

# Salami slicing Attacks

gamma95@gmail.com



## OWASP

The Open Web Application Security Project



\$whoami



**OWASP**

The Open Web Application Security Project

morning

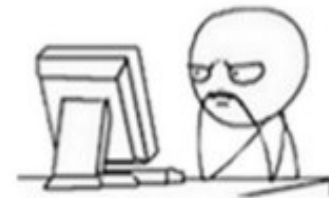


\$whoami

noon



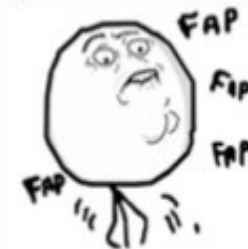
afternoon



evening



midnight



# What's salami slicing attacks?



**OWASP**

The Open Web Application Security Project

Salami slicing refers to a **series of many small actions**, often performed by **clandestine means**, that as an accumulated whole produces a much larger action or result that would be difficult or unlawful to perform all at once. The term is typically used **pejoratively**. Although salami slicing is often used to carry out illegal activities, it is only a **strategy for gaining an advantage** over time by accumulating it in small increments, so it can be used in **perfectly legal ways** as well.

In information security, a salami attack is a **series of minor attacks** that together results in a **larger attack**. Computers are ideally suited to **automating** this type of attack.



**WIKIPEDIA**  
The Free Encyclopedia

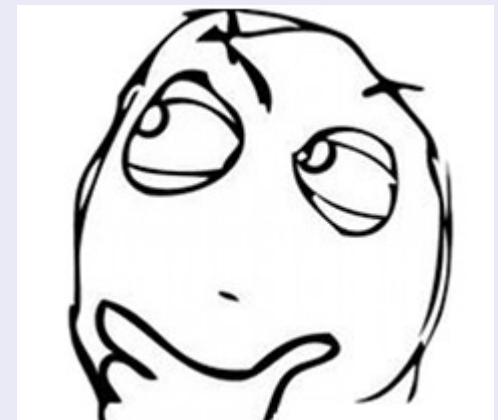


# Salami slicing How to cheat water meter



**OWASP**

The Open Web Application Security Project

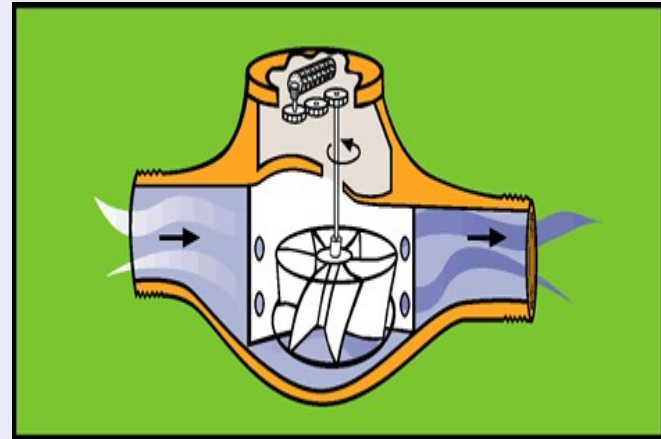
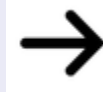


# Salami slicing How to cheat water meter



**OWASP**

The Open Web Application Security Project





# Rounding attacks



## OWASP

The Open Web Application Security Project

1 BA RUI RUI SUON 30.340d  
0,492 x 119.000d/Kg  
2 KHOAI TAY HP 450G 30.700d

---

= TONG CONG 520.460d  
So Luong mat hang : 14

---

TIEN MAT (VND) 1.000.000d  
TIEN THOI LAI =====> -479.600d

---

Voi the Uu dai, Quy khach se tinh luy  
duoc 2.602xu vao tai khoan Big Xu

---

T.Suat - GB chua co GTGT - Thue GTGT  
1> 5% 311.463 15.573  
2>10% 175.839 17.585  
Tong : 487.302 33.158

---

Th. ngan : 000151 Quay : 007  
Ticket: 007000104 01/12/2013 11:32:09

Cam on Quy khach !  
Hen gap lai !  
Website : www.bigc.vn

SKU ecwid-t-shirt1

**In stock**

**\$24.99**

---

3-4 items **\$20.99**

---

12+ items **\$11.99**

---

Save up to 52%

Qty (20 available)

**Add to Bag**

123 7890 <b>99P</b>	1234567890 J. ORTON <b>£9.99</b>	HOME GROWN PENTLAND DEL <b>25MM</b>	316 250 g SANDIACE PET SUPPLIES <b>£1.69</b>	250EC1986 <b>£9.99</b>
ALPHA ATOZ <b>£9.75</b>	SELL BY 12 SEP <b>£1.89</b>	WAS <del>£3.75</del> NOW <b>REDUCED £2.50</b>	123 789 Accent <b>£4.85</b>	AALPHABETZ INGREDIENTS: Flour, Margarine, Sugar, Essence, Baking Powder, Salt, Eggs.
REC. PRICE <del>£2.80</del> <b>£1.99</b>	CODE 1234 SUNDIAL TRADING LTD <b>£9.90</b>	95 12X02 <b>£1.89</b>	22 JAN 500 BEST BEFORE RYANS BAKERY BLAIRNEY 021-85485	REC. PRICE <del>£1.25</del> <b>TIDCO PRICE 99P</b>



### Rounding vulnerabilities

ZeroNights 2013



## Real life example

- How much do you *really* pay?
- What about:  
 $2.85\$ + 3.20\$ = 6.05\$$  ?
- How much does the seller win from rounding?
- We are a bit vulnerable...



