ສາທາລະນະລັດ ປະຊາທິປະໄຕ ປະຊາຊົນລາວ
ສັນຕິພາບ ເອກະລາດ ປະຊາທິປະໄຕ ເອກະພາບ ວັດທະນະຖາວອນ

ກະຊວງໄປສະນີ, ໂທລະຄົມມະນາຄົມ ແລະ ການສື່ສານ ເລກທີ 2088 /ປທສ

ນະຄອນຫຼວງວຽງຈັນ, ວັນທີ 16 ສິງຫາ 2019

ຄຳແນະນຳ

ກ່ຽວກັບ ການສ້າງ, ພັດທະນາ ແລະ ຄຸ້ມຄອງເວັບໄຊ ໃຫ້ມີຄວາມປອດໄພ

- ອີງຕາມ ກົດໝາຍວ່າດ້ວຍ ການຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳທາງລະບົບຄອມພິວເຕີ, ສະບັບເລກທີ 61/ສພຊ, ລົງວັນທີ 15 ກໍລະກົດ 2015;
- ອີງຕາມ ກົດໝາຍວ່າດ້ວຍ ການປົກປ້ອງຂໍ້ມູນເອເລັກໂຕຣນິກ, ສະບັບເລກທີ 25/ສພຊ, ລົງວັນທີ 12 ພຶດສະພາ 2017;
- ອີງຕາມ ດຳລັດຂອງນາຍົກລັດຖະມົນຕີ ສະບັບເລກທີ 22/ນຍ, ລົງວັນທີ 16 ມັງກອນ 2017 ວ່າດ້ວຍ ການຈັດຕັ້ງ ແລະ ເຄື່ອນໄຫວ ຂອງ ກະຊວງໄປສະນີ, ໂທລະຄົມມະນາຄົມ ແລະ ການສື່ສານ.

ລັດຖະມົນຕີ ອອກຄຳແນະນຳ:

ພາກທີ I
ບົດບັນຍັດທົ່ວໄປ

I. ຈຸດປະສົງ

ຄຳແນະນຳສະບັບນີ້ ມີຈຸດປະສົງແນະນຳ ສຳລັບບຸກຄົນ, ນິຕິບຸກຄົນ ຫຼື ການຈັດຕັ້ງ ທີ່ສ້າງເວັບໄຊ, ປັບປຸງ, ພັດທະນາ ແລະ ຄຸ້ມຄອງການບໍລິການຮັບຝາກເວັບໄຊ ເພື່ອຫຼຸດຜ່ອນຄວາມສ່ຽງເວັບໄຊຖືກໂຈມຕີ, ຖືກແຮກ, ເວັບເຊີເວີໃຫ້ບໍລິການຢຸດສະງັກ ແລະ ຖານຂໍ້ມູນທີ່ສຳຄັນຮົ່ວໄຫຼ ຮັບປະກັນໃຫ້ແກ່ການສະໜອງຂໍ້ມູນ, ການເຂົ້ານຳໃຊ້ຂໍ້ມູນ-ຂ່າວສານ ແລະ ການໃຫ້ບໍລິການຂໍ້ມູນ-ຂ່າວສານ ໃຫ້ແກ່ສັງຄົມ ແນໃສ່ໃຫ້ມີຄວາມສະດວກວ່ອງໄວ ແລະ ປອດໄພ.

II. ອະທິບາຍຄຳສັບ

1. **ໜ້າເວັບ (Web Page)** ໝາຍເຖິງ ກະດານຂ່າວເອເລັກໂຕຣນິກໃນຮູບແບບສັນຍາລັກ, ຕົວເລກ, ຕົວໜັງສື, ຮູບພາບ, ວິດີໂອ, ສຽງ ແລະ ຮູບແບບອື່ນ ຜ່ານອິນເຕີເນັດ;
2. **ເວັບໄຊ (Website)** ໝາຍເຖິງ ລະບົບຂໍ້ມູນ ຂ່າວສານ ທີ່ສ້າງຂຶ້ນເປັນໜຶ່ງ ຫຼື ຫຼາຍໜ້າເວັບ;
3. **ທີ່ຢູ່ເວັບໄຊ (Universal Resource Locator: URL)** ໝາຍເຖິງ ຕົວຊີ້ບອກທີ່ຢູ່ໃນອິນເຕີເນັດ ຊຶ່ງປະກອບດ້ວຍ ຊື່ໂປໂຕຄອລ ທີ່ໃຊ້ໃນການເຂົ້າເຖິງຂໍ້ມູນ (ເຊັ່ນ: https://) ແລະ ລະຫັດຊື່ອິນເຕີເນັດ (ເຊັ່ນ: www.laocert.gov.la) ທີ່ໄດ້ລະບຸໄວ້ກັບເວັບເຊີເວີ;
4. **ເວີວາຍເວັບ (www)** ໝາຍເຖິງ ກຸ່ມຂອງເວັບໄຊ ຫຼື ເຄື່ອງຄອມພິວເຕີ ທີ່ມີຂໍ້ມູນ ພ້ອມໃຫ້ຜູ້ໃຊ້ບໍລິການຄົ້ນຫາຂໍ້ມູນ ຜ່ານໂປໂຕຄອລ https;

5. **ເວັບເຊີເວີ (Web server)** ໝາຍເຖິງ ເຄື່ອງຄອມພິວເຕີທີ່ເຮັດໜ້າທີ່ເປັນເຄື່ອງບໍລິການເຊີເວີ ພ້ອມກັບ ໂປຣແກຣມ ທີ່ໃຫ້ບໍລິການຂໍ້ມູນເວັບໄຊຜ່ານເຄືອຂ່າຍ www;
6. **ຊ໋ອບແວໂປຣແກຣມທີ່ໃຫ້ບໍລິການເວັບໄຊ (Web Server Software)** ໝາຍເຖິງ ໂປຣແກຣມທີ່ຕິດຕັ້ງ ເທິງເຄື່ອງບໍລິການເຊີເວີ ເພື່ອເຮັດໃຫ້ເຄື່ອງບໍລິການສາມາດໃຫ້ບໍລິການເວັບໄຊໄດ້ ເຊັ່ນ: ໂປຣແກຣມ Apache ແລະ ໂປຣແກຣມ Internet Information Service (IIS) for Windows Server ເປັນຕົ້ນ;
7. **ໂປຣແກຣມຄົ້ນຫາເວັບໄຊ (Web Browser)** ໝາຍເຖິງ ໂປຣແກຣມທີ່ໃຊ້ເອີ້ນຂໍ້ມູນເວັບໄຊ ຈາກເຄື່ອງ ບໍລິການເວັບຜ່ານເຄືອຂ່າຍ www;
8. **ໂປຣແກຣມປະຍຸກເທິງເວັບໄຊ (Web Application)** ໝາຍເຖິງ ໂປຣແກຣມປະຍຸກທີ່ຖືກພັດທະນາຂຶ້ນ ສຳລັບການເອີ້ນໃຊ້ງານ ແລະ ເຂົ້າເຖິງໄດ້ໂດຍໂປຣແກຣມຄົ້ນຫາເວັບໄຊ ຜ່ານເຄືອຂ່າຍຄອມພິວເຕີ ເຊັ່ນ: ເຄືອຂ່າຍອິນເຕີເນັດ ຫຼື ເຄືອຂ່າຍອິນທາເນັດ ເປັນຕົ້ນ;
9. **ລະບົບບໍລິຫານຈັດການເວັບໄຊ (Content Management System: CMS)** ໝາຍເຖິງ ໂປຣແກຣມ ທີ່ໃຊ້ໃນການບໍລິຫານຈັດການ ແລະ ຄຸ້ມຄອງ ເວັບໄຊ ຜ່ານຈຸດເຊື່ອມຕໍ່ປະສານ (Interface) ຊຶ່ງຊ່ວຍໃຫ້ ງ່າຍໃນການບໍລິຫານຈັດການ ແລະ ຄຸ້ມຄອງໜ້າເວັບ ແລະ ປັບປຸງ ຄ່າຕິດຕັ້ງຕ່າງໆທີ່ກ່ຽວຂ້ອງ.
10. **ການເຂົ້າລະຫັດຂໍ້ມູນສື່ສານເທິງເວັບໄຊ (SSL/TLS)** ຫຍໍ້ມາຈາກ Secure Socket Layer ຊຶ່ງປະຈຸບັນ ໄດ້ພັດທະນາຂຶ້ນມາເປັນ TLS (Transport Layer Security) ໝາຍເຖິງ ເທັກໂນໂລຊີການເຂົ້າລະຫັດຂໍ້ ມູນ ເພື່ອຄວາມປອດໄພໃນການສື່ສານ ຫຼື ສົ່ງຂໍ້ມູນເທິງເຄືອຂ່າຍອິນເຕີເນັດ ລະຫວ່າງ ເຄື່ອງເຊີເວີ ກັບ ໂປຣແກຣມຄົ້ນຫາໜ້າເວັບ (Web Browser) ຫຼື ໂປຣແກຣມປະຍຸກ (Application) ທີ່ໃຊ້ງານ.

