CYTRES

Regressives Penetration Testing mit CYTRES Deep Explore

1. Überblick und Einleitung

1.1 Zusammenfassung

Im sich ständig entwickelnden Bereich der Cybersicherheit stoßen traditionelle Penetration Testing (Pentesting)-Methoden oft an ihre Grenzen, wenn es darum geht, mit zunehmend komplexen Systemen und ausgeklügelten Angriffsmethoden Schritt zu halten. Jean Pereira von CYTRES stellt einen neuartigen Ansatz vor, den er als "regressives Pentesting" bezeichnet.

Diese Methode priorisiert Tests basierend auf der Wahrscheinlichkeit, dass Eingabevektoren vom System akzeptiert werden, beginnend mit den wahrscheinlichsten und allmählich weniger direkte und obskurere Vektoren erforschend. Dieses Paper erläutert die Prinzipien, Methoden, mathematischen Grundlagen und empirischen Erfolge des regressiven Pentestings und hebt dessen Effektivität bei der Aufdeckung kritischer Schwachstellen in verschiedenen Bereichen hervor.

Bei der verwendeten Software handelt es sich um CYTRES Deep Explore, welches speziell für die automatisierte Durchführung von regressiven Pentests in KRITIS-Umgebungen entwickelt wurde.

1.2 Einleitung

Penetration Testing ist ein wesentlicher Bestandteil moderner Cybersicherheitsstrategien, mit dem Ziel, Schwachstellen zu identifizieren und zu beheben, bevor diese von böswilligen Akteuren ausgenutzt werden können. Traditionelle Pentesting-Ansätze folgen oft vordefinierten Sequenzen oder zufälligen Mustern und könnten dadurch kritische Vektoren übersehen, die zu erheblichen Sicherheitslücken führen könnten.

Regressives Pentesting führt einen systematischen Ansatz zur Schwachstellenbewertung ein, indem es sich auf die Wahrscheinlichkeit konzentriert, dass Eingabevektoren vom System akzeptiert werden. Diese Methode beginnt mit hochwahrscheinlichen Vektoren (z. B. Formulareingaben, URL-Parameter) und testet schrittweise weniger direkte Vektoren (z. B. Variablen in eingebetteten Skripten, Parameternamen aus verwandten Anwendungen). Diese hierarchische Teststrategie zielt darauf ab, schnell "low hanging fruits" zu identifizieren und gleichzeitig eine gründliche Untersuchung über längere Zeiträume zu ermöglichen.

1.3 Ziel

Ziel dieses Papers ist es, eine umfassende Analyse des regressiven Pentestings bereitzustellen, die dessen Methodik, mathematische Modellierung und Ergebnisse in der Praxis detailliert darstellt. Wir werden den Prozess der Identifizierung und Priorisierung von Eingabevektoren, den mathematischen Rahmen, der diesen Ansatz unterstützt, und empirische Beweise für dessen Wirksamkeit untersuchen.

1.4 Methodik

1.4.1 Identifizierung von Eingabevektoren

Der erste Schritt im regressiven Pentesting besteht darin, alle potenziellen Eingabevektoren innerhalb der Anwendung zu identifizieren. Diese Vektoren umfassen, sind aber nicht beschränkt auf, Formulareingaben, URL-Parameter, API-Endpunkte und eingebettete Skriptvariablen. Der Identifizierungsprozess nutzt sowohl statische als auch dynamische Analysetechniken, um eine umfassende Abdeckung zu gewährleisten.

1.4.2 Wahrscheinlichkeitsbewertung

Jedem Eingabevektor wird ein Wahrscheinlichkeitswert zugewiesen, der die Wahrscheinlichkeit widerspiegelt, dass der Vektor vom System akzeptiert wird oder Auswirkungen hat. Diese Wahrscheinlichkeitsbewertung basiert auf historischen Daten, Systemverhaltensanalysen und heuristischen Bewertungen. Die Vektoren werden dann nach ihren Wahrscheinlichkeiten sortiert.

