



ຄະນະວິທະຍາສາດທຳມະຊາດ
ພາກວິຊາ ວິທະຍາສາດຄອມພິວເຕີ

ຄວາມປອດໄພເວບໄຊ້ (Web Security)

ສອນໂດຍ: ອຈ ເພັດ ສອນວິໄລ

ມືຖື: 020 58390300

ອີເມວ: p.sonevilay@nuol.edu.la



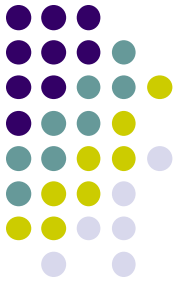
ບົດທີ8

ການປ້ອງກັນການບຸກໂຈມຕີດ້ວຍ Cross Site Scripting



ເນື້ອໃນໂດຍລວມ

- ແນວຄວາມຄິດການປ້ອງກັນ
- ວິທີການປ້ອງກັນ

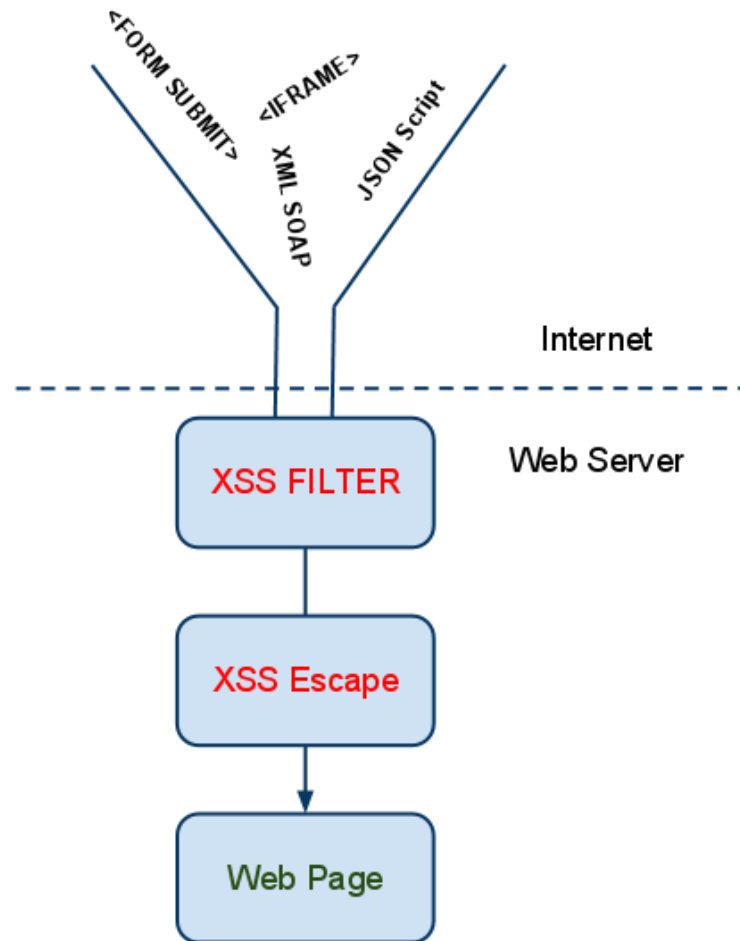
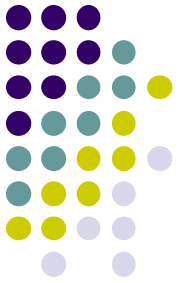




ແນວຄວາມຄິດການປ້ອງກັນ

- Cross site scripting ຫຼື XSS, ເປັນວິທີການໂຈມຕີຜ່ານ ເວບທີ່ຜູ້ພັດທະນາເວບບໍ່ມີການປ້ອງກັນການປ້ອນຂໍ້ມູນຂອງຜູ້ໃຊ້, ຊຶ່ງຜູ້ບຸກໂຈມຕີສາມາດປ້ອນຄໍາສັ່ງ(Code injected) ຜ່ານ ໜ້າຟອມ ຫຼື ປ່ຽນແປງຈຸດເຊື່ອມໂຍງ(Hyperlink) ຈາກເບື້ອງຜູ້ໃຊ້ດ້ວຍພາສາ JavaScript, VBScript, HTML, CSS, Flash, ແລະ ພາສາອື່ນໆ
- ການປ້ອງກັນຕ້ອງກວດສອບຂໍ້ມູນຜູ້ໃຊ້ປ້ອນ(data validation), ການກອງຂໍ້ມູນ(data sanitization), ແລະ ການຍົກເວັ້ນຂໍ້ມູນທີ່ບໍ່ຖືກຕ້ອງ(output escaping)

ແນວຄວາມຄິດການປ້ອງກັນ





ວິທີການປ້ອງກັນ

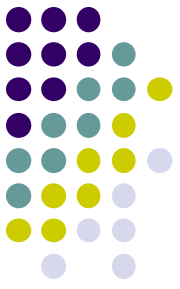
- ການປ້ອງກັນການປ້ອນຂໍ້ມູນຈາກຜູ້ໃຊ້ (Input Validation)
 - ນຳໃຊ້ຄຳສັ່ງ ກວດສອບການປ້ອນຂໍ້ມູນ, ສຳລັບພາສາ PHP ເຊັ່ນວ່າ: ການກວດສອບເລກໂທລະສັບ, ໂຕເລກ ແລະ ອື່ນໆ.
 - preg_match()

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



ວິທີການປ້ອງກັນ

- ການປ້ອງກັນກັນກອງຂໍ້ມູນ(data sanitization)
 - ນຳໃຊ້ຄຳສັ່ງ ການກັນກອງຂໍ້ມູນ, ສຳລັບພາສາ PHP ຈະໃຊ້ `strip_tags()`
`$comment = strip_tags($_POST["comment"]);`



ວິທີການປ້ອງກັນ

- ການຍົກເວັ້ນຂໍ້ມູນທີ່ບໍ່ຖືກຕ້ອງ(output escaping)
 - ນຳໃຊ້ຄຳສັ່ງ ການຍົກເວັ້ນຂໍ້ມູນທີ່ບໍ່ຖືກຕ້ອງ, ສຳລັບພາສາ PHP ຈະໃຊ້ `htmlspecialchars()` ແລະ `htmlentities()`
`$comment = htmlspecialchars($_POST["comment"]);`

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