Request for Proposal (RFP): External Security Audit

Solana Wagering Smart Contract System

Project Overview

We are seeking an experienced security auditing firm to conduct a comprehensive security audit of our Solana-based wagering smart contract system. The system implements a competitive FPS game with Win-2-Earn mechanics where players stake tokens in matches and the winner takes all.

System Description

Core Functionality:

- Game session creation and management (1v1, 3v3, 5v5 modes)
- SPL token escrow system for player stakes
- Automated payout distribution to winning teams
- Pay-to-spawn mechanics for additional respawns
- Emergency refund system for incomplete games

Technology Stack:

- **Blockchain:** Solana
- **Framework:** Anchor (Rust)
- **Token Standard:** SPL Token
- **Program ID:** 8PRQvPo16yG8EP5fESDEuJunZBLJ3UFBGvN6CKLZGBUQ

Codebase Size: ~500 lines of Rust code across 6 instruction modules

Scope of Work

1. Security Audit Requirements

Critical Areas to Review:

- Authorization and access control mechanisms
- Token escrow and fund safety
- Arithmetic operations and overflow protection
- Input validation and sanitization
- Reentrancy and race condition vulnerabilities
- PDA (Program Derived Address) security
- Cross-program invocation (CPI) safety
- State management and consistency

Specific Functions to Audit:

- `create_game_session` - Game session initialization
- `join_user` - Player joining and token escrow
- `pay_to_spawn` - Additional token payments
- `record_kill` - Game state updates
- `distribute_winnings` - Payout distribution
- `refund_wager` - Emergency refund system

2. Deliverables Required

A. Comprehensive Audit Report (PDF)

- Executive summary with risk assessment
- Detailed findings with severity ratings (Critical/High/Medium/Low)
- Proof-of-concept exploits for identified vulnerabilities
- Recommended fixes with code examples
- Risk mitigation strategies
- Compliance with Solana security best practices

B. Technical Documentation

- Vulnerability database with CVE-style entries
- Attack vectors and exploitation scenarios
- Code quality assessment
- Performance and gas optimization recommendations

C. Test Cases and Validation

- Unit tests for identified vulnerabilities
- Integration tests for complex attack scenarios
- Fuzz testing results
- Penetration testing methodology

D. Remediation Support

- GitHub Issues/PRs with suggested fixes
- Code review of implemented fixes
- Follow-up validation testing
- Security training materials

3. Timeline and Milestones

Phase 1: Scoping and Onboarding (Week 1)

- Project kickoff meeting
- Codebase review and understanding
- Threat model development
- Testing environment setup

Phase 2: Manual Code Review (Week 2-3)

- Line-by-line code analysis
- Architecture review
- Design pattern analysis
- Dependency security assessment

Phase 3: Automated Analysis (Week 3-4)

- Static analysis tool execution
- Dynamic analysis and fuzzing
- Formal verification (if applicable)
- Penetration testing

Phase 4: Report Generation (Week 4-5)

- Draft report preparation
- Client review and feedback
- Final report delivery
- Presentation and walkthrough

Phase 5: Remediation Support (Week 5-6)

- Fix implementation review
- Validation testing
- Final security assessment
- Knowledge transfer

Eligibility Requirements

1. Technical Expertise

- **Required:** 3+ years of Solana smart contract auditing experience
- **Required:** 5+ years of blockchain security experience
- **Required:** Rust programming language expertise
- **Required:** Anchor framework knowledge
- **Preferred:** Experience with gaming/DeFi protocols
- **Preferred:** Formal verification experience

2. Past Experience

- **Required:** 10+ completed Solana smart contract audits
- **Required:** Public audit reports for similar projects
- **Required:** References from previous clients
- **Preferred:** Experience with token escrow systems
- **Preferred:** Experience with multi-party protocols

3. Team Composition

- **Required:** Senior security engineer with Solana expertise
- **Required:** Rust developer with security focus
- **Required:** Blockchain security researcher
- **Preferred:** Formal verification specialist
- **Preferred:** Penetration testing expert

Evaluation Criteria

1. Technical Competency (40%)

- Depth of Solana security knowledge
- Quality of past audit reports
- Understanding of complex attack vectors
- Ability to identify novel vulnerabilities

2. Methodology and Process (25%)

- Comprehensive audit methodology
- Use of advanced testing tools
- Systematic approach to vulnerability discovery
- Quality of documentation and reporting

3. Experience and References (20%)

- Relevant past experience
- Client references and testimonials
- Track record of finding critical vulnerabilities
- Industry recognition and reputation

