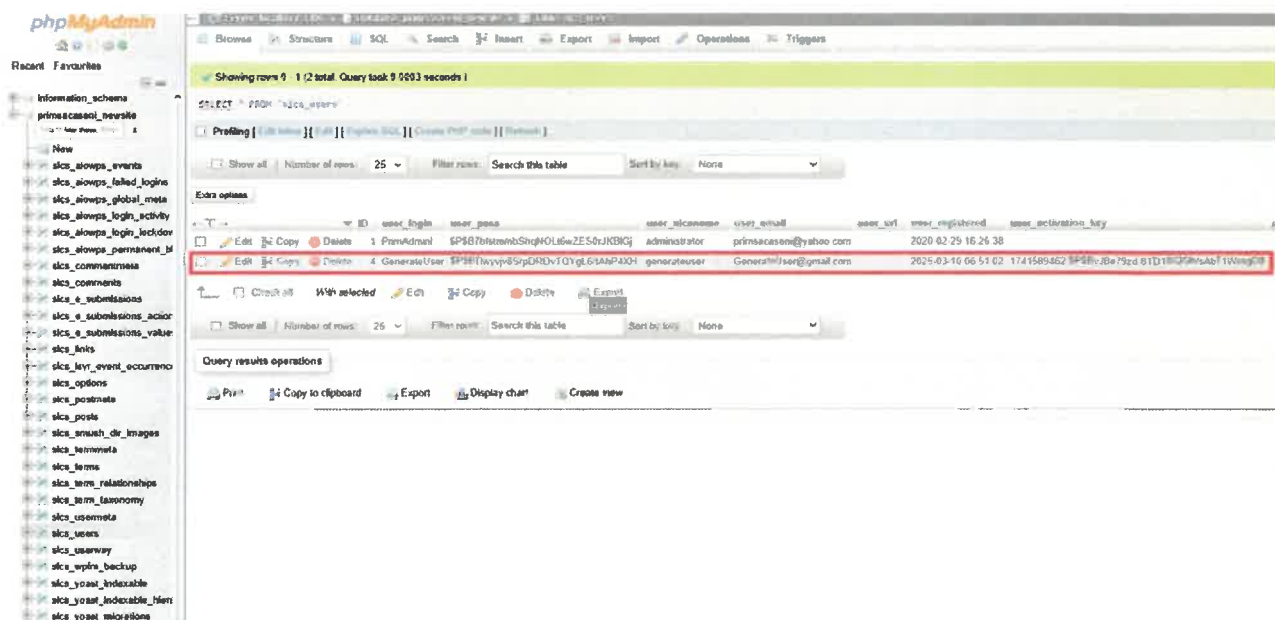


NOTA DE CONSTATARE

În urma solicitării de verificare primite de la Primăria Comunei Săcășeni în data de 10. 03.2025 s-a constatat că site-ul oficial al Primăriei Comunei Săcășeni a fost piratat, ca urmare a unui atac cibernetic. La prima vedere – cu excepția unui mesaj de eroare afișat pe pagina principală – site-ul părea a fi funcțional, dacă facem abstracție de faptul că mesajul afișat era o secvență de cod php codificat. Interfața de administrare a site-ului era inaccesibilă, iar paginile interne – cu excepția paginii principale – erau de asemenea inaccesibile. Toate aceste semne indicau în mod evident un atac asupra site-ului primăriei. De menționat că în aceeași perioadă, mai multe site-uri găzduite pe același server au fost supuse aceluiași proces de atac. Ca primă măsură s-a impus oprirea site-ului pentru a încerca remedierea problemei. La o analiză sumară a bazei de date s-a constatat că în ziua respectivă, la o oră matinală, a fost creat în site un utilizator cu drepturi depline de administrare (vezi captura de ecran de mai jos)



Un prim pas în încercarea de a recupera datele și de a face site-ul funcțional a fost eliminarea utilizatorului respectiv precum și a oricăror alte referințe către utilizator, din baza de date, pentru a bloca accesul acestuia la interfața de administrare.

Având însă în vedere că în structura existentă de fișiere s-au găsit fișiere ale căror cod sursă era codificat (probabil codare Base64) s-a procedat la eliminarea fișierelor respective.

Neavând însă expertiză în decriptarea codului criptat, pentru a putea obține informații legate de sursa de atac sau motivul atacului, și având în vedere că cel mai probabil atacul a fost de tip **SQL Injection**, **Cross-Site Scripting (XSS)** sau **PHP Code Injection** – atacuri posibile mai ales datorită neîntreținerii codului sursă a site-ului prin actualizări constante - s-a procedat la arhivarea întregului conținut al site-ului precum și a bazei de date, oprind astfel site-ul pentru a nu înrăutăți situația și mai mult.

De menționat că tipurile de atac enumerate mai sus, și nu numai, se puteau evita printr-un proces de

S.C. IZI ELECTRONICS S.R.L.
J30/29/2008 RO23031049
RO07 INGB 0000 9999 0673 1324
RO73 TREZ 5465 069 XXX 0099 51
Satu Mare, str. Ion C. Brătianu nr. 4, ap. 5, jud.SM



tel. (004) 0770 208 867
office@vizion-security.ro
LICENȚA DE FUNCȚIONARE
I.G.P.R. NR. 4203/T/03.05.2017
AUTORIZAȚIE C.N.S.I.P.C. – B/1446/1448/25.02.2022

mentenanță și actualizare regulată a codului sursă atât a platformei care a stat la baza site-ului cât și a modulelor sale.

Arhiva site-ului și a bazei de date sunt disponibile pentru oricine dorește să analizeze fișierele respective.

Data:

03.07.2025

SC. IZI ELECTRONICS SRL.

Balogh Ștefan

