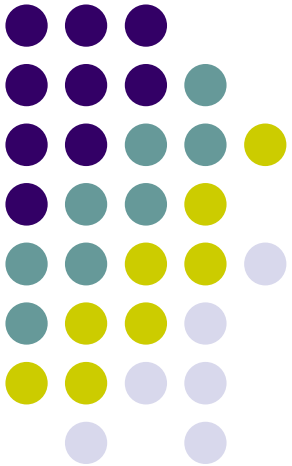
ຄະນະວິທະຍາສາດທຳມະຊາດ
ພາກວິຊາ ວິທະຍາສາດຄອມພິວເຕີ

ຄວາມປອດໄພເວບໄຊ
(Web Security)

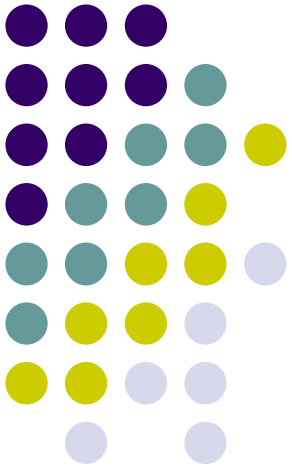


ສອນໂດຍ: ອຈ ເພັດ ສອນວິໄລ
ມືຖື: 020 58390300
ອີເມວ: p.sonevilay@nuol.edu.la

ບົດທີ6

ການບຸກໂຈມຕີດ້ວຍ Local ແລະ Remote File Inclusion (LFI, RFI) Attacks

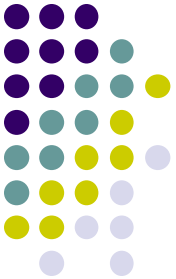
(Local andRemote File Inclusion (LFI, RFI) Attacks)



ເນື້ອໃນໂດຍລວມ

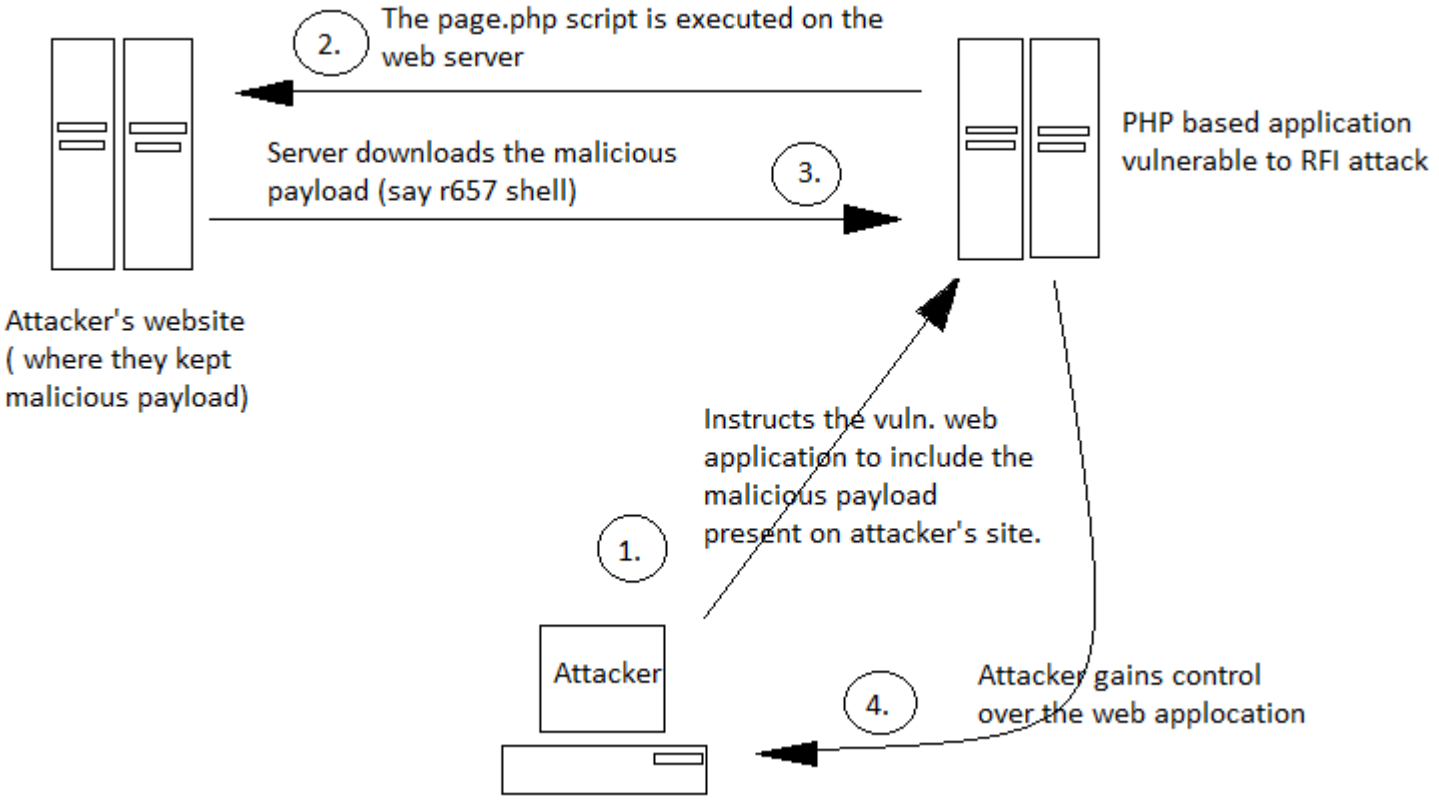
- ແນວຄວາມຄິດການໂຈມຕີດ້ວຍ LFI/RFI
- ວິທີການໂຈມຕີດ້ວຍ LFI/RFI
- ຕົວຢ່າງ ການໂຈມຕີດ້ວຍ LFI/RFI

