Facebook Bug Bounty – H4ck *Instagram Live* dan mendapatkan 5000 USD

Assalamu’alaikum Wr. Wb.

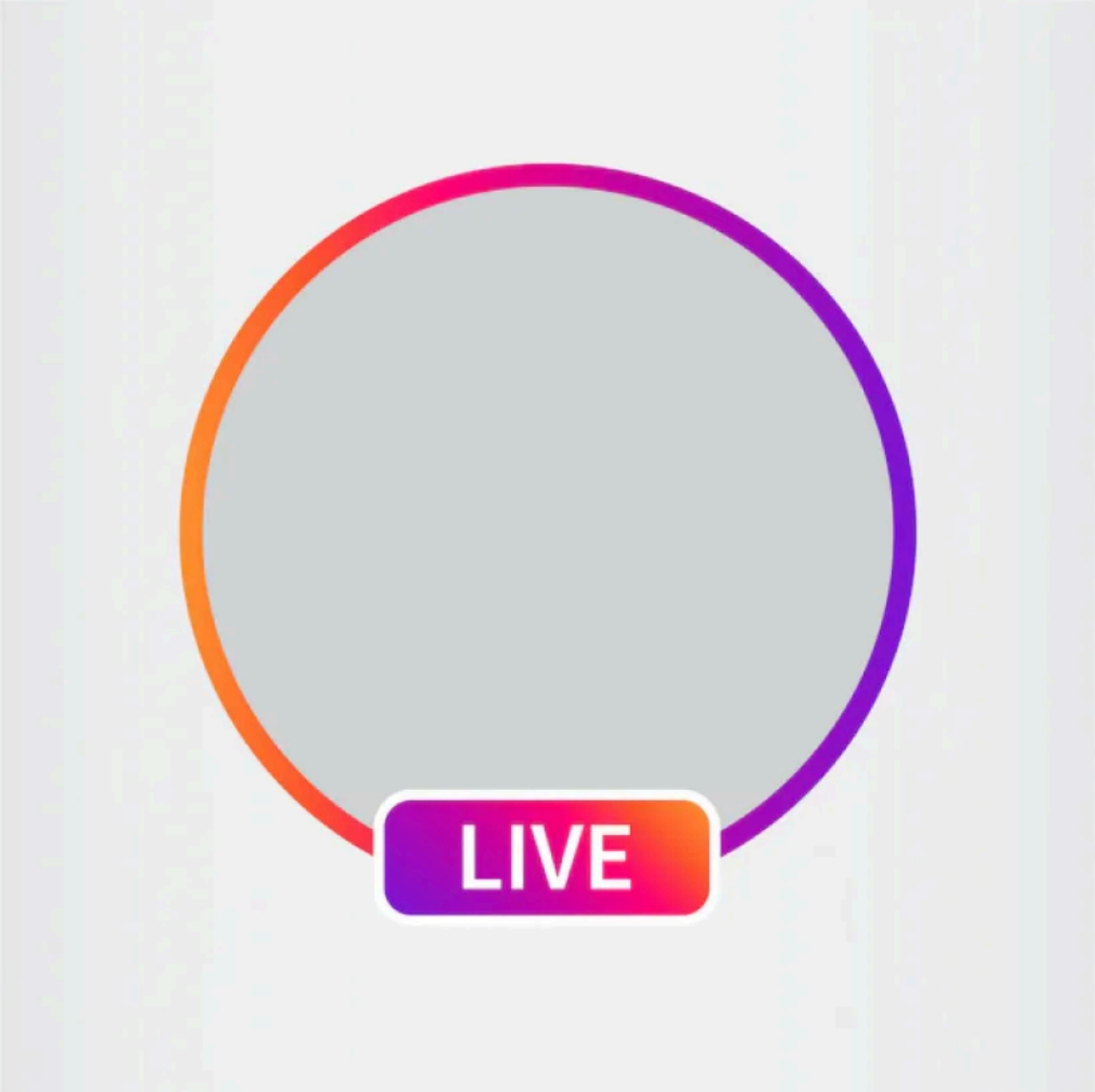
Salam sehat dan sukses untuk semuanya para bug hunter dimana pun anda berada. Kembali lagi bersama saya **rootbakar.** Pada kesempatan yang baik kali ini izinkan