ພາກທີ II
ການສ້າງ ແລະ ຄຸ້ມຄອງເວັບໄຊໃຫ້ມີຄວາມປອດໄພ

III. ການວາງແຜນສ້າງ ແລະ ບໍລິຫານຈັດການເວັບໄຊໃຫ້ມີຄວາມປອດໄພ

1. ການວາງແຜນດ້ານຄວາມປອດໄພຂອງເວັບໄຊ

ການວາງແຜນສ້າງເວັບໄຊໃຫ້ມີຄວາມປອດໄພ ປະກອບມີ 3 ຂັ້ນຕອນ ດັ່ງນີ້:

1.1. ການວາງແຜນສ້າງເວັບໄຊ

ການວາງແຜນສ້າງເວັບໄຊ ຄວນເລືອກໃຊ້ໂປຣແກຣມປະຍຸກ ແລະ ເຄື່ອງມືສຳລັບການພັດທະນາເວັບໄຊ ໃຫ້ເໝາະສົມ, ກວດສອບຄຸນສົມບັດຂອງເວັບເຊີເວີ ລວມໄປເຖິງການເກັບຮັກສາຂໍ້ມູນເທິງເວັບໄຊ ແລະ ນະໂຍ ບາຍກ່ຽວກັບການຮັກສາຄວາມປອດໄພ ເພື່ອຕອບສະໜອງຕາມຈຸດປະສົງໃນການສ້າງເວັບໄຊ. (ລະອຽດເຂົ້າເບິ່ງ ເອກະສານຄັດຕິດ ຂໍ້ທີ່ 1 ຕາມລິ້ງ URL).

1.2. ການຈັດສັນຄວາມສ່ຽງໄພຄຸກຄາມ

ຜູ້ຄຸ້ມຄອງເວັບເຊີເວີ ຄວນຈັດສັນລາຍການຊັບສົມຂອງເວັບໄຊ ເຊັ່ນ: ຈຳນວນເວັບເຊີເວີ, ໂປຣແກຣມ ປະຍຸກເທິງເວັບໄຊ ແລະ ຂໍ້ມູນເທິງເວັບໄຊ ຫຼື ໜ້າເວັບທີ່ກ່ຽວຂ້ອງທັງໝົດ ລວມເຖິງມູນຄ່າເສຍຫາຍທີ່ອາດເກີດ ຂຶ້ນກັບເວັບໄຊ ເພື່ອນຳໄປເປັນຂໍ້ມູນໃນການຈັດລຳດັບຄວາມສ່ຽງຂອງໄພຄຸກຄາມ. (ລະອຽດເຂົ້າເບິ່ງເອກະສານຄັດ ຕິດ ຂໍ້ທີ່ 2 ຕາມລິ້ງ URL).

1.3. ການຈັດລຳດັບຄວາມສ່ຽງຂອງໄພຄຸກຄາມ

ຜູ້ຄຸ້ມຄອງເວັບເຊີເວີ ຄວນຈັດລຳດັບຄວາມສ່ຽງຂອງໄພຄຸກຄາມ ເພື່ອປ້ອງກັນເວັບໄຊຖືກໂຈມຕີ, ຖືກ ແຮັກ, ລະບົບເວັບເຊີເວີໃຫ້ບໍລິການຢຸດສະງັກ ແລະ ຫຼຸດຜ່ອນຄວາມຫຍຸ້ງຍາກໃນການຈັດສັນບຸກຄະລາກອນຄຸ້ມ

ຄອງເວັບເຊີເວີ ລວມໄປເຖິງການເລືອກນຳໃຊ້ເຕັກໂນໂລຊີ, ການກຳນົດມາດຕະຖານຄວາມປອດໄພທີ່ເໝາະສົມ ກັບໄພຄຸກຄາມແຕ່ລະປະເພດ. (ລະອຽດເຂົ້າເບິ່ງເອກະສານຄັດຕິດ ຂໍ້ທີ 3 ຕາມລິ້ງ URL).

2. ການຈົດທະບຽນລະຫັດຊື່ອິນເຕີເນັດ

ການຈົດທະບຽນລະຫັດຊື່ອິນເຕີເນັດ ຄວນປະຕິບັດ ດັ່ງນີ້:

2.1. ການຈົດທະບຽນລະຫັດຊື່ອິນເຕີເນັດຂອງ ສປປ ລາວ ".la"

ການຈົດທະບຽນລະຫັດຊື່ອິນເຕີເນັດ ຕ້ອງໄດ້ປະຕິບັດຕາມຂັ້ນຕອນ ແລະ ວິທີການຈົດທະບຽນລະຫັດຊື່ ອິນເຕີເນັດ ຕາມດຳລັດວ່າດ້ວຍ ການຄຸ້ມຄອງ ແລະ ການນຳໃຊ້ອິນເຕີເນັດ ລະຫັດຊື່ອິນເຕີເນັດ ຂອງ ສປປ ລາວ ສະບັບເລກທີ 164/ລບ, ລົງວັນທີ 23 ມີນາ 2012 (ລະອຽດເຂົ້າເບິ່ງເອກະສານຄັດຕິດ ຂໍ້ທີ 4 ຕາມລິ້ງ URL).

2.2. ການຕັ້ງຄ່າລະຫັດຜ່ານຄວາມປອດໄພບັນຊີລະຫັດຊື່ອິນເຕີເນັດ

ການຕັ້ງຄ່າລະຫັດຜ່ານຄວາມປອດໄພ ຄວນກຳນົດຄ່າລະຫັດຜ່ານໃນການປັບປຸງແກ້ໄຂຂໍ້ມູນການຕັ້ງຄ່າ ລະຫັດຊື່ອິນເຕີເນັດໃຫ້ຊັບຊ້ອນຄາດເດົາໄດ້ຍາກ ເຊັ່ນ: ຕົວເລກ, ຕົວອັກສອນ ໃຫຍ່-ນ້ອຍ, ສັນຍາລັກ ຫຼື ເຄື່ອງ ໝາຍ ເປັນຕົ້ນ # % $ @) ລະບຸຄວາມຍາວຂັ້ນຕ່ຳຂອງລະຫັດຜ່ານຢ່າງນ້ອຍ 12 ຕົວອັກສອນຂຶ້ນໄປ, ບໍ່ຄວນ ໃຊ້ຊ້ຳກັບອີເມວ ຫຼື ບັນຊີທະນາຄານ ແລະ ຈຳກັດອາຍຸການໃຊ້ງານ ເປັນຕົ້ນ ເພື່ອປ້ອງກັນການເຈາະຂໍ້ມູນ.

2.3. ການຢືນຢັນການປ່ຽນແປງຂໍ້ມູນການລົງທະບຽນ

ການປ່ຽນແປງຂໍ້ມູນການລົງທະບຽນລະຫັດຊື່ອິນເຕີເນັດທຸກຄັ້ງ ຜູ້ໃຫ້ບໍລິການລະຫັດຊື່ອິນເຕີເນັດ ຕ້ອງມີ ການແນະນຳຂັ້ນຕອນການປ່ຽນແປງຂໍ້ມູນ ແລະ ມີການແຈ້ງເຕືອນ ພ້ອມທັງມີການຢືນຢັນຕົວຕົນ ເພື່ອປ້ອງກັນບໍ່ ໃຫ້ຜູ້ປະສົງຮ້າຍເຂົ້າມາປ່ຽນແປງຂໍ້ມູນ.

3. ການເລືອກຜູ້ໃຫ້ບໍລິການຮັບຝາກເວັບໄຊ

ການເລືອກຜູ້ໃຫ້ບໍລິການຮັບຝາກເວັບໄຊ ເພື່ອຮັບປະກັນໃນການຕິດຕັ້ງ, ຕັ້ງຄ່າ ແລະ ປັບປຸງເວັບໄຊ ບໍ່ໃຫ້ ເກີດຊ່ອງໂຫວ່ ທີ່ອາດສົ່ງຜົນກະທົບຕໍ່ລະບົບປະຕິບັດການ, ໂປຣແກຣມປະຍຸກທີ່ໃຫ້ບໍລິການເວັບໄຊ ຫຼື ລະບົບ ບໍລິຫານຈັດການເວັບໄຊ ຄວນພິຈາລະນາເລືອກຜູ້ໃຫ້ບໍລິການຮັບຝາກເວັບໄຊ ຕາມເງື່ອນໄຂ ດັ່ງນີ້:

3.1. ຮູບແບບການໃຫ້ບໍລິການຮັບຝາກເວັບໄຊ

ກ. ຮູບແບບການຮັບຝາກເວັບໄຊຮ່ວມກັນ (Shared Hosting) ຈະມີຄ່າໃຊ້ຈ່າຍຕ່ຳ ແຕ່ບໍ່ມີການແບ່ງ ແຍກສິດທິການເຂົ້າເຖິງລະຫວ່າງໂປຣແກຣມປະຍຸກເທິງເວັບໄຊຂອງຜູ້ໃຊ້ບໍລິການ.

