1. ນິຍາມຂອງຄວາມປອດໄພ

ຄວາມປອດໄພ ເປັນພື້ນຖານການປ້ອງກັນຂໍ້ມູນຊັບສິນ, ຊຶ່ງຊັບສິນດັ່ງກ່າວລວມທັງສິ່ງທີ່ຈັບຕ້ອງໄດ້ ເຊັ່ນວ່າ: ເວບເພຈ໌ (Web page), ຖານຂໍ້ມູນເກັບຂໍ້ມູນລູກຄ້າ ຫຼື ຂໍ້ມູນຂອງອົງກອນຕ່າງໆ.

2. ຄວາມປອດໄພຂອງໂປຣແກຣມຕ້ອງປ້ອງການຢູ່ໃນ 3 ລະດັບຄື:
   1) ລະດັບເຄືອຂ່າຍ
   2) ລະດັບເຄື່ອງເຊີເວີ
   3) ລະດັບໂປຣແກຣມ
3. ຄວາມປອດໄພຂອງຂໍ້ມູນປະກອບມີດັ່ງນີ້:
   1) ການຢືນຢັນຜູ້ໃຊ້
   2) ການອານຸຍາດ
   3) ການກວດສອບ
   4) ຄວາມລັບຂອງຂໍ້ມູນ
   5) ຄວາມຖືກຕ້ອງຂໍ້ມູນ
   6) ຄວາມພ້ອມໃຫ້ບໍລິການຂໍ້ມູນ
4. ໄພຄຸກຄາມ

ໄພຄຸກຄາມ ໝາຍເຖິງທຸກບັນຫາທີ່ກໍ່ໃຫ້ເກີດຄວາມເສຍຫາຍຂຶ້ນກັບຂໍ້ມູນ ຫຼື ຊັບສິນ ແລະ ຕໍ່ອົງປະກອບຂອງຄວາມປອດໄພດ້ານໃດດ້ານໜຶ່ງ.

5. ຊ່ອງໂວ່

ຈຸດອ່ອນ ຫຼື ຊ່ອງໂວ່ ໝາຍເຖິງຂໍ້ຜິດພາດຂອງລະບົບທີ່ພາໃຫ້ເກີດມີຄວາມສ່ຽງຕໍ່ການຄຸກຄາມ.

6. ສ້າງເວບໃຫ້ມີຄວາມປອດໄພ

ການອອກແບບ ແລະ ສ້າງເວບໃຫ້ມີຄວາມປອດໄພຈຳເປັນຕ້ອງຮູ້ຈັກຄວາມສ່ຽງທີ່ອາດຈະເກີດຂຶ້ນ ແບບຈຳລອງຄວາມສ່ຽງເປັນສ່ວນປະກອບສຳຄັນໃນການອອກແບບເວບ, ເພື່ອວິເຄາະສະຖາປັດຕະຍະກຳຂອງ ເວບ, ອອກແບບ ແລະ ຮູ້ໄດ້ຈຸດອ່ອນ ຫຼື ຊ່ອງໂວ່ຂອງໂປຣແກຣມ.

7. Information Gathering

Information Gathering ເປັນການພະຍາມສຳຫຼວດແວດລ້ອມ ແລະ ສະແດງຂໍ້ມູນຕ່າງໆຂອງເປົ້າໝາຍທີ່ ຈະໂຈມຕີ.

8. Information Gathering Techniques 2 ແບບຄື:
   1) Active techniques ເປັນການເຊື່ອມຕໍ່ໄປຍັງເຄື່ອງເປົ້າໝາຍທີ່ຈະໂຈມຕີ ເພື່ອສະແດງຂໍ້ມູນຕ່າງໆທີ່ ກ່ຽວຂ່ອງ ເຊັ່ນວ່າ: ໝາຍເລກ Port, ໄຟລ໌ຂໍ້ມູນ ແລະ ອື່ນໆ.

2) Passive techniques ເປັນການນຳໃຊ້ເຄື່ອງມື ແລະເວບໄຊໃນການສະແດງຂໍ້ມູນທີ່ກ່ຽວຂອງກັບເຄື່ອງເປົ້າໝາຍ,ຊຶ່ງເຮົາບໍ່ໄດ້ເຊື່ອມຕໍ່ໄປຍັງເປົ້າໝາຍໂດຍກົງ.

