



ความปลอดภัยคอมพิวเตอร์ (424)

OWASP : Forged Coupon ★★★★★

สำหรับนักศึกษาชั้นปีที่ 4 สาขาวิชาชีวกรรมคอมพิวเตอร์

กรุงฤทธิ์ กิติศรีวงศ์พันธุ์
Email : songrit@npu.ac.th
สาขาวิชาชีวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนគរបเม

Revised 2020-10-04

Agenda Level :



Name	Description
Arbitrary File Write	Overwrite the Legal Information file.
Forged Coupon	Forge a coupon code that gives you a discount of at least 80%.
Forged Signed JWT	Forge an almost properly RSA-signed JWT token that impersonates the (non-existing) user rsa_lord@juice-sh.op.
Imaginary Challenge	rate Solve challenge #999. Unfortunately, this challenge does not exist
Login Support Team	rate Log in with the support team's original user credentials without applying SQL Injection or any other bypass
Confidential Document	เข้าถึงไฟล์เอกสารลับ
Multiple Likes	Like any review at least three times as the same user.
Premium Paywall	Unlock Premium Challenge to access exclusive content.
SSRF	Request a hidden resource on server through server.
SSTi	Infect the server with juicy malware by abusing arbitrary command execution.
Repetitive Registration	Follow the DRY principle while registering a user.
Successful RCE DoS	Perform a Remote Code Execution that occupies the server for a while without using infinite loops.
Video XSS	Embed an XSS payload </script><script>alert('xss')</script> into our promo video.

Agenda

- **Forged Coupon** (★★★★★)
 - Forgotten Developer Backup (★★★★)
 - Forgotten Sales Backup (★★★★)

จำลองเราเป็นลูกค้า

- ร้านขายน้ำผลไม้ออนไลน์มี twitter account : @owasp_juiceshop
https://twitter.com/owasp_juiceshop/
- มีแจกคูปองอยู่เรื่อย ๆ ส่วนลด 10% , 20% บ้าง แต่ไม่มี 80%



The screenshot shows two tweets from the official Twitter account of the OWASP Juice Shop. The first tweet, posted on October 3, encourages users to enjoy 10% off all products using the coupon code pEw8pfFb1k, valid until October 31, 2020. The second tweet, posted on September 3, encourages users to enjoy 20% off all products using the coupon code q:<lrFb4l, valid until September 30, 2020. Both tweets include a small icon of a juice carton.

OWASP Juice Shop @owasp_juiceshop · Oct 3

[🤖] Enjoy 10% off all our juicy products with this #coupon code: pEw8pfFb1k (valid until 2020-10-31)

4 8

OWASP Juice Shop Retweeted

OWASP Juice Shop @owasp_juiceshop · Sep 3

[🤖] Enjoy 20% off all our juicy products with this #coupon code: q:<lrFb4l (valid until 2020-09-30)

ព័ត៌មានគុបែង

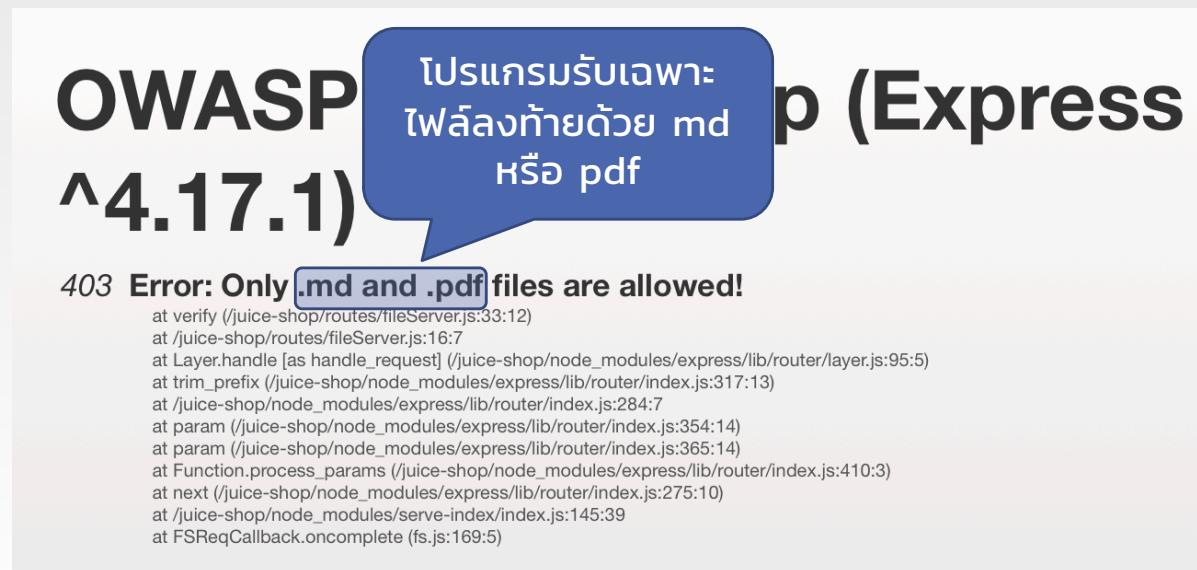
- pEw8pfFb1k (valid until 2020-10-31) 10%
- q:<IrfFb4l (valid until 2020-09-30) 20%
- k#*AgfFb1k (latest on 2020-08-31) 10%
- n(XLufFb7m (latest on 2020-07-31) 30%

