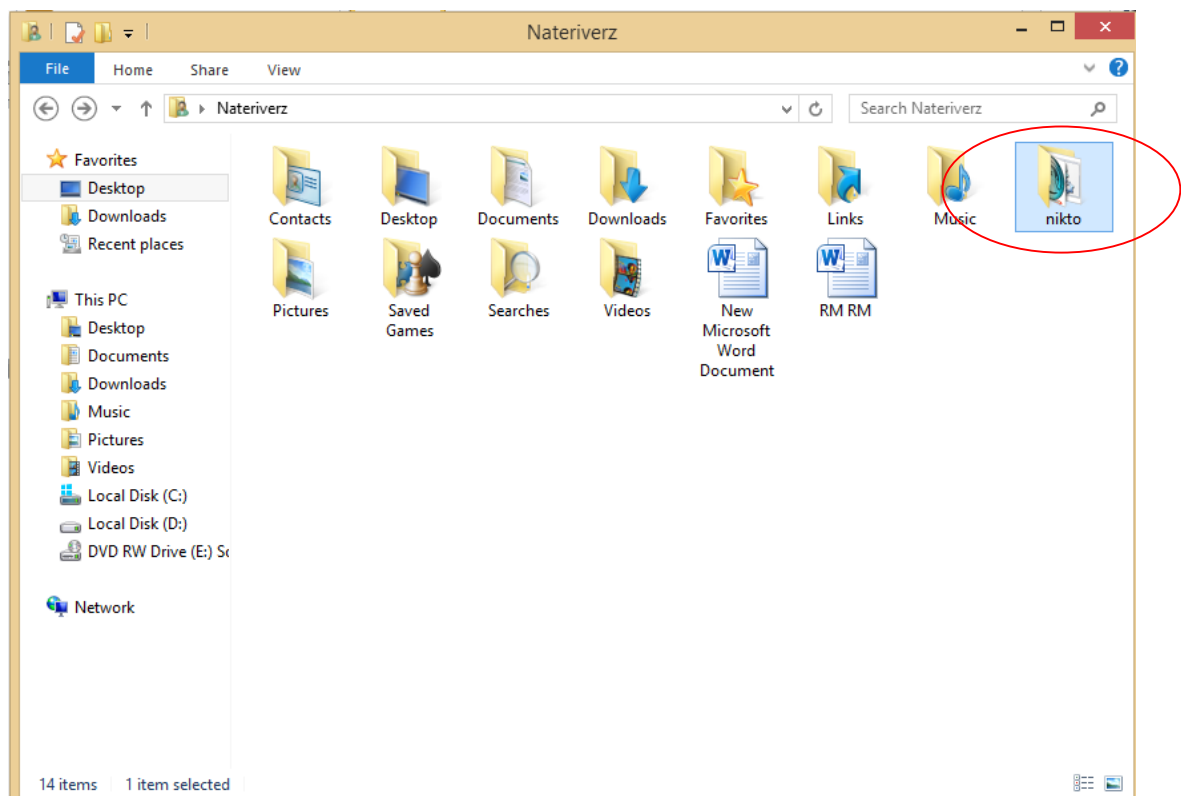
Nikto is not designed as a stealthy tool. It will test a web server in the quickest time possible, and is obvious in log files to an IPS/IDS. However, there is support for LibWhisker's anti-IDS methods in case you want to give it a try (or test your system)

