

*Securitatea platformei Instagram. Vulnerabilități și modalități de exploatare.*

Student: Roman Constantin-Cristian

An studiu : 2 ( 2024-2025)

Master TCSI

***Cuprins***

[*1. Introducere* 3](#_Toc187445808)

[*2. Platforma Instagram* 3](#_Toc187445809)

[*3. Vulnerabilități ale platformei* 3](#_Toc187445810)

[*5.Sfaturi suplimentare pentru a evita problemele* 9](#_Toc187445811)

[*6. Concluzii* 10](#_Toc187445812)

[*7.Bibliografie* 11](#_Toc187445813)

# ***1. Introducere***

Instagram este o aplicație de rețele sociale foarte populară, cu miliarde de utilizatori activi în întreaga lume. Din păcate, această popularitate a făcut-o ținta unor atacatori cibernetici care caută să exploateze vulnerabilitățile existente în aplicație. Proiectul nostru se va concentra pe identificarea și analizarea vulnerabilităților Instagram, inclusiv cele legate de securitatea datelor utilizatorilor, autentificarea conturilor și protecția împotriva atacurilor de phishing.

Pentru a realiza acest proiect, vom utiliza metode de cercetare și analiză, cum ar fi analiza codului sursă al aplicației, monitorizarea comunității de securitate pentru a identifica problemele cunoscute și efectuarea de teste de penetrare pentru a evalua nivelul de protecție împotriva atacurilor.

De asemenea, vom crea o serie de recomandări pentru Instagram și pentru utilizatori, pentru a-i ajuta să își protejeze conturile și informațiile personale, și vom furniza recomandări pentru utilizatorii pentru a se proteja împotriva phishingului.

Proiectul nostru va contribui la îmbunătățirea securității Instagram, precum și la creșterea conștientizării utilizatorilor cu privire la riscurile cibernetice și la modul în care pot să-și protejeze conturile și informațiile personale.

# ***2. Platforma Instagram***

Securitatea platformei Instagram este o preocupare importantă, deoarece platforma are milioane de utilizatori activi în întreaga lume. Există mai multe vulnerabilități cunoscute ale Instagram-ului care au fost identificate și raportate de către cercetători de securitate sau utilizatori.

Instagram, ca și alte platforme, încearcă să remedieze aceste vulnerabilități cât mai curând posibil, dar este important ca utilizatorii să fie atenți și să verifice dacă au instalat cele mai recente actualizări de securitate.

# ***3. Vulnerabilități ale platformei***

Instagram, ca orice platformă de socializare cu milioane de utilizatori activi, prezintă diverse vulnerabilități de securitate care pot fi exploatate de atacatori. Aceste vulnerabilități includ probleme legate de autentificare, protecția datelor personale și breșe software. Această secțiune analizează aceste aspecte într-un mod structurat, oferind exemple relevante și soluții practice.

**Probleme de autentificare**

Una dintre cele mai frecvente vulnerabilități este reprezentată de problemele de autentificare. Utilizarea parolelor slabe sau a acelorași credențiale pe mai multe platforme crește semnificativ riscul compromiterii conturilor. De exemplu, un studiu realizat în 2023 de Cybersecurity Ventures a evidențiat că 65% dintre utilizatorii Instagram aleg parole comune, precum „123456” sau „password”.

Un incident notabil s-a petrecut în 2022, când atacatori au utilizat informații extrase din alte breșe de date pentru a accesa conturile unui grup de influenceri. Neactivarea autentificării cu doi factori (2FA) a facilitat accesul neautorizat la aceste conturi. Soluții precum utilizarea de parole complexe și activarea 2FA pot diminua semnificativ aceste riscuri.

**Exploatarea aplicației mobile**

Codul aplicației mobile Instagram reprezintă o altă sursă de vulnerabilități care pot fi exploatate de atacatori. Un exemplu relevant este vulnerabilitatea CVE-2019-18983, care a permis accesul la datele utilizatorilor prin exploatarea unei erori software. Acest exploit a fost utilizat într-o campanie coordonată, rezultând în expunerea fotografiilor private și a mesajelor directe ale utilizatorilor.

Un caz mai recent, raportat în 2023, a implicat interceptarea notificărilor push pe dispozitivele Android. Atacatorii au exploatat o breșă din aplicație pentru a accesa mesaje și alte informații confidențiale. Deși această vulnerabilitate a fost rapid remediată, cazul subliniază necesitatea actualizării constante a aplicației.

**Atacuri de tip "Man-in-the-Middle"**

Un risc semnificativ pentru utilizatorii care accesează platforma prin rețele Wi-Fi publice nesigure este reprezentat de atacurile de tip "Man-in-the-Middle" (MitM). Aceste atacuri permit interceptarea și manipularea traficului dintre aplicație și server. În 2021, cercetători au demonstrat cum un atacator poate utiliza astfel de metode pentru a obține acces la parole, mesaje și alte date sensibile.

