[pentesting uk]
PENETRATION TESTING SERVICES in partnership with Securious Limited.

Executive Security Assessment Report

1. DOCUMENT CONTROL

1.1 PentestingUK/Securious Limited

Name	Title
Pete Woodward	Director
Ben Strudwick	Cyber Security Consultant
Jack Best	Cyber Security Consultant

1.2 Payrun

Name	Title
Tim Vaines	Technical Director

1.3 Revision History

Status	Version	Name	Date
Draft	0.1	Ben Strudwick	19/11/2018
Quality Assurance	0.2	QA Reviewed	19/11/2018
Issued	1.0	Pete Woodward	19/11/2018

Contents

2 Testing Scope

The scope of this assessment was provided by client technical personnel to PentestingUK and consisted of a penetration test against Payrun's 2 external web applications as defined in Scope.

Scope

URL:	Description:
Developer.payrun.io	Web application portal
Api.payrun.io	Web API
Api.test.payrun.io	Web API

The results of the testing activities enacted against this application stack are detailed in Section 4 of this document, and accompanying Nessus & Burp Suite detailed technical reports.

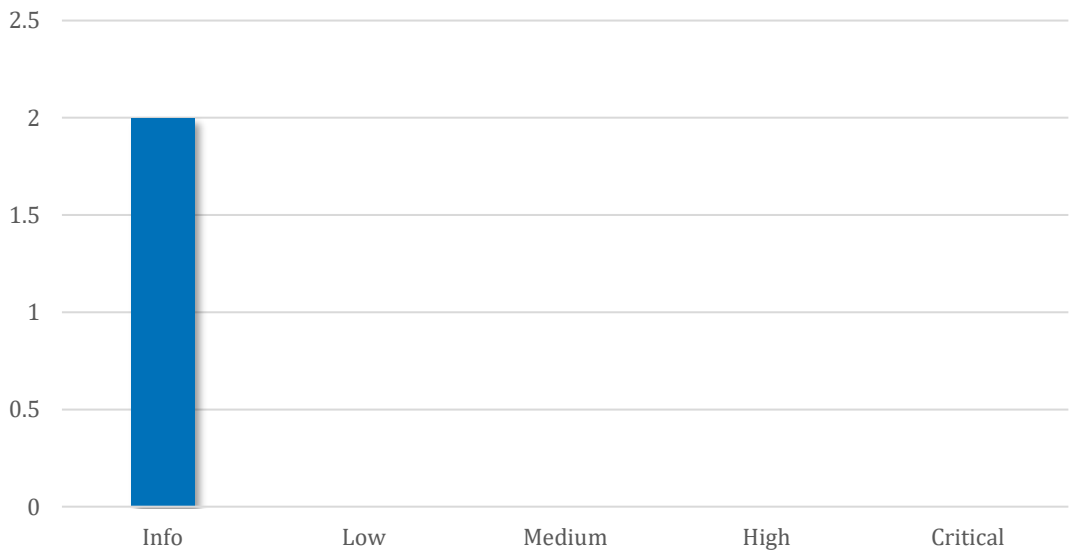
3 Executive Summary

PentestingUK was commissioned to conduct a penetration test, on behalf of Payrun. The goal of such activities was to provide third party assurance that Payrun's 2 external web applications (as defined in the Scope) are adequately protected against unwarranted or unknown risk. Testing activities were conducted on site and from PentestingUK's remote secure office, utilising a combination of manual and automated tools.

Overall Risk Ranking – **NONE**

3.1 Overview of Vulnerabilities

Host Name	INFO	LOW	MEDIUM	HIGH	CRITICAL
api.developer.io	2	0	0	0	0
developer.payrun.io	2	0	0	0	0
TOTAL	2	0	0	0	0



The assessment activities conducted by PentestingUK on behalf of Payrun determined that the assessed web applications were not vulnerable to any of the OWASP 2017 Top 10 listed vulnerabilities.

Those vulnerabilities classified as Informational by PentestingUK should do not present any level of risk as a standalone vulnerability. Vulnerabilities classified as Informational severity may contain information which could be used to better assist an attacker but are not exploitable.