saya untuk membagikan sebuah artikel temuan bug di salah satu platform yang paling sering di gunakan masyarakat di seluruh belahan dunia, apalagi kalo bukan **Instagram**. Dari yang tua sampai yang muda pasti tidak asing dengan sosial media yang satu ini, tapi jangan salah. Dibalik gemerlapnya fitur yang disediakan oleh Instagram terdapat pula bug di dalamnya, salah satunya yaitu di Fitur **Instagram Live**. Salah satu fitur yang paling sering rekan-rekan gunakan pastinya :).

Oke biar gk terlalu basa basi langsung aja yah cek bug seperti apa sih yang saya temukan dan bagaimana dampaknya untuk para pengguna Instagram pada saat melakukan **Live**. *Check this out*…..

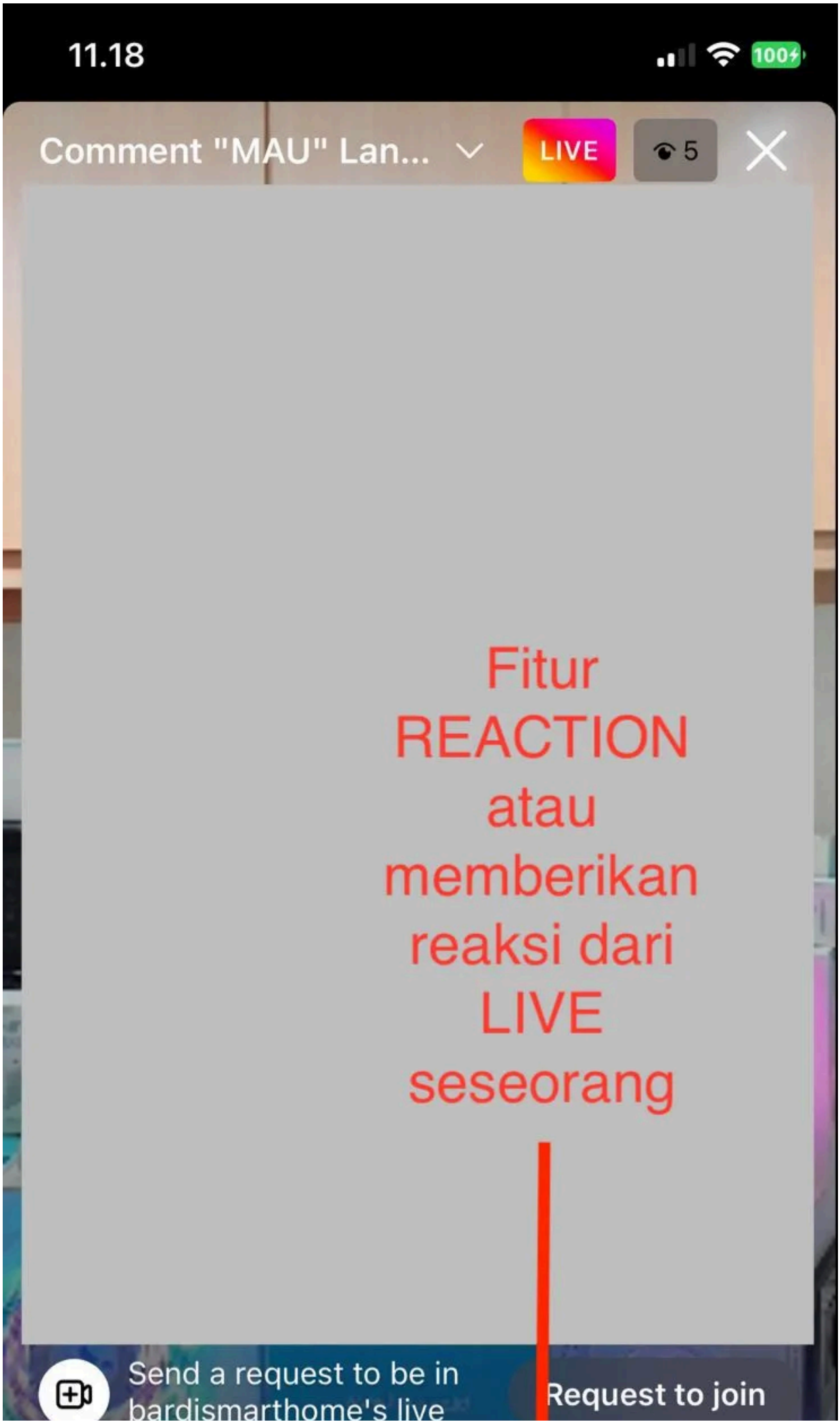
RESUME:

