breachlock

CONFIDENTIAL

BackNine Insurance and Financial Services

(Sep 15th, 2021 To Sep 24th, 2021)

PENETRATION CLEAN REPORT

Disclosure Statement

This document contains sensitive information about the computer security environment, practices, and current vulnerabilities and weaknesses of the client's security infrastructure as well as priopretary tools and methodologies used by BreachLock. This document is subject to the terms and conditions of a non- disclosure agreement between BreachLock and the client.

Document Information

Engagement scope	Project ID
1 asset(s)	BLP1140-JUL29-BAC
Engagement Timeframe	**Pentest ID**
Sep 15th, 2021 to Sep 24th, 2021	BLP-2938

This retest report is limited towards validation of the vulnerabilities that were all-ready discovered in the previous Penetration Test. No additional attempts were made to find new vulnerabilities that may have been introduced due to the addition of new code or changes. If the period between your initial test and retest is greater than 90 days, we strongly advise requesting a fresh penetration test to get a realistic validation of your current security posture.

Version History

Version	Date	Author/Reviewer	Comment
0.1	Sep 15th, 2021	BreachLock	Initial Report
0.2	Sep 24th, 2021	BreachLock	QA
1.0	Sep 24th, 2021	BreachLock	Final Report

Table Of Contents

A. Assessment Scope

API Scan Penetration Testing Retest

Organization	BackNine Insurance and Financial Services
Methodology	Gray Box
Timeline	Sep 15th, 2021 To Sep 24th, 2021
Asset(s)	https://api-staging.back9ins.com/

B. Executive Summary

The BreachLock penetration testing and ethical hacking team conducted an **API Scan** Penetration Retest against the hosts given by **BackNine Insurance and Financial Services**. The security assessment took place over the period of one day, the, **Sep 15th, 2021 until Sep 24th, 2021** from **BreachLock.**

The main goal of this assessment was to ensure that appropriate information security controls are implemented within the network and host environment to preserve the integrity, confidentiality and availability of its information and computing resources.

Pen Testing team that participated in this project has the following global certifications:
CEH, OSCP, OSCE, CREST PT, SANS GSNA

During the assessment, we have identified that the asset was secured well. No vulnerabilities were found during this assessment.

C. Testing Methodology

1. Introduction

Penetration testing methodologies vary depending on goals, scope and customers' specific requirements. BreachLock has adopted the best industry standards for testing - like OWASP plus developed techniques and methodologies based on our own experiences.

The penetration testing team used the following main methodologies depending on the requirements:

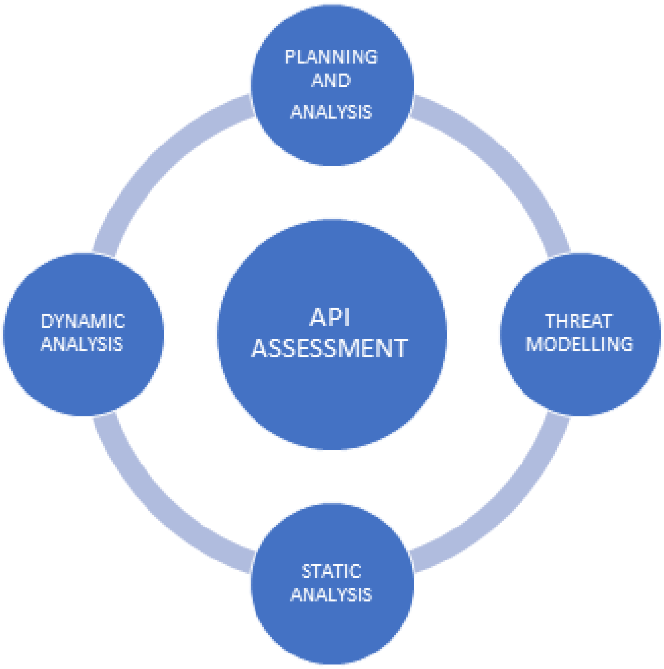
- **Black Box** having the following characteristics:
  - The penetration testing team does not possess any initial knowledge about the target environment.
  - Usually, the customer provides an IP address, URL or domain addresses as a starting point for the test.
  - The team emulates typical attackers' actions who do not know the environment (operating systems, network services, applications operations, network topology, etc.).
  - Black Box testing is the most common methodology for the tests of external facing systems and applications (like DMZ network and internet applications).
  - One of the critical factors in this methodology is gathering any available information about the target environment. Passive techniques are used such as:
    - Passive intelligence gathering, collecting an information about application, technologies, frameworks and APIs.
    - Active environment analysis: DNS enumeration, network scanning, port/ service probing, port scanning, application scanning, OS fingerprinting, or website spidering.

