DATAFARM
COMPANY LIMITED

PROOF OF CONCEPT

ZYXEL BYPASS AUTHENTICATION

BY AUDITZ

14/03/2014

DATAFARM CO., LTD.

HTTP://WWW.DATAFARM.CO.TH

ZYXEL BYPASS AUTHENTICATION

ZyXEL คือยี่ห้อเร้าเตอร์ ที่ผู้ให้บริการ Internet ความเร็วสูง (ADSL) หลายๆบริษัทเลือกใช้ เพื่อให้บริการลูกค้า ดังนั้น โดยส่วนมากแทบทุกบ้านที่ใช้บริการ Internet ความเร็วสูง (ADSL) จะต้องใช้เร้าเตอร์ยี่ห้อ ZyXEL

Bypass authentication คือ เป็นการเข้าถึงไฟล์หรือโฟลเดอร์ ที่มีการกำหนดสิทธิ์ โดยอาศัยวิธีการต่างๆ แม้จะไม่มีสิทธิ์ในการเข้าถึง เช่น นาย ก เป็นเจ้าของตู้เซฟ แต่นาย ข สามารถเข้าถึงตู้เซฟนั้น โดยอาศัยวิธีการต่างๆ โดยไม่ผ่านนาย ก ซึ่งเป็นเจ้าของตู้เซฟ

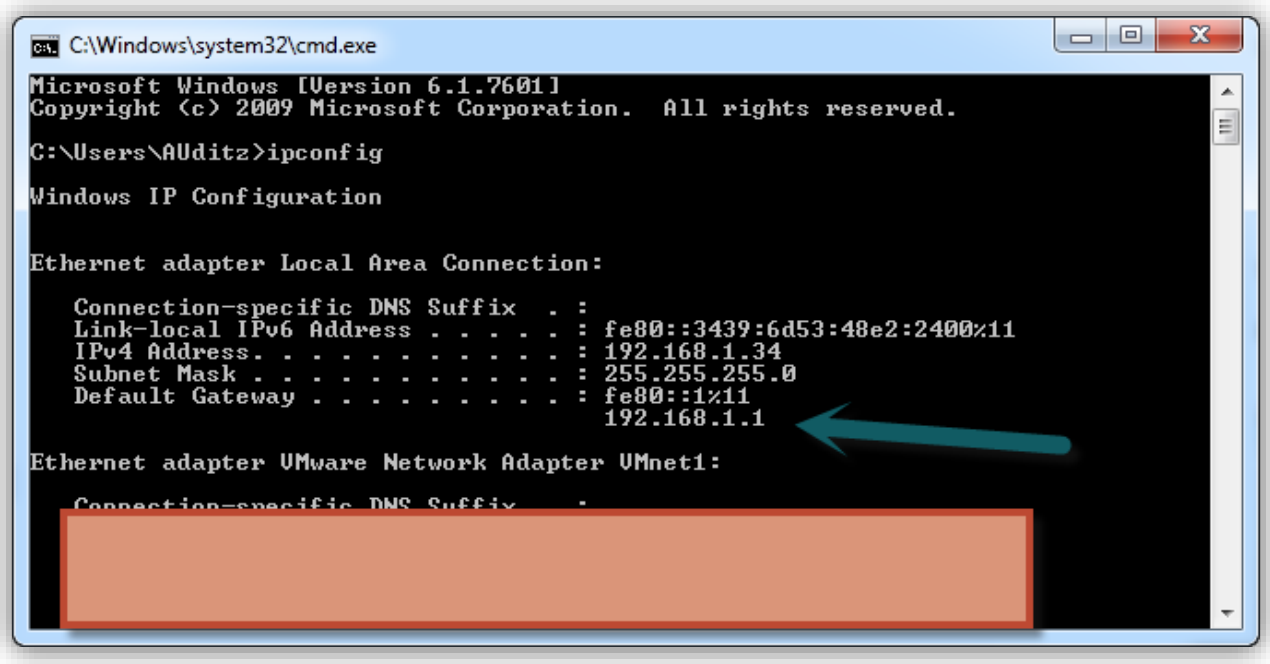
Zyxel bypass authentication หมายถึง สามารถเข้าถึงไฟล์สำคัญๆ แม้ไม่ใช่ admin ตัวอย่างเช่น ผู้ที่ไม่มีพาส admin ก็สามารถเข้าถึงไฟล์ ที่เก็บ Username และ Password ของ Internet ของเราได้ (สามารถเอารหัส ของเราไปต่อเน็ตที่ไหนก็ได้) และสามารถเข้าถึง ไฟล์ที่เป็นการตั้งค่า ของ WIFI เราได้ ดังนั้น ก็สามารถเห็น รหัสผ่าน WIFI เราได้ แม้จะตั้งค่าเป็น WPA2 แล้วก็ตาม

