Capitolo 4

Configurare l'ambiente e intercettare il traffico

Vi risparmierete un sacco di tempo e mal di testa se cercate bug all'interno di un laboratorio ben configurato. In questo capitolo, vi guiderò, passo dopo passo, attraverso l'impostazione del vostro ambiente di hacking.

Configurerete il browser in modo che funzioni con Burp Suite, un proxy web che vi consente di visualizzare e modificare le richieste e le risposte HTTP scambiate tra il vostro browser e i server web. Imparerete a utilizzare le funzionalità di Burp per intercettare il traffico web, a inviare richieste automatiche e ripetute, a decodificare contenuti codificati e a confrontare richieste. Parlerò anche di come prendere buoni appunti sui bug trovati.

Questo capitolo si concentra sulla configurazione di un ambiente specifico per l'hacking web. Se il vostro target è attaccare app per dispositivi mobili, avrete bisogno di configurazioni e strumenti aggiuntivi. Ne parleremo nel Capitolo 23, che tratta dell'hacking di applicazioni per dispositivi mobili.

In questo capitolo

- **Scegliere un sistema operativo**
- **Configurare gli elementi essenziali: un browser e un proxy**
- **Usare Burp**
- **Un appunto finale sul... prendere appunti**

Scegliere un sistema operativo

Prima di procedere, la prima cosa che dovete fare è scegliere un sistema operativo. Il vostro sistema operativo limiterà gli strumenti di hacking a vostra disposizione. Consiglio di utilizzare un sistema basato su Unix, come Kali Linux o macOS, perché molti strumenti di hacking open source sono scritti per questi sistemi. *Kali Linux* è una distribuzione Linux progettata per l'ambiente *digital forensics* e per l'hacking. Include molti utili strumenti di caccia ai bug,

come *Burp Suite*, strumenti di ricognizione come *DirBuster* e *Gobuster* e fuzzer come *Wfuzz*. Potete scaricare Kali Linux da `https://www.kali.org/downloads`.
Se queste opzioni non fanno per voi, siete liberi di utilizzare altri sistemi operativi per l'hacking. Tenete presente che però potreste dover imparare a utilizzare strumenti diversi da quelli menzionati in questo libro.

Configurare gli elementi essenziali: un browser e un proxy

Successivamente, avrete bisogno di un browser web e di un proxy web. Utilizzerete il browser per esaminare le funzionalità di un'applicazione target. Vi consiglio di utilizzare *Firefox*, poiché è il più semplice da configurare con un proxy. Potete anche utilizzare due browser differenti durante l'hacking: uno per esplorare il target e uno per ricercare vulnerabilità su Internet. In questo modo, potrete isolare più facilmente il traffico della vostra applicazione target per ogni ulteriore esame.
Un *proxy* è un software "intermediario" che si colloca tra un client e un server; in questo caso, si trova tra il vostro browser e i server web con cui interagirete. Intercetta le vostre richieste prima di passarle al server e intercetta le risposte del server prima di passarvele, nel seguente modo:

Browser <----------> Proxy <----------> Server

L'uso di un proxy è essenziale nella caccia ai bug. I proxy vi consentono di visualizzare e modificare le richieste in uscita verso il server e le risposte in arrivo nel vostro browser, come spiegherò più avanti in questo stesso capitolo. Senza un proxy, il browser e il server si scambierebbero messaggi automaticamente e a vostra insaputa, e l'unica cosa che vedreste sarebbe la pagina web finale risultante. Un proxy catturerà invece tutti i messaggi prima che raggiungano il destinatario previsto.
I proxy, pertanto, consentono di eseguire la ricognizione esaminando e analizzando il traffico in entrata e in uscita dal server. Consentono inoltre di esaminare richieste interessanti, per cercare potenziali vulnerabilità e sfruttarle, alterando le richieste.
Per esempio, supponiamo che visitiate la vostra casella di posta elettronica e intercettiate con un proxy la richiesta che restituirà la vostra posta. È una richiesta `GET` a un URL che contiene il vostro ID utente. Notate, inoltre, che nella richiesta è incluso un cookie con il vostro ID utente:

```
GET /emails/USER_ID HTTP/1.1
Host: example.com
Cookie: user_id=USER_ID
```

In questo caso, potete provare a modificare lo `USER_ID` nell'URL e l'intestazione `Cookie` con l'ID di un altro utente e vedere se potete accedere all'email di qualcun altro. Due proxy sono particolarmente apprezzati dai cacciatori di bug: *Burp Suite* e *Zed Attack Proxy* (*ZAP*). Questa parte del capitolo vi mostrerà come configurare Burp, ma siete liberi di usare anche ZAP.

Aprire il browser embedded

Sia Burp Suite sia ZAP sono dotati di un loro browser interno (*embedded*). Se per il test scegliete di utilizzare questi browser embedded, potete saltare i due passaggi successivi. Per utilizzare il browser embedded di Burp Suite, fate clic su *Open browser* nella scheda *Proxy* di Burp (Figura 4.1). Il traffico di questo browser embedded verrà automaticamente instradato attraverso Burp senza alcuna configurazione aggiuntiva.

