

**ANALISIS KERENTANAN *INSECURE DESIGN* DAN *SERVER SIDE REQUEST FORGERY (SSRF)* DENGAN METODE PTES (STUDI KASUS OBJEK BUGGY WEB APPLICATION)**

**Muhammad Ridwan Fazli**

**1710511060**

**ABSTRAK**

Saat ini perkembangan teknologi semakin maju dan canggih, mulai dari sistem penyimpanan yang tidak lagi membutuhkan sebuah perangkat keras seperti *harddisk*, *flashdisk*, dll. Sehingga semua data penting yang kita miliki dapat disimpan secara *online*. Namun perkembangan teknologi juga memiliki dampak negatif seperti data yang dicuri pada situs yang kita gunakan untuk menyimpan data oleh peretas atau *hacker* yang tidak bertanggung jawab. Namun setiap data yang dicuri tidak selalu data yang penting, hal ini dikarenakan peretas tidak pandang bulu dalam melakukan peretasan. Alasan peretas yang mencuri segala jenis data karena selama data tersebut memiliki sebuah nilai dan dapat menghasilkan, maka peretas akan mencoba untuk mencuri data tersebut demi keuntungannya sendiri atau orang lain yang membutuhkan data tersebut.

Dengan adanya tindak kejahatan online atau biasa disebut dengan *cybercrime* ini maka diperlukan sebuah sistem keamanan yang dapat mencegah terjadinya tindak kejahatan tersebut. Salah satu tindakan yang dapat diambil dalam melakukan pencegahan *cybercrime* pada suatu situs dengan melakukan *Vulnerability Scanning* yang bertujuan untuk mengetahui celah keamanan pada suatu situs yang rentan untuk diserang oleh peretas. Selain itu juga dilakukan *Penetration Testing* yaitu proses simulasi penyerangan yang dilakukan terhadap

suatu sistem untuk memastikan apakah benar-benar ada kerentanan pada suatu sistem dan dapat merusak sistem tersebut.

Pada penelitian dilakukan analisis terhadap dampak yang ditimbulkan jika suatu situs terinfeksi oleh serangan yang memanfaatkan kerentanan atau *vulnerability* berupa *Insecure Design*, dan *Server Side Request Forgery* (SSRF). Adapun dua jenis kerentanan yang akan dianalisis dipilih berdasarkan jenis kerentanan atau risiko yang baru ditambahkan pada OWASP Top Ten 2021. Dalam melakukan pengujian ini digunakan metode *Penetration Testing Execution Standard* (PTES). Metode ini memiliki 5 (lima) tahapan yaitu *Intelligence Gathering*, *Vulnerability Analysis*, *Exploitation*, *Post-Exploitation*, dan *Report*. Hasil yang akan didapatkan berupa dampak yang akan terjadi pada suatu sistem terhadap suatu serangan dan solusi yang dapat diberikan berdasarkan OWASP Top Ten 2021.

**Kata kunci :** *cybercrime*, bWAPP, OWASP Top Ten, PTES

**ANALISIS KERENTANAN *INSECURE DESIGN* DAN *SERVER SIDE REQUEST FORGERY* (SSRF) DENGAN METODE PTES (STUDI KASUS OBJEK BUGGY WEB APPLICATION)**

**Muhammad Ridwan Fazli**

**1710511060**

**ABSTRACT**

At present the development of technology is increasingly advanced and sophisticated, starting from a storage system that no longer requires a hardware such as hard disk, flash disk, etc. So that all important data that we have can be stored online. But the development of technology also has a negative impact such as the data stolen on the site that we use to store data by hackers or hackers that are not responsible. But every stolen data is not always important data, this is because hackers do not look indiscriminate in hacking. The reason for hackers that steals all types of data is because as long as the data has a value and can produce, the hackers will try to steal the data for their own benefits or other people who need the data.

With the existence of online crime or commonly called cybercrime, a security system is needed that can prevent the crime. One of the actions that can be taken in preventing cybercrime on a site by conducting a vulnerability scanning that aims to find out security gaps on a vulnerable site to be attacked by hackers. In addition, a penetration testing is also carried out, a simulation process of attack carried out on a system to ascertain whether there is a vulnerability to a system and can damage the system.

In the study an analysis of the impact caused if a site is infected by attacks that utilize vulnerability or vulnerability in the form of insecure design, and server side request forgery (SSRF). The two types of vulnerability to be analyzed are

selected based on the new type of vulnerability or risk added to the Owasp Top Ten 2021. In this testing the Penetration Testing Execution Standard (PTES) method is used. This method has 5 (five) stages, namely intelligence gathering, vulnerability analysis, exploitation, post-exploitation, and report. The results that will be obtained in the form of an impact that will occur on a system on an attack and solution that can be given based on Owasp Top Ten 2021.

**Kata kunci :** *cybercrime*, bWAPP, OWASP Top Ten, PTES