SEVERITY: HIGH

PROOF OF CONCEPT (POC)

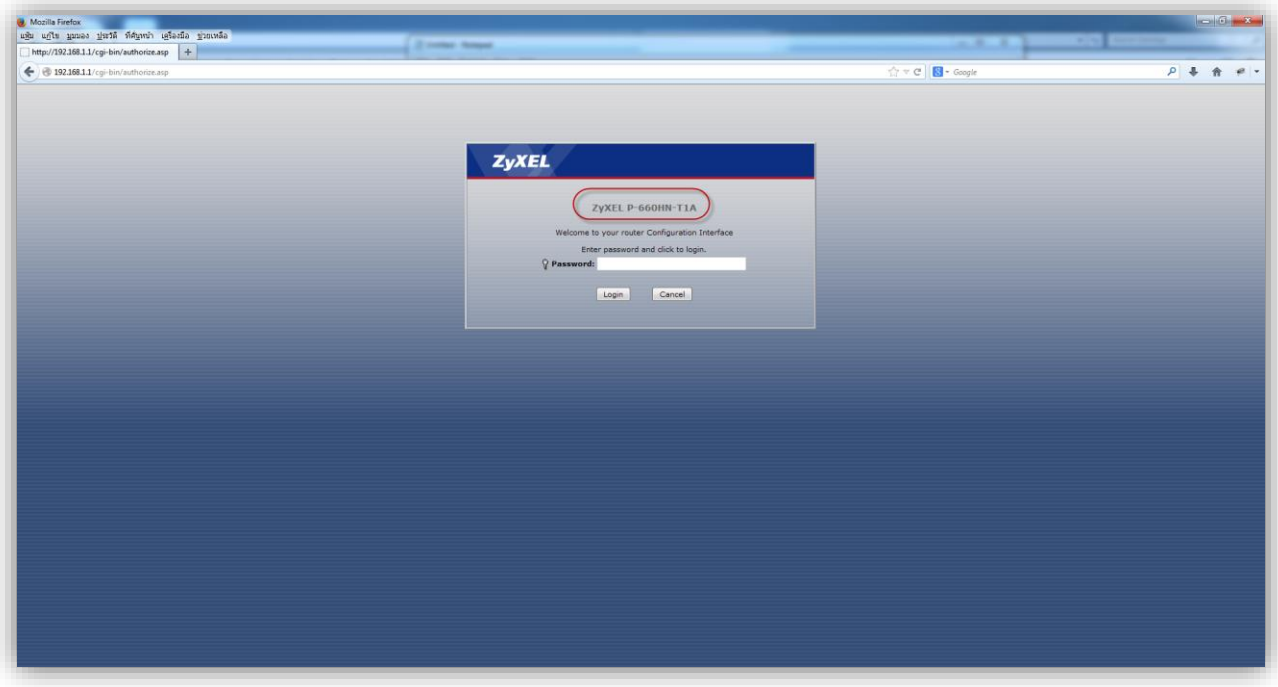
1. ZYXEL DEFAULT AUTHENTICATION

ทดสอบเข้าหน้าเว็บ ผ่านไอพี 192.168.1.1 (ภาพ2)ซึ่งปกติแล้วค่าที่ทาง ผู้ให้บริการ Internet ความเร็วสูง ตั้งจะเป็นค่านี้เสมอ (ในกรณี Hacker โจมตี สามารถเข้าผ่าน IP ของท่านจากภายนอก และจัดการได้ตาม ที่จะ POC) หรือพิมพ์คำสั่ง ipconfig สำหรับ windows (ifconfig สำหรับ linux) เพื่อที่จะดู gateway ดังภาพ1



