BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada tahun 2021 terdapat sebuah artikel di medium.com yang berisi artikel dari seorang bug hunter yang menemukan kerentanan pada Shopify dengan hadiah uang yang cukup besar. Setelah membaca artikel tersebut terdapat keinginan untuk mendalami profesi freelance sebagai bug hunter karena melihat hadiah yang berikan kepada seorang bug hunter cukup besar. Karena sebelumnya mempunyai basic dalam hal Penetration Test (Pentest) yang sudah dipelajari pada saat masih Sekolah Menengah Kejuruan (SMK) jadi tidak perlu membutuhkan waktu yang lama untuk langsung mencoba sebagai bug hunter. Setelah membaca beberapa artikel yang memberikan daftar platform untuk mencari bug atau kerentanan, tedapat salah satu platform yang menarik yang pada akhirnya mendaftar disalah satu platform yaitu Bugcrowd.

Di tahun 2022 publik di gemparkan dengan aksi seorang hacker yang berinisial Bjorka yang melakukan serangan cyber dan mempublikasikan data-data pribadi milik warga Indonesia dari beberapa website atau aplikasi milik pemerintah yang kemudian di perjual belikan dalam sebuah forum hacker. Hal ini menjadi masalah yang serius karena data yang di perjual belikan adalah data yang sangat sensitif seperti NIK, alamat, nomer telepon, dan lain-lain yang sifatnya sangat pribadi. Keamanan data menjadi hal yang sangat serius untuk dilindungi karena jika tidak maka hal terburuk yang akan terjadi yaitu data pribadi milik seseorang akan digunakan untuk tindakan kriminal oleh seseorang atau kelompok yang tidak bertanggung jawab.

Dengan aksi yang dilancarkan oleh Bjorka, keinginan dan motivasi untuk menjadi seorang white hat hacker atau bug hunter semakin besar karena peran tersebut sangat penting untuk saat ini dimana data semua pengguna disimpan secara digital. Peran white hat hacker atau bug hunter bisa membantu sebuah perusahaan atau organisasi dengan cara melaporkan kerentanan yang ditemukan

agar terhindar dari seorang black hat hacker yang mencoba untuk menghancurkan reputasi perusahaan atau organisasi, membocorkan data yang bersifat pribadi, dan mengambil alih akun secara diam-diam. Bug hunter berfokus pada mencari kerentanan atau bug tanpa merusak atau mengambil data penting pada sebuah website atau aplikasi milik perusahaan atau organisasi. Jika bug hunter sudah melanggar peraturan seperti membocorkan data, menghancurkan server, menjual belikan data, dan kejahatan cyber lainnya maka seseorang atau kelompok tersebut bukanlah bug hunter melainkan seorang black hat hacker. Sebelum melakukan aksi Penetration Test (Pentest) lihat terlebih dulu apakah targetnya memperbolehkan untuk seorang hacker atau bug hunter mencari bug atau kerentanan, jika tidak dan tetap memaksa untuk melakukan aksi Penetration Test (Pentest) maka kegiatan tersebut sudah termasuk tindakan yang ilegal. Maka dari itu bug hunter harus tetap melakukan tindakan yang legal atau sah dan memiliki tujuan untuk membantu sebuah perusahaan atau organisasi dalam mengamankan ataupun menemukan bug atau kerentanan pada website atau aplikasi milik mereka agar reputasinya tetap terjaga.

1.2 Profil Pekerjaan

Bug bounty program adalah suatu program pencarian bug / celah keamanan pada suatu website / aplikasi yang diselenggarakan oleh suatu perusahaan, dimana "hacker" atau "bug hunter" yang berhasil menemukan dan melalui proses validasi akan diberikan sebuah reward baik berupa sertifikat, hall of fame, hingga berupa uang. Bug bounty program menjadi andalan dalam strategi keamanan organisasi [1]. Ada sebuah platform yang menyediakan daftar bug bounty program yaitu Bugcrowd [2]. Bugcrowd adalah platform keamanan dimana banyak sekali organisasi atau perusahaan yang terdaftar pada platform tersebut untuk memperbolehkan seorang white hat hacker atau bug hunter meretas website atau aplikasinya dengan syarat tidak melanggar peraturan yang dibuat oleh platform ataupun organisasi atau perusahaan. Program Bug Bounty Bugcrowd memberi penghargaan kepada peretas untuk pengiriman bug yang diterima secara valid dengan hadiah uang. Bugcrowd memiliki banyak sekali

