ReDoS e web framework

Gli attacchi DoS (Denial of Service) contro i web framework utilizzano tecniche che mirano a sovraccaricare un sistema, impedendo ai servizi di funzionare correttamente o di rispondere alle richieste legittime degli utenti. Una delle modalità più insidiose di questi attacchi riguarda l'uso di **espressioni regolari**, strumenti potenti ma che possono diventare estremamente inefficaci in termini di performance se manipolati ad arte da un malintenzionato.

Il problema delle "espressioni regolari vulnerabili"

Le espressioni regolari, o regex, sono utilizzate in molti framework web per la validazione degli input, l'estrazione di dati o il filtraggio di contenuti. Se non implementate correttamente, possono essere sfruttate per eseguire attacchi di **ReDoS** (Regular Expression Denial of Service). L'attacco si basa sulla creazione di input appositamente elaborati che costringono l'algoritmo di matching delle espressioni regolari a richiedere un tempo computazionale esponenziale rispetto alla lunghezza dell'input.

Una regex vulnerabile potrebbe avere la forma seguente:

```
(a+)+
```

Questa espressione cerca di catturare una sequenza di "a" ripetute, ma ha un grave problema di backtracking: per ogni carattere aggiuntivo nel pattern d'attacco, il tempo richiesto per eseguire il matching aumenta drasticamente.

Un esempio di input malevolo potrebbe essere:

```
aaaaaaaaaaaaaaaaaaaaaaaaaaaa!
```

Questo input non è una corrispondenza valida per l'espressione regolare, ma costringerà il motore regex a esplorare tutte le possibili combinazioni di backtracking, rallentando enormemente il sistema. In alcuni casi, potrebbe persino bloccare il server o rallentare drasticamente la risposta, provocando un effetto simile a un attacco DoS.

Impatto sugli applicativi

I web framework che utilizzano espressioni regolari in modo inappropriato per la validazione degli input sono particolarmente vulnerabili a questi tipi di attacchi. Attaccanti possono sfruttare vulnerabilità nel codice del framework o nelle librerie di terze parti per inviare input progettati per provocare un enorme consumo di risorse CPU e memoria. Questo è particolarmente dannoso in ambienti di produzione, dove un attacco mirato può rendere inutilizzabile l'intero sistema o servizio.

Misure di prevenzione

Per proteggersi da questo tipo di attacchi, è fondamentale adottare alcune best practice:

1. **Limitare la complessità delle espressioni regolari**: Evitare espressioni con strutture di backtracking ridondanti o nidificate.
2. **Imporre limiti agli input**: Definire lunghezze massime ragionevoli per gli input che vengono processati con le regex.
3. **Usare librerie sicure**: Esistono implementazioni più sicure di regex che evitano il backtracking, come quelle basate su automi a stati finiti (DFA).

4. **Monitorare le performance**: Implementare un monitoraggio attivo delle risorse per rilevare picchi di utilizzo sospetti e rispondere prontamente.

Conclusione

Gli attacchi DoS basati sulle espressioni regolari rappresentano una minaccia concreta per i web framework, che può essere facilmente sottovalutata. La capacità degli attaccanti di sfruttare regex vulnerabili per sovraccaricare un server rende necessaria una gestione consapevole e attenta del loro utilizzo. Progettare espressioni regolari con attenzione e monitorare i sistemi possono fare la differenza nel prevenire un Denial of Service silenzioso ma devastante.