Scientific Journal of Electronical & Cyber Defence
Vol. 10, No. 2, Summer 2022, Serial No. 38

Detection of the Remote Code Execution Attacks Using the PHP Web Application Intrusion Detection System

M. Maqaleh, M. Bagheri*

*Associate Professor, Imam Hossein University, Tehran, Iran

(Received: 08/06/2021, Accepted: 03/10/2021)

ABSTRACT

With the development of web application software, the lack of access to the application layer and web platform features has become the challenge of conventional intrusion detection systems against web-based attacks. The proliferation of PHP server-side languages has led to the creation of unreliable applications and security issues in this language's software. Remote code execution attack is one of the most important web attacks due to allowing remote access to the processor device and executing the operating system shell commands. Modifying the architecture of network layer intrusion detection systems to the application layer and applying a layered detection approach using the detections methods based on the signature and behavior in PHP application software, facilitates the detection of remote code execution attacks. In this research, remote code execution attacks are detected using the layered approach of PHP web application intrusion detection system, with 90.4% and 95% accuracy in the signature and behavior based approaches respectively .

Keywords: Intrusion detection system, web applications, PHP server side language, Remote code execution attack, Layered approach.

* Corresponding Author Email: Muhammad.maghale@gmail.com

نشریه علمی "پدافند الکترونیکی و سایبری"
سال دهم، شماره ۲، تابستان ۱۴۰۱، ص ۸۵-۷۵

علمی-پژوهشی

تشخیص حملات اجرای کد از راه دور با استفاده از سامانه تشخیص نفوذ نرم‌افزار وبی زبان PHP

محمد مقاله[۱]، مسعود باقری[۲*]

۱- دانشجوی کارشناسی ارشد، ۲- استادیار، دانشگاه جامع امام حسین(ع)، تهران، ایران

(دریافت: ۱۴۰۰/۰۳/۱۸، پذیرش: ۱۴۰۰/۱۱/۱۷)

چکیده

با توسعه نرم‌افزارهای تحت وب چالش سامانه‌های تشخیص نفوذ مرسوم در برابر حملات مبتنی بر وب، عدم دسترسی آن‌ها به ویژگی‌های لایه کاربرد و بستر وب است. گسترش استفاده از زبان سمت سرور PHP، باعث تولید برنامه‌های کاربردی به‌صورت نامطمئن و بروز مشکلات امنیتی در نرم‌افزارهای این زبان شده است. حمله اجرای کد از راه دور به دلیل اجازه دسترسی از راه دور به دستگاه پردازنده و اعمال دستورات پوسته سیستم عامل، یکی از حملات پراهمیت تحت وب، به شمار می‌رود. تغییر معماری سامانه‌های تشخیص نفوذ لایه شبکه به لایه کاربرد و به‌کار بردن رویکرد تشخیص لایه‌ای با استفاده از روش‌های تشخیص مبتنی بر امضاء و رفتار در نرم‌افزارهای کاربردی زبان PHP، امکان تشخیص حملات اجرای کد از راه دور را فراهم می‌کند. در این پژوهش با استفاده از رویکرد لایه‌ای سامانه تشخیص نفوذ نرم‌افزار وبی زبان PHP، با دقت ۹۰/۴٪ و ۹۵٪ در رویکرد مبتنی بر امضاء و رفتار، حملات اجرای کد از راه دور تشخیص داده می‌شوند.

کلیدواژه‌ها: سامانه تشخیص نفوذ، نرم‌افزارهای وبی، زبان سمت سرور PHP، حمله اجرای کد از راه دور، رویکرد لایه‌ای

۱- مقدمه

همه روزه بسیاری از نرم‌افزارهای تحت وب مورد حمله مهاجمین قرار می‌گیرند. حملات مذکور امنیت و حریم خصوصی بسیاری از نرم‌افزارهای کاربردی بستر وب را در معرض خطر قرار می‌دهد. زبان سمت سرور PHP به‌عنوان فناوری مورد استفاده در اغلب نرم‌افزارهای تجاری و سازمانی نیازمند ایجاد لایه حفاظتی در مقابله با حملات تحت وب است [۱]. سامانه‌های تشخیص نفوذ مرسوم، از سازوکارهای اصلی در برآوردن امنیت لایه شبکه استاندارد OSI به‌کار می‌روند. طراحی این سامانه‌ها به گونه‌ای است که بر روی لایه شبکه استقرار می‌یابند و تحت پروتکل TCP/IP عمل می‌کنند. با توجه به استفاده نرم‌افزارهای تحت وب از لایه کاربرد و پروتکل انتقال ابرمتن (HTTP)، سامانه‌های تشخیص نفوذ لایه شبکه قادر به مقابله با حملات به نرم‌افزارهای تحت وب نیستند [۲]. سامانه‌های تشخیص نفوذ از رویکردهای مبتنی بر امضاء و رویکرد مبتنی بر رفتار ناهنجار جهت تشخیص نفوذ استفاده می‌کنند [۳]. تغییر معماری سامانه‌های تشخیص نفوذ از لایه شبکه به لایه کاربرد و استفاده از رویکردهای تشخیص این سامانه‌ها در بستر وب امنیت افزون نرم‌افزارهای تحت وب را به همراه دارند. حملات اجرای کد از راه دور یکی از خطرناک‌ترین حملات به نرم‌افزارهای تحت وب محسوب می‌شوند [۳ و ۴]. بنابراین توجه به اهمیت حملات اجرای کد از راه دور در نرم‌افزارهای زبان PHP، امری ضروری محسوب می‌شود [۵].

نرم‌افزارهای کاربردی یکی از راه‌های نفوذ به شبکه سازمان‌ها و مراکز تجاری است. در سال‌های اخیر تحقیقات متعددی در حوزه سامانه‌های تشخیص نفوذ از سوی مراکز دانشگاهی و شرکت‌های امنیتی با هدف مقابله با حملات تحت وب صورت گرفته است. سامانه تشخیص نفوذ نرم‌افزار زبان PHP با استفاده از قلاب‌هایی در مفسر، سعی در کشف نفوذ حملات در زبان PHP دارد [۶]. ارائه روش‌شناسی[۲] برای سامانه‌های تشخیص نفوذ نرم‌افزارهای تحت وب با مقایسه تمام رویکردهای تشخیص حملات وبی، ایجاد پایه محکمی برای کارهای آتی پژوهشگران محسوب می‌شود [۷]. بررسی حملات تزریق دستور سامانه‌عاملی یا همان حملات اجرای کد از راه دور در نرم‌افزارهای وبی به مقابله مؤثر با این حملات کمک می‌کند [۱۱]. استفاده از رویکرد مبتنی بر امضاء جهت مقابله با حملات شناخته شده از مهم‌ترین روش شناسایی نفوذ، به شمار می‌رود [۱۲]. نمونه اقداماتی است که پژوهشگران برای مقابله با حملات اجرای کد از راه دور به نرم‌افزارهای تحت وب زبان PHP و استفاده از رویکرد سامانه‌های تشخیص نفوذ برای مقابله با حملات ارائه نموده‌اند.

