ปัจจุบันหนึ่งในวิธีการโจมตีเว็บแอพพลิเคชั่นซึ่งเป็นที่นิยมก็คือครอสไซต์สคริปติ้งเนื่องจากการโจมตีดังกล่าวทำได้ง่ายในขณะที่การป้องกันนั้นขึ้นอยู่กับเทคโนโลยีทางฝั่งไคล์เอนต์ทำให้การโจมตีนี้ยากต่อการป้องกัน อีกทั้งเครื่องมือช่วยตรวจสอบโดยทั่วไปส่วนใหญ่จะใช้สตริงโจมตีจริงในการตรวจสอบและไม่ค่อยให้ข้อมูลนอกจากแจ้งว่าการโจมตีเกิดขึ้นได้หรือไม่และความครอบคลุมยังขึ้นอยู่กับปริมาณการโจมตีที่ใช้ จากปัญหาต่างๆเกี่ยวกับครอสไซต์สคริปติ้งจึงได้มีผู้เสนองานวิจัยในการช่วยเหลือเกี่ยวกับปัญหาครอสไซต์สคริปติ้งขึ้นมากมายงานวิจัยนี้จึงรวบรวมเทคนิคที่ได้มีการเสนอซึ่งสามารถนำมาช่วยเหลือบรรเทาปัญหาเกี่ยวกับการโจมตีครอสไซต์สคริปติ้งโดยได้วิเคราะห์จัดแบ่งเป็นประเภทแยกไว้เพื่อศึกษาแนวทางในการรับมือที่กำลังเป็นที่สนใจของนักวิจัยได้ชัดเจนและช่วยให้สามารถมองเห็นสิ่งที่ยังขาดหายไปในการช่วยเหลือเกี่ยวกับครอสไซต์สคริปติ้ง นอกจากนี้ยังได้ทำการพัฒนาเครื่องมือที่ช่วยบรรเทาปัญหาครอสไซต์สคริปติ้งขึ้นโดยเสนอแนวทางให้ข้อมูลในการทรัสต์แก่ผู้ใช้ในเบื้องต้นและได้เสนอเทคนิคในการตรวจสอบความปลอดภัยโดยตรวจสอบจากสิ่งที่ข้อมูลควรจะถูกกรองโดยอาศัยความรู้จากแหล่งความปลอดภัยต่างๆในการพิจารณาอีลีเมนต์ที่เสี่ยง แอททริบิวต์ที่เสี่ยงและคำสำคัญที่ใช้ในการตรวจสอบ ผลจากการทดสอบวิธีการดังกล่าวกับแนวทางป้องกันแบบต่างๆพบว่าเทคนิคในการตรวจสอบที่พัฒนาขึ้นสามารถแจ้งเตือนถึงรูปแบบของอันตรายที่สามารถเกิดขึ้นได้มากกว่าการใช้สตริงโจมตีจริงเมื่อการป้องกันมีจุดอ่อนมากแต่เมื่อการป้องกันมีความแข็งแรงมากวิธีแบบใช้สตริงโจมตีจริงจะสามารถแจ้งเตือนถึงอันตรายได้มากกว่า อย่างไรก็ตามแม้วิธีหนึ่งจะไม่มีการแจ้งเตือนแต่อีกวิธีจะมีการแจ้งเตือนออกมาจึงทำให้ต้องใช้ทั้งสองวิธีร่วมกันในการตรวจสอบ นอกจากนี้เครื่องมือที่ใช้เทคนิคการตรวจสอบที่ได้เสนอนั้นนอกจากจะแสดงจำนวนสตริงทดสอบที่เกิดขึ้นแล้วยังแสดงอีลีเมนต์ที่เสี่ยง แอททริบิวต์ที่เสี่ยงและคำสำคัญที่ไม่ได้ป้องกันออกมาให้ทราบด้วย

Nowadays, one of the most popular attacks on web applications is XSS (cross-site scripting). Since performing an attack is easy (difficult to detect) and depending highly on the client-side technology, protection from such attack is difficult. While most tools usually test with real payloads using real strings from (known) malicious attacks and only report the payload that is harmful to the system, the number of payloads alone cannot determine whether the tests are enough. To reduce the problem, there are many works (research) proposed to counter XSS. In this work, for cleary study and can see what is lack, we review those works and classify them into groups. Furthermore, we propose a preliminary method to give user an information to decide if a site is trustworthy. We propose a new testing concept based on the examination of data that should be filtered out. Our scheme is based on knowledge from several security web sites; risk elements, possible attributes and significant words. We validate our method with other schemes. Result shows that our scheme can inform the risk better than real string attack's schemes in a weak protection system, but in the strong protection, real string attack's schemes perform better. When one scheme does not inform any risk, the other one will do. We propose that both schemes must be used. In addition, the tool that uses our proposed scheme not only reports the payload but it also reports risk elements, possible attributes and significant words that have not be filtered out too.