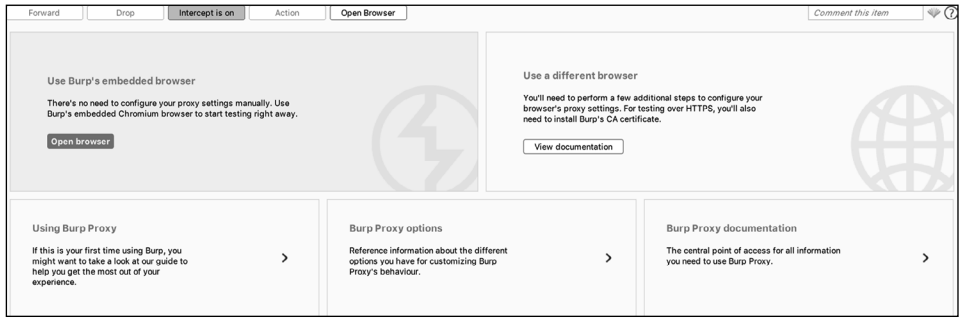

Figura 4.1 Potete utilizzare il browser embedded di Burp invece del vostro browser esterno per i test.

Configurare Firefox

Il browser embedded di Burp offre un modo comodo per iniziare la ricerca di bug con una configurazione minima. Tuttavia, se, come me, preferite provare con un browser cui siete abituati, potete configurare Burp in modo che funzioni in combinazione con il vostro browser. Configuriamo Burp in modo che funzioni con Firefox.

Iniziate scaricando e installando il browser e il proxy. Potete scaricare il browser Firefox da `https://www.mozilla.org/firefox/new` e Burp Suite da `https://portswigger.net/burp`.

I cacciatori di bug utilizzano una delle due versioni disponibili di Burp Suite: Professional o Community. Dovete acquistare una licenza per utilizzare Burp Suite Professional, mentre la versione Community è gratuita. Burp Suite Professional include uno scanner di vulnerabilità e altre utili funzionalità, come l'opzione per salvare una sessione di lavoro per riprenderla in seguito. Offre anche una versione completa dell'intruder Burp, mentre la versione Community include solo una versione limitata. In questo libro, utilizzeremo la versione *Community* per la caccia ai bug.

Ora dovete configurare il vostro browser per instradare il traffico attraverso il vostro proxy. Questa parte del capitolo spiega come configurare Firefox per lavorare con Burp Suite. Se state utilizzando un'altra combinazione di browser e proxy, consultate la loro documentazione ufficiale.

Avviate Firefox. Quindi aprite la pagina Connection Settings (Impostazioni connessioni) scegliendo *Preferences* > *General* > *Network Settings* (*Preferenze* > *Generale* > *Impostazioni di rete*). Potete accedere alla scheda *Preferences* (*Preferenze*) dal menu nell'angolo superiore destro della finestra di Firefox (Figura 4.2).

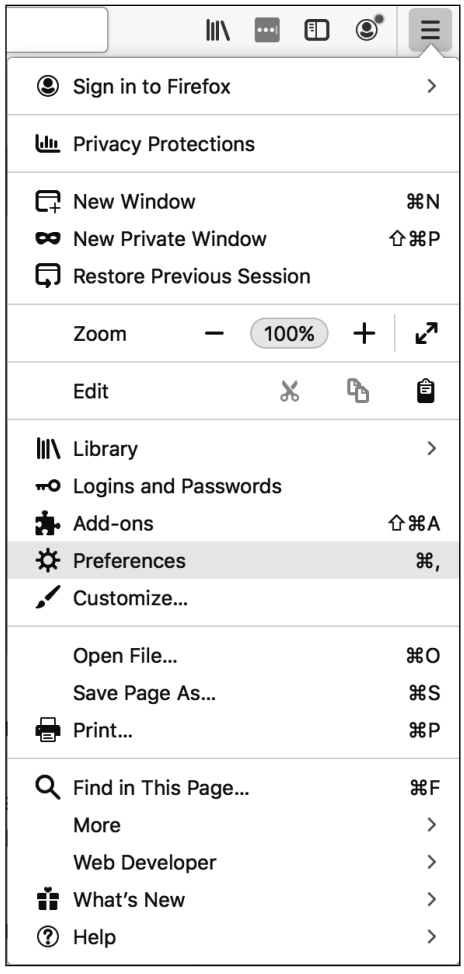

Figura 4.2 Trovate l'opzione Preferences (Preferenze) nell'angolo superiore destro della finestra di Firefox.

La pagina *Connection Settings* (*Impostazioni di connessione*) dovrebbe essere simile a quella rappresentata nella Figura 4.3.
Selezionate *Manual proxy configuration* (*Configurazione proxy manuale*) e inserite l'indirizzo IP `127.0.0.1` e la porta `8080` per tutti i tipi di protocollo. Questo dirà a Firefox di utilizzare come proxy per tutto il suo traffico il servizio in esecuzione sulla porta 8080 della vostra macchina. L'indirizzo IP 127.0.0.1 è quello dell'host locale. Identifica il vostro computer, quindi potete usarlo per accedere ai servizi di rete in esecuzione sulla vostra macchina. Poiché Burp viene eseguito per default sulla porta 8080, questa impostazione chiede a Firefox di instradare tutto il suo traffico attraverso Burp. Fare clic su *OK* per applicare l'impostazione. Ora Firefox instraderà tutto il traffico attraverso Burp.

