هفتمین کنفرانس بین المللی انجمن رمز ایران

۲۴ و ۲۵ شهریورماه ۱۳۸۹، دانشگاه صنعتی خواجه نصیرالدین طوسی

انجمن رمزایران

دانشگاه صنعتی خواجه نصیرالدین طوسی

مقایسه تطبیقی و کمی بسترهای توسعه نرم افزار J2EE وNET. با معیار سطح حمله

سرویه نصیری [۱]، رضا عزمی [۲]، رضا خلج [۳]

کارشناسی ارشد مهندسی فناوری اطلاعات گرایش امنیت اطلاعات، دانشگاه صنعتی مالک اشتر [۱]

nasiri_sa@yahoo.com

استادیار گروه مهندسی کامپیوتر ، دانشگاه الزهرا [۲]

azmi@alzahra.ac.ir

کارشناسی ارشد مهندسی کامپیوترگرایش هوش مصنوعی، دانشگاه علم وصنعت [۳]

r_khalaj@iust.ac.ir

چکیده

بسترهای توسعه نقش مهمی در ایجاد و توسعه نرم افزارهای کاربردی دارند. بررسی‌ها نشان می‌دهد که معیارسطح حمله، مقیاس قابل اطمینانی برای اندازه‌گیری کمی امنیت نرم‌افزارهای مشابه از لحاظ عملکرد می‌باشد. نرخ پتانسیل صدمه یا تعیین میزان مشارکت منابع در حمله یکی از چالش‌های اندازه‌گیری سطح حمله می باشد. در روش پیشنهادی از سیستم امتیازدهی آسیب‌پذیری‌های متداول به نام **CVSS** به عنوان یک معیار قابل اطمینان برای تعیین میزان مشارکت منابع در حمله استفاده شده است.

در این مقاله مقایسه ای بین سطوح حمله در دو بستر بدون توجه به نسخه و در مرحله بعد با در نظر گرفتن نسخه های مختلف از بسترها صورت گرفته است. در حالت خاص مقایسه ای بین سطوح حمله پذیری مکانیزمهای امنیتی بسترها انجام شده و نشان می دهد بطور کلی**J2EE** نسبت به **.NET** سطح حمله بیشتری دارد. اما با توجه به اینکه در عمل تنها بخشی از محیط توسعه بکارگرفته می‌شود تعیین سطح حمله موثر وابسته به نوع کاربرد می باشد و پژوهش انجام شده بستر لازم را برای انجام اینکار فراهم می کند.

کلمات کلیدی

سطح حمله، کاهش مخاطره، پتانسیل صدمه، بردار حمله، مخاطره امنیتی،**CVSS**.

۱- مقدمه !

مشتریان نرم‌افزار اغلب مواجه با انتخاب یک محصول نرم‌افزاری از مجموعه‌ای از محصولات رقیب می باشند که کارکردهای مشابهی را ارائه می دهند. به طور مثال، مدیران سیستم اغلب بین انتخاب سیستم‌عامل‌های موجود، بسترهای توسعه نرم‌افزار، وب سرورها، نرم‌افزارهای مدیریت پایگاه‌داده و سایر سیستم‌های نرم افزاری برای سازمان خود باید تصمیم‌گیری کنند. مشتریان می‌توانند از معیار سطح حمله به عنوان معیاری برای فرآیند تصمیم گیری استفاده نمایند.

در این تحقیق اندازه گیری سطح حملهٔ بسترهای J2EE وNET باالهام از روش پیشنهادی هاوارد [۱] [1]صورت گرفته است. با توجه به اینکه روش هاوارد روی نسخه‌های مختلف ویندوز انجام شده قابل تعمیم برای سایر سیستم‌های نرم افزاری مانند مقایسه سطح حمله بسترهای J2EE و NET. نمی‌باشد. به طور نمونه بردارهای حمله استخراج شده درسیستم عامل ویندوز در حالت کلی قابل استفاده در سیستم های نرم افزاری J2EE و NET. نمی‌باشند. لیکن استخراج بردارهای حمله در این بسترها براساس

[1] Howard

شناسایی دقیق منابع آسیب‌پذیر متفاوت از سیستم‌های عامل صورت گرفته است. علاوه برآن در خصوص وزن‌دهی به بردارهای حمله، هاوارد بر اساس دانش تخصصی خود از سیستم‌های عامل عمل کرده است که این روش نه تنها مستعد خطاست بلکه در حالت کلی قابل استفاده در بسترهای نرم‌افزاری J2EE وNET. نمی باشد. در این مقاله از سیستم امتیازدهی آسیب پذیری به نام CVSS[1] به عنوان یک مقیاس قابل اطمینان تر استفاده شده است. برای اندازه گیری سطح حمله در بسترهای J2EE وNET. از سه روش زیر استفاده شده است :

روش اول : اندازه گیری سطح حمله در سالهای متوالی (از زمان شروع انتشار آسیب پذیریها در دو بستر).

روش دوم : اندازه گیری سطح حمله با توجه به تغییرات نسخه در دو بستر.

روش سوم : اندازه گیری سطح حمله پذیری مکانیزمهای امنیتی در دو بستر.

در روش اول بدون توجه به نسخه، سطح حمله در دو بستر در سالهای مختلف محاسبه می گردد. در روش دوم سطح حمله نسبت به نسخه های مختلف به دست آمده و نسخه های نزدیک به هم از دو بستر با هم مقایسه می گردند. در این روش علاوه بر این که دو بستر J2EE و NET. باهم مقایسه می گردند، نسخه های مختلف هرکدام از بسترها نیز با همدیگر مقایسه خواهند شد و در روش سوم به طور خاص سطح حمله پذیری مکانیزمهای امنیتی در بسترها مقایسه خواهند شد.