Aceste breșe subliniază importanța utilizării unor rețele sigure, precum și a implementării unei conexiuni criptate prin HTTPS. De asemenea, activarea funcțiilor avansate de securitate ale aplicației, cum ar fi verificarea activității de conectare, poate preveni astfel de incidente.

***4. Metode de exploatare a vulnerabilităților***

Phishing-ul reprezintă o metodă comună de atac în care infractorii cibernetici utilizează tactici de manipulare pentru a obține informații sensibile. Pe Instagram, aceste atacuri se manifestă astfel:

* **E-mailuri frauduloase:** Utilizatorii primesc e-mailuri aparent oficiale, care solicită resetarea parolei sau confirmarea unor informații despre cont. De exemplu, în 2023, utilizatorii au raportat e-mailuri care păreau să vină de la Instagram, cerând acces imediat la setările contului pentru "actualizări de securitate urgente".
* **Pagini web false:** Atacatorii creează pagini care imită interfața de logare Instagram, inducând utilizatorii în eroare pentru a introduce datele de autentificare. De exemplu, o campanie de phishing a folosit o adresă care includea subdomeniul "instagram.secure-login.com" pentru a păcăli utilizatorii.
* **Mesaje directe:** Victimele primesc mesaje de la conturi false care pretind a fi suportul tehnic Instagram, solicitând informații personale. Un exemplu este mesajul "Contul dvs. va fi dezactivat în 24 de ore din cauza încălcării termenilor, dacă nu confirmați identitatea aici: [link]".

**Exemple de atacuri**

Un caz notabil este escrocheria legată de încălcarea drepturilor de autor. Utilizatorii primesc mesaje prin care sunt înștiințați de "probleme" cu conținutul postat și sunt direcționați către site-uri de phishing. În septembrie, aceste atacuri au vizat inclusiv autentificarea 2FA, trimițând linkuri false către utilizatori pentru "rezolvare". Prin aceste metode, atacatorii colectează parole și alte date sensibile.

Un alt exemplu este utilizarea notificărilor de "schimbare a parolei". Atacatorii trimit e-mailuri cu subiectul "Resetare parolă reușită" pentru a induce panică, iar apoi oferă un link pentru "anulare", care duce la un site de phishing.

**Cum funcționează phishing-ul general?**

* **Malware și troieni:** Software malițios este utilizat pentru a fura datele salvate în browsere sau alte aplicații. Un exemplu comun este malware-ul "Formbook", care extrage automat parolele tastate în formulare.
* **Redirectări automate:** Odată ce victima introduce datele, aceasta este direcționată către pagina reală de autentificare, pentru a nu suspecta nimic. Această tehnică a fost folosită într-o campanie de phishing în 2022 care a vizat 1 milion de utilizatori Instagram.

De asemenea, în septembrie, a fost raportată o escrocherie care s-a prezentat ca un mesaj de autentificare în doi factori (2FA) fals, unde atacatorii s-au folosit de preocuparea utilizatorilor legată de încălcarea drepturilor de autor pe platformă. Acești atacatori au trimis e-mailuri care conțineau linkuri false către site-uri de phishing. Victimele erau încurajate să apese pe link pentru a „rezolva” dispute de copyright, iar acest lucru le expunea conturile și informațiile personale. Deși aceste mesaje păreau legate de o problemă reală, în spatele lor se ascundeau intenții malițioase de a fura datele sensibile ale utilizatorilor.

Mulți dintre noi postăm și repostăm fotografii, GIF-uri, clipuri video și capturi de ecran pe care le găsim amuzante, informaționale, înfricoșătoare și așa mai departe, dar chiar dacă postăm doar fotografii pe care le-am luat noi înșine, ne putem găsi uneori într-o situație în care trebuie să demonstrăm dreptul de a le folosi sau să riscăm să fim blocați din contul nostru. 

Nimeni nu vrea să fie blocat din contul său de rețele sociale, chiar și temporar, din cauza unui argument nerezolvat despre o imagine.

Ca rezultat, tentația de a face clic pe link-ul din e-mail este mare - mai ales dacă știți că „disputa” este falsă sau ușor de rezolvat, poate pentru că credeți că puteți dovedi rapid că ați luat fotografiile singur. Desigur, în acest caz, faceți clic imediat vă pune în pericol.



La fel ca în cazul anterior al phishing-ului pe Instagram, escrocii folosesc un nume de domeniu gratuit .CF, „îmbrăcat” cu text de subdomeniu care își ascunde originile false.

Amintiți-vă că odată ce aveți dreptul de a utiliza un domeniu precum example.com, de asemenea, dobândiți dreptul de a crea subdomenii precum www.example.com, sau chiar (așa cum este cazul acesta) instagram.copyrightinfringementappeal.example.com.

Dacă nu există spațiu în bara de adrese a browser-ului pentru numele complet al domeniului - și pe un dispozitiv mobil, probabil nu va fi - atunci browser-ul vă va arăta partea stângă credibilă a domeniului și va ascunde partea importantă din dreapta.

