INTIGRITI

Example Comp. Inc.

Hybrid Penetration Test Results

Letter of Attestation

Creation Date: January 1st, 2024

Table of Contents

Introduction

This document is created as evidence and audit proof for our customer Example Comp. Inc explaining the results of their Hybrid Penetration Test via the Intigriti platform.

Intigriti is a cloud solution, providing an ethical hacking platform to companies that desire a structured Bug Bounty & Hybrid Penetration Test.

Intigriti's Hybrid Penetration Test is delivered via the crowdsourced security platform allowing vetted security researchers to engage and communicate with companies quickly, safely, and reliably, offering live updates and communication about found vulnerabilities.

Based on the customer's predefined scope of the Hybrid Penetration Test program, a hand-picked researcher has searched for vulnerabilities and reported their findings through Intigriti's platform.

Benefits of Hybrid Pentesting

Pentest with Bug Bounty benefits
Methodology of a traditional pentest, but with the motivation, reporting, triage and rewards of a Bug Bounty program

Specialised skills
Hybrid penetration testers are hand-picked; selection is based on researcher specialism and activity as well as test criteria

Transparent researcher selection
Testers are based on previous ratings, quality, motivation, expertise, skillset

Work with experts in your field
Fintech, Retail, E-commerce, Media, Health, etc.

Highly motivated testers
Researcher receives an effort-based fee based and a capped bounty fee on top for all accepted submissions

Data-driven platform benefits
All submissions are real-time reported via the Intigriti platform

Executive Summary

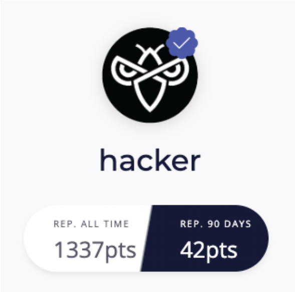
In December 2023, Example Comp. Inc. engaged Intigriti to perform a hybrid penetration test with one of Intigriti's vetted researchers eligible for pentests (see researcher information below).

The hybrid pentest was executed as a black-box assessment, meaning that no access to source code was available. The Intigriti researcher had direct 24/7 access to communication with the Example Comp. Inc. security and development team.

A total of 18 findings was reported during the assessment including 1 high, 5 critical and 2 exceptional vulnerabilities The key issues found would have allowed an attacker to fully compromise an admin user, gaining full access to PII data. Additionally, the integrity of all users could have been affected by changes performed via the admin account.

The Example Comp. Inc. team, together with Intigriti has identified all steps needed to remediate the found issues. Software fixes will be implemented in-line with the Example Comp. Inc. vulnerability remediation program.

Researcher information



hacker

REP. ALL TIME 1337pts

REP. 90 DAYS 42pts

Name:	hacker
Current Intigriti Ranking:	#1
Reputation All Time:	1337pts
Current Submission Streak:	Exceptional
Country:	Belgium
ID Checked:	Yes

Profile: https://app.intigriti.com/profile/hacker

Scope

The scope was selected by Example Comp. Inc. and reviewed by the Intigriti team.

Assets In Scope

Domains
www.example.com/*
www.example2.com/users/*
www.subdomain1.example.com/*
www.subdomain2.example.com/*

Android Applications
com.example.androidapplication

A special test focus was requested by the Example Comp. Inc. team:

- Test if lower privileged roles can get access to admin functionality
- Test if previous cross-site scripting vulnerabilities on example.com have been remediated
- Test if authentication on Android application can be bypassed

Timeframe

This Intigriti Hybrid Penetration Test was executed during the period of December 1st 2023 to December 30th 2023. A total amount of 120 hours was performed testing all Example Comp. Inc. assets in scope.

Results Summary

The high-level results of the test can be found in this document, further details can be shared at the discretion of Example Comp. Inc.

Overview

During the defined testing period, there were 18 vulnerabilities reported of which 18 vulnerabilities were unique and accepted in the Example Comp. Inc. Hybrid Penetration test program.

The total number of accepted vulnerabilities and their severity per asset in scope can be found in the table below:

Asset in Scope	Info	Low	Medium	High	Critical	Exceptional	Σ
https://example.com	0	2	2	0	3	1	8
www.subdomain1.example.com/*	0	0	4	1	1	0	6
com.example.androidapplication	0	2	0	0	1	1	4
Total	0	4	6	1	5	2	18

The breakdown per vulnerability type yielded this result:

Vulnerability Type	Info	Low	Medium	High	Critical	Exceptional	Σ
Vertical Privilege Escalation	0	0	0	0	0	2	2
Blind SQL-Injection	0	0	0	0	1	0	1
Unauthenticated access to public MongoDB instance	0	0	0	0	1	0	1
Insecure Direct Object Reference	0	0	0	0	3	0	3
Subdomain Takeover via dangling DNS record	0	0	0	1	0	0	1
Business Logic Error	0	0	1	0	0	0	1
Improper Access Control	0	0	1	0	0	0	1
Stored Cross-Site Scripting	0	0	4	0	0	0	4
Broken Access Control	0	1	0	0	0	0	1
Sensitive Data Exposure	0	1	0	0	0	0	1
Security Misconfiguration	0	1	0	0	0	0	1
Path Traversal	0	1	0	0	0	0	1
Total	0	4	6	1	5	2	18

Finding Details

Type:	Vertical Privilege Escalation
Severity:	Exceptional
Code:	EX001
Reported Impact:	User role “viewer” can become an admin by setting “rolePermMatrix” POST parameter to 1 within user administration settings. Admin role can be used to obtain access to and change all user data.