9. Enumerating Domains, Files, and Resources

Enumerating Domains, Files, and Resources ເປັນການສຳຫຼວດຂໍ້ມູນດູເມນໄຟລ໌ຂໍ້ມູນ ແລະ ຂໍ້ມູນທີ່ກ່ຽວຂ່ອງຕ່າງໆ ໂດຍນຳໃຊ້ທັງແບບ Active ແລະ Passive Techniques.

10. ຂັ້ນຕອນການບຸກໂຈມຕີມີດັ່ງລຸ່ມນີ້:(Attacking methodology)

1) ການສຳຫຼວດ ແລະ ປະເມີນ
2) ການເຈາະລະບົບ ແລະ ນຳໃຊ້ຜົນໄດ້ຮັບ
3) ການຂະຫຍາຍສິດທິ
4) ການເຈາະຈຸດອ່ອນ
5) ການຍົກເລີກບໍລິການ

11. ຄວາມປອດໄພຂອງເຄືອຂ່າຍປະກອບດ້ວຍອຸປະກອນໃດແດ່?

roulers, firewalls, ແລະ switches.

12. ໄພຄຸກຄາມເຄືອຂ່າຍປະກອບມີດັ່ງນີ້:

1) ການນຳຮອຍຂໍ້ມູນ
2) ການດັກຈັບຂໍ້ມູນ
3) ການປອມໂຕ
4) ການໂຈມຕີໂດຍຄົນກາງ
5) ການປະຕິເສດບໍລິການ

13. ໄພຄຸກຄາມຄອມພິວເຕີໝາຍເຖິງຫຍັງ?

ໄພຄຸກຄາມຄອມພິວເຕີໝາຍການເຂົ້າເຖິງລະບົບຊອບແວ່ທີ່ຕິດຕັ້ງຢູ່ໃນເຄື່ອງໂດຍກົງ ເຊັ່ນວ່າ: ລະບົບປະຕິບັດການWindows server 2003, ເວບເຊີເວີ Internet Information Services (IIS), .NET Framework,ໂປຣແກຣມຖານຂໍ້ມູນ, SQL Server ຂຶ້ນກັບການຕັ້ງຄ່າຄວາມປອດໄພຂອງເຄື່ອງເຊີເວີ.

14. ລຳດັບໄພຄຸກຄາມຂອງເຄື່ອງເຊີເວີ

1) Viruses, Trojan horses ແລະ a worms
2) Footprinting
3) Password cracking

4) Denial of service
5) Arbitrary code execution
6) Unauthorized access

15. ການໂຈມຕີດ້ວຍ SQL Injection

SQL Injection ເປັນຄຳສັ່ງທາງດ້ານເຕັກນິກທີ່ຜູ້ບຸກໂຈມຕີນຳໃຊ້ໃນການເຈາະເຂົ້າສູ່ລະບົບຜ່ານທາງຈຸດອ່ອນຂອງທີ່ເກີດຂຶ້ນໃນລະດັບຖານຂໍ້ມູນຂອງໂປຣຈຸດອ່ອນດັ່ງກ່າວຈະສະແດງອອກມາເມື່ອຜູ້ໃຊ້ປ້ອນຂໍ້ມູນທີ່ເຮັດໃຫ້ລະບົບຜິດພາດ, ການສະແດງຂໍ້ຜິດພາດໂປຣແກຣມ.

16. ຈຸດອ່ອນຂອງໂປຣແກຣມມີດັ່ງນີ້

1) ການຮັບຂໍ້ມູນຈາກຜູ້ໃຊ້
2) ການນຳໃຊ້ SSL
3) ການນຳໃຊ້ HTML forms
4) ການນຳໃຊ້ Cookies
5) ການນຳໃຊ້ HTTP REFERER Header
6) ການນຳໃຊ້ POST & GET method
7) ວິທີການເຂົ້າສູ່ ແລະ ອອກຈາກລະບົບ
8) ການສະແດງຂໍ້ຜິດພາດ

17. ການກວດສອບຈຸດອ່ອນ

ນຳໃຊ້ເຄື່ອງໝາຍ ‘ ຕໍ່ທ້າຍ URL ເພື່ອໃຫ້ສະແດງຂໍ້ຜິດພາດເຊັ່ນວ່າ:

www.examplewebsite.com/index.php?id ‘

18. ວິທີການໂຈມຕີດ້ວຍ SQL Injection ມີດັ່ງຕໍ່ໄປນີ້:

1) Injected through user input.
2) Injection through cookie fields contain attack strings.
3) Injection through Server Variables.
4) Second-Order Injection where hidden statements to be executed at another time by another function.

