



دانشگاه پیام نور

مرکز تهران

پایان نامه برای دریافت درجه کارشناسی ارشد
در رشته مهندسی کامپیوتر - نرم افزار

دانشکده فنی و مهندسی
گروه علمی فناوری اطلاعات و ارتباطات

عنوان پایان نامه:

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 بر روی 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. به کارگیری 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 پایان نامه است.

جهت ارزیابی لایه امنیتی، عملکرد این لایه بر روی 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 پذیری‌ها در قالب WSVDL و استقرار لایه امنیتی بر روی نمونه‌ها و در نتیجه این ارزیابی‌ها، 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 Language Transformation
XSS	Cross Site Scripting

فهرست مطالب

۱۶	فصل اول - مقدمه
۱۸	۱-۱ انگیزه‌ها
۱۹	۲-۱ تعریف مسئله
۲۱	۳-۱ سابقه طرح
۲۲	۴-۱ نوآوری طرح
۲۳	۵-۱ محتوای گزارش
۲۷	فصل دوم - مبانی وب سرویس‌ها و امنیت
۲۸	۱-۲ وب سرویس‌ها
۲۹	۱-۱-۲ مقایسه وب سرویس و وب کاربردی
۳۰	۲-۱-۲ ابزارهای توسعه وب سرویس
۳۹	۳-۱-۲ کاربردها
۴۰	۲-۲ امنیت
۴۱	۱-۲-۲ فرهنگ لغات امنیت
۴۱	۲-۲-۲ مفاهیم اساسی امنیت
۴۷	۳-۲-۲ امنیت از دیدگاه تقسیم بندی حوزه‌ای
۴۸	۳-۲ امنیت سیستم‌های کامپیوتری
۴۸	۱-۳-۲ امنیت زیرساخت و سیستم عامل
۵۱	۲-۳-۲ امنیت داده‌ها و اطلاعات
۵۴	۳-۳-۲ امنیت شبکه
۵۷	۴-۳-۲ امنیت نرم افزار