در ادامه و در بخش ۲، ابتدا مروری بر پژوهشهای قبلی خواهیم داشت. در بخش ۳، معیارسطح حمله و روش تعیین سطح حمله هاوارد معرفی می شود. سپس در بخش۴، اندازه گیری سطح حمله در بسترهای J2EE و NET. ارائه می شود.این بخش شامل نتایج حاصل از مقایسه سطوح حمله دراین دو بستر است و در نهایت در بخش ۵ نتیجه گیری کلی و کارهای آتی ارائه شده اند.

۲-مرور پژوهش‌های قبلی

سطح حمله، معیار قابل قبولی برای اندازه گیری نسبی امنیت سیستم های مشابه از لحاظ عملکرد می باشد. هاوارد سطح حمله را برای سیستم عامل ویندوز به صورت غیر فرمال معرفی کرد[1]. پینکاس[2] و وینگ[3] روی مدل غیر فرمال هاوارد کار بیشتری انجام دادند[2].

کارهای مشابه دیگری مانند اندازه گیری سطح حمله در FTP Deamon متن باز با الهام از روش هاوارد صورت گرفته است. در این مقایسه سطح حمله در ابعاد مختلفی که همگی جزء منابع سیستم محسوب می شوند با استفاده از کد منبع نرم افزارها به دست آمده و نرخ پتانسیل صدمه جهت وزن دهی به بردارهای حمله تعریف شده است [4]. این روش به دلیل اینکه کد منبع سیستم‌های نرم افزاری J2EE و NET. در اختیار نمی باشند یا حداقل به طور کامل نمی توان به آنها دست یافت و یا حتی در صورت دسترسی حجم بسیار بالایی دارد قابل بکارگیری نیست. برای اندازه گیری سطح حمله در سیستم های نرم افزاری با حجم کد زیاد می توان از روشهای مکانیزه استخراج آسیب‌پذیری در سطح کد و درنهایت تعیین سطح حمله مبتنی بر آن استفاده کرد که معمولا دقت بالایی نداشته و میزان خطای آن زیاد است [5]. اندازه گیری سطح حمله برای سایر سیستم های نرم افزاری به ویژه مقایسه نسخه های مختلف لینوکس، سرورIMAP [4] و سایر نرم افزارها به روشهای مشابه انجام شده است [6].

در روش فرمال، معیار سطح حمله، وابسته به کد منبع سیستم‌های نرم‌افزاری، فرموله شده و روش سیستماتیکی برای اندازه‌گیری آن پیشنهاد شده است. [6].

۳-معیار سطح حمله

سطح حمله سیستم زیر مجموعه ای از منابعی است که مهاجم برای حمله به سیستم استفاده می‌کند. هر چه اندازه سطح حمله بزرگ تر باشد، سیستم ناامن‌تر است. تمامی منابع، بخشی از سطح حمله نمی باشند. اگر یک مهاجم بتواند از منبع جهت حمله به سیستم استفاده کند آن منبع بخشی از سطح حمله است. همچنین تمامی منابع به طور یکسان در اندازه گیری سطح حمله مشارکت ندارند[4].

اندازه سطح حمله بزرگتر دلالت بر وجود آسیب پذیری های بیشتر در سیستم ندارد. وجود آسیب پذیری های کمتر هم دلالت بر میزان سطح حمله کمتر ندارد. در عوض، میزان سطح حمله بزرگتر نشان دهنده آن است که یک مهاجم احتمالا از آسیب پذیری ارائه شده در سیستم به راحتی بهره برده و منجر به صدمه بیشتری در سیستم می شود.

هاوارد، پینکاس و وینگ براساس تاریخچه حملات روی ویندوز بیست بردارحمله را شناسایی کرده و به آنها وزنهایی بر اساس دانش تخصصی خود از ویندوز نسبت دادند. نتایج اندازه گیری ایده شهودی در مورد امنیت نسبی هفت نسخه از ویندوز را تائید می کرد. به طور مثال، براساس مشاهدات windows 2000 در مقایسه با windows NT امنیت بهتری دارد. نتایج اندازه گیری هاوارد نشان می دهد که windows 2000 سطح حمله کمتری نسبت به windows NT دارد. بنابراین، اندازه گیری ها، مشاهدات کلی را منعکس می کرد. به طور مشابه، اندازه گیری نشان می دهد که windows server 2003 سطح حمله کمتری در میان هفت

[1] Common Vulnerability Scoring System
[2] Pincus
[3] Wing
[4] Internet Message Access Protocol

نسخه از ویندوز دارد. این اندازه گیری ها با مشاهدات درخصوص رفتارها در برابر آسیب پذیری نسبت به کرمهایی چون CodeRed و Nimda مطابقت دارد.

اولین گام در روش اندازه گیری هاوارد، شناسایی بردارهای حمله است. یعنی ویژگیهایی از سیستم های عامل که اغلب در حمله به آنها استفاده می شوند. نمونه هایی از آنها فایلهای کتابخانه موجود، سرویسهای هویت سنجی و مجازشناسی، صفحات وب پویا و حسابهای کاربری می باشند. همچنین تمامی ویژگیها به طور یکسان در حمله استفاده نمی شوند. به طورمثال، سرویسی که به صورت سیستمی اجرا می گردد، درجه آسیب پذیری بیشتری نسبت به سرویس در حال اجرا به وسیله کاربر معمولی دارد. بنابراین دومین مرحله در روش هاوارد، انتساب وزن به بردارهای حمله است. وزنی که به بردارحمله منتسب می گردد میزان مشارکت بردارحمله در سطح حمله است. آخرین مرحله در روش هاوارد، تخمین سطح حمله با اضافه کردن وزن بردارهای حمله برای هر نمونه از بردارحمله، به سطح حمله کلی می باشد.

