Zap Attack – web app open source scanner

Zed Attack Proxy (zaproxy.org)) è uno strumento OWASP di sicurezza informatica open source progettato per sviluppatori e esperti di sicurezza informatica, finalizzato a identificare e correggere le vulnerabilità nelle applicazioni web.

Questo strumento appartiene al Project OWASP (Open Web Application Security Project), un'organizzazione che si impegna a migliorare la sicurezza delle applicazioni web attraverso la condivisione di conoscenze e risorse. Effettuare test regolari e approfonditi per le web app è fondamentale per garantire la qualità e la sicurezza dell'applicazione e per offrire agli utenti un'esperienza ottimale.

ZAP offre diverse funzionalità per testare e analizzare la sicurezza delle applicazioni web, tra cui SQL-injection, Remote file inclusion, cross-site scripting (XSS), clickjacking, vulnerabilità di sicurezza SSL/TLS e tecniche di fuzzing. Questo tipo di test consente di verificare che le applicazioni siano reattive, intuitive per l'utente e prive di errori o vulnerabilità. Tra i test di funzionalità c'è la verifica che tutte le funzionalità dell'applicazione siano implementate correttamente e rispondano alle aspettative dell'utente, altri test sono le operazione di pentest, ovvero test di sicurezza che individuano eventuali vulnerabilità e rischi per la sicurezza dell'applicazione. Una delle funzioni più interessanti è quella dei ***break-points,*** *funzione che* permette di intercettare una richiesta dal browser e cambiarla prima che raggiunga la Web app, così da poter cambiare o disabilitare campi nascosti, modificare i dati e bypassare la "client-side validation". I *break-points* possono essere impostati o con il pulsante dedicato nella toolbar, oppure su

singoli elementi tramite menu con click sulla voce HTTP break point.



Il fuzzing è una tecnica di testing automatizzata che consiste nel generare input casuali o semi-casuali per un programma informatico allo scopo di individuare vulnerabilità o bug. Questo metodo è particolarmente utile nel contesto della sicurezza informatica, in quanto consente di identificare potenziali falle nel software che potrebbero essere sfruttate da attaccanti.

Il fuzzing può essere eseguito in diverse modalità, come ad esempio il fuzzing basato su mutazione, in cui vengono modificati in modo casuale i dati di input, o il fuzzing basato su generazione di input, in cui vengono creati input validi ma inaspettati.

Questa tecnica è ampiamente utilizzata dagli esperti di sicurezza informatica per testare la robustezza dei software e per individuare vulnerabilità che potrebbero essere sfruttate da malintenzionati. Grazie al fuzzing, è possibile aumentare la sicurezza dei sistemi informatici e proteggere i dati sensibili dagli attacchi informatici. ZAP viene usato per trovare problematiche di security misconfiguration, vulnerable/outdated components e insecure design.



Grazie alla sua interfaccia utente intuitiva e alla sua flessibilità, ZAP è diventato uno strumento popolare tra gli sviluppatori e gli esperti di sicurezza. È in grado di supportare sia test automatizzati che manuali, consentendo agli utenti di scoprire e correggere le vulnerabilità in modo rapido ed efficiente grazie anche alla filosofia open source che sta dietro a questo progetto. Qualsiasi software open source ha il vantaggio di essere gratuito, quindi nessuna

licenza che obblighi a pagare la licenza riducendo il costo dell'attrezzatura per il testing. Un altro vantaggio è la possibilità di personalizzare e quindi migliorare il software data la disponibilità del codice sorgente. Il mese scorso è uscita la release 2.15.0 con una costanza di due rilasci all'anno, non scontato per un progetto open source senza una ditta dietro che stipendia gli sviluppatori. La comunità è molto attiva anche se il progetto è no-profit e aiutato da una società ZAProxy Ltd senza scopo di lucro che si occupa di raccogliere fondi per il progetto. Per le ditte che necessitano di assistenza personalizzata c'è la possibilità di acquistare dei giorni consulenza. Il canale youtube di ZAP è pieno di video che mostrano le novità e come settare le varie funzionalità per le scansioni che terminano con dei risultati esportabili in diversi formati.