19. ປະເພດຂອງ SQL Injection ມີດັ່ງຕໍ່ໄປນີ້:

1) Tautology-based SQL Injection

2) Piggy-backed Queries / Statement Injection
3) Union Query
4) illegal/Logically Incorrect Queries
5) Inference
6) Stored Procedure Injection

## 20. ການບຸກໂຈມຕີໂດຍ Cross-Site Scripting(XSS)

ການບຸກໂຈມຕີໂດຍ XSS ໂດຍພື້ນຖານແລ້ວຈະນຳໃຊ້ການແຊກໂຄດ(script) ເຂົ້າໃນໜ້າຟອມ ການປ້ອນຂໍ້ມູນຂອງຜູ້ໃຊ້ ຫຼື ຜ່ານທາງການເຊື່ອມໂຍງ(Hyperlink)ເພື່ອສະແດງຂໍ້ມູນ.

ໂຄດ XSS ທີ່ນຳມາແຊກໃນເບື້ອງຂອງຜູ້ໃຊ້ໄດ້ແກ່: JavaScript, VBScript, HTML, CSS, Flash, ອື່ນໆ.

XSS ສາມາດບັນທຶກຂໍ້ມູນທີ່ເປັນອັນຕະລາຍລົງໃນເຄື່ອງເຊີເວີ ຫຼື ສັ່ງການຄຳສັ່ງໃດໜຶ່ງໃຫ້ເຮັດວຽກຜ່ານທາງເຄື່ອງຜູ້ໃຊ້ໄດ້.

## 21. ປະເພດຂອງການໂຈມຕີແບບ XSS

ການໂຈມຕີແບບ XSS ມີ 2 ປະເພດຄື:

1) non-persistent XSS - ນຳໃຊ້ການສົ່ງໂຄດເພື່ອສະໄປແດງຂໍ້ມູນ, ຈະບໍ່ເກັບໄວ້ໃນເຄື່ອງເຊີເວີ.
2) persistent XSS - ນຳໃຊ້ການສົ່ງໂຄດໄປເກັບໄວ້ໃນເຄື່ອງເຊີເວີ ແລະ ສັ່ງໃຫ້ເຮັດວຽກ

## 22. ວິທີການໂຈມຕີດ້ວຍ XSS

ສາມາດໂຈມຕີດ້ວຍ XSS ໄດ້:

1) <script>alert("XSS")</script>
2) <script>alert('XSS')</script>/
3) <script>alert('XSS')</script>

## 23. ການໂຈມຕີແບບ RFI

RFI ເປັນເຕັກນິກໜຶ່ງທີ່ໃຊ້ໃນການໂຈມຕີເວບຜ່ານເຄື່ອງຄອມພິວເຕີຄວບຄຸມ(Remote computer).

ການໂຈມຕີແບບ RFI ຈະອານຸຍາດໃຫ້ຜູ້ໃຊ້ສາມາດສັ່ງໃຫ້ໂຄດຄຳສັ່ງຂອງຜູ້ໃຊ້ເຮັດວຽກຢູ່ໃນເຄື່ອງເຊີເວີ ຜ່ານທາງ URL. ເມື່ອໂປຣແກຣມສັ່ງໃຫ້ຄຳສັ່ງ malicious code ເຮັດວຽກແລ້ວຈະນຳໄປສູ່ການ

ໂຈມຕີແບບ back-door exploit ຫຼື ເປັນການສະແດງຂໍ້ມູນທາງດ້ານເຕັກນິກຂອງລະບົບ(technical information retrieval).

24. ແນວຄວາມຄິດການປ້ອງກັນການບຸກໂຈມຕີດ້ວຍ SQL-Injection

❖ ອີງໃສ່ຈຸດອ່ອນຂອງໂປຣແກຣມ

1) ການຮັບຂໍ້ມູນຈາກຜູ້ໃຊ້
2) ການນຳໃຊ້ SSL
3) ການນຳໃຊ້ HTML forms
4) ການນຳໃຊ້ Cookies
5) ການນຳໃຊ້ HTTP REFERER Header
6) ການນຳໃຊ້ POST & GET method
7) ວິທີການເຂົ້າສູ່ ແລະ ອອກຈາກລະບົບ
8) ການສະແດງຂໍ້ຜິດພາດ

25. ວິທີການປ້ອງກັນການບຸກໂຈມຕີດ້ວຍ SQL-Injection

❖ ການປ້ອງກັນການປ້ອນຂໍ້ມູນຈາກຜູ້ໃຊ້

1) ນຳໃຊ້ຄຳສັ່ງ ກວດສອບການປ້ອນຂໍ້ມູນ ເຊັ່ນວ່າ:

mysql_real_escape_string(),

mysqli_real_escape_string(),

trim(), stripslashes().

