Nostromo Web Server From Path Traversal to RCE - CVE-2022-48253

PATH-TRAVERSAL DIRECTORY-TRAVERSAL RCE LOCAL-FILE-INCLUSION

Riccardo Krauter
12/01/2023

Share:

TL;DR: Vi raccontiamo una delle nostre ricerche: CVE-2022-48253 - Directory Traversal su Nostromo Web Server (nhttpd), se configurato con l'opzione "HOMEDIRS"; l'exploit può portare a Remote Command Execution.

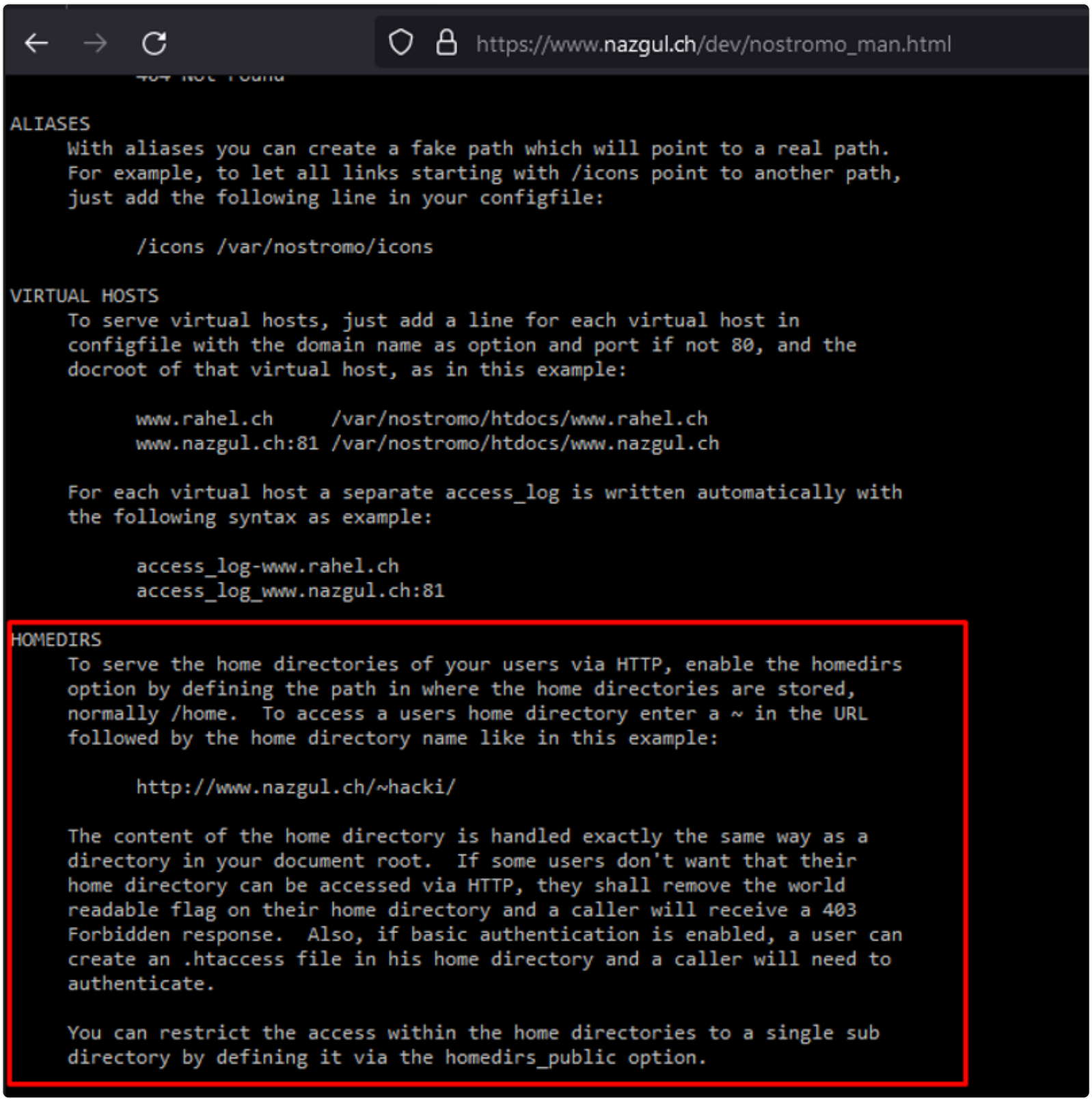
Nostromo Web Server From Path Traversal to RCE with the help of “HOMEDIRS” config - CVE-2022-48253

