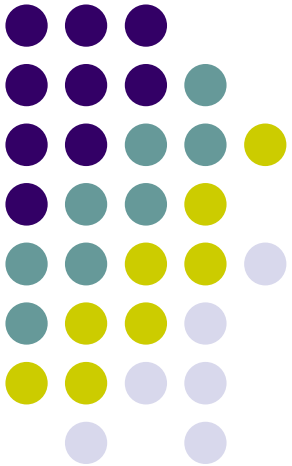
ຄະນະວິທະຍາສາດທຳມະຊາດ
ພາກວິຊາ ວິທະຍາສາດຄອມພິວເຕີ

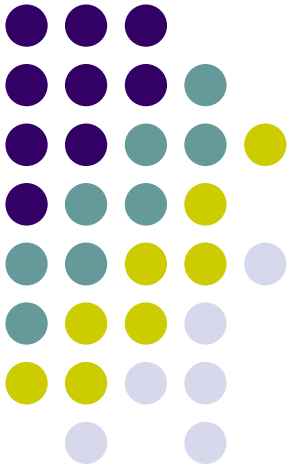
ຄວາມປອດໄພເວບໄຊ
(Web Security)

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

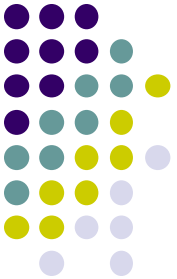


ບົດທີ 4

ການບຸກໂຈມຕີດ້ວຍ SQL Injection
(SQL Injection Attack)



ເນື້ອໃນໂດຍລວມ

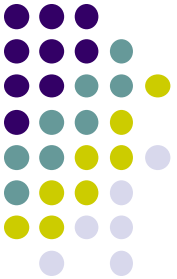


- ສະເໜີເບື້ອງຕົ້ນ
- ແນວຄວາມຄິດການໂຈມຕີດ້ວຍ SQL Injection
- ຈຸດອ່ອນຂອງໂປຣແກຣມ(Application Vulnerability)
- ການກວດສອບຫາຈຸດອ່ອນໂປຣແກຣມ(SQL-Inject Detection)
- ວິທີການໂຈມຕີດ້ວຍ SQL Injection

