



ຄະນະວິທະຍາສາດທຳມະຊາດ
ພາກວິຊາ ວິທະຍາສາດຄອມພິວເຕີ

ຄວາມປອດໄພເວບໄຊ້ (Web Security)

ສອນໂດຍ: ອຈ ເພັດ ສອນວິໄລ

ມືຖື: 020 58390300

ອີເມວ: p.sonevilay@nuol.edu.la



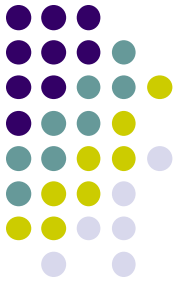
ບົດທີ7

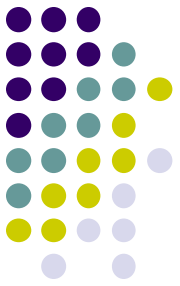
ການປ້ອງກັນການບຸກໂຈມຕີດ້ວຍ SQL- Injection



ເນື້ອໃນໂດຍລວມ

- ແນວຄວາມຄິດການປ້ອງກັນ
- ວິທີການປ້ອງກັນ

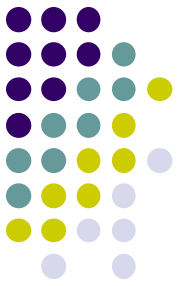




ແນວຄວາມຄິດການປ້ອງກັນ

- ອີງໃສ່ຈຸດອ່ອນຂອງໂປຣແກຣມ(Application Vulnerability)
 - ການຮັບຂໍ້ມູນຈາກຜູ້ໃຊ້ (Input Validation)
 - ການນຳໃຊ້ SSL
 - ການນຳໃຊ້ HTML forms
 - ການນຳໃຊ້ Cookies
 - ການນຳໃຊ້ HTTP REFERER Header
 - ການນຳໃຊ້ POST & GET method
 - ວິທີການເຂົ້າສູ່ ແລະ ອອກຈາກລະບົບ(Login and logout machanism)
 - ການສະແດງຂໍ້ຜິດພາດ(Error Handling)

ວິທີການປ້ອງກັນ



- ການປ້ອງກັນການປ້ອນຂໍ້ມູນຈາກຜູ້ໃຊ້ (Input Validation)
 - ນຳໃຊ້ຄໍາສັ່ງ ກວດສອບການປ້ອນຂໍ້ມູນ ເຊັ່ນວ່າ:
`mysql_real_escape_string()`,
`mysqli_real_escape_string()`, `trim()`, `stripslashes()`.
 - ນຳໃຊ້ຊຸດຄໍາສັ່ງໃນການຕິດຕໍ່ຖານຂໍ້ມູນດ້ວຍ PDO ຫຼື `mysqli`



ວິທີການປ້ອງກັນ

- ຕົວຢ່າງ: ການກວດສອບການປ້ອນຂໍ້ມູນຈາກຜູ້ໃຊ້

```
function check_userinput($data)
{
    $data = trim($data);//
    $data = stripslashes($data);
    $data=mysqli_real_escape_string($conn,$data);
    return $data;
}
```

ວິທີການປ້ອງກັນ



- ຕົວຢ່າງ: ການນຳໃຊ້ mysql prepare statement

```
$stmt = $conn->prepare("INSERT INTO user(firstname,  
lastname, email) VALUES (?, ?, ?)");  
$stmt->bind_param("sss", $firstname, $lastname,  
$email);
```

ໝາຍເຫດ:

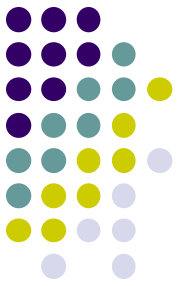
i - integer

d - double

s - string

b - BLOB

ວິທີການປ້ອງກັນ



- ຕົວຢ່າງ: ການນຳໃຊ້ PDO prepare statement

```
$stmt = $conn->prepare("INSERT INTO user (firstname,  
lastname, email)  
VALUES (:firstname, :lastname, :email)");  
$stmt->bindParam(':firstname', $firstname);  
$stmt->bindParam(':lastname', $lastname);  
$stmt->bindParam(':email', $email);
```


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