Introduzione

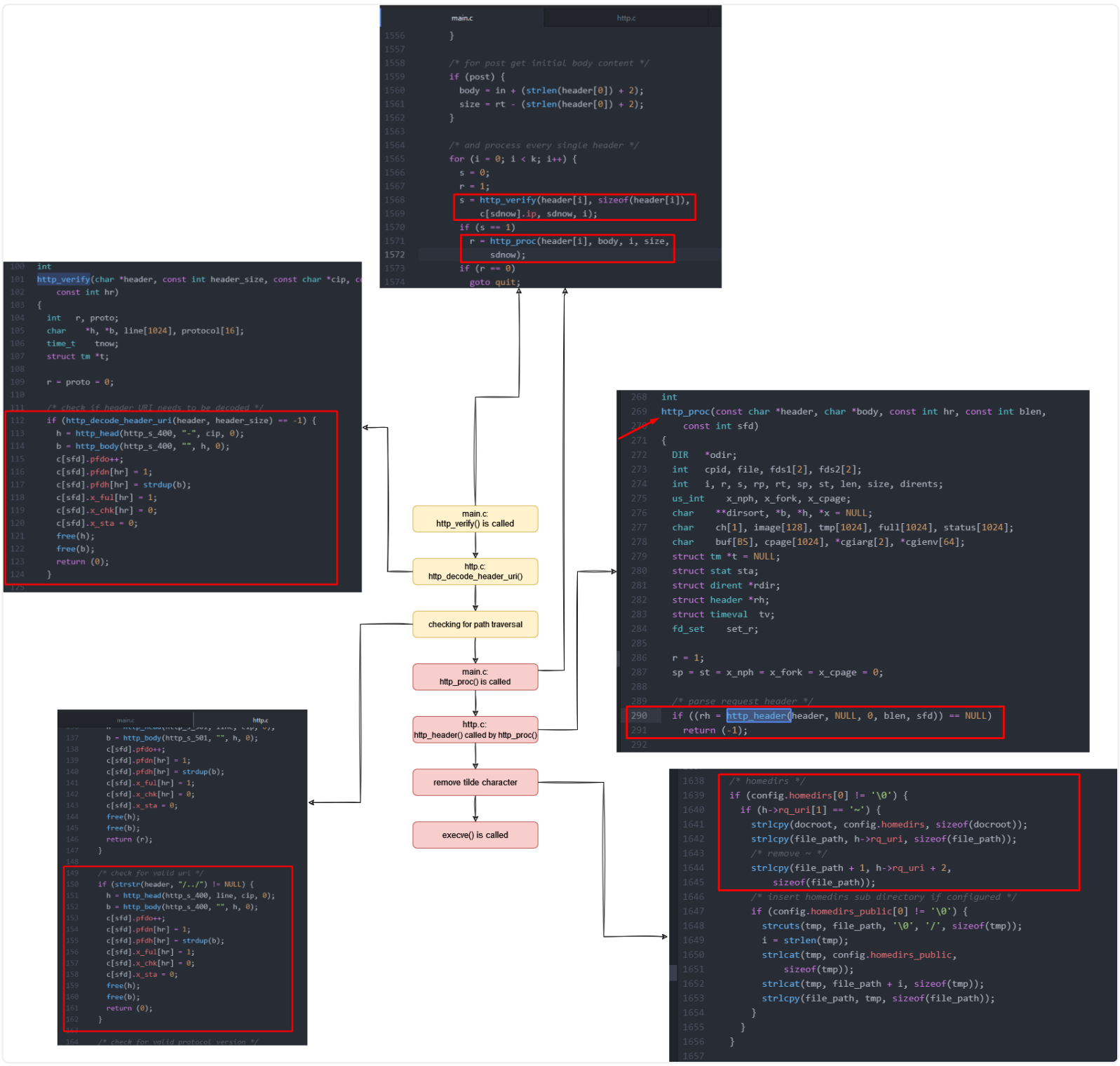
Oggi vi vogliamo parlare della ricerca svolta da Riccardo ‘p4w’ Krauter, su **Nostromo Web Server** che ha portato al **CVE-2022-48253**. La vulnerabilità è sfruttabile se il server viene configurato con l’opzione “HOMEDIRS” e si tratta di un **Path Traversal** che può portare a **RCE**. La vulnerabilità affligge le versioni di Nostromo <= 2.0.