ສະເໜີເບື້ອງຕົ້ນ

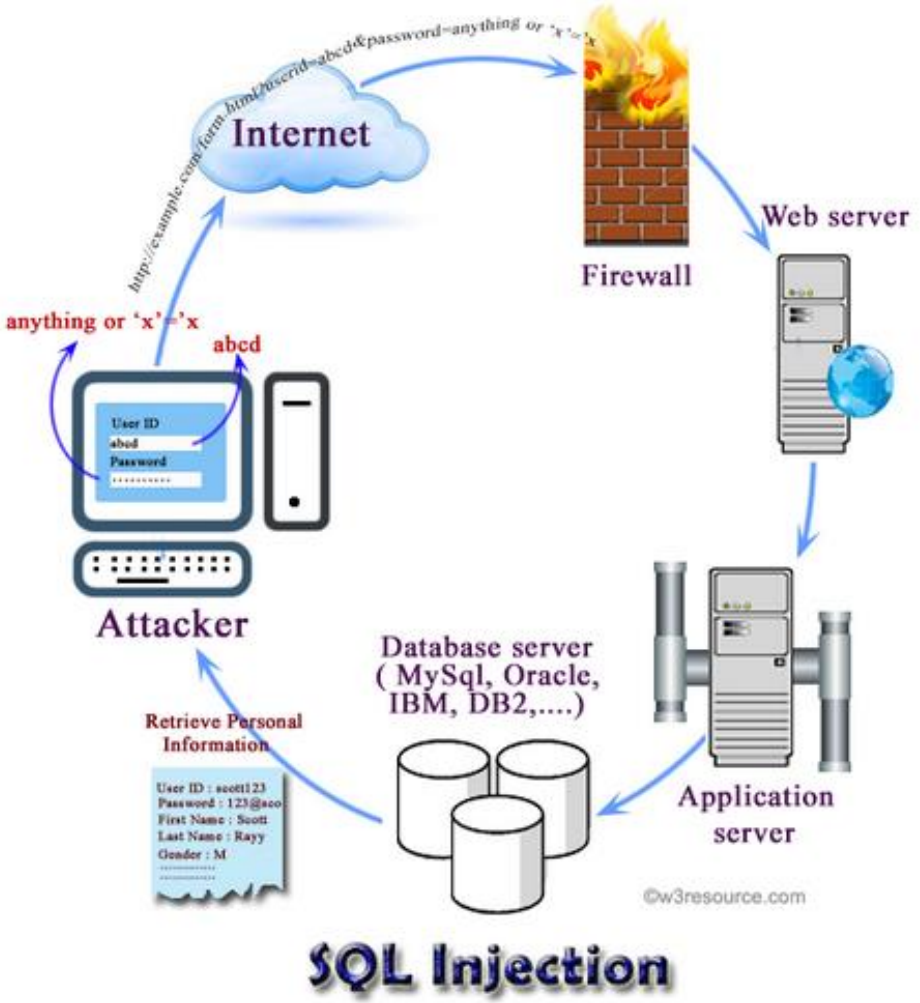
- ເວບໄຊ໌ເປັນເປົ້າໝາຍການບຸກໂຈມຕີ ເພາະວ່າເວບໄຊ໌ເປັນລະບົບເປີດ, ຊຶ່ງມີຄວາມສ່ຽງ ຕໍ່ການໂຈມຕີຈາກຜູ້ບໍ່ຫວັງດີ.
- ເວບໄຊ໌ຈະມີການອານຸຍາດໃຫ້ຜູ້ໃຊ້ປ້ອນຂໍ້ມູນຜ່ານທາງໜ້າເວບ, ຊຶ່ງຂໍ້ມູນດັ່ງກ່າວຈະມີການບັນທຶກ ລົງໃນຖານຂໍ້ມູນ ແລະ ບາງຄັ້ງຈະມີການຄົ້ນຫາຂໍ້ມູນຕ່າງໆ.
- ການຈັດການຂໍ້ມູນຢູ່ໃນຖານຂໍ້ມູນຈະນຳໃຊ້ພາສາ SQL(Structure Query Language), ຊຶ່ງຈະເປັນຈຸດທີ່ຜູ້ບຸກໂຈມຕີນຳໃຊ້ຄຳສັ່ງ SQL ເພື່ອເຈາະເຂົ້າສູ່ລະບົບຖານຂໍ້ມູນ(SQL-Injection) ຜ່ານທາງໜ້າເວບໄດ້ຖ້າບໍ່ມີການປ້ອງກັນ.

ແນວຄວາມຄິດການໂຈມຕີດ້ວຍ SQL Injection

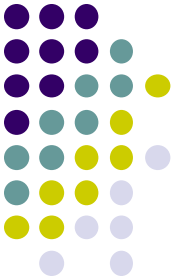


- ການໂຈມຕີດ້ວຍ SQL Injection
  - SQL Injection ເປັນຄຳສັ່ງທາງດ້ານເຕັກນິກທີ່ຜູ້ບຸກໂຈມຕີນຳໃຊ້ໃນການເຈາະເຂົ້າສູ່ລະບົບຜ່ານທາງຈຸດອ່ອນຂອງທີ່ເກີດຂຶ້ນໃນລະດັບຖານຂໍ້ມູນຂອງໂປຣແກຣມ.
  - ຈຸດອ່ອນດັ່ງກ່າວຈະສະແດງອອກມາເມື່ອຜູ້ໃຊ້ປ້ອນຂໍ້ມູນທີ່ເຮັດໃຫ້ລະບົບຜິດພາດ, ການສະແດງຂໍ້ຜິດພາດດັ່ງກ່າວຈະເປັນຊ່ອງທາງໃຫ້ຜູ້ບຸໂຈມຕີດ້ວຍຄຳສັ່ງ SQL.

ແນວຄວາມຄິດການໂຈມຕີດ້ວຍ SQL Injection



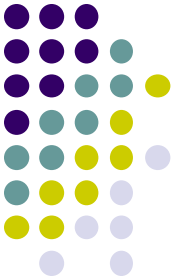
ຈຸດອ່ອນຂອງໂປຣແກຣມ(Application Vulnerability



- ຈຸດອ່ອນຂອງໂປຣແກຣມ
  - 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)

ຈຸດອ່ອນຂອງໂປຣແກຣມ(Application Vulnerability

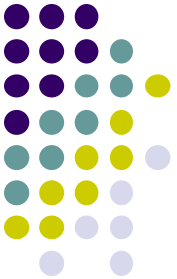
ການກວດສອບຫາຈຸດອ່ອນໂປຣແກຣມ(SQL-Inject Detection)



