BIMANTARA
LABS

2022

Security Report

POSSIBLE SQL INJECTION

LET'S DEFEND

ABDI BIMANTARA

github.com/Abdibimantara

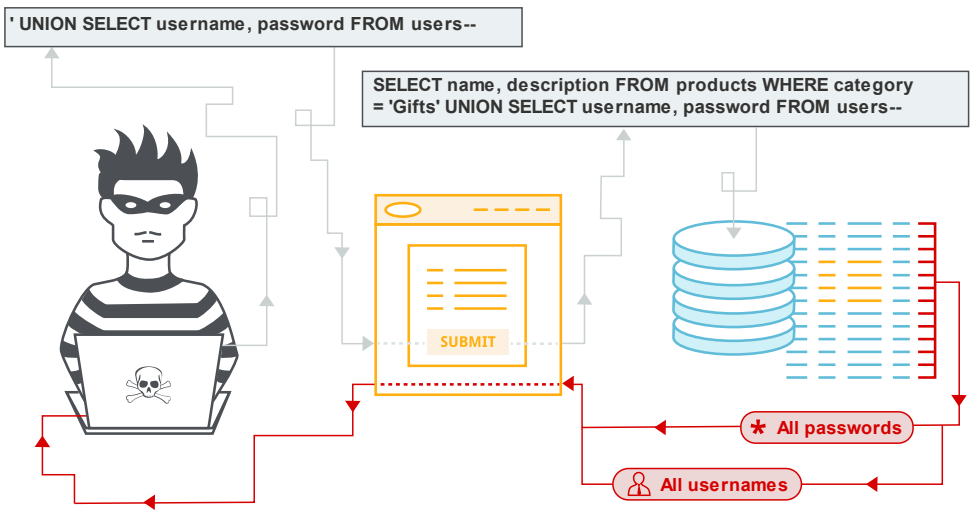
Latar Belakang

Tim SOC Menemukan Event pada dashboard monitoring yang diduga sebagai aktivitas SQL Injection pada tanggal 25 Februari 2022 di jam 4:12 am. Event tersebut memiliki nilai severity “High” dengan event id yaitu 115.

- Rule : SOC165 - Possible SQL Injection Payload Detected
- Destination IP : 172.16.17.18
- Source IP : 167.99.169.17
- Device Action : Allowed

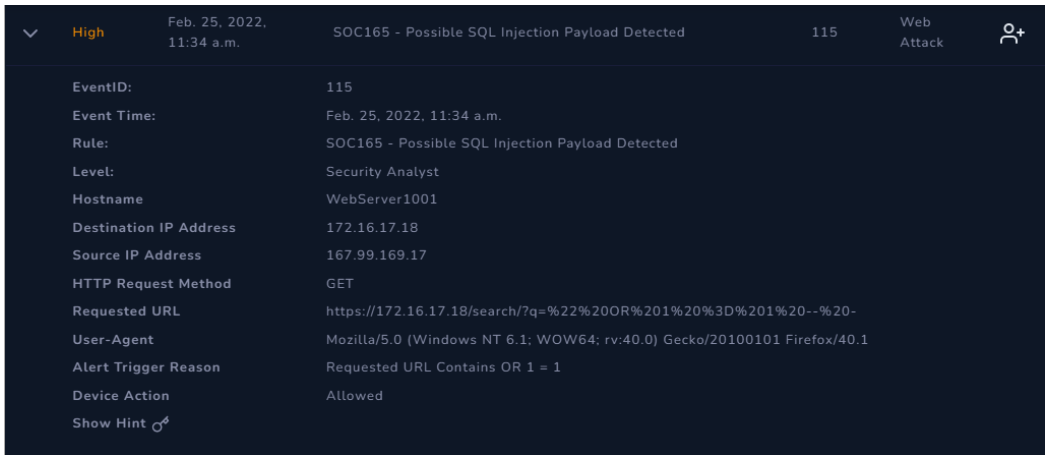
Deskripsi

SQL Injection merupakan salah satu teknik yang sering digunakan oleh attacker dalam memanfaatkan celah keamaan yang ada pada system database SQL pada lapisan basis data aplikasi. Celah tersebut dapat disebabkan oleh adanya proses input dan output yang tidak di filter dengan benar. Sebagai contoh , metode serangan SQL injection melalui form username e yang seharusnya hanya diisikan dengan karakter saja, namun pada hal ini form tersebut bisa diisi dengan karakterlainnya seperti (:;-=OR ORDER BY). Dari beberapa inputan tersebut dapat menyebabkan seorang attacker dapat memasukkan query SQL injection.



