บันทึกข้อความ

ส่วนราชการ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กลุ่มคอมพิวเตอร์และเครือข่าย โทร 1201

ที่ สธ 0202.04/427 **วันที่** 13 กรกฎาคม 2553

เรื่อง ขอเชิญประชุมคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

เรียน คณะกรรมการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

ตามคำสั่งศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ที่ 4/2552 สั่ง ณ วันที่ 2 มีนาคม 255 เรื่อง แต่งตั้งคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ให้มีหน้าที่เสนอนโยบายด้านการรักษาความปลอดภัยระบบฯ ควบคุม กำกับ ดูแลให้มีการปฏิบัติตามระเบียบการรักษาความปลอดภัยระบบฯ อย่างเคร่งครัด นั้น

ในการนี้ จึงขอเรียนเชิญคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เข้าร่วมประชุมครั้งที่ 3/2553 ในวันจันทร์ที่ 19 กรกฎาคม พ.ศ.2553 เวลา 9.30 น. – 16.00 น. ณ ห้องประชุมศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

จึงเรียนมาเพื่อโปรดเข้าร่วมประชุมโดยพร้อมเพรียงกันตามวันและเวลาดังกล่าวด้วย

(นายบุญชัย ฉัตรพิรุฬห์พันธุ์)
ประธานคณะกรรมการรักษาความมั่นคงปลอดภัย
ของระบบเทคโนโลยีสารสนเทศ

กำหนดการ

ประชุมคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ครั้งที่ 1/2553

วันจันทร์ที่ 19 กรกฎาคม พ.ศ.2553 เวลา 9.30 น. – 16.00 น.

ณ ห้องประชุมศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

****

วาระที่ 1 เรื่องที่ประธานแจ้งให้ทราบ

วาระที่ 2 เรื่องเพื่อพิจารณา

- การจัดประชุมเชิงปฏิบัติการโครงการจัดการความเสี่ยงไอทีภายในสำนักงานปลัดกระทรวงสาธารณสุข ประจำปีงบประมาณ 2553
- แบบสำรวจความพึงพอใจของเจ้าหน้าที่สังกัดกระทรวงสาธารณสุขต่อประสิทธิภาพเครือข่าย internet
- แบบสำรวจความพึงพอใจในบริการของ ศทส.สป.สธ.
- แบบสำรวจระบบสารสนเทศภายในสำนักงานปลัดกระทรวงสาธารณสุข
- แบบสำรวจรายชื่อผู้ประสานงานด้านคอมพิวเตอร์และเครือข่ายของหน่วยงานสังกัดกระทรวงสาธารณสุข
- แบบสำรวจทักษะคอมพิวเตอร์ของบุคลากรในส่วนกลาง สป.สธ.

วาระที่ 3 เรื่องอื่นๆ

- ซักซ้อมการดำเนินงานตามแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบฐานข้อมูลและสารสนเทศ(IT Contingency Plan)

รายชื่อผู้เข้าร่วมประชุมคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ครั้งที่ 3/2553

วันจันทร์ที่ 19 กรกฎาคม 2553 เวลา 9.00 – 16.00 น.

ณ ห้องประชุมศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

ลำดับที่	ชื่อ-สกุล	ตำแหน่ง	ลายเซ็น	หมายเหตุ
1	นายแพทย์สินชัย ต่อวัฒนกิจกุล	ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	–	
2	นายบุญชัย ฉัตรพิรุฬห์พันธุ์	หัวหน้ากลุ่มคอมพิวเตอร์และเครือข่าย		
3	นางสาวสุวันต์นา เสมอเนตร	หัวหน้ากลุ่มบริหารเทคโนโลยีสารสนเทศเพื่อการจัดการ		
4	นางทิพย์วรรณ ยงศิริวิทย์	หัวหน้ากลุ่มพัฒนาการบริหารข้อมูล		
5	นางสุรีรัตน์ สกุเกตุ	หัวหน้าฝ่ายบริหารทั่วไป		
6	นางสาวปราณี ฤทธิ์เต็ม	หัวหน้ากลุ่มพัฒนามาตรฐานและบริการคอมพิวเตอร์		
7	นายฐิติ ภู่เพ็ชร์	นักวิชาการคอมพิวเตอร์ชำนาญการ	–	
8	นายพิษณุเดช ปักกุนนัน	เจ้าพนักงานเครื่องคอมพิวเตอร์ชำนาญงาน		
9	นายชวลิต ลิ้มปิยินทรากูล	เจ้าพนักงานเครื่องคอมพิวเตอร์ชำนาญงาน		
10	นายราชิ ปาลือชา	นักวิชาการคอมพิวเตอร์ปฏิบัติการ		
11	นางปัทมา มโนมัธย์	นักวิชาการคอมพิวเตอร์ชำนาญการ		
12	นางรุ่งนิภา อมาตยคง	นักวิชาการคอมพิวเตอร์ปฏิบัติการ		