ຂ. ຮູບແບບການຮັບຝາກເວັບໄຊແບບຈຳລອງ (VPS Hosting) ສາມາດບໍລິຫານຈັດການໄດ້ງ່າຍ, ຕິດ ຕັ້ງໂປຣແກຣມປະຍຸກ ແລະ ປັບຕັ້ງຄ່າຕ່ຳນວນໄດ້ຕາມຄວາມຕ້ອງການ ພ້ອມທັງຮັບປະກັນໃນກໍລະນີເວັບເຊີເວີໃດ ໜຶ່ງເສຍຫາຍ ກໍ່ຈະບໍ່ສົ່ງຜົນກະທົບກັບເວັບເຊີເວີອື່ນ.

ຄ. ຮູບແບບການຮັບຝາກເວັບໄຊແບບແຍກເວັບເຊີເວີສະເພາະ (Dedicated Server) ຈະມີຄ່າໃຊ້ຈ່າຍສູງ ແຕ່ກໍ່ຊ່ວຍຍົກລະດັບການປ້ອງກັນຄວາມສ່ຽງຈາກການຖືກໂຈມຕີຜ່ານຊ່ອງໂຫວ່ຂອງເວັບໄຊອື່ນໄດ້.

3.2. ການຈັດການບັນຫາຊ່ອງໂຫວ່

ຜູ້ໃຫ້ບໍລິການຮັບຝາກເວັບໄຊ ຄວນມີນະໂຍບາຍດ້ານຄວາມປອດໄພຢ່າງຊັດເຈນ ໃນການປ້ອງກັນຄວາມ ເສຍຫາຍທີ່ເກີດຈາກຊ່ອງໂຫວ່ ຫຼື ປ້ອງກັນຄວາມເສຍຫາຍໄດ້.

3.3. ການໂອນຍ້າຍຟາຍຂໍ້ມູນ (Remote File Transfer)

ການໂອນຍ້າຍຟາຍຂໍ້ມູນ ລະຫວ່າງເຄື່ອງຂອງຜູ້ໃຊ້ບໍລິການ ແລະ ຜູ້ໃຫ້ບໍລິການຮັບຝາກເວັບໄຊ ຄວນມີ ການໃຫ້ບໍລິການໂອນຍ້າຍຂໍ້ມູນທາງໄກ Secure File Transfer Protocol (SFTP) ທີ່ມີການເຂົ້າລະຫັດ ໃນ ການໂອນຍ້າຍຟາຍຂໍ້ມູນໃຫ້ມີຄວາມປອດໄພ.

3.4. ການສື່ສານປອດໄພສຳລັບເວັບໄຊ (SSL/TLS)

ຄວນກວດສອບວ່າຜູ້ໃຫ້ບໍລິການຮັບຝາກເວັບໄຊ ມີການໃຫ້ບໍລິການ ການສື່ສານປອດໄພສຳລັບເວັບໄຊ SSL/TLS ຫຼື ບໍ່, ຖ້າຫາກຜູ້ໃຫ້ບໍລິການຮັບຝາກເວັບໄຊ ບໍ່ມີການໃຫ້ບໍລິການດັ່ງກ່າວ ຜູ້ໃຊ້ບໍລິການ ຈຳເປັນຕ້ອງ ໄດ້ຂໍໃບຮັບຮອງການສື່ສານປອດໄພແບບເອເລັກໂຕຣນິກ (SSL Certificate) ຈາກຜູ້ໃຫ້ບໍລິການອື່ນ.

3.5. ການສຳຮອງຂໍ້ມູນ ແລະ ການຮັກສາເວັບເຊີເວີ

ຜູ້ໃຫ້ບໍລິການຮັບຝາກເວັບໄຊ ຄວນມີການສຳຮອງຂໍ້ມູນເທິງເວັບເຊີເວີ ທີ່ຢູ່ໃນການຄຸ້ມຄອງຂອງຕົນຢ່າງສະໝ່ຳສະເໝີ ໂດຍອີງຕາມ ຂໍ້ຕົກລົງວ່າດ້ວຍ ການອະນຸຍາດດຳເນີນກິດຈະການສູນກາງຂໍ້ມູນຂ່າວສານຜ່ານອິນເຕີເນັດ ສະບັບເລກທີ 590/ປທສ, ລົງວັນທີ 18 ພຶດສະພາ 2016 (ລະອຽດເຂົ້າເບິ່ງເອກະສານຄັດຕິດ ຂໍ້ທີ 5 ຕາມລິ້ງ URL).

3.6. ການຕິດຕໍ່ສື່ສານຜູ້ໃຫ້ບໍລິການຮັບຝາກເວັບໄຊເມື່ອເກີດເຫດສຸກເສີນ

ຜູ້ໃຫ້ບໍລິການຮັບຝາກເວັບໄຊ ຄວນມີຊ່ອງທາງໃນການຕິດຕໍ່ສື່ສານສະເພາະ ຫຼື ມີໜ່ວຍງານຮັບຜິດຊອບປະສານງານ ໃນກໍລະນີທີ່ຜູ້ໃຊ້ບໍລິການຕ້ອງການຕິດຕໍ່ສື່ສານ ເພື່ອຂໍຄວາມຊ່ວຍເຫຼືອ ແລະ ແກ້ໄຂເຫດສຸກເສີນທີ່ເກີດຂຶ້ນກັບເວັບໄຊຂອງຕົນ.

4. ການເລືອກລະບົບບໍລິຫານຈັດການເວັບໄຊ (Content Management System: CMS)

ການເລືອກລະບົບບໍລິຫານຈັດການເວັບໄຊໃຫ້ມີຄວາມປອດໄພ ຄວນປະຕິບັດ ດັ່ງນີ້:

4.1. ການເລືອກຄຸນສົມບັດທີ່ກ່ຽວຂ້ອງກັບການຮັກສາຄວາມປອດໄພ

ຜູ້ພັດທະນາລະບົບບໍລິຫານຈັດການເວັບໄຊ ຄວນມີເອກະສານແນະນຳການຕິດຕັ້ງ, ການຕັ້ງຄ່າຄວາມປອດໄພ (Security Best Practice) ແລະ ມີໂປຣແກຣມເສີມ (Plug-in) ຕາມຄວາມຕ້ອງການຂອງຜູ້ໃຫ້ບໍລິການຮັບຝາກເວັບໄຊ ແລະ ຜູ້ໃຊ້ບໍລິການ. (ລະອຽດເຂົ້າເບິ່ງເອກະສານຄັດຕິດ ຂໍ້ທີ 6 ຕາມລິ້ງ URL).

4.2. ການເລືອກຜູ້ສ້າງລະບົບບໍລິຫານຈັດການເວັບໄຊ

ຜູ້ສ້າງ ແລະ ພັດທະນາເວັບໄຊ ຄວນເລືອກຜູ້ສ້າງລະບົບບໍລິຫານຈັດການເວັບໄຊ ທີ່ມີຄຸນນະພາບ, ມີການປັບປຸງແກ້ໄຂຂໍ້ບົກຜ່ອງ ແລະ ຊ່ອງໂຫວ່ ຢ່າງເປັນປົກກະຕິ.

IV. ການຄຸ້ມຄອງເວັບໄຊໃຫ້ມີຄວາມປອດໄພ

1. ການຕັ້ງຄ່າໂປຣແກຣມສຳລັບເວັບເຊີເວີ

ການຕັ້ງຄ່າໂປຣແກຣມສຳລັບເວັບເຊີເວີໃຫ້ມີຄວາມປອດໄພ ຄວນປະຕິບັດ ດັ່ງນີ້:

1.1. ອັບເດດໂປຣແກຣມຕ່າງໆ ຢູ່ໃນເວັບເຊີເວີ ຢ່າງສະໝ່ຳສະເໝີ;

1.2. ກຳນົດໃຫ້ການແຈ້ງເຕືອນ ຫຼື ການສະແດງຂໍ້ຄວາມຜິດພາດຂອງລະບົບ (Error Message) ບໍ່ໃຫ້ປະກົດອອກຢູ່ເທິງເວັບໄຊ ເນື່ອງຈາກວ່າຜູ້ປະສົງຮ້າຍອາດຈະນຳໃຊ້ຂໍ້ຄວາມແຈ້ງເຕືອນດັ່ງກ່າວ ໄປເປັນຂໍ້ມູນພື້ນຖານໃນການໂຈມຕີລະບົບເວັບເຊີເວີ;

1.3. ຈັດກຸ່ມ ຫຼື ໝວດເກັບຟາຍຂໍ້ມູນ, ໜ້າເວັບ, ລະບົບປະຕິບັດການ, ໂປຣແກຣມສຳລັບ ເວັບເຊີເວີ ແລະ ໂປຣແກຣມອື່ນໆ ໂດຍກຳນົດສິດໃນການເຂົ້າເຖິງກຸ່ມ ຫຼື ໝວດຟາຍຂໍ້ມູນ ເພື່ອສະດວກໃນການຄົ້ນຫາ ແລະ ກວດກາຄວາມປອດໄພ;

1.4. ກວດສອບຄືນ ແລະ ລຶບ ໂປຣແກຣມ, ຟາຍຂໍ້ມູນ, ບັນຊີຜູ້ໃຊ້ ທີ່ບໍ່ໄດ້ໃຊ້ງານ ແລະ ບັນຊີທີ່ມີການໃຊ້ງານລະຫວ່າງການຕິດຕັ້ງຂອງເວັບເຊີເວີທັງໝົດ;

1.5. ກວດສອບ ແລະ ປ່ຽນແປງຄ່າເລີ່ມຕົ້ນຂອງ ຊື່ກຸ່ມ ຫຼື ໝວດເກັບຟາຍຂໍ້ມູນ, ຊື່ຟາຍຂໍ້ມູນ, ທີ່ຕັ້ງຟາຍຂໍ້ມູນ ແລະ ລະຫັດຜ່ານ ທີ່ມາພ້ອມກັບເວັບເຊີເວີ;

1.6. ກຳນົດ ເລກໝາຍອິນເຕີເນັດ ຫຼື ລະຫັດຊື່ອິນເຕີເນັດສະເພາະ ໃຫ້ແກ່ຜູ້ໃຊ້ບໍລິການສາມາດເຂົ້າເຖິງເວັບເຊີເວີ;

1.7. ປິດການເຂົ້າເຖິງລະບົບຄວບຄຸມເວັບເຊີເວີທາງໄກທີ່ບໍ່ຈຳເປັນ ເຊັ່ນ: Remote Desktop, VNC, SSH, Telnet ແລະ ອື່ນໆ.