Nikto is written by  
Chris Sullo  
David Lodge

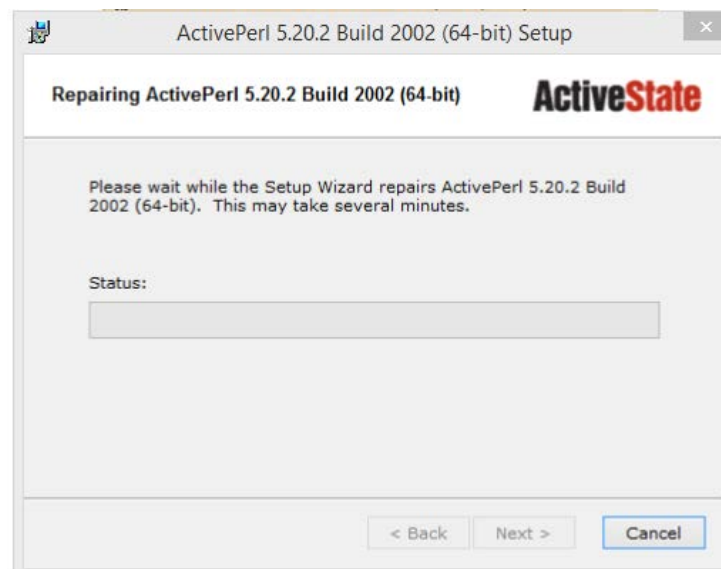
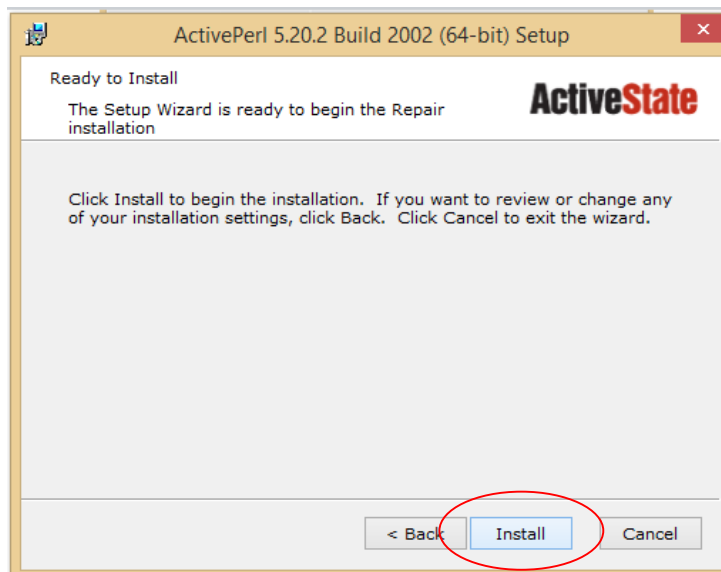
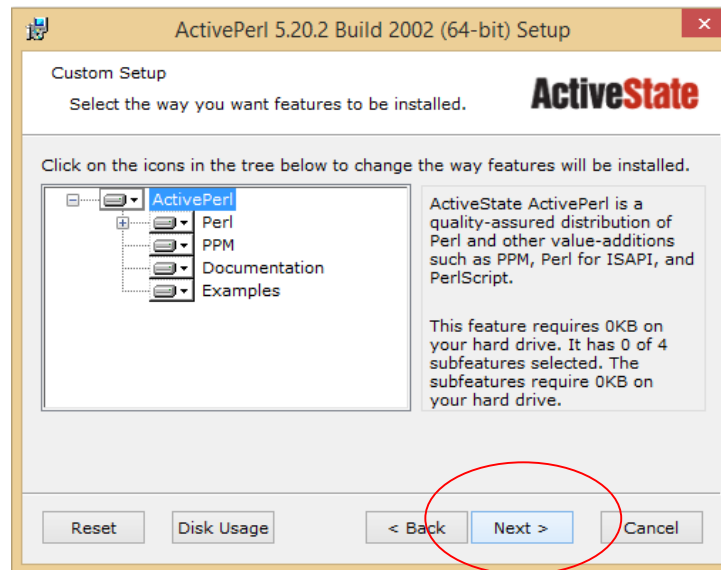
## 2. แยกไฟล์โปรแกรม nikto



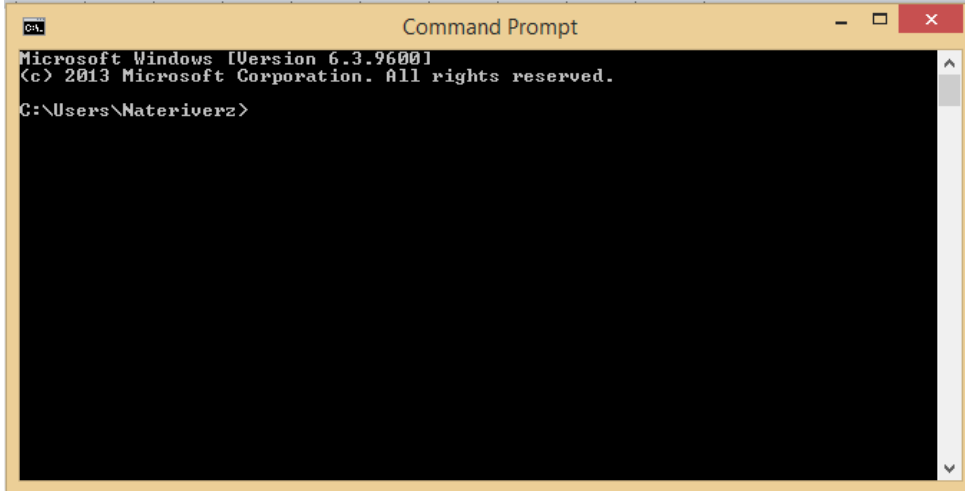
## 3. ตำแหน่งที่ folder โปรแกรมอยู่



4. โหลดโปรแกรม ActivePerl ที่ <http://www.activestate.com/activeperl/downloads> เพื่อให้โปรแกรม nikto รันภาษา perl ได้

