بهبود انتخاب سرویس وب با استفاده از کیفیت حفاظت فازی

مرحله 1: برای تعیین درجه رضایت از هر یک از ملزومات امنیت سرویس وب، همه زنجیره های اشتتقاق ممکن آغاز شده از Q1 و ختم شده به Qn باید اشتقاق شود.

مرحله 2: گره در این دومین لایه به صورت STRIDE. تثبیت می شود. مقدار وزنی هر یک قاعده با ارزیابی سابقه قانون توسط متخصصان انسانی محاسبه می شود که نخست مقادیر ورودی را به مقادیر عضویت فازی با استفاده از توابع عضویت ورودی و سپس اعمال اپراتور به این مقادیر عضویت تبدیل می کند.

مرحله 3: در این لایه گره نام گذاری شده تابع زیگما برای نرمال سازی قدرت تهدید ورودی استفاده می شود.

مرحله 4: این مرحله که موسوم به V min {f(x)} است خروجی کل را به صورت مجموع همه ورودی ها برای مدل دو سویه برای هر تهدید تعریف شده در امنیت وب سرویس محاسبه می کند.

جدول 1: معیار های QoP مورد استفاده برای ارزیابی وب سرویس

شماره sl	پارامتر	دارایی	تهدید	توصیف	اندازه گیری
1	اسکن Wsdl	جمع آوری اطلاعات	افشای اطلاعات	این به توصیف کارکرد وب سرویس و پارامتر های مورد نیاز برای استفاده از آن می پردازد.	رتبه بندی

2	شمارش روش وب	جمع آوری اطلاعات	افشای اطلاعات	همه روش های اجرا شده را نمی توان در WSDL منتشر کرد.	رتبه بندی
3	نشت اطلاعات پیام خطا	جمع آوری اطلاعات	افشای اطلاعات	پیام های خطا درون SOAP که حاوی اطلاعات مفصل پلتفرم و اطلاعات اجرایی نظیر قطعات کد می باشد.	رتبه بندی
4	مقادیر عددی	فازینگ	افشای اطلاعات	هر مقداری که به صورت عددی است و یا انتظار می رود عددی باشد	رتبه بندی
5	مقادیر کد گذاری شده Base64	فازینگ	دستکاری	Base64 برای کدگذاری داده های دودویی به	رتبه بندی

				منظور مطابقت با خصوصیات XML استفاده می شود.	
6	رشته های کاراکتر	فازینگ	دستکاری	این مقوله کلی اشاره به رهنمود های عمومی داده هایی دارد که دارای شکل قابل طبقه بندی مناسب نیست.	رتبه بندی
7	مقادیر عمومی	فازینگ	دستکاری	اگر امکان شناسایی ماهیت مقادیر ورودی وجود ندارد این مقوله دیدگاهی کلی در خصوص نوع ورودی های تست شده می دهد.	رتبه بندی

8	پارامتر زیر سیستم	فازینگ	کلاهبرداری	این مقوله مربوط به هر مقداری است که بر خروجی در طرف مشتری تاثیر می گذارد.	رتبه بندی
9	پارامتر های بررسی	فازینگ	دستکاری	سیستم اغلب از پردازش اطلاعات برای دسترسی به راهنماهای اطلاعات استفاده می کند.	رتبه بندی
10	مقادیر ورودی	فازینگ	دستکاری	هر مقداری که به طور مستقیم به برخی محیط ها وارد می شودپتانسیل اخلال در	رتبه بندی

				ورودی ها را داشته و چشم انداز ناصحیحی را ایجاد می کند.	
11	تزریق Sql	تزریق	کلاهبرداری	هر مقداری که بتواند به صورت بخشی از SQL استفاده شود باید از نظر توانایی تغییر SQL و پردازش آن در جهات خاص تست شود که منجر به افشای اطلاعات می شود.	رتبه بندی
12	تزریق فرمان	تزریق	دستکاری	اگر سیستم داخلی برای	رتبه بندی

				اجرای دستورات فعلی استفاده شود و ورودی این دستورات به طور مناسب ارزشیابی نشوند، امکان اجرای دستورات کاربر وجود دارد	
13	تزریق Lpath	تزریق	کلاهبرداری	اگر سوالات LDAP به طور مستقیم از ورودی کاربر ایجاد شود این موجب خطر زیادی برای سیستم به خصوص در افشای اسرار محرمانه می	رتبه بندی

				شود.	
14	تزریق Xpath	تزریق	افشای اطلاعات	استفاده از ورودی کاربر در جست و جوی XPath می تواند موجب افزایش توانایی اصلاح جست و جو شود.	رتبه بندی
15	تزریق کد	تزریق	افزایش امتیاز	در صورتی که کاربر معتبر با ارزیابی های توع معتبر تامین شود، دستورات بدخیم به طور سهوی توسط وب سرویس اجرا می شوند.	رتبه بندی
16	انتخاب رمز	محرمانه	افشای اطلاعات	انتخاب رمز رمزگشایی بر	رتبه بندی