      Penetration testing team can use socio-technical attacks if the client approves.
  - Next stage of the test is identification and analysis of possible vector attacks against tested system or application if enough information is already available. The penetration testing team uses fuzzing, analysis or requests and responses to/ from tested system, and performs manual testing.
  - PT team verifies detected vulnerabilities to eliminate false positives.
  - PT team can attempt to exploit vulnerabilities, elevate privileges and attack other parts of the system if customer approves and contractual provisions allow.
  - Afterwards, a detailed and comprehensive report is prepared (and undergoes QA) which lists all problems found and suggests fixes for each one.

- **White Box (Crystal Box)** having the following characteristics:
  - The customer furnishes detailed information about their system, usually as documentation or interviews with those (developers, system/ application administrators or IT architects) who know the infrastructure.
  - The test emulates possible actions performed by an attacker having in- depth knowledge about the target (i.e., Advanced Persistent Threat, attacks perpetrated by current or former employees/contractors).
  - Reconnaissance and intelligence gathering is reduced compared to Black Box or Gray Box methodologies.
  - False positives could be confirmed after review of a part of the source code (when source code is available for the PT team).
  - Other phases of the testing are common in Blackbox and Whitebox (the main difference is the amount of knowledge about the target system).
- **Gray Box** having the following characteristics:
  - This is a concatenation of White Box/Black Box.
  - Basic authorization into the system is granted because the goal is to test internal system and elevate privileges if possible.
  - The testers can be provided with additional information about testing environment (highlevel design, services, protocols, etc.).
  - This methodology is the most common for the emulation of attacks against systems where non-privileged credentials or limited knowledge is available for an attacker.
  - Usually, this method is used to assess the security and effectiveness of controls of thirdparty applications.
  - This mode provides an additional advantage which is providing information about findings to a vendor. This cooperation enables performing further verification of findings and publishing security patches for the tested system (better than alternative workaround solutions mitigating existing risks).

2. API Penetration Testing

APIs are one of the favorite attack surfaces for cybercriminals, which they can use to gain further access to the application or server.
BreachLock follows a Four-step Methodology combining various reconnaissance and attack techniques to discover weaknesses in the target Application programing interface and simulate attack scenarios.



2.1 Planning And Analysis

In the first step, we analyse your documentation and identify various API end points to be tested. After initial analysis, we check all your endpoints to see if everything is working as mentioned in documentation.

2.2 Threat Modelling

As part of threat modelling, we model security assessments based on real-time threats and map your API accurately using API documentation.

2.3 Static Analysis

In this step, our security analyst analysis the API endpoints and locate exceptions, based on CERT secure standards. This process results in exposing any vulnerabilities or sensitive information that might be exploited by malicious attacks.

2.4 Dynamic Analysis

As a final step of testing, we perform a vulnerability test based on OWASP API Security project and evaluate the extent to which the identified vulnerabilities could cause losses and recommend steps to reproduce the vulnerabilities, which include following:

- 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

3. Vulnerabilities Classification

Classification methodology is based on OWASP Risk Rating Methodology. Each finding is analyzed in two aspects: likelihood and impact. Every factor of this aspect has a severity between 1 and 9.