۴-اندازه گیری سطح حمله در بسترهای J2EE و .NET

به دلیل اهمیت امنیت سیستم های نرم افزاری، لازم است تا هر دو بستر اصلی توسعه سیستم های نرم افزاری با دیدگاه امنیتی به دقت مورد مطالعه قرارگیرند. زیرا رقابت بی پایانی بین J2EE و NET. وجود داشته و دارد. به طوریکه هرکدام از آنها اغلب به صورت کورکورانه ارزشهای طرف دیگر را انکار کرده درحالیکه راه حلهای خود را می ستایند.

به همین منظور در این پژوهش مقایسه کمی امنیت بین این دو بستر با معیار سطح حمله صورت خواهد گرفت. در این خصوص از روش اندازه گیری هاوارد برای بسترهای J2EE و NET. استفاده می شود. البته این مقایسه به سه روش مختلف و با تعیین وزن بردارهای حمله به کمک استاندارد CVSS صورت خواهد گرفت.

مانند روش هاوارد تاریخچه حملات در بسترهای J2EE و NET. براساس اطلاعات پایگاه داده CVE مطالعه شده و مطابق با شکل ۴-۱ منابع سیستم و بردارهای حملات به کمک دانش امنیتی و شناخت این دو بستر استخراج می شوند[7]. در مرحله بعد بر اساس استاندارد CVSS به هرکدام از این بردارهای حمله وزنی متناسب با میزان تاثیرگذاری آن در سیستم به لحاظ امنیتی اختصاص داده می شود. آنگاه تمامی نمونه های موجود متناسب با بردارحمله را مطابق با جداول ۴-۱ و۴-۲ به دست آورده و اندازه سطح حمله محاسبه می شود.

۴-۱-استخراج بردارهای حمله

همانطور که گفته شد اولین مرحله اندازه گیری سطح حمله، شناسایی بردارهای حمله است. روش هاوارد تعریف فرمالی از بردار حمله سیستم ارائه نمی دهد. بنابراین روش سیستماتیکی برای شناسایی بردارهای حمله وجود ندارد. بنابراین همانطورکه گفته شد از تاریخچه حملات روی بسترهای J2EE و NET. برای شناسایی بردارهای حمله استفاده می شود. برای این منظور از بولتن آسیب پذیری های عمومی مانند CVE استفاده می گردد و ویژگیهایی از J2EE و NET. که اغلب در حمله به آنها مورد استفاده بوده اند را استخراج کرده و مطابق شکل ۴-۱ به صورت ۱۰ بردارحمله نشان داده می شوند:

۱. تزریق اسکریپت
۲. افشای اطلاعات
۳. انسداد سرویس
۴. اجرای کد دلخواه
۵. دور زدن محدودیتهای دسترسی
۶. دستکاری فایلها
۷. اجرای دستور دلخواه
۸. اتصال به میزبان دلخواه
۹. دور زدن احراز هویت
۱۰. سرریز بافر

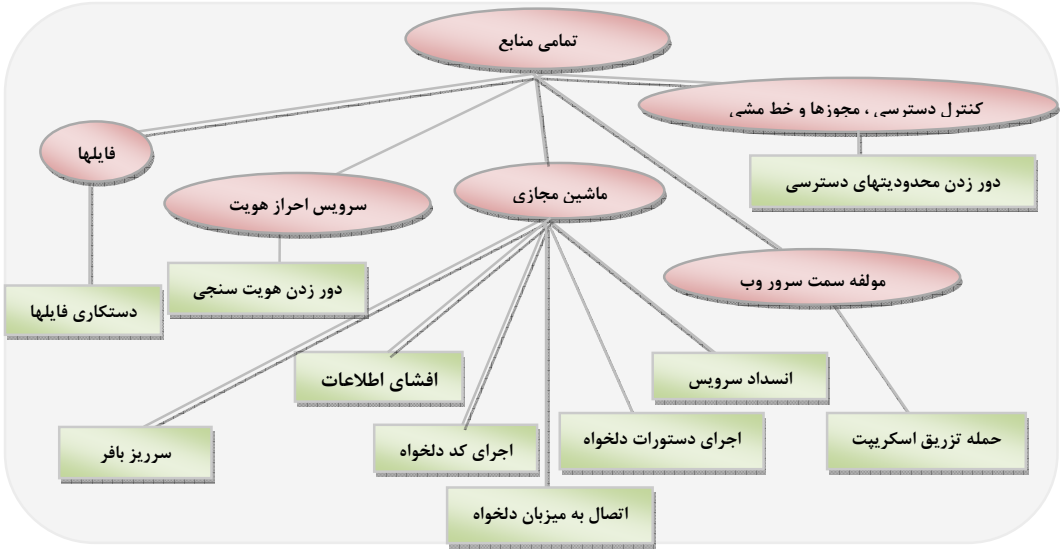
مطابق شکل ۴-۱ منابع سیستم که در حمله مشارکت دارند به صورت بیضی شکل نمایش داده می شوند. سپس حملاتی که روی این منابع اتفاق می افتند به صورت بردارهای حملات دسته بندی کرده و درون جعبه های مستطیل شکل قرار می گیرند.