# Rounding attacks



## OWASP

The Open Web Application Security Project

<b><i>y</i></b>	<b>round down</b> (towards $-\infty$ )	<b>round up</b> (towards $+\infty$ )	<b>round towards zero</b>	<b>round away from zero</b>	<b>round to nearest</b>
+23.67	+23	+24	+23	+24	+24
+23.50	+23	+24	+23	+24	+24
+23.35	+23	+24	+23	+24	+23
+23.00	+23	+23	+23	+23	+23
0	0	0	0	0	0
-23.00	-23	-23	-23	-23	-23
-23.35	-24	-23	-23	-24	-23
-23.50	-24	-23	-23	-24	-24
-23.67	-24	-23	-23	-24	-24



# Rounding attacks

## Ex1: Internet banking



**OWASP**

The Open Web Application Security Project

ZeroNights 2013



### Rounding vulnerabilities

## In Internet Banking apps

- Banks are vulnerable also
- Amounts are specified with two decimals:

	IBAN	Currency	Current Balance
Current Account	RO60 [redacted] 0210000001360445	EUR	0.67
Current Account	RO66 [redacted] 0210000001360434	RON	49.00

- What happens when you transfer 8.34<sup>36</sup> EUR to your account?

Amount += 8.34 EUR => **Bank wins** 0.0036 EUR

# Rounding attacks

## Ex1: Internet banking



**OWASP**

The Open Web Application Security Project

ZeroNights 2013



### Rounding vulnerabilities

## In Internet Banking apps

- Banks are vulnerable also
- Amounts are specified with two decimals:

	IBAN	Currency	Current Balance
Current Account	RO60 0210000001360445	EUR	0.67
Current Account	RO66 0210000001360434	RON	49.00

- What happens when you transfer 8.34<sup>36</sup> EUR to your account?  
Amount += 8.34 EUR => Bank wins 0.0036 EUR
- What happens when you transfer 8.34<sup>78</sup> EUR to your account?  
Amount += 8.35 EUR => **Bank loses** 0.0022 EUR
- Max to win/lose: 0.005 EUR / transaction  
Rounding is done to the closest value (two decimals)

# Rounding attacks

## Ex1: Internet banking



**OWASP**

The Open Web Application Security Project

### XE CURRENCY CONVERTER

Converter

Rates

Analysis

Info

1.00 USD = 21,120.00 VND

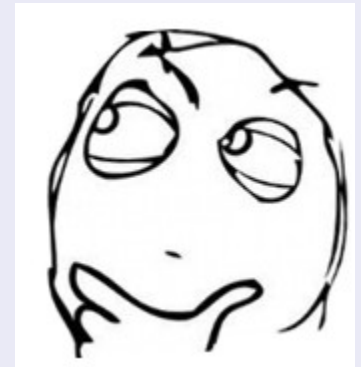


[View Chart](#)

US Dollar ↔ Vietnamese Dong  
1 USD = 21,120.00 VND      1 VND = 0.0000473485 USD

Mid-market rates: 2013-12-07 07:07 UTC

Convert  
again







# OWASP

The Open Web Application Security Project

## Rounding attacks

### XE CURRENCY CONVERTER

Converter

Rates

Analysis

Info

105.60 VND = 0.00500000 USD



View Chart

Vietnamese Dong



US Dollar

1 VND = 0.0000473485 USD

1 USD = 21,120.00 VND

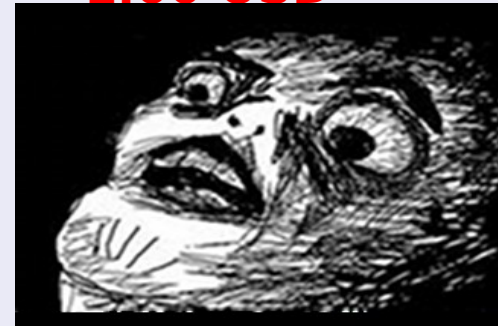
Convert  
again



Mid-market rates: 2013-12-07 06:53 UTC

$\text{Round}(0.005, 2) = 0.01 \text{ USD} = 1 \text{ cent}$

**$100 * (105.60 \text{ VND} \rightarrow 0.01 \text{ USD}) \Rightarrow 10,560.00 \text{ VND} = 1.00 \text{ USD}$**



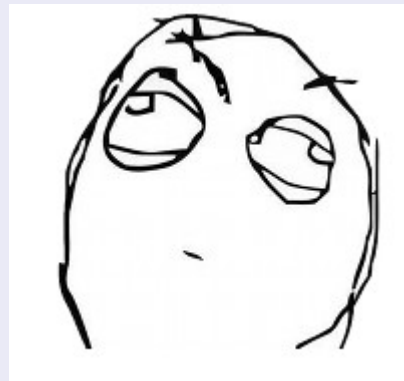
# Rounding attacks

## Ex2: Petrol station



**OWASP**

The Open Web Application Security Project



# Rounding attacks

## Ex2: Petrol station



**OWASP**

The Open Web Application Security Project



22,200.00 VNĐ --> 1 litre  
200 VNĐ --> 0.009009009...