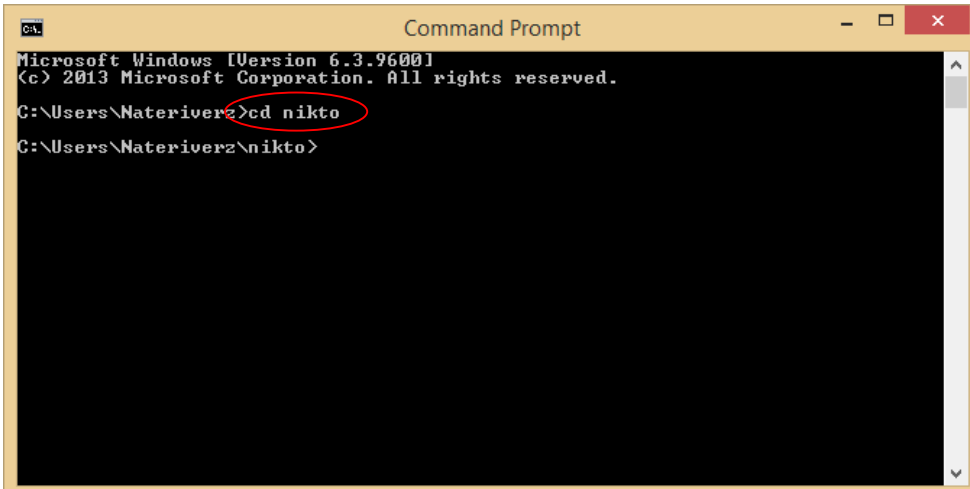


5. ตัวโปรแกรม nikto รันผ่าน cmd



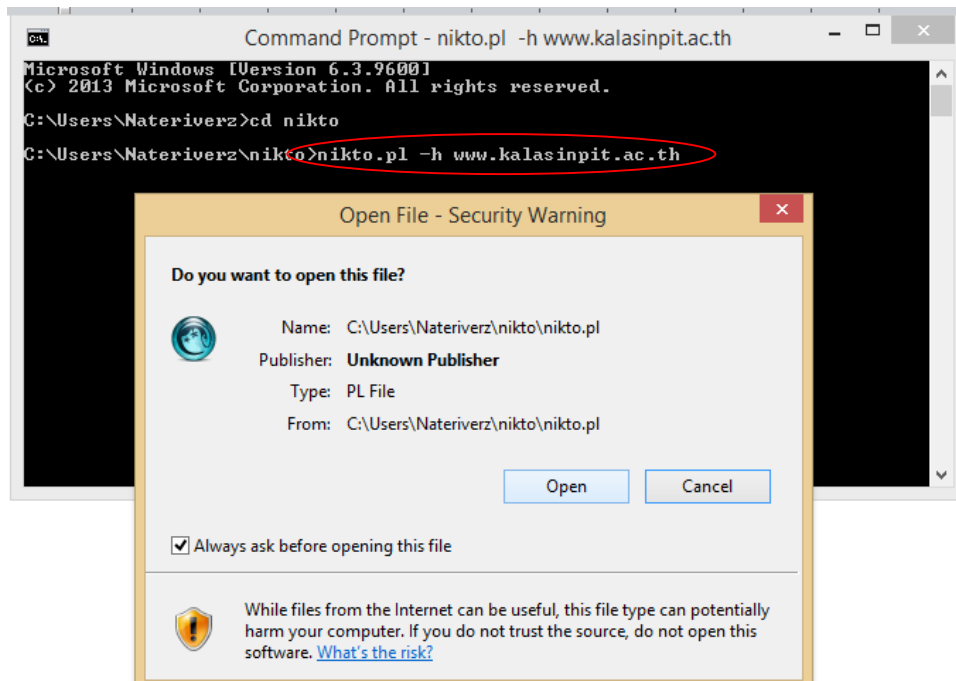
```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Users\Nateriverz>
```