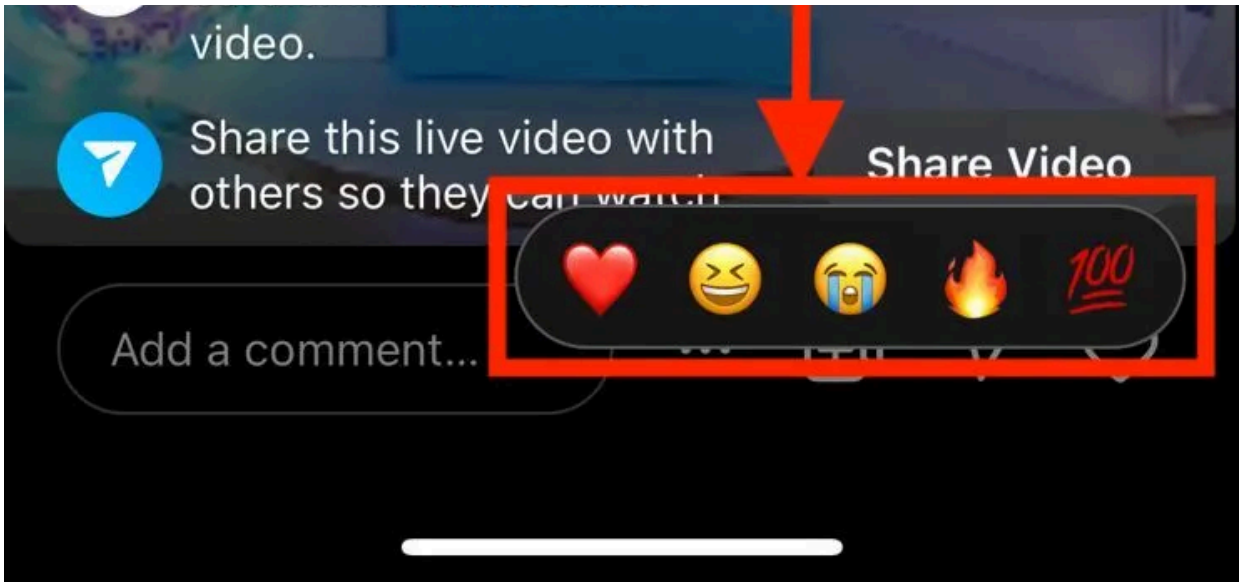
Bug ini saya temukan di fitur Live



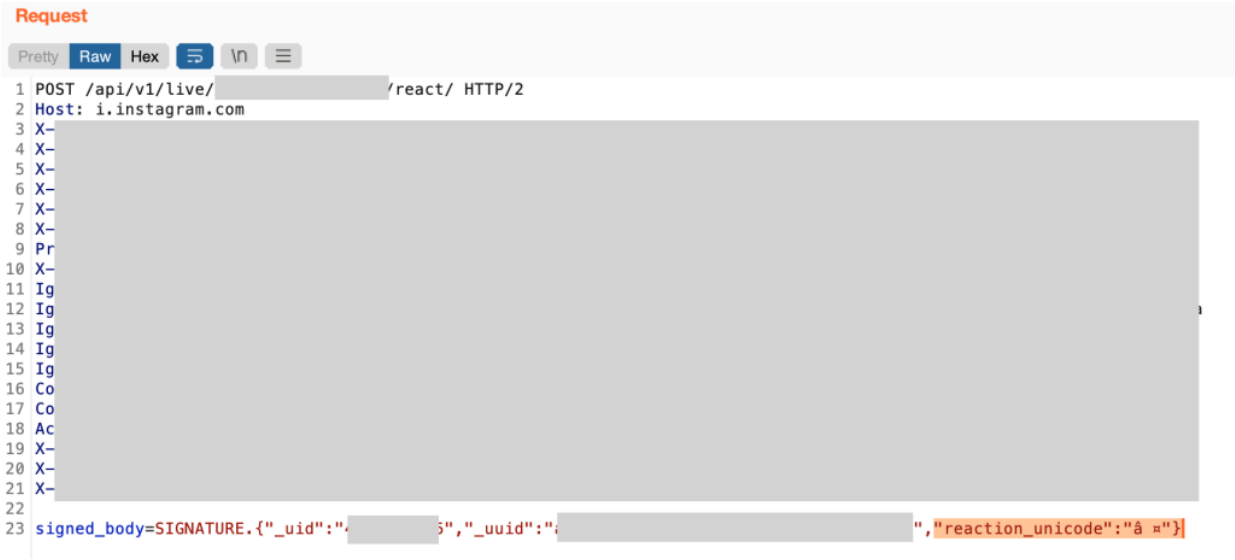
Pada saat seorang user yang terdaftar di **Instagram** baik yang sudah terverifikasi ataupun belum terverifikasi **(dengan catatan menggunakan perangkat/*device* *Android* jenis apapun dan merek apapun)** semuanya dapat terdampak oleh bug atau kerentanan ini. Sementara pada saat saya coba di pengguna ***iPhone*** masih aman dan damai, alias tidak terdampak oleh kerentanan ini.

Jadi pada saat seorang user melakukan *Live* di Instagram terdapat sebuah pilihan untuk mengirimkan *reaction* atau reaksi berupa icon *love, smile, fire* dan lain sebaginya.

