مرکز تهران

پایان‌نامه برای دریافت درجه کارشناسی ارشد

در رشته مهندسی کامپیوتر- نرم افزار

دانشکده فنی و مهندسی

گروه علمی فناوری اطلاعات و ارتباطات

عنوان پایان‌نامه:

# ایجاد یک لایه امنیتی وب سرویس

نگارش:

رضا قلعه

استاد راهنما:

دکتر عباس قائمی بافقی

استاد مشاور:

دکتر احمد فراهی

پاییز ۱۳۸۸

## چکیده

امروزه اهمیت کاربردهای مبتنی بر وب بر هیچ شخصی پوشیده نیست. با ظهور وب سرویس‌ها به عنوان یک بستر ارائه خدمات نوین، بسیاری از مجموعه‌ها از آن برای ارائه خدمات خود به سایرین استفاده کرده‌اند. در کنار نحوه و کیفیت خدمات رسانی، مسائل امنیتی از مهمترین چالش‌های پیش روی سرویس‌های مبتنی بر  وب است. از نگاه مهندسی نرم افزار برآورده ساختن امنیت ، می‌بایست در طول چرخه تولید نرم افزار مورد توجه قرار گیرد. اما بسیاری از کاربردهای موجود، دارای نقایص امنیتی هستند که تهدید بالقوه‌ای برای سرویس دهنده‌ها و مصرف کننده‌ها به حساب می‌آیند. یکی از پر هزینه ترین فعالیت‌ها در چرخه تولید نرم افزار اعمال اصلاحات پس از تولید آن است.

در این پایان نامه، یک لایه امنیتی برای وب سرویس‌ها  با عنوان WSSLayer معرفی شده است. این لایه با قرار گیری برروی وب سرویس‌های موجود و بر اساس توصیف آسیب پذیری‌های آنها در قالب زبان WSVDL، از آنها در قبال تهدیدهای شناخته شده مبتنی بر وب محافظت می‌کند. به‌کارگیری این لایه نیازمند هیچگونه تغییر در کد وب سرویس نبوده و بنابراین هزینه‌ها را تا حدود قابل توجهی برای فراهم ساختن اهداف امنیتی مورد نظر، کاهش می‌دهد. زبان WSVDL نیز زبانی است که برپایه روش‌های استاندارد برای بیان آسیب پذیری‌ها به منظور توصیف آسیب پذیری‌های وب سرویس‌ها توسط مولفین ابداع و معرفی شده است. همچنین ابزار WSScanner برای کشف آسیب پذیری‌های وب سرویس‌ها با قابلیت ارائه گزارش‌ها در قالب WSVDL از دیگر مسائل ابداع شده در این پایان‌نامه است.

جهت ارزیابی لایه امنیتی، عملکرد این لایه برروی سه نمونه آسیب پذیر موجود که توسط مجموعه‌های معتبر برای مقاصد آموزشی تولید شده‌اند، توسط روال‌های خودکار و دستی مورد آزمون قرار گرفت.  پس از مدل ساختن آسیب پذیری ها در قالب WSVDL و استقرار لایه امنیتی برروی نمونه‌ها و در نتیجه این ارزیابی ها، لایه امنیتی WSSLayer توانسته بود تمامی حملات را شناسایی کرده و از نمونه‌ها در مقابل تهدیدها محافظت کند.



## کلمات کلیدی

آسیب پذیری، زبان توصیف آسیب پذیری، لایه امنیتی، وب سرویس‌ها، وفق پذیر،WSScanner، WSVDL ،WSSLayer

