ความปลอดภัยคอมพิวเตอร์ (424)

OWASP : Forged Coupon ★★★★★★

ทรงฤทธิ์ กิติศรีวรพันธุ์

Email : songrit@npu.ac.th

สาขาวิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนครพนม

สำหรับนักศึกษาชั้นปีที่ 4 สาขาวิชาวิศวกรรมคอมพิวเตอร์

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

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

ตัวอย่างคูปอง

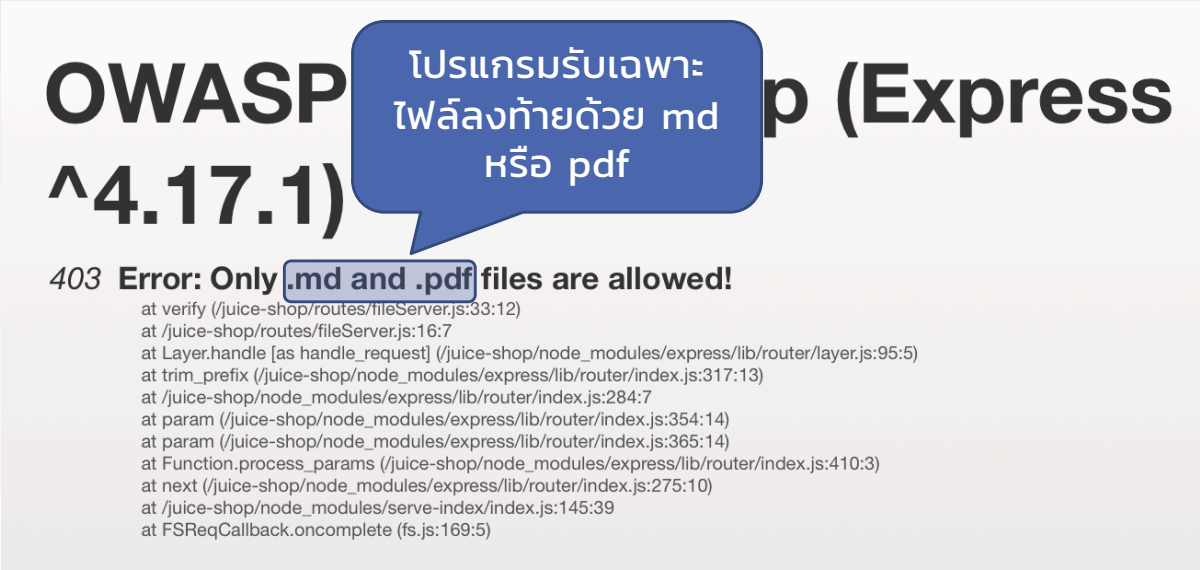
- pEw8pfFb1k (valid until 2020-10-31) 10%
- q:<IrfFb4l (valid until 2020-09-30) 20%
- k#*AgfFb1k (latest on 2020-08-31) 10%
- n(XLufFb7m (latest on 2020-07-31) 30%

Agenda

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

Forgotten Developer Backup (★★★★)

- เว็บมีไฟล์ที่โปรแกรมเมอร์ลืมลบ
- ภารกิจเราหา 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

