



ECHO TALKS

17th Anniversary



“Bug Bounty: Do and Don’t” - @r_u_l_l_y

“How To Bypass Root and JailBreak
Detection “ - HA

“Drone Hacking 101” - MrPick

“Fun with BLE” - SMRX86

“Hacking: For Fun and For Career” -
the_day

Supported by



Bug Bounty: Do and Don't

@r_u_l_l_y

For Educational Purpose Only

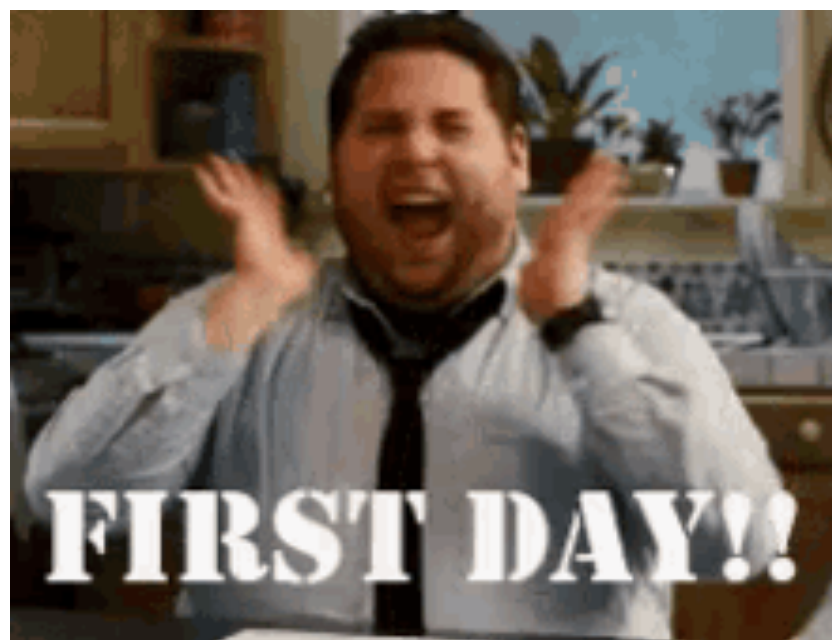


https://about.me/r_u_l_l_y

Bug bounty

February 2019





Bug report

Bounty hunters



☆ Yes, me 2

Inbox Tiket.com (Kerentanan Situs : **Tiket.com - Kerentanan Aplikasi**) - laporannya. Kerentanan ini sebelumnya sudah ...

Feb 5

Screen Shot 20... Tiket.com T...

☆ Raden, me 2

Inbox Fwd: Bug Bounty / Celah Keamanan di [REDACTED] Tiket.com - laporannya. Kerentanan ini sebelumnya sudah ada yan...

Feb 4

Screen Shot 20... Bug_Report... Bug_Report...

Previous reports

Duplicate

They report

E-mail

Private chat

Customer care

The form

Text

Screenshots

Docx

PDF

Video

From all of that

One



Sample cases



[REDACTED] <[REDACTED]12345@gmail.com>

Aug 8, 2019, 2:20 PM

to secops ▾



Indonesian ▾



English ▾

[Translate message](#)

[Turn off fo](#)

Selamat siang tiket com,

Saya telah menemukan bug yang cukup besar pada sistem tiket com yang apabila dibiarkan maka dapat merugikan pihak tiket com.

Tetapi anda harus memberikan kompensasi sebagai imbalan pada saya karena telah memberitahu bug yang besar pada sistem anda

Jadi, sebelum kejadian [TIKET.COM](#) kebobolkan lagi sama yang tidak bertanggung jawab sebaiknya segera di benahi, Melihat BUG seperti ini, kemungkinan bisa terjadi di fasilitas lain [TIKET.COM](#) yang berhubungan dengan POINT , SALI

6 minutes later



[REDACTED] <[REDACTED]@gmail.com>

Jul 21, 2019, 8:10 PM

to cs, secops ▾

🌐 Indonesian ▾ > English ▾ [Translate message](#)

[Turn off fi](#)

Maaf, Lupakan.

Sepertina saya yang salah memahami , cara kerja penukaran [REDACTED].