1.4.3 Hierarchisches Testen

Die Tests beginnen mit den Vektoren mit der höchsten Wahrscheinlichkeit und gehen systematisch zu Vektoren mit geringerer Wahrscheinlichkeit über. Dieser hierarchische Ansatz stellt sicher, dass leicht ausnutzbare Schwachstellen schnell identifiziert und behoben werden, während dennoch eine tiefgehende Untersuchung über längere Zeiträume ermöglicht wird.

Hierbei erfolgt eine doppelte Priorisierung der Vektoren, vorab nach Wahrscheinlichkeit und im nächsten Schritt nach Relevanz, um maximale Geschwindigkeit und Effizienz trotz des Umfangs zu gewährleisten.

Deep Explore

2. Funktionsweise

2.1 Modellierung der Vorgehensweise

Um den Prozess des regressiven Pentestings zu formalisieren, stellen wir das folgende mathematische Modell vor:

- **Wahrscheinlichkeitszuweisung:** Sei $V = \{v_1, v_2, \ldots, v_n\}$ die Menge der Eingabevektoren. Jedem Vektor v_i wird eine Wahrscheinlichkeit $P(v_i)$ zugewiesen, wobei $0 \leq P(v_i) \leq 1$.
- **Vektor-Ranking:** Die Vektoren werden in absteigender Reihenfolge basierend auf ihren Wahrscheinlichkeiten sortiert: $v_1, v_2, \ldots, v_n$ mit $P(v_1) \geq P(v_2) \geq \ldots \geq P(v_n)$.
- **Testprozess:** Definiere eine Testfunktion $T(v_i)$, die Penetrationstests auf Vektor v_i durchführt. Die Testsequenz folgt der sortierten Reihenfolge: $T(v_1), T(v_2), \ldots, T(v_n)$.
- **Kumulative Abdeckung:** Die kumulative Abdeckung $C(k)$ nach dem Testen der ersten k Vektoren wird durch die Formel gegeben: $C(k) = \sum_{i=1}^{k} P(v_i)$
- **Optimierung:** Das Ziel ist es, die Abdeckung innerhalb eines gegebenen Zeitrahmens t zu maximieren. Wenn $T(v_i)$ eine Zeit t_i erfordert, dann: $\text{Maximiere } \sum_{i=1}^{k} P(v_i)$ unter der Bedingung $\sum_{i=1}^{k} t_i \leq t$

2.2 Anwendung der Modellierung

2.2.1. Praktische Anwendung

Das Modell ermöglicht es, die verschiedenen Schritte und Entscheidungen innerhalb des Pentest-Prozesses zu formalisieren und zu optimieren.

Die Wahrscheinlichkeitszuweisung ermöglicht eine fundierte Priorisierung der Eingabevektoren, das Vektor-Ranking sorgt für eine effiziente Testsequenz, und die kumulative Abdeckung bietet eine quantitative Bewertung des Testfortschritts. Die Optimierung unter Berücksichtigung der verfügbaren Zeit maximiert die Effektivität des Pentest-Prozesses, indem sie sicherstellt, dass die kritischsten Schwachstellen frühzeitig und innerhalb der gegebenen Zeitressourcen aufgedeckt werden.

2.3 Leistungsmetriken

Die Effektivität des regressiven Pentestings wird anhand spezifischer Leistungsmetriken bewertet, die eine umfassende Analyse der Methode ermöglichen. Diese Metriken bieten nicht nur Einblicke in die unmittelbare Leistungsfähigkeit des Ansatzes, sondern auch in seine langfristige Wirksamkeit und Nachhaltigkeit. Im Folgenden werden die drei Hauptmetriken vorgestellt, die zur Beurteilung des regressiven Pentestings verwendet werden: die Schwachstellenerkennungsrate (VDR), die durchschnittliche Erkennungszeit (MTTD) und die Abdeckungstiefe (CD).