* رایانامه نویسنده مسئول: Muhammad.maghale@gmail.com

[1] Methodology

در این تحقیق، سامانه تشخیص نفوذ نرم‌افزار کاربردی به‌عنوان پروژه حفاظت از نرم‌افزارهای تحت وب زبان PHP مطرح می‌شود. این سامانه دفاع از نرم‌افزار کاربردی زبان PHP، علیه حملات طرح شده را بر عهده دارد. رویکرد پیشنهادی این تحقیق PHP-WA-IDS[1] تمرکز بر تشخیص حملات اجرای کد از راه دور به‌صورت حملات اولیه[2] و حملات ثانویه[3] در نرم‌افزارهای زبان PHP دارد. حملات اجرای کد از راه دور با استفاده از رویکرد لایه‌ای در سامانه تشخیص نفوذ PHP-WA-IDS بررسی می‌شوند. در رویکرد لایه‌ای، حملات اولیه اجرای کد از راه دور با استفاده از روش‌های مبتنی بر امضاء به ویژه استخراج قوانین حملات در چارچوب عبارات منظم تشخیص داده می‌شوند. همچنین حملات ثانویه اجرای کد از راه دور با استفاده از روش‌های تشخیص نفوذ به‌صورت رفتاری مانند تشخیص رفتار ناهنجار کاربر و رفتار حمله اجرای کد از راه دور تشخیص داده می‌شوند. ساختار این تحقیق به‌صورت زیر ساماندهی شده است:

در بخش ۱ "مقدمه"، یک نمای کلی از تحقیق و اهداف آن بیان شده است. در بخش ۲ "پیشینه تحقیق"، به بررسی پژوهش‌های مرتبط، در حوزه سامانه‌های تشخیص نفوذ لایه کاربرد و بستر وب پرداخته می‌شود. در بخش ۳ "راهکار پیشنهادی"، طرح پیشنهادی PHP-WA-IDS، جهت مقابله با حملات اجرای کد از راه دور بیان می‌شود. در بخش ۴ "ارزیابی راهکار پیشنهادی"، به ارزیابی روش پیشنهادی در حوزه سامانه تشخیص نفوذ و نتایج آن‌ها پرداخته می‌شود. در بخش ۵ "نتیجه‌گیری"، به بیان نتایج تحقیق پرداخته می‌شود. در بخش ۶ "مراجع"، لیستی از منابع مورد استفاده بیان می‌شود.

۲- پیشینه تحقیق

در رابطه با اهمیت تشخیص نفوذ از طریق حملات به نرم‌افزارهای تحت وب، تحقیقات متعددی انجام شده است که در ادامه به‌صورت مختصر به بیان آن‌ها پرداخته می‌شود.

۲-۱- تشخیص نفوذ ذاتی در برنامه کاربردی PHP با استفاده از ZENIDS

پژوهش ZENIDS به‌طور پویا مسیرهای اجرایی معتبر نرم‌افزارهای کاربردی را در کوتاه مدت یاد می‌گیرد و ناهنجاری‌های بالقوه نفوذ را به‌عنوان خطر گزارش می‌دهد. ZENIDS به‌عنوان یک رابط PHP با پشتیبانی از ۸ قلاب[4] در مفسر زبان PHP اجرایی شده است. ZENIDS مجموعه‌ای از ویژگی‌هایی را یاد می‌گیرد که بازدید کننده نرم‌افزار کاربردی از آن‌ها استفاده کرده است. ZENIDS دارای این ویژگی است که در برابر حملات وبی تزریق XSS[5] و یا تزریق SQL، به خوبی نفوذ را تشخیص می‌دهد [۶].

۲-۲- نگاه دقیق‌تر به سامانه‌های تشخیص نفوذ نرم‌افزارهای تحت وب

پژوهش اگاروال یک روش‌شناسی جدید برای بهبود سامانه‌های تشخیص نفوذ بر پایه وب ارائه می‌دهد. در این پژوهش مرور کلی بر سامانه‌های تشخیص و نفوذی که منحصراً بر روی ترافیک وب، عمل می‌کند، انجام گرفته است. تمرکز این پژوهش بر مشکلات سامانه‌های تشخیص در زمینه نظارت و شناسایی حملات مبتنی بر وب است. در این پژوهش سامانه تشخیص نفوذ پیشنهادی با ویژگی‌های پنج سامانه تشخیص معروف از قبیل، AppSensor، PHPIDS، ModSecurity، Shadow Daemon و AQTRONIX Web Knight مقایسه می‌شود که قدرت و قابلیت‌های اضافی چارچوب پیشنهادی را برجسته می‌کند [۷].

۲-۳- بررسی حملات تزریق دستور سامانه‌عاملی (اجرای کد) بر روی نرم‌افزارهای وبی آسیب‌پذیر

پژوهش محمد الاهمد و همکاران بر روی شناخت حملات تزریق دستور یا همان اجرای کد متمرکز است. این پژوهش حمله تزریق دستور در نرم‌افزارهای وبی را مورد بررسی جامعی قرار می‌دهد. بر طبق گزارشات OWASP حمله تزریق دستور، یکی از مهم‌ترین تهدیدات امنیتی بر روی نرم‌افزارهای کاربردی وبی به شمار می‌آید. در این پژوهش، جزئیات حمله تزریق دستور، گام‌ها و برخی از نمونه‌های این حمله بررسی می‌شوند. از سوی دیگر تأثیر این حمله و راه‌های پیشگیری از این نوع حملات مورد شناسایی قرار می‌گیرند [۱۱].

۲-۴- قابلیت شناسایی سامانه تشخیص مبتنی بر امضاء در زمینه حملات بستر وب

سامانه‌های تشخیص نفوذ مبتنی بر امضاء، نقش حیاتی در امنیت سازمان‌ها ایفاء می‌کنند. سامانه تشخیص مبتنی بر امضاء شامل پایگاه داده‌ای از قوانین تشخیص است، این قوانین برای عملکرد بهینه می‌بایست طبق محیط عمل، متناسب‌سازی شود. در پژوهش جیسوس و همکاران از مجموعه قوانین دارای عملکرد

[1] PHP Web Application Intrusion Detection System
[2] First Order
[3] Second Order
[4] Hook
[5] Cross Site Scripting

بهینه جهت تشخیص حملات بستر وب استفاده می‌شوند. نتایج این پژوهش با سامانه‌های تشخیص Snort، ModSecurity و Nemesida با استفاده از ۷ مجموعه داده، مورد ارزیابی قرار می‌گیرد. نتایج نشان دهنده این است که انتخاب تنظیمات تعیین شده در هر سامانه تشخیص دهنده به قابلیت تشخیص و نرخ هشدار اشتباه آن تأثیر می‌گذارد [۱۲].

به‌صورت کلی در بررسی پژوهش‌های ذکر شده، از نقاط ضعف آن‌ها می‌توان به موارد زیر اشاره کرد:

۱. ضعف تشخیص مؤثر حملات اجرای کد از راه دور: در پروژه PHPIDS ضعف ساختاری برای مقابله با حملات اجرای کد از راه دور وجود دارد. در پژوهش ZENIDS ضعف تشخیص حملات اجرای کد از راه دور به‌صورت شفافی ذکر شده است.

۲. عدم استفاده از رویکرد مبتنی بر رفتار ناهنجار برای تشخیص حملات: در رویکردهای تشخیص نفوذ موارد ذکر شده، استفاده از قوانین تحت رویکرد مبتنی بر امضاء به‌کار گرفته شده است و از رویکرد مبتنی بر رفتار ناهنجار حملات برای تشخیص نفوذ استفاده نشده است.

۳. عدم استفاده از روش‌های تشخیص حملات ثانویه اجرای کد از راه دور: حملات ثانویه اجرای کد از راه دور زمانی رخ می‌دهند که در مرحله اول دسترسی ابتدایی از سامانه گرفته شده باشد و برای تثبیت و قرار دادن درب پشتی از این حملات استفاده می‌شود.

