แนวปฏิบัติในการจัดทำเว็บไซต์มหาวิทยาลัยสงขลานครินทร์

พ.ศ. 2567

บันทึกการแก้ไข

แก้ไขครั้งที่	วันที่	รายละเอียด
1.0	22 เมษายน 2567	ฉบับออกใหม่

วัตถุประสงค์

1. ผู้ดูแลเว็บไซต์ทราบขั้นตอน “ลงทะเบียนเว็บไซต์ ม.อ.”
2. ผู้ดูแลเว็บไซต์สามารถตรวจสอบความมั่นคงปลอดภัยทางไซเบอร์ของเว็บไซต์ที่รับผิดชอบในเบื้องต้นได้เอง ตามภาคผนวก
3. ผู้ดูแลเว็บไซต์ได้ทราบ “แนวปฏิบัติการรักษาความมั่นคงปลอดภัยเว็บไซต์ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)”
4. ผู้ดูแลเว็บไซต์ได้ทราบ “รายละเอียดมาตรฐานเว็บไซต์ภาครัฐ เวอร์ชัน 3.0 ที่ออกเมื่อวันที่ 28 กันยายน 2566 สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (มสพร.)”
5. ผู้ดูแลเว็บไซต์ได้ทราบ “รายละเอียด รายงาน OVAL และเกณฑ์เปรียบเทียบ CIS Benchmarks โดย Center for Internet Security)”
6. ลดโอกาสที่เว็บไซต์ ม.อ. จะถูกโจมตี
7. ลดจำนวนหนังสือที่สำนักนวัตกรรมดิจิทัลและระบบอัจฉริยะต้องส่งแจ้งให้ส่วนงานในมหาวิทยาลัยแก้ไขช่องโหว่เว็บไซต์
8. เพิ่มจำนวนเว็บไซต์ภายใต้ชื่อโดเมนของ ม.อ. ที่ได้มาตรฐานเว็บไซต์ภาครัฐ

ขอบเขต

เว็บไซต์ ม.อ. คือ เว็บไซต์คณะ/ส่วนงานภายในมหาวิทยาลัยสงขลานครินทร์ ที่อยู่ภายใต้ชื่อโดเมนย่อย และภายใต้ชื่อโดเมน psu.ac.th และ psu.th

แนวปฏิบัติ มาตรฐาน และ เกณฑ์เปรียบเทียบ

1. แนวปฏิบัติการรักษาความมั่นคงปลอดภัยเว็บไซต์ (Website Security Guideline) สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) หัวข้อ มาตรฐานและแนวทางปฏิบัติ
   https://www.ncsa.or.th/standards-and-practices.html
2. มาตรฐานเว็บไซต์ภาครัฐ เวอร์ชัน 3.0 วันที่ 28 กันยายน 2566 มสพร.11-2566
   https://standard.dga.or.th/wp-content/uploads/2023/09/มสพร.-11-2566-ว่าด้วยมาตรฐานเว็บไซต์ภาครัฐ-เวอร์ชัน-3.0.pdf
3. มาตรฐานเว็บไซต์ภาครัฐ เวอร์ชัน 3.0 รายการตรวจสอบ (Checklist)

https://standard.dga.or.th/wp-content/uploads/2023/09/เอกสารประกอบเล่มมาตรฐานเว็บไซต์_Checklist_v0.1-1.pdf

4. เกณฑ์เปรียบเทียบ CIS Benchmarks ต่างๆ ที่ Center for Internet Security สำหรับส่วนประกอบต่างๆ ของเว็บไซต์

   OS เช่น CentOS, Debian, Microsoft Windows Server, Oracle, Red Hat, Ubuntu

   Server Software เช่น Apache HTTP, Apache Tomcat, BIND, Docker, Kubernetes, MariaDB, Microsoft IIS, Microsoft SQL Server, MongoDB, NGINX, Oracle Database, PostgreSQL, VMware

