



ຄະນະວິທະຍາສາດທຳມະຊາດ
ພາກວິຊາ ວິທະຍາສາດຄອມພິວເຕີ

ຄວາມປອດໄພເວບໄຊ້ (Web Security)

ສອນໂດຍ: ອຈ ເພັດ ສອນວິໄລ

ມືຖື: 020 58390300

ອີເມວ: p.sonevilay@nuol.edu.la



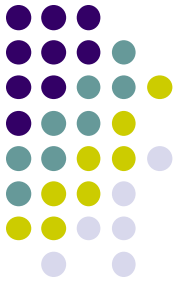
ບົດທີ9

ການປ້ອງກັນການບຸກໂຈມຕີດ້ວຍ
Remote/Local File including



ເນື້ອໃນໂດຍລວມ

- ແນວຄວາມຄິດການປ້ອງກັນ
- ວິທີການປ້ອງກັນ





ແນວຄວາມຄິດການປ້ອງກັນ

- ການໂຈມຕີແບບ RFI ຈະອາໄສຍາດໃຫ້ຜູ້ໃຊ້ສາມາດສັງເກດໂຄດຄໍາສັ່ງຂອງຜູ້ໃຊ້ເຮັດວຽກຢູ່ໃນເຄື່ອງເຊີເວີ ຜ່ານທາງ URL. ເມື່ອໂປຣແກຣມສັງເກດຄໍາສັ່ງ malicious code ເຮັດວຽກແລ້ວຈະນໍາໄປສູ່ການໂຈມຕີແບບ back-door exploit ທີ່ເປັນການສະແດງຂໍ້ມູນທາງດ້ານເຕັກນິກຂອງລະບົບ(technical information retrieval).
- ຈຸດອ່ອນທີ່ພາໃຫ້ເກີດຊ່ອງໂງ່ໃນການໂຈມຕີແບບ RFI ມາຈາກການບໍ່ກວດສອບການປ້ອນຂໍ້ມູນຂອງຜູ້ໃຊ້.
- ຄໍາສັ່ງທີ່ໃຊ້ໃນການ include ໄຟລ ມີຄື:
`include(),include_once(),require(),require_once()`

ວິທີການປ້ອງກັນ



- ຕົວຢ່າງ:

```
if(empty($_GET["url"]))  
    $url = 'step_welcome.php';  
else  
    $url = $_GET["url"];  
<p><? include('step/'.$url) ?></p>
```

- ທົດສອບ

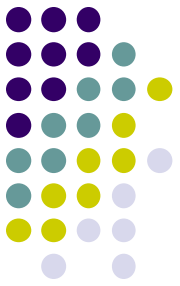
<http://localhost/install/install.php?url=../../../../../../../../etc/passwd>

ວິທີການປ້ອງກັນ



- ການປ້ອງກັນສາມາດນຳໃຊ້
 - ຕ້ອງກວດສອບການເອີ້ນໄຟລຂໍ້ມູນໂດຍບໍ່ອະນຸຍາດໃຫ້ນຳໃຊ້ອັກສອນພິເສດ, ເຊັ່ນວ່າ: ກວດສອບຖ້າມີຈຳເລັດໃນຕົວປ່ຽນໃຫ້ຕັດອອກ (Don't allow special chars in variables.Simple way : filter the dot ".“)
 - ກວດສອບຖ້າມີເຄື່ອງໝາຍ "/" , "\" and "." ໃນຕົວປ່ຽນໃຫ້ຕັດອອກ (Another way : Filter "/" , "\" and ".") ໂດຍນຳໃຊ້ຄຳສັ່ງ htmlspecialchars() ແລະ stripslashes().

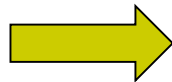
ວິທີການປ້ອງກັນ



- ການປ້ອງກັນສາມາດນຳໃຊ້ (ຕໍ່)
 - ກວດສອບໄຟລທີ່ຕ້ອງການເອີ້ນໃຊ້ໃນຕົວປ່ຽນ

```
<?php
```

```
$whitelist = array(  
    'file1.php',  
    'file2.php',  
    'file3.php',  
    'file4.php',  
    'file5.php',  
);
```



```
<?php  
    $file = strtolower($_GET['page']) . '.php';  
    if(isset($whitelist[$file]) &&  
file_exists($file)) {  
        include($_GET['page'] . '.php');  
    }  
    ?>
```

```
?>
```



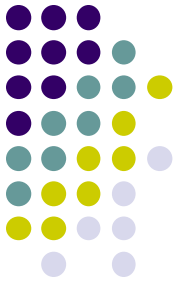
ວິທີການປ້ອງກັນ

- ການປ້ອງກັນສາມາດນຳໃຊ້ (ຕໍ່)
 - ແກ້ໄຂໄຟລ `php.ini` ໃນເຄື່ອງເຊີເວີ
 - `allow_url_include = off`
 - `Display_errors = off`
 - `Register_global = off`
 - ນຳໃຊ້ຄຳສັ່ງໃນ PHP
 - `base64_encode()` ເຊັ່ນວ່າ:
`http://bac.com/index.php?page=PD9waHAgaZWNoZGkX0dFVFsneCddKTsgLy8gT01HIHlvdSBib3RoZXJlZCB0byBkZWVvZGUgYmFzZSA2ND8gPz4`

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



ព្យាបាល និង ព្យាបាល

ឧបករណ៍