به دلیل اینکه برخی از این بردارهای حملات در شرایط مختلف، سطوح متفاوتی از آسیب پذیری را ایجاد می کنند لذا دسته بندی دیگری نیز برای آنها تعریف شده است. که با مقیاس زیاد[5] (H) ، متوسط[6] (M) و کم[7] (L) مشخص می گردند. این دسته بندی براساس مقدار وزن بردارهای حمله و تعریف آن در استاندارد CVSS به دست آمده است. به طوریکه مقدار وزن (۳،۹-۰) نشان دهنده درجه آسیب پذیری کم ، (۶،۹-۴) درجه آسیب پذیری متوسط و محدوده (۱۰-۷) درجه آسیب پذیری زیاد را نشان می دهد[9].

برای برخی بردارهای حمله در بستر NET. نمونه آسیب پذیری در پایگاه داده CVE وجود نداشت. به همین دلیل درجدول ۴-۱ مشاهده نمی شوند به عبارت دیگر، افشای اطلاعات با درجه بندی L، انسداد سرویس با درجه بندی H، اجرای دستور دلخواه، اتصال به میزبان دلخواه، دورزدن محدودیت دسترسی با درجه بندی Lو M، دستکاری فایلها و در سرریز بافر نمونه آسیب پذیری مشاهده نگردید. در J2EE نیز برای برخی آسیب پذیریها، شامل

[5] High
[6] Medium
[7] Low

انسداد سرویس با درجه بندی L و دور زدن احراز هویت بردار حمله ای شناسایی نشد.



شکل ۴-۱- نمایش بردارهای حملات بدست آمده پس از تحلیل آسیب پذیریها در بسترهای J2EE و.NET.

بردار حمله		وزن	آسیب پذیری				
افشای اطلاعات	L	۲.۱	CVE-2008-4747				
	M	۵.۰	CVE-2009-3880 CVE-2009-3884	CVE-2009-2690 CVE-2008-5356	CVE-2006-6737	CVE-2006-6009	CVE-2002-0941
	H	۷.۸	CVE-2009-3881	CVE-2003-1123			
انسداد سرویس	M	۵.۰	CVE-2009-3885 CVE-2009-3877 CVE-2009-3876	CVE-2009-2720 CVE-2009-1100 CVE-2009-1093	CVE-2009-3868 CVE-2008-1194 CVE-2007-0012	CVE-2004-1503 CVE-2004-2540 CVE-2004-0651	CVE-2003-1301 CVE-2002-2072
	H	۷.۸	CVE-2009-5349 CVE-2008-0628	CVE-2008-5348 CVE-2008-3105	CVE-2008-5350 CVE-2007-3698	CVE-2006-2426 CVE-2005-3583	CVE-2002-1292
اجرای کد دلخواه	M	۶.۸	CVE-2008-1187				
	H	۹.۳	CVE-2009-3874 CVE-2009-3871 CVE-2009-3869 CVE-2009-3867	CVE-2009-1672 CVE-2009-1671 CVE-2008-1195 CVE-2008-5359	CVE-2008-5358 CVE-2008-5357 CVE-2008-5355 CVE-2008-5354	CVE-2008-1185 CVE-2008-1193 CVE-2008-1186	CVE-2007-3716 CVE-2007-5689 CVE-2006-6731
دور زدن محدودیت دسترسی	L	۴.۰	CVE-2006-0617	CVE-2006-0616	CVE-2006-0615		
	M	۶.۸	CVE-2009-1102 CVE-2008-5360	CVE-2007-3922 CVE-2007-0243	CVE-2006-6736	CVE-2006-0614	CVE-2002-0058
	H	۱۰	CVE-2009-1098 CVE-2009-1094 CVE-2009-3873 CVE-2009-3872	CVE-2008-5352 CVE-2008-5353 CVE-2008-5347 CVE-2008-3107	CVE-2008-3108 CVE-2008-0657 CVE-2007-4381 CVE-2006-6745	CVE-2005-3907 CVE-2005-3906 CVE-2005-3905	CVE-2004-2764 CVE-2003-0111 CVE-2002-2764
دستکاری فایل‌ها	M	۵.۰	CVE-2005-0471	CVE-2003-1156	CVE-2000-0162		
	H	۷.۵	CVE-2008-3109	CVE-2003-0896	CVE-2002-0076	CVE-2002-0866	CVE-2001-1480
اجرای دستورات دلخواه		۹.۳	CVE-1999-0766				
اتصال به میزبان دلخواه		۷.۵	CVE-2009-2673 CVE-2008-5345	CVE-2000-0327	CVE-1999-0141	CVE-1999-0142	CVE-1999-0440
سرریز بافر		۷.۵	CVE-2009-1099	CVE-2009-1097	CVE-2009-1096	CVE-2009-1095	

جدول 4-1- آسیب پذیریهای موجود در بستر .NET. براساس پایگاه داده CVE

بردار حمله		وزن	آسیب پذیری			
تزریق اسکریپت		۴,۳	CVE-2008-3842 CVE-2008-3843	CVE-2008-3422 CVE-2007-4433	CVE-2006-7192 CVE-2006-3436	CVE-2005-0452 CVE-2003-0768
افشای اطلاعات	M	۵,۰	CVE-2006-6104	CVE-2006-1300	CVE-2002-0409	
	H	۷,۸	CVE-2007-0042	CVE-2005-1664		
انسداد سرویس	L	۲,۶	CVE-2009-1536			
	M	۵,۰	CVE-2005-2224	CVE-2005-1665		
اجرای کد دلخواه	M	۶,۸	CVE-2006-1511			
	H	۹,۳	CVE-2009-2504 CVE-2009-2497	CVE-2009-0091 CVE-2009-0090	CVE-2008-3852 CVE-2007-0041	CVE-2007-0043 CVE-2002-0369
دور زدن محدودیت دسترسی		۱۰	CVE-2008-5100			
دورزدن احراز هویت		۷,۵	CVE-2004-0847			