   สำหรับอุปกรณ์เครือข่ายต่างๆ เช่น Cisco, Fortinet, Palo Alto Networks

   สำหรับโปรแกรมเว็บเบราเซอร์ เช่น Edge, Google Chrome, Mozilla Firefox, Safari

   สำหรับโปรแกรมต่างๆ เช่น Microsoft 365, Microsoft Office, Zoom

   https://www.cisecurity.org/cis-benchmarks

ขั้นตอนลงทะเบียนเว็บไซต์ ม.อ. (PSU Website Registration)

1. ผู้ดูแลเว็บไซต์ได้จัดทำเว็บไซต์ตาม “แนวปฏิบัติ มาตรฐาน และเกณฑ์เปรียบเทียบ” ข้างบนครบถ้วน
2. ผู้ดูแลเว็บไซต์อีเมลถึง itoc@psu.ac.th โดยระบุ ชื่อเรื่อง (Subject)

ขอเปิดเว็บไซต์ (ชื่อเว็บไซต์) ให้เข้าถึงได้จากอินเทอร์เน็ต

ในอีเมลให้แจ้งรายละเอียดดังต่อไปนี้

========== เริ่มต้น รายละเอียด แจ้ง ขอเปิดเว็บไซต์ ==========

1. ข้าพเจ้าชื่อ...(ระบุชื่อ นามสกุล) เป็น ผู้ดูแลเว็บไซต์ มีความประสงค์ขอเปิดเว็บไซต์ให้เข้าถึงได้จากอินเทอร์เน็ต
2. โดยมีผู้บริหารไอทีส่วนงานชื่อ...(ระบุชื่อ นามสกุล)
3. เว็บไซต์ชื่อ...(ระบุ URL ของเว็บไซต์ https://...)
4. ซึ่งเป็นเว็บไซต์ของส่วนงาน...(ระบุชื่อส่วนงาน และหน่วยงานย่อย)
5. IP Address...(ระบุ Private IP Address ของเครื่องที่มีเว็บไซต์นี้)
6. ข้าพเจ้ายืนยันว่า (ได้/ไม่ได้) ติดตั้งใบรับรองดิจิทัล (SSL Certificate) เพื่อรองรับ https port 443
7. นอกจาก port 80, 443 แล้ว ต้องการเปิดให้เข้าถึง port ต่อไปนี้ (ระบุเลข port เพิ่มเติม)

8. ข้าพเจ้ารับทราบว่า เว็บไซต์ที่ขอเปิด จะถูกตรวจสอบเพื่อจัดทำรายงานช่องโหว่ด้วย Nessus Vulnerability Scanner และเมื่อได้รับรายงานข้าพเจ้าจะแก้ไขไม่ให้มีช่องโหว่ Critical, High, Medium หลงเหลืออยู่ โดยรายละเอียดเกี่ยวกับเว็บไซต์มีดังต่อไปนี้
   8ก. OS เป็นระบบ และ รุ่นใด?
   8ข. Web Server เป็นระบบ และ รุ่นใด?
   8ค. ติดตั้งระบบ Web Server และส่วนประกอบ อ้างอิง คำแนะนำจาก URL ใด?
9. หากโปรแกรมเว็บไซต์ใช้บน OS Linux ให้ส่งรายงาน OVAL เป็นลิงก์ หรือเป็นไฟล์แนบมากับอีเมล ตามคำแนะนำภาคผนวก ฉ. ในแนวปฏิบัติในการจัดทำเว็บไซต์มหาวิทยาลัยสงขลานครินทร์