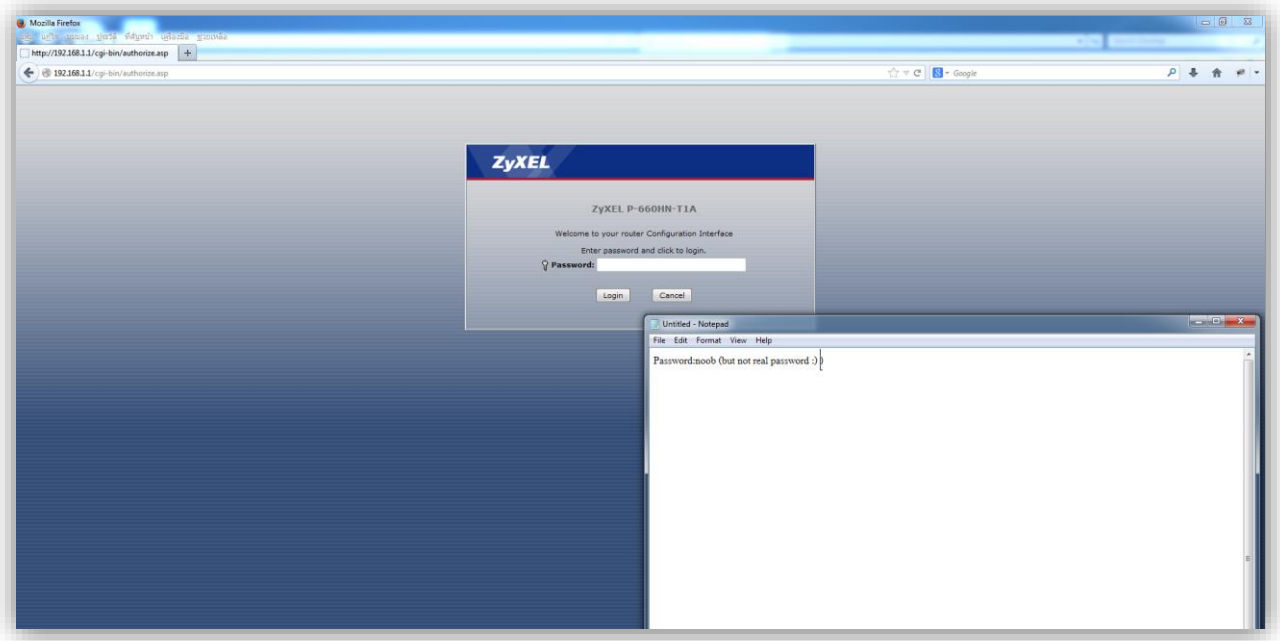
ภาพ1 แสดง การดู Default Gateway

เมื่อเข้าผ่านหน้าเว็บ ในกรณีถ้าเร้าเตอร์รุ่นเดียวกับที่ใช้ POC ก็จะขึ้นหน้าเว็บดังภาพ2 ซึ่งจะต้องรู้ Password สำหรับ Login ถึงจะเข้าไปจัดการในระบบ ของเร้าเตอร์ได้