# فهرست علائم اختصاری

| | |
|---|---|
| ACL | Access Control Lists |
| B2B | Business to Business |
| CAPEC | Common Attack Pattern Enumeration and Classification |
| CEE | Common Event Expression |
| CPE | Common Platform Enumeration |
| CSRF | Cross Site Request Forgery |
| CVE | Common Vulnerability and Exposures |
| CWE | Common Weakness Enumeration |
| DAS | Direct Attached Storage |
| DOS | Denial Of Services |
| DTD | Document Type Definition |
| FTP | File Transfer Protocol |
| HTTP | Hyper Text Transfer Protocol |
| IDS | Intrusion Detection System |
| NAD | Network Attached Storage |
| OASIS | Advancing Open Standards for the Information Society |
| OVAL | Open Vulnerability and Assessment Language |
| OWASP | Open Web Application Security Project |
| PGP | Pretty Good Privacy |
| PKI | Public Key Infrastructure |
| S/MIME | Secure/Multipurpose Internet Email Extension |
| SAML | Security Assertion Markup Language |
| SAN | Storage Area Network |
| SCAP | Security Content Automation Protocol |
| SMTP | Simple Mail Transfer Protocol |
| SOAP | Simple Object Access Protocol |
| SSL | Secure Socket Layer |
| SSO | Single Sign-On |
| TCP | Transmission Control Protocol |
| TLS | Transport Layer Security |
| UDDI | Universal Directory Discovery Indexes |
| URI | Uniform Resource Identifier |
| W3C | World Wide Web Consortium |
| WASC | Web Application Security Statistics |

| | |
|---|---|
| WSDL | Web Services Description Language |
| WS-I | Web Services Interoperability Organization |
| WSScanner | Web Services security Scanner |
| WSSLayer | Web Services Security Layer |
| WSVDL | Web Services Vulnerability Description Language |
| XACML | eXtensible Access Control Markup Language |
| XCCDF | Extensible Configuration Checklist Description Format |
| XEE | External Entity Attack |
| XKMS | XML Key Management Specification |
| XML | eXtensible Markup Language |
| XSD | XML Schema Definition |
| XSLT | eXtensible Stylesheet Langauge Transformation |
| XSS | Cross Site Scripting |

## فهرست مطالب

## فهرست جداول

## فهرست اشکال

## فهرست قطعه کدها

# فصل اول

## مقدمه

امروزه اهمیت وب و کاربردهای مبتنی بر آن بر هیچ شخص و سازمانی پوشیده نیست. بسیاری از دولت‌ها و سازمان‌ها به منظور کاهش هزینه‌ها و افزایش کیفیت خدمات رسانی، وب را به عنوان درگاه خدمات رسانی دولت و سازمان خود مورد استفاده قرار می‌دهند. به دلیل اینکه خدمات مبتنی بر وب به صورت ۲۴ ساعته و بدون وقفه ارائه می‌گردند، کاندید بسیار مناسبی برای ارائه اینگونه خدمات به صورت الکترونیکی و برخط هستند.

کاربردهای مختلفی برروی بستر وب قابل ارائه می‌باشند. وب سرویس یکی از این کاربردها است. وب سرویس یک سیستم نرم افزاری است که برای پشتیبانی از تعاملات ماشین به ماشین در سطح یک شبکه طراحی شده است. به بیان دقیقتر وب سرویس یک سیستم نرم افزاری می‌باشد که با یک URI[۱] شناسایی شده باشد، واسط عمومی و ارتباطات آن از طریق XML[۲] تعریف شده و تعریف وب سرویس توسط سایر سیستم‌ها قابل کشف است. این سیستم‌ها برای ارتباط با وب سرویس‌ها، با توجه به تعاریف آنها از پیام‌های مبتنی بر XML استفاده می‌کنند. رد و بدل کردن این پیام‌ها معمولا از طریق پروتکل‌های اینترنت صورت می‌پذیرد.