Discovering

La ricerca è partita dall’analisi di vecchie vulnerabilità. In passato, **Nostromo** era vulnerabile a **Path Traversal** che poteva portare all’esecuzione di comandi, i CVE correlati sono CVE-2011-0751 e CVE-2019-16278. Partendo da questi risultati la domanda è stata: esiste ancora qualche flusso inesplorato di **Path Traversal**? La risposta a questa domanda è sì, ed è arrivata grazie alla ricerca condotta da p4w, che ha portato alla scoperta di una nuova vulnerabilità su **Nostromo**. Leggendo la documentazione di **Nostromo**, risulta curiosa l’opzione “HOMEDIRS”, riportiamo di seguito uno screenshot del manuale che spiega a cosa serve tale opzione.



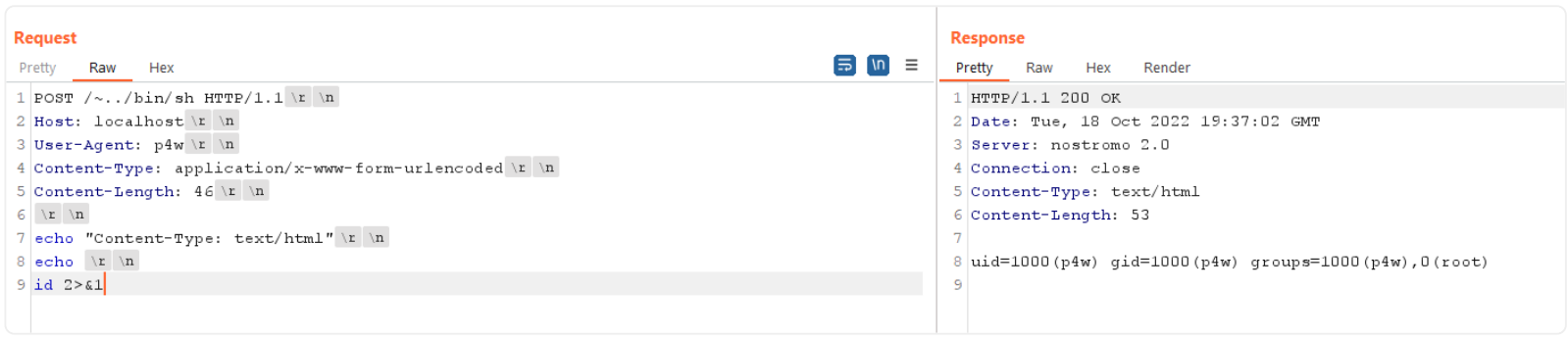
Questa opzione è interessante, in quanto intuitavamente ci si aspetta che il normale flusso del codice entri in una diramazione che eseguirà qualche sorta di manipolazione sull'input controllabile da un utente (in particolare sulla Request-URI contenuta nella richiesta HTTP). Questo perchè l'opzione sembra che in qualche modo associ una URI che inizia con il carattere `~` con una directory scelta, ma la domanda è: come lo fa? Una delle cose più importanti per la discovery della vulnerabilità è stata la comprensione del flusso del codice che gestisce le richieste HTTP. A tal proposito, l'immagine sottostante racchiude i passaggi chiave del codice che si occupa di elaborare una richiesta HTTP quando il server viene configurato per usare l'opzione "HOMEDIRS".



Osservando il flusso, è possibile notare che il carattere `~` viene rimosso dopo il controllo di sicurezza che cerca il pattern `/../` per evitare problemi di **Path Traversal**. Sembra quindi possibile aggirare il controllo con questo payload `/~../`. Facciamo un esempio e ripercorriamo il flusso. Se l'opzione **HOMEDIRS** punta alla directory `/home` del file system (come suggerito nel manuale) e l'URI richiesta fosse `/~../bin/sh`, allora il flusso sarà il seguente:

