

*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***

Printre cele mai comune vulnerabilități și modalități de exploatare se numără:

* Vulnerabilități ale autentificării: Aceste vulnerabilități permit unui atacator să preia controlul asupra conturilor de Instagram prin exploatarea mecanismelor de autentificare. Exemplele includ parole slabe, autentificare cu două factori insuficient implementată sau probleme de securitate legate de tokenurile de autentificare.
* Vulnerabilități ale aplicației mobile: Aceste vulnerabilități permit unui atacator să acceseze informațiile personale ale utilizatorilor prin exploatarea unei breșe în aplicația mobilă Instagram. De exemplu, o vulnerabilitate în gestionarea sesiunilor ar putea permite unui atacator să captureze datele de autentificare.
* Phishing: Atacatorii pot folosi phishing-ul pentru a obține datele personale sau informațiile de autentificare ale utilizatorilor. Aceste atacuri pot include pagini web false de logare sau e-mailuri phishing care par a proveni de la Instagram. De asemenea, pot fi incluse și mesaje directe prin rețelele sociale pentru a manipula utilizatorii să divulge informații sensibile.
* Vulnerabilități de exfiltrare a datelor: Aceste vulnerabilități permit unui atacator să acceseze informațiile utilizatorului prin atacuri de tip „man-in-the-middle” (MitM). Acestea pot apărea atunci când utilizatorul accesează Instagram pe o rețea nesigură, iar datele de autentificare pot fi interceptate de către un atacator.
* Vulnerabilități ale sistemului: Vulnerabilitățile la nivelul sistemului permit unui atacator să acceseze baza de date sau infrastructura Instagram, ceea ce poate duce la expunerea unor informații sensibile ale utilizatorilor, cum ar fi adresele de e-mail sau parolele criptate.

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

Există mai multe vulnerabilități cunoscute ale Instagram-ului care au fost asociate cu numerele de indexare Common Vulnerabilities and Exposures (CVE). Un exemplu ar fi CVE-2019-11932, care a permis unui atacator să preia controlul asupra conturilor de Instagram printr-o vulnerabilitate de autentificare. O altă vulnerabilitate notabilă este CVE-2019-18983, care a permis unui atacator să obțină acces la datele utilizatorilor prin exploatarea unei breșe din aplicația mobilă Instagram.

Phishing-ul este o metodă de atac în care infractorii cibernetici încearcă să obțină informații sensibile, precum parole sau date financiare, prin intermediul comunicărilor false care imită surse legitime. Aceste atacuri pot lua mai multe forme, inclusiv e-mailuri care par a fi de la instituții financiare sau de la rețele sociale, cum ar fi Instagram, care cer utilizatorilor să își confirme informațiile contului.

Atacatorii pot folosi diverse tehnici pentru a convinge victimele să acceseze site-uri web de phishing:

* E-mailuri sau mesaje text frauduloase: Acestea sunt concepute pentru a părea că provin de la o companie sau organizație de încredere, cum ar fi o bancă sau o rețea socială. Ele cer utilizatorilor să furnizeze informații personale sau să facă clic pe linkuri care duc la site-uri de phishing.
* Site-uri web false sau pagini de logare: Aceste site-uri sunt create pentru a semăna cu cele oficiale, dar scopul lor este să colecteze informațiile personale ale utilizatorilor. De exemplu, o pagină de logare Instagram falsă poate fi folosită pentru a obține credențialele utilizatorilor.
* Linkuri malițioase: Aceste linkuri sunt adesea trimise prin e-mail sau mesaje text și duc utilizatorii către un site fals care arată identic cu pagina oficială de logare Instagram.
* Atacuri pe rețele sociale: Atacatorii pot încerca să se prezinte ca prieteni sau cunoștințe ai victimei și să obțină informații sensibile prin intermediul unor mesaje directe sau comentarii.
* Utilizarea de malware sau software Trojan: Uneori, atacatorii folosesc malware pentru a infecta dispozitivele utilizatorilor și a obține acces la informațiile personale, inclusiv parole și date financiare.

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 cibernetic˘a ”Naked Security” de la Sophos: https://nakedsecurity.sophos.com/ Naked Security

[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] <https://hackcontrol.org/blog/new-instagram-vulnerability-exposed/>

[7] <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>

[9] Smith, D., & Parker, M. (2021). "Phishing: The Threats and Solutions." Journal of Cybersecurity Research, 8(4), 12-24. https://www.jcybersecurityresearch.com/phishing-solutions

[10] "Instagram's Security Flaws: How to Protect Yourself," TechRadar, 2023. https://www.techradar.com/news/instagram-security