BAB I
PENDAHULUAN

1.1. LATAR BELAKANG

Perkembangan teknologi informasi bergerak begitu cepat, penggunaan teknologi informasi telah diterapkan pada berbagai bidang pekerjaan dan layanan. Penggunaan teknologi informasi dapat mempersingkat proses bisnis yang diperlukan, mempercepat pengerjaan suatu tugas, dan menghemat biaya yang mungkin dikeluarkan dalam pelaksanaan pelayanan publik. Salah satu bentuk dari teknologi informasi yang sering digunakan dalam penyelenggaraan layanan publik adalah aplikasi berbasis web. Badan Siber dan Sandi Negara (BSSN) selaku Instansi Pemerintah turut serta menyelenggarakan layanan yang bergerak pada bidang keamanan siber dan sandi. Salah satu bentuk layanan tersebut yakni akan diselenggarakannya program *bug bounty* pada sektor pemerintah melalui *Voluntary Vulnerability Identification and Protection Program* (VVIP Program). VVIP Program adalah sebuah program pencarian kerentanan secara terbuka atau biasa dikenal sebagai *bug bounty*. *Bug bounty* atau disebut juga sebagai imbalan kerentanan adalah program pencarian kerentanan perangkat lunak yang dapat dieksploitasi pada sebuah aplikasi. Program *bug bounty* dilakukan secara terbuka kepada para *bug hunter* yang meliputi namun tidak terbatas pada peneliti keamanan independen, *penetration tester*, dan *white hat hacker* [1].

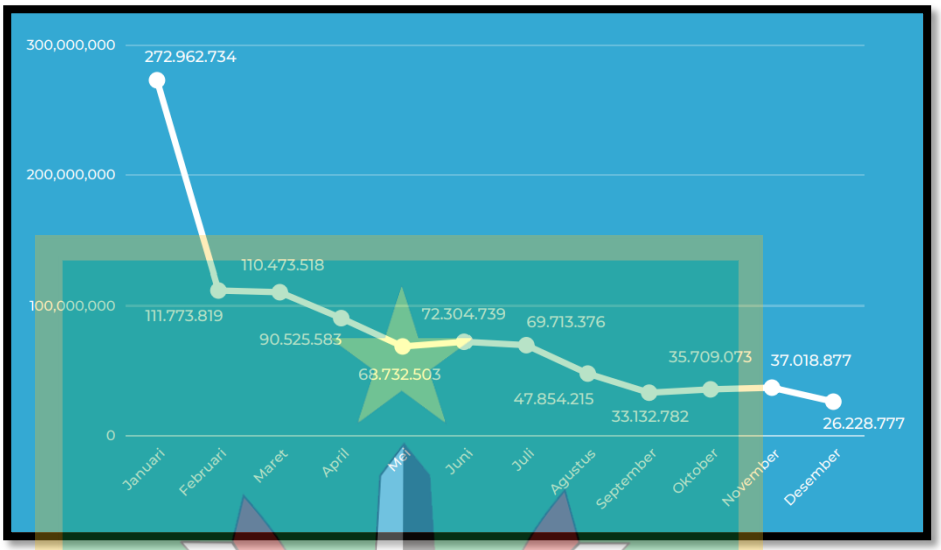
Program *bug bounty* seringkali dilakukan melalui sebuah platform yang menghubungkan antara penyelenggara program *bug bounty*, pemilik aplikasi yang akan diuji, dan para *bug hunter*. Termasuk pada Program VVIP yang akan diluncurkan oleh BSSN, terdapat sebuah platform dalam bentuk aplikasi berbasis web yang akan digunakan sebagai portal pendaftaran para *bug hunter* dan para instansi yang ingin mengikuti program tersebut. Saat ini *platform* tersebut masih dalam tahap pengembangan dan pengujian keamanan aplikasi sebelum resmi diluncurkan. Pengujian keamanan sendiri diperlukan untuk mengetahui celah kerentanan yang ada pada aplikasi sehingga mengurangi risiko dimanfaatkannya celah kerentanan pada aplikasi dan mengurangi risiko

terjadinya kebocoran data [2]. karena data yang disimpan pada aplikasi termasuk data sensitif berupa identitas yang digunakan pada tahap registrasi bug hunter.