				قدرت رمزگشایی و توانایی مهاجم برای کرک کردن موفق رمزگشایی و بازیابی داده های متنی تاثیر می گذارد.	
17	پوشش رمزگشایی	محرمانه	افشای اطلاعات	رمزگشایی باید به کل پورت های حساس پیام ها برای اطمینان از حفاظت آن ها در برابر استراق سمع غیر مجاز اعمال شود.	رتبه بندی
18	حملات پاسخ	یکپارچگی	کلاهبرداری	یک حمله پاسخ شامل استفاده	رتبه بندی

				بدخیمانه از مجموعه پیام های معتبر و یا مجموعه پیام هایی پذیرفته شده توسط وب سرویس	
19	پوشش کنترل یکپارچگی	یکپارچگی	دستکاری	کنترل یکپارچگی باید برای حفاظت داده های مهم در برابر تغییرات غیر مجاز انجام شود.	رتبه بندی
20	Xml غیر معتبر	یکپارچگی	محرومیت از سرویس	امنیت ws و دیگر استاندارد های امنیت وب سرویس مبتنی بر XML بوده و کاربرد آن ها	رتبه بندی

				مستلزم ایجاد XML مناسب و کارکرد ویژه است.	
21	الگوریتم های پشتیبانی نشده	یکپارچگی	دستکاری	تایید این که آیا الگوریتم های پشتیبانی نشده درخواست شده اند و یا ادعای مشتری مبنی بر پشتیبانی مورد نیاز	رتبه بندی
22	تزریق تفکیک کننده	لاگینگ	تضرر	ورودی های لگاریتمی برای تعیین حد و مرز کاراکتر تفکیک کننده	رتبه بندی
23	تزریق فضای سفید	لاگینگ	تضرر	کاراکتر های فضای سفید را می توان برای	رتبه بندی

				اصلاح ظاهر ورودی های لگاریتمی در صورت مشاهده استفاده می شود.	
24	حملات واژه نامه و BruteForce	تصدیق	افزایش امتیاز	این انواع حملات غالبا در برابر سیستم های تایید رمز عبور استفاده شده و برای آزمون مکرر رمز های ورودی بالقوع در برابر سرویس صحت سنجی متکی به توانایی هستند.	رتبه بندی
25	اعتبارنامه های	تصدیق	افزایش امتیاز	اعتبارنامه ها	رتبه بندی

	ایجاد شده			باید توسط یک گروه مجاز صادر شده و در صورت ارایه توسط نرم افزار صحت سنجی شوند.	
26	اعتبار نامه های مفقود	تصدیق	کلاهبرداری	کاربری که قادر به ارایه اعتبار نامه های دست تیست نباید دسترسی داشته باشد و نرم افزار باید در خواست آن ها را رد کند	رتبه بندی
27	جعل رمز	تصدیق	افزایش امتیاز	از آن جا که SOAP یک پروتوکل مبتنی بر پیام بدون حالت است،	رتبه بندی

				برخی از مکانیسم ها بایستی برای تصدیق و صحت سنجی بین درخواست های SOAP و یا حفظ حالت ماموریت اعمال می شود.	
28	حملات ربایش	تصدیق	دستکاری	از آن جا که SOAP یک پروتوکل مبتنی بر پیام بدون حالت است، برخی از مکانیسم ها بایستی برای تصدیق و صحت سنجی بین	رتبه بندی

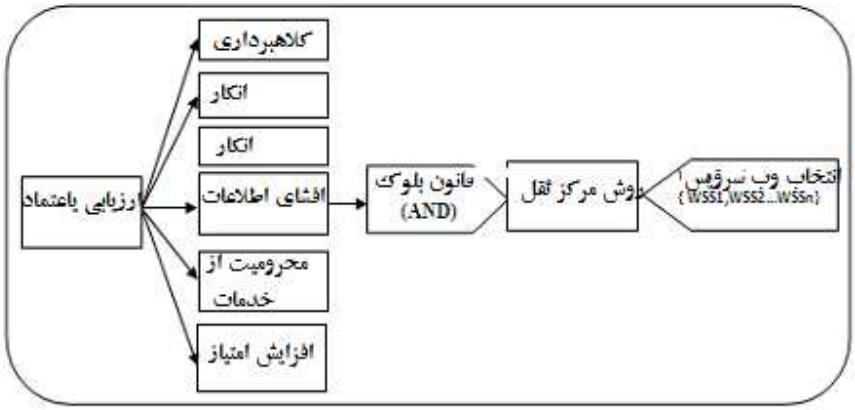
				درخواست های SOAP و یا حفظ حالت ماموریت اعمال می شود.	
29	دستکاری پارامتر	قابلیت دسترسی	محرومیت از سرویس	این دسته گسترده از حملات اشاره به اصلاح پارامتر های درخواست SOAP در حد فاصل بین مشتری و سرور دارند.	رتبه بندی
30	تجزیه اجباری	قابلیت دسترسی	محرومیت از سرویس	تجزیه اجباری نامی است که به دسته ای از حملاتی اطلاق می شود که در بر گیرنده عرضه	رتبه بندی

				درخواست های غیر قانونی و SOAP نامطلوب به وب سرویس به منظور انجام رفتار نامطلوب می باشد.	

