Michele Di Bonaventura

PENETRATION TESTER | OFFENSIVE APPLICATION SECURITY ENGINEER

Profile

Penetration Tester with 4+ years of hands-on experience. Secured applications for top-tier companies in finance, energy, technology, and government sectors. In love with Web (In)Security.

Employment History

Software Security Consultant, IMQ Minded Security, Milan (Remote)

JANUARY 2023 — PRESENT

- Conducted Web Application Penetration Tests (WAPTs) to identify and exploit vulnerabilities in web-based systems and applications.
- Executed Mobile Application Penetration Tests (MAPTs) to assess security weaknesses in Android applications.
- Performed Secure Code Reviews (SCR) to analyze source code for security flaws and provided actionable recommendations for secure coding practices.
- Produced detailed reports with top-notch technical writing, outlining findings, vulnerabilities, and recommended remediation strategies.
- Collaborated with cross-functional teams to ensure effective implementation of security measures and mitigation of identified risks.
- Contributed to the integration of security tests into the CI/CD pipeline for agile workflow, ensuring the seamless incorporation of security practices into the development lifecycle.

Penetration Tester, BIP, Rome

MAY 2021 — DECEMBER 2022

- Conducted Web Application Penetration Tests (WAPTs) to identify vulnerabilities and assess security risks in web-based systems and applications.
- Performed Network Penetration Tests (NPTs) to evaluate the security posture of network infrastructure and identify potential weaknesses.
- Conducted Vulnerability Assessments to proactively identify security gaps and recommend measures to strengthen overall security posture.
- Generated comprehensive reports detailing findings, vulnerabilities, and actionable recommendations for remediation.

Penetration Tester, Deloitte (Quantum Leap), Rome

FEBRUARY 2020 — APRIL 2021

- Conducted Web Application Penetration Tests (WAPTs) to identify vulnerabilities and assess security risks in web-based systems and applications.
- Developed custom security tools to streamline and enhance WAPT activities, enabling more efficient and effective vulnerability identification and exploitation.
- Consistently delivered comprehensive reports detailing findings and recommendations, enabling clients to enhance their web application security and mitigate potential risks effectively.

Details

dibonaventuramichele@gmail.com

Links

Security Blog

LinkedIn

GitHub

HackerOne

OpenBugBounty

Skills

Web Applications Security

Android Applications Security

iOS Appications Security

Linux Server Security

Windows and Active Directory Security

Scripting and custom tools writing

Languages

English

Italian

CVEs

CVE-2023-46456 - RCE in GL.iNet

In GL.iNET GL-AR300M routers with firmware 3.216 it is possible to inject arbitrary shell commands through the OpenVPN client file upload functionality.

CVE-2023-46455 - Arbitrary File Write in GL.iNet

In GL.iNET GL-AR300M routers with firmware v4.3.7 it is possible to write arbitrary files through a path traversal attack in the OpenVPN client file upload functionality.

CVE-2023-46454 - RCE in GL.iNet

In GL.iNET GL-AR300M routers with firmware v4.3.7, it is possible to inject arbitrary shell commands through a crafted package name in the package information functionality.

CVE-2021-36389 - IDOR in Yellowfin

In Yellowfin before 9.6.1 it is possible to enumerate and download uploaded images through an Insecure Direct Object Reference vulnerability exploitable by sending a specially crafted HTTP GET request to the page "MIImage.i4".

CVE-2021-36388 - IDOR in Yellowfin

In Yellowfin before 9.6.1 it is possible to enumerate and download users profile pictures through an Insecure Direct Object Reference vulnerability exploitable by sending a specially crafted HTTP GET request to the page "MIIAvatarImage.i4".

CVE-2021-36387 - Stored XSS in Yellowfin

In Yellowfin before 9.6.1 there is a Stored Cross-Site Scripting vulnerability in the video embed functionality exploitable through a specially crafted HTTP POST request to the page "ActivityStreamAjax.i4".

CVE-2020-12103 - Path Traversal in Tiny File Manager

In Tiny File Manager 2.4.1 there is a vulnerability in the ajax file backup copy functionality which allows authenticated users to create backup copies of files (with .bak extension) outside the scope in the same directory in which they are stored.

CVE-2020-12102 - Path Traversal in Tiny File Manager

In Tiny File Manager 2.4.1, there is a Path Traversal vulnerability in the ajax recursive directory listing functionality. This allows authenticated users to enumerate directories and files on the filesystem (outside of the application scope).

Achievements

PortSwigger Bug Bounty - Hackerone

DECEMBER 2021

Reported an IIS Tilde Enumeration / IIS Short Filename Disclosure vulnerability found on portswigger.net.

Conference Speaker - HackInBo Spring Edition 2023, Bologna

JUNE 2023

Presented a technical talk in HackInBo Spring Edition 2023 security conference titled "IIS Tilde Enumeration - an evergreen vulnerability".

Conference Speaker - OWASP Italy Day 2023, Milano

SEPTEMBER 2023

Presented a technical talk in OWASP Italy Day 2023 security conference titled "IIS Tilde Enumeration - an evergreen vulnerability".

Projects

Burp Extension - IIS Tilde Enumeration Scanner

DECEMBER 2021

A Burp extension to enumerate all the short names in an IIS webserver by exploiting the IIS Tilde Enumeration vulnerability.

https://portswigger.net/bappstore/523ae48da61745aaa520ef689e7503

3b

badmoodle

NOVEMBER 2021

A moodle community-based vulnerability scanner.

https://github.com/cyberaz0r/badmoodle

Certifications

eMAPT - eLearnSecurity Mobile Application Penetration Tester

MARCH 2021

https://verified.elearnsecurity.com/certificates/c9aa0f

bd-c7d7-4661-8ebf-c5a7e1d87553

Education

High School Diploma, ITGC Moretti, Abruzzo, Italy

SEPTEMBER 2012 — JUNE 2017

References

References available upon request