Maah kalau mengganggu.

regards,

[redacted] <[redacted]27@gmail.com>

Sun, Jun 9, 2:32 PM

to secops ▾

🌐 Indonesian ▾ > English ▾ [Translate message](#)

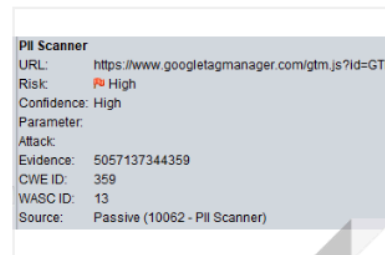
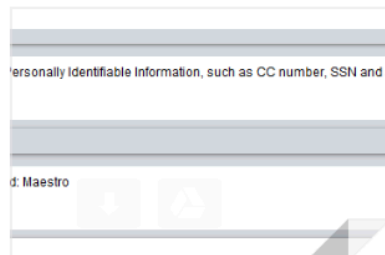
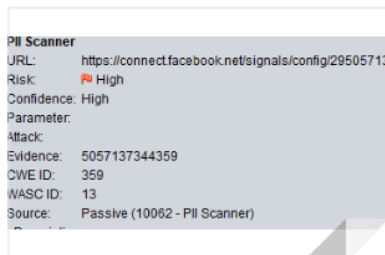
[Turn off fi](#)

Perkenalkan Nama Saya [redacted] Asal [redacted] Umur 16 Tahun Saya mendapatkan bug dari [tiket.com](#) dan saya mau melaporkan bug tersebut seperti yang 4 bug dari [tiket.com](#) yang bugnya semua berbahaya dan rentan terhadap informasi sensitif pelanggan dari [tiket.com](#)

PII Scanner adalah salah satu bug yang berbahaya karena dapat mengambil data identitas kartu pelanggan dan kemudian bisa berakibat dicuri atau dilakukan teknik carding yang d carding ini hanya memanfaatkan nomor cc dan angka dibelakang kartu tersebut untuk dipakai belanja dll


Bisakah Kita Kerja Sama????

3 Attachments



PII Scanner

URL: <https://connect.facebook.net/signals/config/295057137344359?v=2.8.51&r=stable>

Risk:  High

Confidence: High

Parameter:

Attack:

Evidence: 5057137344359

CWE ID: 359

WASC ID: 13

Source: Passive (10062 - PII Scanner)

Description:


The response contains Personally Identifiable Information, such as CC number, SSN and similar sensitive data.

Other Info:

Credit Card Type detected: Maestro

PII Scanner

URL: <https://www.googletagmanager.com/gtm.js?id=GTM-PLRJPPQ>

Risk:  High

Confidence: High

Parameter:

Attack:

Evidence: 5057137344359

CWE ID: 359

WASC ID: 13

Source: Passive (10062 - PII Scanner)

To: [REDACTED] <[\[REDACTED\]@tiket.com](mailto:[REDACTED]@tiket.com)>

Pada tanggal Sel, 11 Jun 2019 pukul 00.48 [REDACTED] <[\[REDACTED\]@gmail.com](mailto:[REDACTED]@gmail.com)> menulis:

Pada tanggal Min, 9 Jun 2019 pukul 18.16  <@tiket.com">[redacted]@tiket.com> menulis:

PoC (Proof of Concept) merupakan detail laporan dari **bug** yang anda temukan, minimal terdapat point-point seperti berikut :

1. Description (Penjelasan detail mengenai **bug** yang ditemukan)
2. Step to Reproduce (Merupakan langkah-langkah cara exploitsnya, beserta lampirkan bukti screenshotnya)
3. Impact (Dampak yang diberikan ketika **bug** berhasil diexploitasi)
4. Recommendation (rekomendasi yang diberikan)

~~_____~~

Source Code Disclosure - SQL

2 <https://cdn.jsdelivr.net/pouchdb/5.3.1/pouchdb.min.js>

C  High

vidence: Medium

parameter:

ck:

SELECT sql FROM sqlite_master WHERE tbl_name

EID: 540

3C ID: 13

rice: Passive (10099 - Source Code Disclosure)

[illegible]

Proper report

Description

Impact

Recommendation

Severity

OWASP Risk Rating

CVSS v3.1

Proof of Concept

Bug bounty program?



Want to report?

secops@tiket.com

Thank you