فصل سوم - امنیت وب سرویس‌ها ۶۲

۱-۳ آسیب پذیری‌ها در وب سرویس ۶۳

۱-۱-۳ تلاش‌های صورت گرفته برای معرفی آسیب پذیری‌های برتر ۶۴

۲-۱-۳ آسیب پذیری‌های برتر ۶۶

۲-۳ ارزیابی امنیتی وب سرویس ۷۱

۱-۲-۳ روش‌های شناسایی و معیارها ۷۱

۲-۲-۳ ابزارهای شناسایی ۷۳

۳-۲-۳ روش‌های توصیف ۷۴

۳-۳ شیوه‌های ایجاد امنیت در وب سرویس‌ها ۷۹

۱-۳-۳ XML Encryption ۷۹

۲-۳-۳ XML Signature ۸۰

۳-۳-۳ XKMS ۸۱

۴-۳-۳ SAML ۸۳

۵-۳-۳ XACML ۸۳

۶-۳-۳ WS-Security ۸۴

۴-۳ جمع بندی ۸۵

فصل چهارم - طرح لایه امنیتی پیشنهادی ۸۸

۱-۴ طرح کلی لایه ۸۹

۲-۴ محل قرارگیری لایه ۹۰

۱-۲-۴ شیوه‌های مبتنی بر میزبان ۹۱

۲-۲-۴ شیوه‌های مبتنی بر شبکه ۹۲

۳-۲-۴ راهکار انتخابی برای محل قرارگیری لایه امنیتی ۹۳

۳-۴ پایگاه دانش	۹۴
۴-۴ واحد کشف تهدید	۹۶
۵-۴ واحد جلوگیری	۹۸
۶-۴ واحد بایگانی	۹۹
۷-۴ واحد سیاست گذاری	۱۰۰
فصل پنجم - توصیف آسیب پذیری ها و پویشگر WSScanner	
۱-۵ شیوه برخورد با آسیب پذیری های مختلف	۱۰۳
۱-۱-۵ شیوه برخورد با آسیب پذیری های عام	۱۰۵
۲-۱-۵ شیوه برخورد با آسیب پذیری های خاص	۱۰۷
۲-۵ زبان توصیف آسیب پذیری های وب سرویس WSVDL	۱۰۸
۱-۲-۵ چرا AVDL توانایی بیان آسیب پذیری های وب سرویس ها را ندارد	۱۰۸
۲-۲-۵ ساختار WSVDL	۱۰۹
۳-۲-۵ تولید WSVDL	۱۱۶
۳-۵ ابزار کشف آسیب پذیری های وب سرویس WSScanner	۱۱۷
۱-۳-۵ معماری WSScanner	۱۱۸
۲-۳-۵ واحد کاوشگر وب سرویس	۱۱۹
۳-۳-۵ واحد شبیه سازی حمله	۱۲۱
۴-۳-۵ واحد تولید گزارش	۱۲۳
فصل ششم - پیاده سازی و ارزیابی لایه امنیتی پیشنهادی	
۱-۶ زیر ساخت مورد استفاده	۱۲۷
۲-۶ ساختار پایگاه دانش	۱۲۸
۱-۲-۶ روش های مختلف بازنمایی دانش	۱۲۹

۱۳۱.....	۲-۲-۶ ارزیابی روش‌های بازنمایی و انتخاب راهکار مورد استفاده
۱۳۵.....	۳-۶ توصیف آسیب‌پذیری‌های خاص توسط WSVDL
۱۳۵.....	۱-۳-۶ تزریق SQL
۱۳۸.....	۲-۳-۶ پیمایش مسیر
۱۴۰.....	۳-۳-۶ XSS
۱۴۱.....	۴-۳-۶ سرریز بافر
۱۴۲.....	۵-۳-۶ XPath تزریق
۱۴۳.....	۴-۶ توصیف آسیب‌پذیری‌های عام توسط فیلترها
۱۴۴.....	۱-۴-۶ حمله موجودیت خارجی یا XEE
۱۴۵.....	۲-۴-۶ XML نامعتبر
۱۴۶.....	۳-۴-۶ XML حجیم
۱۴۷.....	۵-۶ ارزیابی لایه امنیتی
۱۴۸.....	۱-۵-۶ نمونه‌های آسیب پذیر
۱۴۸.....	۲-۵-۶ شیوه ارزیابی
۱۴۹.....	۳-۵-۶ نتایج ارزیابی
۱۵۳.....	فصل هفتم - نتیجه‌گیری و کارهای آینده
۱۵۶.....	منابع و مراجع
۱۶۱.....	واژه‌نامه انگلیسی به فارسی
۱۶۳.....	واژه‌نامه فارسی به انگلیسی

فهرست جداول

- جدول ۱-۲: ارتباط بین سرویس‌ها و مکانیزم‌های امنیتی ۴۶
- جدول ۱-۳: زبان‌های توصیف آسیب پذیری‌ها ۷۶
- جدول ۱-۶: مشخصات تکنولوژی پیاده سازی WSSLayer ۱۲۷
- جدول ۲-۶: مشخصات کامپیوتر مورد استفاده برای ارزیابی شیوه بازنمایی دانش ۱۳۲
- جدول ۳-۶: نتایج آزمون کارایی وب سرویس بدون لایه امنیتی ۱۳۲
- جدول ۴-۶: نتایج آزمون کارایی وب سرویس با لایه XML + ۱۳۳
- جدول ۵-۶: نتایج آزمون کارایی وب سرویس با لایه + کد اجرایی ۱۳۴
- جدول ۶-۶: نتایج آزمون کارایی شیوه‌های مختلف بیان دانش بر روی وب سرویس نمونه ۱۳۴
- جدول ۷-۶: اطلاعات نگهداری شده در موجودیت AttackSteps در پایگاه دانش ۱۳۸
- جدول ۸-۶: خلاصه تعداد آسیب پذیری‌های یافت شده ۱۴۹
- جدول ۹-۶: جزئیات تعداد آسیب پذیری‌های یافت شده ۱۵۰

