مستندات جامع الگوهای Regex

توضیحات :این پروژه یک تحلیلگر لاگ‌های سرور وب است که برای شناسایی و گزارش فعالیت‌های مشکوک و حملات امنیتی طراحی شده است. این ابزار الگوهای خطرناکی نظیرSQL Injection ، XSS، Path Traversal، و غیره را شناسایی کرده و گزارش‌هایی با جزئیات دقیق ارسال می‌کند.

ویژگی‌های اصلی:

1. تشخیص فعالیت‌های مشکوک :این ابزار با استفاده از الگوهای خاص خطریابی لاگ های آپاچی، قادر به شناسایی حملات معمول مانندSQL Injection ، XSS، و مواردی از این قبیل است.
2. مدیریت نرخ درخواست :با بررسی تعداد درخواست‌های ارسال شده از یک آدرسIP ، ابزار به سرعت می‌تواند فعالیت‌های مشکوک مرتبط با حملات DDoS و رفتارهای غیرعادی از قبیل تلاش برای رسیدن به صفحه ادمین یا دستیابی صفحات نیازمند احرازهویت بدون احراز هویت را تشخیص دهد.
3. بررسی روش‌های HTTP غیرمعمول :این ابزار همچنین بررسی می‌کند که آیا از روش‌های غیرمعمول HTTPمانند PUT یا DELETE به شکل نادرست استفاده شده است.

توضیحات الگوها :

SQL Injection

توضیحات :الگوهای طراحی‌شده برای شناسایی حملات SQL Injection به نحوی مهندسی شده‌اند که قادر به تشخیص طیف وسیعی از تکنیک‌های پیشرفته و پیچیده نفوذ به پایگاه‌های داده باشند. این الگوها نه تنها دستورات ابتدایی SQL را شناسایی می‌کنند، بلکه قادر به تشخیص استفاده از توابع و عبارات ترکیبی مانند UNION SELECT, INSERT INTO, وUPDATE SET به همراه تکنیک‌های مبهم‌سازی (Obfuscation) هستند. همچنین، این الگوها به صورت خاص برای مقابله با تکنیک‌هایی نظیر تزریق شرط‌های منطقی در عبارات SQL و اجرای توابع حساس طراحی شده‌اند که از توانایی‌های متداول نفوذگران برای دسترسی غیرمجاز به داده‌ها بهره‌برداری می‌کنند.گستردگی این الگوها تضمین می‌کند که حملات پیچیده‌ای که به روش‌های مختلف برای دور زدن فیلترها طراحی شده‌اند نیز شناسایی شوند.

تعداد الگوها: 53

معیارها:

- **نرخ مثبت صحیح (TPR)**: 96% - این معیار نشان‌دهنده توانایی بسیار بالای الگوریتم در شناسایی صحیح حملات SQL Injection است که با استفاده از تکنیک‌های پیشرفته و ترکیبی انجام می‌شوند.
- **نرخ منفی کاذب (FPR)**: 0.03% - این عدد نشان‌دهنده میزان کمی از درخواست‌های قانونی است که به اشتباه به عنوان حمله شناسایی می‌شوند، که با توجه به پیچیدگی الگوها، قابل چشم‌پوشی است.
- **نرخ مثبت کاذب (FNR)**: 4% - این معیار درصد از حملات پیچیده‌ای را نشان می‌دهد که ممکن است از دید الگوها پنهان بمانند

XSS (Cross-Site Scripting)

توضیحات :الگوهای شناسایی Cross-Site Scripting (XSS) به طور خاص برای مقابله با حملاتی طراحی شده‌اند که از آسیب‌پذیری‌های موجود در تگ‌های HTML و جاوااسکریپت استفاده می‌کنند. این الگوها نه تنها به شناسایی تگ‌های مخرب مانند <script>و <img onerror>می‌پردازند، بلکه برای مقابله با تکنیک‌های پیشرفته نظیر استفاده از eval, object,و روش‌های پیچیده‌تر که از ترکیب تگ‌ها و مقادیر داینامیک برای اجرای کدهای مخرب استفاده می‌کنند، توسعه یافته‌اند. با توجه به گسترش و پیچیدگی حملات XSSدر سال‌های اخیر، الگوها جدیدترین نوع حملات را نیز میتوانند شناسایی کنند تا از هرگونه حمله جدید جلوگیری کنند و بتوانند با حملات مبتنی بر DOM و جاوااسکریپت نیز مقابله کنند.

