# Abstract

The input handling, account recovery and privacy of user's information play an important role in today's web applications. The improper treatment of any of these features may result in exfiltration of sensitive information. The goal of this dissertation is threefold.

First, we review how top mobile and desktop web applications are handling user supplied contents which may be malicious and cause Cross-Site Scripting (XSS) problem. In addition, we include top PHP frameworks, PHP's built-in functions, popular PHP-based customized solutions and rich-text editors powering thousands of web applications in our investigation of input handling routines. Our analysis reveals that almost all solutions can be bypassed and we also found that 50% of Alexa top sites (10*10) are vulnerable.

We subsequently design three solutions for an XSS protection. It includes one regular expression based filtering solution which utilizes black-list approach. The solution is part of OWASP ModSecurity (web application firewall engine having around 1,000,000 deployments) Core Rule Set (CRS). The second solution is based on an output encoding of potentially dangerous characters. It supports five common output contexts found in web application and based on minimalistic encoding. It has been adopted by a popular in-browser web development editor having more than 50,000 downloads along with one popular Content Management System (CMS). Further, we also present a fine-grained policy language for the mitigation of an XSS vulnerability. The policy language pushes the boundries of Mozilla's Content Security Policy (CSP). CSP is a page-wise policy while the policy language presented in this work gives an individual element-wise control.

Secondly, we delve into the account recovery feature of web applications. In particular, we review forgot your password implementation of 50 popular social networks. We found Trusted Friend Attack (TFA) and Chain Trusted Friend Attack (CTFA) on the account recovery feature of Facebook. The forgot your password feature of Facebook supports social authentication. The attacker can compromise real Facebook accounts with the help of TFA and CTFA. In addition, we also found weaknesses in account recovery feature deployed in other popular social networking sites including Twitter. More specifically, we were able to compromise accounts on 7 social networks.

Finally, given the widespread use of web applications, it is a challenge to provide the user better control over their sensitive information. We address this challenge by providing a Mozilla Firefox addon and we call it TTPCookie. TTPCookie provides the user a fine-grained control over the cookies. TTPCookie is neither user-centric nor advertiser-centric solution because it enables behavioral targeting with low privacy risks.