فهرست اشکال

- شکل ۱-۲: پشته معماری وب سرویس‌ها ۳۱
- شکل ۲-۲: فراخوانی وب سرویس‌ها ۴۰
- شکل ۳-۲: دیوار آتش برنامه کاربردی وب ۵۴
- شکل ۴-۲: دسته بندی انواع سیستم‌های تشخیص نفوذ ۵۶
- شکل ۱-۳: امنیت در سطح پیام در مقابل امنیت در سطح انتقال ۶۴
- شکل ۲-۳: فرمو امتیاز دهی CCWAPSS ۷۳
- شکل ۳-۳: ساختار کلی AVDL ۷۸
- شکل ۴-۳: نحوه تعامل XKMS با PKI ۸۲
- شکل ۱-۴: معماری کلی لایه امنیتی WSSLayer ۹۰
- شکل ۲-۴: محل قرار گیری لایه امنیتی WSSLayer ۹۳
- شکل ۳-۴: مولفه‌های پایگاه دانش ۹۵
- شکل ۴-۴: موجودیت نگهداری کاربران مسدود شده ۹۹
- شکل ۵-۴: موجودیت نگهداری اطلاعات بایگانی ۹۹
- شکل ۱-۵: محل قرار گیری فیلترها در فایل سیستم ۱۰۷
- شکل ۲-۵: ساختار کلی WSVDL ۱۱۰
- شکل ۳-۵: اجزای تشکیل دهنده WSScanner ۱۱۸

فهرست قطعه کدها

۳۲	قطعه کد ۱-۲: نمونه ای از یک سند XML
۳۳	قطعه کد ۲-۲: قالب کلی یک پیام SOAP
۳۴	قطعه کد ۳-۲: نمونه ای از عنصر Header
۳۴	قطعه کد ۴-۲: نمونه ای از یک درخواست
۳۵	قطعه کد ۵-۲: پاسخ درخواست قطعه کد ۴-۲
۳۶	قطعه کد ۶-۲: نحوه استفاده از SOAP در HTTP
۳۷	قطعه کد ۷-۲: تعریف type در یک سند WSDL
۳۸	قطعه کد ۸-۲: تعریف Message در سند WSDL
۳۸	قطعه کد ۹-۲: تعریف Port Type در سند WSDL
۹۷	قطعه کد ۱-۴: عملکرد واحد کشف تهدید WSSLayer
۱۰۵	قطعه کد ۱-۵: واسط پیاده سازی HTTPInputFilter
۱۰۵	قطعه کد ۲-۵: واسط پیاده سازی HTTPOutputFilter
۱۰۶	قطعه کد ۳-۵: واسط پیاده سازی SOAPInputFilter
۱۰۶	قطعه کد ۴-۵: واسط پیاده سازی SOAPOutputFilter
۱۰۶	قطعه کد ۵-۵: کلاس در بردارنده مشخصات حمله کشف شده
۱۱۰	قطعه کد ۶-۵: عنصر ریشه یک سند WSVDL
۱۱۱	قطعه کد ۷-۵: نمونه ای از یک traversal session
۱۱۲	قطعه کد ۸-۵: نمونه ای از یک sopa-traversal
۱۱۲	قطعه کد ۹-۵: نمونه ای از یک vulnerability session
۱۱۵	قطعه کد ۱۰-۵: نمونه ای از یک soap probe
۱۱۵	قطعه کد ۱۱-۵: نمونه ای از یک test script
۱۱۶	قطعه کد ۱۲-۵: نمونه ای از یک test description
۱۲۰	قطعه کد ۱۳-۵: نمونه ای از سند WSDL برای وب سرویس محصولات
۱۲۱	قطعه کد ۱۴-۵: کلاسه پایه Attack برای WSScanner
۱۲۳	قطعه کد ۱۵-۵: ساختار کلاس AttackDefinition به همراه انواع وابسته