Agenda

- **Forged Coupon** (★★★★★)
 - **Forgotten Developer Backup** (★★★★)
 - **Forgotten Sales Backup** (★★★★)

Forgotten Developer Backup (★★★★)

- เว็บมีไฟล์ที่โปรแกรมเมอร์ลืมลบ
- การกิจเรaha URL เก็บไฟล์เหล่านั้น
- เข้า <http://j10.dyn.npu.world/ftp> ดูไฟล์ package.json.bak



ใช้ Null byte ทำให้โปรแกรมเข้าใจผิด

- สัญลักษณ์ Null byte ใน C (\0) ใช้เป็นตัวจบ String
 - **COM-SEC-03 (E-lab)**
- ตัวอักษร Null byte ให้ string ยาวๆ ถูกตัดให้จบ

- prog1.c

```
#include <string.h>
#include <stdio.h>

void main()
{
    char src[40] = "Hello world \0 Extra string";
    char dest[40];

    strcpy(dest, src);
    printf("%s\n", dest);
}
```

Null byte ใน Javascript คือ %00

- Poison Null Byte ใน javascript ได้แก่ %00
- /package.json.bak%00.m



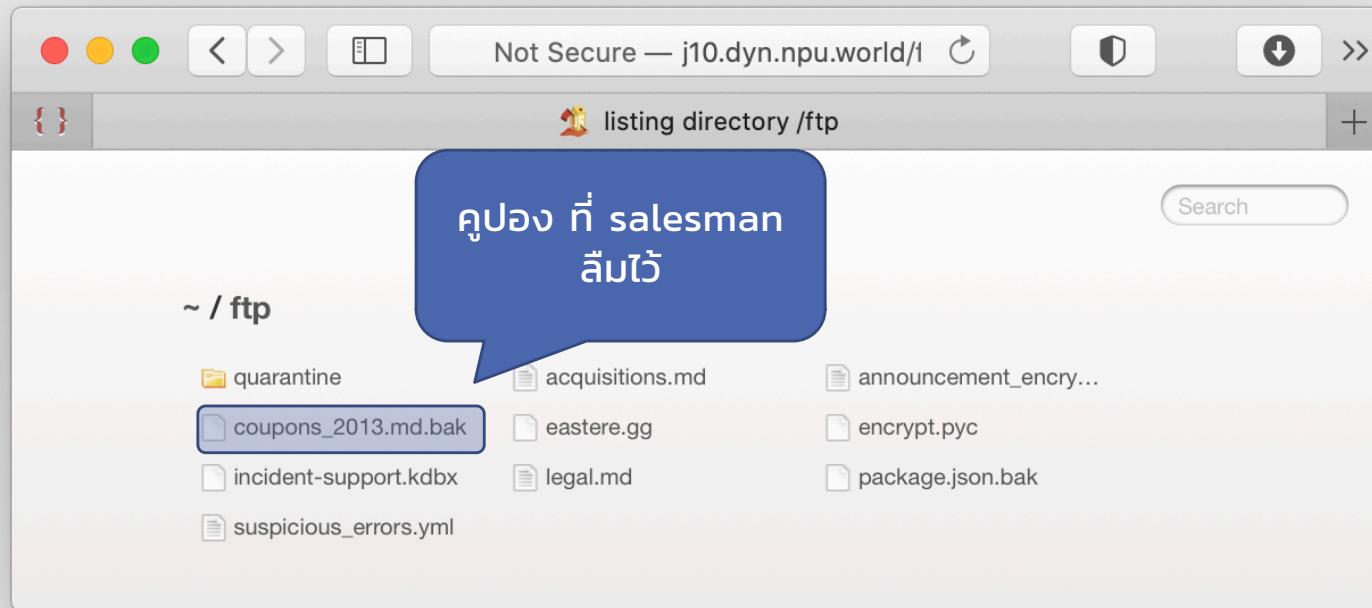
- แต่ % ส่งผ่าน URL ไม่ได้ใช้ encode URL
- package.json.bak%00.md → package.json.bak%2500.md
- http://j10.dyn.npu.world/ftp/package.json.bak%2500.md