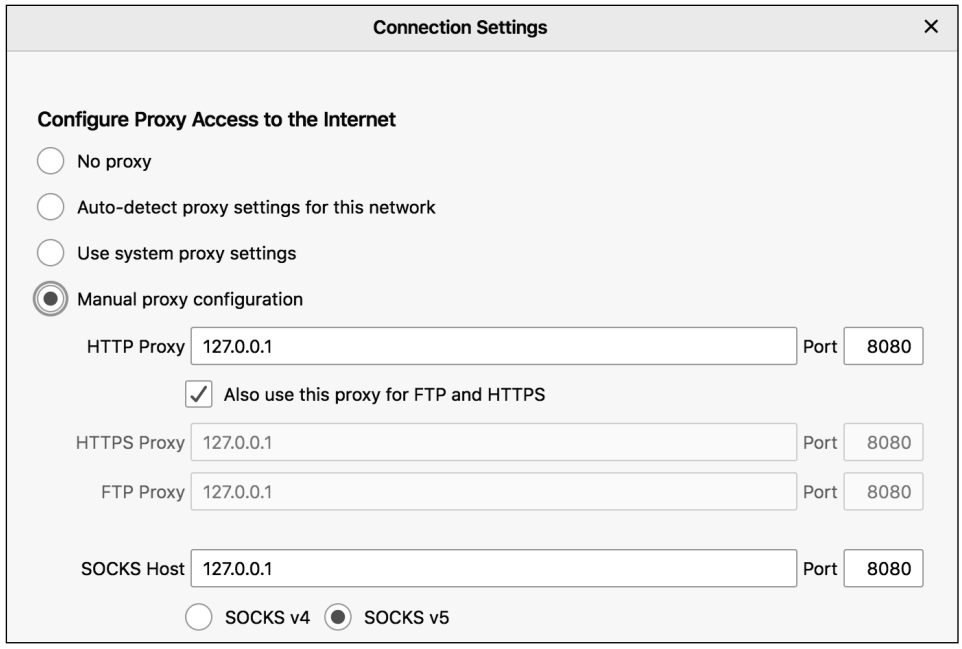

Figura 4.3 Configurate le impostazioni proxy di Firefox nella pagina Connection Settings (Impostazioni connessione).

Configurare Burp

Dopo aver scaricato Burp Suite, apritelo e fate clic su *Next*, quindi su *Start Burp*. Dovreste vedere una finestra come quella rappresentata nella Figura 4.4.

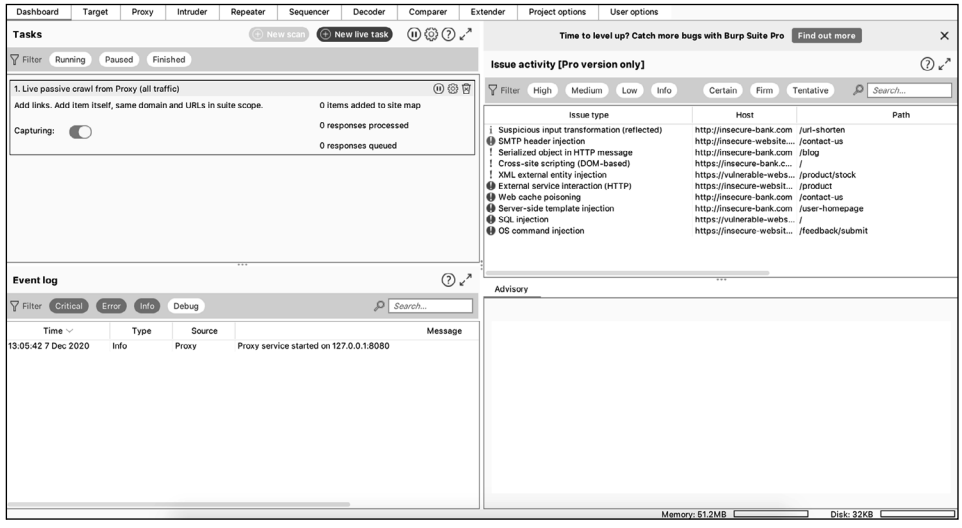

Figura 4.4 Finestra di avvio di Burp Suite Community Edition.

Ora, configuriamo Burp in modo che possa funzionare con il traffico HTTPS. HTTPS protegge la privacy dei dati crittografando il traffico, assicurandovi quindi che solo le due parti in comunicazione (il vostro browser e il server) possano decrittografarlo. Ciò implica anche che il vostro proxy Burp non sarà in grado di intercettare il traffico HTTPS in entrata e in uscita dal vostro browser. Per aggirare questo problema, dovete mostrare a Firefox che il vostro proxy Burp è una parte attendibile, installando il suo certificato CA, emesso dall'autorità di certificazione.
Installate il certificato di Burp su Firefox in modo da permettergli di vedere il traffico HTTPS. Con Burp aperto e in esecuzione e le impostazioni del proxy impostate su 127.0.0.1:8080, andate su `http://burp/` nel vostro browser. Dovreste vedere la pagina di benvenuto di Burp (Figura 4.5). Fate clic su *CA Certificate* (*Certificato CA*) in alto a destra per scaricare il file del certificato; quindi, fate clic su *Save File* (*Salva file*) per salvarlo in un luogo sicuro.

