* Analisi Metodi HTTP
* Il nostro gruppo ha elaborato un codice che ci permetta di sapere quali metodi sono ammessi nell’ HTTP sul Web Server aziendale.

Effettuando una scansione dei metodi ammessi abbiamo ottenuto i risultati elencati.

Con il system target intende l’IP del server.



* Analizzando il codice possiamo affermare che i metodi GET, PATCH, OPTIONS, HEAD, TRACE sono ammessi correttamente, senza creare vulnerabilità.

L’ammissione dei seguenti metodi POST, DELETE, PUT permettono a utenti esterni di abusare impropriamente dei dati senza autenticazioni richieste.

Mentre il metodo CONNECT non viene ammesso dal server.

* GET: Questo metodo permette di richiedere informazioni dal server agli utenti senza modificare i dati contenuti.
* PATCH: Viene utilizzato per aggiornare parzialmente una risorsa esistente, andando a modificare le informazioni necessarie.
* OPTIONS: Consente di ottenere informazioni sui metodi concessi dal server per una determinata risorsa.
* HEAD: Con lo stesso funzionamento del GET ma senza restituire il corpo della risposta.
* TRACE: Permette di visualizzare le modifiche apportate ad esempio al firewall e di facilitare il debugging o i troubleshooting.

I metodi erroneamente ammessi sono:

* POST: Fa si che un utente possa aggiungere dati al server compromettendone l’integrità.
* DELETE: La più rischiosa che consente l’eliminazione delle risorse del server.
* PUT: Il comando rimpiazza le risorse eseguendo un aggiornamento completo.

Metodo correttamente non ammesso:

* CONNECT: Ammettere questo metodo poteva rappresentare un rischio di sicurezza se non strettamente controllato, in quanto potrebbe consentire connessioni indesiderate.