TECHNISCHE HOCHSCHULE DEGGENDORF

Bachelor Cyber Security

Kryptologie 2 Projektbericht

Ausarbeitung Cryptochallenge: CurveBall

Autor:

Manuel Friedl, Matrikel-Nr.: 1236626
Christof Renner, Matrikel-Nr.: 22301943

Betreuer:

Prof. Dr. Martin Schramm

Deggendorf – 28.07.2025

Contents

1 Einführung

Willkommen zur CurveBall CTF Challenge!
Diese Challenge behandelt eine der kritischsten Sicherheitslücken in der Windows-Geschichte: CVE-2020-0601, bekannt als *CurveBall*. Sie lernen die Grundlagen der Elliptic Curve Cryptography (ECC) kennen und verstehen, wie Schwachstellen in kryptographischen Implementierungen ausgenutzt werden können.

2 Systemvoraussetzungen

- **Docker** und **Docker Compose** (Version 20.10 oder höher)
- **Webbrowser** (empfohlen: Firefox oder Chrome)
- **Grundlegende Kenntnisse:**
  - Kryptographie-Grundlagen
  - Python-Programmierung
  - Umgang mit Zertifikaten
- **Texteditor oder IDE** für die Bearbeitung von Code
- **Mindestens 2 GB freier Arbeitsspeicher**

3 Challenge-Setup und Start

Wichtiger Hinweis: Stellen Sie sicher, dass Docker auf Ihrem System installiert und gestartet ist, bevor Sie mit dem Setup beginnen.

1. **Repository klonen:**

```
git clone https://mygit.th-deg.de/cr02943/kryptologie2-curveball
```

2. **Zum Challenge-Verzeichnis navigieren:**

```
cd kryptologie2-curveball/curveball-ctf/
```

3. **Challenge-Umgebung starten:**

```
docker-compose up --build -d
```

4. **Challenge aufrufen:**
   Öffnen Sie Ihren Webbrowser und navigieren Sie zu:

   https://localhost:8443

Zertifikatswarnung: Da die Challenge ein selbstsigniertes Zertifikat verwendet, erhalten Sie eine Sicherheitswarnung im Browser. Akzeptieren Sie das Zertifikat, um fortzufahren.