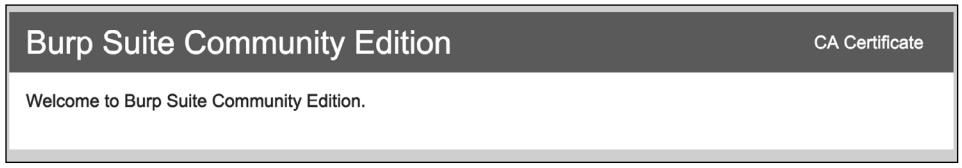

Figura 4.5 Andate su http://burp/ per scaricare il certificato CA di Burp.

Successivamente, in Firefox, fate clic su *Preferences* > *Privacy & Security* > *Certificates* > *View Certificates* > *Authorities* (*Preferenze* > *Privacy e sicurezza* > *Certificati* > *Visualizza certificati* > *Autorità*). Fate clic su *Import* (*Importa*) e selezionate il file appena salvato, quindi fate clic su *Open* (*Apri*). Seguite le istruzioni contenute nella finestra di dialogo per considerare attendibile il certificato per identificare i siti web (Figura 4.6).

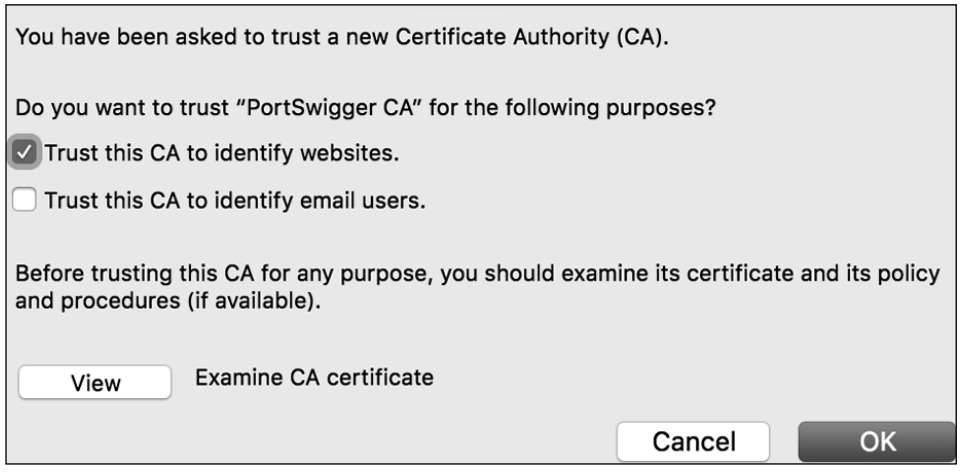

Figura 4.6 Selezionate l'opzione Trust this CA to identify websites (Considera attendibile questa CA per identificare i siti web) nella finestra di dialogo di Firefox.

Riavviate Firefox. Ora dovreste essere pronti per intercettare sia il traffico HTTP sia quello HTTPS.
Eseguiamo un test per assicurarci che Burp funzioni correttamente. Passate alla scheda *Proxy* in Burp e attivate l'intercettazione del traffico facendo clic su *Intercept is off*. Il pulsante ora dovrebbe indicare *Intercept is on* (Figura 4.7). Ciò significa che ora state intercettando il traffico da Firefox o dal browser embedded.

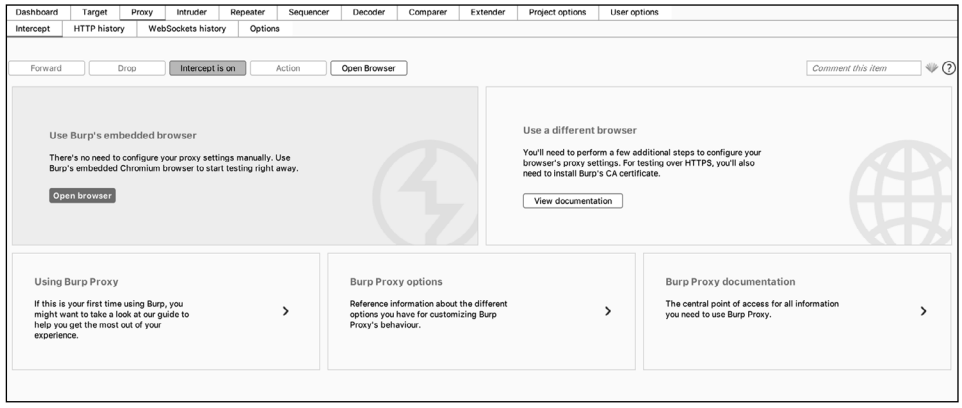

Figura 4.7 L'intercettazione ora è attiva e ciò significa che state intercettando il traffico.