۴-۲-اندازه گیری سطح حمله

مرحله سوم، تخمین اندازه سطح حمله می باشد. اکنون با داشتن بردارهای حملات، وزن آنها و داشتن آسیب پذیریهای متناظر، مطابق جداول ۴-۱ و ۴-۲ می توان اندازه سطح حمله را به دست آورد. برای این منظوربه سه روش اندازه گیری صورت می گیرد :

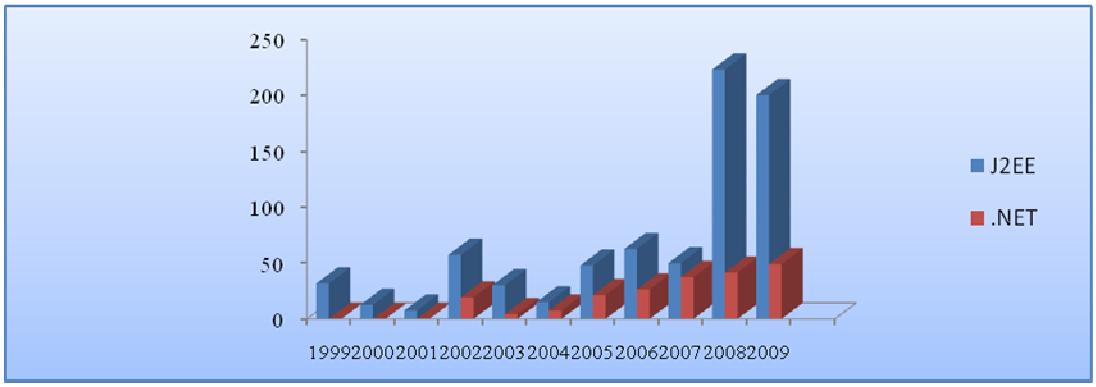
روش اول : اندازه گیری سطح حمله در سالهای متوالی

در این روش مطابق جدول ۴-۳ نمونه بردارهای حملات درسالهای مختلف از اولین زمان انتشار آسیب پذیریها توسط CVE برای هرکدام از بسترها تا پایان سال ۲۰۰۹ به دست می‌آید. اولین آسیب پذیری در J2EE در سال ۱۹۹۹ و NET. در سال ۲۰۰۲ منتشر گردیده است. آنگاه اندازه سطح حمله در آن سال متناسب با وزن محاسبه شده، در انتهای هر ستون به صورت مجموع منابع مشارکت کننده در حمله تعیین می گردد.

در نتیجه در هر سال سطوح حمله به صورت جداگانه برای هر دو بستر محاسبه شده اند. نتیجه این محاسبات به صورت نمودار ۴- ۱ نشان داده شده است.

جدول ۴-3- تعداد بردارهای حملات در سالهای مختلف در بسترهای J2EE وNET.

بردار حمله		وزن	۱۹۹۹		۲۰۰۰		۲۰۰۱		۲۰۰۲		۲۰۰۳		۲۰۰۴		۲۰۰۵		۲۰۰۶		۲۰۰۷		۲۰۰۸		۲۰۰۹	
			J	N	J	N	J	N	J	N	J	N	J	N	J	N	J	N	J	N	J	N	J	N	J	N
تزریق اسکریپت	M	۴,۳										1				2		2		1		3		2		
افشای اطلاعات	L	۲,۱																			۱					
	M	۵,۰							1	1							۲	2			۱		3			
	H	۷,۸							1						۱				1		۱		۱			
انسداد سرویس	L	۲,۶																								1
	M	۵,۰							1	۱	1		3		1	2					۱		۷			
	H	۷,۸							۱		1				1		۱	1	۱		۵					
اجرای کد دلخواه	M	۶,۸															۱				۱					
	H	۹,۳							1								۱		۲	2	۹	2	6	۵		
دور زدن محدودیت دسترسی	L	۴,۰															۳									
	M	۶,۸							۱								۲		۲		۱		۱			
	H	۱۰							۱		1		1		۳		۱		۱		۶	۱	۴			
دستکاری فایلها	M	۵,۰			۱						1				۱											
	H	۷,۵					۱		۲		۱										۱					
اجرای دستور دلخواه		۹,۳	1																							
اتصال به میزبان دلخواه		۷,۵	۳		1																۱		۱			
دورزدن احراز هویت		۷,۵											۱													
سرریز بافر		۷,۵																					۴			
سطح حمله			۳۱,۸	۰	۱۲,۶	۰	۰	۰	۱۹,۳	۵۷,۴	۳۰,۲	۴,۳	۱۵	۷,۵	۴۷,۹	۲۱,۴	۶۲,۷	۲۶,۴	۵۰	۳۷,۵	۲۳۳,۴	۴۱,۵	۲۰۰,۵	۴۹,۱		



نمودار ۴-۱- اندازه سطح حمله در سالهای متوالی دربسترهای J2EE و NET.

