# *ABSTRACT*

# *SECURITY ANALYSIS ON THE XYZ LOCAL GOVERNMENT WEBSITE USING THE PENETRATION TESTING EXECUTION STANDARD* (PTES) *METHOD*

Oleh

Ditya Putri Anggraeni

18102047

*The rapid development of Information Technology (IT) has had a positive impact on various fields, one of which is website technology. Following the development of the internet at present, it is increasingly increasing its users. So that will be very vulnerable to hacker attacks. Attacks that are often carried out by hackers include Malware attacks, website hacking, Denial of Service (DoS), Cross Site Scripting (XSS), Phishing, and Defacement, these attacks are carried out with a specific purpose. In this study, researchers used the Penetration Testing Execution Standard (PTES) method to analyze and perform vulnerability testing on the DK, BR, PBG, CMS, RBG, and BJR local government websites. After testing the Cross Site Scripting (XSS) attack with the results that five out of six local government websites were successfully marked with status code 200, which means the payload was successful, one local government website failed, namely the CMS district government due to a firewall on the website from the platform used. namely wordpress. Furthermore, the attack in the form of a dorking vulnerability was tested on six local government websites, two out of the six successful websites, where family card data were found on the DK local government website and URLs containing directories and government data on the CMS local government website. The DK local government website uses the Bootstrap platform and the CMS local government website uses the WordPress platform.*

***Keywords: cyber security, Pentest, XSS, Website, Dorking***