2. ການຕັ້ງຄ່າລະບົບບໍລິຫານຈັດການເວັບໄຊ

ການຕັ້ງຄ່າລະບົບບໍລິຫານຈັດການເວັບໄຊ ໃຫ້ມີຄວາມປອດໄພ ຄວນປະຕິບັດ ດັ່ງນີ້:

2.1. ຕ້ອງກຳນົດສິດການໃຊ້ງານ (Permission) ແລະ ຄວບຄຸມການເຂົ້າເຖິງ (Access Control) ຟາຍຂໍ້ມູນຕ່າງໆ ໃຫ້ເໝາະສົມ;

2.2. ຄວນລຶບຟາຍຂໍ້ມູນ ຫຼື ຍົກເລີກການຕິດຕັ້ງໂປຣແກຣມເສີມ ທີ່ບໍ່ຈຳເປັນ ແລະ ບໍ່ໄດ້ໃຊ້ງານ;

2.3. ຕິດຕາມ ແລະ ປັບປຸງ ລະບົບບໍລິຫານຈັດການເວັບໄຊຢ່າງເປັນປະຈຳ;

2.4. ດາວໂຫຼດຟາຍຂໍ້ມູນ ແລະ ປັບປຸງລະບົບບໍລິຫານຈັດການຈາກເວັບໄຊຜູ້ຜັດທະນາເທົ່ານັ້ນ;

2.5. ລຶບ, ປ່ຽນຊື່ ແລະ ລະຫັດຜ່ານບັນຊີຜູ້ໃຊ້ ທີ່ມາກັບການຕິດຕັ້ງລະບົບບໍລິຫານຈັດການເວັບໄຊໃນເບື້ອງຕົ້ນ;

2.6. ປ່ຽນຕາຕະລາງ Table Prefix ຂອງຖານຂໍ້ມູນທີ່ມາໃນລະຫວ່າງການຕິດຕັ້ງລະບົບບໍລິຫານຈັດການເວັບໄຊ. ຕົວຢ່າງ: ຢູ່ໃນລະບົບບໍລິຫານຈັດການເວັບໄຊ WordPress ຈະມີການໃຊ້ໃນຕາຕະລາງ Table Prefix ທີ່ຂຶ້ນຕົ້ນດ້ວຍຊື່ wp_xxx ໃຫ້ປ່ຽນເປັນຊື່ອື່ນ ເພື່ອບໍ່ໃຫ້ຜູ້ປະສົງຮ້າຍສາມາດຮູ້ເຖິງໂຄງສ້າງ ແລະ ທຳລາຍຖານຂໍ້ມູນ.

3. ການຕັ້ງຄ່າລະບົບຖານຂໍ້ມູນ

ການຕັ້ງຄ່າລະບົບຖານຂໍ້ມູນໃຫ້ມີຄວາມປອດໄພ ຄວນປະຕິບັດ ດັ່ງນີ້:

3.1. ຕັ້ງຄ່າ ອະນຸຍາດໃຫ້ສະເພາະແຕ່ໂປຣແກຣມປະຍຸກ ແລະ ເວັບເຊີເວີ ທີ່ກ່ຽວຂ້ອງເຂົ້າເຖິງລະບົບຖານຂໍ້ມູນໄດ້ເທົ່ານັ້ນ;

3.2. ຕັ້ງຄ່າຄວາມປອດໄພຂອງຖານຂໍ້ມູນ ໃນການຄວບຄຸມການເຂົ້າເຖິງລະບົບຖານຂໍ້ມູນ ເພື່ອບໍ່ໃຫ້ຜູ້ໃຊ້ທົ່ວໄປເຂົ້າເຖິງຖານຂໍ້ມູນ ເຊັ່ນ: ລະບົບປ້ອງກັນ (Firewall) ເຫຼົ່ານີ້ເປັນຕົ້ນ;

3.3. ກວດສອບ ແລະ ປິດການບໍລິການໃນລະບົບຖານຂໍ້ມູນ ທີ່ບໍ່ຈຳເປັນ ຫຼື ບໍ່ໄດ້ໃຊ້ງານ;

3.4. ກວດສອບ ແລະ ລຶບ ບັນຊີຜູ້ໃຊ້ ທີ່ບໍ່ໄດ້ມີການໃຊ້ງານ ອອກຈາກລະບົບຖານຂໍ້ມູນຕາມໄລຍະເວລາທີ່ກຳນົດໄວ້;

3.5. ປິດ ຫຼື ປ່ຽນລະຫັດຜ່ານບັນຊີຜູ້ໃຊ້ ທີ່ມາພ້ອມກັບການຕິດຕັ້ງລະບົບຖານຂໍ້ມູນເບື້ອງຕົ້ນ;

3.6. ກຳນົດຄ່າຕິດຕັ້ງລະບົບຖານຂໍ້ມູນ ເພື່ອບໍ່ອະນຸຍາດໃຫ້ໃຊ້ງານສຳລັບບັນຊີທີ່ບໍ່ມີລະຫັດຜ່ານ;

3.7. ກວດສອບ ແລະ ລຶບຟາຍຊົ່ວຄາວ (Temporary File) ທີ່ຖືກສ້າງຂຶ້ນໃນລະຫວ່າງການຕິດຕັ້ງລະບົບຖານຂໍ້ມູນ;

3.8. ເພີ່ມປະສິດຕິພາບໃຫ້ໂປຣແກຣມລະບົບຖານຂໍ້ມູນມີຄວາມປອດໄພສູງ ຕ້ອງໄດ້ປັບປຸງໂປຣແກຣມດັ່ງກ່າວໃຫ້ໃໝ່ຫຼ້າສຸດສະເໝີ;

3.9. ກຳນົດສິດທິບັນຊີຜູ້ໃຊ້ງານ ແລະ ການຄວບຄຸມການເຂົ້າເຖິງລະບົບຖານຂໍ້ມູນໃຫ້ເໝາະສົມ;

3.10. ລະຫັດຜ່ານທີ່ເກັບໄວ້ໃນລະບົບຖານຂໍ້ມູນ ຕ້ອງເຂົ້າລະຫັດລັບທີ່ຄາດເດົາໄດ້ຍາກ.

4. ການຕັ້ງຄ່າ Server-Side Script Engine

ການຕັ້ງຄ່າ Server-Side Script Engine ໃຫ້ມີຄວາມປອດໄພ ຄວນປະຕິບັດ ດັ່ງນີ້:

4.1. ກຳນົດສິດທິການເຂົ້າເຖິງຟາຍຂໍ້ມູນ, ກຸ່ມ ຫຼື ໝວດຟາຍຂໍ້ມູນ ໃຫ້ຖືກຕ້ອງ;

4.2. ກຳນົດຄ່າຕິດຕັ້ງ Server-Side Script Engine ບໍ່ໃຫ້ສະແດງຂໍ້ມູນເວີຊັ່ນ (Version) ໃນ HTTP Header ເທິງເວັບເຊີເວີ;

4.3. ກຳນົດຄ່າຕິດຕັ້ງ Server-Side Script Engine ບໍ່ໃຫ້ມີການສະແດງລາຍລະອຽດຂໍ້ມູນ ຫຼື ສະແດງຂໍ້ຄວາມຜິດພາດ (Error Message) ແຕ່ຄວນຈະສະແດງຂໍ້ມູນເທົ່າທີ່ຈຳເປັນເທົ່ານັ້ນ;

4.4. ຕ້ອງປັບປຸງ Server-Side Script Engine ໃຫ້ເປັນເວີຊັ່ນ (Version) ໃໝ່ຫຼ້າສຸດ.