$\text{Round}(0.00909, 2) = 0.01$  litre

**$100 * (200 \text{ VND} \rightarrow 0.01 \text{ litre}) \Rightarrow 20,000.00 \text{ VND} = 1 \text{ litre}$**





# Rounding attacks

## Ex2: Petrol station



# OWASP

The Open Web Application Security Project



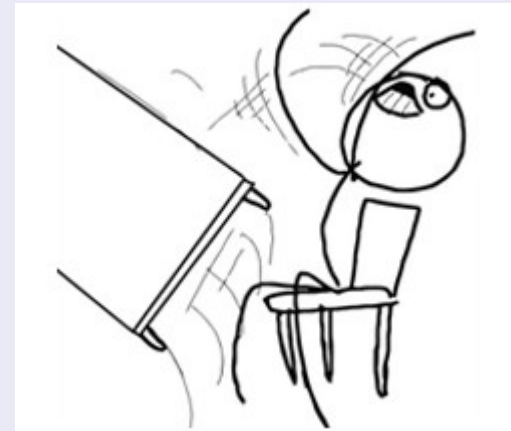
22,200.00 VNĐ

--> 1 litre

50,000.00 VNĐ

--> 2.2522522522...

$\text{Round}(2.252252, 2) = 2.25$  litre



# Rounding attacks

## Ex2: Petrol station

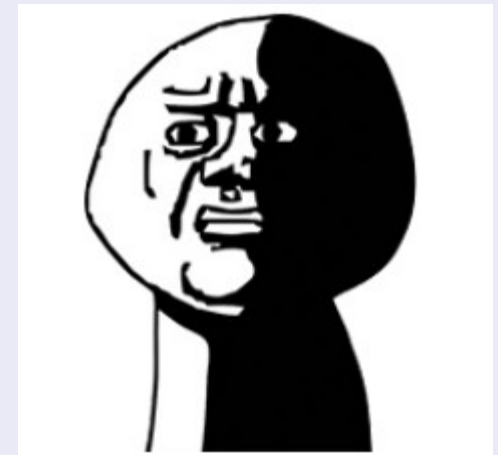


**OWASP**

The Open Web Application Security Project

In Viet Nam, Petrol station uses round down/ truncate function. That means you guys always lose :)

<b>y</b>	<b>round down (towards <math>-\infty</math>)</b>
+23.67	+23
+23.50	+23
+23.35	+23
+23.00	+23
0	0
-23.00	-23
-23.35	-24
-23.50	-24
-23.67	-24



# Deposit account Ex 3



## OWASP

The Open Web Application Security Project

Lãi suất dành cho khách hàng cá nhân			
Branch: <span>Nam Sài Gòn ▼</span>			
Kỳ hạn	VND	EUR	USD
Tiết kiệm			
Không kỳ hạn	1.20 %		0.10 %
7 ngày	1.20 %		
14 ngày	1.20 %		
1 tháng	5.00 %	0.01 %	1.20 %
2 tháng	6.50 %	0.01 %	1.20 %
3 tháng	6.80 %	0.01 %	1.20 %
6 tháng	7.00 %	0.01 %	1.20 %
9 tháng	7.00 %	0.02 %	1.20 %
12 tháng	7.50 %	0.10 %	1.20 %
24 tháng	7.75 %	0.50 %	1.20 %
36 tháng	7.75 %	0.50 %	1.20 %
48 tháng	7.75 %		
60 tháng	7.75 %	0.50 %	1.20 %

You have 100\$, you deposit 100\$ --> 1.2\$/month

You deposit **42** cents --> **0.00504\$**/month

**Round(0.00504,2) = 0.01\$ = 1 cent**/month

You should share 100\$ to 238 accounts (42 cents per account). After one month, You will get **238 x 0.01\$ = 2.38\$** :)



# References



**OWASP**

The Open Web Application Security Project

1. Salami attack at Asia Commercial Bank

<http://www.vnsecurity.net/2008/05/salami-attack-at-asia-commercial-bank/>

2. Adrian Furtuna - Practical exploitation of rounding vulnerabilities in internet banking applications

<http://2013.zeronights.org/materials>

3. Is Your Online Bank Vulnerable To Currency Rounding Attacks

<http://blog.acrossecurity.com/2012/01/is-your-online-bank-vulnerable-to.html>

4. <http://en.wikipedia.org/wiki/Rounding>



# OWASP

The Open Web Application Security Project

# Questions?