Gambar 1 Voluntary Vulnerability Identification and Protection Program (VVIP Program)

Berdasarkan hasil monitoring yang dilakukan oleh BSSN, pada tahun 2022 terdapat 976.429.996 anomali serangan yang terjadi di Indonesia [3]. Dari banyaknya anomali tersebut, sebanyak 2348 kasus diantaranya menjadi sebuah insiden *web defacement*. Serangan *web defacement* merupakan serangan yang dilakukan untuk mengeksploitasi sebuah aplikasi web atau server web yang rentan dengan memanfaatkan kerentanan dari sistem sehingga penyerang dapat memodifikasi, merusak, dan menghapus konten halaman web yang menjadi target [4]. Sektor yang paling banyak terdampak dari serangan tersebut adalah sektor pemerintah dengan jumlah 855 insiden terdeteksi. Hal ini menunjukan bahwa kerentanan aplikasi milik pemerintah masih sering menjadi target dan seringkali rentan terhadap serangan yang dilakukan oleh pihak-pihak tidak bertanggung jawab. Oleh karena itu, upaya

keamanan perlu dilakukan untuk menghindari aplikasi dari serangan yang dapat mengancam aplikasi yang dimiliki [5].



Gambar 2 Tren Anomali Trafik Keamanan Siber Tahun 2022

Banyak teknik dan metode yang dapat digunakan dalam upaya melakukan pengamanan terhadap aplikasi yang kita miliki dari ancaman serangan, diantaranya adalah pelaksanaan *vulnerability scanning*/pemindaian kerentanan, *penetration testing*/pengujian keamanan, audit keamanan informasi, penerapan *web application firewall* (WAF), *intrusion detection system* (IDS). *intrusion prevention system* (IPS), dan enkripsi server [6]. Pada penelitian ini, akan dilakukan salah satu upaya keamanan aplikasi melalui kegiatan audit keamanan informasi. Audit keamanan informasi adalah suatu proses pengumpulan data dan evaluasi bukti terhadap penerapan mekanisme-mekanisme dalam sebuah standar/kebijakan untuk menetapkan apakah suatu sistem informasi telah menerapkan standar/kebijakan dengan tepat atau belum [7]. Audit keamanan informasi dilakukan untuk mengetahui apakah aplikasi telah menerapkan upaya keamanan sehingga dapat terlindungi dengan baik dan juga menjamin kerahasiaan, ketersediaan, dan integritas data yang disimpan pada aplikasi. Pelaksanaan audit diharapkan mampu memberikan informasi terkait tingkat keamanan aplikasi, serta menghasilkan rekomendasi untuk meningkatkan keamanan dari aplikasi tersebut. Oleh karena itu, pada

penelitian ini akan dilakukan audit keamanan informasi pada aplikasi yang digunakan sebagai portal pelaksanaan program VVIP yang akan diluncurkan oleh BSSN. Aplikasi akan diaudit menggunakan standar keamanan aplikasi berbasis web yang dikeluarkan oleh *Open Web Application Security Project Foundation* (OWASP Foundation), sebuah organisasi nirlaba yang berdedikasi untuk meningkatkan keamanan aplikasi web [8]. Standar tersebut adalah *OWASP Application Security Verification Standard* (OWASP ASVS).

1.2. RUMUSAN MASALAH

Berdasarkan latar belakang yang telah dijelaskan, maka dibuat rumusan masalah pada penelitian ini, yakni bagaimana proses pelaksanaan audit keamanan informasi pada aplikasi portal program VVIP berdasarkan standar *OWASP Application Security Verification Standard*.

1.3. PEMBATASAN MASALAH

Berdasarkan rumusan masalah tersebut, maka diberikan beberapa pembatasan masalah sebagai berikut:

a. Pada penelitian audit dilakukan berdasarkan *requirement* yang dipersyaratkan pada OWASP ASVS Level 1;
b. Metode audit yang digunakan pada penelitian ini adalah metode wawancara, observasi langsung dan pengujian keamanan/*penetration testing*.

1.4. TUJUAN PENELITIAN

Tujuan yang ingin dicapai dari penelitian ini adalah sebagai berikut :

a. Mengetahui tingkat penerapan standar keamanan pada aplikasi portal VVIP
b. Melakukan analisis peningkatan keamanan aplikasi portal VVIP
c. Memberikan rekomendasi untuk peningkatan nilai keamanan aplikasi portal VVIP

1.5. MANFAAT PENELITIAN

Ditinjau dari segi akademis, hasil dari penelitian ini diharapkan dapat memberikan pemahaman dan pengetahuan terhadap pelaksanaan audit keamanan informasi menggunakan standar keamanan OWASP ASVS

Ditinjau dari segi praktis, hasil dari penelitian ini diharapkan dapat menjadi rekomendasi bagi pemilik aplikasi untuk mengetahui kesesuaian keamanan platform yang sedang dikembangkan untuk program VVIP sehingga mengurangi risiko dari serangan siber.

1.6. SISTEMATIKA PEMBAHASAN

Dokumen penelitian ini terdiri dari 6 bagian utama dengan rincian sebagai berikut :

BAB I : PENDAHULUAN

BAB II : LANDASAN TEORI

BAB III : METODOLOGI PENELITIAN

BAB IV : PEMBAHASAN

BAB V : ANALISIS DAN REKOMENDASI

BAB VI : KESIMPULAN DAN SARAN