4. Timeline and Cost (15%)

- Ability to meet project timeline
- Competitive pricing
- Resource allocation and availability

- Value for money

Submission Requirements

1. Technical Proposal

- Detailed audit methodology
- Team composition and qualifications
- Tools and techniques to be used
- Risk assessment approach
- Quality assurance processes

2. Past Work Examples

- 3-5 relevant audit reports (anonymized if necessary)
- Case studies of complex vulnerability discoveries
- References from previous clients
- Certifications and credentials

3. Project Plan

- Detailed timeline with milestones
- Resource allocation and team structure
- Communication and reporting schedule
- Risk mitigation strategies

4. Cost Breakdown

- Fixed price for complete audit
- Cost breakdown by phase
- Additional services and pricing
- Payment terms and schedule

Technical Specifications

1. Codebase Access

- **Repository:** Private GitHub repository
- **Access:** Read-only access for audit team
- **Documentation:** Comprehensive README and inline comments
- **Dependencies:** Cargo.toml with all dependencies listed

2. Testing Environment

- **Network:** Solana devnet/testnet
- **Tools:** Anchor CLI, Solana CLI
- **Tokens:** Test SPL tokens provided
- **Accounts:** Test keypairs provided

3. Reporting Standards

- **Format:** PDF with searchable text
- **Structure:** Executive summary, detailed findings, recommendations
- **Severity:** CVSS-style severity ratings
- **Code Examples:** Syntax-highlighted code snippets
- **Diagrams:** Attack flow diagrams where applicable

Security Requirements

1. Confidentiality

- **NDA:** Required for all team members
- **Data Handling:** Secure storage and transmission
- **Access Control:** Limited access to sensitive information
- **Retention:** Secure disposal after project completion

2. Independence

- **Conflict of Interest:** No prior relationship with development team
- **Objectivity:** Unbiased assessment and reporting
- **Transparency:** Clear methodology and findings
- **Integrity:** Honest and accurate reporting

Success Metrics

1. Vulnerability Discovery

- **Critical:** 0 vulnerabilities in production
- **High:** <5 high-severity vulnerabilities
- **Medium:** <10 medium-severity vulnerabilities
- **Coverage:** 100% of codebase reviewed

2. Quality Assurance

- **Accuracy:** 95%+ accuracy in vulnerability identification

- **Completeness:** All attack vectors identified
- **Clarity:** Clear and actionable recommendations
- **Timeliness:** On-time delivery of all milestones

Budget and Timeline

1. Budget Range

- **Minimum:** $15,000
- **Maximum:** $50,000
- **Preferred:** $25,000 - $35,000

2. Timeline

- **Start Date:** January 2025
- **Duration:** 6 weeks
- **Delivery:** February 2025

Submission Instructions

1. Submission Deadline

- **Proposal Due:** December 31, 2024
- **Questions Due:** December 20, 2024
- **Response Time:** 3 business days

2. Submission Format

- **Email:** audit-rfp@company.com
- **Subject:** "Solana Wagering Contract Audit Proposal"
- **Format:** PDF attachment with supporting documents
- **Size Limit:** 10MB total

3. Required Information

- Company name and contact information
- Team member profiles and qualifications
- Technical proposal (5-10 pages)
- Past work examples (3-5 reports)
- Cost breakdown and timeline
- References (3-5 clients)

Questions and Clarifications

For questions about this RFP, please contact:

- **Email:** audit-questions@company.com
- **Phone:** +1-555-0123
- **Response Time:** 24 hours

Evaluation Process

1. Initial Review (Week 1)

- Proposal completeness check
- Technical qualification review
- Reference verification
- Cost and timeline assessment

2. Technical Evaluation (Week 2)

- Methodology review
- Past work analysis
- Team qualification assessment
- Technical interview (if needed)

3. Final Selection (Week 3)

- Scoring and ranking
- Client presentation
- Contract negotiation
- Project kickoff

Terms and Conditions

1. Intellectual Property

- Audit reports become property of client
- Auditor retains right to use methodology
- Confidentiality obligations apply
- No reverse engineering of client code

2. Liability and Insurance

- Professional liability insurance required
- Errors and omissions coverage

- Cyber liability insurance
- Indemnification clauses

3. Payment Terms

- 50% payment on contract signing
- 30% payment on draft report delivery
- 20% payment on final report acceptance
- Net 30 payment terms

RFP Issued: December 2024
Project Start: January 2025
Expected Completion: February 2025
Contact: audit-rfp@company.com