Quindi aprite Firefox e visitate `https://www.google.com/`. Nel proxy Burp, dovreste vedere la finestra principale che inizia a popolarsi di richieste. Il pulsante *Forward* in Burp invierà la richiesta corrente al server designato. Fate clic su *Forward* fino a visualizzare la richiesta con il nome host `www.google.com`. Se vedete la seguente richiesta, Burp sta correttamente intercettando il traffico di Firefox. Dovrebbe iniziare così:

```
GET / HTTP/1.1
Host: www.google.com
```

Fate clic su *Forward* per inviare la richiesta al server di Google. Nella finestra di Firefox dovrebbe comparire la home page di Google.
Se non vedete le richieste nella finestra di Burp, potreste non aver installato correttamente il certificato CA di Burp. Seguite i passaggi precedenti di questo capitolo per reinstallare il certificato. Inoltre, controllate di aver configurato correttamente le impostazioni proxy su `127.0.0.1:8080` nelle impostazioni di connessione di Firefox.

Usare Burp

Burp Suite offre varie funzioni utili, oltre al proxy web. Burp Suite include anche un *intruder* per automatizzare gli attacchi, un *repeater* per manipolare le singole richieste, un *decoder* per decodificare i contenuti codificati e uno strumento *comparer* per confrontare richieste e risposte. Di tutte le funzionalità di Burp, queste sono le più utili per la caccia ai bug.

Il proxy

Vediamo come utilizzare il *proxy di Burp* per esaminare le richieste, modificarle e inoltrarle agli altri moduli di Burp. Aprite Burp e passate alla scheda *Proxy* e iniziate a esplorare quello che fa. Per iniziare a intercettare il traffico, assicuratevi che il pulsante *Intercept* indichi *Intercept is on* (Figura 4.8).

Quando fate login a un sito su Firefox o sul browser embedded di Burp, dovreste visualizzare una richiesta HTTP/HTTPS nella finestra principale. Quando l'intercettazione è attivata, ogni richiesta inviata dal vostro browser passerà attraverso Burp, che non la invierà al server a meno che non facciate clic su *Forward* nella finestra del proxy. Potete sfruttare questa opportunità per modificare la richiesta prima di inviarla al server o per inoltrarla ad altri moduli di Burp. Potete anche utilizzare la barra di ricerca nella parte inferiore della finestra per cercare determinate stringhe nelle richieste o nelle risposte.

Per inoltrare la richiesta a un altro modulo di Burp, fate clic destro sulla richiesta e selezionate *Send to* nome-modulo (Figura 4.9).

Figura 4.9 Con un clic destro potete inoltrare la richiesta o la risposta ai diversi moduli di Burp.

Facciamo una prova intercettando e modificando il traffico con Burp Proxy. Andate su Burp Proxy e attivate l'intercettazione del traffico. Quindi aprite Firefox o il browser embedded di Burp e visitate `https://www.google.com`. Come avete fatto nel paragrafo precedente, fate clic su *Forward* fino a visualizzare la richiesta con il nome host `www.google.com`. Dovreste vedere una richiesta come la seguente:

```
GET / HTTP/1.1
Host: www.google.com
User-Agent: Mozilla/5.0
Environmental Setup and Traffic Interception 53
Accept-Language: en-US
Accept-Encoding: gzip, deflate
Connection: close
```

Modificate questa richiesta prima di inviarla. Cambiate il valore dell'intestazione `Accept-Language` in `de`.

```
GET / HTTP/1.1
Host: www.google.com
User-Agent: Mozilla/5.0
Accept-Language: de
Accept-Encoding: gzip, deflate
Connection: close
```

Fate clic su *Forward* per inviare la richiesta al server di Google. Nella finestra del vostro browser dovreste vedere la home page di Google *in tedesco* (Figura 4.10).

Figura 4.10 La home page di Google in tedesco.

Potete anche cambiare il valore dell'intestazione `Accept-Language` da `de` a `en` e dovreste ottenere la home page di Google in inglese. Congratulazioni! Ora avete correttamente intercettato, modificato e inoltrato una richiesta HTTP tramite un proxy.

L'intruder

Lo strumento Burp *intruder* automatizza l'invio delle richieste. Se state utilizzando la versione Community di Burp, il vostro intruder sarà una versione di prova limitata. Tuttavia, anch'essa vi consente di eseguire attacchi come il *forza bruta,* tramite il quale l'hacker invia molte richieste a un server utilizzando un elenco di valori predeterminati e verifica se il server cambia le sue risposte. Per esempio, un hacker che ottiene un elenco di password comunemente utilizzate può tentare di entrare nel vostro account inviando ripetutamente richieste di accesso con tutte le password più comuni. Potete inviare richieste all'intruder facendo clic destro su una richiesta nella finestra del proxy e selezionando *Send to intruder.*
La schermata *Target* nella scheda dell'intruder consente di specificare l'host e la porta da attaccare (Figura 4.11). Se inoltrate una richiesta dal proxy, l'host e la porta saranno già precompilati.

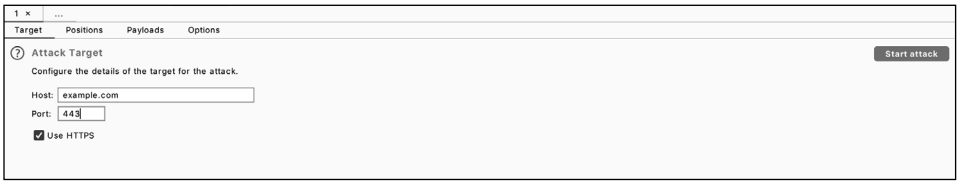

Figura 4.11 Nella schermata Target potete specificare l'host e la porta da attaccare.