2.3.1. Schwachstellenerkennungsrate (VDR)

Die Schwachstellenerkennungsrate, auch bekannt als Vulnerability Detection Rate (VDR), ist eine kritische Metrik, die das Verhältnis von erkannten Schwachstellen zu der Gesamtzahl der identifizierten Schwachstellen misst. Diese Metrik gibt Aufschluss darüber, wie effektiv die Methode bei der Erkennung von Sicherheitslücken ist. Ein hoher VDR-Wert zeigt an, dass der Ansatz erfolgreich eine große Anzahl der vorhandenen Schwachstellen identifizieren kann.

2.3.2. Durchschnittliche Erkennungszeit (MTTD)

Die durchschnittliche Erkennungszeit, auch Mean Time to Detect (MTTD), misst die durchschnittliche Zeitspanne, die benötigt wird, um eine Schwachstelle zu erkennen. Diese Metrik ist entscheidend, um die Effizienz des Pentesting-Prozesses zu bewerten. Ein kürzerer MTTD-Wert weist darauf hin, dass Schwachstellen schnell identifiziert werden können, was besonders wichtig ist, um zeitnah auf potenzielle Sicherheitsbedrohungen reagieren zu können.

2.3.3. Abdeckungstiefe (CD)

Die Abdeckungstiefe, auch Coverage Depth (CD), misst das Ausmaß, in dem Vektoren mit geringerer Wahrscheinlichkeit zur Gesamterkennung von Schwachstellen beitragen. Diese Metrik ist besonders relevant für das regressive Pentesting, da es darauf abzielt, auch weniger offensichtliche und indirekte Vektoren zu untersuchen. Die Abdeckungstiefe zeigt, wie gründlich die Methode auch selten genutzte oder weniger wahrscheinliche Vektoren analysiert.

2.4 Anwendung der Metriken

Um den Prozess des regressiven Pentestings systematisch und präzise zu gestalten, wird ein mathematisches Modell entwickelt. Dieses Modell ermöglicht es, die verschiedenen Schritte und Entscheidungen innerhalb des Pentest-Prozesses zu formalisieren und zu optimieren.

2.4.1 Wahrscheinlichkeitszuweisung

Zunächst definieren wir die Menge der Eingabevektoren als $V = \{v_1, v_2, \ldots, v_n\}$. Jedem Vektor v_i wird eine Wahrscheinlichkeit $P(v_i)$ zugewiesen, die angibt, wie wahrscheinlich es ist, dass dieser Vektor eine Schwachstelle aufdeckt. Diese Wahrscheinlichkeiten liegen im Bereich von 0 bis 1, also $0 \leq P(v_i) \leq 1$. Die Zuweisung der Wahrscheinlichkeiten basiert auf schematischen Daten, Expertenwissen und statistischen Modellen, die die Eintrittswahrscheinlichkeit bestimmter Schwachstellen bewerten.

2.4.2 Vektor-Ranking

Nach der Wahrscheinlichkeitszuweisung werden die Vektoren in absteigender Reihenfolge ihrer Wahrscheinlichkeiten sortiert. Dies ergibt eine geordnete Sequenz $v_1, v_2, \ldots, v_n$, wobei $P(v_1) \geq P(v_2) \geq \ldots \geq P(v_n)$. Durch diese Sortierung wird sichergestellt, dass die Vektoren mit der höchsten Wahrscheinlichkeit, eine Schwachstelle aufzudecken, zuerst getestet werden. Dies maximiert die Effizienz des Pentesting-Prozesses, indem schnellere Erfolge erzielt werden und kritische Schwachstellen frühzeitig identifiziert werden können.