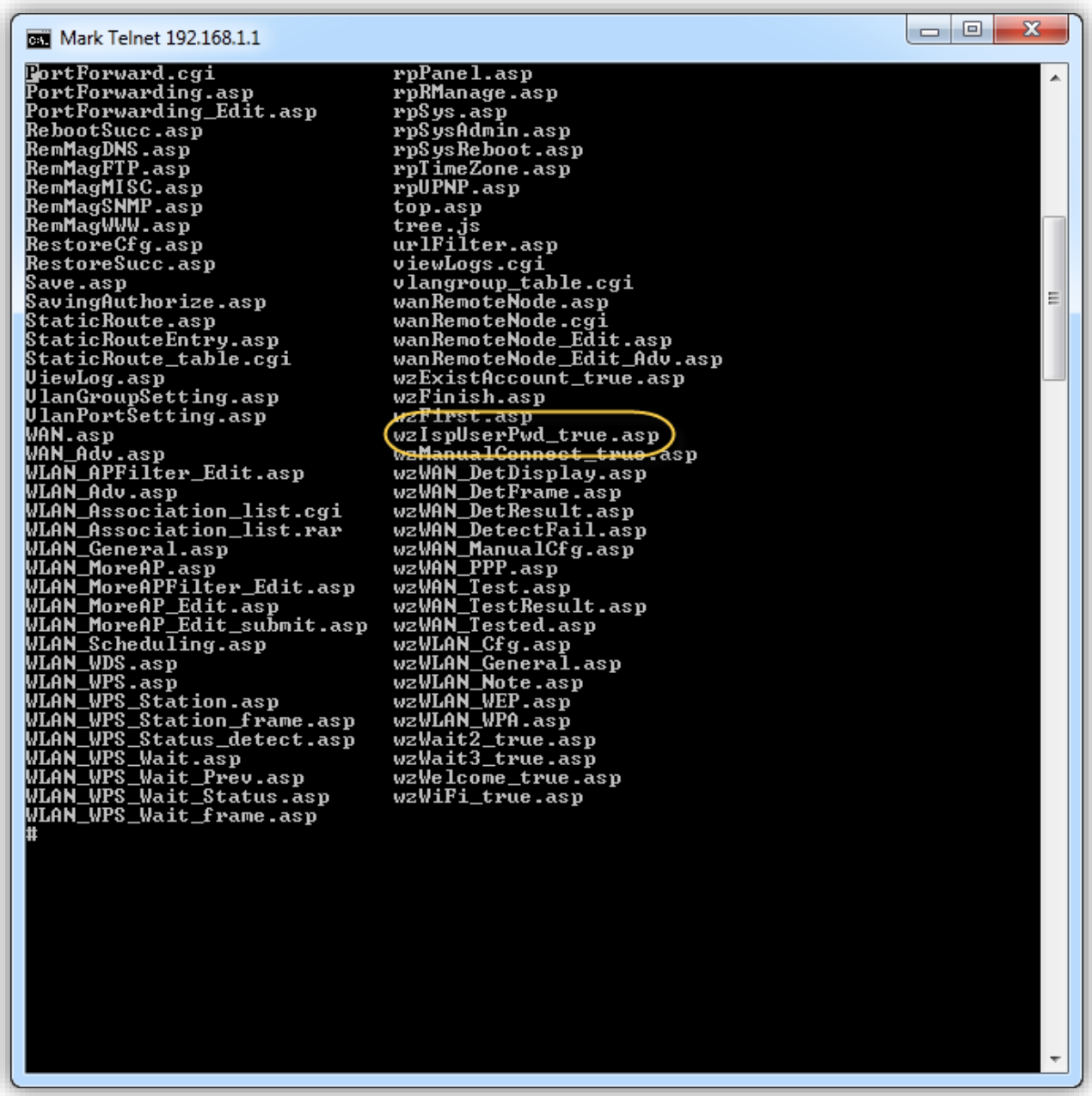
ภาพ2 แสดงให้เห็นว่า ในการเข้าถึงการจัดการเร้าเตอร์หน้าเว็บต้อง login ก่อนทุกครั้ง

แต่ช่องโหว่มันเกิดขึ้น คือไม่ต้องรู้พาส ที่ถูกต้องแม้จะใส่พาสไปมั่วๆ ก็สามารถเข้าถึงไฟล์ที่เป็นข้อมูลสำคัญ ได้ โดยในที่นี้ ขอยกตัวอย่าง ให้ดูพอให้เข้าใจ เมื่อทดสอบใส่พาสเวิด คือ noob ในการ login ก็ไม่สามารถผ่านการยืนยันตัวตนได้ เพราะ พาสเวิดที่ใส่ไปไม่ถูกต้อง ดังภาพ 3



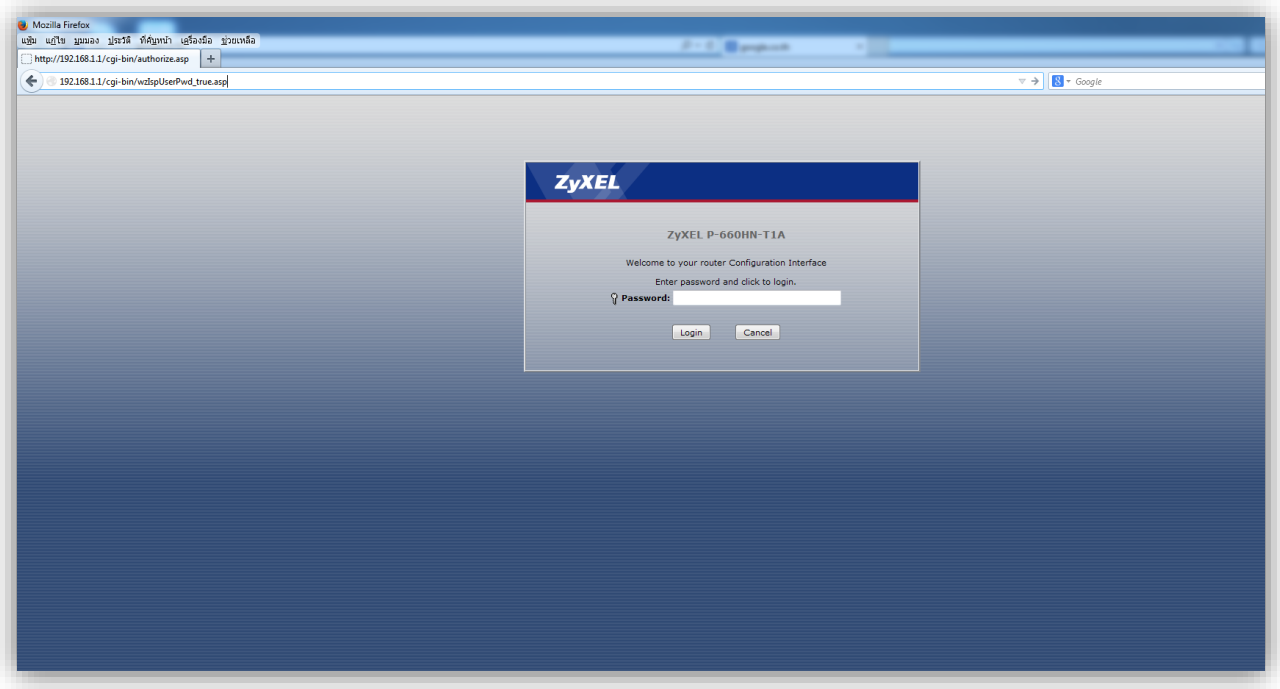
ภาพ3 แสดงการ ใส่ พาสเวิด noob แต่ไม่สามารถ login ได้พาสได้