perusahaan atau kelompok yang memperbolehkan seorang bug hunter atau white hat hacker meretas website atau aplikasi milik perusahaan atau kelompok tersebut. Di dalam Bugcrowd terdapat 2 tipe program yaitu publik dan private. Publik program dapat diakses oleh semua pengguna baik yang baru mendaftar, pengguna lama ataupun visitor yang hanya melihat-lihat atau mengunjungi website Bugcrowd. Sedangkan private program dapat diakses jika pengguna telah banyak menemukan bug atau kerentanan, jika sudah mendapatkan beberapa bug atau kerentanan maka Bugcrowd akan mengirimkan email berupa undangan untuk dapat mengakses ke private program. Pada platform Bugcrowd terdapat staff yang akan menilai dan melihat laporan yang dikirimkan, jika staff sudah memvalidasi laporan maka staff akan meneruskan laporan ke perusahaan atau organisasi. Jika organisasi atau perusahaan menanggapi laporan kerentanan yang ditemukan berbahaya ataupun berdampak pada pengguna dan reputasi perusahaan maka perusahaan atau kelompok tersebut akan memberikan hadiah berupa uang ataupun poin.

1.3 Project Yang Dikerjakan

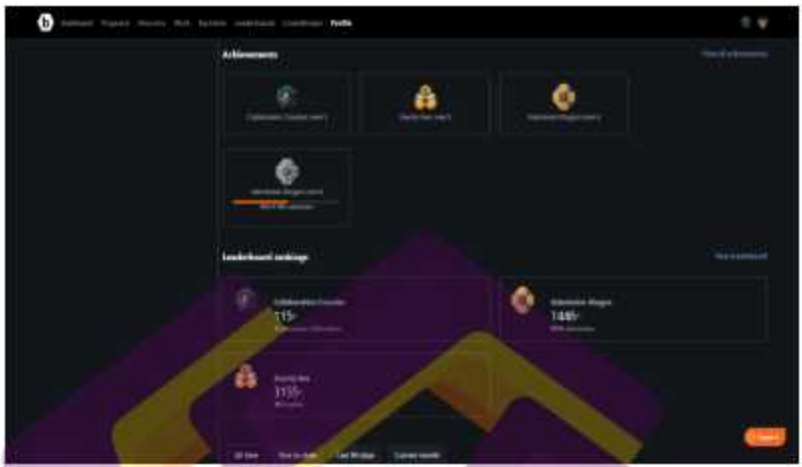
Project yang dikerjakan adalah mencari kerentanan atau bug yang terdapat pada aplikasi atau website milik perusahaan atau organisasi. Website yang pertama kali diretas yaitu website Cloudinary. Beberapa laporan ditolak oleh Cloudinary karena dampak dari kerentanan tidak berbahaya bagi pengguna ataupun reputasi dari perusahaan. Dan beberapa laporan dianggap duplikat karena sudah ada bug hunter lain yang melaporkan kerentanan yang sama. Setelah dari website Clodinary target selanjutnya yaitu website Indeed, hanya 2 kerentanan yang ditemukan dan 2 kerentanan tersebut dianggap sebagai duplikat. Sekian lama tidak menemukan bug pada website Indeed, pada akhirnya berpindah target ke website Atlassian. Atlassian memiliki beberapa produk seperti Confluence, Jira, Bitbucket, Trello, dan lain-lain yang membuat jangkauan target nya menjadi sangat luas. Karena jangkauan target yang luas akhirnya memutuskan untuk memfokuskan target pada Atlassian. Pada website Atlassian banyak sekali kerentanan yang ditemukan, dengan total 30 kerentanan yang diterima, 20

kerentanan yang dianggap duplikat dan 41 kerentanan yang dianggap tidak berbahaya bagi pengguna ataupun reputasi perusahaan. Dan muncul Dropbox pada platform Bugcrowd, hanya 1 kerentanan yang ditemukan pada Dropbox karena akun yang diberikan trial hanya 14 hari yang membuat akses ke beberapa fitur menjadi terbatas.

1.4 Performa

Performa dari jasa penyedia freelance platform Bugcrowd dapat dilihat pada gambar dibawah ini :

Gambar 1.1 Performa Akun Bugcrowd



Gambar 1.2 Performa Akun Bugcrowd

Gambar 1.3 Performa Akun Bugcrowd

Gambar 1.4 Performa Akun Bugcrowd