1. Record Nr.	UNINA9910873162803321
Titolo	2011 11th IEEE International Working Conference on Source Code Analysis and Manipulation
Pubbl/distr/stampa	[Place of publication not identified], : IEEE, 2011
Descrizione fisica	1 online resource
Disciplina	005.1
Soggetti	Source code (Computer science)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Sommario/riassunto	More and more web applications suffer the presence of cross-site scripting vulnerabilities that could be exploited by attackers to access sensitive information (such as credentials or credit card numbers). Hence proper tests are required to assess the security of web applications. In this paper, we resort to a search based approach for security testing web applications. We take advantage of static analysis to detect candidate cross-site scripting vulnerabilities. Input values that expose these vulnerabilities are searched by a genetic algorithm and, to help the genetic algorithm escape local optima, symbolic constraints are collected at run-time and passed to a solver. Search results represent test cases to be used by software developers to understand and fix security problems. We implemented this approach in a prototype and evaluated it on real world PHP code.