- ການກວດສອບຈຸດອ່ອນ
  - ນຳໃຊ້ເຄື່ອງໝາຍ ‘ ຕໍ່ທ້າຍ URL ເພື່ອໃຫ້ສະແດງຂໍ້ຜິດພາດ

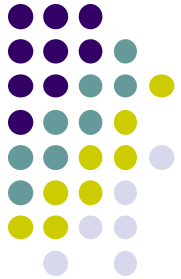
    ເຊັ່ນວ່າ: www.examplewebsite.com/index.php?id=1‘
  - ຖ້າສະແດງຂໍ້ຜິດພາດເກີດຂຶ້ນ ເຊັ່ນວ່າ: "You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right etc...“ ສະແດງວ່າ ຜູ້ໂຈມຕີສາມາດນຳໃຊ້ SQL Injection ໄດ້.

ວິທີການໂຈມຕີດ້ວຍ SQL Injection



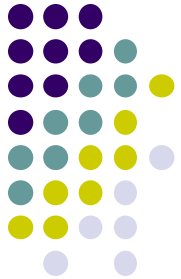
- Injected through user input.
- Injection through cookie fields contain attack strings.
- Injection through Server Variables.
- Second-Order Injection where hidden statements to be executed at another time by another function.

ປະເພດຂອງ SQL Injection



- Tautology-based SQL Injection
- Piggy-backed Queries / Statement Injection
- Union Query
- Illegal/Logically Incorrect Queries
- Inference
- Stored Procedure Injection

Tautology-based SQL Injection

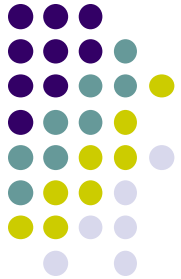


- Identify injectable parameters
- Bypass authentication
- Extract data

ເຊັ່ນວ່າ:

```
select * from user_details where userid = 'abcd' and
    password = 'anything' or 'x'='x'
```

Piggy-backed Queries / Statement Injection

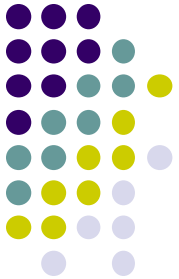


- Extract data
- Modify dataset
- Execute remote commands
- Denial of service

ເຊັ່ນວ່າ:

```
select * from user_details where userid = 'abcd' and
   password = ''; drop table xyz -- '
```

Union Query

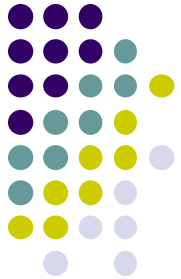


- Bypassing authentication
- Extract data

ເຊ່ນວ່າ:

```
SELECT * FROM user_details WHERE userid ="
   UNION SELECT * FROM EMP_DETAILS --
    ' and password =  'abcd'
```

Illegal/Logically Incorrect Queries



- Identify injectable parameters
- Identify database
- Extract data

ກໍລະນີສຶກສາ

- **Testing sites for vulnerabilities**

ຈຳລອງຜ່ານ http://testphp.vulnweb.com/

- ກວດສອບຊ່ອງໂວ່

http://testphp.vulnweb.com/listproducts.php?cat=1’

Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' at line 1 Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/listproducts.php on line 74

ทໍລະນີສຶກສາ

- ສະແດງຂໍ້ມູນຈຳນວນ Column ທັງໝົດດ້ວຍ Order by+ຈຳນວນໄປຈົນກວ່າສະແດງ Error.

http://testphp.vulnweb.com/listproducts.php?cat=1+order+by+10

Error: Unknown column '12' in 'order clause' Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/listproducts.php on line 74

ກໍລະນີສຶກສາ

- ສຳລັບຫ້ອງທົດລອງ ໃຫ້ເບິ່ງຂໍ້ມູນຈາກ https://infopedia.su/10x3627.html
- ຜ່ານ Web browser
- Sqlmap ຢູ່ໃນ Kali Linux
- ເຄື່ອງມື ອື່ນໆ

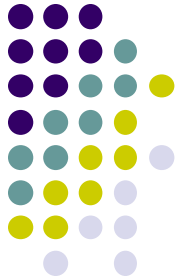
ຂໍ້ມູນອ້າງອີງ

[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

[3] https://portswigger.net/web-security/sql-injection

[4] https://infopedia.su/10x3627.html



ຖາມ ແລະ ຕອບ

ຂອບໃຈ