در مقایسه وب سرویس‌ها با کاربردهای عادی مبتنی بر وب می‌توان به چند نکته اشاره کرد. اولین نکته این است که کاربران کاربردهای عادی مبتنی بر وب یا وب سایت‌ها انسان‌ها می‌باشند. این

---

[۱] Uniform Resource Identifier

[۲] eXtensible Markup Language

بدان معنی است که همیشه یک سوی این ارتباط انسان بوده که درخواست‌های خود را به اشکال مختلف و تعبیه شده، با وب سایت‌ها مطرح می‌کند، اما دوسوی تعاملات وب سرویس‌ها معمولا ماشین‌ها می‌باشند. همانطور که یک فرد برای ارسال پست الکترونیک از یک سایت ارائه دهنده خدمات الکترونیک بهره می‌برد، یک سایت ارائه خدمات الکترونیک نیز می‌تواند خدمات خود را از طریق وب سرویس‌های سایر مجموعه‌های موجود درخواست نماید.

دومین نکته مهم در تفاوت کاربردهای عادی وب و وب سرویس‌ها در شکل خروجی آنها می‌باشد. وب سایت‌ها معمولا ترکیبی از عناصر HTML[1] برای تشکیل یک صفحه تعامل پذیر برای کاربران است، اما خروجی وب سرویس‌ها معمولا به صورت داده‌هایی است که فاقد قالب نمایشی بوده و در قالب XML می‌باشد.

با ظهور وب سرویس‌ها به عنوان یک بستر ارائه خدمات نوین، بسیاری از شرکت‌ها و سازمان‌ها از این بستر برای ارائه خدمات خود به سایر مجموعه‌ها و اشخاص به صورت برخط استفاده می‌کنند. چالش‌ها و مسائل مختلفی پیش روی ارائه یک خدمت الکترونیک در قالب وب سرویس است. به عنوان مثال کارایی، دسترس پذیری، صحت و امنیت از این دسته مسائل به شمار می‌روند. در کنار نحوه و کیفیت خدمات رسانی به مشتریان، مسائل امنیتی از مهمترین چالش‌های پیش روی سرویس‌های مبتنی بر وب است. از طرف دیگر با فراگیرتر شدن استفاده از بستر وب و اینترنت، حجم سوء استفاده‌ها و تهدیدهای وب روز به روز در حال افزایش است [Stol 08].

تهدیدهای امنیتی هر دوسوی ارتباطات وب یعنی سرویس دهنده و سرویس گیرنده را مورد هدف قرار داده اند. از نگاه مهندسی نرم افزار برآورده ساختن امنیت به عنوان یک هدف، می‌بایست در طول چرخه تولید یک نرم افزار مورد توجه قرار گیرد [Howa 03]. پارامترها و شاخص‌های گوناگونی به منظور رعایت مسائل امنیتی موجود است که علاوه بر زمان تولید نرم افزار، در زمان‌های استقرار، بهره وری و پشتیبانی نیز بایستی مدنظر قرار گیرند.

امنیت درجه ای از محافظت در مقابل خطر و نابودی و جرم، است. واژه امنیت در حوزه‌های مختلف به‌کار برده می‌شود. در هر حوزه امنیت دارای تعاریف خاص خود می‌باشد. اگر خواسته باشیم

[1] Hyper Text Transfer Protocol

حوزه‌های درگیر در این پایان نامه را مشخص کنیم می‌توانیم به ترتیب از کل به جزء به امنیت اطلاعات، امنیت کامپیوتر و امنیت اینترنت اشاره کنیم.

امنیت اطلاعات به معنی محافظت از اطلاعات و سیستم‌های اطلاعاتی از دسترسی، استفاده، نشر غیرمجاز و افشا، دستکاری و تخریب است. محافظت از داده بدون توجه به قالب داده هدف اصلی این حوزه است. داده‌ها می‌توانند در قالب الکترونیکی، چاپی و یا سایر شیوه‌ها مورد محافظت قرار گیرند.

امنیت کامپیوتر، شاخه ای از امنیت اطلاعات است که برروی کامپیوترها اعمال می‌شود. هدف امنیت در این حوزه شامل محافظت از اطلاعات و خصوصیات یک سیستم در قبال نفوذ، دستکاری، افشا و تخریب به صورتی می‌باشد که همیشه اطلاعات و خصوصیات یک سیستم برای کاربران مجاز در دسترس باشد.

