BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan dunia Teknologi Informasi (TI) yang sangat pesat, mempunyai dampak positif di berbagai bidang, satu diantaranya bidang teknologi *website*. Jumlah pengguna semakin meningkat seiring dengan perkembangan internet saat ini. Hal ini terlihat dengan adanya tabel pengguna internet dari tahun 2019 sampai 2021 pada gambar 1.1.

TOP 20 COUNTRIES WITH THE HIGHEST NUMBER OF INTERNET USERS

TOP 20 COUNTRIES WITH HIGHEST NUMBER OF INTERNET USERS - 2021 Q1

#	Country or Region	Internet Users 2021 Q1	Internet Users 2000 Q4	Population, 2021 Est.	Population 2000 Est.	Internet Growth 2000 - 2021
1	China	854,000,000	22,500,000	1,439,062,022	1,283,198,970	3,796 %
2	India	560,000,000	5,000,000	1,368,737,513	1,053,050,912	11,200 %
3	United States	313,322,868	95,354,000	331,002,651	281,982,778	328 %
4	Indonesia	171,260,000	2,000,000	273,523,615	211,540,429	8,560 %
5	Brazil	149,057,635	5,000,000	212,392,717	175,287,587	2,980 %
6	Nigeria	126,078,999	200,000	206,139,589	123,486,615	63,000 %
7	Japan	118,626,672	47,080,000	126,854,745	127,533,934	252 %
8	Russia	116,353,942	3,100,000	145,934,462	146,396,514	3,751 %
9	Bangladesh	94,199,000	100,000	164,689,383	131,581,243	94,199 %
10	Mexico	88,000,000	2,712,400	132,328,035	2,712,400	3,144 %
11	Germany	79,127,551	24,000,000	83,783,942	81,487,757	329 %
12	Philippines	79,000,000	2,000,000	109,581,078	77,991,569	3,950 %
13	Turkey	69,107,183	2,000,000	84,339,067	63,240,121	3,455 %
14	Vietnam	68,541,344	200,000	68,541,344	200,000	34,250 %
15	United Kingdom	63,544,106	15,400,000	67,886,011	58,950,848	413 %
16	Iran	67,602,731	250,000	83,992,949	66,131,854	27,040 %
17	France	60,421,689	8,500,000	65,273,511	59,608,201	710 %
18	Thailand	57,000,000	2,300,000	69,799,978	62,958,021	2,478 %
19	Italy	54,798,299	13,200,000	60,461,826	57,293,721	415 %
20	Egypt	49,231,493	450,000	102,334,404	69,905,988	10,940 %
TOP 20 Countries		3,241,273,512	251,346,400	5,233,377,837	4,312,497,691	1,289 %
Rest of the World		1,332,876,622	109,639,092	2,563,237,873	1,832,509,298	1,216 %
Total World		4,574,150,134	360,985,492	7,796,615,710	6,145,006,989	1,267 %

NOTES: (1) Top 20 Internet Countries Statistics were updated for Dec 31, 2019. (2) Growth percentage represents the increase in the number of Internet users between the years 2000 and 2020. (3) The most recent user information comes from data published by Facebook, International Telecommunications Union, official country telecom reports, and other trustworthy research sources. (4) Data from this site may be cited, giving the due credit and establishing a link back to www.internetworldstats.com.