همانطورکه در نمودار ۴-۱ مشاهده می گردد، به دلیل اینکه NET. اولین بار در سال ۲۰۰۲ منتشر گردیده است امکان مقایسه بین بسترها قبل از آن وجود ندارد. بنابراین اولین مقایسه بین بسترها در سال ۲۰۰۲ امکان پذیر می باشد، که مطابق نمودار در این سال NET. سطح حمله کمتری نسبت به J2EE دارد. در J2EE کمترین اندازه سطح حمله مربوط به سال ۲۰۰۱ و بیشترین آن مربوط به سال ۲۰۰۸ می باشد. همچنین در بستر NET. کمترین و بیشترین اندازه سطح حمله به ترتیب مربوط به سالهای ۲۰۰۳ و ۲۰۰۹ می باشند. با گذشت زمان تقریبا در بستر NET. با افزایش سطح حمله مواجه هستیم. در حالیکه در بستر J2EE نوسان سطح حمله مشاهده می گردد. با اینحال اندازه سطح حمله تقریبا در تمامی سالها در بستر J2EE به طور قابل ملاحظه ایی از بستر NET. بیشتر است.

روش دوم : اندازه‌گیری سطح حمله با توجه به تغییرات نسخه در دو بستر

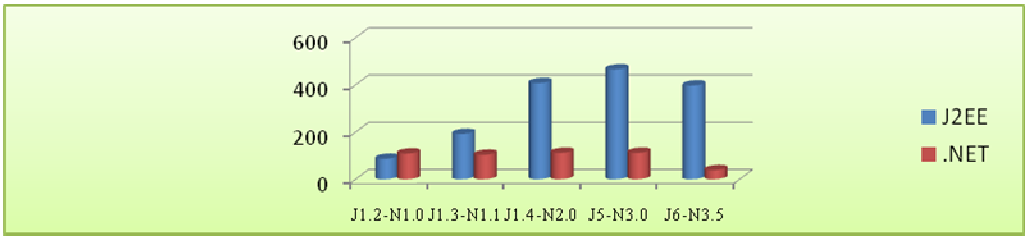
در این روش پنج نسخه مختلف از J2EE متناظر با نسخه محیط زمان اجرای J2EE (JRE) شامل JRE1.2 ، JRE1.3 ، JRE1.4 ، JRE5 و JRE6 در نظر گرفته می شوند[10] . آنگاه مطابق با جدول ۴- ۴ نمونه حملات متناظر با هر بردار حمله برای پنج نسخه مختلف J2EE با استفاده از پایگاه داده CVE به دست می آیند و در انتها سطح حمله محاسبه شده و در انتهای هر ستون برای هر نسخه درج می شود. به همین روش پنج نسخه مختلف از NET. متناظر با نسخه چارچوب NET. شامل NET1.0 ،NET1.1 ،NET2.0 ،NET3.0 و NET3.5. در نظرگرفته می شوند[11]. آنگاه مطابق با جدول ۴- ۵ نمونه حملات متناظر با هر بردار حمله برای پنج نسخه مختلف NET. با استفاده از پایگاه داده CVE به دست می آیند و اندازه سطح حمله محاسبه می گردد. آنگاه مطابق با نمودار ۴- ۲ مقایسه‌ای بین نسخه های نزدیک به هم صورت می گیرد. برای نمایش J2EE در نمودار از کارکتر"J" و برای NET. ازکارکتر "N" استفاده شده است. همچنین شماره نسخه ها در کنار هر علامت به صورت J1.2-N1.0 ، J1.3-N1.1 ، J1.4-N2.0 ، J5-N3.0 و J6-N3.5 مشخص می باشند.

جدول ۴-۴- تعداد بردارهای حملات نسخه های مختلف J2EE

بردارحمله		وزن	JRE۱،۲	JRE۱،۳	JRE۱،۴	JRE۵	JRE۶
افشای اطلاعات	L	۲،۱			۱	۱	۱
	M	۵،۰		۱	۳	۵	۳
	H	۷۸			۱	۱	۱
انسداد سرویس	M	۵،۰	۲	۶	۸	۷	۷
	H	۷،۸			۴	۶	۶
اجرای کد دلخواه	M	۶،۸			۱	۱	۱
	H	۹،۳		۴	۱۳	۱۳	۱۴
دور زدن محدودیتهای دسترسی	L	۴،۰			۱	۳	
	M	۶،۸	۱	۴	۵	۵	۳
	H	۱۰	۱	۷	۱۲	۱۳	۸
دستکاری فایلها	M	۵،۰	۱		۲		
	H	۷،۵	۲	۲	۱		۱
اجرای دستور دلخواه		۹،۳	۱				
اتصال به میزبان دلخواه		۷،۵	۴	۱	۱	۲	۲
سرریز بافر		۷،۵				۴	۴
اندازه سطح حمله			۸۶،۲	۱۹۱،۹	۴۰۷	۴۶۵،۴	۳۹۶،۶

جدول ۴-۵- تعداد بردارهای حملات نسخه های مختلف .NET.

بردارحمله		وزن	.NET ۱،۰	.NET ۱،۱	.NET۲،۰	.NET۳،۰	.NET۳،۵
تزریق اسکریپت		۴،۳	۵	۶	۶	۶	۴
افشای اطلاعات	M	۵،۰	۲		۲	۲	
	H	۷،۸	۲	۲	۱	۱	
انسداد سرویس	L	۲،۶			۱	۱	۱
	M	۵،۰	۲	۲			
اجرای کد دلخواه	M	۶،۸	۱	۱			
	H	۹،۳	۴	۴	۶	۶	۲
دور زدن محدودیتهای دسترسی	H	۱۰			۱	۱	
دور زدن احراز هویت		۷،۵	۱	۱			
اندازه سطح حمله			۱۰۸،۶	۱۰۲،۹	۱۱۱،۵	۱۱۱،۵	۳۷،۹



نمودار ۴-۲- مقایسه سطح حمله در نسخه های مختلف J2EE و .NET.