No remediation is required based on the findings of this report. Payrun may choose to review any Information vulnerabilities to ensure they are comfortable with the information discovered by PentestingUK.

3.2 OWASP Top Ten

The Ten Most Critical Web Application Security Risks

A1: Injection	*Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.*	Not vulnerable
A2: Broken Authentication	*Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.*	Not vulnerable
A3: Sensitive Data Exposure	*Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.*	Not vulnerable
A4: XML External Entities (XXE)	*Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.*	Not vulnerable
A5: Broken Access Control	*Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.*	Not vulnerable

A6: Security Misconfiguration	*Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched and upgraded in a timely fashion.*	Not vulnerable
A7: Cross-Site Scripting (XSS)	*XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.*	Not vulnerable
A8: Insecure Deserialization	*Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.*	Not vulnerable
A9: Using Components with Known Vulnerabilities	*Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defences and enable various attacks and impacts.*	Not vulnerable
A10: Insufficient Logging & Monitoring	*Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.*	Not vulnerable

4 Vulnerability Summary

The aim of the testing activities undertaken by PentestingUK was to determine if exploitable vulnerabilities exist within the assessed Payrun external web applications which may be used by an attacker to perform a variety of actions, namely:

- Obtaining privileged rights and permissions on assessed networks and websites;
- Installation of potentially malicious software on assessed networks and websites;
- Use of website as a pivot to attack other network hosts, segments, or users;
- System enumeration and data gathering.

PentestingUK conducted internal vulnerability testing activities against the web application defined within the Scope.

4.1 Definition of Vulnerabilities

PentestingUK's Vulnerability Assessment Criteria	The vulnerability ratings in this report are generated using the 'Common Vulnerability Scoring System' v3.0 (CVSSv3.0) which is an open framework for communicating the characteristics and severity of security vulnerabilities within computer systems.
CVSS Score	There are three metric groups for vulnerability assessment however the provided score is only a representation of the intrinsic values of the vulnerability and does not consider Temporal or Environmental factors. PentestingUK has however considered these metrics in our assessment and have communicated these within the report. Find the current specification linked here: https://www.first.org/cvss/cvss-v30-specification-v1.7.pdf
Critical (9.0-10.0)	Those vulnerabilities determined as being Critical by PentestingUK are those that can directly lead to host or data compromise. Critical vulnerabilities should be understood as having the largest combination of likelihood and impact upon operationally security.
High (7.0-8.9)	Significant vulnerabilities present a defined threat to operational performance or security integrity of assessed hosts. Exploitation of such vulnerabilities can lead to compromise of host (or host data) but typically only as a blended threat.
Medium (4.0-6.9)	Those vulnerabilities determined as being Medium by PentestingUK are those that can negatively affect regular system operations but either have a degree of difficulty in their execution or are unlikely to result in a total loss of availability, integrity or confidentiality.
Low (0.1-3.9)	If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
None (Informational) (0.0)	Vulnerabilities determined as being Informational in nature by PentestingUK are those that afford an attacker with limited host data that is typically required for operational purposes and has limited or no impact upon the security posture of an organisation.

4.2 Testing Overview

The security assessment activities enacted by PentestingUK utilise a variety of automated and manual processes to enact simulated attacks against assessed website. The aim is to determine the presence of vulnerabilities within the website that could be exploited by an attacker. Whilst such simulated attacks emulate the potential actions of an attacker they are not designed to be disruptive and result in loss of system availability, data, or cessation of normal host or network operations.

It should be noted that the activities performed by PentestingUK are not designed to be stealthy in nature and are performed in such a manner as to make such attacks easy to detect and respond to for network operations personnel. No attempts are made to obfuscate attack origins or activities during the compressed time window available to the assessment process.

It should also be noted that any assessment activities performed only reflect the vulnerability exposure of an organisation at the time of test, and that additional vulnerabilities may subsequently arise following assessment completion. Every effort is made to ensure that assessment resources are up to date as of the time of assessment, and that all public exploit data is utilised as part of the engagement process. In addition, every effort is made to determine those vulnerabilities that present an imminent, goal focused risk to the security posture of an organisation, however no warranty should be inferred as additional vulnerabilities within the estate may not have been detected during the time compressed assessment cycle.

[REPORT ENDS]