## Paper: Onderzoeksvoorstel

# Onderzoek naar penetratietesten binnen een webomgeving.

### Bachelorproef, 2023-2024

Levi Van Achter

E-mail: levi.vanachter@student.hogent.be
Project repo: https://github.com/LeviVanA/BPVoorstel_PenTest

## Samenvatting

Dit onderzoek richt zich specifiek op penetratietesten binnen een webomgeving, waarbij de focus ligt op het identificeren en beveiligen van kwetsbaarheden in webapplicaties. Het omvat een grondige verkenning van methodologieën en technieken die worden toegepast bij het testen van de beveiliging van webapplicaties. Het onderzoek analyseert populaire webgerichte aanvalsvectoren zoals SQL-injecties, cross-site scripting (XSS) en cross-site request forgery (CSRF). Daarnaast wordt een vergelijkende studie uitgevoerd om de effectiviteit van de testen op meten bij 3 verschillende we applicaties.

**Keuzerichting:** Mobile & Enterprise development
**Sleutelwoorden:** Penetratietesten, Webapplicaties, Beveiliging, Ethical Hacking, Cybersecurity

## Inhoudsopgave



## 1. Inleiding

De groei van webapplicaties heeft de manier waarop we communiceren, winkelen en informatie delen veranderd. Deze toename in het gebruik van webtechnologieën heeft ook nieuwe uitdagingen met zich meegebracht op het gebied van cybersecurity. Het belang van het waarborgen van de beveiliging van webapplicaties kan niet worden overschat. Zelfs de kleinste kwetsbaarheid kan leiden tot grote gevolgen, waaronder gegevensdiefstal, reputatieschade en financiële verliezen. Om deze reden is het uitvoeren van penetratietesten binnen een webomgeving van cruciaal belang om potentiële beveiligingszwakheden te identificeren (K e.a., 2019).

Deze bachelorproef richt zich op het verkennen van penetratietestmethodologieën binnen een webomgeving. Ook zal er een focus gelegd worden op het begrijpen van het concept van penetratietesten, de identificatie van veelvoorkomende beveiligingszwakheden in webapplicaties en de toepassing van praktijkgerichte onderzoeken om de beveiliging van webapplicaties te evalueren. Het praktijkgerichte onderzoek zal worden gerealiseerd door middel van een test waarin drie verschillende webprojecten onderworpen zullen worden aan penetratietesten. Dit onderzoek heeft als doel inzicht te krijgen in de effectiviteit van de toegepaste methodologieën en zo vast te kunnen stellen hoe veilig verschillende soorten webprojecten zijn tegen penetratietesten.

## 2. Literatuurstudie

In de literatuurstudie gaan we dieper in op de kernaspecten van penetratietesten binnen webomgevingen. We verkennen theoretische concepten, bestaande methodologieën en cruciale technieken, waarbij er zowel klassieke als recente bronnen raadplegen. Het doel is een grondig begrip te krijgen van de huidige stand van zaken en best practices op het gebied van webapplicatiebeveiliging.

Een essentieel startpunt is het onderzoeken van de fundamentele principes van penetratietesten. Hierbij wordt er gekeken naar de rol van ethisch hacken en het identificeren van beveiligingszwakheden. Werken zoals "The Web Application Hacker's Handbook"van Dafydd Stuttard en Marcus Pinto dienen als goede referentiepunten (Stuttard & Pinto, 2011). Vervolgens richten we ons op het begrijpen van veelvoorkomende webgerichte aanvalsmethoden, waaronder SQL-injecties, cross-site scripting (XSS), cross-site request forgery (CSRF) en andere.

Een cruciaal aspect van onze literatuurstudie richt zich op een kritische evaluatie van diverse webapplicatiebeveiligingstools. Het onderzoek bevat welgekende tools zoals Burp Suite, OWASP ZAP, Nmap... waarbij er een zo grondig mogelijk inzicht word verkregen van hun mogelijkheden, beperkingen en toepasbaarheid in diverse scena-

rio's. Een specifieke bron die wordt bestudeerd, is "An Empirical Comparison of Pen-Testing Tools for Detecting Web App Vulnerabilities-(Albahar e.a., 2022). Deze bron biedt onderbouwde inzichten in de prestaties van verschillende pentesttools bij het detecteren van kwetsbaarheden in webapplicaties. De onderzoekers nemen de resultaten van deze vergelijking mee in de evaluatie om de praktische relevantie en effectiviteit van de besproken tools beter te begrijpen.

Een opmerkelijke evolutie binnen het domein van penetratietesten wordt gevormd door de opkomst van geavanceerde automatiseringstools. Een voorbeeld van zo'n innovatie is het artikel "PentestGPT: An LLM-empowered Automatic Penetration Testing Tool-(Deng e.a., 2023). Deze publicatie schetst de opkomst van een automatisch penetratietestinstrument, aangedreven door Large Language Model (LLM) technologie, genaamd PentestGPT. Dit vooruitstrevende instrument maakt gebruik van geavanceerde algoritmes, mogelijk gemaakt door Language Models zoals GPT (Generative Pre-trained Transformer), om automatisch penetratietests uit te voeren binnen webomgevingen. Het artikel belicht hoe PentestGPT in staat is om potentiële beveiligingszwakheden te identificeren, kwetsbaarheden te evalueren en rapporten te genereren, waardoor het proces van penetratietesten grotendeels wordt gestroomlijnd.

