مجله علمی ـ پژوهشی «پدافند الکترونیکی و سایبری»
سال اول، شماره ۳، پاییز ۱۳۹۲، ص ۲۴- ۱۳

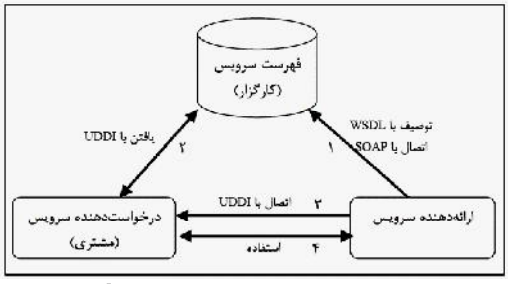
ارتقای امنیت سرویس‌های وب با استفاده از فنون تحمل‌پذیری خطا با تأکید بر فن تنوع طراحی

صادق بجانی[1*]، محمد عبداللهی ازگمی[2]
۱- دانشجوی دکتری مهندسی کامپیوتر، دانشگاه جامع امام حسین (ع)،
۲- استادیار دانشکده مهندسی کامپیوتر، دانشگاه علم و صنعت ایران
(دریافت۹۱/۱۰/۰۳، پذیرش: ۹۲/۰۲/۲۸)

چکیده
بی‌توجهی به امنیت سیستم‌های نرم‌افزاری مبتنی بر سرویس‌های وب، به‌علت چالش‌های امنیتی آنها، نتایج زیان‌بار و جبران‌ناپذیری به‌همراه دارد. تاکنون استانداردهای امنیتی بر اساس مکانیزم‌های سنتی امنیتی، نظیر رمزنگاری و امضاء دیجیتال، در رابطه با امنیت سرویس‌های وب و سیستم‌های مبتنی بر آنها مطرح شده است. همچنین فنون کلاسیک تحمل‌پذیری خطا و روش‌های متعارف امنیتی برای ارتقای امنیت سرویس‌های وب قابل بهره‌برداری است. علی‌رغم استفاده از استانداردهای امنیتی و فنون یادشده، تاکنون امنیت کامل سرویس‌های وب فراهم نشده و شاهد استمرار نفوذ در سرویس‌های وب هستیم. در مقاله حاضر برای ارتقای امنیت سرویس‌های وب، رویکردی مبتنی بر روش‌های متعارف امنیتی و تکنیک‌های کلاسیک تحمل‌پذیر خطا، با تأکید بر تکنیک‌های افزونگی و تنوع طراحی برای طراحی سرویس‌های وب پیشنهادشده است. عملکرد سیستم نرم‌افزاری مبتنی بر سرویس وب که با استفاده از تکنیک‌های تحمل‌پذیری خطا و سیستم نرم‌افزاری مبتنی بر وب و بدون استفاده از تکنیک‌های تحمل‌پذیری خطا طراحی شده، با بهره‌گیری از زنجیره‌های مارکوف مدل‌سازی شده و کارایی آنها با استفاده از نرم‌افزار Maple محاسبه شده است. نتایج ارزیابی نشان می‌دهد که میزان سرویس‌دهی سیستم‌های مبتنی بر وب که از تکنیک‌های تحمل‌پذیری نفوذ بهره می‌برند، به‌طور قابل توجهی افزایش می‌یابد.

واژه‌های کلیدی: نفوذ، تکنیک‌های تحمل‌پذیری خطا، تحمل‌پذیری نفوذ، تکنیک‌های افزونگی، تنوع طراحی.

۱. مقدمه
سرویس‌های وب راه حل اصلی تحقق معماری سرویس‌گرا محسوب شده و برسکوهای متفاوت توزیع‌شده در سطح اینترنت اجرا می‌شوند. رابط سرویس‌های وب براساس XML[1] تعریف می‌شود [۱]. سرویس‌های وب از طریق ارسال پیام‌های XML، با سیستم‌های نرم‌افزاری تبادل اطلاعات نموده و یک تعریف قابل پردازش ماشین، به‌نام WSDL[2] دارند [۲]. آنها به‌طور عمومی از سیستم‌های ناهمگن تشکیل شده‌اند و برای توسعه آنها، از معماری سرویس‌گرا استفاده می‌شود [۲]. شکل ۱، تعامل اجزای سرویس‌های وب را نشان می‌دهد.



شکل ۱: تعامل اجزای سرویس وب [۳]

در معماری مبتنی بر سرویس‌های وب بر پایه SOAP[3] که فراهم کننده قالب تعاملات آنهاست، پروتکل UDDI[4]، امکانات انتشار، جستجو و استفاده از این سرویس‌ها را فراهم می‌کند و از XML به‌عنوان شالوده توصیف، انتشار و ارتباط خود استفاده می‌نماید [۴]. با وجود اهمیت این سرویس‌ها در اثربخشی سیستم‌های توزیع شده در زمینه‌های کاربردی مختلف، چالش‌ها و مسائل امنیتی خاصی نیز دارند که به برخی از آنها در ذیل اشاره می‌شود.

۱-۱. مسائل امنیتی و حملات ویژه سرویس‌های وب
پروتکل HTTP از پروتکل‌های پرکاربرد انتقال در وب است و آسیب‌پذیری‌های آن، تهدیدات سرویس‌های وب تلقی می‌شود [۲]. ده مورد از بیشترین آسیب‌پذیری کاربردهای وب که از طرف مؤسسه OWASP در سال ۲۰۱۰ منتشر شده، در مورد سرویس‌های وب نیز صادق است [۵]. براساس مرجع [۶]، حملات رایجی که هدف اصلی آنها از کار انداختن یا سوءاستفاده از سرویس‌های وب است، عبارتند از:
سوءاستفاده از فایل توصیف سرویس وب: مشخصه در دسترس بودن توصیف سرویس وب در WSDL در محیط باز اینترنت، می‌تواند مبنایی برای سوءاستفاده و تدارک حمله باشد.

* ایمیل نویسنده پاسخگو: sbejani@ihu.ac.ir
[1] eXtensible Markup Language
[2] Web Service Description Language
[3] Simple Object Access Protocol
[4] Universal Description, Discovery and Integration