L'intruder vi offre diversi modi per personalizzare l'attacco. Per ogni richiesta, potete scegliere i payload e le posizioni dei payload da utilizzare. I *payload* sono i dati che volete inserire in posizioni specifiche nella richiesta. Le *posizioni del payload* specificano quali parti della richiesta verranno sostituite dai payload scelti. Per esempio, supponiamo che gli utenti facciano login a `example.com` inviando una richiesta `POST` a `example.com/login`. In Burp, la richiesta potrebbe essere simile alla seguente:

```
POST /login HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0
Accept: text/html,application/xhtml+xml,application/xml
Accept-Language: en-US
Accept-Encoding: gzip, deflate
Connection: close

username=vickie&password=abc123
```

Il corpo della richiesta `POST` contiene due parametri: `username` e `password`. Se stavate cercando di forzare l'account di un utente, potreste cambiare il campo della `password` della richiesta e mantenere tutto il resto uguale. Per farlo, specificate le posizioni del payload nella schermata *Positions* (Figura 4.12). Per aggiungere una parte della richiesta alle posizioni del payload, evidenziate il testo e fate clic su *Add*, a destra.

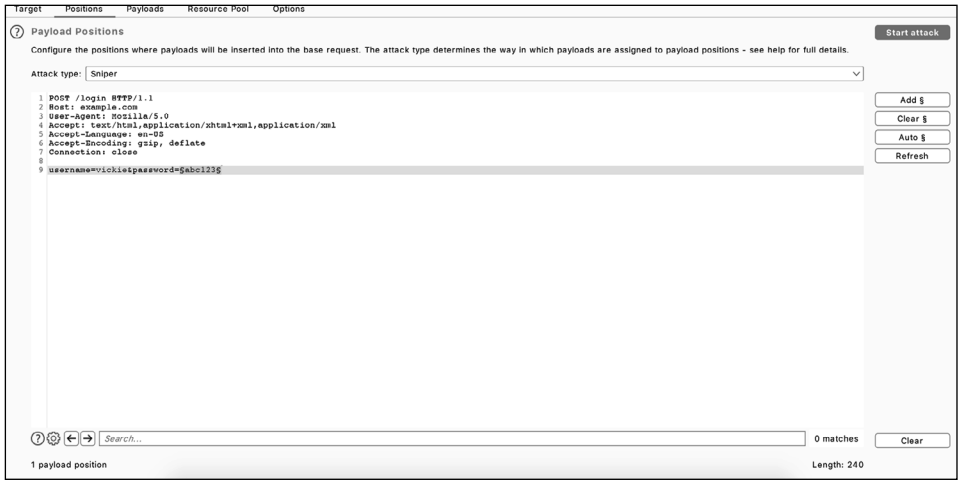

Figura 4.12 Nella schermata Positions potete specificare le posizioni del payload.

Poi, passate alla schermata *Payloads* (Figura 4.13). Qui potete scegliere i payload da inserire nella richiesta. Per applicare la forza bruta a una password di login, potete aggiungere qui un elenco di password comunemente utilizzate. Ma potete anche, per fare un esempio, utilizzare un elenco di numeri con cui attaccare a forza bruta gli ID nelle richieste o utilizzare un elenco di payload di attacco scaricato da Internet.
Il riutilizzo dei payload di attacco condivisi da altri può aiutarvi a trovare i bug più velocemente. Vedremo come utilizzare i payload riutilizzati per cercare le vulnerabilità nel Capitolo 25.

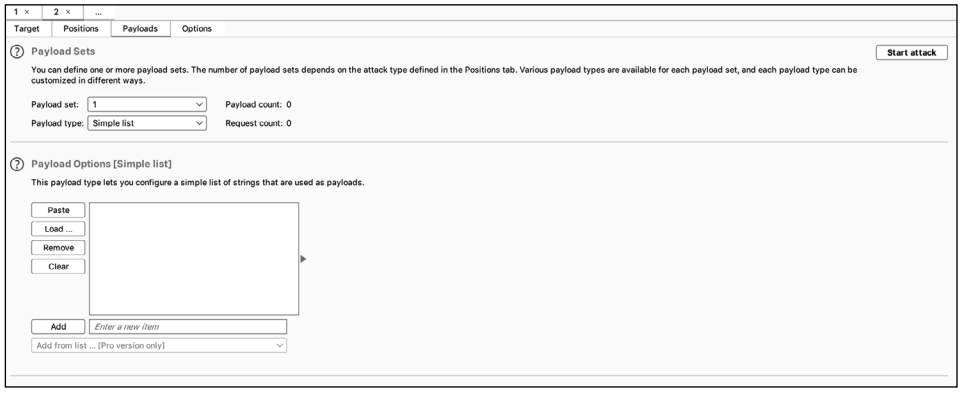

Figura 4.13 Scegliete il vostro elenco di payload nella schermata Payloads.

Dopo averli specificati, fate clic sul pulsante *Start attack* per avviare il testing automatico. L'intruder invierà una richiesta per ogni payload elencato e registrerà tutte le risposte. Poi potrete rivedere le risposte e i codici di risposta e cercare risultati interessanti.