ทดสอบการ recovery web

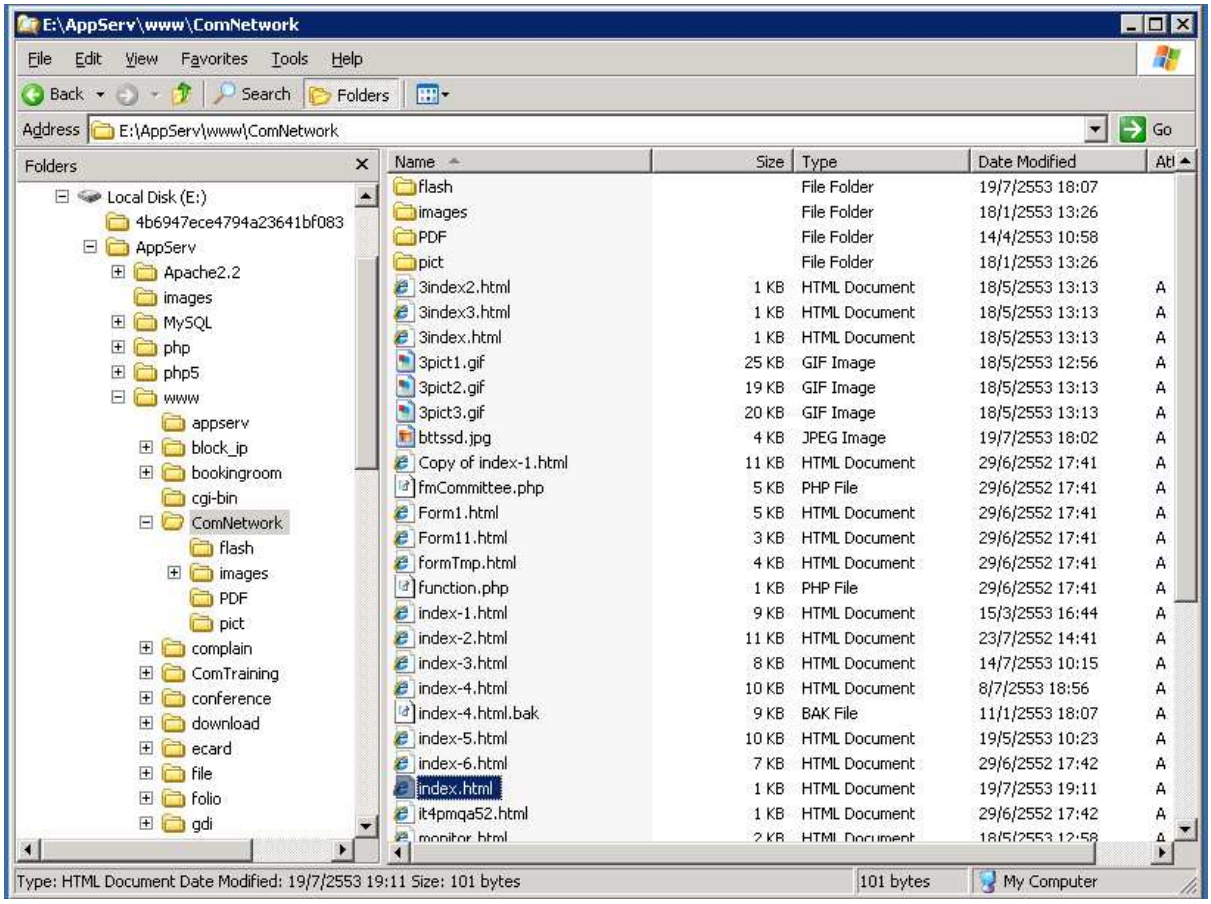
ทดสอบเมื่อ กรกฎาคม 2553

Web ที่ใช้ในการทดสอบ http://ict3.moph.go.th/comnetwork

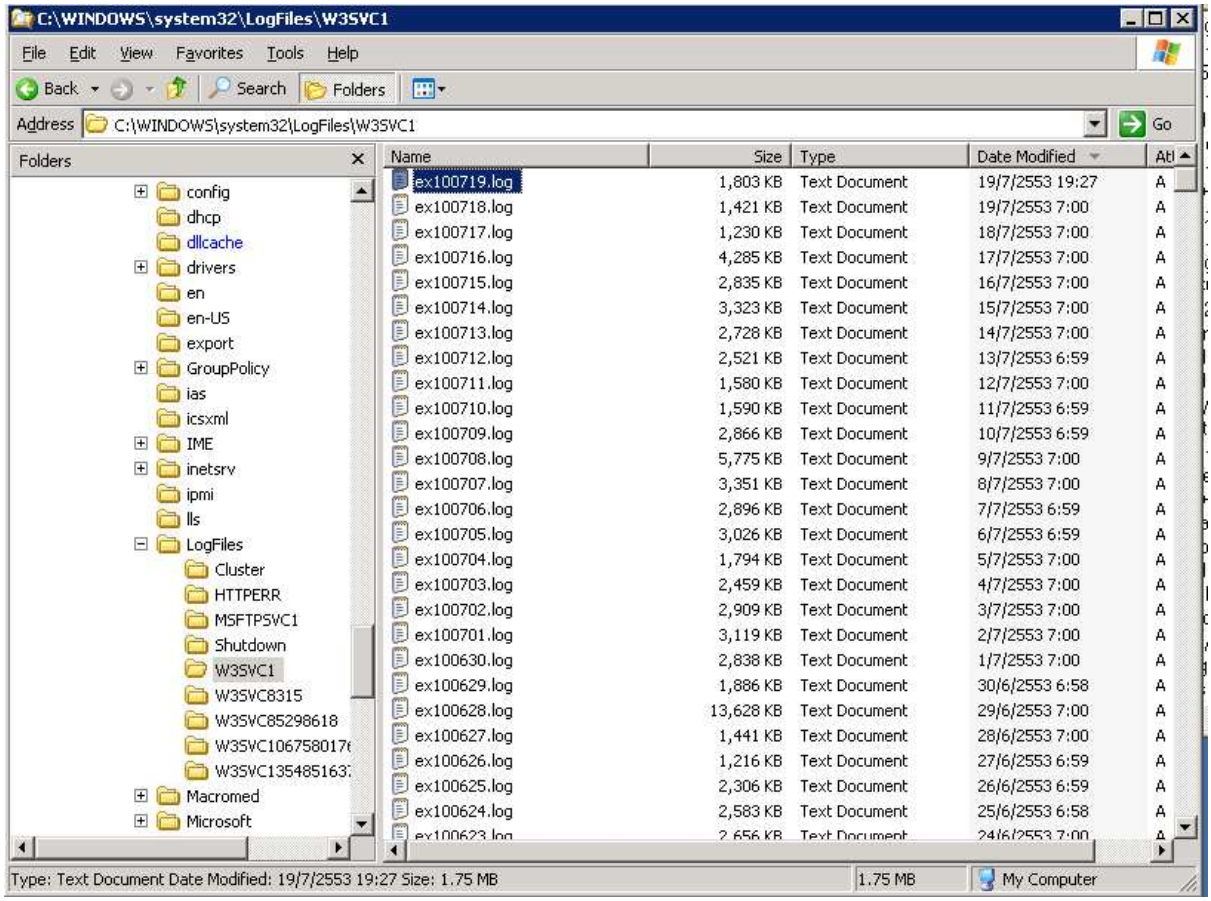
จากหน้า page ปกติ

หน้า page หลังจากโดน hack

ให้ทำการเข้าไปตรวจสอบ file index.html ดูที่วันเวลาของ file มีการสร้างใหม่เมื่อไร ในที่นี้คือ 19/7/2553 19:11