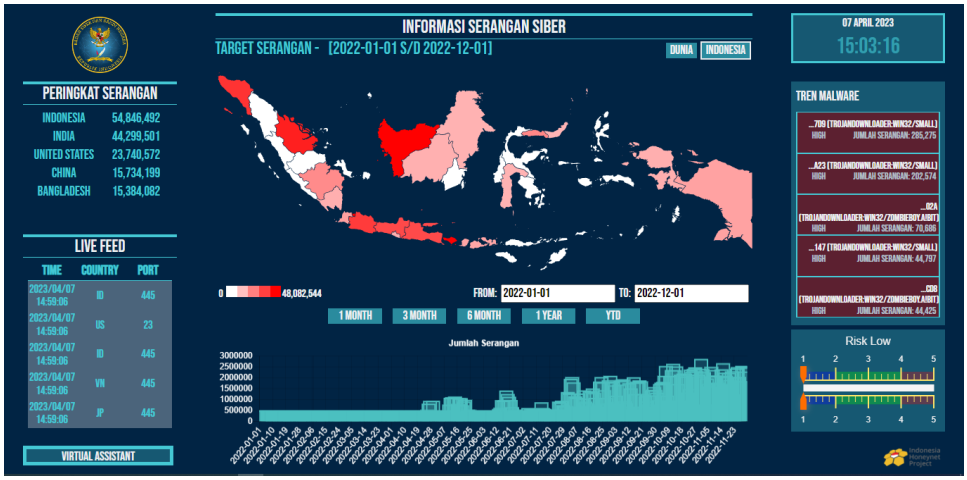
Gambar 1. 1 Statistik Pengguna Internet Tahun 2019 sampai 2021

Berdasarkan data pada gambar di atas yang dilansir dari *website* resmi internet *world stats* menunjukkan bahwa pengguna internet dari top 20 negara sebanyak 3,2 miliar orang dan Indonesia menduduki nomor 4 pengguna internet terbanyak[1]. Dapat dipastikan pengguna internet semakin meningkat pada setiap

tahun, semakin banyak pengguna internet maka akan rentan terjadinya serangan *hacker*.

Website merupakan salah satu layanan informasi yang banyak diakses oleh pengguna di dalam dunia teknologi informasi yang terhubung ke internet. Dalam lingkup *website* juga masih terdapat banyak *vulnerability* keamanan yang bisa dimasuki oleh pihak yang tidak bertanggung jawab atau *hacker*[2]. Banyaknya masalah peretasan *website* baik yang terekspos ataupun tidak terekspos. Dalam dunia teknologi informasi keamanan merupakan kebutuhan yang penting dalam menjaga dan menjamin kerahasiaan, integritas, dan ketersediaan data atau informasi[3].

Melihat gambar 1.1 diatas banyaknya pengguna internet di dunia maka akan rentan terjadinya kejahatan siber. Dilihat dari serangan siber melalui *website* resmi Badan Siber dan Sandi Negara (BSSN) melalui *honeynet project* membuktikan banyaknya serangan yang terjadi di Indonesia. Bentuk serangan yang dilakuakn *hacker* yang terjadi saat ini diantaranya serangan *Malware*, peretasan *website*, *Denial of Service* (Dos), serangan *Cross Site Scripting* (XSS), serangan *Phising* dan serangan *Defacement*. Dapat dilihat pada gabar 1.2 di bawah jumlah serangan siber yang terjadi di Indonesia.



Gambar 1. 2 Peta sebaran serangan yang ada di Indonesia pada tahun 2022

Adapun laporan serangan siber pada bulan Desember 2020 sebanyak 72 juta, dengan berbagai macam serangan siber berdasarkan klasifikasi anomaly

diantaranya *Malware, Denial of Service, Web Application Attack, Information Getring* dan lain sebagainya. Dari laporan bulanan BSSN terdapat 531 kasus peretasan *website* di Indonesia dengan sebaran kasus diantaranya sekolah, daerah, pusat, swasta, Organisasi, keuangan, kesehatan, militer, dan personal. Dari sebaran kasus yang ada sector akademik memiliki kasus sebanyak 214 kasus, sector swasta 136 kasus dan sector daerah sebanyak 104 kasus[4].

Gambar 1. 3 Data peretasa *website* dari laporan bulan Desember BSSN

Madeline Carr menjelaskan dalam jurnalnya yang berjudul *Crossed Wires: International Cooperation on Cyber Security* bahwa keamanan siber merupakan permasalahan *post-state*. Artinya adalah keamanan siber merupakan bentuk ancaman yang tidak bisa ditangani menggunakan paradigma Westphalia yaitu mengatasi ancaman melalui instrumen negara seperti militer. Carr menegaskan bahwa ancaman yang datang dari dunia maya bersifat *borderless* dan tidak terlihat namun dampaknya sangat terasa[5].