همانطور که در نمودار ۴-۲ مشاهده می گردد، در هر دو بستر با نوسان سطح حمله در نسخه های مختلف مواجه هستیم به طوریکه نمی توان ادعا کرد که با افزایش نسخه، کاهش سطح حمله اتفاق افتاده است. با اینحال در هر دو بستر در اخرین نسخه با کاهش سطح حمله مواجه هستیم . البته در .NET. آخرین نسخه یعنی نسخه ۳،۵ کمترین سطح حمله را در بین تمامی نسخه هایش دارد در حالیکه در J2EE این کاهش سطح حمله نسبت به نسخه قبلی یعنی نسخه ۵ می باشد.

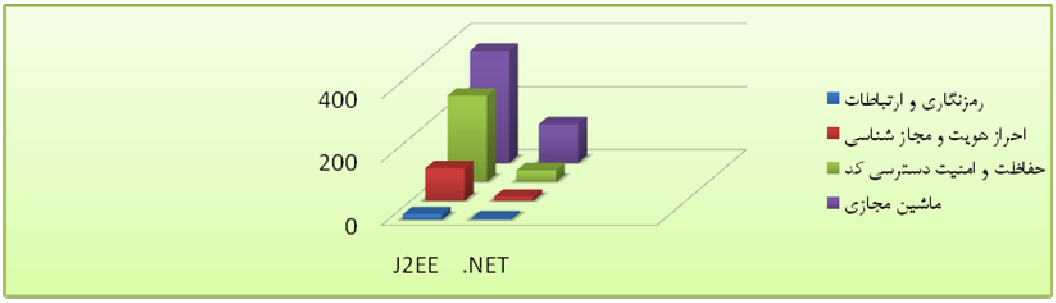
درحالت کلی بین نسخه های نزدیک به هم در دو بستر اختلاف سطح حمله قابل ملاحظه‌ایی مشاهده می گردد به طوریکه تقریبا در اغلب حالات سطح حمله در J2EE بیشتر از .NET. می باشد.

روش سوم : اندازه گیری سطح حمله پذیری مکانیزمهای امنیتی

در این روش آسیب پذیریهای مرتبط با هر کدام از مکانیزمهای رمزنگاری و ارتباطات ، احراز هویت و مجاز شناسی ، حفاظت و امنیت دسترسی کد و همچنین ماشین مجازی در دو بستر مطابق جدول ۴-۶ استخراج شده و سطح حمله محاسبه می گردد که نتایج آن مطابق نمودار ۴-۳ نشان داده شده است .

جدول ۴-۶- آسیب پذیریهای مرتبط با مکانیزمهای امنیتی در بسترهای J2EE و .NET.

مکانیزم	.NET	J2EE
رمزنگاری و ارتباطات	CVE-2005-1665	CVE-2007-3698, CVE-2007-3716
احراز هویت و مجازشناسی	CVE-2006-1300 CVE-2004-0847	CVE-2002-2072 ,CVE-2008-5348, CVE-2008-3105 CVE-2008-1195, CVE-2008-1185, CVE-2008-1193, CVE-2008-1186, CVE-2009-2673, CVE-2008-5345 CVE-2000-0327, CVE-1999-0142 CVE-1999-0440 , CVE-1999-0141
حفاظت و امنیت دسترسی کد	CVE-2006-6104 CVE-2007-0042 CVE-2005-1664 CVE-2008-5100 CVE-2008-3422 CVE-2007-4433	CVE-2009-3880, CVE-2008-5356, CVE-2008-5341, CVE-2006-6009, CVE-2009-3884,CVE-2003-1123 ,CVE-2007-0012, CVE-2004-2540, CVE-2009-1102, CVE-2008-5360, CVE-2007-0243, CVE-2006-6736, CVE-2006-0614, CVE-2008-5350, CVE-2006-2426, CVE-2005-3583, CVE-2007-5689 CVE-2007-4381, CVE-2009-1094, CVE-2009-3873, CVE-2009-3872, CVE-2008-5353, CVE-2008-3107, CVE-2008-0657, CVE-2006-6745, CVE-2005-3907, CVE-2005-3906, CVE-2005-3905, CVE-2004-2764,CVE-1999-0766,CVE-2006-0616, CVE-2006-0617, CVE-2006-0615,CVE-2008-3109, CVE-2003-0896 , CVE-2002-0076
ماشین مجازی	CVE-2005-2224 CVE-2007 0041 CVE-2002-0409 CVE-2006-1511 CVE-2009-2504 CVE-2009-2497 CVE-2009-0090 CVE-2009-0091 CVE-2007-0043 CVE-2007-0043 CVE-2007-0041 CVE-2002-0369 CVE-2009-1536 CVE-2008-3842 CVE-2008-3843 CVE-2006-7192 CVE-2006-3436 CVE-2005-0452 CVE-2003-0768	CVE-2000-0162, CVE-2002-0866, CVE-2006-6737, CVE-2002-0941, CVE-2009-2690,CVE-2009-3881, CVE-2009-3877, CVE-2009-3876, CVE-2009-1100, CVE-2009-1093, CVE-2009-3868 , CVE-2008-1194 , CVE-2004-1503 , CVE-2004-0651 , CVE-2003-1301 , CVE-2009-2720, CVE-2008-1187, CVE-2008-5357 , CVE-2008-5355 , CVE-2008-5354 , CVE-2006-6731 CVE-2009-3874 , CVE-2009-38771, CVE-2009-3869 , CVE-2009-3867 , CVE-2009-167 CVE-2009-38712 , CVE-2009-1671 , CVE-2008-5359 , CVE-2008-5358, CVE-2007-3922, CVE-2002-0058 CVE-2009-1098 , CVE-2008-3108 , CVE-2008-5347 ,CVE-2008-5352, CVE-2003-0111, CVE-2002-2764, CVE-2008-5349, CVE-2008-0628, CVE-2002-1292, CVE-2003-1156, CVE-2005-0471, CVE-2009-1095 , CVE-2009-1096 , CVE-2009-1097 , CVE-2009-1099



نمودار ۴-۳- مقایسه سطح حمله مکانیزمهای امنیتی دربسترهای J2EE و.NET.