- ۱۲۴ قطعه کد ۵-۱۶: تعریف حمله SQL Injection
- ۱۲۵ قطعه کد ۵-۱۷: بیان WSVDL آسیب پذیری تزریق SQL در سرویس GetProduct
- ۱۳۲ قطعه کد ۶-۱: خروجی فراخوانی وب سرویس نمونه
- ۱۳۳ قطعه کد ۶-۲: بیان آسیب پذیری‌ها در قالب XML نمونه
- ۱۳۳ قطعه کد ۶-۳: شبه کد پردازش دانش XML
- ۱۳۴ قطعه کد ۶-۴: نمونه کد بررسی وقوع حمله در لایه امنیتی
- ۱۳۵ قطعه کد ۶-۵: فراخوانی سرویس Login
- ۱۳۶ قطعه کد ۶-۶: حمله تزریق SQL به سرویس Login
- ۱۳۷ قطعه کد ۶-۷: بیان WSVDL آسیب پذیری تزریق SQL در سرویس Login
- ۱۳۸ قطعه کد ۶-۸: بیان آسیب پذیری تزریق SQL سرویس Login در پایگاه دانش
- ۱۳۸ قطعه کد ۶-۹: فراخوانی سرویس GetProductInfo
- ۱۳۹ قطعه کد ۶-۱۰: حمله پیمایش مسیر به سرویس GetProductInfo
- ۱۳۹ قطعه کد ۶-۱۲: بیان آسیب پذیری پیمایش مسیر سرویس GetProductInfo در پایگاه دانش
- ۱۴۰ قطعه کد ۶-۱۳: فراخوانی سرویس SetComment
- ۱۴۰ قطعه کد ۶-۱۴: حمله XSS به سرویس SetComment
- ۱۴۱ قطعه کد ۶-۱۶: بیان آسیب پذیری XSS سرویس SetComment در پایگاه دانش
- ۱۴۱ قطعه کد ۶-۱۷: فراخوانی سرویس CallCCode
- ۱۴۱ قطعه کد ۶-۱۸: حمله سرریز بافر به سرویس CallCCode
- ۱۴۲ قطعه کد ۶-۲۰: بیان آسیب پذیری سرریز بافر سرویس CallCCode در پایگاه دانش
- ۱۴۲ قطعه کد ۶-۲۱: سند XML حاوی اطلاعات کاربران
- ۱۴۲ قطعه کد ۶-۲۲: فراخوانی سرویس Login
- ۱۴۳ قطعه کد ۶-۲۳: حمله تزریق XPath به سرویس Login
- ۱۴۳ قطعه کد ۶-۲۵: بیان آسیب پذیری تزریق XPath سرویس Login در پایگاه دانش
- ۱۴۴ قطعه کد ۶-۲۶: نمونه‌هایی از XEE در سند XML
- ۱۴۵ قطعه کد ۶-۲۷: نمونه فیلتر برای آسیب پذیری XEE
- ۱۴۶ قطعه کد ۶-۲۸: نمونه فیلتر برای آسیب پذیری XML نامعتبر

- قطعه کد ۶-۲۹: نمونه ای از XML با حجم بالا ۱۴۶
- قطعه کد ۶-۳۰: نمونه ای از XML با حجم بالا ۱۴۷
- قطعه کد ۶-۳۱: نمونه فیلتر برای آسیب پذیری XML با حجم بالا ۱۴۷
- قطعه کد ۶-۳۲: قطعه ای از توصیف آسیب پذیری تزریق SQL ۱۵۱

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 بر روی 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 معمولاً 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

Uniform Resource Identifier ^۱
eXtensible Markup Language ^۲

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 معمولاً 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 معمولاً ترکیبی از عناصر HTML^۱ برای تشکیل یک صفحه تعامل پذیر برای کاربران است، اما خروجی وب سرویس‌ها معمولاً 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، بهره‌وری 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 به کار برده می‌شود. در هر حوزه امنیت دارای تعاریف خاص خود می‌باشد. اگر خواسته باشیم

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، شاخه‌ای از امنیت اطلاعات است که بر روی 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 بر روی نرم افزاری که به صورت کاربردی مورد استفاده می‌باشد، همیشه یکی از چالش‌های مهم پیش روی توسعه دهندگان نرم افزارهای می‌باشد. رفع خطاها، به روز رسانی‌ها، ارتقاءها 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 پرهزینه‌ترین 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 پذیری‌ها 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 معمولاً 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 تمامی سرویس‌های موجود در یک مجموعه، فعالیتی است که منجر به 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 رمزنگاری‌ها و موارد مشابه را نیز مورد بررسی قرار داد. یعنی محتوا را پس از رمزگشایی شدن نیز مورد بررسی قرار داد.

۲-۱ تعریف مسئله

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

"ایجاد یک لایه امنیتی بر روی 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 بر روی 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 نمی‌شود. 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 می‌شوند.

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