แล้วทำการตรวจสอบ log file ของ web server ณ ช่วงเวลาที่มีการเปลี่ยนแปลง file นั้น



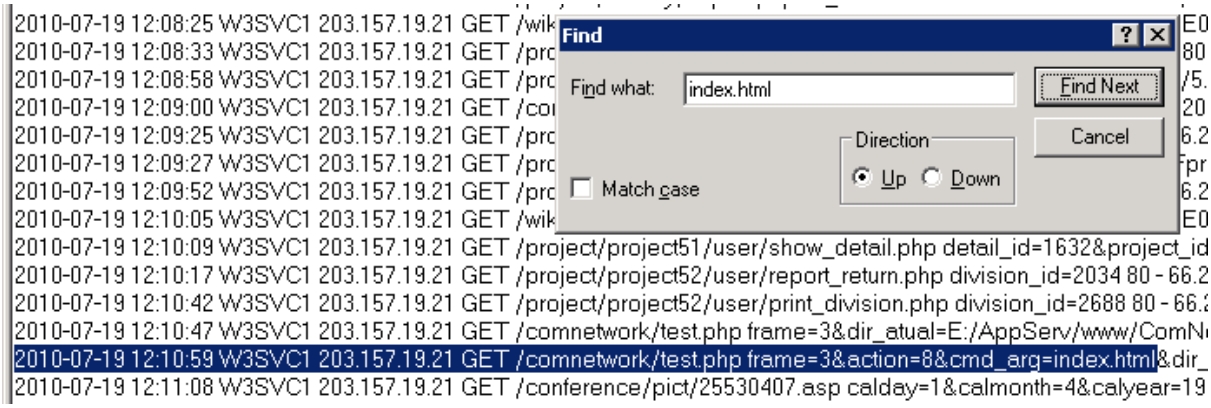
จาก log file ของ IIS web server (ซึ่งเวลาระบุเป็น standard time 0:00 เมื่อต้องการหาเป็นเวลาในประเทศไทย จะต้อง +07:00) ให้ตรวจสอบว่ามีหมายเลข IP Address ใดเรียก file index.html ในช่วงเวลานั้น ในที่นี้คือ 2010-07-19 12:11:53

```
2010-07-19 12:11:37 W3SVC1 203.157.19.21 GET /wiki/index.php title=%E0%B8%81%E0%B8%A3%E0%
2010-07-19 12:11:46 W3SVC1 203.157.19.21 POST /comnetwork/test.php - 80 - 180.180.108.62 Mozilla/4.
2010-07-19 12:11:53 W3SVC1 203.157.19.21 GET /comnetwork/index.html - 80 - 180.180.108.62 Mozilla/4.
2010-07-19 12:12:00 W3SVC1 203.157.19.21 GET /project/project52/user/report_return.php division_id=
```