همانطور که در نمودار مشاهده می کنید در تمامی حالات سطح حمله پذیری مکانیزمهای امنیتی و ماشین مجازی در بستر J2EE بیشتر از بستر .NET می باشد.

۵- نتیجه گیری کلی و کارهای آتی

در این مقاله مقایسه کمی امنیت با استفاده از معیار سطح حمله در بسترهای J2EE و .NET انجام گرفت. نتایج مقایسات نشان می دهد که با توجه به وجود اختلاف قابل ملاحظه سطح حمله در دو بستر، .NET نسبت به J2EE دارای سطح حمله کمتری می باشد. از عمده ترین دلایل آن، پیچیدگی موجود در بستر J2EE و حفظ طراحی آسیب پذیر قبلی به دلیل سازگاری با نسخه های قدیمی و طراحی قویتر بستر .NET با درس گرفتن از مشکلات قبلی بسترJ2EE می باشد.

البته باید اشاره کرد با توجه به اینکه در عمل تنها بخشی از محیط توسعه بکارگرفته می شود تعیین سطح حمله موثر وابسته به نوع کاربرد می باشد، علاوه بر این مورد روش اندازه گیری سطح حمله کمبودهای نیز دارد که در زیر به دو مورد از مهمترین آنها اشاره می شود:

- روش اندازه گیری تعریف فرمالی از سطح حمله سیستم و بردارهای حمله ارائه نمی دهد. بنابراین، روش سیستماتیکی برای شناسایی بردارهای حمله وجود ندارد.
- استخراج بردارهای حمله براساس سابقه حملات روی این دو بستر به دست آمده اند و فرآیند شناسایی به صورت دستی صورت گرفته است بنابراین نمی توان از شناسایی تمامی بردارهای حمله اطمینان حاصل نمود.

همان طورکه قبلا بیان شد در روش غیر فرمال، نیاز به دانش تخصصی نسبت به سیستم های قابل مقایسه می باشد که در روش فرمال به این دانش تخصصی نیازی وجود ندارد. از مهم ترین دلایل انتخاب روش غیر فرمال، وجود این تجربه و دانش نسبت به بسترهای نرم افزاری J2EE و .NET و عدم دسترسی به کد منبع این بسترهای نرم افزاری بوده است.

در ادامه پژوهش راهکارهای زیر برای بهبود روش پیشنهادی و نتایج حاصل از آن ارائه می شوند:

الف- تعیین خودکار بردارهای حمله با تحلیل آسیب پذیری ها (در سطح کد منبع یا تعامل بین مولفه ها)

ب- تعیین وزن دهی با معیار مناسب تر و با توجه به میزان بکارگیری مولفه ها

ج- بررسی امکان بکارگیری روش فرمال بدون دسترسی به کد منبع برای افزایش قابلیت اطمینان به نتایج

مراجع

[1] Michael Howard. **"Fending off future attacks by reducing attack surface"**, http://msdn.microsoft.com/library/default.asp?url=/library/en us/dncode/html/secure02132003.asp, 2003. 2.1, 7.1.

[2] M. **Howard**, J. Pincus, and J. M.Wing, "**Measuring Relative Attack Surfaces**," Proceedings of Workshop on Advanced Developments in Software and Systems Security, Taipei, December 2003.

[3] J. Alves-Foss and S. Barbosa. "**Assessing computer security vulnerability"**. ACM SIGOPS Operating Systems Review, 29(3):3–13, 1995. 7.2.

[4] P. K. Manadhata, J. M. وینگ, M.Flynn and M.McQueen, **"Measuring the attack surfaces of two FTP daemons" ,** Proceedings of the 2nd ACM workshop on Quality of protection**,** 2006.

[5] Pratyusa K. Manadhata, Yuecel Karabulut, and Jeannette M. وینگ, **"Measuring the Attack Surfaces of Enterprise Software"**, International Symposium on Engineering Secure Software and Systems, Leuven, Belgium, February 2009.

[6] P. K. Manadhata and J. M. وینگ, "**An Attack Surface Metric**," CMU School of Computer Science Technical Report CMU-CS-08-152, July 2008.

[7] MITRE, "**Common Vulnerabilities and Exposures**," http://www.cve.mitre.org/, visited December 2009.

[8] NVD Vulnerability Severity Ratings "**National Vulnerability Database Search Vulnerabilities** , " http://nvd.nist.gov/cvss.cfm? , visited 2009.

[9] Mell, P.,Scarfon ,K.,Romanosky ,S., ***A Complete Guide to the Common Vulnerability Scoring System Version* 2.0** Available at http://www.first.org/cvss/cvss-guide.html, August 2007.

[10] J2EE Runtime Enviroment, www.sun.org, visited January 2010.

[11] .NET Framework, www.microsoft.com, visited January 2010.