Il repeater

Il *repeater* (Figura 4.14)è probabilmente lo strumento che userete più spesso. Potete usarlo per modificare le richieste ed esaminare in dettaglio le risposte del server. Potete usarlo anche per contrassegnare le richieste più interessanti, da rivedere più tardi.
Sebbene sia il repeater sia l'intruder consentano di manipolare le richieste, i due strumenti hanno scopi molto diversi. L'intruder automatizza gli attacchi inviando automaticamente richieste modificate a livello di codice. Il repeater è pensato per apportare modifiche manuali e dettagliate per una singola richiesta. Potete inviare richieste al repeater facendo clic destro sulla richiesta e selezionando *Send to repeater.*
Sulla sinistra della schermata del repeater troverete le richieste. Potete modificare una richiesta e inviarla richiesta modificata al server facendo clic su *Send,* in alto. La risposta corrispondente dal server apparirà sulla destra.
Il repeater è utile per sfruttare manualmente i bug, per provare a bypassare i filtri e sottoporre a test diversi metodi di attacco che prendono di mira lo stesso endpoint.

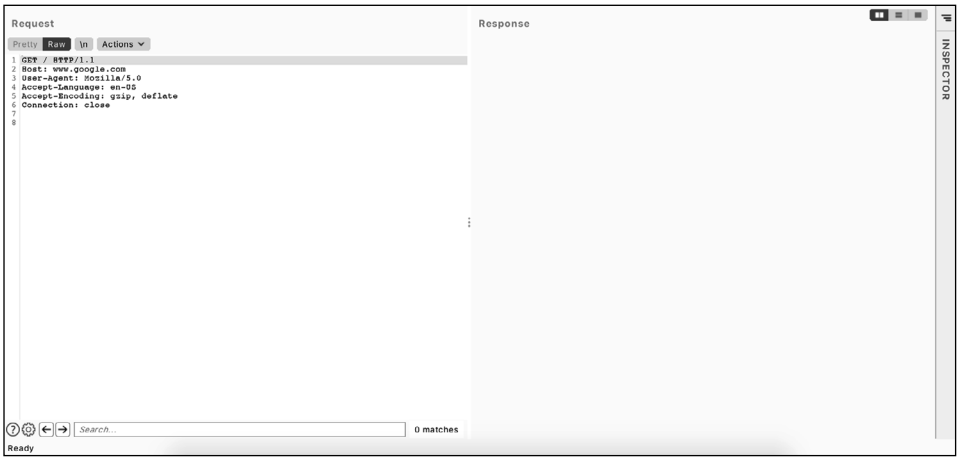

Figura 4.14 Il repeater è utile per un attento esame delle richieste e per l'utilizzo manuale.

Il decoder

Il *decoder* di Burp (Figura 4.15) è comodo per codificare e decodificare i dati che trovate nelle richieste e nelle risposte. Lo uso molto spesso per decodificare, manipolare e ricodificare i dati delle applicazioni, prima di inoltrarli alle applicazioni.

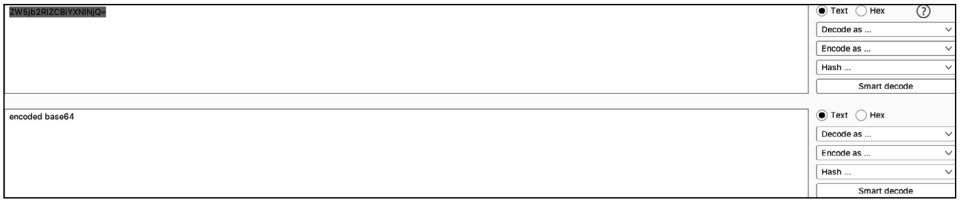

Figura 4.15 Potete utilizzare il decoder per decodificare i dati dell'applicazione in modo da leggerne o manipolarne il testo.

Potete inviare i dati al decoder evidenziando un blocco di testo in qualsiasi richiesta o risposta, quindi facendo clic destro e selezionando *Send to decoder.* Utilizzate i menu a discesa sulla destra per specificare l'algoritmo da utilizzare per codificare o decodificare il messaggio. Se non siete sicuri di quale algoritmo sia stato utilizzato per codificare il messaggio, provate *Smart decode*. Burp tenterà di rilevare la codifica e poi di decodificare il messaggio.

Il comparer

Il *comparer* (Figura 4.16) è un modo per confrontare richieste o risposte, evidenziando le differenze esistenti tra due blocchi di testo. Potete usarlo per esaminare come una differenza nei parametri influisce sulla risposta che ottenete dal server, per esempio.
Potete inviare i dati al comparer evidenziando un blocco di testo in qualsiasi richiesta o risposta, facendo clic destro e selezionando *Send to comparer.*

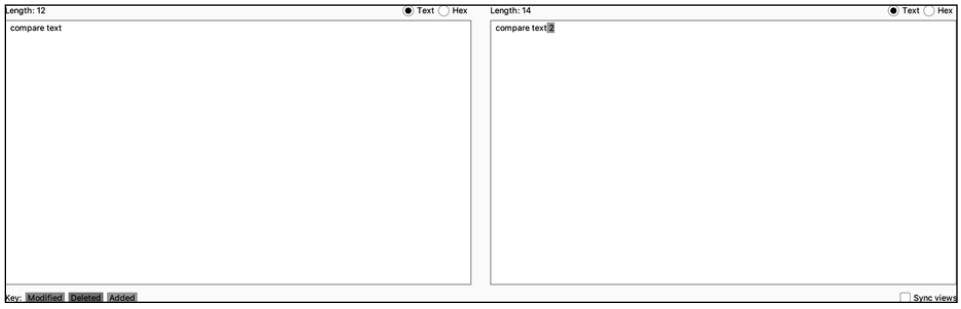

Figura 4.16 Il comparer evidenzierà le differenze tra due blocchi di testo.

