Michele Di Bonaventura

PENETRATION TESTER | OFFENSIVE APPLICATION SECURITY ENGINEER

Profile

Penetration Tester with 5+ years of hands-on experience. Secured applications for top-tier companies in finance, energy, technology, aviation and government sectors.

In love with Web (In)Security.

Employment History

Penetration Tester, Redigo Security, Stockholm

OCTOBER 2024 — 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 and iOS applications.
- Performed Thick Client Application Penetration Tests to detect vulnerabilities in Windows .NET and Java applications.
- Exploited LLM vulnerabilities in AI-powered features using prompt injection, knowledge-file exfiltration and workflow manipulation.
- Tested AWS S3 web endpoints for misconfigurations, including presigned URL flaws and permissive bucket policies.
- Produced detailed reports with top-notch technical writing, outlining findings, vulnerabilities, and recommended remediation strategies.
- Presented vulnerabilities to customers both on-site and remotely, showcasing impact through attack scenarios, exploits, and live demos to highlight potential real-world consequences.
- Configured firewall rules and compliance policies for hardening and securing internal Linux systems.
- Contributed to the company growth by designing architecture and build internal processes to improve productivity and automate tasks.

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

JANUARY 2023 — AUGUST 2024

- 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.
- Managed security tickets in JIRA throughout agile sprints, including triaging, updating, and collaborating with developers to resolve vulnerabilities within the SDLC.
- Led security discussions with development teams to ensure vulnerabilities were addressed before production, escalating critical issues to security managers when necessary.
- Integrated security testing into the CI/CD pipeline, performing continuous assessments during sprints and participating in weekly dev demos to mitigate risks.

Details

Stockholm, Sweden
dibonaventuramichele@gmail.com

Links

Security Blog

LinkedIn

GitHub

HackerOne

OpenBugBounty

Skills

- Web Application Security
- Android Application Security
- iOS Application Security
- Thick Client Application Security
- Linux Server Security
- AI and LLM Security
- Cloud Security
- Windows and Active Directory Security
- Scripting and custom tools writing

Languages

- English
- Italian
- Swedish
- Spanish

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.
- Led vulnerability management using Nessus and Qualys to scan networks, systems, and applications, analyzing results to prioritize and remediate vulnerabilities.
- 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.

CVEs

CVE-2024-35540 - Stored XSS in Typecho

A stored cross-site scripting (XSS) vulnerability in Typecho v1.3.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.

CVE-2024-35539 - Race Condition in Typecho

Typecho v1.3.0 was discovered to contain a race condition vulnerability in the post commenting function. This vulnerability allows attackers to post several comments before the spam protection checks if the comments are posted too frequently.

CVE-2024-35538 - Client IP Spoofing in Typecho

Typecho v1.3.0 was discovered to contain a Client IP Spoofing vulnerability, which allows attackers to falsify their IP addresses by specifying an arbitrary IP as value of X-Forwarded-For or Client-Ip headers while performing HTTP requests.

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).

Certifications

eMAPT - eLearnSecurity Mobile Application Penetration Tester

MARCH 2021

https://verified.elearnsecurity.com/certificates/c9aa0fbd-c7d7-4661-8ebf-c5a7e1d87553

Achievements

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".

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".

PortSwigger Bug Bounty - Hackerone

DECEMBER 2021

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

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/523ae48da61745aaa520ef689e75033b

badmoodle

NOVEMBER 2021

A moodle community-based vulnerability scanner.

https://github.com/cyberaz0r/badmoodle

Education

High School Diploma, ITGC Moretti, Abruzzo, Italy

SEPTEMBER 2012 — JUNE 2017

References

References available upon request