Following factors describe likelihood:

- Threat Agent Factors: The first set of factors are related to the threat agent involved. The goal here is to estimate the likelihood of a successful attack by this group of threat agents. Use the worst-case threat agent.
    - Skill level: How technically skilled is this group of threat agents? Security penetration skills (9), network and programming skills (6), an advanced computer user (4), some technical skills (3), no technical skills (1)
    - Motive: How motivated is this group of threat agents to find and exploit this vulnerability? Low or no reward (1), possible reward (4), high reward (9)
    - Opportunity: What resources and opportunity are required for this group of threat agents to find and exploit this vulnerability? full access or expensive resources required (0), special access or resources required (4), some access or resources required (7), no access or resources required (9)
    - Size: How large is this group of threat agents? Developers (2), system administrators (2), intranet users (4), partners (5), authenticated users (6), anonymous Internet users (9)

- Vulnerability Factors: The next set of factors are related to the vulnerability involved. The goal here is to estimate the likelihood of the particular vulnerability involved being discovered and exploited. Assume the threat agent selected above.
    - Ease of discovery: How easy is it for this group of threat agents to discover this vulnerability? Practically impossible (1), difficult (3), easy (7), automated tools available (9)
    - Ease of exploit: How easy is it for this group of threat agents to exploit this vulnerability? Theoretical (1), difficult (3), easy (5), automated tools available (9)
    - Awareness: How well known is this vulnerability to this group of threat agents? Unknown (1), hidden (4), obvious (6), public knowledge (9)
    - Intrusion detection: How likely is an exploit to be detected? Active detection in application (1), logged and reviewed (3), logged without review (8), not logged (9)

Following factors describe possible impact:

- Technical Impact Factors: Technical impact can be broken down into factors aligned with the traditional security areas of concern: confidentiality, integrity, availability, and accountability. The goal is to estimate the magnitude of the impact on the system if the vulnerabilities were to be exploited.
    - Loss of confidentiality: How much data could be disclosed and how sensitive is it? Minimal non- sensitive data disclosed (2), minimal critical data disclosed (6),

extensive non- sensitive data disclosed (6), extensive critical data disclosed (7), all data disclosed (9)
    - Loss of integrity: How much data could be corrupted and how damaged is it? Minimal slightly corrupt data (1), minimal seriously corrupt data (3), extensive slightly corrupt data (5), extensive seriously corrupt data (7), all data totally corrupt (9)
    - Loss of availability: How much service could be lost and how vital is it? Minimal secondary services interrupted (1), minimal primary services interrupted (5), extensive secondary services interrupted (5), extensive primary services interrupted (7), all services completely lost (9)
    - Loss of accountability: Are the threat agents' actions traceable to an individual? Fully traceable (1), possibly traceable (7), completely anonymous (9)
- Business Impact Factors: The business impact stems from the technical impact, but requires a deep understanding of what is important to the company running the application. In general, you should be aiming to support your risks with business impact, particularly if your audience is executive level. The business risk is what justifies investments in fixing security problems. Many companies have an asset classification guide and/or a business impact reference to help formalize what is important to their business. These standards can help you focus on what's truly important for security. If these aren't available, then talk with people who understand the business to get their take on what's important. The factors below are common areas for many businesses, but this area is even more unique to a company than the factors related to threat agent, vulnerability, and technical impact.
    - Financial damage: How much financial damage will result from an exploit? Less than the cost to fix the vulnerability (1), minor effect on annual profit (3), significant effect on annual profit (7), bankruptcy (9)
    - Reputation damage: Would an exploit result in reputation damage that would harm the business? Minimal damage (1), Loss of major accounts (4), loss of goodwill (5), brand damage (9)
    - Non- compliance: How much exposure does non- compliance introduce? Minor violation (2), clear violation (5), high profile violation (7)
    - Privacy violation: How much personally identifiable information could be disclosed? One individual (3), hundreds of people (5), thousands of people (7), millions of people (9)

D. Vulnerabilities Details and Recommendations

During the assessment, it was observed that all the vulnerabilities found in previous pen test have been patched successfully.

breachlock

Find and Fix Your next Cyber Breach

https://www.breachlock.com

clientsupport@breachlock.com

https://twitter.com/breachlock