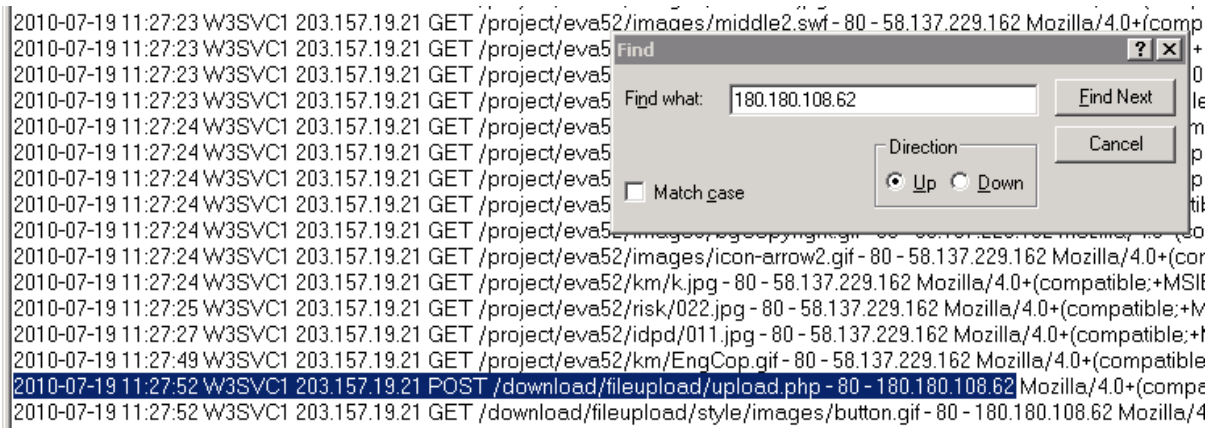
นำหมายเลข IP Address ที่ได้ไปค้นหาย้อนหลังกลับไปว่า มีการเรียกใช้งาน Script file ใดเป็นพิเศษหรือไม่

```
2010-07-19 12:11:37 W3SVC1 203.157.19.21 GET /wiki/index.php title=%E0%B8%81%E0%B8%A3%E
2010-07-19 12:11:46 W3SVC1 203.157.19.21 POST /comnetwork/test.php - 80 - 180.180.108.62 Mozilla/
2010-07-19 12:11:53 W3SVC1 203.157.19.21 GET /comnetwork/index.html - 80 - 180.180.108.62 Mozilla
```

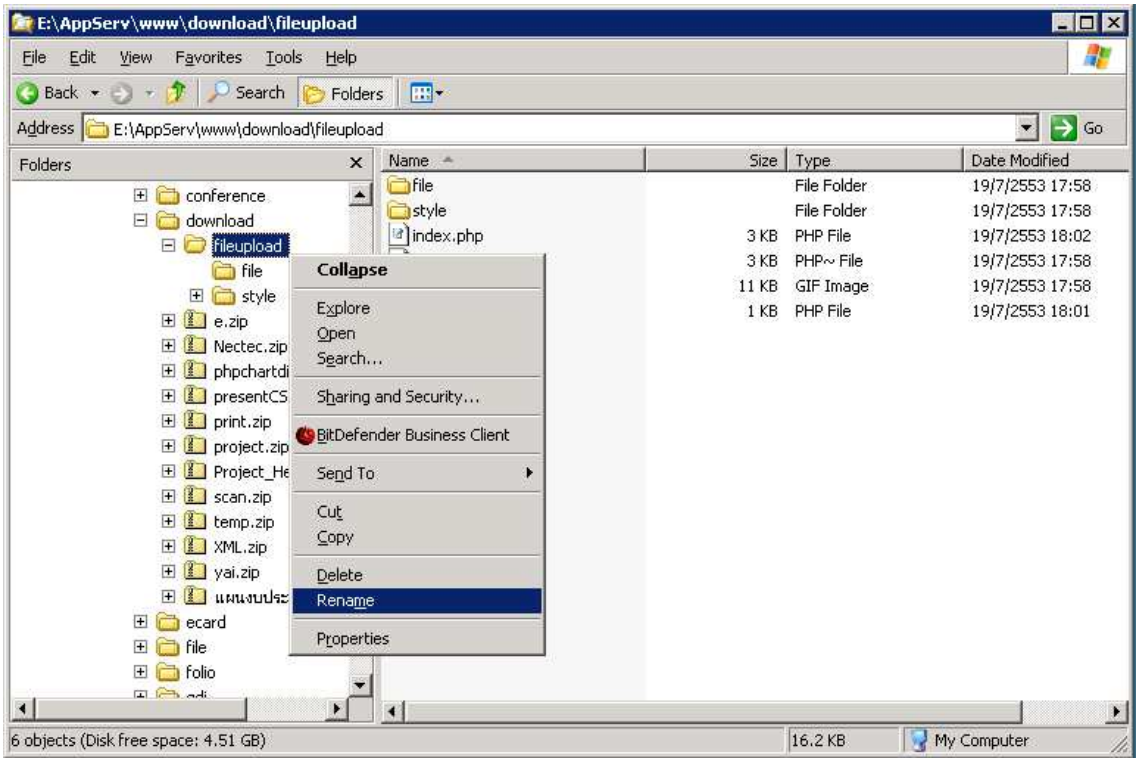
ในที่นี้พบว่าหมายเลข IP Address 180.180.108.62 มีการเรียกใช้งาน Script file test.php