========== สิ้นสุด รายละเอียด แจ้ง ขอเปิดเว็บไซต์ ==========

3. ผู้ดูแลเว็บไซต์ ใช้ PSU Microsoft Teams Chat ติดต่อ songkrant.m หรือ tipaporn.p เพื่อรับรายงาน Nessus Scan เป็นแนวทางดำเนินการแก้ไข และประสานงานการแก้ไขช่องโหว่ จนไม่มีช่องโหว่ Critical, High, Medium หลงเหลืออยู่
4. itoc@psu ได้รับแจ้งจาก songkrant.m หรือ tipaporn.p ว่ารายงาน Nessus ของเว็บไซต์ ไม่มีช่องโหว่ Critical, High, Medium แล้ว จึงจะกำหนดค่าบนไฟร์วอลล์ของมหาวิทยาลัย เพื่อเปิดเว็บไซต์ให้เข้าถึงได้จากอินเทอร์เน็ต
5. เมื่อเว็บไซต์เข้าถึงได้จากอินเทอร์เน็ตแล้ว ผู้ดูแลเว็บไซต์ ตรวจสอบ Public IP Address ได้จาก URL **https://bgp.he.net/dns/ชื่อเว็บไซต์**
6. ผู้ดูแลเว็บไซต์ ใช้เครื่องมือตรวจสอบ Shodan ว่ามีรายงานช่องโหว่ของเว็บไซต์ ปรากฏสู่สาธารณะหรือไม่ ได้จาก URL **https://www.shodan.io/host/เลข Public IP Address** (ภาคผนวก ก)
7. ผู้ดูแลเว็บไซต์ ใช้เครื่องมือตรวจสอบ Qualys SSL Server Test ว่ามีการเข้ารหัสข้อมูล (Encryption) เพื่อเพิ่มความปลอดภัยในการสื่อสารผ่านเครือข่าย ตามคำแนะนำ https://www.tenable.com/plugins/nessus/156899 ครบถ้วนหรือไม่ ได้จาก URL **https://www.ssllabs.com/ssltest/analyze.html** (ภาคผนวก ข)
8. ผู้ดูแลเว็บไซต์ ใช้เครื่องมือตรวจสอบ Security Headers ว่ามี การกำหนดรายละเอียดในส่วนหัวของเว็บไซต์ ครบถ้วนหรือไม่ ได้จาก URL **https://securityheaders.com/** (ภาคผนวก ค)
9. ผู้ดูแลเว็บไซต์ ใช้เครื่องมือตรวจสอบ SSL Checker ว่าใบรับรองดิจิทัลได้ติดตั้งถูกต้องหรือไม่ ได้จาก URL **https://www.sslshopper.com/ssl-checker.html** (ภาคผนวก ง)
10. ผู้ดูแลเว็บไซต์ ตรวจสอบว่าในหน้าแรกของเว็บไซต์ มี หมายเลขโทรศัพท์ หรือ อีเมล ที่ผู้ใช้บริการสามารถติดต่อสื่อสารกับหน่วยงานได้ (ภาคผนวก จ)

11. ผู้ดูแลเว็บไซต์ ที่โปรแกรมเว็บไซต์ใช้บน OS Linux ให้ทำรายงาน OVAL ตามคำแนะนำ (ภาคผนวก ฉ)
12. ผู้ดูแลเว็บไซต์ จะได้รับรายงาน Nessus Scan เดือนละครั้งทาง PSU Microsoft Teams Chat ที่ได้ติดต่อไว้ และสามารถติดต่อให้ทำรายงานเพิ่มเติมได้ หากมีการปรับปรุงระบบหรือส่วนประกอบเว็บไซต์ หรือมีข้อสงสัยเกี่ยวกับความปลอดภัย

ภาคผนวก ก

ก. <u>เครื่องมือตรวจสอบ **Shodan** รายงานช่องโหว่ของเว็บไซต์ ปรากฏสู่สาธารณะ</u>

ค่าเป้าหมาย :

ก1 ไม่มี Vulnerability หรือ CVE ปรากฏ
ก2 Server Type ไม่แสดงข้อมูล เกี่ยวกับระบบปฏิบัติการและรุ่นของโปรแกรมเว็บไซต์

ผู้ดูแลเว็บไซต์ ใช้เครื่องมือตรวจสอบ Shodan ว่ามีรายงานช่องโหว่ของเว็บไซต์ ปรากฏสู่สาธารณะหรือไม่ ได้จาก URL

https://www.shodan.io/host/เลข Public IP Address

1. Last Seen จะแสดง ปี ค.ศ. เดือน และวันที่ ล่าสุด ที่ Shodan มีข้อมูล Public IP Address ของเว็บไซต์
2. หาก Shodan ไม่มี ข้อมูล Public IP Address ของเว็บไซต์ จะแสดง No Information
3. หาก Shodan มีข้อมูล Server Type และ Server Type นั้นมีปรากฏช่องโหว่ที่ National Vulnerability Database https://nvd.nist.gov/ จะแสดงเลข Common Vulnerabilities and Exposures (CVE) และมีคำอธิบายย่อของช่องโหว่ ผู้ดูแลเว็บไซต์ ต้องแก้ไขช่องโหว่
4. ผู้ดูแลเว็บไซต์ “ต้องแก้ไข” Server Type “ไม่ให้แสดงข้อมูล” เกี่ยวกับระบบปฏิบัติการและรุ่นของโปรแกรมเว็บไซต์ ทำให้แฮคเกอร์ยากที่จะหาช่องโหว่ที่ตรงรุ่นกับระบบ