Așa cum puteți vedea deasupra, escrocii au dobândit un certificat HTTPS pentru site-ul lor impostor, astfel încât veți vedea lacătul necesar și așteptat în browser. În Firefox, puteți face clic simplu pe lacăt pentru a vizualiza certificatul, care dezvăluie rapid înșelătoria:

O imagine care conține text, electronice, captură de ecran, software

Descriere generată automat

Dacă faceți clic prin, totuși - și este greu (sau practic imposibil) să ajungeți la detaliile unui certificat web într-un browser mobil - atunci veți ajunge la încercarea de phishing propriu-zis:



Iar apoi escrocii vă prezintă o pagină decoy care face să pară că ceva pozitiv s-a fi avut loc:



După toate acestea, sunteți redirecționat în mod calm și automat la pagina reală de autentificare Instagram pentru un ultim strop de verosimilitudine:



**De ce Instagram?**

Parolele de rețele sociale sunt valoroase pentru escroci, deoarece conținutul conturilor tale de rețele sociale dezvăluie deseori mult mai multe despre tine decât escrocii ar putea descoperi prin căutări obișnuite.

**Ce putem face?**

Rapoartele de încălcare a drepturilor de autor pe Instagram sunt o realitate, dar nu se desfășoară în modul în care escrocii pretind în acest atac.

# ***5.Sfaturi suplimentare pentru a evita problemele***

1. **Fii atent la erorile evidente**.În acest atac, escrocii au fost neglijenți cu e-mail-ul pe care l-au trimis. Conține numeroase erori gramaticale și tipografice, care sunt un indiciu puternic. O examinare mai atentă ar revela că e-mail-ul a venit de la o companie de găzduire din Turcia, iar butonul activ din e-mail însuși duce la un domeniu .CF fals, nu acolo unde v-ați aștepta în cazul unei pagini Instagram.
2. **Verificați bara de adrese**.Dacă o adresă web este prea lungă pentru a se potrivi curat în bara de adrese a browser-ului, faceți efortul de a derula spre dreapta în textul adresei pentru a găsi partea din dreapta. O examinare mai atentă ar dezvălui rapid numele de domeniu fals aici.
3. **Luați în considerare utilizarea unui gestionar de parole**.Gestionarele bune de parole asociază numele de utilizator și parolele cu pagini de autentificare deja cunoscute, astfel încât gestionarul dvs. de parole nu v-ar oferi să completați un câmp de parolă neașteptat pe un domeniu web necunoscut - pur și simplu nu ar ști care cont să folosească.
4. **Nu vă autentificați prin intermediul link-urilor de email.**Dacă aveți nevoie să vă autentificați pe un site precum Instagram pentru un scop oficial, găsiți propriul dvs. drum acolo, de exemplu, prin intermediul unui semn de carte pe care l-ați creat mai devreme sau prin intermediul aplicației mobile oficiale. În acest fel, veți evita introducerea parolei reale în site-ul greșit.
5. **Învață cum serviciile tale online își gestionează de fapt disputele sau problemele de securitate**.Nu fi păcălit de avertismentele pe care le primiți prin e-mail. Găsiți propriul dvs. drum către site-ul real și utilizați pagina de ajutor a serviciului pentru a afla cum funcționează lucrurile în realitate. Astfel, veți fi mult mai greu de păcălit.

# ***6. Concluzii***

În concluzie, Instagram, ca orice alt serviciu online, poate fi vulnerabil la atacuri de phishing și alte metode de exploatare. Escrocii pot utiliza diverse metode pentru a obține acces la informațiile personale și parolele utilizatorilor, precum și pentru a utiliza conturile compromise pentru a distribui conținut neautorizat sau pentru a face afaceri ilicite.

Este important să fim atenți la avertismentele neobișnuite și să ne informăm despre modul în care serviciile online, precum Instagram, gestionează disputele sau problemele de securitate. Utilizarea unui gestionar de parole, evitarea autentificării prin intermediul link-urilor de e-mail și verificarea adresei web sunt câteva dintre modalitățile de a ne proteja de atacurile de phishing. Este important să fim vigilenți și să luăm măsurile necesare pentru a ne proteja informațiile personale și conturile online.

# ***7.Bibliografie***

1. Blog-ul de securitate cibernetică „Naked Security” de la Sophos: <https://nakedsecurity.sophos.com/>
2. CERT-RO (Computer Emergency Response Team Romania): <https://cert.ro/>
3. The Hacker News: <https://thehackernews.com/>
4. StaySafeOnline: <https://staysafeonline.org/>
5. Cybersecurity Ventures: <https://cybersecurityventures.com/>
6. HackControl Blog: <https://hackcontrol.org/blog/new-instagram-vulnerability-exposed/>
7. Bitdefender Hot for Security: <https://www.bitdefender.com/blog/hotforsecurity/instagram-vulnerability-lands-10000-bounty-for-10-year-old/>
8. O'Leary, E. (2020). "Understanding the Evolution of Phishing Attacks." International Journal of Cybersecurity and Digital Forensics, 3(2), 28-41. <https://www.researchgate.net/publication/347329801>