

ارائه یک مدل جهت ارزیابی امنیت در چرخه حیات نرم افزارهای تحت وب

علیرضا بابائی*، رضا ابراهیمی آتانی،

1394-06-29

امروزه پیشرفت تکنولوژی ارتباطات و سیستم های کامپیوتری بسرعت رو به رشد است. امنیت شبکه و برنامه های کاربردی به این ترتیب به چالش بزرگی تبدیل شده اند، پرواضح است که پیشرفت اطلاعات مشکلات خاص خود را ایجاد میکند. همچنین دستکاری اطلاعات بعنوان زیربنای فکری ملتها توسط گروههای سازماندهی شده بین المللی به نوعی مختل ساختن امنیت ملی و تهاجم علیه دولتها و تهدیدی ملی محسوب میشود. ایجاد کاربردهای نرم افزار امن بدون انجام بررسی های امنیتی امکان پذیر نیست، این امر لزوم پرداختن به ارزیابی امنیتی را بیش از پیش نمایانگر می کند. با توجه به روشها و مدل هایی که برای ارزیابی امنیت برنامه های کاربردی تحت وب ارائه شده است، همچنان شاهد حملات و آسیب پذیری های جدی در برنامه های کاربردی تحت وب هستیم. بنابراین نیاز به رویکردی داریم تا ارزیابی امنیت برنامه های کاربردی تحت وب را بر اساس استاندارد و در طول چرخه حیات نرم افزار اجرا کند. به همین علت در این پایان نامه به ارائه رویکردی جهت ارزیابی امنیت برنامه های کاربردی تحت وب خواهیم پرداخت. در رویکرد ارزیابی امنیت پیشنهادی، سعی بر ارائه رویکردی برای در نظر گرفتن امنیت در همان آغاز تولید نرم افزار بوده است. در رویکرد پیشنهادی در طول چرخه حیات تولید برنامه های کاربردی تحت وب، اقدامات امنیتی برای بهبود امنیت این برنامه ها در نظر گرفته شده است. با ارزیابی امنیت در هر فاز از تولید نرم افزار، اطمینان از اینکه آسیب پذیری ها در هر فاز بدرستی شناسایی و کاهش یابند، حاصل می شود و سپس فاز بعدی آغاز می گردد. رویکرد پیشنهادی یک رویکرد مبتنی بر استاندارد IEC/ISO 12207 و استاندارد ASVS OWASP است. واژگان کلیدی: ارزیابی امنیت، استاندارد IEC/ISO 12207، استاندارد ASVS OWASP، برنامه های کاربردی تحت وب

کلمات کلیدی : ارزیابی امنیت، استاندارد IEC/ISO 12207، استاندارد ASVS OWASP، برنامه های کاربردی تحت وب