# 11. Module - SSRF

## Abusing Intermediate Devices

Breaking Parser Logic - Take Your Path Normalization Off and Pop 0days Out (blackhat.com)

to acces the hidden Tomcat manager
-> `..;/` instead of `../`
-> ajp proxy (runs on port 8009), ajp13 is a binary protocol and it might be a gateway to internal resources like admin panels. You can configure your own Apache instance to connect to a remote ajp port and then visit http://127.0.0.1

**To connect to remote ajp port:**

> `apt-get install apache2` && `apt install libapache2-mod-jk` && `a2enmod proxy_ajp`

then create a file here `/etc/apache2/sites-enabled/ajp.conf`

```
ProxyRequests Off
# Only allow localhost to proxy requests
<Proxy *>
Order deny,allow
Deny from all
Allow from localhost
</Proxy>
# Change the IP address in the below lines to the remote servers IP address hosting the
Tomcat instance
ProxyPass / ajp://[TARGETIP]:8009/
ProxyPassReverse / ajp://[TARGETIP]:8009/
```

## Server-Side Request Forgery (SSRF)