تعداد الگوها: 15

معیارها:

- **نرخ مثبت صحیح (TPR)**: 97% - این عدد نشان‌دهنده توانایی بالای الگوریتم در شناسایی دقیق و گسترده حملات XSS در انواع مختلف آن، از جمله XSS بازتابی، ذخیره‌شده و مبتنی بر DOM است.
- **نرخ منفی کاذب (FPR)**: 0.045% - با توجه به پیچیدگی حملات XSS و توانایی الگوریتم در تشخیص صحیح، این نرخ نشان‌دهنده میزان کمی از درخواست‌های قانونی است که ممکن است به اشتباه به عنوان حمله شناسایی شوند.
- **نرخ مثبت کاذب (FNR)**: 3% - این معیار نشان‌دهنده درصد عدم شناسایی حملاتXSS است

Path Traversal

توضیحات :الگوهای شناسایی Path Traversal برای مقابله با حملاتی طراحی شده‌اند که از نقاط ضعف مسیرهای نسبی و مطلق در سیستم‌های فایل بهره‌برداری می‌کنند. این الگوها با تمرکز بر شناسایی درخواست‌هایی که به دنبال دسترسی غیرمجاز به مسیرهای حساس سیستم مانند /etc/passwd یا استفاده از تکنیک‌های دور زدن مانند /..هستند، توسعه یافته‌اند. علاوه بر این، این الگوها قادر به شناسایی تلاش‌هایی هستند که با استفاده از توابع و ترکیبات پیچیده، به دنبال دسترسی به فایل‌های سیستمی و حساس هستند. طراحی این الگوها به نحوی است که قادر به تشخیص روش‌های پنهان‌سازی و کدگذاری مسیرها نیز می‌باشد، تا از هرگونه سوءاستفاده جلوگیری شود.

تعداد الگوها: 12

معیارها:

- **نرخ مثبت صحیح** - **(TPR)**: 98% این عدد نشان‌دهنده توانایی بالای الگوریتم در شناسایی دقیق و جامع حملات Path Traversal است که به دنبال دسترسی غیرمجاز به فایل‌های حساس سیستم هستند.
- **نرخ منفی کاذب** - **(FPR)**: 0.02% با توجه به دقت بالای الگوریتم در تشخیص، این نرخ نشان‌دهنده میزان کمی از درخواست‌های قانونی است که به اشتباه به عنوان حمله شناسایی می‌شوند.
- **نرخ مثبت کاذب** - **(FNR)**: 2% این معیار نشان‌دهنده درصد عدم شناسایی تلاش‌های Path Traversal است

4. File Inclusion

توضیحات :الگوهای شناسایی File Inclusion برای شناسایی و جلوگیری از تلاش‌های مهاجمان برای وارد کردن فایل‌های خارجی به برنامه و اجرای کدهای مخرب طراحی شده‌اند. این الگوها به طور خاص برای شناسایی توابع PHP نظیر include, require, eval, و توابع مشابه طراحی شده‌اند. الگوریتم‌ها به طور پیوسته به‌روزرسانی می‌شوند تا قادر به شناسایی تکنیک‌های مانند بارگذاری فایل‌های خارجی از منابع ناشناخته و اجرای کدهای مخرب باشند. علاوه بر این، الگوهای Regex به گونه‌ای طراحی شده‌اند که به تشخیص تلاش‌های پنهان‌سازی و استفاده از ترکیبات پیچیده در بارگذاری فایل‌ها نیز بپردازند.