5. ການກຳນົດ ແລະ ຮັກສາລະຫັດຜ່ານ

ການກຳນົດ ແລະ ຮັກສາລະຫັດຜ່ານ ໃຫ້ມີຄວາມປອດໄພ ຄວນປະຕິບັດ ດັ່ງນີ້:

5.1. ການຕັ້ງຄ່າລະຫັດຜ່ານ ຄວນໃຫ້ມີລະຫັດທີ່ຊັບຊ້ອນ ແລະ ຄາດເດົາໄດ້ຍາກ ເຊັ່ນ: ຕົວເລກ, ຕົວອັກສອນ (ໃຫຍ່-ນ້ອຍ) ແລະ ສັນຍາລັກ ຫຼື ເຄື່ອງໝາຍ ເປັນຕົ້ນ # % $ @ ຢ່າງໜ້ອຍ 12 ຕົວຂຶ້ນໄປ;

5.2. ຄວນປ່ຽນລະຫັດຜ່ານຢ່າງໜ້ອຍ 3 ເດືອນຕໍ່ຄັ້ງ;

5.3. ບໍ່ເກັບລະຫັດຜ່ານ ທີ່ບໍ່ໄດ້ເຂົ້າລະຫັດລັບເທິງເວັບເຊີເວີ;

5.4. ຫາກຈຳເປັນຕ້ອງເກັບລະຫັດຜ່ານ ຄວນຢູ່ໃນຮູບແບບທີ່ໄດ້ເຂົ້າລະຫັດລັບ ຕາມມາດຕະຖານດ້ານຄວາມປອດໄພກຳນົດໄວ້ (ລະອຽດເຂົ້າເບິ່ງເອກະສານຄັດຕິດ ຂໍ້ທີ 7 ຕາມລິ້ງ URL).

ພາກທີ III
ມາດຕະການປ້ອງກັນການໂຈມຕີເວັບໄຊ

V. ມາດຕະການປ້ອງກັນການໂຈມຕີເວັບໄຊ

1. ການປ້ອງກັນການໂຈມຕີໃນຮູບແບບ SQL Injection

ຜູ້ປະສົງຮ້າຍ ຈະສົ່ງຄຳສັ່ງ SQL ເຂົ້າໄປທາງ Input Form ເທິງໜ້າເວັບ ເຮັດໃຫ້ສາມາດດຳເນີນການຕ່າງໆ ໃນລະບົບຖານຂໍ້ມູນໄດ້ ໂດຍຜ່ານຄຳສັ່ງ SQL ເຊັ່ນ: Insert Update Delete ຫຼື ຄຳສັ່ງປົດລະບົບຖານຂໍ້ມູນ.

ການປ້ອງກັນການໂຈມຕີແບບໃນຮູບແບບ SQL Injection ຄວນປະຕິບັດ ດັ່ງນີ້:

1.1 ແຍກຄຳສັ່ງ ແລະ ຄ່າຄຳນວນ ການປະມວນຜົນອອກຈາກກັນ (ລະອຽດເຂົ້າເບິ່ງເອກະສານຄັດຕິດ ຂໍ້ທີ 8 ຕາມລິ້ງ URL);

1.2 ກວດສອບຂໍ້ມູນທີ່ໄດ້ຮັບ ກ່ອນຈະປະມວນຜົນຕົວຈິງເປັນວິທີການທີ່ສຳຄັນ ແລະ ຈຳເປັນ ຕໍ່ຂະບວນການພັດທະນາເວັບໄຊໃຫ້ມີຄວາມປອດໄພ;

1.3 ຂໍ້ມູນທີ່ຮັບມາຈາກພາຍນອກ ຄວນ Encoding ຫຼື Sanitization ກ່ອນນຳເອົາຄ່າຄຳນວນມາປະມວນຜົນ (ລະອຽດເຂົ້າເບິ່ງເອກະສານຄັດຕິດ ຂໍ້ທີ 9 ຕາມລິ້ງ URL).

2. ການປ້ອງກັນການໂຈມຕີໃນຮູບແບບ Session Hijacking

ການປ້ອງກັນການໂຈມຕີໃນຮູບແບບ Session Hijacking ຄວນປະຕິບັດ ດັ່ງນີ້:

2.1. ເຂົ້າລະຫັດລັບ Session ID ທີ່ມີຂໍ້ມູນການຮັບຮອງຕົວຕົນຂອງຜູ້ໃຊ້ບໍລິການ;

2.2. ກຳນົດ Session Timeout ໃນໄລຍະເວລາທີ່ເໝາະສົມ ເພື່ອປ້ອງກັນການໂຈມຕີຮູບແບບ Session Hijacking;

2.3. ກຳນົດເວລາ ແລະ ຕັ້ງຄ່າ Session ID ທີ່ຄາດເດົາໄດ້ຍາກ ແລະ ບໍ່ຊ້ຳກັນ;

2.4. ກຳນົດການສົ່ງຄ່າ Session ID ທີ່ມີການເຂົ້າລະຫັດລັບ ເຊັ່ນ: ການສົ່ງຂໍ້ມູນຜ່ານໂປໂຕຄອລ HTTPS ເພື່ອປ້ອງກັນການລັດເອົາຂໍ້ມູນ (ລະອຽດເຂົ້າເບິ່ງເອກະສານຄັດຕິດ ຂໍ້ທີ 10 ຕາມລິ້ງ URL).

3. ການປ້ອງກັນການໂຈມຕີໃນຮູບແບບ Cross-Site Scripting

ການປ້ອງກັນການໂຈມຕີໃນຮູບແບບ Cross-Site Scripting ຄວນປະຕິບັດ ດັ່ງນີ້:

3.1. ກວດສອບການປ້ອນຂໍ້ມູນເຂົ້າໃນເວັບໄຊ (Input Validation) ກ່ອນທີ່ຈະສົ່ງມາປະມວນຜົນຕົວຈິງ ຕ້ອງຕັ້ງຄ່າໃຫ້ອະນຸຍາດອັບໂຫຼດ (Upload) ໄດ້ສະເພາະຟາຍທີ່ມີນາມສະກຸນເປັນ .txt, .docx, .xlsx, .pdf ຫຼື ຕາມທີ່ຕ້ອງການເທົ່ານັ້ນ;

3.2. ກວດສອບການຮັບຂໍ້ມູນຊຸດຄຳສັ່ງ (Script) ທີ່ຜິດປົກກະຕິ ເປັນອັນຕະລາຍຕໍ່ເວັບໄຊ ໂດຍທີ່ມີເຄື່ອງໝາຍເປັນສັນຍາລັກພິເສດ ເຊັ່ນ: " < > ? & # " ໃຫ້ເປັນພາສາ HTML Character ກ່ອນ ເຊັ່ນ: ເຄື່ອງໝາຍນ້ອຍກວ່າ "<" ຄວນປັບຄ່າເປັນ "& l t ;" ເປັນຕົ້ນ;

3.3. ກວດສອບການສະແດງຜົນຂອງຂໍ້ມູນ (Output Validation) ເພື່ອປ້ອງກັນການສະແດງຂໍ້ຄວາມຜິດພາດ (Error Message);

3.4. ກຳນົດການຕັ້ງຄ່າ (HTTP Only Cookie flag) ເພື່ອປ້ອງກັນການເຂົ້າເຖິງຄ່າ Cookie ຂອງເວັບໄຊ.

4. ການປ້ອງກັນການໂຈມຕີໃນຮູບແບບ Cross Site Script Forgery (CSRF)

ການປ້ອງກັນການໂຈມຕີໃນຮູບແບບ Cross Site Script Forgery ຄວນປະຕິບັດ ດັ່ງນີ້:

4.1. ກຳນົດການໃຊ້ງານ Unique Token ແລະ/ຫຼື ກວດສອບ Referrer ຮ່ວມກັບການສົ່ງຂໍ້ມູນ ຫຼື ຄຳສັ່ງຜ່ານແບບຟອມ ເພື່ອກວດສອບຂໍ້ມູນແທ້ຈິງທີ່ມາຈາກຜູ້ໃຊ້ງານ;

4.2. ກຳນົດການໃຊ້ Captcha ເພື່ອຢັ້ງຢືນຕົວຕົນຂອງຜູ້ໃຊ້ງານ.

5. ການປ້ອງກັນການໂຈມຕີຈາກການເປີດເຜີຍຂໍ້ມູນລັບ (Sensitive Data Exposure)

ການປ້ອງກັນໂຈມຕີການເປີດເຜີຍຂໍ້ມູນລັບ ຄວນປະຕິບັດ ດັ່ງນີ້:

5.1. ບໍ່ຄວນກຳນົດທີ່ຢູ່ເວັບໄຊທີ່ຄາດເດົາໄດ້ງ່າຍ ສຳລັບການເຂົ້າເຖິງໜ້າເວັບໄຊ ເພື່ອບໍລິຫານຈັດການເວັບໄຊ (Administrator Control Panel Web Page) ເຊັ່ນ: /admin.php ຫຼື /login.php ເປັນຕົ້ນ.

