Falla di sicurezza Immagini Spaggiari

Benvenuti a tutti

Sono Yassine, ma sono conosciuto come Giasin, ho 15 anni e sono un appassionato programmatore. Nonostante la mia giovane età, sono il fondatore di GiaFlix.it, un hub di progetti che collabora con diverse società.

ho posto la mia attenzione sulle falle di sicurezza che possono mettere in pericolo la privacy degli utenti. Sono convinto che la sicurezza dei dati degli utenti sia una priorità assoluta, soprattutto in un'epoca in cui la tecnologia è sempre più pervasiva e i dati personali sono un bene prezioso.

Da tempo ho scoperto una vulnerabilità nel registro elettronico Spaggiari, noto anche come ClasseViva, che potrebbe permettere a utenti registrati di accedere alle fototessere degli studenti. Ciò potrebbe comportare il rischio di furto di identità o la vendita delle immagini su dark web.

Partiamo dall'inizio. Spaggiari, comunemente noto come ClasseViva, è un registro elettronico fornito da Gruppo Spaggiari Parma. Il registro è basato su PHP, un noto linguaggio di programmazione per siti dinamici con cui ho avuto a che fare in precedenza. Molti criticano il modo in cui Spaggiari è stato realizzato, e su questo punto non ho nulla da obiettare. In effetti, PHP è un buon linguaggio per questo scopo, ma lo stile di Spaggiari è discutibile. In particolare, il foglio di stile utilizzato da Spaggiari è del 2013, e questo potrebbe essere uno dei motivi per cui il registro è molto critico per la sua lentezza e il suo stile.

Ma cosa è successo? La spiegazione è semplice: Spaggiari offre alle scuole la possibilità di inserire le fototessere degli studenti, scattate durante una lezione al primo anno, che poi vengono inviate al server di Spaggiari. Tuttavia, la parte problematica riguarda la visualizzazione di queste immagini. Poiché le immagini sono disponibili per tutti i professori della scuola in base alla classe, ci sono problemi riguardanti chi può effettivamente vederle. Qualsiasi persona che abbia un account Spaggiari, sia essa uno studente o un genitore della mia scuola, può vedere la mia fototessera, così come quelle dei miei compagni di classe e degli altri studenti della scuola.

Per visualizzare le fototessere, devi andare nella sezione "Assenze", quindi selezionare "Anagrafica" in alto a destra. Troverai la tua immagine del profilo, ma devi farlo su un computer o tramite un browser o sull'app usando la sezione "Menu" e poi "ClasseViva Web". In alcuni casi, l'immagine potrebbe non essere stata caricata correttamente all’interno del server di Spaggiari. In tal caso, facendo clic con il pulsante destro del mouse e selezionando "Apri su una nuova scheda", potresti trovare un file vuoto chiamato "ximage.php". In alternativa, dovresti trovare la tua fototessera.

Per visualizzare la fototessera di un altro studente è sufficiente guardare il link generato dal sistema Spaggiari, che è formato dal dominio seguito dal percorso per trovare il file

ximage.php e vari parametri, tra cui il parametro "**studente_codice**". Questo parametro consente di trovare l'immagine in base al codice studente, che è composto dalla lettera "S" che indica lo studente, seguita da 7 cifre o anche 8 cifre che rappresentano l'id studente e infine una lettera maiuscola che va dalla A alla Z. Ad esempio, il link *"https://web.spaggiari.eu/tools/app/default/ximage.php?t=studente&**studente_codice**=S9471612O&f=fototessera&cache=1"* consente di visualizzare la mia fototessera. Inoltre, va tenuto presente che gli studenti di altre scuole non possono visualizzare le fototessere degli studenti della mia scuola poiché il sistema Spaggiari potrebbe consentire la visualizzazione solo a coloro che appartengono ad una scuola che ha abilitato il sistema delle fototessere. In ogni caso, le foto degli studenti di altre scuole non dovrebbero essere accessibili a chi non appartiene alla mia scuola.

La fototessera degli altri può essere visualizzata tramite un link univoco che deve essere trovato per caso, o usando il programma che avevo scritto precedentemente. Questo codice e la relativa guida saranno presto disponibili a scopo informativo sul mio profilo di github, in modo che chiunque si trovi in una situazione simile possa valutare la gravità della situazione. Tuttavia, per coloro che non sono esperti di programmazione, è possibile tentare di indovinare il codice. Ad esempio, se il link di un'altra persona è *https://web.spaggiari.eu/tools/app/default/ximage.php?t=studente&studente_codice=S9471612O&f=fototessera&cache=1*, è possibile sostituire "S9471612O" con "S9471613A" e continuare a provare tutti i possibili codici, da "S9471613A" a "S9471613Z". È comunque importante sottolineare che questa pratica è scorretta e viola la privacy degli studenti, e pertanto non è consigliabile, fatelo solo con vostri amici che acconsentano.

"Oddio, sono uscito/a male in quella foto! Cosa posso fare?"
È una domanda comune, e non sei l'unico/a a porla. Personalmente, ho provato a contattare Spaggiari diverse volte attraverso vari canali di comunicazione (social, e-mail, assistenza Spaggiari). Ho anche parlato dell'argomento l'anno scorso con il professore referente del registro elettronico, il quale si è dimostrato disponibile e ha inoltrato una segnalazione. Tuttavia, ho fatto un'altra segnalazione a settembre 2022, ma non ho ottenuto alcun risultato.

"E' grave questa cosa?"
Beh, pensa che per fare questa documentazione, prima di aprire bocca (visto che non ci credeva nessuno), ho dovuto ingegnarmi. Diciamo che, dopo aver ostacolato il problema delle immagini false su Spaggiari, ah sì... me lo ero dimenticato... Spaggiari ha voluto mettere delle immagini false a tutti i link incorretti. Queste immagini hanno dimensione di 1px x 1px, veramente semplice da superare. Questo indica che Spaggiari non sta salvaguardando in modo adeguato le nostre immagini, il che è completamente inaccettabile.

Conclusione
Desidero richiamare l'attenzione di Spaggiari sull'urgenza di risolvere il problema della vulnerabilità nella sicurezza del sistema. In caso contrario, invito le scuole che utilizzano il servizio di Spaggiari a considerare seriamente questa grave falla di sicurezza e a valutare l'adozione di un registro alternativo.

P.S. Il server possiede ancora le immagini di ex studenti che ora sono in altre scuola e che non usano più i servizi offerti da spaggiari.

Aggiornamento 07/03/2023
Dopo aver discusso con il vicepreside della mia scuola, è stata decisa la rimozione temporanea delle fototessere al fine di garantire la privacy.
Nonostante ciò, alcuni studenti che sono stati bocciati o che hanno abbandonato la scuola sono ancora presenti.

Cordialmente

Padova, 27/02/2023

Yassine Zarouali
Giasin@giaflix.it