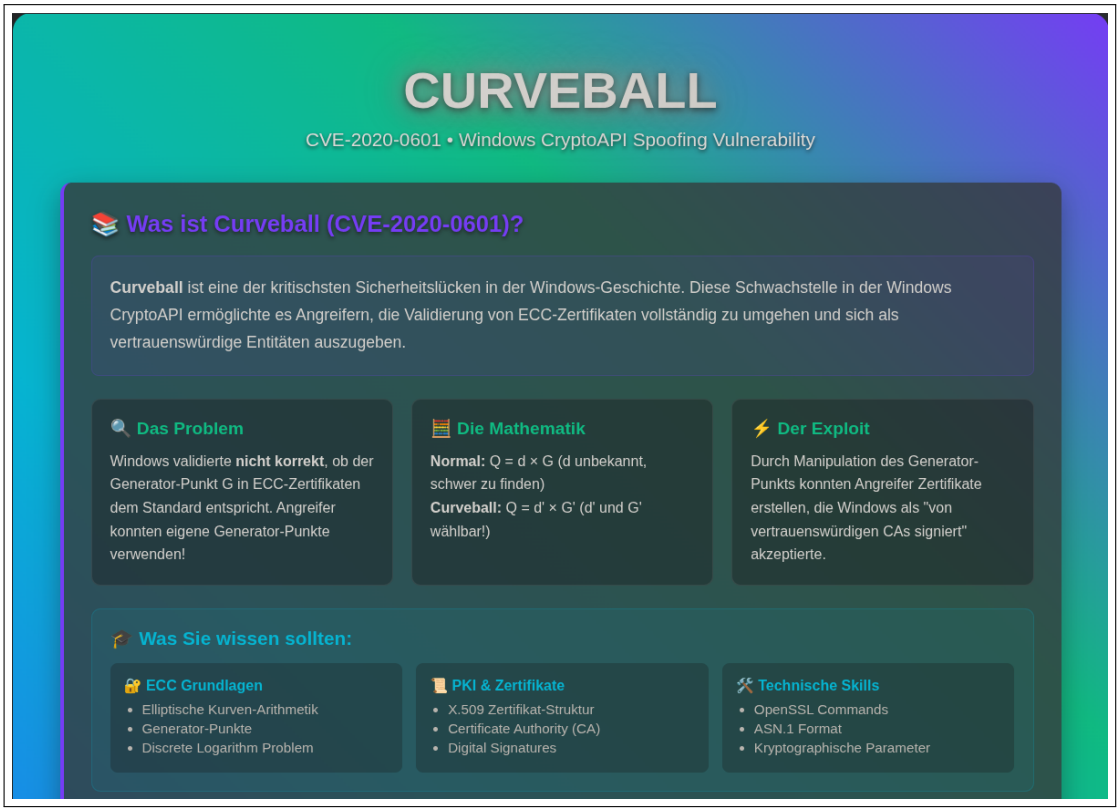

Figure 1: **Challenge Weboberfläche - Hauptseite**

4 Challenge-Struktur

Die CurveBall CTF-Challenge ist modular aufgebaut und besteht aus vier aufeinander aufbauenden Bereichen. Jeder Bereich behandelt spezifische Aspekte der ECC-Kryptographie und der CurveBall-Schwachstelle.

4.1 Einführungsbereich

Theoretische Grundlagen
Der Einführungsbereich vermittelt das notwendige Hintergrundwissen für die praktischen Challenges.

Inhalte:

- **Elliptic Curve Cryptography (ECC):** Mathematische Grundlagen und Algorithmen
- **CVE-2020-0601 Schwachstelle:** Technische Details und Auswirkungen
- **Historischer Kontext:** Entdeckung durch die NSA und globale Auswirkungen
- **Kryptographische Konzepte:** Schlüsselgenerierung, Signaturen und Zertifikate

4.2 Challenge 1: ECC-Grundlagen

Lernziele

- Verstehen der mathematischen Struktur elliptischer Kurven
- Praktische Anwendung von Punktoperationen auf elliptischen Kurven
- Implementierung und Verständnis von ECC-Algorithmen

Praktische Aufgaben:

- Berechnung von Punktaddition und -multiplikation auf elliptischen Kurven
- Analyse und Manipulation der Parameter einer elliptischen Kurve
- Implementierung grundlegender ECC-Operationen in JavaScript

4.3 Challenge 2: Zertifikatsgenerierung

Lernziele

- Verstehen der Struktur und des Formats von X.509-Zertifikaten
- Erstellung und Verarbeitung von Certificate Signing Requests (CSR)
- Manipulation und Analyse von Zertifikatsparametern

Praktische Aufgaben:

- Generierung von ECC-Schlüsselpaaren für verschiedene Kurven
- Erstellung, Signierung und Validierung von X.509-Zertifikaten
- Forensische Analyse von Zertifikatsstrukturen und -inhalten

4.4 Challenge 3: Kurvenmanipulation

Lernziele

- Verstehen der technischen Details der CurveBall-Schwachstelle
- Praktische Manipulation von elliptischen Kurvenparametern
- Ausnutzung von Schwächen in der Zertifikatsvalidierung

Praktische Aufgaben:

- Modifikation von elliptischen Kurvenparametern (a, b, p)
- Erstellung von Zertifikaten mit manipulierten Kurven
- Demonstration der Umgehung der Windows CryptoAPI-Validierung

4.5 Challenge 4: Signature-Spoofing

Lernziele

- Praktische Ausnutzung der CVE-2020-0601 Schwachstelle
- Erstellung und Validierung gefälschter digitaler Signaturen
- Verstehen der weitreichenden Auswirkungen auf PKI-Systeme

Praktische Aufgaben:

- Implementierung von erweiterten Signature-Spoofing-Techniken
- Validierung und Verifikation manipulierter Zertifikatsketten
- Umfassende Demonstration der Sicherheitslücke und ihrer Auswirkungen

5 Container-Management und Troubleshooting

5.1 Grundlegende Docker-Befehle

Wichtig: Führen Sie alle Befehle im Verzeichnis `curveball-ctf/` aus.

5.1.1 Challenge stoppen

```
docker-compose down
```

5.1.2 Container neu starten

```
docker-compose restart
```

5.1.3 Logs anzeigen

```
# Alle Logs anzeigen
docker-compose logs -f

# Nur Webserver-Logs anzeigen
docker-compose logs -f webserver
```

5.1.4 Container-Status überprüfen

```
docker-compose ps
```

5.1.5 Komplette Neuinstallation

```
# Container stoppen und entfernen
docker-compose down --volumes --remove-orphans

# Images neu erstellen und starten
docker-compose up --build -d
```