# Penetration Testing Reconnaissance Report: Rockstar Games

**OSINT and Passive Footprinting** |

Target | rockstargames.com |

## 1. Executive Summary

***For Non-Technical Management***

This report summarizes the first phase of our security test, called **Reconnaissance** (or intelligence gathering).

**The Good News:** The primary website's core setup is strong; we couldn't find any easy, forgotten domains using standard IP checks.

**The Key Finding:** By analyzing the main website's security certificate (the 'digital ID'), we discovered a large and critical list of hidden systems the company uses. These include private internal tools, unreleased staging websites, and API systems used by mobile apps.

**Overall Recommendation:** The focus of our next phase must immediately shift to testing these newly discovered systems—especially the mobile API and internal content management systems (CMS)—as they represent the biggest opportunity for security flaws.

## 2. Scope and Objectives

### What We Tested

- **Primary Target:** The main domain rockstargames.com.
- **Expanded Scope:** All subdomains and associated domains identified during the passive analysis.

### What We Were Trying to Find

1. **Expand the Attack Surface:** Find all associated domains and subdomains the company owns.
2. **Identify Hidden Systems:** Locate high-value targets like Content Management Systems (CMS), Mobile APIs, and staging environments.
3. **Gather Intelligence:** Collect publicly available data (employee names, email patterns) for potential social engineering or credential testing.

## 3. Methodology

***Simple Explanation of the Steps***

We only used public, non-intrusive methods (like searching public records and using opensource tools) that leave no trace on the target's network.

| Step | Tool/Method Used | Why We Used It (Purpose) |
|---|---|---|
| A. Core DNS Mapping | Standard Lookup Tools (nslookup) | To find the Name Servers (NS) and their IP addresses, which tell us where the domain is hosted. |
| B. Reverse IP Lookup | dnsrecon -t rvl | To check if the name server's IP address is sharing its network block with any other, potentially forgotten, websites. |
| C. SSL Certificate Analysis | openssl s_client | To read the main website's security certificate, which lists every other system it is authorized to secure (Subject Alternative Names, or SANs). This was the most critical step. |
| D. Social Media Footprinting | Google Dorking (site:linkedin.com) | To find employee names and job titles (especially IT/Security) that are publicly listed, which helps us infer email patterns. |

## 4. Findings and Vulnerabilities

The problems we found are not direct "hacks," but rather exposures that will make the next phase of testing much easier and more impactful.

| ID | Finding/Exposure | Category | Severity | Impact |
|---|---|---|---|---|
| F-01 | Exposed Internal Systems (Staging/EAA) | Infrastructure Exposure | High | These are systems that often skip full security checks. If breached, they could expose code, data, or even be used as a pivot point to reach the live production network. |
| F-02 | Identified CMS and API Endpoints | Web Application Exposure | High | Subdomains like cms-prod and mobileapi are direct application entry points. Flaws here could lead to data theft, control over website content, or unauthorized account access. |
| F-03 | Brand and Game Domain Sprawl | Attack Surface Expansion | Medium | We found numerous associated domains (reddeadonline.com, lifeinvader.com, etc.). Each one is a new, separate target that must be checked for vulnerabilities. |
| F-04 | Employee Email Pattern Inferred | Credential Harvesting Risk | Medium | By finding employee names and roles, we confirmed a standard email format (e.g., first.last@rockstargames.com). This makes a password spraying attack highly efficient. |

## 5. Risk Assessment

We assess the risk based on Likelihood (how easy it is to exploit) and Impact (how much damage it could cause).

| Finding ID | Likelihood | Impact | Overall Risk | Simple Explanation |
|---|---|---|---|---|
| F-01 (Staging/EAA) | High | High | CRITICAL | If an internal/staging system is found, it's often an easy, high-value target. |

| | | | | |
|---|---|---|---|---|
| F-02 (API/CMS) | Medium | High | HIGH | These are custom applications. They are designed to be public-facing, but if they contain common flaws (like weak password reset), the impact is severe. |
| F-04 (Email Pattern) | High | Medium | MEDIUM | It's easy to guess emails, but the only impact is making password guess attempts more efficient. |

# 6. Recommendations

The primary recommendations are to harden the discovered systems and authorize the next testing phase immediately.