Peneliti menggunakan enam *website* pemerintah daerah yaitu DK, BR, PBG, CMS, RBG, dan BJR yang digunakan untuk sempel penelitian pengujian PTES dimana *website-website* tersebut sudah menggunakan *Hypertext Transfers Protocol Secure* (HTTPS). Peneliti memilih ke-6 *website* pemerintah daerah secara acak dan

tidak ada alasan khusus dalam pemilihan *website*. Dasar dilakukannya pengujian pada *website* tersebut masih banyaknya *website* pemerintah yang tingkat keamanannya rendah dan rentan untuk diserang oleh pihak yang tidak bertanggung jawab.

Dari permasalahan tersebut akan dilakukan penelitian tentang pengujian keamanan website pemerintah dengan judul **ANALISIS KEAMANAN PADA WEBSITE PEMERINTAH DAERAH XYZ MENGGUNAKAN METODE *PENETRATION TESTING EXECUTION STANDARD* (PTES)**, untuk melihat celah keamanan dan tingkat kerentanan pada *website* pemerintah daerah.

Terdapat penelitian sebelumnya yang mengulas pengujian keamanan *website* pada sektor pendidikkan yang meng hasil pengujian ditemukannya celah keamanan pada *Web Server Transmits Cleartext Credentials, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF)*. Oleh karena itu, dalam penelitian ini akan dibuat pengujian keamanan *website* menggunakan sempel *website* pemerintah daerah.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, permasalahan yang terjadi pada *website* pemerintah daerah adalah tingkat keamanan yang cukup rendah, dari beberapa kasus yang terjadi di Indonesia beberapa website pemerintah daerah seperti BR, DK, PBG, CMS, BJR, dan RBG adalah beberapa website yang tingkat keamanannya harus diuji, dari hal tersebut maka peneliti akan melakukan pengujian kerentanan *website* tersebut dari segi data yang kredensial.

1.3 Pertanyaan Penelitian

Adapun pertanyaan penelitian sebagai berikut:

1. Bagaimana tingkat keamanan pada beberapa *website* pemerintah daerah DK, BR, CMS, BJR, RBG, dan PBG?
2. Bagaimana hasil pengujian dan analisis keamanan pada *website* pemerintah daerah DK, BR, CMS, BJR, RBG, dan PBG?
3. Penggunaan metode apa yang tepat untuk melakukan pengujian keamanan?

1.4 Batasan Masalah

Agar penelitian ini lebih terarah, terfokus, dan tidak meluas, penulis membatasi penelitian sesuai dengan rumusan masalah, dan diperoleh batasan – batasan masalah penelitian sebagai berikut:

1. Website yang digunakan untuk melakukan penelitian yaitu *website* DK, BR, PBG, RBG, CMS, dan BJR.
2. Hanya menggunakan metode *penetration testing execution standard* (PTES).
3. Peneliti melakukan seluruh rangkaian tahapan PTES, tetapi tahapan post exploitation tidak di publikasikan.

1.5 Tujuan Penelitian

Berdasarkan pertanyaan penelitian diatas, tujuan dari penelitian ini adalah:

1. Untuk mengetahui celah kerentanan yang ada pada *website* pemerintah daerah DK, BR, CMS, BJR, RBG, dan PBG dengan cara menyerang website tersebut dan memberikan rekomendasi keamanan pada website tersebut.
2. Untuk mengetahui hasil dari pengujian penyerangan dan keamanan pada *website* pemerintah daerah DK, BR, CMS, BJR, RBG, dan PBG.

1.6 Manfaat Penelitian

Penelitian ini diharapkan dapat menjadi rekomendasi tingkat keamanan yang ada pada *website* pemerintah daerah. Penyusupan oleh pihak yang tidak bertanggung jawab yang membuat tampilan *website* berubah ataupun kebocoran data yang ada dalam *website* pemerintah daerah.