عنوان مقاله:
تشخیص ایستای آسیب پذیری های برنامه های کاربردی وب با استفاده از تحلیل جریان داده معکوس با هدف پوشش حداکثری نقاط حساس به آسیب پذیری

محل انتشار:
نهمین کنفرانس بین‌المللی انجمن رمز ایران (سال: 1391)

تعداد صفحات اصل مقاله: 6

نویسندگان:
محمود قربان زاده - *دانشکده مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی امیرکبیر، تهران*

حمیدرضا شهریاری - *دانشکده مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی امیرکبیر، تهران*

خلاصه مقاله:
با توجه به نقش برنامه های کاربردی وب در فناوری اطلاعات و نیز تبادل اطلاعات و ارایه سرویس های تحت وب، لزوم امن بودن این دسته از برنامه ها و نیز تبادل امن اطلاعات کاملا محسوس و حایز اهمیت می باشد. از این رو سعی بر آن است تا با تشخیص آسیب پذیری های برنامه های تحت وب، مانع سوءاستفاده از این آسیب پذیری ها توسط نفوذگر شویم. شمار زیادی از روش های تشخیص آسیب پذیری با تحلیل بر روی متن برنامه و بصورت ایستا، پویا و یا ترکیبی از این دو در جهت کشف آسیب ذیری های موجود در برنامه تحت وب تلاش می کنند. در این مقاله، روشی ایستا به منظور تشخیص آسیب پذیری ها در کد متن برنامه تحت وب ارایه می شود که برای تشخیص هر چه بیشتر نقاط آسیب پذیر، از تحلیل جریان داده بصورت معکوس استفاده می کند. این نوع تحلیل را تحلیل جریان داده معکوس نام نهاده ایم و برای این منظور از گراف کنترل جریان معکوس استفاده می شود. روش ارایه شده به زبان C++ پیاده سازی شده است و ابزار حاصل را کاشف نام نهاده ایم. این ابزار بر روی چند برنامه متن باز تحت وب اجرا شده و شماری از آسیب پذیری های این برنامه ها تشخیص داده شد که تعدادی از آنها جدید بودند.

کلمات کلیدی:
تشخیص آسیب پذیری برنامه های کاربردی وب، تحلیل جریان داده معکوس، گراف کنترل جریان