ภาคผนวก ข

ข. <u>เครื่องมือตรวจสอบ Qualys การเข้ารหัสข้อมูล (Encryption)</u>

ค่าเป้าหมาย : A+

ข1 Configuration > Cipher Suites TLS 1.3 สีเขียว ไม่มี Weak Cipher สีเหลือง ปรากฏ
ข2 Configuration > Cipher Suites TLS 1.2 สีเขียว ไม่มี Weak Cipher สีเหลือง ปรากฏ
ข3 Configuration > Miscellaneous HTTP server signature ไม่แสดงข้อมูล เกี่ยวกับระบบปฏิบัติการและรุ่นของโปรแกรมเว็บไซต์

ผู้ดูแลเว็บไซต์ ใช้เครื่องมือตรวจสอบ Qualys SSL Server Test ว่ามี การเข้ารหัสข้อมูล (Encryption) เพื่อเพิ่มความปลอดภัยในการสื่อสารผ่านเครือข่าย ตามคำแนะนำ https://www.tenable.com/plugins/nessus/156899 ซึ่งให้ใช้เฉพาะ TLS 1.2 และ TLS 1.3 ครบถ้วนหรือไม่ ได้จาก URL https://www.ssllabs.com/ssltest/analyze.html

1. ให้เลือก Do not show the results on the boards
2. ให้ใส่ชื่อเว็บไซต์ที่ต้องการตรวจสอบ
3. หาก Configuration > Cipher Suites ยังมี Weak Cipher และไม่ได้ใช้เฉพาะ TL 1.2 และ TLS 1.3 ผู้ดูแลเว็บไซต์ ต้องแก้ไข ให้ใช้ Cipher Suites ตามคำแนะนำ
4. หาก Configuration > Miscellaneous HTTP server signature แสดงข้อมูล เกี่ยวกับระบบปฏิบัติการและรุ่นของโปรแกรมเว็บไซต์ ผู้ดูแลเว็บไซต์ “ต้องแก้ไข” ไม่ให้แสดงข้อมูลเกี่ยวกับระบบปฏิบัติการและรุ่นของโปรแกรมเว็บไซต์ ทำให้แฮคเกอร์ยากที่จะหาช่องโหว่ที่ตรงรุ่นกับระบบ

ภาคผนวก ค

ค. <u>เครื่องมือตรวจสอบ Security Headers การกำหนดรายละเอียดในส่วนหัวของเว็บไซต์</u>

ค่าเป้าหมาย : A+

ค1 Security Report Summary > Headers: สีเขียว ทั้งหมด ไม่มี Missing Headers สีแดง และไม่มี Warnings สีเหลือง ปรากฏ
ค2 Raw Headers > server ไม่แสดงข้อมูล เกี่ยวกับระบบปฏิบัติการและรุ่นของโปรแกรมเว็บไซต์

ผู้ดูแลเว็บไซต์ ใช้เครื่องมือตรวจสอบ Security Headers ว่ามี การกำหนดรายละเอียดในส่วนหัวของเว็บไซต์ ครบถ้วนหรือไม่ ได้จาก URL