Salvare le richieste in Burp

Con Burp potete anche salvare le richieste e le risposte. È sufficiente fare clic destro su qualsiasi richiesta e selezionare *Copy URL, Copy as curl command* o *Copy to file* per archiviare questi risultati nella directory degli appunti per quel target. L'opzione *Copy URL* copia l'URL della richiesta. Il comando *Copy as curl command* copia l'intera richiesta, inclusi il metodo, l'URL, le intestazioni e il corpo, come un comando curl. *Copy to file* salva l'intera richiesta in un file a parte.

Un appunto finale sul... prendere appunti

Prima di iniziare a cercare vulnerabilità, dal prossimo capitolo, un breve consiglio: le competenze organizzative sono fondamentali se volete avere successo nella caccia ai bug. Quando lavorate su target con ampi ambiti o sottoponete ad hacking più target contemporaneamente, le informazioni che raccogliete dai target potrebbero crescere al punto da diventare difficili da gestire.
Spesso non sarete in grado di trovare subito i bug. Invece, noterete molti comportamenti anomali e configurazioni errate, che non sono sfruttabili al momento, ma che potreste

combinare con altri comportamenti in un attacco complesso. Dovrete prendere appunti su eventuali nuove funzionalità, configurazioni errate, piccoli bug ed endpoint sospetti che trovate, in modo da poter tornare rapidamente indietro e utilizzarli.
Gli appunti vi aiutano anche a pianificare gli attacchi. Potete tenere traccia dei vostri progressi di hacking, delle funzionalità che avete sottoposto a test e di quelle che dovete ancora provare. Questo vi eviterà di perdere tempo sottoponendo a test le stesse funzionalità più e più volte.
Un altro buon uso degli appunti è quello di annotare le informazioni sulle vulnerabilità di cui venite a conoscenza. Registrate i dettagli di ogni vulnerabilità, come il suo funzionamento teorico, il potenziale impatto, i passi finora applicati e il codice impiegato. Nel tempo, questo rafforzerà le vostre capacità tecniche e creerà un archivio di tecniche che potrete rivisitare, se necessario.
Dal momento che questi appunti tendono a crescere di volume e a diventare molto caotici, è bene tenerli organizzate fin dall'inizio. Mi piace prendere appunti in file di testo in chiaro utilizzando *Sublime Text* (`https://www.sublimetext.com`) e organizzarli in directory, con subdirectory per ogni target e argomento.
Per esempio, potete creare una directory per ogni target su cui state lavorando, come Facebook, Google o Verizon. Quindi, all'interno di ciascuna di queste directory, potete creare dei file per documentare endpoint interessanti, funzionalità nuove e nascoste, risultati delle ricognizioni, bozze di report e PoC.
Trovate una strategia nella vostra organizzazione e per prendere appunti che funzioni per voi. Per esempio, se siete come me e preferite archiviare gli appunti sotto forma di puro testo, potete cercare un ambiente di sviluppo integrato (IDE) o un editor di testi in cui vi sentite più a vostro agio. Alcuni preferiscono prendere appunti utilizzando il formato *Markdown*. In questo caso, *Obsidian* (`https://obsidian.md`) è uno strumento eccellente, che mostra i vostri appunti in modo organizzato. Se vi piace utilizzare le mappe mentali per organizzare le idee, potete provare lo strumento di mappatura *XMind* (`https://www.xmind.net`).
Conservate i vostri appunti di caccia ai bug in un luogo centralizzato, come un disco rigido esterno o un servizio di archiviazione cloud come Google Drive o Dropbox, e non dimenticatevi di eseguire regolarmente il backup dei vostri appunti.
In sintesi, ecco alcuni suggerimenti per aiutarvi a prendere appunti.

- Prendete appunti su eventuali comportamenti anomali, nuove funzionalità, configurazioni errate, piccoli bug ed endpoint sospetti, per tenere traccia di potenziali vulnerabilità.
- Prendete appunti per tenere traccia dei vostri progressi di hacking, delle funzionalità che avete sottoposto a test e di quelle che dovete ancora verificare.
- Prendete appunti mentre imparate: annotate le informazioni su ogni vulnerabilità che conoscete, come il comportamento teorico, il potenziale impatto, le fasi del test applicato e il codice PoC di esempio.
- Mantenete i vostri appunti organizzati fin dall'inizio, così potrete trovarli quando ne avrete bisogno.
- Trovate un processo per organizzarvi e per prendere appunti che funzioni per voi. Potete provare strumenti per prendere appunti come Sublime Text, Obsidian e XMind, per trovare quello che preferite.