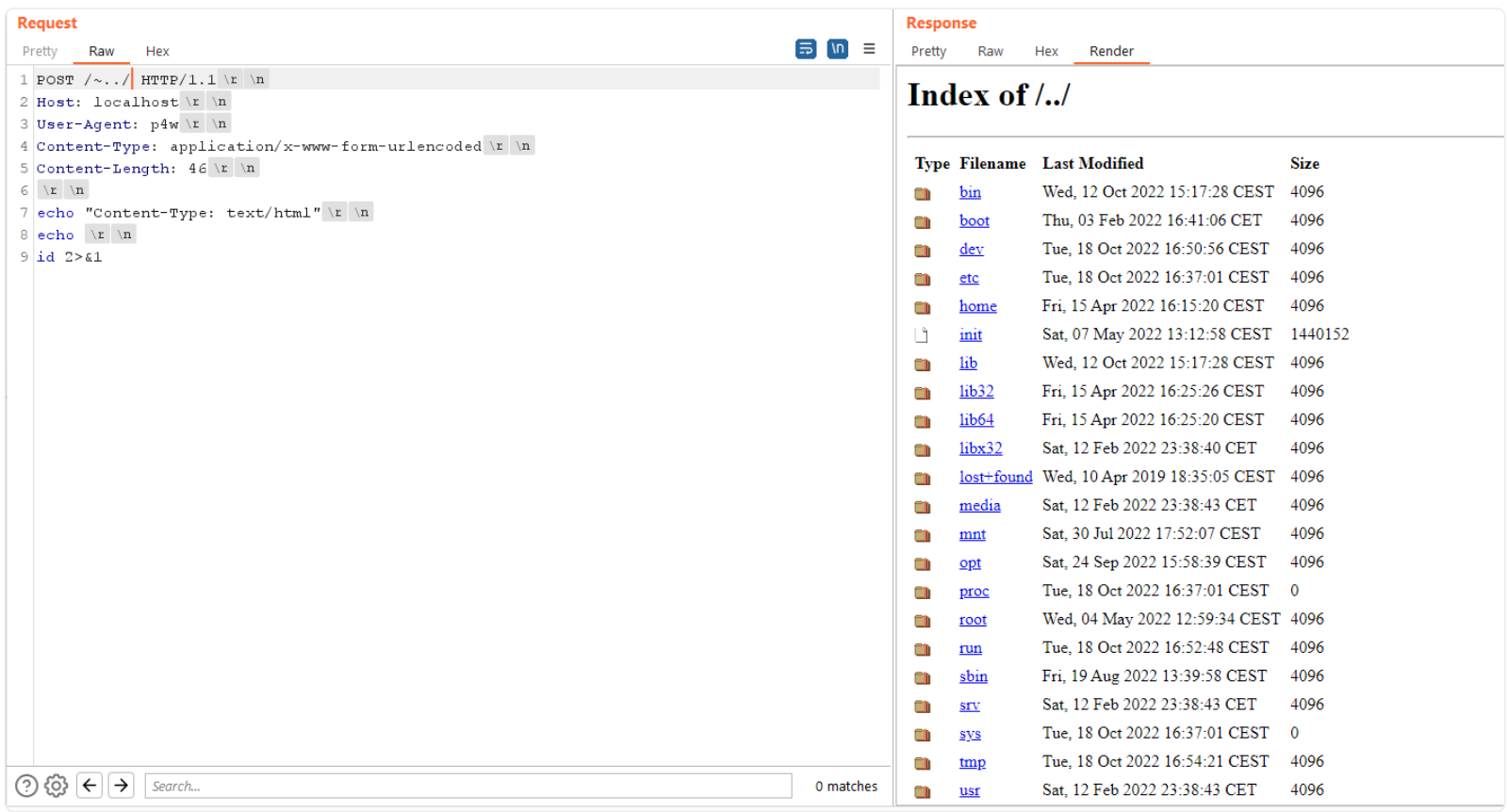
- il server chiama la funzione `http_verify()`, decodifica tutti gli header e poi controlla la presenza del pattern `/../`, che non verrà trovato visto che il percorso URI richiesto è il seguente `/~../bin/sh`;
- il server chiama poi la funzione `http_proc()` che, a sua volta, richiama la funzione `http_header()`, responsabile della cancellazione del `~` dall'URI richiesta, che diventa `/../bin/sh`;
- ora il server concatena la stringa `/../bin/sh` con la directory `/home` scelta da configurazione. La risorsa finale che il server andrà a recuperare sarà la seguente `/home/../bin/sh`;
- nell'ultimo step il server controlla se la risorsa richiesta sia un file eseguibile e in caso affermativo viene richiamata la syscall `execve("/home/../bin/sh")` che può essere utilizzata per eseguire comandi arbitrari sul server.