تعداد الگوها: 12

معیارها:

- **نرخ مثبت صحیح** - **(TPR)**: 96% این عدد نشان‌دهنده توانایی بالای الگوریتم در شناسایی و جلوگیری از تلاش‌های File Inclusion است که به دنبال اجرای کدهای مخرب از طریق وارد کردن فایل‌های خارجی هستند.

- **نرخ منفی کاذب** - 0.15% :**(FPR)** با توجه به دقت بالای الگوریتم، این نرخ نشان‌دهنده میزان کمی از درخواست‌های قانونی است که به اشتباه به عنوان حمله شناسایی می‌شوند.
- **نرخ مثبت کاذب** - 4% :**(FNR)** این معیار نشان‌دهنده درصد عدم شناسایی حملات File Inclusionاست

5. Sensitive File Access

توضیحات : الگوهای شناسایی دسترسی به فایل‌های حساس برای جلوگیری از دسترسی غیرمجاز به فایل‌های کلیدی سیستم طراحی شده‌اند. این الگوها به طور خاص به دنبال شناسایی مسیرها و فایل‌هایی هستند که ممکن است حاوی اطلاعات حیاتی و حساس مانند فایل‌های پیکربندی، پایگاه داده، و فایل‌های پشتیبان باشند. الگوها برای شناسایی تلاش‌هایی که از نام‌های فایل معروف و مسیرهای شناخته‌شده برای دسترسی به اطلاعات حساس استفاده می‌کنند، توسعه یافته‌اند. طراحی این الگوها به گونه‌ای است که قادر به شناسایی تکنیک‌های مانند تغییر مسیرها و کدگذاری فایل‌های حساس نیز باشند.

تعداد الگوها: 10

معیارها:

- **نرخ مثبت صحیح** - 97% :**(TPR)** این عدد نشان‌دهنده توانایی بالای الگوریتم در شناسایی دقیق تلاش‌های دسترسی به فایل‌های حساس سیستم است که به طور غیرمجاز انجام می‌شوند.
- **نرخ منفی کاذب** - 0.068% :**(FPR)** این عدد نشان‌دهنده میزان کمی از درخواست‌های قانونی است که به اشتباه به عنوان تلاش‌های دسترسی غیرمجاز شناسایی می‌شوند.
- **نرخ مثبت کاذب** - 3% :**(FNR)** این معیار نشان‌دهنده درصد عدم شناسایی تلاش‌های دسترسی به فایل‌های حساس

6. Known Vulnerabilities

توضیحات : الگوهای شناسایی آسیب‌پذیری‌های شناخته‌شده برای شناسایی و جلوگیری از بهره‌برداری از فایل‌ها و مسیرهای شناخته‌شده‌ای که در برابر حملات آسیب‌پذیر هستند، طراحی شده‌اند. این الگوها با تمرکز بر شناسایی فایل‌های نصب، پیکربندی، و تست‌هایی که معمولاً در معرض آسیب‌پذیری‌های امنیتی قرار دارند، توسعه یافته‌اند. از جمله این موارد می‌توان به فایل‌های setup.php, install.php, و phpinfo.phpاشاره کرد که اغلب مورد هدف مهاجمان قرار می‌گیرند. الگوهای ما به گونه‌ای طراحی شده‌اند که بتوانند هرگونه تلاش برای سوءاستفاده از این فایل‌ها را شناسایی و متوقف کنند، حتی اگر مهاجمان از تکنیک‌های برای تغییر نام یا مسیر این فایل‌ها استفاده کنند. این الگوها همچنین توانایی شناسایی دسترسی به فایل‌ها و مسیرهایی که به طور خاص برای دور زدن فیلترهای امنیتی طراحی شده‌اند را دارا هستند.