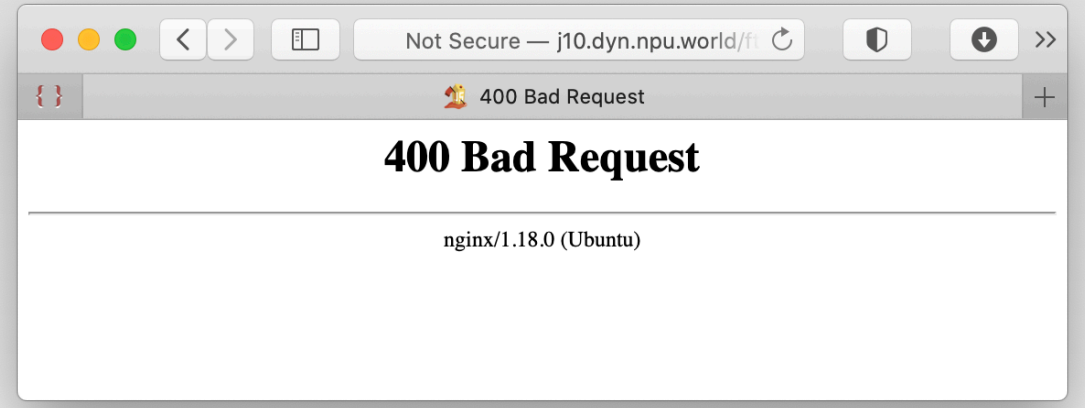
```c
#include <string.h>
#include <stdio.h>

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



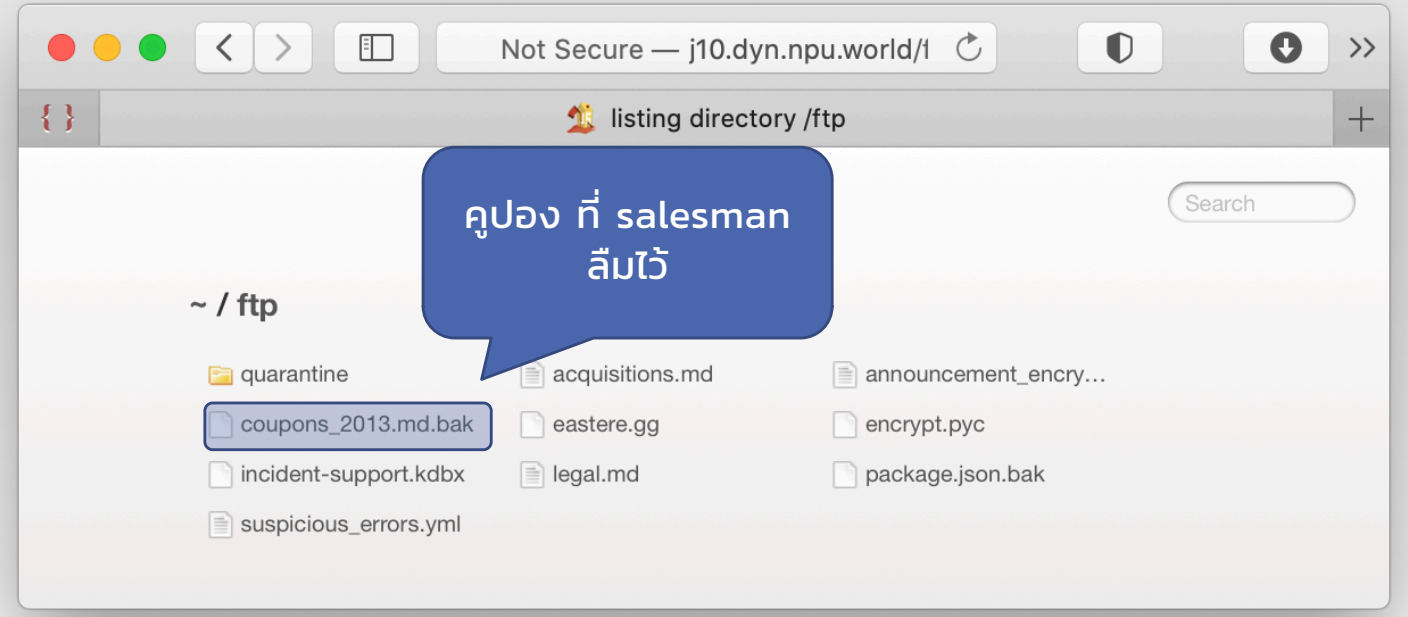
- แต่ % ส่งผ่าน URL ไม่ได้ ใช้ encode URL
- package.json.bak%00.md → package.json.bak%2500.md
- http://j10.dyn.npu.world/ftp/package.json.bak%2500.md

Agenda

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

Forgotten Sales Backup (★★★★)

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

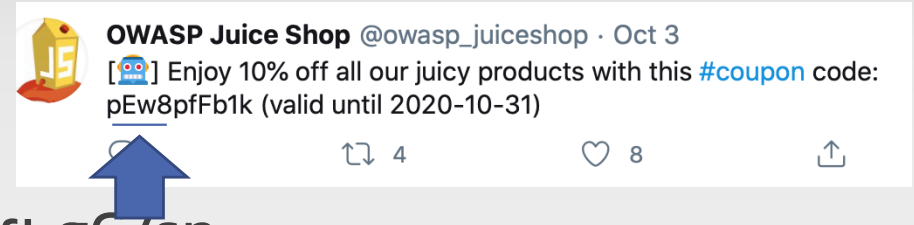


coupons_2013.md.bak (cryptanalysis)

```
n<MibgC7sn
mNYS#gC7sn
o*IVigC7sn
k#pDlgC7sn
o*I]pgC7sn
n(XRvgC7sn
(XLtgC7sn
#*AfgC7sn
q:<IqgC7sn
pEw8ogC7sn
pes[BgC7sn
l}6D$gC7ss
```

เดือนตุลาคม ปี 2013

- มีทั้งหมด 12 โค้ด
- เซลล์น่าจะได้โค้ดทุกเดือน
- โค้ดเดือนนี้



- มีลงท้ายด้วย gC7sn
- มีรหัสเดียวลงท้ายด้วย gC7ss
  - น่าจะเป็นโค้ดให้ส่วนลดต่างเพื่อน
- คูปองล่าสุด pEw8pfFb1k
  - https://twitter.com/owasp_juiceshop/status/1312263933726732288

วิเคราะห์รหัส 10 ตัวอักษร

- 4 อักษรแรกใช้แทนเดือน

เดือน	Backup	ล่าสุด
Jan	n<MibgC7sn	
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#*AgfFb1k
Sep	q:<IqgC7sn	q:<IrfFb4l
Oct	pEw8ogC7sn	pEw8pfFb1k
Nov	pes[BgC7sn	
Dev	l}6D$gC7ss	