จากนั้น ผมได้พบไฟล์ ที่หน้าสนใจ เพราะเป็นไฟล์ที่เก็บค่า username และ password ของผู้ใช้งาน Internet ชื่อไฟล์คือ wzIspUserPwd_true.asp ซึ่งไฟล์นี้หาได้จากการ telnet เข้าไปที่เร้าเตอร์ จากนั้นก็ ดูรายชื่อไฟล์ ดังภาพ4



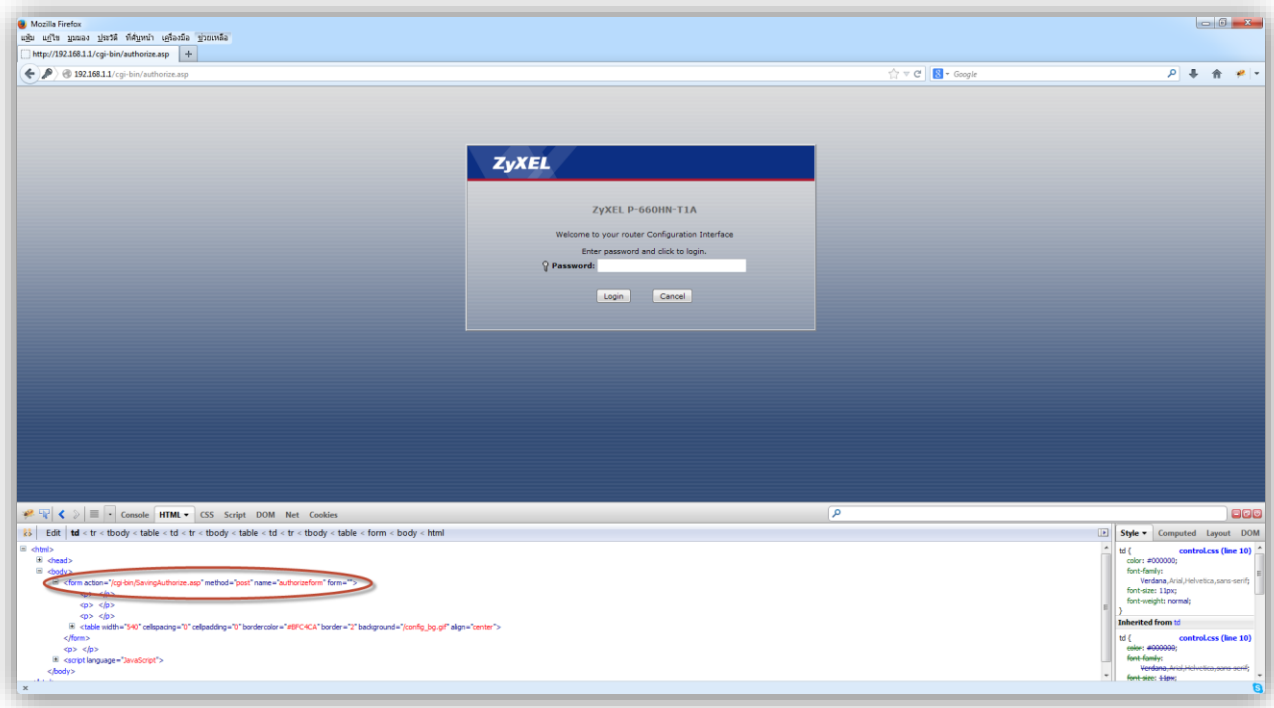
ภาพ4 แสดงรายชื่อไฟล์ที่อยู่บนเร้าเตอร์

จากการทดสอบเมื่อทราบว่ามีไฟล์นี้มีอยู่จริง และนำไฟล์นี้ไปวางแล้วคลิกผ่านหน้าเว็บปกติธรรมดา จะไม่สามารถเข้าถึงไฟล์ดังกล่าวได้ เพราะเร้าเตอร์มีการตั้งค่าความปลอดภัย ต้องมีการยืนยันตัวตน ก่อนเสมอถึงจะสามารถเข้าถึงไฟล์ดังกล่าวได้ ดังภาพ 5



ภาพ6 เมื่อทดสอบเรียกไฟล์ตรงๆ ไม่สามารถเข้าถึงไฟล์ได้ ต้องมีการยืนยันตัวตนทุกครั้งเสมอ

หลังจากนั้นได้ทำการแก้ไข ค่าให้มีการเรียกหน้าเว็บใหม่ เมื่อมีการใส่ค่า password โดยตัวอย่างดังภาพ 7



ภาพ7 แก้ค่าการเรียกค่าหน้าเว็บ โดยใช้โปรแกรม firebug

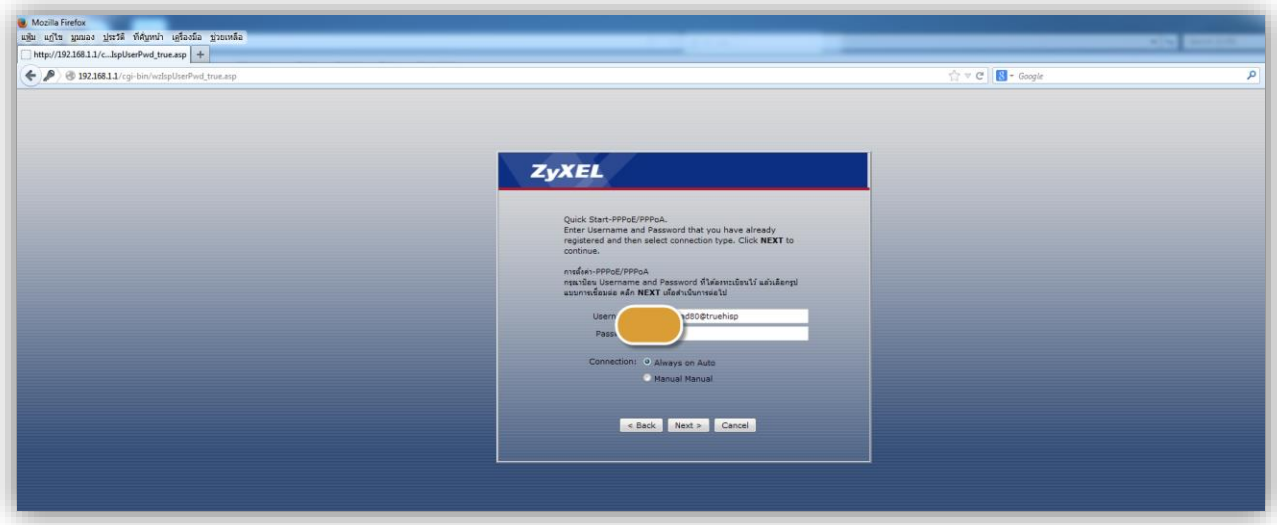
ซึ่งค่าปกติ ของเร้าเตอร์ที่มีการตั้งไว้ เมื่อมีการใส่ พาสเวิด แล้วคลิกปุ่ม Login จะมีการเรียกไปที่หน้าเพจ SavingAuthorize.asp นี้เสมอ จากการทดสอบ เมื่อแก้ไขค่าดังกล่าว จาก SavingAuthorize.asp เป็นค่า wzIspUserPwd_true.asp และ พาสเวิด ก็ใส่พาสมั่วๆ แล้วกดปุ่ม Login ปรากฏว่า สามารถเข้าถึงไฟล์ wzIspUserPwd_true.asp โดยไม่ต้องยืนยันตัวตนที่ถูกต้อง

ค่าที่แก้ไข ปกติคือ

```
<form action="/cgi-bin/SavingAuthorize.asp" method="post" name="authorizeform" form="">
```