ແນວຄວາມຄິດການໂຈມຕີດ້ວຍ LFI/RFI

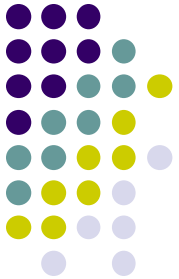


- ການໂຈມຕີແບບ RFI
  - RFI ເປັນເຕັກນິກໜຶ່ງທີ່ໃຊ້ໃນການໂຈມຕີເວບຜ່ານເຄື່ອງຄອມພິວເຕີຄວບຄຸມ(Remote computer).
  - ການໂຈມຕີແບບ RFI ຈະອານຸຍາດໃຫ້ຜູ້ໃຊ້ສາມາດສັ່ງໃຫ້ໂຄດຄຳສັ່ງຂອງຜູ້ໃຊ້ເຮັດວຽກຢູ່ໃນເຄື່ອງເຊີເວີ ຜ່ານທາງ URL. ເມື່ອໂປຣແກຣມສັ່ງໃຫ້ຄຳສັ່ງ malicious code ເຮັດວຽກແລ້ວຈະນຳໄປສູ່ການໂຈມຕີແບບ back-door exploit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

ແນວຄວາມຄິດການໂຈມຕີດ້ວຍ

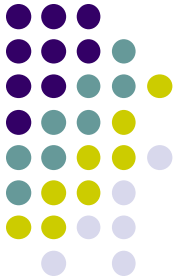


ແນວຄວາມຄິດການໂຈມຕີດ້ວຍ LFI/RFI



- ຂໍ້ແນະນຳສຳລັບການທົດລອງ
  - ໃຫ້ໄປຕັ້ງຄ່າ ໃນໄຟລ php.ini ໃຫ້ຕັ້ງຄ່າ **allow_url_include=Off** ໃຫ້ກຳນົດເປັນ **On**

ວິທີການໂຈມຕີດ້ວຍ RFI

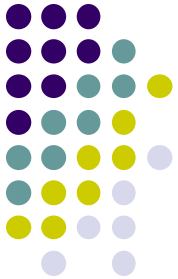


- ຕົວຢ່າງ:

lfi.php

```
<html>
<head><title>Vulnerable to LFI </title> </head>
<body> <h1>Welcome to this Website</h1>
<?php $page = isset($_GET['page']) ? $_GET['page'] :
'index.html'; ?> <p>You are currently at <?php echo"<a
href='$page'>$page</a>";?></p>
<?php include($page); ?>
</body>
</html>
```