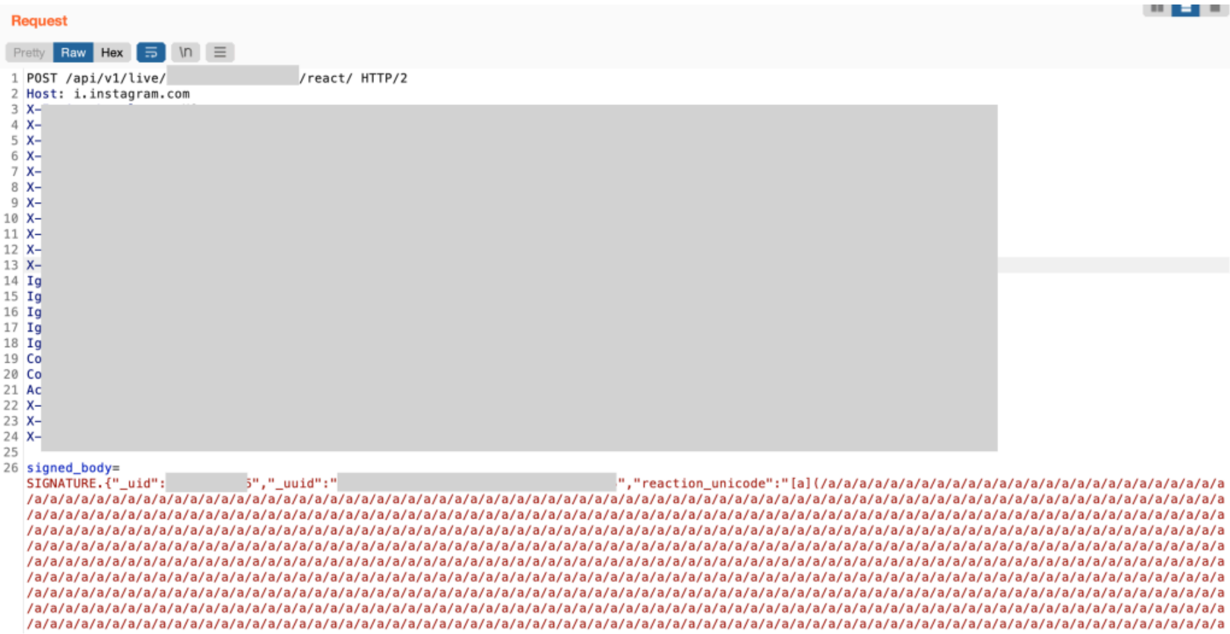

11.18
Comment "MAU" Lan...
LIVE
5
Fitur
REACTION
atau
memberikan
reaksi dari
LIVE
seseorang
Send a request to be in
bardismarthome's live
Request to join



Ketika *reaction* itu dikirimkan dan kita intercept dengan menggunakan *Burp Suite* akan mendapatkan *endpoint* ***/api/v1/live/{user_live_id}/react/*** dan terdapat *parameter* ***reaction_unicode***. Sampai disini saya sudah menemukan sebuah *vulnerable endpoint* dan *parameter* yang terdapat di fitur **Live** di **Instagram**.

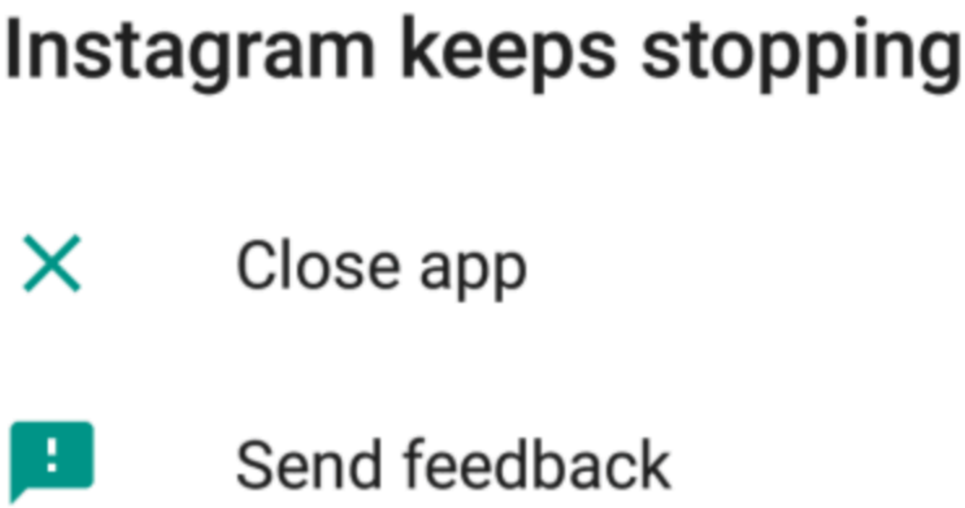


Original Request



Exploit Request

Oke sampai di baris ini, rekan-rekan dapat melihat bagaimana proses exploitasi ini dapat berdampak fatal bagi pengguna Instagram yang sedang melakukan Live, karena secara otomatis ketika serangan ini dijalankan user yang melakukan live ataupun yang menonton live akan secara otomatis ter*kick* atau terlempar keluar sesi live dan akan muncul pesan *error* atau *error warning* seperti di bawah ini.



Jika sudah muncul pesan eror seperti di atas, artinya user sudah berhasil di eksploitasi. Simple sih tapi nyakitin :), lagi enak nonton live malah keluar hehehehe.

PROOF OF CONCEPT:

1. User A login ke akun Instagram miliknya;
2. User B login dan melakukan *Live* di Instagram;
3. User A mencari akun User B dan bergabung di dalam *Live* tersebut;
4. User A mengirimkan reaksi dan melakukan intercept dengan menggunakan Burp Suite untuk mendapatkan *endpoint Live* Instagram User B tersebut;
5. User C dan User D juga bergabung di dalam *Live* tersebut;
6. User A mengirimkan *malicious request* dengan memanfaatkan langkah no 4 dan memasukan *payload* ke dalam parameter ***reaction_unicode***; dan
7. User B, User C dan User D semua berhasil di keluarkan dari *Live* tersebut.