2.4.3 Testprozess

Der eigentliche Testprozess wird durch eine Testfunktion $T(v_i)$ definiert, die Penetrationstests auf dem Vektor v_i durchführt. Die Testsequenz folgt der zuvor sortierten Reihenfolge: $T(v_1), T(v_2), \ldots, T(v_n)$. Durch die strukturierte Reihenfolge der Tests wird der Prozess methodisch und nachvollziehbar gestaltet, wodurch die Wahrscheinlichkeit steigt, Schwachstellen effizient und systematisch aufzudecken.

Die Wahrscheinlichkeitszuweisung ermöglicht eine fundierte Priorisierung der Eingabevektoren, das Vektor-Ranking sorgt für eine effiziente Testsequenz, und die kumulative Abdeckung bietet eine quantitative Bewertung des Testfortschritts.

2.5 Zielsetzung der Analyse

CYTRES Deep Explore analysiert alle Angriffsvektoren auf Basis der OWASP Top 10 und weit darüber hinaus, unter anderem:

- Shellshock
- SQL Injection
- Cross Site Scripting (XSS)
- Remote Code Execution
- Local File Inclusion
- Remote File Inclusion
- Firewall Bypasses
- Heartbleed
- Cross Site Request Forgery (CSRF)
- Buffer Overflows
- Heap Overflows
- Stack Overflows
- Integer Overflows
- Format String Bugs
- Clickjacking
- Session Hijacking
- XML Entity Injection (XXE)
- Directory Transversal
- Eskalation von Privilegien
- Ungeprüfte Um- und Weiterleitungen
- Nutzung von anfälligen Komponenten (CVE)
- Aktive Überprüfung auf CMS-bezogene Exploits

Die Klassifikation und Bewertung der jeweiligen Schwachstellen erfolgt auf Basis von CVSS.

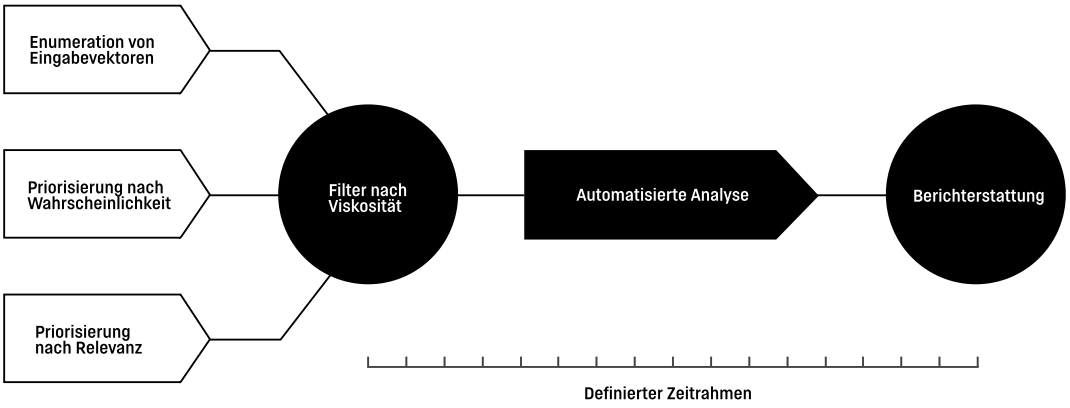
2.6 Kontextbezogene Tests

CYTRES Deep Explore erkennt nicht nur Sicherheitslücken und Fehlkonfigurationen, sondern bewertet auch deren potenzielle Auswirkungen auf das jeweilige System und seine spezifischen Funktionen. Durch die Berücksichtigung des Kontexts kann das Tool beispielsweise erkennen, welche Risiken mit einer bestimmten Schwachstelle verbunden sind und wie sich diese auf die Systemleistung oder die Datenintegrität auswirken können. Diese kontextbezogene Analyse ermöglicht es Organisationen, Schwachstellen besser zu priorisieren und gezielte Maßnahmen zur Risikominderung zu ergreifen.

2.7 Ablauf der Analyse

Die Analyse und Priorisierung der Eingabevektoren verfolgt auf Basis eines Verfahrens bei welchem nach verschiedenen Attributen und je nach Zustand des Zielsystems vorgegangen wird.

