

Gamifizierte Lernplattform für Binary Exploitation

Ausgangslage

Binary Exploitation ist ein fundamentaler Bereich der IT-Sicherheit, der jedoch für viele Einsteiger eine steile Lernkurve aufweist. Die praktische Anwendung von Konzepten wie Buffer Overflows, Stack Cookies, Address Space Layout Randomization (ASLR), Data Execution Prevention (DEP) und Control Flow Integrity (CFI) ist essentiell für das Verständnis moderner Sicherheitsmechanismen. Traditionelle Lehrmethoden sind oft theorielastig und bieten wenig interaktive Übungsmöglichkeiten. Gleichzeitig zeigt die Forschung, dass spielbasiertes Lernen die Motivation und den Lernerfolg deutlich steigern kann.

Während es bereits verschiedene Plattformen für das Erlernen von Web Security gibt, existieren nur wenige moderne, browserbasierte Angebote für Binary Exploitation. Die vorhandenen Lösungen sind entweder veraltet, setzen komplexe lokale Setups voraus oder behandeln nicht das vollständige Spektrum moderner Schutzmechanismen. Eine webbasierte, spielerische Lernplattform könnte diese Lücke schließen und den Einstieg in dieses wichtige Gebiet erleichtern.

Zielsetzung / Methodik / Vorgehen

Im Rahmen dieser Masterarbeit soll eine browserbasierte, gamifizierte Lernplattform für Binary Exploitation entwickelt werden. Die Plattform soll Nutzer schrittweise an die Konzepte heranführen und durch praktische Übungen ein tiefgreifendes Verständnis ermöglichen.

Konkrete Ziele sind:

- Entwicklung einer modularen, webbasierten Spielumgebung mit progressivem Schwierigkeitsgrad
- Integration eines WebAssembly-basierten Backends zur sicheren Ausführung von exploitbarem Code
- Implementierung interaktiver Tutorials und Übungen für verschiedene Exploit-Techniken
- Gestaltung eines Belohnungssystems mit Achievements und Fortschrittsanzeigen
- Integration von Hilfesystemen und Visualisierungen zur Unterstützung des Lernprozesses
-

Die Entwicklung erfolgt iterativ mit regelmäßiger Evaluation durch Studierende und Sicherheitsexperten. Besonderer Fokus liegt auf:

(1) Implementierung einer sicheren Sandbox-Umgebung, (2) Entwicklung aussagekräftiger Visualisierungen für Stack und Memory, (3) Integration von modernen Gamification-Elementen.

Verlangte Skills: Kenntnisse in Web Development (JavaScript/TypeScript), Grundverständnis von Linux

Teilaufgaben

Das Projekt kann in 3 Stufen durchgeführt werden:

P7: Konzeption der Plattform, Entwicklung der grundlegenden Spielmechanik und Implementation einfacher Buffer Overflow Challenges, P8: Integration fortgeschrittener Schutzmechanismen (Stack Cookies, ASLR), Entwicklung des Visualisierungssystems, P9: Implementation komplexer Schutzmechanismen (DEP, CFI), Evaluation und Optimierung der Lerneffektivität

Studienart: [x] Vollzeitstudium
[x] Teilzeitstudium 50%

Projektorganisation: Einzelarbeit

Projektfinanzierung: -

Arbeitsort: Windisch

Advisor: Prof. Dr. Christopher Scherb