Agenda

- **Forged Coupon (★★★★★)**
 - Forgotten Developer Backup (★★★★)
 - **Forgotten Sales Backup (★★★★)**

Forgotten Sales Backup (★★★★)

- ใช้เทคนิค Poison Null Byte
- แบบเดียวกับ Forgotten Developer Backup (★★★★)



coupons_2013.md.bak (cryptanalysis)

n<MibgC7sn

mNYS#gC7sn

o*IVigC7sn

k#pD1gC7sn

o*I]pgC7sn

n(XRvgC7sn

(XLtgC7sn

#*AfgC7sn

?:<IqgC7sn

pEw8ogC7sn

pes[BgC7sn

1}6D\$gC7ss

เดือน
ตุลาคม
ปี 2013

- มีกั้งหมด 12 โค้ด
- เชลล์น่าจะได้โค้ดทุกเดือน
- โค้ดเดือนนี้



OWASP Juice Shop @owasp_juiceshop · Oct 3

[🤖] Enjoy 10% off all our juicy products with this #coupon code:
pEw8pfFb1k (valid until 2020-10-31)

4

8

↑

- มีลงก้ายด้วย gC7rn
- มีรหัสเดียวกับลงก้ายด้วย gC7ss
 - น่าจะเป็นโค้ดให้ส่วนลดต่างเพื่อสนับสนุน
- คูปองล่าสุด pEw8pfFb1k
 - https://twitter.com/owasp_juiceshop/status/1312263933726732288

វិគ្រាមេរីម៉ាស 10 ពាក្យបាន

- 4 វាក្យបាននៅក្នុងកើតឡើងដែលបាន

ដែលបាន	Backup	តាមអ្នកបង្កើត
Jan	n<Mi bgC7sn	
Feb	mNYS#gC7sn	
Mar	o*IVigC7sn	
Apr	k#pDlgC7sn	
May	o*I]pgC7sn	
Jun	n(XRvgC7sn	
Jul	n(XLtgC7sn	n(XLuFFb7m
Aug	k#*AfgC7sn	k#*AgffFb1k
Sep	q:<IqgC7sn	q:<IrffFb41
Oct	pEw8ogC7sn	pEw8pfFb1k
Nov	pes[BgC7sn	
Dev	1}6D\$gC7ss	

pEw8pfFb1k (valid until 2020-10-31) 10%
q:<IrffFb41 (valid until 2020-09-30) 20%
k#*AgffFb1k (latest on 2020-08-31) 10%
n(XLuFFb7m (latest on 2020-07-31) 30%



pEw8pfFb1k (valid until 2020-10-31) 10%
q:<IrffFb41 (valid until 2020-09-30) 20%
k#*AgffFb1k (latest on 2020-08-31) 10%
n(XLuFFb7m (latest on 2020-07-31) 30%

เหลือส่วนที่ต้อง brute force

pEw8pfFb1k (valid until 2020-10-31)	10%
q:<IrfFb4l (valid until 2020-09-30)	20%
k#*AgfFb1k (latest on 2020-08-31)	10%
n(XLuFFb7m (latest on 2020-07-31)	30%

pEw8?ff???