```
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%
```


```
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%
```

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

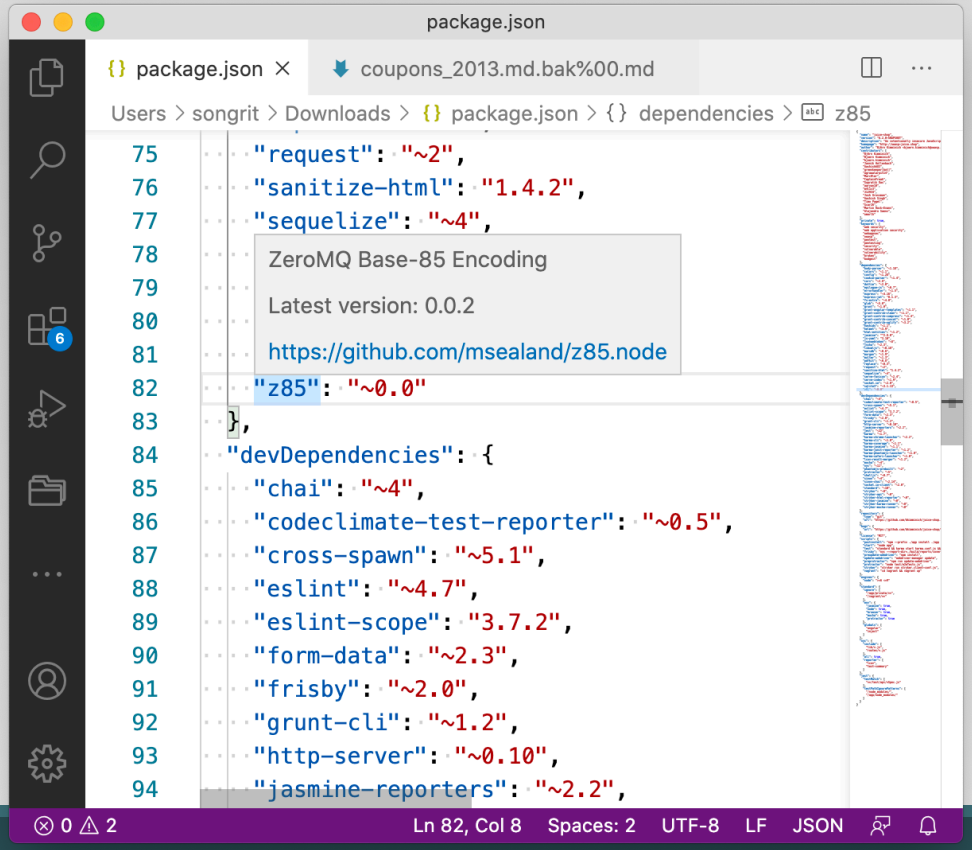
ตัวอย่างโค้ดสร้างรหัส (วิธีนี้หนักไป)

```
#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);
}
```

อีกแนวทาง

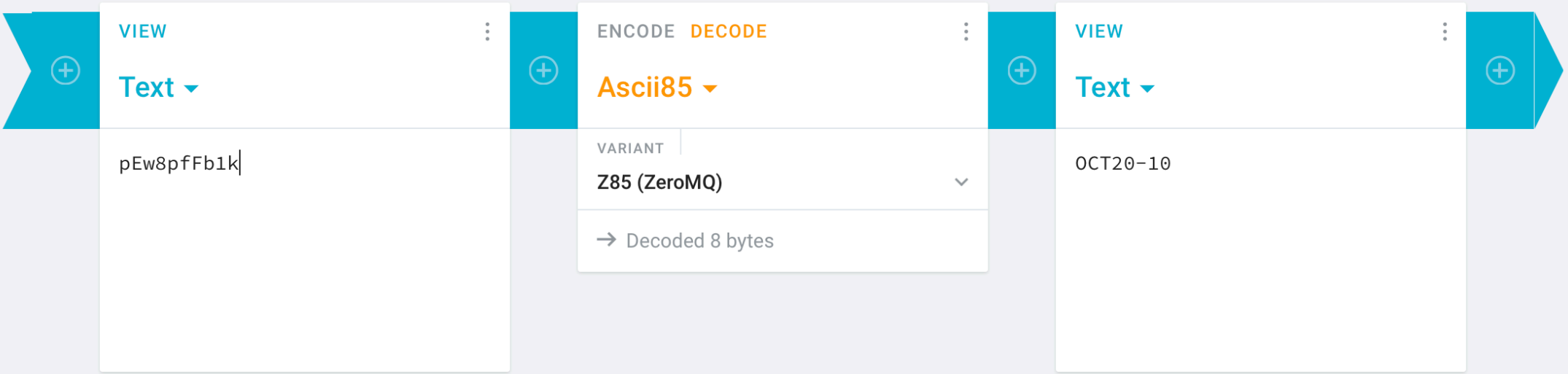
- จาก “Forgotten Developer Backup” ไฟล์ package.json.bak



ZeroMQ Base-85 Encoding

Z85 decoder

- สังเกตโค้ดคูปอง ที่เคยแจก



เลือกสินค้า แล้ว checkout