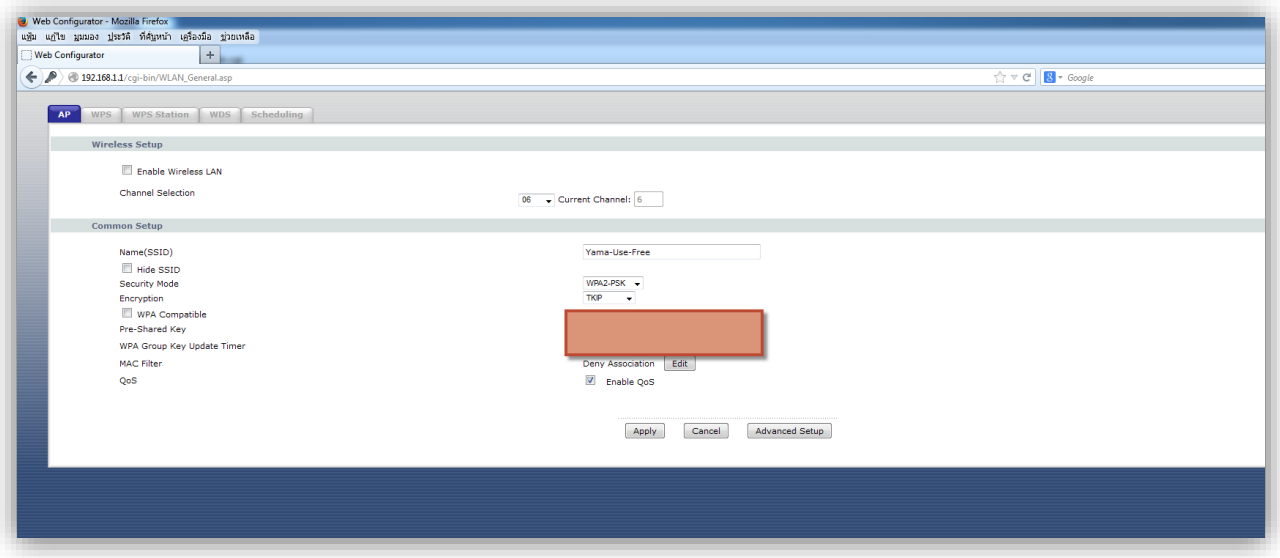
แก้ไขค่าเป็น

```
<form action="/cgi-bin/ wzIspUserPwd_true.asp " method="post" name="authorizeform"
```



ภาพ8 แสดงการถึงไฟล์ wzIspUserPwd_true.asp และเห็นรายละเอียด Username & Password

และสามารถเข้าถึงไฟล์อื่น ยกตัวอย่างเช่นไฟล์ WLAN_General.asp ซึ่งเป็นไฟล์กำหนดการตั้งค่า WIFI ดังนั้น พาสเวิด แม้จะมีการตั้งยากแค่ไฟล์ เข้ารหัสแบบ WPA2 อย่างไรก็ตาม ก็สามารถเห็น พาสเวิด ได้ ดังภาพ9



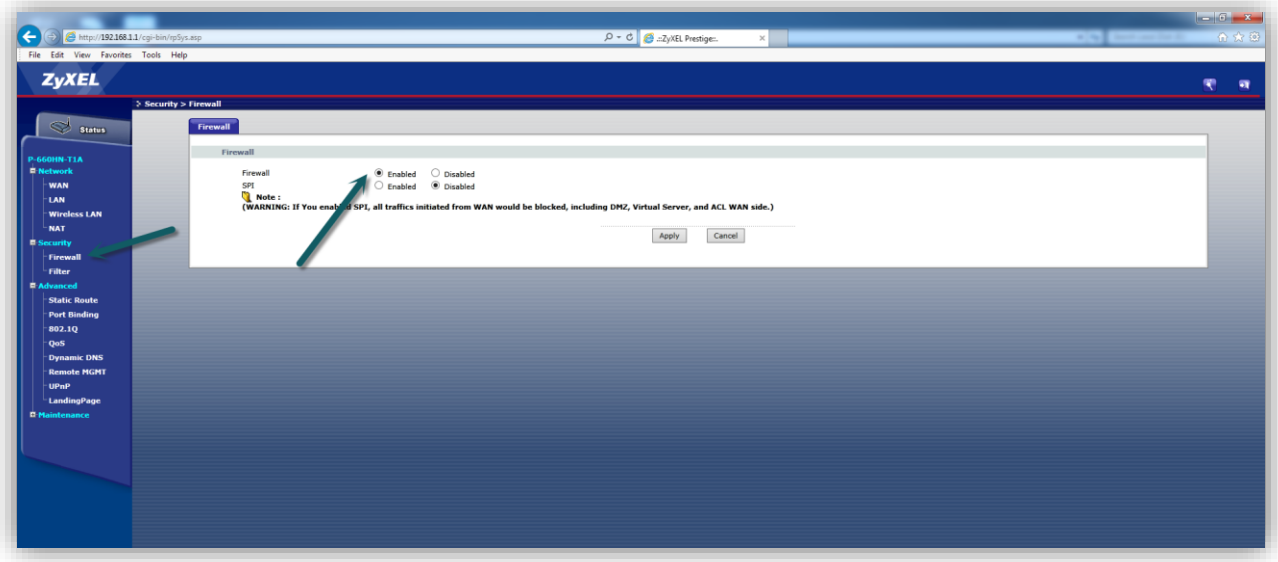
ภาพ9 แสดงรายละเอียดหน้า WLAN_General.asp และ Password WIFI