Di seguito uno screenshot con un **PoC di RCE** su un server di test installato in locale (come è possibile osservare negli header di risposta la versione di Nostromo usata è la 2.0).

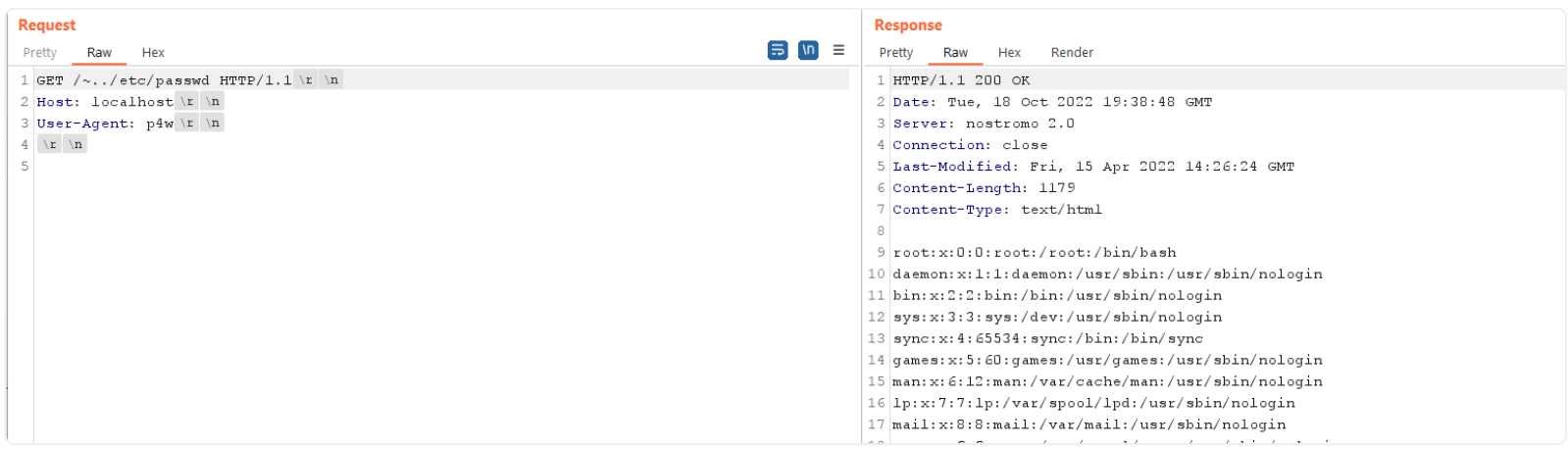


Impatti e limitazioni

Abbiamo già visto come, nel caso peggiore, la vulnerabilità può essere sfrutatta per eseguire comandi arbitrari sul server. Ora vediamo anche quali sono le limtazioni dell'exploit. La prima limitazione è che la vulnerabilità è presente solo se il server viene configurato per utilizzare l'opzione **HOMEDIRS**. Questa condizione riduce sicuramente il numero dei server Nostromo vulnerabili. Il **Path Traversal** è limitato ad una directory indietro. Di conseguenza non è possibile "traversare" più di una directory, nonostante ciò se la directory usata come configurazione risulta solo un livello sopra al punto di mount del file system, allora è possibile navigare l'intero file system come mostra lo screenshot seguente.



Un'altro impatto è la semplice lettura di file al di fuori della web-root directory come mostrato di seguito.



Anche se il server usasse più di un livello per la directory "home", ad esempio `/usr/nostromo`, la vulnerabilità può essere utlizzata per ottenere la disclosure di file potenzailmente sensibili (ad esempio file di configurazione, file di sistema, chiavi ssh ecc.).

Disclosure Timeline

- 18/10/2022: Scoperta la vulnerabilità su Nostromo
- 24/10/2022: Contattato Marcus Glocker, principale sviluppatore del progetto nhttpd e condiviso con lui un report dettagliato sulla vulnerabilità
- 14/12/2022: Rilasciato il fix con la versione 2.1 di Nostromo (https://nazgul.ch/dev/nostromo_cl.txt)

Reference

- https://nazgul.ch/dev/nostromo_cl.txt
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-48253
- https://www.sudokaikan.com/2019/10/cve-2019-16278-unauthenticated-remote.html
- https://portswigger.net/daily-swig/nostromo-web-servers-exposed-by-resurrected-rce-vulnerability