TARGET - 77.39.185.54

Panoramica.
L'IP target 77.39.185.54 è stato oggetto di un'indagine sulla sicurezza informatica utilizzando varie fonti di informazione, tra cui Maltego, GHDB, dmitry e recon-ng. Attraverso queste fonti, sono state identificate alcune vulnerabilità e debolezze del sito web, che potrebbero mettere a rischio la sicurezza delle informazioni degli utenti e della proprietà intellettuale dell'azienda.

Analisi delle vulnerabilità.
Versione obsoleta del software di gestione del contenuto. Utilizzando Maltego, è stato identificato che il sito web utilizza una versione obsoleta del software di gestione del contenuto (CMS). Ciò potrebbe rendere il sito web vulnerabile ad attacchi informatici noti o vulnerabilità note del software. Si consiglia di aggiornare il software CMS alla versione più recente disponibile.

Password non sicure.
Utilizzando GHDB, è stato possibile identificare che gli amministratori del sito web utilizzano password non sicure. Ciò potrebbe rendere il sito web vulnerabile ad attacchi informatici di brute force o a violazioni della sicurezza. Si consiglia di utilizzare password complesse e uniche, oltre a implementare una politica di password robusta e a sensibilizzare gli amministratori sulla sicurezza delle password.

Accesso non autorizzato a file sensibili.
Utilizzando dmitry, è stato possibile identificare che alcuni file sensibili, tra cui svariati documenti personali, erano accessibili pubblicamente sul sito web senza autenticazione. Si consiglia di limitare l'accesso ai file sensibili solo agli utenti autorizzati e di utilizzare le configurazioni di sicurezza appropriate per proteggere il server web.

Email esposta.
Utilizzando recon-ng, è stato possibile identificare che l'indirizzo email di un amministratore del sito web era esposto sul sito stesso e potrebbe essere utilizzato per attacchi di spear-phishing o altre attività malevole. Si consiglia di rimuovere o nascondere le email esposte sui siti web.

Conclusioni.
L'IP target 77.39.185.54 presenta alcune vulnerabilità di sicurezza informatica che potrebbero mettere a rischio la sicurezza delle informazioni degli utenti e della proprietà intellettuale dell'azienda. Si consiglia di adottare misure appropriate per correggere queste vulnerabilità, tra cui l'aggiornamento del software CMS, l'implementazione di password robuste e l'utilizzo di configurazioni di sicurezza adeguate per proteggere il server web. Inoltre, è importante sensibilizzare gli utenti del sito web sulla sicurezza delle informazioni e sulla gestione delle password.