امنیت در حوزه اینترنت به معنی اندازه‌گیری انجام شده به منظور محافظت از یک سیستم و منابع آن از دسترسی غیرمجاز، تغییر، تخریب و از دست دادن آنها می‌باشد. فارغ از حوزه کاربرد، امنیت اطلاعات دارای یک سری از مفاهیم و اصول است. این اصول و مفاهیم در بسیاری از حوزه‌های زیر شاخه امنیت اطلاعات به صورت مشترک مطرح می‌باشند.

## ۱-۱ انگیزه‌ها

فارغ از بحث امنیت در چرخه تولید یک نرم افزار، بسیاری از کاربردهای موجود، دارای نقایص امنیتی می‌باشند که تهدید بالقوه‌ای برای سرویس دهنده‌ها و سرویس گیرنده‌ها به حساب می‌آیند. اعمال هرگونه تغییرات برروی نرم افزاری که به صورت کاربردی مورد استفاده می‌باشد، همیشه یکی از چالش‌های مهم پیش روی توسعه دهندگان نرم افزار های می‌باشد. رفع خطاها، به روز رسانی ها، ارتقاء ها و رفع آسیب پذیری‌ها از این دسته تغییرات می‌باشند. هرگونه تغییرات در نرم افزار، آنرا از حالت استوار و ثابت خود خارج می‌سازد.

یکی از پر هزینه ترین فعالیت‌ها در چرخه تولید نرم افزار اعمال اصلاحات پس از تولید آن است. با انجام تغییرات در سیستم ممکن است خطاهایی بروز کند حتی اگر آن تغییرات خود رفع خطا باشند. به مزاح به گفته تنی چند از دوستان در توسعه سیستم، قانونی به عنوان قانون "بقای خطا" وجود دارد و آن این است که "هیچ گاه خطا در یک نرم افزار از بین نمی‌رود بلکه از شکلی به شکل

دیگر در می‌آید". این جمله یک شوخی بیش نیست ولی واقعیتی در آن است که بسیار مهم بوده و همان هزینه بر بودن انجام تغییرات پس از ایجاد نرم افزارها می‌باشد.

اصلاحات امنیتی نیز از همین دسته تغییرات می‌باشند. یکی از انگیزه‌های مهم و شاید اصلی ترین انگیزه طرح ما این است که سیستم و شیوه ای ابداع گردد که به منظور رفع آسیب پذیری‌های وب سرویس‌ها نیازی به انجام تغییرات در کد آنها نباشد. آسیب پذیری‌های یک وب سرویس به گونه ای به سیستم معرفی گردند و این سیستم به صورتی از وب سرویس‌ها در مقابل آن آسیب پذیر ی ها محافظت کند که همانند آن باشد که آن آسیب پذیری در وب سرویس مرتفع گردیده باشد.

یکی دیگر از انگیزه‌های طرح مباحث مربوط به کارایی است. به دلیل اینکه وب سرویس‌ها معمولا به صورت گسترده توسط منابع مختلفی استفاده شده و به عنوان یک زیر ساخت برای سایر سرویس‌ها و خدمات مورد استفاده قرار می‌گیرند، انجام تغییرات امنیتی می‌بایست کمترین تاثیر را در کارایی کلی وب سرویس‌ها داشته باشد. بسیاری از آسیب پذیری‌ها مختص یک سرویس خاص می‌باشد و ممکن است سایر سرویس‌های یک مجموعه به آن دچار نشده باشند. بررسی اینگونه از آسیب پذیری‌ها برای تمامی‌سرویس‌های موجود در یک مجموعه، فعالیتی است که منجربه کاهش کارایی کل مجموعه خواهد شد.