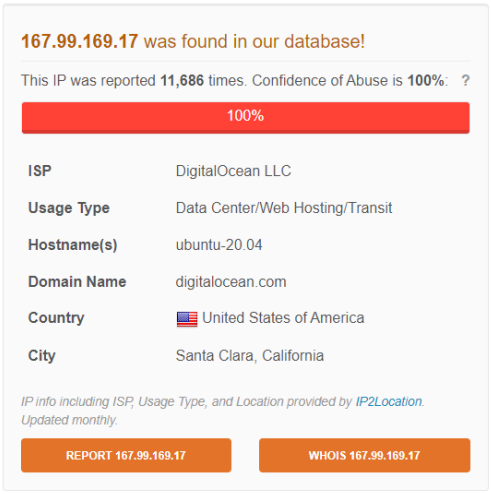
Hasil Temuan

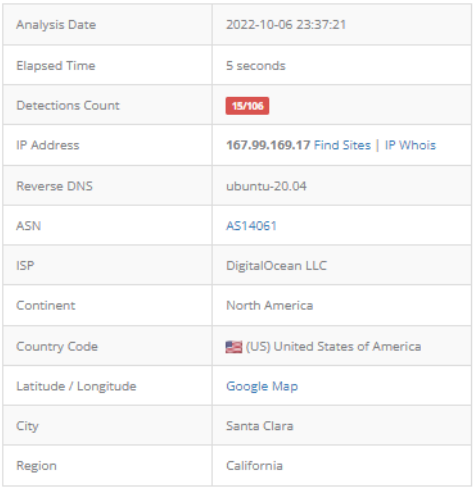
Pada tanggal 25 Februari 2022 di jam 4:12 am, tim SOC menemukan event yang diduga sebagai aktivitas SQL Injection. Event tersebut memiliki nilai severity high dan dapat dilihat pada gambar dibawah :



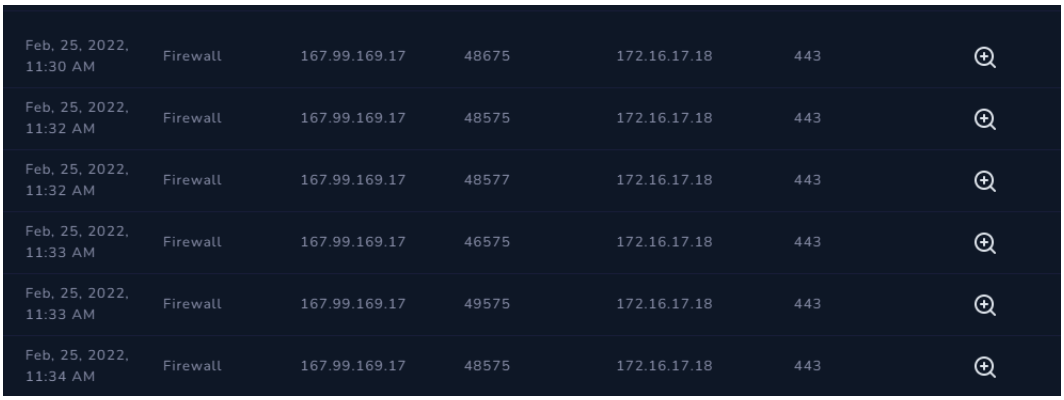
Analisa

Tim soc melakukan Analisa dengan diawali mengecek reputasi dari source ip tersebut. Setelah dilakukan pengecekkan, diketahui bahwa ip tersebut memiliki reputasi yang cukup buruk. Dimana Hal ini menandakan adanya indikasi serangan yang disebabkan oleh ip tersebut. sebanyak 12 vendor security pada virus totals menandai ip tersebut sebagai malicious, sebanyak 1168 laporan mengenai ip tersebut pada abuseipdb, pada ip void ip tersebut juga masuk dalam daftar blacklist dengan nilai sebesar 15/106.