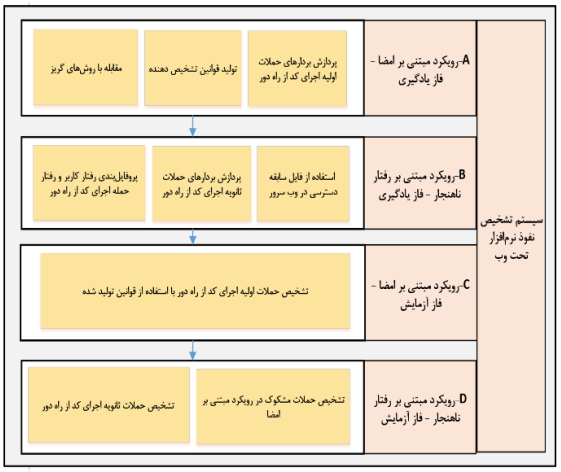
۴. عدم ارزیابی روش‌های ارائه شده جدید در سامانه تشخیص نفوذ نرم‌افزارهای تحت وب: ارائه روش‌شناسی، برای سامانه‌های تشخیص نفوذ نرم‌افزارهای تحت وب نیازمند پیاده‌سازی به‌صورت آزمایشی و استفاده از بردارهای حملات برای ارزیابی دقت تشخیص، نرخ مثبت کاذب، منفی کاذب و منفی صحیح جهت اثر بخشی بهتر است.

۳- ارائه راهکار سامانه‌های تشخیص نفوذ نرم‌افزار تحت وب

براساس آنچه که در پژوهش‌های مطرح شده ارائه شد، ضعف تشخیص حملات اجرای کد از راه دور و عدم استفاده از رویکرد تشخیص مبتنی بر رفتار ناهنجار حمله، مشهود است. اهمیت حملات اجرای کد از راه دور در نرم‌افزارهای کاربردی زبان PHP، لزوم تمرکز بر تشخیص حملات اجرای کد از راه دور به‌صورت حملات اولیه و حملات ثانویه را در رویکرد لایه‌ای سامانه تشخیص نفوذ PHP-WA-IDS ایجاب می‌کند.

۳-۱- مبانی طرح پیشنهادی

چالش اصلی حملات اجرای کد از راه دور استفاده از دو حالت حملات اولیه و ثانویه است. برای تشخیص حملات اجرای کد از راه دور نیاز است که رویکرد تشخیص مبتنی بر امضاء جهت تشخیص حملات اولیه و رویکرد تشخیص مبتنی بر رفتار برای تشخیص حملات ثانویه به‌صورت رویکرد لایه‌ای در نرم‌افزارهای زبان PHP به‌کار گرفته شوند. استفاده هم‌زمان رویکرد لایه‌ای از دو رویکرد مبتنی بر امضاء و رفتار به‌صورت لایه‌های متوالی جهت تشخیص نفوذ، مزایای هر دو رویکرد مبتنی بر امضاء و رفتار را بهبود می‌دهد و معایب هر دو رویکرد را کاهش می‌دهد. استفاده از رویکرد لایه‌ای مسئله حملات ناشناخته و نرخ مثبت کاذب پایین را حل می‌کند. شکل (۱)، معماری پیشنهادی لایه‌ای سامانه تشخیص نفوذ نرم‌افزار تحت وب PHP-WA-IDS را نمایش می‌دهد.



شکل (۱): معماری پیشنهادی لایه‌ای سامانه تشخیص نفوذ نرم‌افزارهای تحت وب PHP-WA-IDS

۳-۲- راه‌کار پیشنهادی

روش‌های مبتنی بر امضاء در رویکرد لایه‌ای PHP-WA-IDS جهت تشخیص حملات اولیه اجرای کد از راه دور با استفاده از عبارات منظم استخراج شده از بردارهای حملات صورت می‌گیرد. عبارات منظم به دلیل پیچیدگی زمانی خطی جهت بررسی بردارهای حملات و جستجوهای رشته‌ای بسیار کاربرد دارند [۱۲]. استفاده از روش‌های مبتنی بر رفتار در رویکرد لایه‌ای

PHP-WA-IDS جهت تشخیص حملات ثانویه اجـرای کـد از راه دور با استفاده از پروفایـل‌هـای رفتـار هنجـار صـورت مـی‌گیـرد. پروفایل‌های استفاده شده در تشخیص مبتنی بر رفتـار بـه رفتـار کاربر و رفتار حمله اجرای کـد از راه دور در نـرم‌افـزار تحـت وب وابسته است.

۳-۲-۱- سامانه تشخیص نفوذ نرم‌افـزار تحـت وب PHP-WA-IDS

مسیر اصلی بهره‌برداری[1] از آسیب‌پـذیری اجـرای کـد از راه دور، ورودی کاربران است. مهاجمین اغلب بردارهای حملات خود را از طریق متد انتقال GET یـا POST از پروتکـل HTTP بـه سـمت نرم‌افزار کاربردی ارسال می‌کنند [۴]. با درخواسـت‌هـای ارسـال شده توسط کاربران، سـامانه تشـخیص نفـوذ PHP-WA-IDS بـه بررسی بردارهای ورودی با استفاده از رویکردهای تشخیص خـود می‌پردازد. در ادامه به بررسی هر یک از لایه‌های رویکـرد لایـه‌ای در سامانه تشخیص نفوذ PHP-WA-IDS بر طبق معماری شـکل (۱)، پرداخته می‌شود.

۳-۲-۲- رویکرد مبتنی بر امضاء (فاز یادگیری)

کلمات رزرو نقش مؤثری در حملات اولیـه اجـرای کـد از راه دور برعهده دارند و به‌عنوان پایگاه داده امضاءها در روش تولید قوانین تحلیل می‌شوند. توابع PHP مورد نیاز حمله اجرای کـد از راه دور در حالت اولیه عبارتند از: shell_exec، exec، passthru، system، backtick operator و eval. این توابع رشته‌های ورودی را به‌عنوان دستورات پوسته سیستم عامل اجرا می‌کنند [۱۵-۱۳]. دستورات سیستم عاملی از جمله دستورات سیستم عامل لینوکس مانند ls، pwd و id و دستورات سیستم عامل ویندوز مانند whoami، dir و ipconfig دستورات پرکاربرد مهاجمین در بردارهای حملات اولیه اجرای کد از راه دور هستند. برای تشخیص حملات اولیه نیاز بـه استفاده از قوانین تولید شده در قالب عبارات مـنظم وجـود دارد. الگوهای توابع اجرای دستور در زبـان PHP و دسـتورات سیسـتم عامل، در تولید قوانین تشخیص دهنده عبارات منظم نقش مهمی را ایفاء می‌کنند.

۳-۲-۲-۱- پیش‌پردازش بردارهای حملات اجـرای کـد از راه دور در حالت اولیه

کلمات رزرو نقش مؤثری در حملات اولیـه اجـرای کـد از راه دور دارند. این کلمات در اغلب توابع اجـرای دسـتور در زبـان PHP و دستورات پوسته سیستم عامل، توجه ویژه‌ای را می‌طلبند. اگر در حملات اجرای کد از راه دور، در بردارهای حمـلات از روش‌هـای مبهم‌ساز[2] و فریب[3] استفاده شود نقش کلمات رزرو و توابع اجرای دسـتور در ایـن بردارهـا پررنـگ خواهـد بـود. از الگـوریتم‌هـای دسته‌بندی برای پیش‌پردازش بردارهای حمله استفاده می‌شود تا قوانین مؤثر در دسته‌هـای مطلـوب بـرای جلـوگیری از حمـلات اسـتخراج شـود. در ایـن مرحلـه از الگـوریتم TF-IDF[4] بـرای پیش‌پردازش بردارهای حمله استفاده می‌شود. این الگوریتم برای تکه‌سازی بردارهای ورودی جهت شکستن به کلمات و عبارات بـا معنی به‌کار می‌رود [۱۶]. با اعمـال الگـوریتم TF-IDF بردارهـای حملات در سه وزن متفاوت دسته‌بندی می‌شوند. ایـن دسـته‌هـا شامل توابع اجرای دستور در زبان PHP، دستورات و کدهای زبان PHP، بردارهای دستورات سیستم عامل و ارزیـابی شـبکه اسـت. بردارهای هر دسته، شباهت وزن کلمه‌ای نسبت به یکدیگر دارند. مثال زیر نمونه‌ای از بردارهای حملات اولیه اجرای کـد از راه دور است.

```
; uname –a // OS and Network Command Category
shell_exec("ls {$_GET['dir']}") // PHP Command Execution Function Category
|| phpinfo() // PHP Code category
```