همان‌طور که در ادامه این پایان‌نامه به صورت کامل به آن اشاره خواهد شد، شیوه‌های خاصی برای مسائل امنیتی در پیام‌های وب سرویس‌ها مورد استفاده قرار می‌گیرند. یکی از این شیوه‌ها رمزنگاری پیام و یا بخشی از پیام است. یکی دیگر از انگیزه‌های این طرح آن است که بتوان مسائل امنیتی مخفی شده در پشت این رمزنگاری ها و موارد مشابه را نیز مورد بررسی قرار داد. یعنی محتوا را پس از رمزگشایی شدن نیز مورد بررسی قرار داد.

## ۱-۲ تعریف مسئله

با توجه به انگیزه‌های بیان شده و مسائل موجود، طرح مورد نظر به صورت خلاصه عبارت است از:

"ایجاد یک لایه امنیتی برروی وب سرویس‌های موجود که توسط آن بتوان بازه وسیعی از آسیب پذیری‌های لایه کاربردی وب سرویس‌ها را بدون نیاز به تغییر کد برنامه رفع کرد"

در این تعریف چند نکته قابل توجه است.

اولین نکته این است که جامعه هدف ما "وب سرویس‌های موجود" است. همانطور که در بخش انگیزه‌ها به آن اشاره شده به دلیل وجود آسیب پذیری‌ها در وب سرویس‌های موجود، تاکید ما برروی اینگونه وب سرویس‌ها است. البته این بدان معنی نیست که راهکار ارائه شده را نمی‌توان برای وب سرویسی که در حال تولید می‌باشد مورد استفاده قرار داد. نرم افزاری که در حال تولید است، پس از آن به صورت نرم افزار موجود تبدیل شده و در داخل تعریف راهکار ما قرار می‌گیرد. اما توصیه می‌شود برای وب سرویسی که می‌خواهد از ابتدا توسعه داده شود، حتما مسائل امنیتی در طول چرخه تولید مدنظر قرار گیرند [Howa 03].

نکته بعدی انواع آسیب پذیری‌های مورد نظر می‌باشد. این آسیب پذیری‌ها در تعریف به عنوان آسیب پذیری‌های لایه کاربردی وب سرویس‌ها معرفی شده اند. این بدان معنی است که سایر آسیب پذیری‌ها در حوزه‌های مختلف مانند شبکه، میزبان و یا سرویس دهنده خارج از حوزه پوشش این طرح می‌باشند. شیوه‌ها و سرویس‌های امنیتی گسترده ای برای سایر آسیب پذیری‌ها نظیر سیستم‌های تشخیص نفوذ، دیوار آتش، سیستم‌های ضد ویروس، به روز رسانی نرم افزارهای میزبان‌ها و ... از این دسته شیوه‌ها و سرویس‌های امنیتی می‌باشند. آسیب پذیری‌های لایه کاربردی مواردی هستند که به طور مشخص با کد و نحوه توسعه وب سرویس سروکار دارند. معمولا این نوع آسیب پذیری‌ها بر اساس شیوه‌های نادرست کد نویسی در وب سرویس‌ها و سایر سیستم‌های وابسته مانند مفسرهای XML و چارچوبهای توسعه وب سرویس‌ها بوجود می‌آیند.

با توجه به گستردگی مباحث مربوط به امنیت به طور طبیعی حوزه‌هایی وجود خواهند داشت که در محدوده این طرح به آن پرداخته نمی شود. یکی از مهمترین این حوزه‌ها امنیت پیام است. روشهای مختلفی برای امن سازی و رمزنگاری پیام‌های وب سرویس وجود دارد. در ادامه این گزارش و در فصل سوم روش‌های و شیوه‌های موجود در زمینه رمزنگاری و امنیت پیام‌ها به صورت کامل معرفی می شوند.

با توجه به موارد فوق در این طرح یک لایه امنینی با عنوان WSSLayer[۱] معرفی شده است که با قرار گیری برروی وب سرویس‌ها و دریافت توصیف آسیب پذیری‌های آنها در قالب زبان WSVDL[۱]، از وب سرویس‌ها در قبال آسیب پذیری‌های معرفی شده محافظت می‌کند.

---

[۱] Web Services Security Layer