### TRACCIA S1L2 ASSET ORGANIZZATIVI, MINACCE E VULNERABILITÀ

UN'AZIENDA VI HA INCARICATO DI SVOLGERE UN'ANALISI DELLE VULNERABILITÀ E DELLE MINACCE SUI PROPRI ASSET ORGANIZZATIVI. L'AZIENDA OPERA NEL SETTORE METALMECCANICO, PRODUZIONE DI INGRANAGGI, HA CIRCA 200 IMPIEGATI ED UN PROPRIO E-COMMERCE. SONO PRESENTI CIRCA 200 PC (1.000 €/PC) E 30 SERVER (3.000 €/SERVER). I SERVIZIO DI CUI DISPONE SONO: SITO E-COMMERCE (FATTURATO 1 0.000 €/GIORNO), ERP DI GESTIONE AZIENDALE(30.000€), SERVER DI POSTA ELETTRONICA(5.000€) E UN SISTEMA DI SICUREZZA COMPOSTO DA FIREWALL, IDS E SIEM DI (25.000€). NELLA GESTIONE DEL RISCHIO, L'IDENTIFICAZIONE DEGLI ASSET, L'ANALISI DELLE MINACCE E DELLE VULNERABILITÀ AVVIENE IN CONTEMPORANEA E SI INTEGRANO A VICENDA. CREARE UN REPORT IN CUI INCLUDERE:

- 1. IDENTIFICAZIONE E VALORE DEGLI ASSET
- 2. ANALISI DELLE VULNERABILITÀ
- ANALISI DELLE MINACCE SIETE LIBERI DI ESTENDERE ED IPOTIZZARE LO SCENARIO, IL NUMERO DI ASSET DA CUI PARTIRE È A VOSTRA SCELTA. POTETE UTILIZZARE QUALSIASI SUPPORTO COME CVE, CVSS, TABELLE NIST SP 800-30, ECC.

### 1 ANALISI DELLE VULNERABILITÀ E DELLE MINACCE

#### Identificazione e Valore degli Asset

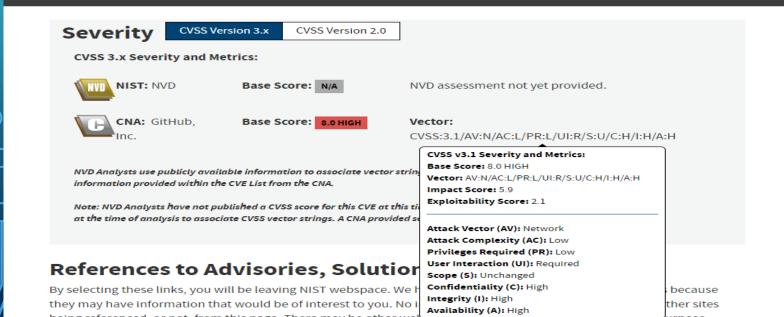
- PC: 200 unità, valore totale 200.000€ (1.000€ per PC)
- Server: 30 unità, valore totale 90.000€ (3.000€ per server)
- Sito e-commerce: Fatturato di 10.000€ al giorno
- ERP di gestione aziendale: Valore 30.000€
- Server di posta elettronica: Valore 5.000€
- Sistema di sicurezza (firewall, IDS, SIEM): Valore 25.000€

- Common Vulnerabilities and Exposures (CVE): Il CVE è un dizionario pubblico di vulnerabilità note in ambito informatico, gestito dal MITRE Corporation. Ogni vulnerabilità identificata riceve un identificatore unico in formato CVE-ANNO-NUMERO (es. CVE-2021-12345). Questo sistema permette di identificare e riferirsi in modo univoco alle vulnerabilità, facilitando la condivisione di informazioni e la collaborazione tra organizzazioni.
- Common Vulnerability Scoring System(CVSS): Il CVSSè uno standard aperto per valutare la gravità delle vulnerabilità informatiche. Assegnaunpunteggio numerico compreso tra 0 e10,basato su metriche che considerano il vettore di attacco, l'impatto sulla riservatezza,l'integrità e ladisponibilità,e altri fattori. È ampiamente utilizzato dalle organizzazioni e dai produttori di software per comunicare la gravità delle vulnerabilità e stabilire priorità di mitigazione. Queste sono due delle reportistiche e dizionari che utilizzeremo per catalogare e classificare le vulnerabilità presenti nelle slide successive