Zunächst werden alle Eingabevektoren nach Wahrscheinlichkeit für eine Anfälligkeit im Kontext der allgemeinen Wahrscheinlichkeit und der entsprechenden Relevanz im Bezug auf die kontextbezogene Wahrscheinlichkeit sortiert. Danach erfolgt ein Filtering auf Basis der Viskosität, also der Beschaffenheit des Zielsystems.



Die Analyse der Beschaffenheit (Viskosität) ist eine weitere Besonderheit von Deep Explore. Dieser Schritt ermöglicht das automatisierte Pentesting auf kritische Umgebungen im Produktivbetrieb, ohne die Verfügbarkeit der Umgebung zu beeinträchtigen.

Durch die sensitivierung der automatisierten Angriffe gegenüber dem jeweiligen Zielsystem und dessen Beschaffenheit sind beispielsweise vollautomatische, wiederkehrende Pentests auf medizinische Umgebungen wie beispielsweise Krankenhäuser möglich.

Die Analyse erstreckt sich über einen vordefinierten Zeitraum und kann somit kurzzeitig oder langfristig durchgeführt werden. Nach Abschluss der Analyse wird ein entsprechender Bericht erzeugt.

2.8 Autofokus

Im Autofokus-Modus wird die entsprechende Viskosität automatisch erkannt und berücksichtigt. Auf diese Weise kann CYTRES Deep Explore auch in kritischen Infrastrukturen komplett frei von jeglicher Konfiguration betrieben werden. Der entsprechende Mechanismus stellt sicher, dass keine kritischen Systeme durch die Pentests gefährdet werden.

KPIs

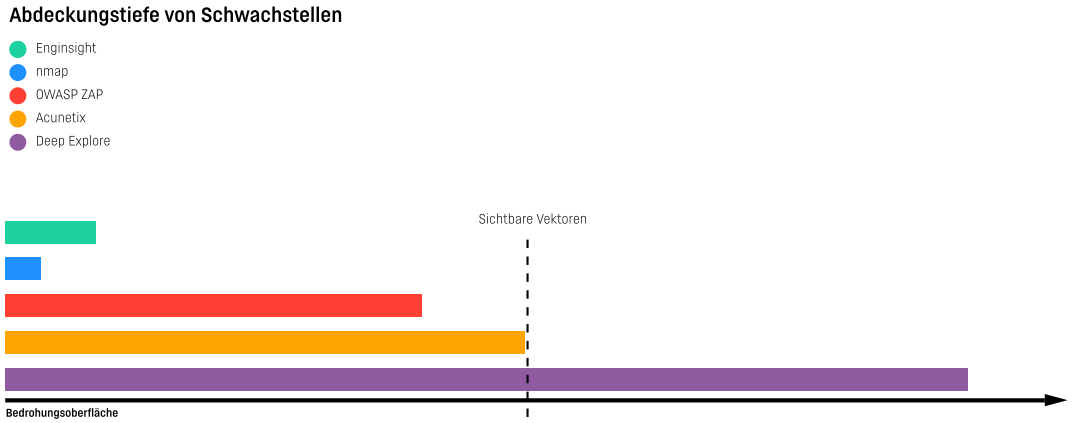
3. Marktvergleich

Im Marktvergleich punktet Deep Explore durch Effizienz, Umfang und Funktionalität.