ວິທີການໂຈມຕີດ້ວຍ RFI



- ຕົວຢ່າງ:

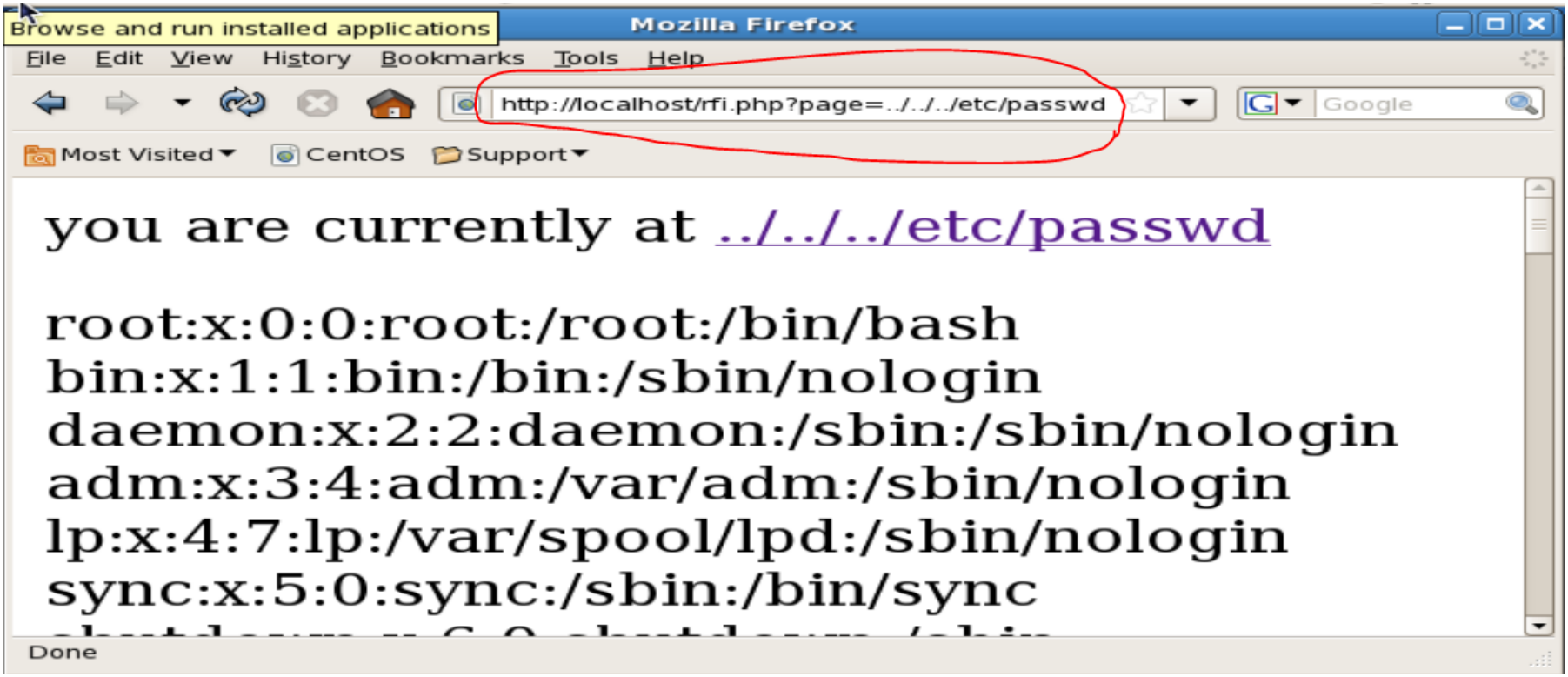
index.html

Hello I am a sample page my name is index.html

- ທົດສອບ

../../etc/passwd

ວິທີການໂຈມຕີດ້ວຍ RFI



ຂໍ້ມູນອ້າງອີງ

[1] J.D. Meier, Alex Mackman, Michael Dunner, Srinath Vasireddy, Ray Escamilla and Anandha Murukan. Improving Web Application Security, Microsoft Corporation, 2013

[2] ການປ້ອງກັນ ແລະ ຮັກສາຄວາມປອດໄພເຄືອຂ່າຍ, www.mict4u.net

ຖາມ ແລະ ຕອບ

ຂອບໃຈ