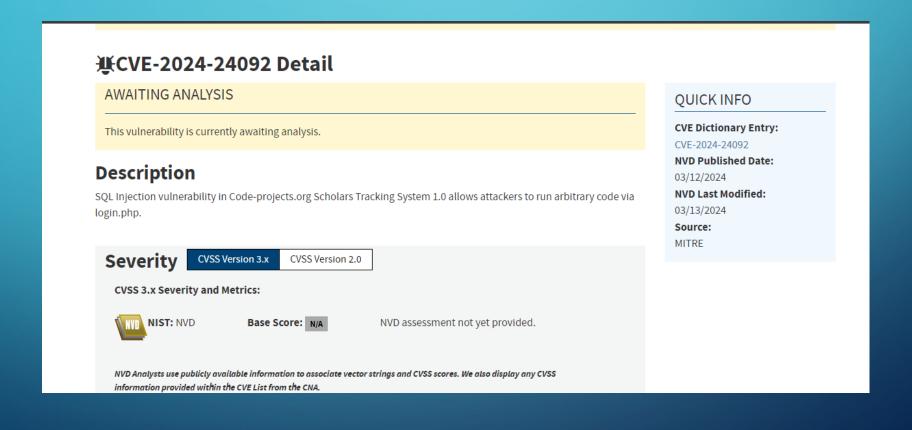
#### 2. ANALISI DELLE VULNERABILITÀ

LE VULNERABILITÀ SONO STATE INDIVIDUATE NEI SEGUENTI ASSET PER L'ANALISI DELLE VULNERABILITÀ, SI POTREBBE FARE RIFERIMENTO A DATABASE DI VULNERABILITÀ COME IL COMMON VULNERABILITIES AND EXPOSURES (CVE) E UTILIZZARE IL COMMON VULNERABILITY SCORING SYSTEM (CVSS) PER VALUTARE LA GRAVITÀ DELLE VULNERABILITÀ IDENTIFICATE.

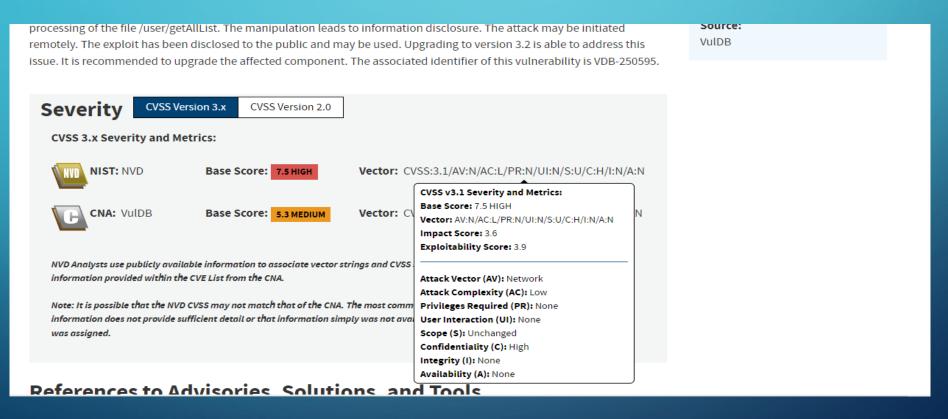
- Sito e-commerce:
- CVE-2024-29184 : Vulnerabilità XSS che potrebbe permettere ad attaccanti di eseguire script malevoli sul browser dei clienti.



## CVE-2024-24092: VULNERABILITÀ DI INJECTION CHE POTREBBE CONSENTIRE AD UN ATTACCANTE DI ESEGUIRE COMANDI NON AUTORIZZATI SUL SERVER.



# CVE-2024-0490: VULNERABILITÀ DI AUTENTICAZIONE DEBOLE CHE POTREBBE CONSENTIRE AD UN ATTACCANTE DI ACCEDERE INDEBITAMENTE AL SISTEMA ERP. MENTRE NELL'IMMAGINE È PRESENTE LA CLASSIFICA (CVSS)



### CVE-2023-24932: VULNERABILITÀ DI SPOOFING DELL'INDIRIZZO EMAIL CHE POTREBBE ESSERE SFRUTTATA PER INVIARE EMAIL FRAUDOLENTE AI CLIENTI.



- Hardware:
- Mancanza di aggiornamenti regolari del software operativo sui PC e sui server, rendendo gli asset vulnerabili a exploit noti.

### 3. ANALISI DELLE MINACCE SULLA BASE DELLE VULNERABILITÀ IDENTIFICATE, SONO STATE ANALIZZATE LE POSSIBILI MINACCE:

- Attacchi informatici:
- Attacchi di tipo XSS e Injection sul sito e-commerce per compromettere i dati dei clienti o rubare informazioni sensibili.
- Tentativi di accesso non autorizzato all'ERP aziendale per rubare informazioni finanziarie o sensibili dell'azienda.
- Utilizzo di email spoofing per ingannare i clienti e rubare informazioni personali o finanziarie.
- Perdita di dati:
- Rischio di perdita di dati sensibili dei clienti e dell'azienda a causa di violazioni della sicurezza informatica.
- Interruzione dei servizi:
- Possibilità di interruzione dei servizi critici come il sito e-commerce e l'ERP aziendale a causa di attacchi informatici o malfunzionamenti dei sistemi.

### CONCLUSIONI

L'azienda deve affrontare urgentemente le vulnerabilità identificate per mitigare i rischi di attacchi informatici, perdita di dati e interruzione dei servizi. Si raccomanda di:

- Applicare patch e aggiornamenti regolari per correggere le vulnerabilità esistenti nei software e nei sistemi.
- Implementare misure di sicurezza aggiuntive come firewall avanzati e sistemi di rilevamento delle intrusioni per proteggere i sistemi critici.
- Condurre sessioni di formazione sulla sicurezza informatica per sensibilizzare il personale e ridurre il rischio di phishing e altre minacce basate sull'ingegneria sociale.
- Implementare politiche di accesso sicuro e autenticazione a due fattori per proteggere l'accesso ai sistemi critici.