۳-۲-۲-۲- تولید قوانین تشخیص دهنده حملات

برای تولید عبارات منظم جهت تشـخیص ورودی‌هـای مخـرب از الگوریتم انگرام[5] استفاده مـی‌شـود. از انگـرام در دو حالـت بـرای تشخیص بردار حملات و جلوگیری از بردارهای مبهم‌ساز استفاده می‌شود [۱۷ و ۱۸]. موتور اصلی تشـخیص نفـوذ حمـلات اولیـه اجرای کد از راه دور در روش مبتنی بر امضاء، متشکل از قـوانین تولید شده از الگـوریتم انگـرام اسـت. مراحـل اسـتخراج قـوانین تشخیص دهنده حملات به‌صورت زیر است:

۱. تولید قانون از طریق الگوریتم انگرام، با استفاده از n برابر بـا ۳ تا ۹، بر روی بردارهای حملات اولیه اجرای کـد از راه دور انجـام می‌گیرد. بردارهای حملات اولیه اجرای کـد از راه دور بـه‌صـورت میانگین از حداقل حروف سه‌تایی و حداکثر حـروف نـه‌تـایی بـه دلیل عبارت‌های با معنی در زبان PHP انجام می‌شود.

[1] Exploit

[2] Obfuscation
[3] Evasion
[4] Term Frequency–Inverse Document Frequency
[5] N-Gram

۲. عبارات مکرر از نتایج الگوریتم انگرام محاسبه شده و به‌عنوان الگوهای حملات جهت تشخیص حمله استفاده می‌شوند. از الگوهای مکرر برای انتخاب الگوی بهینه جهت ایجاد عبارات منظم نهایی استفاده می‌شوند.

۳. قوانین تهیه شده با تطبیق الگو مکرر استخراج شده با بردارهای حملات ورودی به‌کار می‌روند. مثال زیر مراحل استخراج قوانین تشخیص دهنده حملات در قالب عبارات منظم را نمایش می‌دهد.

۱. Attack Vector --> <!-- #exec%20cmd="/bin/cat%20/etc/passwd"-->

۲. N-gram Algorithm --> exe ---> ['c', 'c', 'c', 'c', 'c', 'c', 'c', 'c', 'c', 'c', 'c', 'c', 'c', 'c', 'c', 'c', 'c']

۳. Producing Rule (Regular Expression) --> ^(.*?exe.*)$

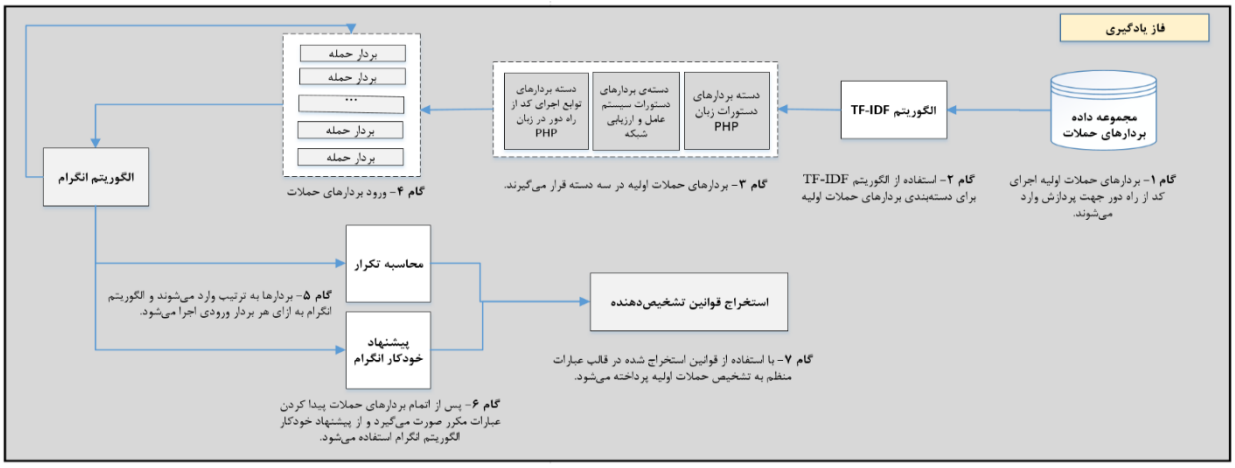
۳-۲-۲-۳- جلوگیری از کاربرد روش‌های گریز در مقابله با حملات

یکی از مشکلات عمده سامانه‌های تشخیص حملات به‌صورت رویکرد مبتنی بر امضاء، دستکاری بردارهای حملات توسط مهاجمین است. تغییرات حاصل از این دستکاری‌ها با استفاده از روش‌های گریز[1] و مبهم‌سازی[2] پدید می‌آید [۱۲]. برای حل این مشکل در سامانه تشخیص نفوذ PHP-WA-IDS از گراف انتقالی[3]، ترکیبات و پروفایل پیش‌گویی الگوریتم انگرام استفاده شده است. با توجه به این مورد که کلمات رزرو به ترتیب در بردارهای حمله قرار می‌گیرند بنابراین هر گونه استفاده از روش‌های گریز و مبهم‌ساز در بین کلمات بردار حمله با استفاده از روش ذکر شده قابل خنثی‌سازی است.

شکل (۲)، با جزئیات کامل نحوه استخراج عبارات منظم از بردارهای حملات اولیه اجرای کد از راه دور در فاز یادگیری را نشان می‌دهد.

۳-۲-۳- رویکرد مبتنی بر رفتار ناهنجار (فاز یادگیری)

سناریوی ورود کاربران جهت بررسی در رویکرد رفتار ناهنجار سامانه تشخیص نفوذ PHP-WA-IDS به دو صورت اجرا می‌شود. در حالت اول، وقتی کاربری بر طبق روش مبتنی بر امضاء مشکوک تشخیص داده شود، آدرس IP وی استخراج شده و وارد رویکرد تشخیص مبتنی بر رفتار ناهنجار برای بررسی‌های بیشتر می‌شود. در حالت دوم، تشخیص مبتنی بر رفتار ناهنجار در حملات اجرای کد از راه دور در حالت ثانویه با تحلیل لاگ دسترسی وبسرور اجرا می‌شود. رویکرد مبتنی بر رفتار از احتمال نفوذ برای بررسی رفتار ناهنجار کاربران و رفتار حمله اجرای کد از راه دور استفاده می‌کند. بنابراین رویکرد مبتنی بر رفتار ناهنجار سامانه تشخیص نفوذ PHP-WA-IDS بر انحراف پروفایل‌های رفتاری از شاخص‌های آماری و رفتار هنجار نظارت می‌کند.



شکل (۲): رویکرد مبتنی بر امضاء در فاز یادگیری سامانه تشخیص نفوذ نرم‌افزار تحت وب PHP-WA-IDS

[1] Evasion
[2] Obfuscation
[3] Transition Graph

۳-۲-۳-۱- ایجاد پروفایل رفتار هنجار

در سامانه تشخیص نفوذ PHP-WA-IDS، برای تشخیص نفوذ مبتنی بر رویکرد ناهنجار از دو پروفایل هنجار استفاده می‌شود. این دو پروفایل بر رفتار هنجار کاربر مورد نظر و رفتار حمله اجرای کد از راه دور در نرم‌افزار کاربردی نظارت دارند. جهت استخراج این دو پروفایل از لاگ وبسرور استفاده می‌شود. خطوط ثبت شده بر روی لاگ وب‌سرور، شامل مجموعه درخواست‌هایی است که به سمت نرم‌افزار کاربردی می‌آید و پاسخ این درخواست‌ها که به سمت کاربران درخواست کننده فرستاده می‌شود [۱۹ و ۲۰]. در سامانه تشخیص نفوذ PHP-WA-IDS در شروع فرآیند تشخیص نفوذ برای هر فرد مشکوک، ابتدا آدرس IP وی استخراج شده و سپس در قسمت رویکرد رفتاری، پروفایل رفتار او با تعیین تعداد روزهای مورد بررسی از لاگ دسترسی وب‌سرور جمع‌آوری می‌شود. نتیجه بررسی بر روی پروفایل جمع‌آوری شده درنهایت به‌صورت احتمال نفوذ بیان می‌شود. پروفایل رفتار کاربر و پروفایل حمله اجرای کد، دارای احتمال مستقل هستند که مجموع شاخص‌های آن‌ها در تعیین این احتمال نقش دارند.