5.2. ອອກແບບ ແລະ ຄວບຄຸມ ບໍ່ໃຫ້ສະແດງຂໍ້ຄວາມແຈ້ງເຕືອນ ຫຼື ຂໍ້ຄວາມຜິດພາດ (Notification or Error Message) ເນື່ອງຈາກວ່າຜູ້ປະສົງຮ້າຍອາດຈະນຳໃຊ້ຂໍ້ຄວາມແຈ້ງເຕືອນດັ່ງກ່າວ ເພື່ອໄປເປັນຂໍ້ມູນພື້ນຖານໃນການໂຈມຕີລະບົບເວັບໄຊ;

5.3. ປິດການໃຊ້ງານ Autocomplete ໃນແບບຟອມສຳຄັນຂອງເວັບໄຊ ເຊັ່ນ: ແບບຟອມການລົງທະບຽນ ຫຼື ແບບຟອມການເຮັດທຸລະກຳທາງການເງິນ ເປັນຕົ້ນ;

6. ການເຂົ້າລະຫັດຂໍ້ມູນສື່ສານເທິງເວັບໄຊ (SSL/TLS)

ຢູ່ໃນໂປໂຕຄອລ SSL/TLS ຄວນເລືອກການເຂົ້າລະຫັດຂໍ້ມູນເທິງເວັບໄຊ ໃຫ້ມີຄວາມປອດໄພດ້ວຍພື້ນຖານທີ່ສຳຄັນ ດັ່ງນີ້:

1) ຢືນຢັນຕົວຕົນຂອງເວັບເຊີເວີ;

2) ຢືນຢັນຕົວຕົນຂອງຜູ້ໃຊ້ບໍລິການ;

3) ເຂົ້າລະຫັດຂໍ້ມູນທີ່ໃຊ້ໃນການ ຮັບ-ສົ່ງ ຂໍ້ມູນເທິງເວັບໄຊ.

7. ການນຳໃຊ້ໃບຮັບຮອງເອເລັກໂຕຣນິກ (Certificate Authentication)

ການນຳໃຊ້ໃບຮັບຮອງເອເລັກໂຕຣນິກ ໃຫ້ປະຕິບັດດັ່ງນີ້:

7.1 ເລືອກເວີຊັ່ນ (Version) SSL/TLS ທີ່ໄດ້ຮັບການປັບປຸງ ແລະ ແກ້ໄຂດ້ານຄວາມປອດໄພຫຼ້າສຸດ;

7.2 ຕິດຕັ້ງໃບຮັບຮອງເອເລັກໂຕຣນິກ ເພື່ອຮັບປະກັນດ້ານຄວາມປອດໄພຂໍ້ມູນເວັບໄຊ;

7.3 ກຳນົດຄ່າຕິດຕັ້ງທີ່ກ່ຽວກັບ SSL/TLS ເພື່ອກວດສອບຄວາມຖືກຕ້ອງຂອງໃບຮັບຮອງເອເລັກໂຕຣນິກ;

7.4 ບຳລຸງຮັກສາໃບຮັບຮອງເອເລັກໂຕຣນິກຄວນປະຕິບັດຄື: ກວດສອບອາຍຸການນຳໃຊ້ຂອງໃບຮັບຮອງເອເລັກໂຕຣນິກເປັນປະຈຳ, ຕໍ່ອາຍຸການນຳໃຊ້ຂອງໃບຮັບຮອງເອເລັກໂຕຣນິກທັນທີ ເມື່ອໃກ້ໝົດອາຍຸ ແລະ ກວດສອບຂໍ້ມູນຜູ້ໃຫ້ບໍລິການ ໃບຮັບຮອງເອເລັກໂຕຣນິກຢູ່ສະເໝີ.

VI. ການກວດກາຕິດຕາມ ແລະ ຮັບມື ກັບໄພຄຸກຄາມເວັບໄຊ

1. ການກວດກາຕິດຕາມ ຄວາມປອດໄພເວັບໄຊ

ການກວດກາຕິດຕາມຄວາມປອດໄພຂອງເວັບໄຊ ຄວນປະຕິບັດ ດັ່ງນີ້:

1.1 ເລືອກໂປຣແກຣມທີ່ໜ້າເຊື່ອຖື ຫຼື ປະຕິບັດຕາມຄຳແນະນຳຈາກ ສູນສະກັດກັ້ນ ແລະ ແກ້ໄຂເຫດສຸກເສີນທາງຄອມພິວເຕີ;

1.2 ອັບເດດໂປຣແກຣມກວດສອບຂໍ້ບົກຜ່ອງໃຫ້ເປັນເວີຊັ່ນຫຼ້າສຸດ ເພື່ອກວດສອບຊ່ອງໂຫວ່ໃໝ່ໆ;

1.3 ສຳຮອງຂໍ້ມູນທຸກຄັ້ງ ກ່ອນນຳໃຊ້ໂປຣແກຣມກວດສອບຂໍ້ບົກຜ່ອງ ເພື່ອປ້ອງກັນຜົນກະທົບຕໍ່ເວັບເຊີເວີ;

1.4 ໃຊ້ໂປຣແກຣມຫຼາຍກວ່າສອງໂປຣແກຣມຂຶ້ນໄປ ໃນການກວດສອບຂໍ້ບົກຜ່ອງ ເພື່ອປຽບທຽບຜົນທີ່ໄດ້ຈາກການກວດສອບເວັບໄຊ (ລະອຽດເຂົ້າເບິ່ງເອກະສານຄັດຕິດ ຂໍ້ທີ 11 ຕາມລິ້ງ URL).

2. ການຮັບມືໄພຄຸກຄາມເວັບໄຊ

ການຮັບມື ແລະ ແກ້ໄຂເຫດສຸກເສີນທີ່ເກີດຂຶ້ນກັບເວັບໄຊ ແບ່ງອອກເປັນ 03 ກໍລະນີ ດັ່ງນີ້:

2.1 ເວັບໄຊຖືກບຸກລຸກ ແລະ ຄວບຄຸມ (Intrusions)

ການຮັບມືໃນເວລາເກີດເຫດກ່ຽວກັບເວັບໄຊຖືກບຸກລຸກ ແລະ ຄວບຄຸມ ຄວນປະຕິບັດ ດັ່ງນີ້:

1) ປິດການເຊື່ອມຕໍ່ຂອງເວັບໄຊ;

2) ສຳເນົາຂໍ້ມູນທີ່ກ່ຽວຂ້ອງກັບການບຸກລຸກ ເພື່ອມາໃຊ້ວິເຄາະເຊັ່ນ: Web Log Sourcecode Database;

3) ກວດສອບຊ່ອງທາງການໂຈມຕີ ແລະ ຊ່ອງໂຫວ່ ທີ່ມີໃນເວັບໄຊ;

4) ສ້າງໜ້າເວັບໄຊແບບ Static ຊົ່ວຄາວ ແລະ ນຳໄປຕິດຕັ້ງເທິງເວັບເຊີເວີໃໝ່ ເພື່ອແຈ້ງສະຖານະການ, ການປິດປັບປຸງເວັບໄຊ ແລະ ໃຫ້ຜູ້ຄຸ້ມຄອງລະບົບດຳເນີນການແກ້ໄຂບັນຫາໃນຂັ້ນຕໍ່ໄປ.

5) ປ່ຽນແປງການຕັ້ງຄ່າເວັບເຊີເວີ ເພື່ອຫຼຸດຄວາມສ່ຽງ ແລະ ປ້ອງກັນບໍ່ໃຫ້ມີຜົນກັບຂໍ້ມູນຕ່າງໆ ທີ່ຢູ່ເທິງເວັບເຊີເວີເກົ່າ;

6) ກູ້ຄືນທຸກໂປຣແກຣມປະຍຸກທີ່ກ່ຽວຂ້ອງກັບຂໍ້ມູນເວັບໄຊ ແລະ ຖານຂໍ້ມູນ ເວັບໄຊກ່ອນໜ້າທີ່ຈະຖືກບຸກລຸກ;

7) ກວດສອບຊ່ອງໂຫວ່ຂອງເວັບໄຊ ກ່ອນໜ້າທີ່ຈະຖືກໂຈມຕີ ເພື່ອແກ້ໄຂຊ່ອງໂຫວ່ຂອງເວັບໄຊ;

8) ບັນທຶກເຫດການ ແລະ ຂັ້ນຕອນການດຳເນີນການ ທີ່ເກີດຂຶ້ນທັງໝົດ ເພື່ອໃຊ້ເປັນຂໍ້ມູນໃນການປ້ອງກັນ ແລະ ການປະສານງານ ເພື່ອແກ້ໄຂຮ່ວມກັບ ສູນສະກັດກັ້ນ ແລະ ແກ້ໄຂເຫດສຸກເສີນທາງຄອມພິວເຕີ.