2) ນຳໃຊ້ຊຸດຄຳສັ່ງໃນການຕິດຕໍ່ຖານຂໍ້ມູນດ້ວຍ PDO ຫຼື mysqli

26. ແນວຄວາມຄິດການປ້ອງກັນການບຸກໂຈມຕີດ້ວຍ Cross Site Scripting

Cross site scripting ຫຼື XSS, ເປັນວິທີການໂຈມຕີຜ່ານເວບທີ່ຜູ້ພັດທະນາເວບບໍ່ມີການປ້ອງກັນການປ້ອນຂໍ້ມູນຂອງຜູ້ໃຊ້ຊຶ່ງຜູ້ບຸກໂຈມຕີສາມາດປ້ອນຄຳສັ່ງ(Code injected) ຜ່ານໜ້າຟອມ ຫຼື ປ່ຽນແປງຈຸດເຊື່ອມໂຍງ(Hyperlink) ຈາກເບື້ອງຜູ້ໃຊ້ດ້ວຍພາສາ JavaScript, VBScript, HTML, CSS, Flash, ແລະ ພາສາອື່ນໆ.

27. ວິທີການປ້ອງກັນການບຸກໂຈມຕີດ້ວຍ Cross Site Scripting

❖ ການປ້ອງກັນການປ້ອນຂໍ້ມູນຈາກຜູ້ໃຊ້

1) ນຳໃຊ້ຄຳສັ່ງ ກວດສອບການປ້ອນຂໍ້ມູນ, ສຳລັບພາສາ PHP ເຊັ່ນວ່າ: ການກວດສອບເລກໂທລະສັບ, ໂຕເລກ ແລະ ອື່ນໆ.

2) preg_match()

```
if(preg_match("/^[0,2,0-1]{3}-[0-9]{4}-[0-9]{4}$/", $phone)) {
echo $phone . " is valid format.";
}
```

## 28. ແນວຄວາມຄິດການປ້ອງກັນການບຸກໂຈມຕີດ້ວຍ Remote/Local File including

ການໂຈມຕີແບບ RFI ຈະອານຸຍາດໃຫ້ຜູ້ໃຊ້ສາມາດສັ່ງໃຫ້ໂຄດຄຳສັ່ງຂອງຜູ້ໃຊ້ເຮັດວຽກຢູ່ໃນເຄື່ອງເຊີເວີ ຜ່ານທາງ URL. ເມື່ອໂປຣແກຣມສັ່ງໃຫ້ຄຳສັ່ງ malicious code ເຮັດວຽກແລ້ວຈະນຳໄປສູ່ການໂຈມຕີແບບ back-door exploit ຫຼື ເປັນການສະແດງຂໍ້ມູນທາງດ້ານເຕັກນິກຂອງລະບົບ(technical information retrieval).

ຈຸດອ່ອນທີ່ພາໃຫ້ເກີດຊ່ອງໂວ່ໃນການໂຈມຕີແບບ RFI ມາຈາກການບໍ່ກວດສອບການປ້ອນຂໍ້ມູນຂອງຜູ້ໃຊ້.

ຄຳສັ່ງທີ່ໃຊ້ໃນການ include ໄຟລ ມີຄື: include(),include_once(), require(),require_once()

## 29. ການນຳໃຊ້ເຄື່ອງມື WebCruiser

WebCruiser ເປັນເຄື່ອງມືທີ່ຊ່ວຍໃນການກວດສອບຫາຈຸດອ່ອນ ຫຼື ຊ່ອງໂວ່ຂອງ Web application.

WebCruiser ສາມາດຕອບສະໜອງການກວດສອບຫາຈຸດອ່ອນຂອງເວບ POC (Proof of concept) ໄດ້ດັ່ງນີ້: SQL Injection, Cross Site Scripting, Local File Inclusion, Remote File Inclusion, Redirect ແລະ ອື່ນໆ.

WebCruiser ເປັນເຄື່ອງມືທົດສອບຂ້ອນຂ້າງນ້ຳໃຊ້ງ່າຍຖ້າ
ທຽບໃສ່ກັບເຄື່ອງມືອື່ນໆ