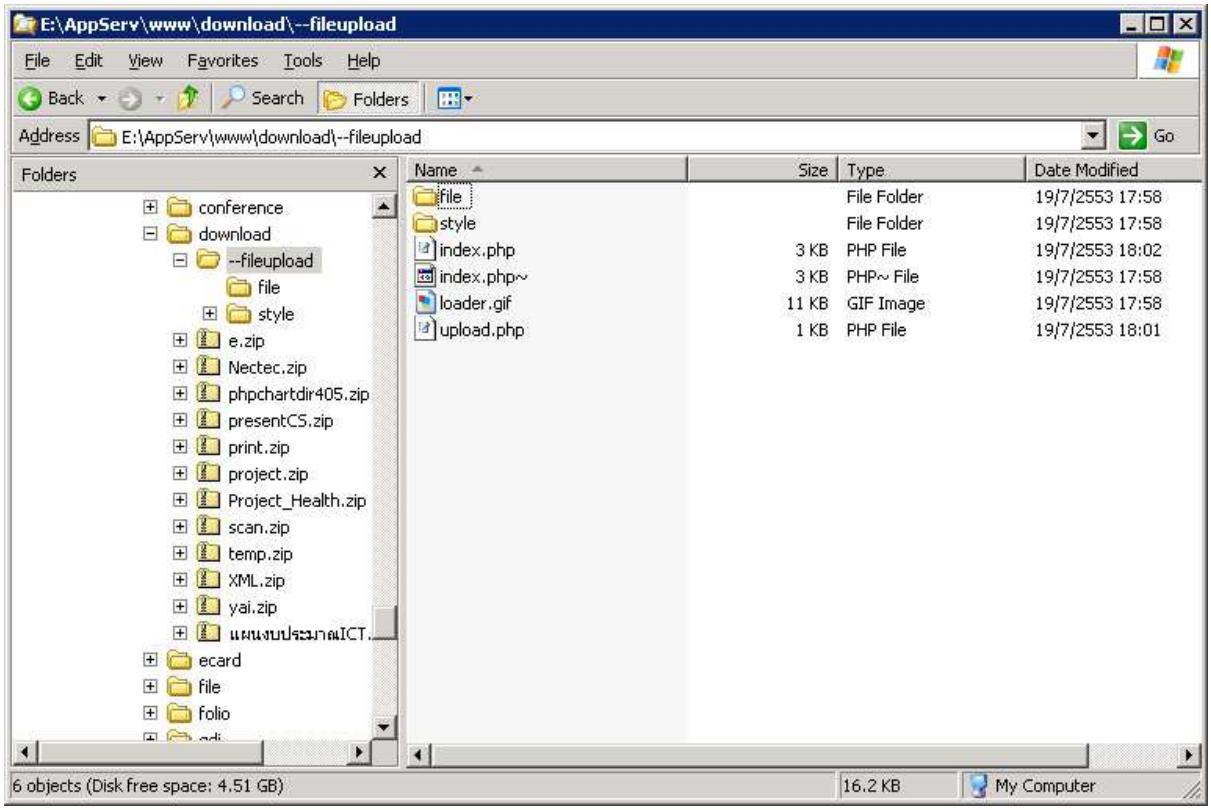


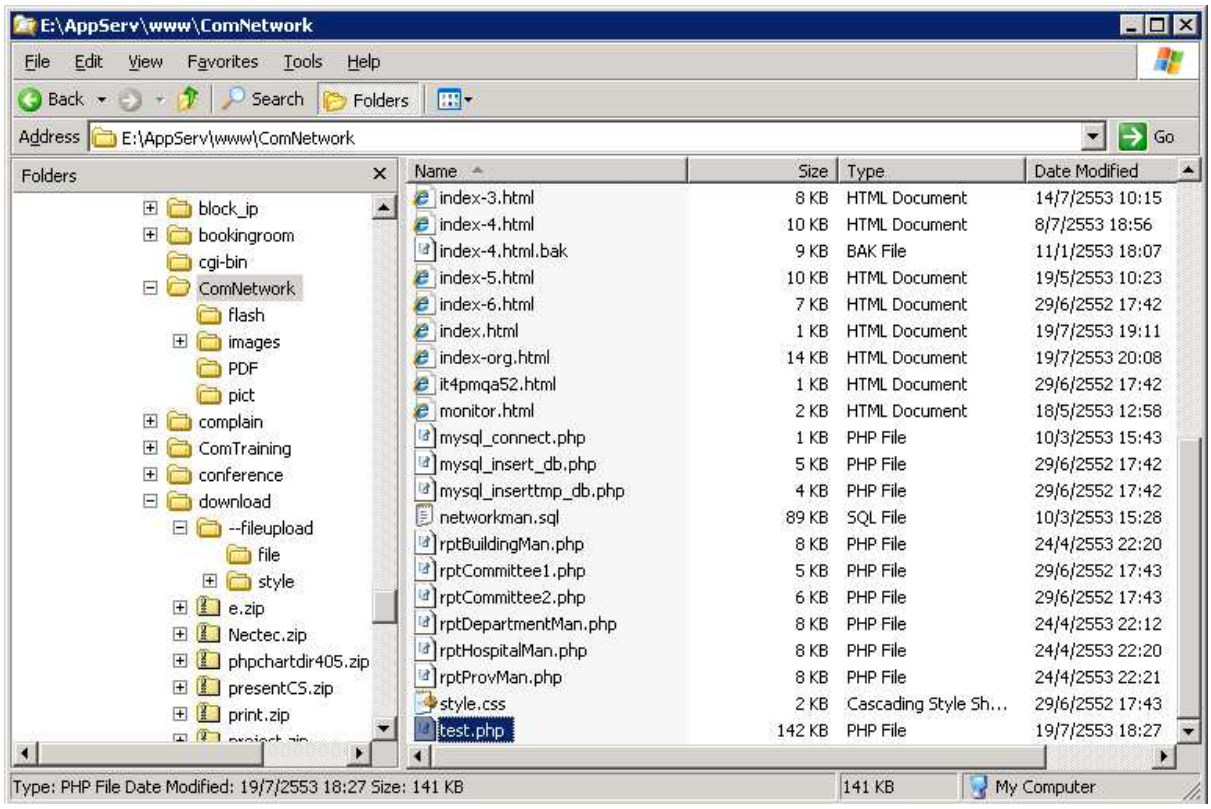
และมีการเรียกใช้งาน Script file upload.php ที่ folder /download/fileupload



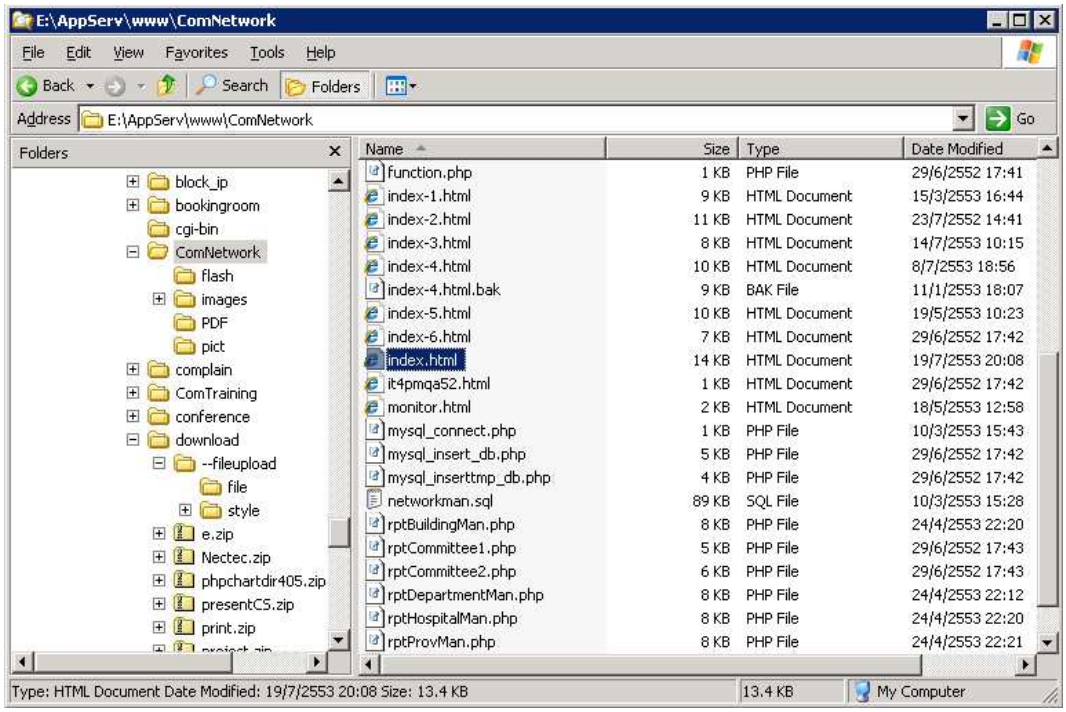
การแก้ไขให้ทำการ rename หรือ ลบ folder /download/fileupload ออก