2.2 ເວັບໄຊຖືກໂຈມຕີໃນຮູບແບບ DoS (Denial of Service) ແລະ DDoS (Distributed Denial of Service)

ໃນກໍລະນີ ເວັບໄຊຖືກໂຈມຕີໃນຮູບແບບ DoS (Denial of Service) ແລະ DDoS (Distributed Denial of Service) ຄວນປະຕິບັດ ດັ່ງນີ້:

1) ປິດການເຊື່ອມຕໍ່ຂອງເວັບໄຊ;

2) ສຳເນົາຂໍ້ມູນທີ່ກ່ຽວຂ້ອງກັບການບຸກລຸກ ເພື່ອມາໃຊ້ວິເຄາະ ເຊັ່ນ: Web Log ຫຼື Firewall Log;

3) ກວດສອບໝາຍເລກໄອພີ ທີ່ໜ້າສົງໄສໃນການສົ່ງຂໍ້ມູນເຂົ້າມາເວັບເຊີເວີແບບຜິດປົກກະຕິ;

4) ປິດກັ້ນການເຂົ້າເຖິງຈາກໝາຍເລກໄອພີດັ່ງກ່າວ ແລະ ແຈ້ງຫາຜູ້ໃຫ້ບໍລິການອິນເຕີເນັດ ເພື່ອຫາມາດຕະການຮອງຮັບໃນກໍລະນີທີ່ອຸປະກອນປ້ອງກັນຂອງໜ່ວຍງານ ບໍ່ສາມາດຮອງຮັບປະລິມານຂໍ້ມູນທີ່ຫຼວງຫຼາຍໄດ້;

5) ບັນທຶກເຫດການ ແລະ ຂັ້ນຕອນການດຳເນີນການ ທີ່ເກີດຂຶ້ນທັງໝົດ ເພື່ອໃຊ້ເປັນຂໍ້ມູນໃນການປ້ອງກັນ ແລະ ສະເໜີໃຫ້ ສູນສະກັດກັ້ນ ແລະ ແກ້ໄຂເຫດສຸກເສີນທາງຄອມພິວເຕີ ເພື່ອດຳເນີນການແກ້ໄຂຊ່ວຍ.

2.3 ລະຫັດຊື່ອິນເຕີເນັດຖືກລັກ (Domain Hijack)

ໃນກໍລະນີລະຫັດຊື່ອິນເຕີເນັດຖືກລັກ ຄວນປະຕິບັດ ດັ່ງນີ້:

1) ເກັບກຳຫຼັກຖານ ທີ່ເກີດຂຶ້ນທັງໝົດ ເຊັ່ນ: ວັນ, ເດືອນ, ປີ ໃນເວລາທີ່ຂໍ້ມູນລະຫັດຊື່ອິນເຕີເນັດຖືກປ່ຽນ;

2) ກວດສອບກັບຜູ້ຈົດທະບຽນລະຫັດຊື່ອິນເຕີເນັດ ໃນການປ່ຽນແປງລະຫັດຊື່ອິນເຕີເນັດ;

3) ແຈ້ງໃຫ້ຜູ້ຈົດທະບຽນລະຫັດຊື່ອິນເຕີເນັດ ຮັບຊາບກ່ຽວກັບການຖືກລັກຂໍ້ມູນລະຫັດຊື່ອິນເຕີເນັດ;

4) ຫຼັງຈາກຮັບສິດທິໃນການບໍລິຫານຈັດການລະຫັດຊື່ອິນເຕີເນັດຄືນມາ ໃຫ້ກວດສອບຂໍ້ມູນທີ່ໃຊ້ໃນການຢືນຢັນຕົວຕົນ ແລະ ປ່ຽນລະຫັດຜ່ານ;

5) ບັນທຶກເຫດການ ແລະ ຂັ້ນຕອນການດຳເນີນການ ທີ່ເກີດຂຶ້ນທັງໝົດ ເພື່ອໃຊ້ເປັນຂໍ້ມູນໃນການປ້ອງກັນ ແລະ ການປະສານງານກັບໜ່ວຍງານທີ່ກ່ຽວຂ້ອງໃນກໍລະນີທີ່ຈຳເປັນ.

ພາກທີ IV
ການສຳຮອງ ແລະ ການເກັບຮັກສາຂໍ້ມູນຈໍລະຈອນທາງເວັບໄຊ

VII. ການສຳຮອງ ແລະ ການເກັບຮັກສາຂໍ້ມູນຈໍລະຈອນທາງເວັບໄຊ

1. ການສຳຮອງຂໍ້ມູນເວັບໄຊ

ຜູ້ຄຸ້ມຄອງເວັບເຊີເວີ ຄວນດຳເນີນການສຳຮອງຂໍ້ມູນຂອງເວັບເຊີເວີຢ່າງສະໝ່ຳສະເໝີ ໂດຍອ້າງອີງຕາມມາດຕະຖານຂອງ National Institute of Standard and Technology (NIST) ດັ່ງນີ້:

1) ສອດຄ່ອງກັບຂໍ້ກຳນົດທາງກົດໝາຍ;
2) ສອດຄ່ອງກັບຂໍ້ຜູກພັນທາງສັນຍາ;
3) ສອດຄ່ອງກັບແນວທາງນະໂຍບາຍທີ່ກ່ຽວຂ້ອງຂອງອົງກອນ;
4) ກຳນົດຈຸດປະສົງ ແລະ ຂອບເຂດຂອງແນວປະຕິບັດ;
5) ສິດ ແລະ ໜ້າທີ່ຂອງຜູ້ກ່ຽວຂ້ອງ;
6) ເວັບເຊີເວີທີ່ກ່ຽວຂ້ອງກັບແນວປະຕິບັດ;

7) ຄຳນິຍາມຂອງຄຳສັບສະເພາະ ໃນທາງກົດໝາຍ ແລະ ທາງເຕັກນິກ;

8) ຄວາມສະໝ່ຳສະເໝີຂອງການສຳຮອງຂໍ້ມູນ;

9) ຂັ້ນຕອນສຳລັບຢັ້ງຢືນຂໍ້ມູນທີ່ສຳຮອງ ໄດ້ຮັບການບຳລຸງຮັກສາ ແລະ ການປ້ອງກັນ ຢ່າງເໝາະສົມ;

10) ຂັ້ນຕອນສຳລັບຢັ້ງຢືນວ່າຂໍ້ມູນໄດ້ຮັບການທຳລາຍ ຫຼື ມີການເກັບຮັກສາ ເມື່ອບໍ່ມີຄວາມຈຳເປັນໃນການໃຊ້ງານ;

11) ຂັ້ນຕອນສຳລັບຢືນຢັນວ່າຂໍ້ມູນທີ່ສຳຮອງໄວ້ ສາມາດນຳອອກມາໃຊ້ງານໄດ້ຢ່າງຖືກຕ້ອງ ໃນກໍລະນີທີ່ມີການຮ້ອງຂໍ;

12) ຄວາມຮັບຜິດຊອບຂອງຜູ້ທີ່ມີສ່ວນຮ່ວມໃນການ ເກັບຮັກສາ, ປ້ອງກັນ ແລະ ລຶບລ້າງຂໍ້ມູນ;

13) ລະບຸໄລຍະເວລາການເກັບຮັກສາຂໍ້ມູນແຕ່ລະປະເພດ;

14) ໜ້າທີ່ຮັບຜິດຊອບຂອງຜູ້ສຳຮອງຂໍ້ມູນ ໃນກໍລະນີທີ່ອົງກອນມີຜູ້ຮັບຜິດຊອບວຽກງານ ດັ່ງກ່າວ.
(ລະອຽດເຂົ້າເບິ່ງເອກະສານຄັດຕິດ ຂໍ້ທີ່ 12 ຕາມລິ້ງ URL).

2. ການເກັບຮັກສາຂໍ້ມູນຈໍລະຈອນທາງຄອມພິວເຕີ

ການເກັບຮັກສາຂໍ້ມູນຈໍລະຈອນທາງຄອມພິວເຕີ ຫຼື ຂໍ້ມູນການເຂົ້າໃຊ້ງານເວັບໄຊ ໃຫ້ປະຕິບັດຕາມ ກົດໝາຍ ວ່າດ້ວຍ ການປົກປ້ອງຂໍ້ມູນເອເລັກໂຕຣນິກ, ສະບັບເລກທີ 25/ສພຊ, ລົງວັນທີ 12 ພຶດສະພາ 2017.

ພາກທີ V
ການປະສານງານເວລາເກີດເຫດສຸກເສີນ

VIII. ການປະສານງານ

ສູນສະກັດກັ້ນ ແລະ ແກ້ໄຂເຫດສຸກເສີນທາງຄອມພິວເຕີ ເປັນສູນກາງປະສານງານ ພາຍໃນ ແລະ ຕ່າງປະເທດ ເພື່ອແກ້ໄຂເຫດສຸກເສີນທາງລະບົບຄອມພິວເຕີ, ຮັບແຈ້ງ ແລະ ໃຫ້ຄຳປຶກສາ ທາງດ້ານເຕັກນິກວິຊາການ ໃນການແກ້ໄຂບັນຫາໄພຄຸກຄາມທີ່ເກີດຂຶ້ນກັບລະບົບເວັບເຊີເວີ, ເວັບໄຊ ແລະ ໄພຄຸກຄາມອື່ນໆ ດ້ວຍຊ່ອງທາງການຕິດຕໍ່ປະສານງານ ມີດັ່ງນີ້:

1. ຊ່ອງທາງໃນການແຈ້ງເຫດການໄພຄຸກຄາມຫາສູນລາວເຊີດ

1) ໂທຕັ້ງໂຕະ:	+856-21-254508
2) ແຟັກ:	+856-21-254508
3) ໂທມືຖື:	+856-30-5764222
4) ອີເມວ:	report@laocert.gov.la
5) ເວັບໄຊ	https://www.laocert.gov.la/incident

6) ແອັບພິເຄຊັ່ນ ລາວເຊີດ (Application Laocert)

2. ຂໍ້ມູນສຳຄັນຂອງຜູ້ແຈ້ງໄພຄຸກຄາມຫາສູນລາວເຊີດ

1) ຊື່ ແລະ ນາມສະກຸນ;

2) ໜ່ວຍງານ ຫຼື ອົງກອນທີ່ຜູ້ແຈ້ງສັງກັດຢູ່;

3) ໝາຍເລກໂທລັບທີ່ໃຊ້ຕິດຕໍ່ກັບຜູ້ແຈ້ງ;

4) ອີເມວທີ່ໃຊ້ຕິດຕໍ່ກັບຜູ້ແຈ້ງ.