Type:	Vertical Privilege Escalation
Severity:	Exceptional
Code:	EX002
Reported Impact:	Admin privileges can be obtained for the user role “guest” by modifying a cookie set upon the site’s first visit. This results in the ability for any guest user to impact the data on the platform.

Type:	Blind SQL-Injection
Severity:	Critical
Code:	EX003
Reported Impact:	An attacker can dump all data from the database.

Type:	Unauthenticated access to public MongoDB instance
Severity:	Critical
Code:	EX004
Reported Impact:	An attacker can anonymously login to the publicly exposed MongoDB instance to get access to all data.

Type:	Insecure Direct Object Reference
Severity:	Critical
Code:	EX005
Reported Impact:	An attacker can get access to any user’s personal records.

Type:	Insecure Direct Object Reference
Severity:	Critical
Code:	EX006
Reported Impact:	Confidential support chat transcripts can be retrieved by an attacker by modifying the URL.

Type:	Insecure Direct Object Reference
Severity:	Critical
Code:	EX007
Reported Impact:	By modifying the request sent to pull inventory data, an attacker can gain access to the inventory back-end database.

Type:	Subdomain Takeover via dangling DNS record
Severity:	High
Code:	EX008
Reported Impact:	Controlling the subdomain, an attacker is able to serve malicious content trusted by company users, using the domain for phishing purposes or e.g. for stealing session cookies enabling account takeovers.

Type:	Business Logic Error
Severity:	Medium
Code:	EX009
Reported Impact:	2FA TOTP token is not bound to user allowing an attacker to create a valid token to log in.

Type:	Improper Access Control
Severity:	Medium
Code:	EX010
Reported Impact:	An attacker can use all endpoints under /api/example/read/* without having the right permission group set.

Type:	Stored Cross-Site Scripting
Severity:	Medium
Code:	EX011
Reported Impact:	An attacker can use this XSS vulnerability to post victim’s private information as a comment in thread functionality.

Type:	Stored Cross-Site Scripting
Severity:	Medium
Code:	EX012
Reported Impact:	The XSS vulnerability can be used to run malicious Javascript within the browser, by exploiting the commenting functionality.

Type:	Stored Cross-Site Scripting
Severity:	Medium
Code:	EX013
Reported Impact:	The commenting functionality can be exploited by the attacker to send malicious Javascript to any user browsing the site.

Type:	Stored Cross-Site Scripting
Severity:	Medium
Code:	EX014
Reported Impact:	Client-side scripts can be used to steal customer’s cookies and personal information.

Type:	Broken Access Control
Severity:	Low
Code:	EX015
Reported Impact:	Attacker can get information if a certain email address has already registered a user.

Type:	Sensitive Data Exposure
Severity:	Low
Code:	EX016
Reported Impact:	Stacktrace exposes the tech stack and plugins used by the application.

Type:	Security Misconfiguration
Severity:	Low
Code:	EX017
Reported Impact:	CAPTCHA can be bypassed by setting setting “valid” parameter to “true”.

Type:	Path Traversal
Severity:	Low
Code:	EX018
Reported Impact:	Attacker can upload arbitrary files to any location.

Methodology

Depending on the scope of the assessment, Intigriti's vetted researcher base is following the methodologies and standards discussed in this chapter.

Web application

During the security assessment of a web application, an extensive range of vulnerabilities is tested for, including those defined in the OWASP Top 10 – 2021:

- A01:2021-Broken Access Control
- A02:2021-Cryptographic Failures
- A03:2021-Injection
- A04:2021-Insecure Design
- A05:2021-Security Misconfiguration
- A06:2021-Vulnerable and Outdated Components
- A07:2021-Identification and Authentication Failures
- A08:2021-Software and Data Integrity Failures
- A09:2021-Security Logging and Monitoring Failures
- A10:2021-Server-Side Request Forgery

A common methodology that is followed is the OWASP Web Security Testing Guide.

API

For the security assessments of API's, the focus of testing lies on the security vulnerabilities defined in the OWASP API Top 10 - 2019:

- API1:2019-Broken Object Level Authorization
- API2:2019-Broken User Authentication
- API3:2019-Excessive Data Exposure
- API4:2019-Lack of Resources & Rate Limiting
- API5:2019-Broken Function Level Authorization
- API6:2019-Mass Assignment
- API7:2019-Security Misconfiguration
- API8:2019-Injection
- API9:2019-Improper Assets Management
- API10:2019-Insufficient Logging & Monitoring

Mobile application

During the security assessment of mobile applications, the OWASP MAS checklist and the OWASP Mobile Application Security Testing Guide play a predominant role in test coverage. These include vulnerabilities out of the following categories:

- Architecture, Design and Threat Modelling
- Data Storage and Privacy
- Cryptography
- Authentication and Session Management
- Network Communication
- Platform Interaction
- Code Quality and Build Setting
- Resilience

Submissions

Each submission gets triaged by Intigriti’s in-house team to validate the proof of concept and ensure that the submission can be replicated.

Scoring the severity of submissions:

Intigriti’s severity scoring system is based on the CVSSv3 scoring system together with business impact factors that are determined during the scoping phase of the engagement.

Contact us| Visit intigriti.com | Request a demo