E:\AppServ\www\download\--fileupload
File Edit View Favorites Tools Help
Back Search Folders
Address E:\AppServ\www\download\--fileupload
Go
Folders
conference
download
--fileupload
file
style
e.zip
Nectec.zip
phpchartdir405.zip
presentCS.zip
print.zip
project.zip
Project_Health.zip
scan.zip
temp.zip
XML.zip
yai.zip
ecard
file
folio
Name Size Type Date Modified
file File Folder 19/7/2553 17:58
style File Folder 19/7/2553 17:58
index.php 3 KB PHP File 19/7/2553 18:02
index.php~ 3 KB PHP~ File 19/7/2553 17:58
loader.gif 11 KB GIF Image 19/7/2553 17:58
upload.php 1 KB PHP File 19/7/2553 18:01
6 objects (Disk free space: 4.51 GB)
16.2 KB
My Computer


E:\AppServ\www\ComNetwork
File Edit View Favorites Tools Help
Back Search Folders
Address E:\AppServ\www\ComNetwork
Go
Folders
block_ip
bookingroom
cgi-bin
ComNetwork
flash
images
PDF
pict
complain
ComTraining
conference
download
--fileupload
file
style
e.zip
Nectec.zip
phpchartdir405.zip
presentCS.zip
print.zip
Name Size Type Date Modified
index-3.html 8 KB HTML Document 14/7/2553 10:15
index-4.html 10 KB HTML Document 8/7/2553 18:56
index-4.html.bak 9 KB BAK File 11/1/2553 18:07
index-5.html 10 KB HTML Document 19/5/2553 10:23
index-6.html 7 KB HTML Document 29/6/2552 17:42
index.html 1 KB HTML Document 19/7/2553 19:11
index-org.html 14 KB HTML Document 19/7/2553 20:08
it4pmqa52.html 1 KB HTML Document 29/6/2552 17:42
monitor.html 2 KB HTML Document 18/5/2553 12:58
mysql_connect.php 1 KB PHP File 10/3/2553 15:43
mysql_insert_db.php 5 KB PHP File 29/6/2552 17:42
mysql_inserttmp_db.php 4 KB PHP File 29/6/2552 17:42
networkman.sql 89 KB SQL File 10/3/2553 15:28
rptBuildingMan.php 8 KB PHP File 24/4/2553 22:20
rptCommittee1.php 5 KB PHP File 29/6/2552 17:43
rptCommittee2.php 6 KB PHP File 29/6/2552 17:43
rptDepartmentMan.php 8 KB PHP File 24/4/2553 22:12
rptHospitalMan.php 8 KB PHP File 24/4/2553 22:20
rptProvMan.php 8 KB PHP File 24/4/2553 22:21
style.css 2 KB Cascading Style Sh... 29/6/2552 17:43
test.php 142 KB PHP File 19/7/2553 18:27
Type: PHP File Date Modified: 19/7/2553 18:27 Size: 141 KB
141 KB
My Computer

เสร็จแล้วทำการส่ง file index.html กลับคืนไปยัง server



ทดลองเปิดหน้า webpage ดูอีกครั้ง