| Priority | Recommendation | Simple Action to Take |
|---|---|---|
| 1. CRITICAL | Harden Staging/Internal Sites (F-01) | Immediately put any internal or staging sites (eaa, dev) behind a VPN or internal firewall. They should not be reachable from the public internet. |
| 2. HIGH | Targeted API Audit (F-02) | Focus the next security audit exclusively on the mobileapi and cms-prod endpoints. Check for issues like missing rate limiting and insecure access controls. |
| 3. MEDIUM | Review Brand Domain Security (F-03) | Ensure all newly discovered brand domains have the same level of security patching and monitoring as the main rockstargames.com site. |

# 7. Evidence and Documentation

## SSL Certificate SAN (Subject Alternative Name) Extraction

**Proof:** The following data was extracted directly from the main domain's security certificate, proving ownership and active use of these systems.

| High-Priority Subdomains | Associated Brand/Game Domains |
|---|---|
| cms-prod.ros.rockstargames.com | reddeadonline.com |
| mobileapi.rockstargames.com | lifeinvader.com |
| support-eaa.rockstargames.com | thediamondcasinoandresort.com |
| www-eaa.rockstargames.com | wheelerrawson.com |
| cdn.sc.rockstargames.com | circolocorecords.com |
| graph.rockstargames.com | themusiclocker.com |

## Technical Suffix Explanation

The suffixes used on the discovered subdomains provide critical technical clues:

- **-prod** (e.g., cms-prod): This stands for **Production**. This is the live, active system that updates content for the public.
- **-eaa** (e.g., www-eaa): This is highly likely an internal code for **Staging, Development, or Quality Assurance (QA)** environments. These systems are used for testing changes before they go live and are historically less secure than the main production environment.

## 8. Remediation Plan

This is a proposed plan. Responsible parties and exact dates will be finalized after the Vulnerability Assessment phase is complete.

| Finding | Remediation Action | Responsibility | Proposed Deadline |
|---|---|---|---|
| F-01 (Staging/EAA) | Implement mandatory VPN access or strict IP whitelisting for all staging domains. | Network Operations / Security Team | 2 Weeks |
| F-02 (API/CMS) | Begin targeted API security review and implement rate limiting on all login endpoints. | Development Team | 4 Weeks |
| F-03 (Domain Sprawl) | Conduct a full asset inventory of all 30+ discovered domains to ensure consistent security policy. | Security Team | 3 Weeks |

## 9. Distribution and Confidentiality

This report contains highly sensitive information regarding the network architecture and potential security exposures.

- **Distribution:** Restricted to$$List authorized management/security personnel$$ .
- **Confidentiality:** This document is classified as **"Strictly Confidential"** and must not be shared externally under any circumstances.

## 10. Appendix: Technical Evidence Log

This appendix serves as a direct reference to the raw output and visual evidence collected during the reconnaissance phase, originally found in the Project _Reconnaisance.pdf.

| **Evidence Marker** | **Methodology Step** | **Technical Proof Provided** | **Supporting Finding** |
|---|---|---|---|
| **Screenshot 1** (DNS Lookup) | A. Core DNS Mapping | Proof of nslookup command execution showing the primary IP address (2.22.14.160) and authoritative Name Servers. | General Footprinting |

| | | | |
|---|---|---|---|
| **Screenshot 2** (WHOIS Data) | Passive Footprinting | Output of the whois lookup, confirming domain registrar, creation, and expiration dates. | General Footprinting |
| **Screenshot 3** (Wayback Machine) | Passive Footprinting | Screenshot showing historical captures of the target site, used for identifying previous changes and forgotten pages. | F-03 (Domain Sprawl) |
| **Screenshot 4** (TheHarvester) | D. Email Harvesting | Screenshot from theHarvester tool, used for extracting public employee names and email patterns (e.g., first.last@rockstargames.com). | F-04 (Email Pattern) |
| **Screenshot 5** (Social Media) | D. Social Media Footprinting | Screenshot of the official social media profile (e.g., Instagram), used for finding associated domains and branding intelligence. | F-03 (Domain Sprawl) |

| | | | |
|---|---|---|---|
| **Screenshot 6** (DNS Recon) | B. Reverse IP Lookup | Output from dnsrecon -t rvl command, demonstrating the check for cohosted or forgotten | General Footprinting |
| | | domains on the same IP block. | |