به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه


# بررسی روش‌های تشخیص حملات روی برنامه‌های کاربردی تحت وب توسط دیواره آتش برنامه‌ها

# *A Survey on Web Application Attack Detection Methods by Web Applications Firewall*

امیررضا علیزاده نیکو

زمان: شنبه ۲۰ آبان ماه ۱۳۹۶ ساعت ۸:۳۰

مکان: دانشکده مهندسی کامپیوتر دانشگاه صنعتی شریف، طبقه چهار، سالن خوارزمی

در حال حاضر بیش از ۷۰ درصد حملات اینترنتی از طریق بستر وب صورت می‌گیرد و برنامه‌های کاربردی تحت وب به عنوان بزرگترین هدف مهاجمین جهت نفوذ به زیرساخت‌های اطلاعاتی سازمان‌ها تبدیل شده‌اند. با توجه به رشد روزافزون حملات مبتنی بر وب و عدم کارایی سیستم‌های تشخیص و جلوگیری از نفوذ، ابزارهایی تحت عنوان «دیواره آتش برنامه‌های کاربردی تحت وب (WAF)» به منظور مقابله با حملات معمول وب نظیر XSS و تزریق SQL با نظارت بر روی پروتکل ارتباطی نظیر HTTP توسعه یافته‌اند. امروزه روش‌های زیادی در طراحی WAF به کار گرفته می‌شوند که به دو دسته مبتنی بر امضا و مبتنی بر ناهنجاری قابل دسته‌بندی هستند. در روش‌های مبتنی بر امضا قواعد مربوط به امضای حملات توسط افراد خبره استخراج و در سیستم، مورد استفاده قرار می‌گیرند. ولیکن در روش‌های مبتنی بر ناهنجاری ابتدا رفتار عادی برنامه با پایش رفتار برنامه در طول یک مدت زمان مشخص توسط سیستم یادگیری شده و سپس رفتارهای ناهنجار استخراج و به عنوان حمله شناسایی می‌گردند. در این سخنرانی، به بررسی دو روش ذکر شده پرداخته خواهد شد.

شرکت در این جلسه برای تمامی علاقه‌مندان آزاد است.