เบื้องต้นข้าพเจ้าทดสอบเพิ่มอีก WAN.asp , rpSysAdmin.asp ซึ่งสามารถใช้วิธีการเดียวกันเข้าถึงได้เลย

แนวทางการป้องกัน

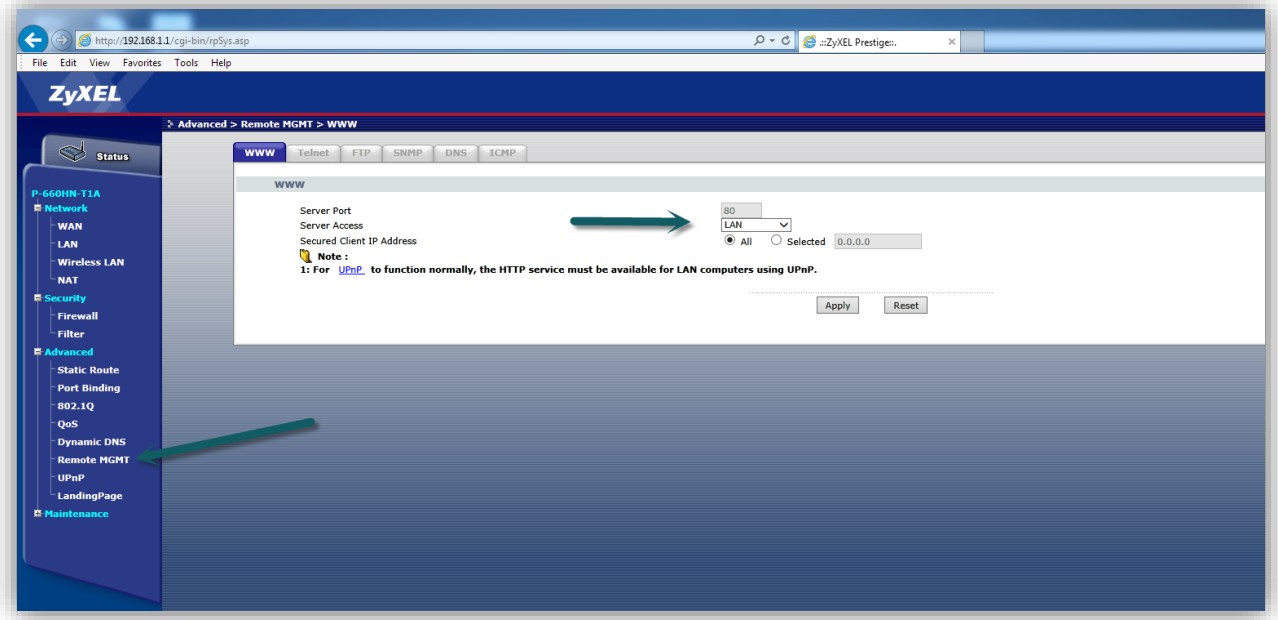
1. เปิดใช้งาน Firewall ที่ตัวเร้าเตอร์ของท่าน (เพื่อไม่ให้ไอพีจากภายนอกเข้าถึงเร้าเตอร์เราได้)

ดังภาพ 10



ภาพ 10 แสดงการ เปิด firewall ที่เร้าเตอร์

2. อัพเกรด firmware จากผู้ให้บริการ
3. กำหนดการเข้าถึงใช้งานหน้าเว็บ เฉพาะ LAN ดังภาพ 11



ภาพ 11 แสดงการ กำหนดสิทธิ์ให้เข้าถึงหน้าเว็บได้เฉพาะ LAN