۳-۲-۳-۱-۱- پروفایل رفتار کاربر

پروفایل رفتاری کاربر نسبت به درخواست‌های داده شده فرد به صفحات نرم‌افزار تحت وب، پاسخ‌های دریافت شده از سمت وب‌سرور و موارد مانند آن در تشکیل آن نقش دارند. ساختار پروفایل رفتار کاربر به شرح زیر است:

- **تعیین حد آستانه‌ها برای شاخص‌های رفتار ناهنجار**: تعیین حد آستانه مناسب برای وقوع هشدارهای خوشه‌بندی بر اساس کد حالت[1]، تعیین حد آستانه برای تعداد بازدیدها در هفته، تعیین حد آستانه برای صفحات با قابلیت درخواست POST، تعیین حد آستانه برای صفحات و مسیرهای غیر مجاز و ناهنجار و حد آستانه تصمیم‌گیری نهایی رفتاری در پروفایل رفتار کاربر در فاز یادگیری تعیین می‌شود.
- **تهیه پروفایل صفحات با قابلیت درخواست متد انتقال POST**: صفحاتی که امکان ارسال اطلاعات به آن‌ها از طریق متد POST پروتکل HTTP مجاز است در این پروفایل قرار می‌گیرند.
- **تعیین صفحات و مسیرهای غیر مجاز و ناهنجار**: برخی از صفحات خاص در نرم‌افزار تحت وب تنها توسط مدیران نرم‌افزار کاربردی استفاده می‌شوند، اینگونه صفحات نرم‌افزار اجازه بازدید از سمت افراد عادی را ندارند. این صفحات در فاز یادگیری توسط پروفایل صفحات و مسیرهای غیر مجاز ثبت می‌شوند.

۳-۲-۳-۱-۲- پروفایل رفتار حمله اجرای کد از راه دور

پروفایل حمله اجرای کد از راه دور شامل مؤلفه‌های حمله اجرای کد است که در درخواست‌های مهاجمین وجود دارند. از موارد پروفایل حمله اجرای کد می‌توان به پروفایل چکیده‌ساز، پارامترهای درخواستی صفحات نرم‌افزار و پروفایل صفحات نرم‌افزار تحت وب نام برد. ساختار این پروفایل به شرح زیر است:

- **تهیه پروفایل چکیده از صفحات نرم‌افزار کاربردی**: محتوای صفحات نرم‌افزار تحت وب در ابتدای استقرار سامانه تشخیص نفوذ، بر اساس الگوریتم‌های چکیده‌ساز مورد بررسی قرار می‌گیرند و هش آن‌ها با استفاده از الگوریتم MD5[2] تهیه می‌شوند. هش ایجاد شده به همراه حجم فایل‌های نرم‌افزار تحت وب در این پروفایل قرار می‌گیرند. مثال زیر نمونه‌ای از اعمال این پروفایل است:

```
۱. index.php--
>b9142a5f513a565bcb15430f4982000e
۲. wp-activate.php-->
4d6026066ab2cbd07ff2db603fa30c85
```

- **تهیه پروفایل پارامترهای مورد نیاز صفحات نرم‌افزار کاربردی**: در حالت کلی پارامترهای متد انتقال GET از پروتکل HTTP در صفحات نرم‌افزار کاربردی ثابت هستند. در فاز یادگیری رفتار ناهنجار، تمامی صفحات نرم‌افزار زبان PHP و پارامترهای آن‌ها و ترتیب‌شان در این پروفایل قرار می‌گیرند. مثال زیر نمونه‌ای از اعمال این پروفایل است:

```
۱. /databasepannellogin/phpmyadmin.css.p
nocache=4437063584ltr hp-->
۲. /database/navigation.php-->
ajax_request=1&token=73ba6e5e36f77c
62c52e98c05fc6c7d1
```

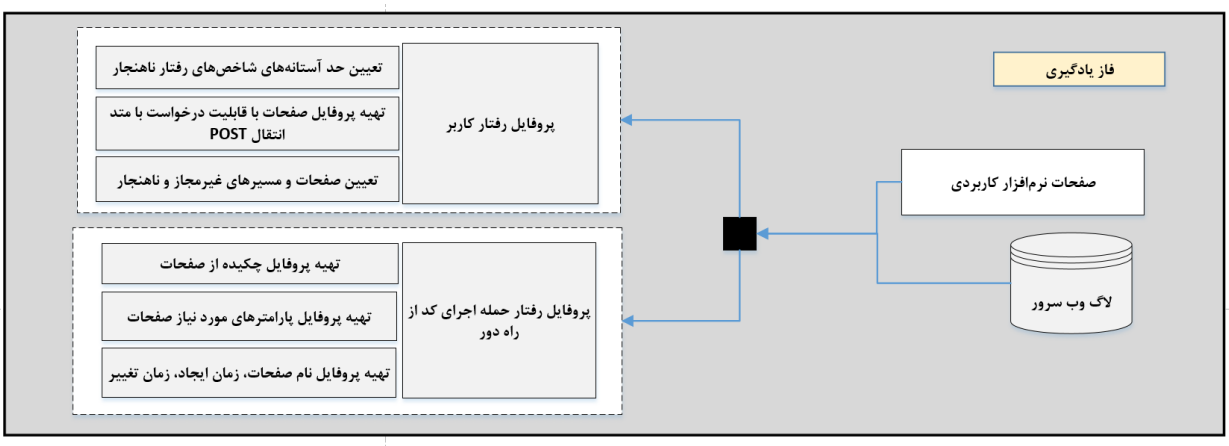
- **تهیه پروفایل نام صفحات نرم‌افزار کاربردی**: نام صفحات نرم‌افزار کاربردی زبان PHP به همراه تاریخ ایجاد و تغییرات آن‌ها که در پروفایل صفحات نرم‌افزار کاربردی قرار می‌گیرند. مثال زیر نمونه‌ای از اعمال این پروفایل است:

[1] Status Code

2. MD5-Message Digest Algorithm

۱. index.php-->Wed Apr 15 20:58:55 2020-->Fri Dec 1 02:41:00 2017
۲. wp-activate.php-->Wed Apr 15 20:59:13 2020-->Tue Sep 3 05:11:05 2019

شکل (۳)، به‌صورت خلاصه فاز یادگیری رویکرد مبتنی بر رفتار ناهنجار در سامانه تشخیص نفوذ PHP-WA-IDS را نمایش می‌دهد.



شکل (۳): نمودار فاز یادگیری رویکرد مبتنی بر رفتار ناهنجار در سامانه تشخیص نفوذ PHP-WA-IDS

۳-۲-۴- رویکرد مبتنی بر امضاء (فاز آزمایش)

پس از استخراج قوانین تشخیص دهنده حملات اجرای کد از راه دور در حالت اولیه، این قوانین به‌صورت آزمایشی بر روی نرم‌افزار کاربردی تحت وب مستقر می‌شوند. استقرار قوانین تولید شده در جهت مقابله با حملات اجرای کد از راه دور در حملات اولیه به‌کار می‌روند. گام‌های زیر به ترتیب با پردازش بردار ورودی نرم‌افزار کاربردی در سامانه تشخیص نفوذ PHP-WA-IDS برداشته می‌شوند.