https://securityheaders.com

1. ให้เลือก Hide results
2. ให้ใส่ชื่อเว็บไซต์ที่ต้องการตรวจสอบ
3. หาก Security Report Summary > Headers ยังมีรายการ สีแดง ผู้ดูแลเว็บไซต์ ต้องแก้ไขให้เป็น สีเขียว ทั้งหมด ตามคำแนะนำ ในส่วน Missing Headers สีแดง และส่วน Warnings สีเหลือง
4. หาก Raw Headers > server หรือมีส่วนใด แสดงข้อมูล เกี่ยวกับระบบปฏิบัติการและรุ่นของโปรแกรมเว็บไซต์ ผู้ดูแลเว็บไซต์ “ต้องแก้ไข” ไม่ให้แสดงข้อมูลเกี่ยวกับระบบปฏิบัติการและรุ่นของโปรแกรมเว็บไซต์ ทำให้แฮคเกอร์ยากที่จะหาช่องโหว่ที่ตรงรุ่นกับระบบ
5. หาก Security Report Summary > Sites แสดง http://ชื่อเว็บไซต์ (Scan again over https) ผู้ดูแลเว็บไซต์ “ต้องแก้ไข” ตามคำแนะนำ HSTS
   https://sysadmin.psu.ac.th/2018/09/12/hardening-your-http-response-headers/

ภาคผนวก ง

ง. <u>เครื่องมือตรวจสอบ SSL Checker การติดตั้งใบรับรองดิจิทัล</u>

ค่าเป้าหมาย : เครื่องหมายถูก สีเขียว

ง1 The certificate will expire in …. days มีระยะเวลาอย่างน้อย 7 วัน เพื่อไม่ให้ใบรับรองดิจิทัลหมดอายุ ผู้ดูแลเว็บไซต์มีระยะเวลาอย่างน้อย 7 วันในการติดตั้งใบรับรองดิจิทัลใหม่
ง2 ถ้ามี Server Type ต้องไม่แสดงข้อมูล เกี่ยวกับระบบปฏิบัติการและรุ่นของโปรแกรมเว็บไซต์
ง3 Certificate Chain แสดงลูกศร สีเขียว ทั้งหมด ไม่มี ลูกศรหัก สีแดง และไม่มี Warnings สีเหลือง ปรากฏ

ผู้ดูแลเว็บไซต์ ใช้เครื่องมือตรวจสอบ SSL Checker ว่าใบรับรองดิจิทัลได้ติดตั้งถูกต้องหรือไม่ ได้จาก URL https://www.sslshopper.com/ssl-checker.html

1. ให้ใส่ชื่อเว็บไซต์ที่ต้องการตรวจสอบ
2. หากมี Server Type แสดงข้อมูล เกี่ยวกับระบบปฏิบัติการและรุ่นของโปรแกรมเว็บไซต์ ผู้ดูแลเว็บไซต์ “ต้องแก้ไข” ไม่ให้แสดงข้อมูลเกี่ยวกับระบบปฏิบัติการและรุ่นของโปรแกรมเว็บไซต์ ทำให้แฮคเกอร์ยากที่จะหาช่องโหว่ที่ตรงรุ่นกับระบบ
3. หากปรากฏ Certificate Chain แสดงด้วยเครื่องหมาย สีเหลือง หรือ ลูกศรหัก สีแดง ผู้ดูแลเว็บไซต์ ต้องแก้ไขโดยติดตั้งใบรับรองดิจิทัล Intermediate/chain Certificate ให้ถูกต้องตามคำแนะนำ ของบริษัทที่พัฒนาโปรแกรมเว็บไซต์ หรือบริษัทที่ออกใบรับรองดิจิทัล ให้แสดงลูกศร สีเขียว ทั้งหมด

ภาคผนวก จ

จ. <u>รายการตรวจสอบ (Checklist) ประกอบมาตรฐานเว็บไซต์ภาครัฐ เวอร์ชัน 3.0</u>

ค่าเป้าหมาย : มีข้อมูลแสดงรายละเอียดช่องทางที่ผู้ใช้บริการสามารถติดต่อสื่อสารกับหน่วยงานได้ (Contact us) และมีการประกาศนโยบายครบถ้วน (ดู **<u>แนวปฏิบัติ มาตรฐาน และ เกณฑ์เปรียบเทียบ ข้อที่ 2 ด้านบน)</u>**