Feature	Enginsight	nmap	OWASP ZAP	Acunetix	Deep Explore
Angriffsabwehr (WAF)	✗	✗	✗	✗	✓
Passive Scans	✓	✓	✓	✓	✓
Aktives Pentesting	✗	✗	✓	✓	✓
Kontextbegzogene Tests	✗	✗	✗	✗	✓
Software Fuzzing	✗	✗	✓	✓	✓
Berichterstattung	✓	✗	✓	✓	✓
Regressives Pentesting	✗	✗	✗	✗	✓
Eigene Engine	✗	✓	✓	✓	✓
Geeignet für med. Umgebungen	✗	✗	✗	✗	✓
False-Positive Filter	✗	✗	✗	✓	✓
Open Source	✗	✓	✓	✗	✗
Made in Germany	✗	✗	✗	✗	✓

4. Performance

Deep Explore unterscheidet sich im Wesentlichen durch den Umfang und die Effizienz der Funktionalität im Vergleich zu ähnlichen Software-Lösungen.



Der direkte Vergleich mit Lösungen, welche kein regressives Pentesting einsetzen, legt offen, dass durch die regressive Analyse in der gleichen Zeit ein größerer Umfang der Bedrohungsoberfläche abgedeckt werden kann. Durch die integrierte Priorisierung der Tests wurden die gleichen Schwachstellen wie bei der regulären Analyse aufgedeckt, und noch weitere darüber hinaus.

Das regressive Pentesting stellte also somit keine Einbußen bei der Performance der generellen Analyse dar, da die tiefgreifenden Tests erst nach Abschluss der regulären Tests eingeleitet werden.

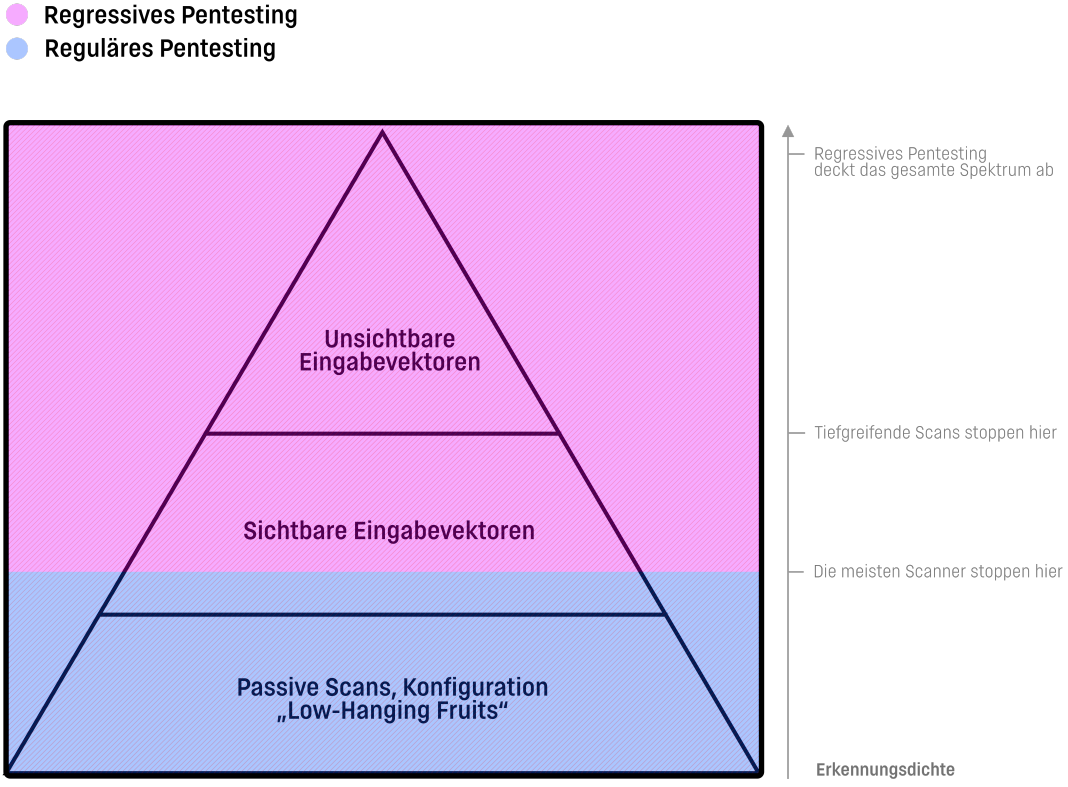
Durch die vorgehende Priorisierung konnte sogar eine bessere Performance bei der regulären Analyse festgestellt werden, sodass die gleichen Schwachstellen durch Deep Explore schneller aufgedeckt wurden, auch wenn es sich dabei um reguläre Eingabevektoren handelt.