6. เข้า folder ที่ลง nikto ไว้

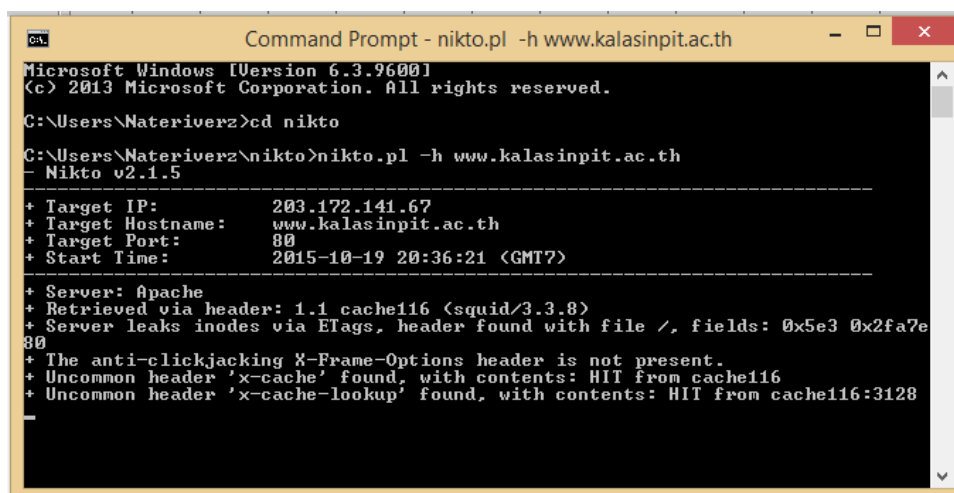


```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Users\Nateriverz>cd nikto
C:\Users\Nateriverz\nikto>
```

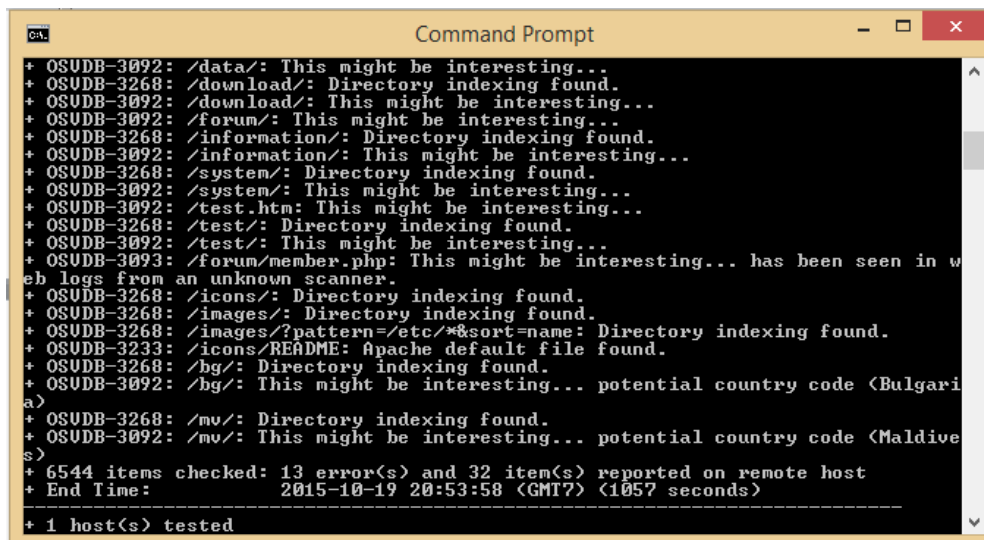
## 7. เข้าโปรแกรม nikto



8. โปรแกรมทำการสแกนหาช่องโหว่ และรายละเอียดต่าง ๆ ของเว็บไซต์ เว็บไซต์ตัวอย่าง คือ [www.kalasinpit.ac.th](http://www.kalasinpit.ac.th) เช่น IP, Port, ภาษาที่ใช้พัฒนา ฯลฯ

