INTISARI

Berdasarkan informasi dari salah satu mahasiswa Universitas XYZ Purwokerto yang berinisial ZH, website Universitas XYZ Purwokerto.ac.id pernah diserang menggunakan teknik serangan DDOS dan defacing dengan tidak semestinya oleh pihak yang tidak bertanggung jawab, sehingga mengakibatkan website tersebut lumpuh dalam waktu beberapa hari. Penelitian ini bertujuan untuk menganalisis kerentanan yang terkait dengan keberadaan backdoor PHP dalam website Universitas XYZ Purwokerto.ac.id. Kerentanan yang ditemukan terhadap serangan yaitu melalui backdoor PHP pada file input berkas. Metode observasi digunakan untuk memantau aktivitas dan interaksi pada website guna mendeteksi tanda-tanda penggunaan backdoor PHP yang tidak sah. Hasil dari penelitian ini adalah kemungkinan penyisipan file backdoor seperti 403.php dapat dilakukan melalui proses input berkas yang rentan pada platform tersebut. Keberadaan celah ini mengindikasikan potensi ancaman yang signifikan, di mana penyerang dapat memanfaatkannya untuk meretas sistem, mendapatkan akses tak sah, dan bahkan mengambil alih kontrol penuh atas sistem website.

Kata kunci: Webshell, Keamanan Cyber Security, Backdoor PHP

ABSTRACT

Based on information from one of the XYZ Purwokerto University students with the initials ZH, the XYZ University Purwokerto.ac.id website was attacked using DDOS attack techniques and improper defacing by irresponsible parties, resulting in the website being paralyzed within several days. This research aims to analyze vulnerabilities related to the existence of a PHP backdoor on the XYZ University Purwokerto.ac.id website. The vulnerability found against the attack was through a PHP backdoor in the input file. The observation method is used to monitor activities and interactions on the website to detect signs of unauthorized use of the PHP backdoor. The result of this research is that it is possible to insert backdoor files such as 403.php through a vulnerable file input process on the platform. The existence of this vulnerability indicates a significant potential threat, where attackers can exploit it to hack the system, gain unauthorized access, and even take full control of the website system.

Keywords: Webshell, Cyber Security, PHP Backdoor