L'obbiettivo del progetto è il compito di vulnerability assessment, pratica che comprende sia l'identificazione delle vulnerabilità attraverso l'analisi dei sistemi che delle reti, cosi da individuare le possibili vulnerabilità se presenti, consentendo agli addetti IT di prendere misure per prevenire e mitigare i rischi. Stabilito una priorità delle minacce partendo dalle minacce più rilevanti si organizza poi il lavoro successivo, cosi da limitare possibili attacchi informatici. Il progetto permette l'ampliamento delle sue funzionalità tramite plug-in gratuiti presenti nel marketplace. ZAP Marketplace contiene i componenti aggiuntivi di ZAP scritti dal team di ZAP e dalla comunità. I componenti aggiuntivi aiutano a estendere le funzionalità di ZAP. L'icona per la lista degli add-ons si trova nella barra degli strumenti della GUI. Tra i plug-in in versione alpha, beta e release più rilevanti c'è "FuzzDB Offensive", "OAST Support", "Spider", "Ajax Spider", "Technology Detection", "Passive scanner rules" e "Python Scripting". Le diverse modalità di scansione come standard, attack, protetta e sicura permettono approcci sia aggressivi che lievi agli obbiettivi.

La possibilità di estrapolare i report generati, con formati quali XML e HTML dal menù Report, permettono di personalizzare le informazioni filtrando per allarmi high, medium, low e false positive. Una funzione utile è la possibilità di confrontare gli esiti di due sessioni diverse, magari per verificare quali bug di un sito sono stati effettivamente risolti e quali hanno bisogno di ulteriore lavoro.

Zap permette quindi avere due strumenti in uno. Sia scanner di vulnerabilità automatizzato e ampliato con i plug-in sia di operare come proxy per ispezionare il traffico e tutta la comunicazione HTTP in modo da analizzare i loro trigger. ZAP è utilizzabile anche tramite script da CLI in modo da automatizzare procedure di pentesting. ZAP è un prodotto OWASP acronimo di Open Web Application Security Project, ovvero progetto della comunità online, ormai un punto di riferimento, specializzata in temi di sicurezza applicazione Web.

La comunità ZAP si mette a disposizione per ogni problema nel gruppo ZAP user group (groups.google.com/g/zaproxy-users) o presso il canale IRC (https://web.libera.chat/#zaproxy).

ZAP è uno strumento essenziale per il tecnico cyber security analyst IT che sia coinvolto nella gestione di applicazioni web, quindi orientato a personale preparato e con le giuste competenze per valutare i risultati e le modalità di attacco. Grazie alla sua potente suite di strumenti e alla sua facilità d’uso, ZAP aiuta gli utenti a mantenere le loro applicazioni web sicure e protette da minacce esterne con uno strumento gratuito. Inoltre il progetto ZAP con la filosofia free e open source supporta molti standard aperti e protocolli noti, rendendo più semplice l’integrazione con sistemi operativi e plug-in personalizzabili. Filosofia che permette di sviluppare questo tipo di progetti aperti alla comunità in cui appassionati e professionisti possono contribuire al progetto e al suo miglioramento.

Articolo a cura di **Fabio Carletti**

Profilo Autore

Fabio Carletti aka Ryuw è un White Hat del gruppo (SoldierX Hacker team).

Esperto di sicurezza informatica con una vasta esperienza nel campo della protezione dei sistemi, delle reti e dei dati sensibili. Con più di 20 anni di esperienza nel settore della sicurezza informatica, ha lavorato con diverse organizzazioni per implementare strategie di difesa avanzate e mitigare le minacce informatiche in continua evoluzione.

Collabora come membro volontario del Tor Project team.

Ospite di rilevanti eventi italiani riguardanti la privacy, gnu/linux e software open source dedica le sue energie alla ricerca nella sicurezza informatica.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/zap-attack-web-app-open-source-scanner/