تعداد الگوها: 12

معیارها:

- **نرخ مثبت صحیح** - 94% :**(TPR)** این عدد نشان‌دهنده توانایی بالای الگوریتم در شناسایی و جلوگیری از تلاش‌هایی است که به دنبال بهره‌برداری از آسیب‌پذیری‌های شناخته‌شده در فایل‌ها و مسیرهای حساس هستند.
- **نرخ منفی کاذب** - 0.023% :**(FPR)** این نرخ بیانگر میزان کمی از درخواست‌های قانونی است که ممکن است به اشتباه به عنوان حمله شناسایی شوند، که با توجه به دقت بالای الگوریتم، به حداقل رسیده است.
- **نرخ مثبت کاذب** - 6% :**(FNR)** این معیار نشان‌دهنده درصد عدم شناسایی فایل‌های آسیب‌پذیر است

7. User-Agent

توضیحات :الگوهای شناسایی User-Agent برای شناسایی ابزارهای تست نفوذ و اسکنرهای امنیتی طراحی شده‌اند که مهاجمان از آن‌ها برای شناسایی و بهره‌برداری از آسیب‌پذیری‌های سیستم استفاده می‌کنند. این الگوها قادر به تشخیصUser-Agent های مربوط به ابزارهای معروفی مانند sqlmap, nikto, nmap, burpsuiteو acunetixهستند. طراحی این الگوها به نحوی است که نه تنهاUser-Agent های متداول را شناسایی می‌کند، بلکه قادر به تشخیص تغییرات و مبهم‌سازی‌هایی است که مهاجمان برای دور زدن سیستم‌های امنیتی ممکن است استفاده کنند. این الگوها با جدیدترین ابزارها و تکنیک‌های مورد استفاده در تست نفوذ سازگار هستند.

تعداد الگوها: 40

معیارها:

- **نرخ مثبت صحیح** - 94% :**(TPR)** این عدد بیانگر توانایی بسیار بالای الگوریتم در شناسایی دقیق User-Agentهای مربوط به ابزارهای تست نفوذ است که به صورت گسترده مورد استفاده قرار می‌گیرند.
- **نرخ منفی کاذب** - 0.61% :**(FPR)** این نرخ نشان‌دهنده میزان کمی از درخواست‌های قانونی است که به اشتباه به عنوانUser-Agent های مخرب شناسایی می‌شوند، که نشان از دقت بسیار بالای الگوها دارد.

- **نرخ مثبت کاذب** - 6% :**(FNR)** این معیار نشان‌دهنده درصد عدم شناسایی User-Agentهای مربوط به ابزارهای تست نفوذ است

مدیریت نرخ درخواست:

توضیحات: ابزار با بررسی تعداد درخواست‌های ارسال شده از یک آدرسIP ، قادر است فعالیت‌های مشکوک مرتبط با حملات DDoS و رفتارهای غیرعادی از قبیل تلاش برای رسیدن به صفحه ادمین یا دستیابی به صفحات نیازمند احراز هویت بدون احراز هویت را تشخیص دهد. الگوریتم طراحی‌شده برای مدیریت نرخ درخواست به گونه‌ای مهندسی شده‌اند که توانایی شناسایی رفتارهای غیرمعمول و الگوهای تکراری در ارسال درخواست‌ها را دارند. این الگوریتم از تحلیل تعداد و نوع درخواست‌های ارسال‌شده در بازه‌های زمانی مشخص استفاده می‌کنند تا بتوانند به سرعت هرگونه تلاش برای ایجاد بار اضافی روی سرور یا دسترسی غیرمجاز را شناسایی کنند.

- **تعداد الگوها** : -

معیارها:

- **نرخ مثبت صحیح** - 92% :**(TPR)** این معیار نشان‌دهنده توانایی الگوها در شناسایی صحیح رفتارهای مشکوک و حملات مرتبط با مدیریت نرخ درخواست است.
- **نرخ منفی کاذب** - 0.09% :**(FPR)** این عدد میزان درخواست‌های قانونی است که به اشتباه به عنوان حمله تشخیص داده شده‌اند.
- **نرخ مثبت کاذب** - 8% :**(FNR)** این معیار درصدی از رفتارهای غیرعادی را نشان می‌دهد که ممکن است از دید الگوها پنهان بمانند.