5-آسیب پذیری و طبقه بندی وزنی

مجموعه های منطق فازی بر اساس قوانین زبان شناسی می باشند که تخصص تولید کننده را در مدل سازی تهدید لحاظ می کنند. در ذین مدل، روش استنباط ممدانی برای پوشش دادن دانش متخصص به روش بصری و انسانی و برای جمع مقادیر فازی با استفاده از روش مرکز ثقل به منظور غیر فازی سازی استفاده شد. قوانین AND، مقادیر فوق العاده مرتبط با یکدیگر هستند که وابسته به هم می باشند. قواعد OR و ترکیبی از قواعد OR و AND تنها برای متغیر های با ارتباط گسسته استفاده می شوند. تعداد قواعد تحت تصمیم متخصص آشنا به سیستم مورد مدل سازی است. با این حال هیچ متخصصی قابل دسترس نبوده و تعداد وظایف اعضای منتسب به هر کیفیت ورودی به طور تجربی با بررسی داده های ورودی و خروجی مطلوب انتخاب می شود(19). با این حال در مثال ما، مجموعه نسبتا کوچک از قواعد و تنها شش متغیر ورودی و خروجی تغریف می شوند.

شکل 2: سیستم طرح برای کیفیت حفاظت فازی



قواعد فازی: شش ورودی فازی نظیر کلاهبرداری، دستکاری، تضرر(انکار)، افشای اطلاعات، محرومیت از سرویس، افزایش امتیاز و خروجی فازی، نرخ رتبه بندی اعتماد می باشد. قواعد فازی ذیلا برای مدل STRIDE برای تست هر وب سرویس برای ارزیابی خطر اجرا می شوند.

اگر (کلاهبرداری پایین باشد) و (دستکاری پایین باشد) و (تضرر پایین باشد) و (محرومیت از سرویس پایین باشد) و (افزایش امتیاز پایین باشد)، آنگاه (رتبه اعتماد=بسیار پایین خواهد بود).

6- ارزیابی اعتماد

به منظور ارزیابی قدرت رویکردفازی انتخاب شده، مقایسه ای با رویکرد وزنی برای موارد STRIDE که در جدول 1 ارایه شده است انجام شده که در آن عرضه کنندگان خدمات کاربران را با مقادیر اعتماد اشتباه فریب می دهند(20). نخستین گام استفاده از ورودی های STRIDE بوده و فازی سازی در برابر مجموعه های فازی زبانی مناسب برای تعیین درجه تعلق ورودی ها به مجموعه فازی مناسب است. این ورودی یک مقدار عددی است. ورودی های فازی شده برای سابقه اپراتور فازی جهت کسب یک تک عددی اعمال می شوند که نشان دهنده نتایج ارزیابی قبلی هستند.

تابع عضویت هر یک از تهدید های بالقوه را بیان می کند که در نهایت به مقدار عضویت بین [0, 1] برای 5 اصطلاح زبانی نقشه یابی شده و برای هر تهدید به صورت بسیار پایین، نسبتا پایین، نسبتا بالا، بالا و بسیار بالا منتسب می شوند. در نهایت مجموعه فازی ورودی یک خروجی فازی از سیستم استنباط فازی را به خروجی اولیه تبدیل می کند.

بر طبق آسیب پذیر یها و طبقه بندی های فوق الذکر اوزان، مقدار تهدید STRIDE یک آسیب پذیری مطلقی است که برای هر وب سرویس اطلاق می شود. بعد از تعیین مجموع اوزان، سطح تهدید نهایی برای هر وب سرویس حاصل می شود. آنگاه، رتبه کلی با تابع عضویت تعیین می شود. فرمول های خاص نشان دهنده مقدار تهدید امنیت وب سرویس هستند و O(R) مقدار رتبه نهایی تهدید است:

$$\text{Weight (i)} = \sum_{1}^{n} R(i).S$$

$$\begin{aligned}\text{Overall Rating} &= WS(R) \\ &= \min\{ WS1\ldots n * R(S),\ WS1\ldots n * R(T) \\ &\quad ,WS1\ldots n * R(R),\ WS1\ldots n * R(I),\ WS1\ldots n \\ &\quad * R(D),\ WS1\ldots n * R(E) \} \\ &= \min(WS1\ldots n\ \{O(R)\})\end{aligned}$$

6-نتیجه گیری

در این مقاله، ما یک انتخاب سرویس وب و رتبه بندی مبتنی بر QoP را با مدیریت رتبه بندی اعتماد معرفی کردیم. این مقاله یک روش ارزیابی بر اساس مدل STRIDE در امنیت وب سرویس ارایه می دهد که از طریق سطح طبقه بندی تهدید انجام می شود. رویکرد های مبتنی بر فازی در نهایت برای رتبه بندی وب سرویس برای کاربرد های واقع گرایانه تر در نمایش و ارزیابی ملزومات QoP استفاده شده اند.انتخاب مقدار تهدید پایش شده توسط متخصص معتمد یک نکته جالبی است که هنوز ذکر نشده است.