TIMELINE:

- **Report:** June, 2022
- **Triage:** July, 2022
- **Fix:** July, 2022
- **Rewards:** July, 2022

HALL OF FAME:

Thanks!

On behalf of over three billion users, we would like to thank the following people for making a responsible disclosure to us:

2022 2021 2020 2019 2018 2017 2016 2015 2014 More

1. Youssef Sammouda
2. Neeraj Sharma
3. Sameer Rao
4. Marcos Vinicius Ferreira
5. Lokesh Kumar
6. Islam R AL said (zika)
7. Dzmitry Lukyanenka
8. Mustafa Ahmed
9. Brian McNulty
10. Robin Justin
11. Yaala Abdellah
12. Rikesh Baniya
13. Samuel Orellana
14. Ruben Bos
15. Mujahid Saifaldin Awad Sharif
16. Gtm Mänôz
17. Bassem M Bazzoun
18. Kassem Bazzoun
19. Nguyễn Quốc Khánh
20. Mariamo
21. Gowtham N
22. Joshua Regio
23. Rony K Roy
24. Nawaf Alkhaldi
25. Shanta Bahadur Gharti Magar
26. Samip Aryal
27. Fredmoore Damian
28. Dan Melamed
29. Ash King
30. Hamza Fourtassi
31. Robin Talaohu
32. Linus Särud
33. Lukas Gerlach
34. Antonio Macovei
35. Richard Telleng
36. Rey Julius Sanchez
37. Nan Wang
38. Dragos Albastroiu
39. साजन कार्की
40. Tom Van Goethem

Demikian writeup yang dapat saya tulis dan saya bagikan pada kesempatan kali ini, semoga tulisan ini dapat bermanfaat dan memotivasi rekan-rekan bug hunter yang lain. Jika ada kesalahan atau kekurangan pada penulisan kali ini saya sangat mengharapkan kritik dan masukan dari rekan-rekan bug hunter semua.

Terimakasih untuk semua pihak yang sudah berkenan bergabung ke *Live* yang saya buat pada saat reproduksi bug tersebut yang tidak bisa saya sebutkan satu persatu.

Salam sehat dan sukses untuk kita semua.

Best Regards,

rootbakar

Wassalamu'alaikum Wr. Wb.

By: rootbakar | **September 27, 2022** | Categories : Bug Bounty, Facebook, Write Up | Tags: bug bounty facebook live instagram rewards

‹ Apple Bug Bounty – How I Got $6000 From Apple Security Bounty

Misconfig on Try Wrong Password Lead To DoS ›

4 Replies to "Facebook Bug Bounty – H4ck *Instagram Live* dan mendapatkan 5000 USD"

test

September 27, 2022 at 19:03

nicceee

Reply

pr0gr35528

September 28, 2022 at 05:20

thanks

Reply

rescook

June 25, 2023 at 00:29

Apakah kerjanya seperti DOS sehingga mengakibatkan crash ?
Terimakasih apabila sudah menjawab
Salam hormat

Reply

rootbakar

July 8, 2023 at 18:48

iya bg kurang lebih sama

Reply

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment *

Name *

Email *

Website

Save my name, email, and website in this browser for the next time I comment.

POST COMMENT

FIND HERE

Search …

RECENT POSTS

[Tips & Trick] 0-Click Account Takeover via OSINT

P1 – Account Takeover via Forgot Password API

P1 – OTP Code Leak to Account Takeover

P3 – Panel Admin Takeover via Credential Leak on API Documentation Link

P1 – RCE Via Upload PDF File

CATEGORIES

Alibaba Security Response Center (1)

Apple (1)

Bug Bounty (28)

Bugcrowd (1)

Facebook (1)

Google VRP (1)

Hackerone (1)

Peris.ai (1)

Redstorm (5)

Tips (16)

Write Up (21)