CRYPTOGRAPHY AND INFORMATION SECURITY Ew-401

MATSUURA LAB.

[Static analysis of XSS attacks vulnerabilities in Web applications implemented with object oriented programming]

Department of Informatics and Electronics

http://kmlab.iis.u-tokyo.ac.jp

Information Security

Information and communication engineering department

Cross Site Scripting (XSS) attack

Cross Site Scripting (XSS) attack is the attack which attackers inject malicious scripting against web applications by taking advantage of inappropriate input process in server side.

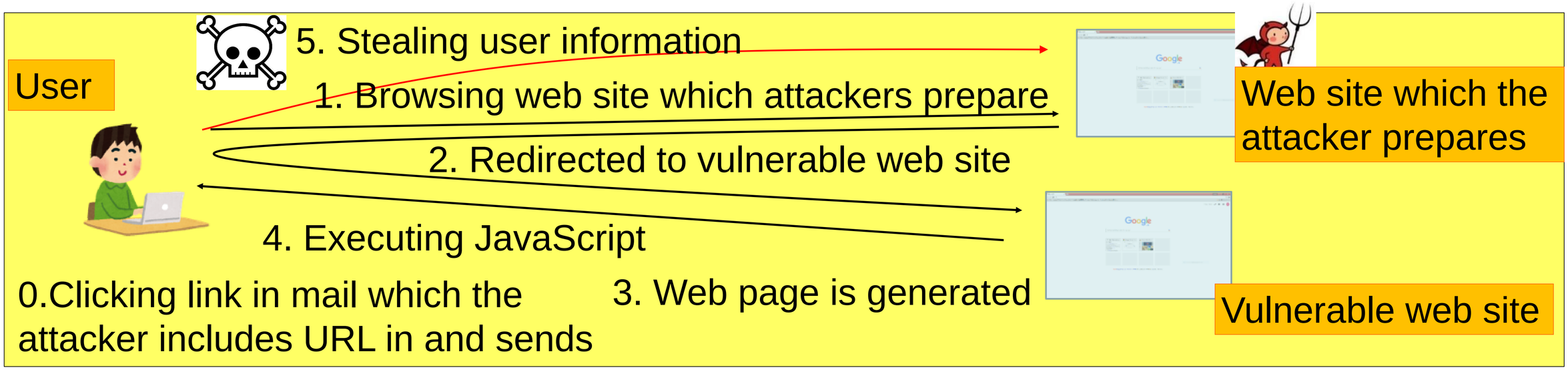


Figure 1 : Reflected XSS attack.

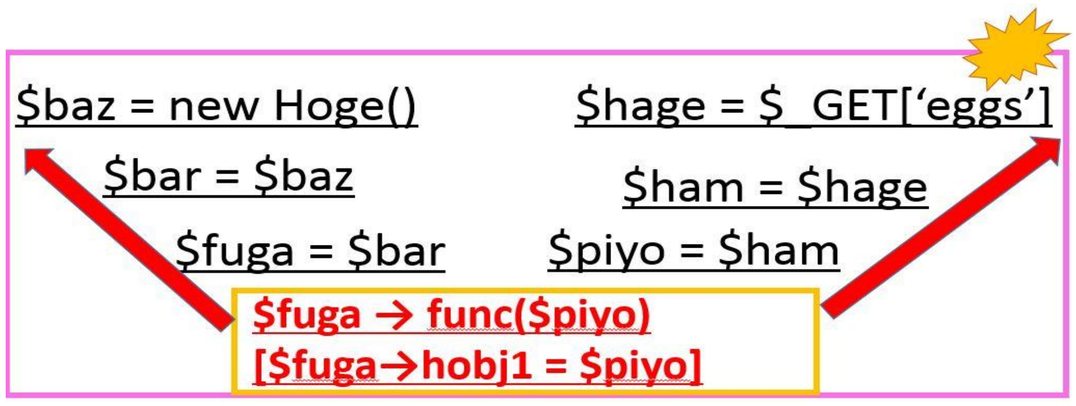
Application implemented with object oriented script language

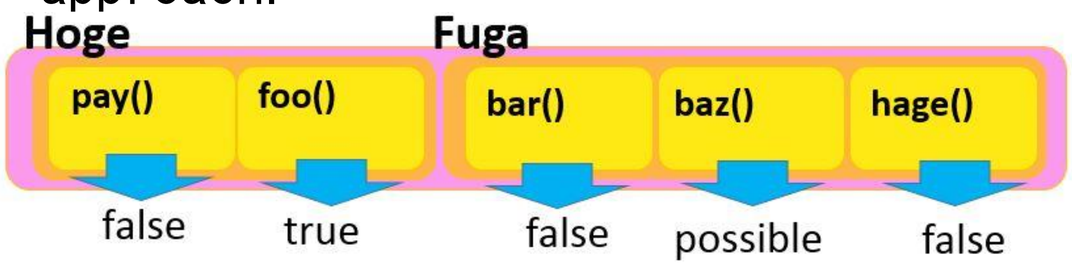
◇In field of static analysis of object oriented analysis, there are researches which analyze based on type information in typed programming language such as Java, C++. However, script language which does not have type information cannot be applied to this approach.

How to detect

◆This research targets at Reflected XSS and Stored XSS vulnerability detection in script language implemented with Object Oriented Programming.

◆Our approach introduces Class cache and 2-way backward directed analysis as an approach.





◆We confirms improving detection rate of XSS attacks by keeping vulnerabilities information in class cache in advance and execute 2 way backward-directed analysis.