۱. به ازای هر بردار ورودی، گراف انتقالی با حد آستانه معین جهت جلوگیری از حملات گریز و مبهم‌سازی ساخته می‌شود. با استفاده از ترکیبات سه حرف به بالاتر، بردار ورودی به قطعات کوچک‌تر تبدیل می‌شود.

۲. قطعات ساخته شده بردار ورودی با استفاده از قوانین استخراج شده عبارات منظم جهت تشخیص بردار حمله مورد ارزیابی قرار می‌گیرند.

۳. نتیجه ارزیابی سامانه تشخیص نفوذ مبتنی بر امضاء در سه حالت قرار می‌گیرد. در صورت عادی بودن بردار ورودی، سامانه تشخیص نفوذ آن درخواست را به سمت نرم‌افزار کاربردی می‌فرستد. در مقابل اگر بردار ورودی، بردار حمله تشخیص داده شود این درخواست ثبت و به مدیر سامانه تشخیص نفوذ هشدار حمله داده می‌شود. اگر نتیجه ارزیابی بردار ورودی مشکوک باشد از رویکرد مبتنی بر رفتار ناهنجار برای تشخیص دقیق‌تر در سامانه تشخیص نفوذ PHP-WA-IDS استفاده می‌شود.

۳-۲-۵- رویکرد مبتنی بر رفتار ناهنجار (فاز آزمایش)

در این رویکرد با استفاده از پروفایل رفتار کاربر و پروفایل رفتار حمله اجرای کد از راه دور که در فاز یادگیری آماده‌سازی شده‌اند به تشخیص نفوذ در رویکرد مبتنی بر رفتار ناهنجار سامانه تشخیص نفوذ PHP-WA-IDS پرداخته می‌شود. اگر کاربری بر طبق روش‌های تشخیص مبتنی بر امضاء مشکوک شناخته شود نیازمند بررسی بیشتر با استفاده از روش‌های مبتنی بر رفتار ناهنجار در سامانه تشخیص نفوذ PHP-WA-IDS است.

۳-۲-۵-۱- شناسایی کاربر مهاجم با استفاده از پروفایل رفتار ناهنجار

پروفایل رفتار کاربر شامل شاخص‌های آماری برای بررسی رفتار کاربر در نرم‌افزار کاربردی است که هر یک از شاخص‌ها از احتمال نفوذ برای هشدار دادن رفتار ناهنجار استفاده می‌کنند. در حالت عادی هر شاخص امتیاز صفر به رفتار هنجار می‌دهد. برآیند کلی این پروفایل به‌صورت احتمال نفوذ به ازای کاربر مورد بررسی بیان می‌شود. شاخص‌های مورد استفاده در پروفایل‌بندی رفتار کاربر به شرح زیر هستند:

۱. خوشه‌بندی بر اساس Status code: یکی از موارد مهم در پردازش لاگ وب‌سرور پاسخ‌های پروتکل HTTP به درخواست‌های کاربران است که تحت شماره کدی برگردانده می‌شود [۱۹]. چهار دسته کلی کدهای ۲۰۰ و مشابه، ۳۰۰ و مشابه، ۴۰۰ و مشابه، ۵۰۰ برای سنجش رفتار کاربر در نرم‌افزار تحت وب اهمیت زیادی در بین پاسخ‌های پروتکل HTTP دارند. این چهار دسته کد شامل سایر کدهای شبیه خود در دسته مربوطه هستند و به‌عنوان تعداد خوشه‌ها درنظر گرفته می‌شوند. هدف از خوشه‌بندی با استفاده از الگوریتم K-Mean بدین صورت است که در بازه زمانی تعیین شده، رفتار کاربر مورد بررسی قرار گیرد. در نتیجه نزدیکی کاربر مورد نظر به خوشه‌های پرخطر بررسی می‌شود. خوشه تعداد پاسخ کد[1] دسته ۴۰۰ در بازه زمانی تعیین شده، بدین صورت که کاربران پرخطر همواره تعداد درخواست‌های بالایی از این پاسخ را دریافت می‌کنند. خوشه تعداد پاسخ کد دسته ۵۰۰ در بازه زمانی تعیین شده، بدین صورت که کاربران پرخطر در حین به خطا کشیدن وب‌سرور و نرم‌افزار تحت وب با پاسخ دسته کد ۵۰۰ روبه‌رو می‌شوند.

۲. درخواست‌های متد POST وارد شده به صفحات: در فاز یادگیری سامانه تشخیص نفوذ، مسیرهای متداول نرم‌افزار تحت وب که درخواست POST بر روی آن‌ها اعمال شده، در پروفایلی مشخص می‌شوند. اگر کاربر مورد بررسی به صفحه‌ای که متداول نیست، درخواست POST دهد احتمال حمله به او تعلق می‌گیرد.

۳. خوشه‌بندی بر اساس مسیر و فایل درخواستی: در فاز یادگیری پروفایلی از مسیرها و فایل‌های حساس نرم‌افزار تحت وب تهیه شده است و خوشه‌هایی با مرکزیت این مسیر و فایل‌ها ساخته می‌شود. شباهت و فاصله ورودی کاربر از این خوشه‌ها احتمال حمله درنظر گرفته می‌شود.

۴. تعداد درخواست در هفته به ازای هر آدرس IP: تعداد بازدیدهای کاربر در طی هفته شمارش می‌شود و در صورت انحراف غیر عادی از حد آستانه، احتمال حمله به وی تعلق می‌گیرد.

مجموع تشخیص‌های انجام گرفته شده توسط چهار شاخص رفتار ناهنجار کاربر در سامانه تشخیص نفوذ PHP-WA-IDS، در ضریب‌های درنظر گرفته شده ضرب می‌شود و در صورت بیشتر شدن احتمال برآیند از حد آستانه کلی، هشدار نفوذ برای کاربر صادر می‌شود.

[1] Response Code

۳-۲-۵-۲- تشخیص حملات ثانویه اجرای کد از راه دور

در برخی از حملات بر روی نرم‌افزارهای کاربردی تحت وب، امکان وقوع حمله‌ای متفاوت از اجرای کد از راه دور در حمله اولیه به نرم‌افزار تحت وب وجود دارد. در این حال پس از کسب دسترسی اولیه برای تثبیت دسترسی، قرار دادن درب پشتی و ایجاد وب‌شل از بردارهای حملات ثانویه اجرای کد از راه دور استفاده می‌شود. اهداف مهاجمین از حملات ثانویه اجرای کد از راه دور در به شرح زیر است:

۱. تثبیت دسترسی: مهاجمین با قرار دادن آپلودر فایل در نرم‌افزار تحت وب، تثبیت دسترسی انجام می‌دهند.

۲. قرار دادن درب پشتی: برای تثبیت دسترسی توسط مهاجمین، تغییر کد یکی از صفحات اجرایی نرم‌افزار تحت وب، امکان اجرای دستورات پوسته سیستم‌عاملی با استفاده از پارامترهای فعال‌ساز را فراهم می‌کند.

۳. ایجاد وب‌شل: وب‌شل‌ها عملکردهای بیشتری برای گسترش نفوذ مهاجمین فراهم می‌کنند. این عملکردها شامل ارتباط با پایگاه داده سرور میزبان، مدیریت فایل‌های میزبان و سایر امکانات است.