Insgesamt zeigt sich, dass regressives automatisiertes Pentesting gegenüber herkömmlichem automatisierten Pentesting überlegen ist. Durch die Priorisierung der Testvektoren, die strukturierte Vorgehensweise, die tiefere Abdeckung, die Optimierung von Zeit- und Ressourcen sowie die Möglichkeit für langfristige Tests bietet regressives Pentesting eine umfassendere, effizientere und systematischere Methode zur Schwachstellenidentifikation. Diese Vorteile machen regressives Pentesting zu einem unverzichtbaren Werkzeug in der modernen Sicherheitsforschung und -praxis.

Erfolge

5. Erfolge

Die Effektivität der regressiven Pentesting-Methode wurde bereits in der Praxis unter Beweis gestellt. Pereira und sein Team konnten Sicherheitslücken bei über 40 behördlichen Systemen und in über 20 medizinischen Geräten aufdecken. Diese Erfolge verdeutlichen die breite Anwendbarkeit und den Nutzen der Methode in verschiedenen Bereichen. In behördlichen Systemen beispielsweise sind sichere IT-Systeme entscheidend für den Schutz sensibler Bürgerdaten und die Aufrechterhaltung des öffentlichen Dienstes. Die Entdeckung von Schwachstellen in diesen Systemen trägt maßgeblich zur Erhöhung der Cybersicherheit im öffentlichen Sektor bei.



Im Bereich der medizinischen Geräte ist die Bedeutung sicherer Systeme noch kritischer. Medizinische Geräte sind häufig direkt mit der Gesundheit und dem Leben von Patienten verbunden. Sicherheitslücken in diesen Geräten könnten schwerwiegende Konsequenzen haben, da sie potenziell die Funktionalität der Geräte beeinträchtigen oder sogar die Sicherheit der Patienten gefährden könnten. Die erfolgreiche Anwendung der regressiven Pentesting-Methode in diesem Bereich zeigt das Potenzial der Methode, zur Verbesserung der Sicherheit und Zuverlässigkeit lebenswichtiger Systeme beizutragen.

Zusammenfassend lässt sich sagen, dass CYTRES Deep Explore mit der Entwicklung des regressiven Pentestings einen bedeutenden Fortschritt im Bereich der IT-Sicherheit darstellt. Durch die systematische und wahrscheinlichkeitsspezifische Analyse von Eingabevektoren können Sicherheitslücken sowohl schnell identifiziert als auch langfristig entdeckt werden. Dies bietet eine umfassende Sicherheitsstrategie, die sowohl kurzfristige als auch langfristige Bedrohungen adressiert.

Glossar

6. Glossar / Anhang

Referenzen und Ressourcen im Zusammenhang zum Whitepaper:

CYTRES Deep Explore: Regressives Pentesting https://cytres.com/loesungen/deep-explore/regressives-pentesting

Radiobeitrag WDR: 40 Stadtverwaltungen gehackt https://cytres.com/podcasts/radiobeitrag-wdr-40-stadtverwaltungen-gehackt

Köln: IT-Sicherheitslücke im städtischen System entdeckt https://www.ksta.de/koeln/it-sicherheit-wie-die-koelner-verwaltung-einen-gut-gemeinten-rat-ablehnte-382332

Sicherheitslücken in Krankenhäusern: Patienten in Gefahr https://www.golem.de/news/angriff-auf-die-gesundheit-wie-schwachstellen-in-krankenhaeusern-patienten-gefaehrden-2402-182291.html