- 4 ตัวอักษร ($26+26+10+33 = 95$) ตัวอักษร มี 95^4 ช่อง = 81,450,625 รูปแบบ

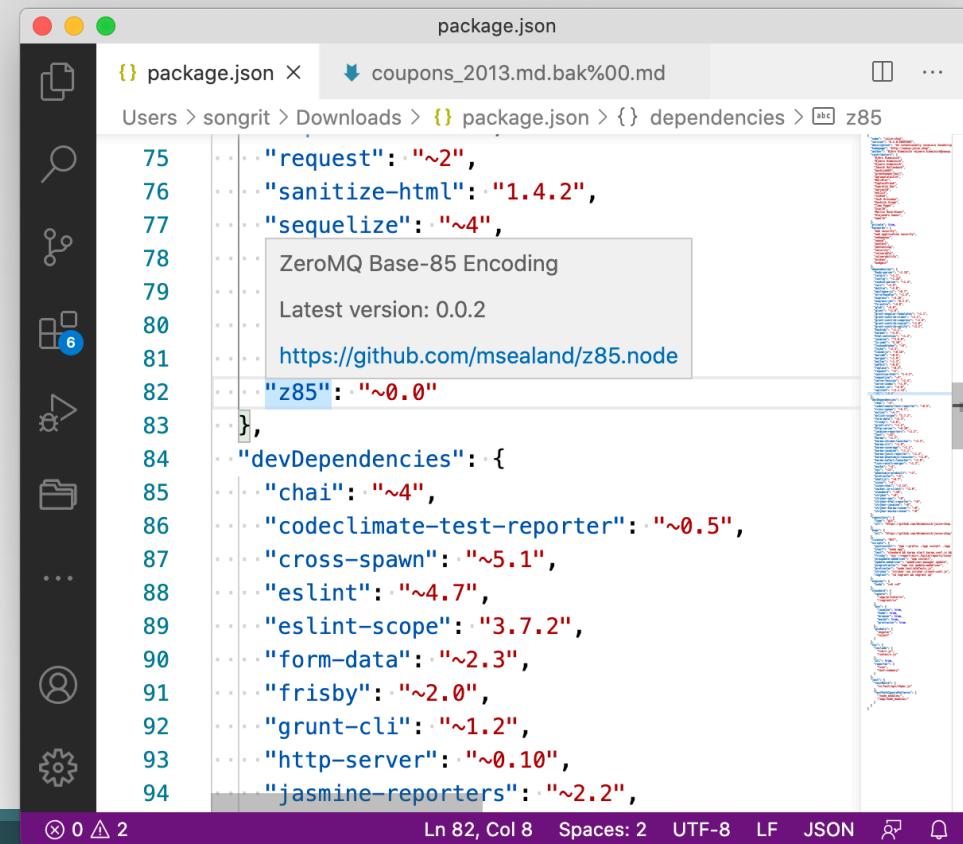
ຕັວຢ່າງໂຄດສຮ້າງຮັສ (ວິຣີນີ້ໜັກໄປ)

```
#include<stdio.h>

int main(){
    int i,j,k,l;
    for(i=33;i<127;i++)
        for(j=33;i<127;j++)
            for(k=33;i<127;k++)
                for(l=33;i<127;l++)
                    printf("ipEw8%cFF%c%c%c\n",i,j,k,l);
    return (0);
}
```

ວັດແນວຖາງ

- ຈາກ “Forgotten Developer Backup” ໃຫ້ package.json.bak



A screenshot of a code editor showing a JSON file named "package.json". The file contains a list of dependencies. A tooltip is displayed over the "z85" dependency, which is highlighted in red. The tooltip provides information about ZeroMQ Base-85 Encoding, stating "Latest version: 0.0.2" and providing a link to "https://github.com/msealand/z85.node". The code editor interface includes a sidebar with various icons and a status bar at the bottom.

```
75  "request": "^2",
76  "sanitize-html": "1.4.2",
77  "sequelize": "~4",
78  "ZeroMQ Base-85 Encoding
79  Latest version: 0.0.2
80
81  https://github.com/msealand/z85.node
82  "z85": "~0.0"
83 },
84 "devDependencies": {
85   "chai": "~4",
86   "codeclimate-test-reporter": "~0.5",
87   "cross-spawn": "~5.1",
88   "eslint": "~4.7",
89   "eslint-scope": "3.7.2",
90   "form-data": "~2.3",
91   "frisby": "~2.0",
92   "grunt-cli": "~1.2",
93   "http-server": "~0.10",
94   "jasmine-reporters": "~2.2",
```

ZeroMQ Base-85
Encoding

Z85 decoder

- สั่งเกตโค้ดคูปอง กีเครยแจก

The screenshot shows a sequence of four rectangular boxes connected by arrows, representing a flow from input to output. Each box has a blue header bar with a white circle containing a plus sign (+) on its right side.

- Box 1 (Input):** Labeled "VIEW" and "Text ▾". It contains the text "pEw8pfFb1k".
- Box 2 (Decoder):** Labeled "ENCODE DECODE" and "Ascii85 ▾". It includes a dropdown menu set to "VARIANT Z85 (ZeroMQ)". Below it, a message says "→ Decoded 8 bytes".
- Box 3 (Output):** Labeled "VIEW" and "Text ▾". It contains the text "OCT20-10".
- Box 4 (Final Output):** An empty box with a blue arrow pointing to the right.

เลือกสินค้า แล้ว checkout

