ANALISA DAN PERBAIKAN KEAMANAN PADA WEBSITE SDN 9 BANTAN

Nama : Muhammad Zuhri Febriansyah

Nim 6404211030

Dosen Pembimbing : Agus Tedyyana, M.Kom

ABSTRAK

Keamanan website saat ini menjadi salah satu fokus utama, karena website berisi informasi dan data yang sensitif dan berharga. Penelitian ini bertujuan untuk mengetahui tingkat keamanan website dan memberikan perbaikan pada celah-celah keamanan pada website SDN 9 Bantan dengan menggunakan metode *Vulnerability Assesment* dan menggunakan *tools OWASP ZAP* dan *Mozilla Observatory*. Dari hasil pemindaian, ditemukan beberapa celah pada website SDN 9 Bantan seperti *Content Security Policy* (CSP) *Header Not Set* yang memungkinkan serangan XSS bisa terjadi, *Missing Anti-clickjacking Header* ketiadaan *anti-clickjacking header* membuka celah *clickjacking*, tidak adanya *Content Security Policy* (CSP) meningkatkan risiko serangan XSS, redirection yang tidak aman dapat dimanfaatkan untuk phishing, tidak adanya *Strict Transport Security* (HSTS) membuat situs rentan terhadap serangan *Man-in-the-Middle* (MitM), dan *tanpa X-Frame-Options* meningkatkan risiko serangan clickjacking.. Untuk mengatasi celah keamanan ini, dilakukan *Vulnerability Assessment* untuk menentukan tingkat risiko dari celah keamanan website SDN 9 Bantan yang berada pada tingkat *medium*. Setelah proses perbaikan beberapa celah keamanan berhasil dihilangkan pada *Mozilla Observatory*. Namun celah *Content Security Policy (CSP) Header Not Set* masih terdeteksi pada *OWASP ZAP*.

Kata Kunci: Analisa, *Website*, Perbaikan, Keamanan, *Vulnerability Assesment*

ANALISA DAN PERBAIKAN KEAMANAN PADA WEBSITE SDN 9 BANTAN

Nama : Muhammad Zuhri Febriansyah

Nim 6404211030

Dosen Pembimbing : Agus Tedyyana, M.Kom

ABSTRACT

Website security is currently one of the main focuses, because websites contain sensitive and valuable information and data. This research aims to determine the level of website security and provide improvements to security gaps on the SDN 9 Bantan website using the Vulnerability Assessment method and using the OWASP ZAP and Mozilla Observatory tools. From the scan results, several gaps were found on the SDN 9 Bantan website such as Content Security Policy (CSP) Header Not Set which allows XSS attacks to occur, Missing Anti-clickjacking Header, absence of anti-clickjacking header opens clickjacking gaps, absence of Content Security Policy (CSP) increases the risk of XSS attacks, insecure redirection can be exploited for phishing, absence of Strict Transport Security (HSTS) makes the site vulnerable to Man-in-the-Middle (MitM) attacks, and without X-Frame-Options increases the risk of clickjacking attacks. To overcome this security gap, a Vulnerability Assessment was carried out to determine the risk level of the SDN 9 Bantan website security gap which is at the medium level. After the repair process, several security gaps were successfully removed in the Mozilla Observatory. However, gaps such as Content Security Policy (CSP) Header Not Set is still detected in OWASP ZAP.

Keywords: Analysis, Website, Repair, Security, Vulnerability Assessment