



ความปลอดภัยคอมพิวเตอร์ (424)

OWASP : Arbitrary File Write ★★★★★

สำหรับนักศึกษาชั้นปีที่ 4 สาขาวิชาวิศวกรรมคอมพิวเตอร์

กรงฤทธิ์ กิติศรีวงศ์พันธุ์

Email : songrit@npu.ac.th

สาขาวิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนครพนม

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 <code>rsa_lord@juice-shop.op</code> .
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 <code></script><script>alert('xss')</script></code> into our promo video.

Arbitrary File Write

- แก้ไขข้อความใน [Legal Information](#)
- @owasp_juiceshop เป็น twitter ลูกค้า สัมพันธ์
- ข้อความบอกรว่า
 - ลูกค้ามีความเห็นเกี่ยวกับหลายโปรดักซ์ใช่ไหม
 - เบียน complaints แต่ละโปรดักซ์ทำเสียเวลา
 - เราออกแบบระบบให้คุณทำส่งข้อความเป็น zip ไฟล์ โดยอัพโหลดได้ที่ [**/#/complain**](#)



ចំងួរ ZIP

- ឈាមរានី zip កីមិចំងួរខាងក្រោម zip slip
- <https://snyk.io/research/zip-slip-vulnerability>

Vendor	Product	Language	Confirmed vulnerable	Fixed Version	CVE	Fixed
npm library	unzipper	JavaScript	YES	0.8.13	CVE-2018-1002203	17/4/2018
npm library	adm-zip	JavaScript	YES	0.4.9	CVE-2018-1002204	23/4/2018
Java library	codehaus/plexus-archiver	Java	YES	3.6.0	CVE-2018-1002200	6/5/2018
Java library	zeroturnaround/zt-zip	Java	YES	1.13	CVE-2018-1002201	26/4/2018
Java library	zip4j	Java	YES	1.3.3	CVE-2018-1002202	13/6/2018
.NET library	DotNetZip.Semverd	.NET	YES	1.11.0	CVE-2018-1002205	7/5/2018

ช่องโหว่ ZIP slip

- เกิดเมื่อคลายไฟล์ zip กี่ไฟล์กрайในมีการอ้างอิงตำแหน่งໄດ້ເຮັດວຽກນອກ
- https://www.youtube.com/watch?v=Ry_yb5Oipq0

```
5 Tue Jun 5 11:04:29 BST 2018 good.sh  
20 Tue Jun 5 11:04:42 BST 2018 ../../../../../../tmp/evil.sh
```



ช่องโหว่ ZIP slip

Directory traversal

- Windows

```
cd \windows\system32  
cd ..\..\users
```

- Unix / Linux / MacOS

```
cd /user/local/bin  
cd ../../../../../home/u1
```

ช่องโหว่ ZIP slip

- เมื่อใส่ไฟล์ภายใน zip โดยอ้างคำแนะนำจาก directory traversal
- จะทำให้วางไฟล์ในไดเรกทอรีใดก็ได้ในระบบปฏิบัติการ
- ด้วยสิทธิ์เท่ากับ users ที่คุณยกzip นั้น
- มีไดเรกทอรีที่ทุกคนสามารถเขียน-อ่านได้
 - ls -l /

```
drwxrwxrwt 18 root root 16384 Oct 5 18:09 tmp
```

Permission 777

ตำแหน่งไฟล์ legal.md

- <http://j10.dyn.npu.world/ftp/legal.md>
- แอกເກອຣີໄມ່ກຮາບຕຳແຫນ່ງໄຟລ໌ເລັ້ງວັພໂຮດໄຟລ໌ຂຶ້ນ server
- ຕົວຢ່າງ ອາຈະອຍຸກໍ
 - <http://j10.dyn.npu.world/upload/2020/exploit.md>
 - ເນື່ອ
 - <http://j10.dyn.npu.world/upload/exploit.md>
 - <http://j10.dyn.npu.world/exploit.md>
 - <http://j10.dyn.npu.world/ftp/exploit.md>

สร้างไฟล์ legal.md

- ใช้ path (../../)
- สร้างไฟล์ legal.md ใหม่

```
mkdir -p ../../ftp  
echo "Hacked by CPE" > ../../ftp/legal.md  
zip complain.zip ../../ftp/legal.md
```

ເພົ່າ /#/complain

