XIPS : a model-based prevention mechanism for preventing blind XPath injection in database-centric web services environment.

ABSTRACT

Web services have become a powerful interface for backend database systems which provides many services such as automatic purchasing, inventory tracking and clinical management. However, along the benefit of Web services, comes a serious risk of security breaches. Most Web services are deployed with security flaws and these vulnerabilities expose them to XPath (XML Path Language) injection. This kind of attack can cause serious damage to the database at the back end of Web services. This paper proposes XIPS, a prevention mechanism against Blind XPath injection attacks within Web services environment. The prevention mechanism employs the model-based approach to detect malicious queries and thwart them before they are executed on the Web services back end database. This approach uses run time monitoring to check on the dynamically-generated queries and compares them against the statistically-built model. The employment of the XIPS architecture should be able to prevent Web services from any kinds of XPath injection attacks.

Keyword: Web services; Database security; Blind XPath injection; Model-based; Hotspot.