۳-۲-۵-۲-۱- شناسایی مهاجم با استفاده از پروفایل حمله اجرای کد از راه دور

پروفایل رفتار حمله اجرای کد از راه دور شامل شاخص‌هایی است که هر یک از شاخص‌ها از احتمال نفوذ برای هشدار دادن رفتار حمله اجرای کد از راه دور استفاده می‌کنند. برآیند کلی این پروفایل به‌صورت احتمال بیان می‌شود. اگر احتمال برآیند از حد آستانه تعریف شده در فاز یادگیری بیشتر باشد، رفتار مورد بررسی به‌عنوان رفتار حمله شناسایی می‌شود. شاخص‌های تشخیص نفوذ با استفاده از پروفایل رفتار حمله اجرای کد از راه دور از لاگ وب‌سرور استخراج می‌شود و به شرح زیر است:

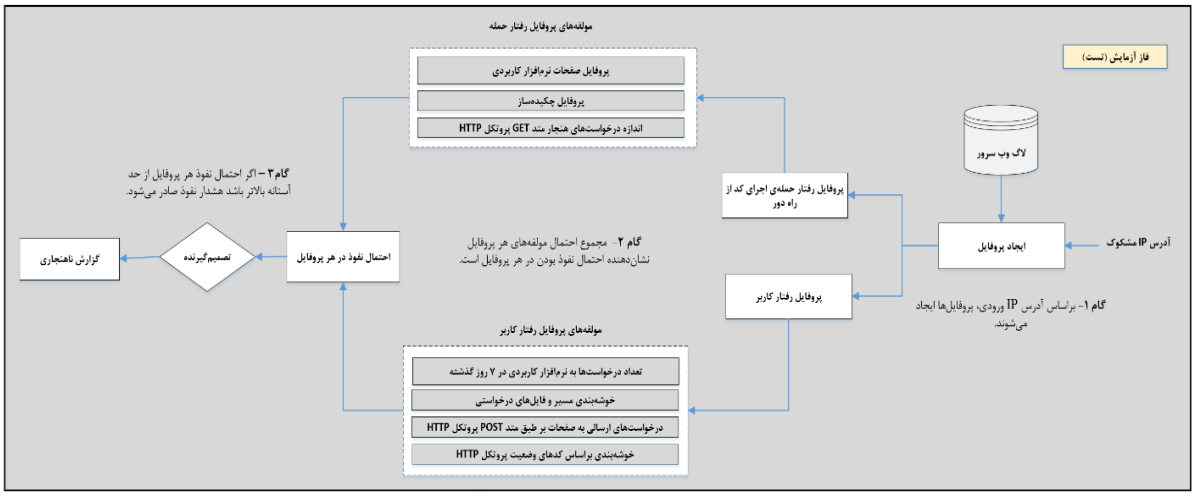
۱. پروفایل چکیده‌ساز: مهاجمین برای قرار دادن آپلودر فایل به‌صورت پنهان ناچار هستند که یکی از صفحات‌های نرم‌افزار کاربردی را تغییر دهند. برای تشخیص تثبیت دسترسی ناشی از حملات ثانویه، کلیه فایل‌های مورد استفاده در نرم‌افزار زبان PHP در فاز آزمایش مورد بررسی قرار می‌گیرند. اگر هش محتوای فایل‌های نرم‌افزار کاربردی با پروفایل چکیده‌ساز فاز یادگیری تفاوتی داشته باشند، هشدار حمله صادر می‌شود.

۲. ترتیب پارامترهای صفحات نرم‌افزار کاربردی: در حالت کلی پارامترهای متد انتقال GET از پروتکل HTTP در صفحات

نرم‌افزار کاربردی ثابت هستند. اگر مهاجمین مسیری را تولید کنند که پارامترهای متفاوتی داشته باشند، این تغییر می‌تواند نشانگر حمله باشد. این شاخص برای تشخیص قرار دادن درب پشتی معیار قابل اطمینانی است، زیرا درب‌های پشتی ناشی از حملات اجرای کد در حالت ثانویه برای اجرا شدن و فعال‌سازی نیاز به پارامترهای فعال‌ساز دارند. تغییر در ترتیب پارامترها یا ایجاد پارامتر جدید در صفحات نرم‌افزار کاربردی توسط پروفایل ترتیب پارمترها، تشخیص داده شده و درنهایت هشدار نفوذ صادر می‌شود.

۳. پروفایل صفحات نرم‌افزار تحت وب: این شاخص با مقایسه فایل‌های خارج از پروفایل تهیه شده صفحات نرم‌افزار در فاز یادگیری، به واکنش در قبال ایجاد فایل‌های جدید می‌پردازد. کلیه فایل‌های ایجاد شده به وسیله مهاجمین از قبیل وب‌شل، آپلودر فایل و فایل‌های دیگر، اگر به‌صورت فایل مجزا در کنار صفحات نرم‌افزار کاربردی قرار گیرند، توسط این پروفایل کشف و هشدار نفوذ صادر می‌شود.

درنهایت شکل (۴)، شمای کامل رویکرد مبتنی بر رفتار سامانه تشخیص نفوذ PHP-WA-IDS را نمایش می‌دهد.



شکل (۴): نمودار فاز آزمایش رویکرد مبتنی بر رفتار ناهنجار در سامانه تشخیص نفوذ PHP-WA-IDS

۴- ارزیابی راهکار پیشنهادی

در این قسمت نتایج حاصل از ارزیابی سامانه‌های تشخیص نفوذ نرم‌افزار تحت وب PHP-WA-IDS بیان می‌شود. همچنین معیارهای ارزیابی جهت اندازه‌گیری عملکرد سامانه تشخیص نفوذ شرح داده می‌شوند. با استفاده از مجموعه داده‌های مورد نیاز به ارزیابی رویکرد لایه‌ای در سامانه تشخیص نفوذ PHP-WA-IDS در مقابله با حملات اولیه و ثانویه اجرای کد از راه دور پرداخته می‌شود.

۴-۱- معیارهای ارزیابی

استفاده از معیارهای ماتریس سردرگمی[1] برای اندازه‌گیری دقت سامانه تشخیص نفوذ پیشنهادی به‌کار می‌رود.

با توجه به جدول (۱)، ماتریس سردرگمی عملکرد سامانه تشخیص نفوذ را نشان می‌دهد و شامل پارامترهای مثبت صحیح، منفی صحیح، مثبت کاذب و منفی کاذب است.

جدول (۱): ماتریس سردرگمی

	نتیجه آزمایش مثبت	نتیجه آزمایش منفی
نتیجه حقیقی مثبت	مثبت صحیح (T.P.)	منفی کاذب (F.N.)
نتیجه حقیقی منفی	مثبت کاذب (F.P)	منفی صحیح (T.N.)

دقت[2] بر اساس معادله (۱)، نسبت داده‌هایی که به درستی تشخیص داده شده‌اند بر کل داده‌های مجموعه داده را نشان می‌دهد.

$$Accuracy = \frac{T.P+T.N}{T.P+T.N+F.P+F.N} \qquad (۱)$$

۴-۲- مجموعه داده‌های ارزیابی

از مجموعه داده‌های استاندارد برای ارزیابی سامانه تشخیص نفوذ PHP-WA-IDS استفاده می‌شود. بردارهای حملات شامل بردارهای حملات اولیه و ثانویه اجرای کد از راه دور هستند.

[1] Confusion Matrix

[2] Accuracy

مجموعه داده‌های حملات اجرای کد از راه دور به شرح زیر هستند:

- بردارهای حملات اجرای کد از راه دور مجموعه داده استاندارد ECML/PKDD 2007.
- مجموعه داده‌ی بردارهای حمله از مراجع مختلف بهره‌برداری آسیب‌پذیری تهیه شده است [۲۱ و ۲۲].
- لاگ وب‌سرور حاوی درخواست‌های فرستاده شده به سمت نرم‌افزار تحت وب که شامل ۱۶۰۰۰ درخواست HTTP است.

۴-۳- نتایج ارزیابی

در این قسمت از مجموعه داده‌های حملات مختلف، برای ارزیابی سامانه تشخیص نفوذ PHP-WA-IDS استفاده شده است.

نتایج به‌دست آمده از سامانه تشخیص نفوذ PHP-WA-IDS با سامانه‌های تشخیص نظیر دیوار آتش نرم‌افزار تحت وب ModSecurity نسخه V3.3.0 و همچنین PHPIDS مورد مقایسه قرار می‌گیرد [۱۲، ۱۲ و ۲۴].

