

Badan Siber dan Sandi Negara (BSSN) mencatat Komisi Pemilihan Umum (KPU) mengalami 28,8 juta percobaan serangan siber terhadap server KPU sepanjang 2018 hingga 23 Mei 2019. BSSN mengungkapkan setidaknya ada beberapa jenis serangan siber yang dialami KPU.

Pertama, jenis serangan *Information Leakage*. Direktur Deteksi Ancaman BSSN Sulistyو mengatakan jenis serangan ini berada pada peringkat pertama dengan jumlah 12,9 juta.

"*Information Leakage* terdapat kerawanan pada sistem yang menyebabkan informasi sensitif dapat diketahui oleh penyerang. Penyerang dapat memanfaatkan informasi tersebut untuk menembus ke sistem," kata Sulistyو saat dihubungi *CNNIndonesia.com*, Kamis (12/7).

Kedua, jenis serangan *HTTP Parser Attack*. Sulistyو mengatakan jenis serangan ini berjumlah 2,1 juta.

"*HTTP Parser Attack* merupakan percobaan untuk mengeksekusi kode yang malicious, mengekstrak informasi atau menetapkan target DoS melalui *HTTP parser* secara langsung," kata Sulistyو.

Ketiga, serangan *Non-Browsing Client*. Jenis serangan ini berjumlah 879,2 ribu serangan. Sulistyو menjelaskan jenis serangan ini penyerang menggunakan suatu pengais (*crawler*), atau suatu script yang membuat simulasi seolah-olah manusia yang mengakses sistem tersebut.

Keempat, serangan *Cross Site Scripting (XSS)* dengan jumlah 549,9 ribu. Jenis serangan ini dilakukan dengan cara penyerang memasukkan kode HTML atau *client script code* suatu situs ke sistem situs lain. Oleh karena itu, serangan ini seolah-olah datang dari situs tersebut.

Kelima adalah *SQL Injection*. Jenis serangan ini berjumlah 512,3 ribu. Serangan ini mampu membuat peretas mendapatkan akses ke dalam sistem.

Keenam, *Predictable Resource Location* yakni serangan yang akan mengungkap secara paksa lokasi suatu file sensitif yang seharusnya tidak dipublikasikan. Jenis serangan ini berjumlah 338,4 ribu.

"Lokasi suatu file pada sistem yang mudah diprediksi sehingga memudahkan penyerang dalam melakukan serangan," kata Sulistyو.