จ1 เว็บไซต์มี Contact us (อ้างอิง หน้าที่ 5 มาตรฐานเว็บไซต์ภาครัฐ ver.3)
จ2 เว็บไซต์มี หมายเลขโทรศัพท์ ที่ผู้ใช้บริการสามารถติดต่อสื่อสารกับหน่วยงานได้
จ3 เว็บไซต์มี นโยบายเว็บไซต์ (อ้างอิง 10.1 หน้าที่ 22 และ ภาคผนวก ค. หน้าที่ 32-36 มาตรฐานเว็บไซต์ภาครัฐ ver.3)
จ4 เว็บไซต์มี นโยบายการคุ้มครองข้อมูลส่วนบุคคล และ นโยบายคุกกี้ (อ้างอิง 10.2 หน้าที่ 22 และ ภาคผนวก ค. หน้าที่ 37-40 มาตรฐานเว็บไซต์ภาครัฐ ver.3)
จ5 เว็บไซต์มี นโยบายการรักษาความมั่นคงปลอดภัยเว็บไซต์ (อ้างอิง 10.3 หน้าที่ 23 และ ภาคผนวก ค. หน้าที่ 40-43 มาตรฐานเว็บไซต์ภาครัฐ ver.3)

ผู้ดูแลเว็บไซต์ “ต้องจัดทำให้มี” ข้อมูลแสดงรายละเอียดช่องทางที่ผู้ใช้บริการสามารถติดต่อสื่อสารกับหน่วยงานได้ (Contact us) และมีการประกาศนโยบายครบถ้วน โดยค่าเป้าหมาย จ1 ถึง จ5 เป็นข้อกำหนดขั้นต่ำที่ต้องปรากฏใน เว็บไซต์ ตามแนวปฏิบัติในการจัดทำเว็บไซต์มหาวิทยาลัยสงขลานครินทร์

ทั้งนี้หากเว็บไซต์ส่วนงานมีรายละเอียดบริการที่เกี่ยวข้องกับธุรกรรมอิเล็กทรอนิกส์เพิ่มเติม ผู้ดูแลเว็บไซต์ ต้องดำเนินการเพิ่มเติมในข้ออื่น ๆ ที่เกี่ยวข้อง เพื่อให้เป็นไปตาม มาตรฐานเว็บไซต์ภาครัฐ ver.3 จนครบถ้วน

ภาคผนวก ฉ

ฉ. <u>รายงาน OVAL (Open Vulnerability and Assessment Language) สำหรับ Linux</u>

ค่าเป้าหมาย : OS ของเว็บไซต์ “ไม่มีช่องโหว่” ที่ยังไม่ได้แก้ไข (#X = 0)

ฉ1 OS ของเว็บไซต์ “ไม่มีช่องโหว่” ที่ยังไม่ได้แก้ไข (#X = 0)

ผู้ดูแลเว็บไซต์ ทุกๆ OS “ต้องปรับปรุง อัพเดต” OS และส่วนประกอบโปรแกรมต่างๆ ตามที่ผู้ผลิต OS แนะนำ อย่างสม่ำเสมอเพื่อไม่ให้มีช่องโหว่

สำหรับ OS ที่เป็น Linux ให้ทำรายงาน OVAL ซึ่งแสดงรายการแก้ไขช่องโหว่ ตาม NIST NVD CVE ใช้เปรียบเทียบกับ CVE ตามรายงาน Nessus

1. Debian สร้างรายงาน OVAL ตามคำแนะนำ
   https://sysadmin.psu.ac.th/2024/01/02/debian-oval/
   ไฟล์สำหรับตรวจสอบ Debian OVAL ล่าสุดอยู่ที่ลิงก์
   https://www.debian.org/security/oval/
2. Ubuntu สร้างรายงาน OVAL ตามคำแนะนำ
   https://sysadmin.psu.ac.th/2023/02/14/ubuntu-oval/
   ไฟล์สำหรับตรวจสอบ Ubuntu OVAL ให้ใช้แบบ(Type) CVE ตามรุ่นของ OS ล่าสุด อยู่ที่ลิงก์ https://security-metadata.canonical.com/oval/
3. Windows และ OS อื่นๆ ที่ไม่มีรายงาน OVAL แนะนำให้ใช้ CIS Benchmark
   https://www.cisecurity.org/cis-benchmarks