Minacce comuni

Sommario

Traccia esercizio extra

Per ogni scenario proposto identifica:

- OWASP Top 10 (se presente);
- MITRE ATT&CK Enterprise (tecnica principale);
- Mitigazione suggerita da MITRE ATT&CK.

Scenari:

1. Un'azienda ha ricevuto segnalazioni da utenti che hanno subito attacchi XSS. Gli utenti hanno inserito dati in un form online che eseguiva script dannosi nel loro browser. Questo ha permesso agli attaccanti di rubare i cookie di sessione e impersonare altri utenti.
2. Un attaccante è riuscito a ottenere accesso non autorizzato ai dati aziendali sfruttando una vulnerabilità SQL Injection nell'interfaccia di login di un'applicazione. L'attaccante ha manipolato l'input per eseguire comandi SQL non autorizzati, estraendo dati sensibili dal database.
3. Un attaccante è riuscito a eseguire codice arbitrario sul server sfruttando una vulnerabilità di deserializzazione non sicura del client in una funzione che accetta oggetti serializzati dall'utente. Manipolando l'oggetto inviato, l'attaccante ha ottenuto l'esecuzione remota di codice sul server.

Spiegazione

OWASP Top 10

Definizione: L'OWASP Top 10 è una lista delle dieci vulnerabilità di sicurezza più critiche per le applicazioni web, pubblicata dall'Open Web Application Security Project (OWASP), un'organizzazione no-profit dedicata alla sicurezza delle applicazioni.
Spiegazione: L'OWASP Top 10 può essere paragonato a un elenco di difetti di costruzione per edifici, evidenziando le vulnerabilità più comuni che possono rendere le applicazioni web suscettibili ad attacchi. Le vulnerabilità incluse nell'OWASP Top 10 (versione 2021 https://owasp.org/www-project-top-ten/) sono:

1. **A01:2021 - Controllo degli accessi non corretto**: Problemi nell'impedire l'accesso non autorizzato alle funzionalità dell'applicazione, riscontrati in molte applicazioni testate.
2. **A02:2021 - Errori nella gestione della crittografia**: Problemi nell'utilizzo corretto della crittografia, che possono portare alla fuga di informazioni sensibili.
3. **A03:2021 - Iniezione di codice**: Vari modi in cui un utente malintenzionato può inserire codice dannoso nell'applicazione, come attraverso moduli di ricerca o di login.
4. **A04:2021 - Progettazione non sicura**: Nuova categoria che riguarda i rischi dovuti a problemi nella progettazione iniziale dell'applicazione.
5. **A05:2021 - Configurazione non sicura**: Errori nella configurazione dell'applicazione e dei suoi ambienti di esecuzione, che possono comprometterne la sicurezza.
6. **A06:2021 - Componenti vulnerabili e obsoleti**: Uso di parti software (librerie, framework, ecc.) con vulnerabilità note, un problema diffuso e persistente.
7. **A07:2021 - Errori di identificazione e autenticazione**: Problemi nella gestione di come gli utenti si identificano e si autenticano nell'applicazione.
8. **A08:2021 - Problemi di integrità di software e dati**: Ipotesi non verificate su aggiornamenti software, dati critici e processi di sviluppo continuo.
9. **A09:2021 - Mancanze nella registrazione e monitoraggio di sicurezza**: Assenza di adeguate attività di registrazione e controllo degli eventi di sicurezza dell'applicazione.
10. **A10:2021 - Server-Side Request Forgery**: Nuova categoria che riguarda vulnerabilità legate a richieste indesiderate inviate al server dell'applicazione.

MITRE ATT&CK Enterprise

MITRE ATT&CK Enterprise è un framework che offre una raccolta di informazioni sulle tecniche utilizzate da attaccanti informatici nel mondo reale. Serve come guida per comprendere i metodi di attacco e migliorare la difesa delle organizzazioni. https://attack.mitre.org/matrices/enterprise/

Struttura: Il framework è organizzato in matrici che coprono diverse fasi di un attacco informatico, dalla fase di accesso iniziale fino al mantenimento dell'accesso. Ogni tecnica è accompagnata da descrizioni dettagliate e esempi di come è stata utilizzata in attacchi reali.

Obiettivo: L'obiettivo di MITRE ATT&CK è aiutare le organizzazioni a identificare le vulnerabilità nei loro sistemi e a migliorare le loro capacità di rilevamento e risposta agli attacchi. Fornisce anche un linguaggio comune per i professionisti della sicurezza informatica, facilitando la comunicazione e la collaborazione.

Utilizzo: Le organizzazioni possono utilizzare MITRE ATT&CK per:

- Valutare le proprie difese contro tecniche di attacco note.
- Progettare e implementare strategie di difesa più efficaci.
- Eseguire simulazioni di attacco per testare le proprie risposte.

Importanza: Questo framework è ampiamente riconosciuto nella comunità della sicurezza informatica e viene utilizzato da aziende, governi e ricercatori per migliorare la sicurezza delle informazioni e proteggere i sistemi da minacce informatiche.