Analisa dilanjutkan dengan mencari tahu aktivitas yang disebabkan oleh ip 167.99.169.17 menuju 172.16.17.18 pada log management. Terlihat pada gambar dibawah, traffic yang berasal dari ip 167.99.169.17 sebanyak 6 kali. Dimana semua traffic tersebut menuju ke ip 172.16.17.18.

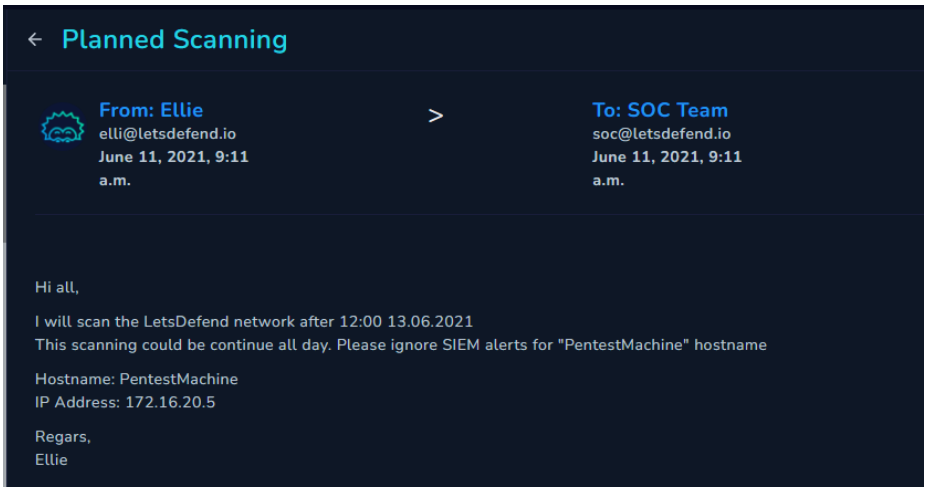


Beradasarkan data raw log, tim soc menemukan adanya indikasi payload SQL injection yang terdapat pada request url yang dibuat oleh ip 167.99.169.17. Payload sql injection berusaha diinputkan oleh attacker dengan maksud untuk mendapatkan aksess ke dalam database target yaitu 172.16.18. Berikut beberapa payload yang berhasil tim soc dapatkan :

- https://172.16.17.18/search/?q=%27%20OR%20%271
- https://172.16.17.18/search/?q=%27%20OR%20%27x%27%3D%27x
- https://172.16.17.18/search/?q=1%27%20ORDER%20BY%203--%2B
- https://172.16.17.18/search/?q=%22%20OR%201%20%3D%201%20--%20-

Terlihat dari beberapa request yang dibuat oleh ip 167.99.169.17 memuat payload sql injection. Dimana payload tersebut menggunakan karakter “OR, --, ORDER BY”. Namun disini tim SOC mendapati bahwa response yang didapatkan dari payload tersebut adalah 500.

Kami mencoba melakukan koordinasi pada tim lapangan, dengan mengecek apakah ada kegiatan yang disengaja pada kedua ip tersebut dan menggunakan hostname “Webserver 1001”. Kami juga mengecek Email untuk mengetahui apakah ada notifikasi pesan mengenai kegiatan baik pada hostname serta kedua ip tersebut. Namun kami tidak menemukan apa apa, dan tim lapangan juga mengkonfirmasi tidak ada kegiatan lainnya.



Melihat dari konfirmasi dari tim internal bahwa tidak ada kegiatan, terindikasi bahwa pengguna ip tersebut berasal dari pihak luar (Eksternal). Sehingga kami Kembali melakukan pengecekkan pada Enpoint Security untuk mengetahui Riwayat perintah atau command yang kemungkinan dijalankan pada mesin target. Setelah ditelusuri, Tim SOC tidak menemukan command atau perintah sensitive.

Kesimpulan

Event tersebut merupakan True Positive, dibuktikan dengan adanya beberapa payload sql injection yang terdapat pada url req. Namun aktivitas request tersebut mendapakan response code 500 yang berati “Internal Server Error”. Sehingga event tersebut dapat ditutup dan tidak diperlukan action lebih lanjut.

Referensi

- https://app.letsdefend.io/
- https://github.com/payloadbox/sql-injection-payload-list