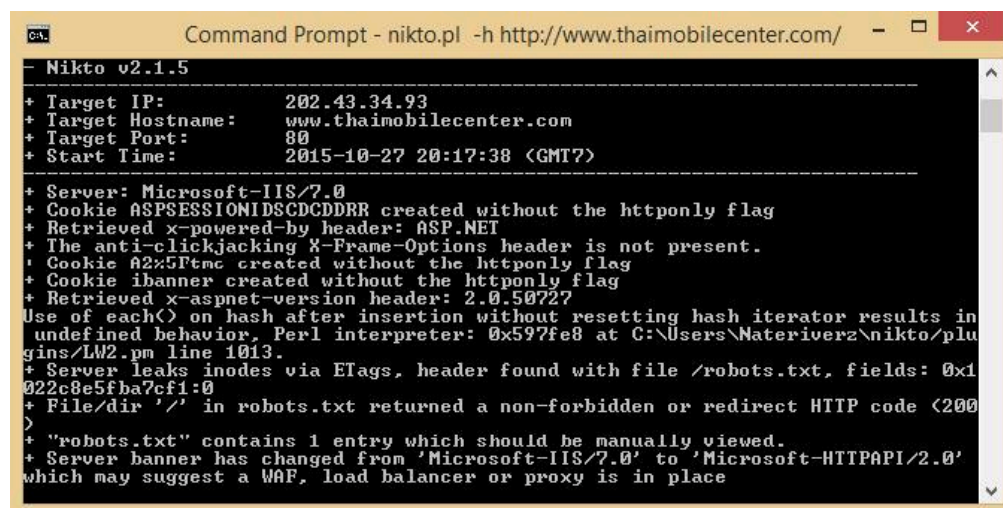


9. เมื่อโปรแกรมทำงานเสร็จจะแสดงรายละเอียดต่าง ๆ ของเว็บไซต์ เช่น ช่องโหว่ ไฟล์ต่าง ๆ ในเว็บไซต์



```
Command Prompt
+ OSUDB-3092: /data/: This might be interesting...
+ OSUDB-3268: /download/: Directory indexing found.
+ OSUDB-3092: /download/: This might be interesting...
+ OSUDB-3092: /forum/: This might be interesting...
+ OSUDB-3268: /information/: Directory indexing found.
+ OSUDB-3092: /information/: This might be interesting...
+ OSUDB-3268: /system/: Directory indexing found.
+ OSUDB-3092: /system/: This might be interesting...
+ OSUDB-3092: /test.htm: This might be interesting...
+ OSUDB-3268: /test/: Directory indexing found.
+ OSUDB-3092: /test/: This might be interesting...
+ OSUDB-3093: /forum/member.php: This might be interesting... has been seen in w
eb logs from an unknown scanner.
+ OSUDB-3268: /icons/: Directory indexing found.
+ OSUDB-3268: /images/: Directory indexing found.
+ OSUDB-3268: /images/?pattern=/etc/*&sort=name: Directory indexing found.
+ OSUDB-3233: /icons/README: Apache default file found.
+ OSUDB-3268: /hg/: Directory indexing found.
+ OSUDB-3092: /hg/: This might be interesting... potential country code <Bulgari
a>
+ OSUDB-3268: /mv/: Directory indexing found.
+ OSUDB-3092: /mv/: This might be interesting... potential country code <Maldiv
es>
+ 6544 items checked: 13 error(s) and 32 item(s) reported on remote host
+ End Time: 2015-10-19 20:53:58 <GMT?> <1057 seconds>
-----
+ 1 host(s) tested
```

10. สแกนเว็บทำให้รู้ว่าเว็บใช้ภาษา asp.net ในการพัฒนาทำให้สามารถใช้ช่องโหว่นี้ทำการ sql injection ได้



```
Command Prompt - nikto.pl -h http://www.thaimobilecenter.com/
-----
- Nikto v2.1.5
-----
+ Target IP: 202.43.34.93
+ Target Hostname: www.thaimobilecenter.com
+ Target Port: 80
+ Start Time: 2015-10-27 20:17:38 <GMT?>
-----
+ Server: Microsoft-IIS/7.0
+ Cookie ASPSESSIONIDSCDCDDRR created without the httponly flag
+ Retrieved x-powered-by header: ASP.NET
+ The anti-clickjacking X-Frame-Options header is not present.
+ Cookie A2x5Ftmc created without the httponly flag
+ Cookie ibanner created without the httponly flag
+ Retrieved x-aspnet-version header: 2.0.50727
Use of each() on hash after insertion without resetting hash iterator results in
undefined behavior, Perl interpreter: 0x597fe8 at C:\Users\Nateriverz\nikto/plu
gins/LW2.pm line 1013.
+ Server leaks inodes via ETags, header found with file /robots.txt, fields: 0x1
022c8e5fba7cf1:0
+ File/dir '/' in robots.txt returned a non-forbidden or redirect HTTP code <200
>
+ "robots.txt" contains 1 entry which should be manually viewed.
+ Server banner has changed from 'Microsoft-IIS/7.0' to 'Microsoft-HTTPAPI/2.0'
which may suggest a WAF, load balancer or proxy is in place
```