جدول (۲): مقایسه نتایج سامانه تشخیص نفوذ نرم‌افزارهای وبی PHP-WA-IDS

	روش استفاده شده	فناوری وبی	مجموعه داده استفاده شده	دقت تشخیص حملات اولیه اجرای کد از راه دور	دقت تشخیص حملات ثانویه اجرای کد از راه دور
دیوار آتش نرم‌افزار تحت وب OWASP ModSecurity 2021	عبارات منظم	مستقل از سکو[1]	مجموعه داده ۱، ۲ و ۳ (۶۲۰۰ بردار حمله)	٪۷۳/۸	ندارد
سامانه تشخیص نفوذ PHPIDS پروژه Expose 2017	عبارات منظم	زبان PHP	مجموعه داده ۱، ۲ و ۳ (۶۲۰۰ بردار حمله)	٪۳۷/۶	ندارد
سامانه تشخیص نفوذ PHP-WA-IDS	عبارات منظم – پروفایل‌های رفتاری	زبان PHP	مجموعه داده ۱، ۲ و ۳ (۶۲۰۰ بردار حمله)	٪۹۰/۴	٪۹۵
سامانه تشخیص grMalwrScanner 2019	قوانین YARA [۲۵]	زبان PHP	۲۱۰۰ بردار حمله	ندارد	٪۸۵/۵

بر طبق جدول (۲) مشاهده می‌شود که سامانه تشخیص نفوذ PHP-WA-IDS با دقت میانگین ٪۹۰/۴ و ٪۹۵ در رویکرد مبتنی بر امضاء و مبتنی بر رفتار ناهنجار، حملات اجرای کد از راه دور را در حالت اولیه و ثانویه تشخیص می‌دهد. سامانه تشخیص نفوذ پیشنهادی نسبت به سامانه‌های ذکر شده بهبود در درصد تشخیص، به‌کار بردن رویکرد رفتاری و کاهش نرخ مثبت کاذب را به همراه دارد.

۵- نتیجه‌گیری

در پژوهش انجام شده مشاهده می‌شود که سامانه تشخیص نفوذ نرم‌افزارهای وبی لایه کاربرد، با استفاده از رویکردهای مبتنی بر امضاء و رفتار در قالب رویکرد لایه‌ای، بهینه‌سازی روش‌های تشخیص حملات را به دنبال دارد. استفاده از رویکرد لایه‌ای جهت تشخیص حملات اجرای کد از راه دور با توجه به تفکیک مرتبه حملات، مؤثر واقع شده است. بهبود در درصد تشخیص، به‌کار بردن رویکرد رفتاری و کاهش نرخ مثبت کاذب از نتایج به‌کار بردن رویکرد لایه‌ای است.

کارهای آتی این تحقیق بر طبق برنامه، شامل بهبود و ایجاد سامانه تشخیص نفوذ مستقل از زبان سمت سرور بر روی نرم‌افزارهای تحت وب است.

۶- مراجع

[1] "Server-side Programming Languages, "April 1 2021. [Online]. Available: https://w3techs.com.

[2] I. Ristic, Apache Security (The Complete Guide to Securing Your Apache Web Server), O'Reilly, 2005.

[3] M. Amerei and A. Beigi, "Intrusion Detection System with Hybrid Method," *A collection of the fifteenth Conference of Iran's secret conference*, In Persian, 2018.

[1] Cross Platform

[4] "Acunetix Web Application Vulnerability Report 2020," 2020. [Online]. Available: https://www.acunetix.com/acunetix-web-application-vulnerability-report/. [Accessed 2020].

[5] S. Biswas, M. M. H. K. Sajal, T. Afrin, T. Bhuiyan, and M. M. Hassan, "A Study on Remote Code Execution Vulnerability in Web Application," in *International Conference on Cyber Security and Computer Science (ICONCS'18)*, 2018.

[6] R. Chauhan, "PHP Code: Top Ten Security Vulnerabilities," DZone - Web Dev Zone, [Online]. Available: https://dzone.com/articles/php-code-top-ten-security-vuln. [Accessed 2018].

[7] B. Hawkins and B. Demsky, "ZENIDS: Introspective Intrusion Detection for PHP Applications," *IEEE/ACM 39th International Conference on Software Engineering*, 2017.

[8] N. Agarwal and S. Z. Hussain, "A Closer Look at Intrusion Detection System for Web Applications," *Department of Computer Science*, 2018.

[9] M. Alahmad, A. Alkandari, and N. Alawadhi, "Survey of Os Command Injection Web Application Vulnerability Attack," *Journal of Engineering Science and Technology, vol. 17, no. 1, pp 1-5*, 2022.

[10] J. Díaz-Verdejo, J. Muñoz-Calle; and A. E. Alonso, "On the Detection Capabilities of Signature-Based Intrusion Detection System in the Context of Web Attacks," *mdpi, vol. 9, no. 1, pp 2-10*, 2022.

[11] B. Harsh, *Log based Dynamic Intrusion Detection of Web Application*, M.S. Thesis, Department of Computer Science and Engineering Indian Institute of Technology Kanpur, 2019.

[12] "PHP Security Cheat Sheet, Draft Cheatsheet, OWASP_Code_Review_Guide-V1_1," 2016. [Online]. Available: https://www.owasp.org/index.php/PHP_Security_Cheat_Sheet.

[13] l. Alshanersky, php | Architect's Guide to PHP Security, A Step-by-Step Guide to Writing Secure and Reliable PHP Applications, 2005.

[14] "PHP Manual," PHP, [Online]. Available: https://www.php.net/manual/en/. [Accessed 3 2020].

[15] K. Kowsari, K. Jafari Meimandi, M. Heidarysafa, S. Mendu, L. Barnes, and D. Brown, "Text Classification Algorithms: A Survey," *Information, vol. 10, no. 4, pp 1-8*, 2019.

[16] K. L. Ingham, *Anomaly Detection for HTTP Intrusion Detection: Algorithm Comparisons and the Effect of Generalization on Accuracy*, M.S. Thesis, The University of New Mexico, 2007.

[17] D. Jurafsky and J. Martin, Speech and Language Processing, stanford, 2019.

[18] K. R. Suneetha and D. R. Krishnamoorthi, "Identifying User Behavior by Analyzing Web Server Access Log File," *IJCSNS International Journal of Computer Science and Network Security, vol. 58, no. 2, pp 1-10*, 2009.

[19] K. U. Raut, "Log Based Intrusion Detection System," *IOSR Journal of Computer Engineering (IOSR-JCE), vol. 20, no. 5, pp 1-5*, 2018.

[20] İ. Taşdelen, "Command Injection Payload List," Nov 2018. [Online]. Available: https://github.com/payloadbox/command-injection-payload-list. [Accessed 10 2019].

[21] "Exploit Database," [Online]. Available: https://www.exploit-db.com. [Accessed 21 1 2021].

[22] "Expose: An IDS for PHP," Github, 2017. [Online]. Available: https://github.com/enygma/expose. [Accessed 2021].

[23] "OWASP ModSecurity Core Rule Set," OWASP, 2020. [Online]. Available: https://coreruleset.org. [Accessed 4 2020].

[24] V. G. Le and H. T. Nguyen, "GuruWS: A Hybrid Platform for Detecting Malicious Web Shells and Web Application Vulnerabilities," *Springer-Verlag GmbH Germany, vol. ?, no. ?, pp ?*, 2019.

[25] "web-application-attacks-datasets," [Online]. Available: https://gitlab.fing.edu.uy/gsi/web-application-attacks-datasets. [Accessed 21 1 2021].

[26] "OWASP (2014). Owasp Modsecurity Core Rule Set," [Online]. Available: https://github.com/SpiderLabs/owasp-modsecurity-crs/blob/master/base_rules/modsecurity_crs_40_generic_attack.conf.