3. ລາຍລະອຽດຂອງໄພຄຸກຄາມ ທີ່ແຈ້ງ

1) ອ້າງອີງຕາມປະເພດໄພຄຸກຄາມ ຊຶ່ງສາມາດລະບຸໄດ້ຫຼາຍກວ່າ 01 ປະເພດ ເນື່ອງຈາກໄພຄຸກຄາມເຫດການໜຶ່ງອາດປະກອບໄປດ້ວຍຫຼາຍປະເພດໄພຄຸກຄາມ;

2) ວັນທີ, ເດືອນ, ປີ ແລະ ເວລາ ທີ່ແຈ້ງໄພຄຸກຄາມ;

3) ຂໍ້ມູນເຄື່ອງທີ່ໄດ້ຮັບຜົນກະທົບ ລາຍລະອຽດຂອງເຄື່ອງໄດ້ແກ່ ໝາຍເລກໄອພີ, ໜ້າທີ່ຂອງເຄື່ອງ, ລະບົບປະຕິບັດການ ແລະ ຊອບແວຕ່າງໆ ທີ່ຕິດຕັ້ງເທິງເຄື່ອງ;

4) ຂໍ້ມູນລາຍລະອຽດຂອງເຄື່ອງທີ່ໃຊ້ກໍ່ເຫດ ທີ່ສາມາດກວດສອບ ແລະ ສະແດງໄດ້ ເຊັ່ນ: ໝາຍເລກໄອພີ, ຊື່ຜູ້ລົງທະບຽນລະຫັດຊື່ອິນເຕີເນັດ, ສະຖານທີ່ເຄື່ອງຜູ້ກໍ່ເຫດ ແລະ ສະຖານະພາບເຄື່ອງຜູ້ກໍ່ເຫດ;

5) ລະບຸລາຍລະອຽດຂອງໄພຄຸກຄາມທີ່ພົບເຫັນ ຫຼື ໄດ້ຮັບແຈ້ງອື່ນໆ ນອກເໜືອຈາກຂໍ້ມູນໃນຂໍ້ 01-04 ຂ້າງເທິງ.

ພາກທີ VI
ບົດບັນຍັດສຸດທ້າຍ

IX. ການຈັດຕັ້ງປະຕິບັດ

ມອບໃຫ້ ສູນສະກັດກັ້ນ ແລະ ແກ້ໄຂເຫດສຸກເສີນທາງຄອມພິວເຕີ ປະສານສົມທົບກັບພາກສ່ວນທີ່ກ່ຽວຂ້ອງ ແລະ ອົງການປົກຄອງທ້ອງຖິ່ນ ຈັດຕັ້ງໂຄສະນາ, ເຜີຍແຜ່, ແນະນຳ, ຝຶກອົບຮົມ ແລະ ປະຕິບັດຄຳແນະນຳສະບັບນີ້ ໃຫ້ໄດ້ຮັບຜົນດີ.

ບຸກຄົນ, ນິຕິບຸກຄົນ ຫຼື ການຈັດຕັ້ງ ທີ່ສ້າງ, ປັບປຸງ, ພັດທະນາ ແລະ ຄຸ້ມຄອງເວັບໄຊ ພາຍໃນ ສປປ ລາວ ຈົ່ງຮັບຮູ້ ແລະ ນຳໄປຈັດຕັ້ງປະຕິບັດໃຫ້ເໝາະສົມ.

X. ຜົນສັກສິດ

ຄຳແນະນຳສະບັບນີ້ ມີຜົນສັກສິດແຕ່ວັນລົງລາຍເຊັນເປັນຕົ້ນໄປ ແລະ ຈັດຕັ້ງປະຕິບັດພາຍຫຼັງທີ່ໄດ້ລົງໃນຈົດໝາຍເຫດທາງລັດຖະການ ສິບຫ້າວັນ.

ລັດຖະມົນຕີ

ປອ. ທັນສະໄໝ ກົມມະສິດ

ເອກະສານຄັດຕິດ

1. ການວາງແຜນສ້າງເວັບໄຊ ສາມາດປະຕິບັດຕາມ ຂໍ້ທີ 3 "Planing and Managing web server" ຂອງ ມາດຕະຖານ NIST SP 800-44.
   https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-44ver2.pdf
2. ວິທີການ ແລະ ຂັ້ນຕອນການປະເມີນຄວາມສ່ຽງເວັບໄຊ ໄດ້ກຳນົດໄວ້ໃນມາດຕະຖານ ISO/IEC 27005:2011.
   https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-3:v1:en
3. ມາດຕະການທີ່ເໝາະສົມ ເພື່ອປ້ອງກັນໄພຄຸກຄາມ ອີງຕາມມາດຕະຖານ ISO/IEC 27002:2013.
   https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en
4. ການຈົດທະບຽນລະຫັດຊື່ອິນເຕີເຂອງ ".la" ໃຫ້ປະຕິບັດຕາມເອກະສານ ສະບັບເລກທີ ເລກທີ 164/ລບ, ລົງ ວັນທີ 23 ມີນາ 2012.
   http://mpt.gov.la/index.php?r=site%2Fdetail&id=44
5. ການສຳຮອງຂໍ້ມູນ ແລະ ການຮັກສາເວັບເຊີເວີ ໃຫ້ປະຕິບັດຕາມເອກະສານ ສະບັບເລກທີ 590/ປທສ, ນະຄອນຫຼວງວຽງຈັນ ລົງວັນທີ 18 ພຶດສະພາ 2016.
   http://www.itd.gov.la/Law/ຂໍ້ຕົກລົງ%20ວ່າດ້ວຍ%20ການອະນຸຍາດດຳເນີນກິດຈະການສູນກາງຂໍ້ມູນຂ່າວສານ%20ຜ່ານອິນເຕີເນັດ%20590.ປທສ@18.3.2016.pdf
6. ລາຍລະອຽດ SA's Office of Citizen Services and Innovative Technologies and the Federal Web Managers Council, "choosing CMS", 31 October 2013.
   http://www.howto.gov/webcontent/technology
7. E. Barker and A. Roginsky, "NIST Special Publication 800-131A", National Institute of Standards and Technology (NIST), U.S. Department of Commerce , 2011
   https://csrc.nist.gov/publications/detail/sp/800-131a/archive/2011-01-13
8. ລາຍລະອຽດເພີ່ມຕື່ມກ່ຽວກັບ Stored Procedure :
   https://www.owasp.org/index.PHP/Guide_to_SQL_Injection ແລະ
   https://www.owasp.org/index.PHP/Avoiding_SQL_Injection#Parameterized_Stored_Procedures .
9. ລາຍລະອຽດເພີ່ມຕື່ມກ່ຽວກັບ OWASP
   https://www.owasp.org/index.PHP/SQL_Injection_Prevention_Cheat_Sheet ແລະ
   https://www.owasp.org/index. PHP/Query_Parameterization_Cheat_Sheet
10. ລາຍລະອຽດເພີ່ມຕື່ມກ່ຽວກັບການປ້ອງກັນການໂຈມຕີຈາກເຕັກນິກ Session Hijacking :
    https://www.owasp.org/index.PHP/Session_Management_Cheat_Sheet
11. ລາຍລະອຽດເພີ່ມຕື່ມກ່ຽວກັບ How to Secure Your Website ຂອງ IPA
    https://www.ipa.go.jp/files/000017318.pdf
12. ມາດຕະຖານການສຳຮອງຂໍ້ມູນເວັບໄຊຂອງ NIST (Guidelines on Securing Public Web Servers)
    https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=51222

ໝາຍເຫດ: ສຳລັບຂັ້ນຕອນການປະຕິບັດທີ່ກ່າວມາທັງໝົດໃນຂ້າງເທິງຂອງຄຳແນະນຳສະບັບນີ້ ບໍ່ໄດ້ຮັບຮອງເວັບໄຊທີ່ຄຸ້ມຄອງຈະມີຄວາມປອດໄພຈາກການໂຈມຕີ, ການບຸກລຸກເວັບໄຊ ທີ່ມີໄພຄຸກຄາມໃນຮູບແບບທີ່ບໍ່ເຄີຍເກີດຂຶ້ນມາກ່ອນ (Zero Day Attack) ຫຼື ຖືກໂຈມຕີລະບົບເວັບເຊີເວີ (Web server) ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ ເປັນຕົ້ນ.