La pagina **Tattiche - Enterprise** di MITRE ATT&CK® spiega le strategie che gli hacker usano quando attaccano un sistema. Le tattiche mostrano il "perché" di un attacco, cioè quali obiettivi vogliono raggiungere. Ecco un elenco semplice delle principali tattiche https://attack.mitre.org/tactics/enterprise/ :

1. **Ricognizione**: Gli hacker raccolgono informazioni per pianificare i loro attacchi futuri.
2. **Sviluppo delle Risorse**: Gli hacker preparano strumenti e risorse per aiutarsi durante l'attacco.
3. **Accesso Iniziale**: Gli hacker cercano di entrare nella rete di un'organizzazione.
4. **Esecuzione**: Gli hacker tentano di far partire software dannoso.
5. **Persistenza**: Gli hacker cercano di rimanere dentro il sistema anche dopo che sono stati scoperti.
6. **Escalation dei Privilegi**: Gli hacker cercano di ottenere più poteri per fare di più nel sistema.
7. **Evasione della Difesa**: Gli hacker cercano di non farsi scoprire.
8. **Accesso alle Credenziali**: Gli hacker cercano di rubare nomi utente e password.
9. **Scoperta**: Gli hacker cercano di capire come è organizzato il sistema dell'obiettivo.
10. **Movimento Laterale**: Gli hacker si spostano all'interno della rete per raggiungere altri sistemi.
11. **Raccolta**: Gli hacker raccolgono dati che potrebbero essere utili per i loro scopi.
12. **Comando e Controllo**: Gli hacker comunicano con i sistemi che hanno colpito per controllarli.
13. **Esfiltrazione**: Gli hacker cercano di rubare dati.
14. **Impatto**: Gli hacker cercano di danneggiare o distruggere i dati e i sistemi dell'organizzazione.

Svolgimento esercizio

Scenario 1 – Attacco XSS

La vulnerabilità principale è identificata nell'OWASP Top 10 come **A03:2021 - Iniezione di codice**. Gli attaccanti sfruttano la mancanza di controlli adeguati sui dati immessi dagli utenti.

- A03:2021-Injection slides down to the third position. 94% of the applications were tested for some form of injection, and the 33 CWEs mapped into this category have the second most occurrences in applications. Cross-site Scripting is now part of this category in this edition.

MITRE ATT&CK: La tecnica principale coinvolta è il Scripting (T1059), che si riferisce all'esecuzione di comandi o script malevoli nel browser.

T1059	Command and Scripting Interpreter	Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of Unix Shell while Windows installations include the Windows Command Shell and PowerShell.

Mitigazione Suggerita: È molto importante controllare e pulire i dati che gli utenti inseriscono nei moduli. Questo significa assicurarsi che non ci siano codici o script dannosi nei dati. Per esempio, si possono usare strumenti speciali che rimuovono qualsiasi cosa che potrebbe essere pericolosa. Inoltre, le aziende dovrebbero utilizzare una **Content Security Policy (CSP)**. Questa è una regola che dice al browser quali script possono essere eseguiti. In questo modo, anche se un attaccante prova a inserire codice dannoso, il browser non lo eseguirà, aumentando la sicurezza dell'applicazione.

Scenario 2 – SQL Injection

La vulnerabilità principale è identificata nell'OWASP Top 10 come **A01:2021 - Iniezione**. Gli attaccanti sfruttano la mancanza di controlli adeguati sui dati immessi dagli utenti, come nel caso della SQL Injection, per eseguire comandi non autorizzati.

- A01:2021-Broken Access Control moves up from the fifth position; 94% of applications were tested for some form of broken access control. The 34 Common Weakness Enumerations (CWEs) mapped to Broken Access Control had more occurrences in applications than any other category.

MITRE ATT&CK: La tecnica principale coinvolta è l'Exploit di Applicazioni Pubbliche (T1190). Questa tecnica riguarda lo sfruttamento di vulnerabilità in applicazioni esposte su Internet per accedere a reti e dati sensibili. https://attack.mitre.org/techniques/T1190/

Mitigazione Suggerita: È fondamentale implementare un Web Application Firewall (WAF). Questo strumento aiuta a filtrare e bloccare le richieste malevole prima che raggiungano l'applicazione. Inoltre, le aziende dovrebbero regolarmente aggiornare e patchare il software per correggere eventuali vulnerabilità. Infine, è importante validare e pulire i dati inseriti dagli utenti per prevenire attacchi di iniezione.

Scenario 3- Vulnerabilità di deserializzazione

La vulnerabilità principale è identificata nell'OWASP Top 10 come **A08:2021 - Iniezione di deserializzazione**. Gli attaccanti sfruttano la mancanza di controlli adeguati sui dati serializzati immessi dagli utenti, consentendo l'esecuzione di codice malevolo.

- A08:2021-Software and Data Integrity Failures is a new category for 2021, focusing on making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity. One of the highest weighted impacts from Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) data mapped to the 10 CWEs in this category. Insecure Deserialization from 2017 is now a part of this larger category.

MITRE ATT&CK: La tecnica principale coinvolta è l'Esecuzione Remota di Codice (T1203). Questa tecnica si riferisce all'esecuzione di codice arbitrario su un server, sfruttando vulnerabilità nelle applicazioni che accettano oggetti serializzati non sicuri. https://attack.mitre.org/techniques/T1203/

Mitigazione Suggerita: È fondamentale implementare controlli rigorosi sulla deserializzazione. Le applicazioni dovrebbero evitare di accettare oggetti serializzati da fonti non fidate. Inoltre, è utile utilizzare librerie di deserializzazione sicure e limitare le classi che possono essere deserializzate. Infine, è importante monitorare e registrare le attività anomale per identificare tentativi di exploit.