Een essentieel element van de literatuurstudie betreft de integratie van actuele inzichten en best practices in de praktijk. Deze bron kijkt naar de evolutie van automatische penetratietesten en biedt een overzicht van de huidige stand van zaken op dit gebied (Abu-Dabaseh & Alshammari, 2018). De onderzoekers analyseren hoe automatische penetratietesten zich ontwikkelen als een veelbelovende benadering om beveiligingskwetsbaarheden te identificeren en het testproces te versnellen. De publicatie belicht de voordelen en uitdagingen van geautomatiseerde tools, waarbij de focus ligt op de integratie van AI-technologieën en machine learning in penetratietestprocessen.

## 3. Methodologie

Fase 1: Identificatie van Penetratietesttools(1 week) Voer een grondige literatuurstudie uit om relevante penetratietesttools te identificeren, waaronder tools zoals Burp Suite, OWASP ZAP, en Nmap. Kies tools die bekend staan om hun effectiviteit bij het testen van webapplicaties en die geschikt zijn voor verschillende scenario's.

Fase 2: Selectie van Webapplicaties(1 week) Kies drie verschillende types webapplicaties om een breed scala aan beveiligingsuitdagingen te vertegenwoordigen. Een standaard WordPress website zonder aanpassingen. Een voltooide WordPress applicatie met aangepaste functionaliteiten en plugins. Een op Laravel gebaseerde PHP-applicatie.

Fase 3: Configuratie van Testomgeving(2 weken) Stel voor elke webapplicatie een afzonderlijke testomgeving in, gebruikmakend van replica's van de live omgevingen, om realistische testresultaten te waarborgen.

Fase 4: Voorbereiding van Penetratietesttools(1 week) Configureer elke geselecteerde tool om te voldoen aan de specifieke kenmerken van de te testen webapplicatie. Zorg ervoor dat de tools zijn ingesteld om zowel geautomatiseerde als handmatige tests uit te voeren.

Fase 5: Uitvoering van Penetratietesten(3 weken) Voer penetratietesten uit op de drie geselecteerde webapplicaties met behulp van de geconfigureerde tools. Documenteer gedetailleerde resultaten, inclusief geïdentificeerde kwetsbaarheden, mogelijke aanvalsscenario's en beveiligingssterkten.

Fase 6: Vergelijking van Testresultaten(1 week) Analyseer de resultaten van de penetratietesten per applicatie en per tool. Identificeer consistent gedetecteerde kwetsbaarheden en vergelijk de nauwkeurigheid en diepgang van de tools in verschillende scenario's.

Fase 7: Selectie van Bestpassende Tool(1 week) Overweeg de bevindingen van de vergelijking en bepaal welke tool het meest geschikt is voor welk type webapplicatie. Houd rekening met factoren zoals gebruiksgemak, rapportagefunctionaliteit en snelheid van detectie.

Fase 8: Evaluatie van Geschikte Tool in Praktijktests (2 weken) Test de geselecteerde tool opnieuw op de drie webapplicaties om de praktische toepasbaarheid en effectiviteit te valideren. Documenteer eventuele verbeteringen of uitdagingen in vergelijking met de initiële testresultaten.

## 4. Verwachte resultaten

De verwachte resultaten van het onderzoek omvatten een uitgebreide vergelijking van de penetratietesttools, waarbij zowel de sterke als zwakke punten van elke tool worden geïdentificeerd. Deze evaluatie richt zich specifiek op de effectiviteit van de tools bij het detecteren van kwetsbaarheden in diverse webapplicaties en hun vermogen om nauwkeurige en informatieve rapporten te genereren.

Daarnaast worden de kwetsbaarheden binnen elke webapplicatie zorgvuldig geanalyseerd. Dit omvat een overzicht van de ernst van de geïdentificeerde beveiligingszwakheden.

De selectie van de meest geschikte penetratietesttool per webapplicatie wordt uitgevoerd. Effectiviteit, nauwkeurigheid en gebruiksgemak zijn slechts enkele van de factoren waar rekening mee wordt gehouden. Het doel is om niet alleen een tool te identificeren die kwetsbaarheden kan

blootleggen, maar ook om ervoor te zorgen dat deze praktisch toepasbaar is in de specifieke context van elke webomgeving.

Na de initiële penetratietesten volgt een fase van herhalingstests, waarbij de geselecteerde tool opnieuw wordt geëvalueerd in real-world scenario's. Deze praktijkresultaten bieden inzicht in de bruikbaarheid van de tool in dynamische omgevingen, waarin eventuele verbeteringen of uitdagingen worden gedocumenteerd.

Ten slotte zal het onderzoek resulteren in een samenvattend rapport. Dit rapport omvat niet alleen een overzicht van de bevindingen en geïdentificeerde kwetsbaarheden, maar ook de algehele beveiligingsstatus van elke webapplicatie. De combinatie van deze uitgebreide resultaten geeft waardevolle inzichten voor een doeltreffende benadering van webapplicatiebeveiliging.

## 5. Discussie, conclusie

Na analyse en uitvoering van de methodologie voor het vergelijken en testen van penetratietesttools op diverse webapplicaties, komen verschillende essentiële conclusies naar voren.

Allereerst biedt de vergelijking van de penetratietesttools een inzicht in hun prestaties en mogelijkheden. De identificatie van sterke en zwakke punten helpt bij het vormen van een solide besluit over welke tools het meest geschikt zijn voor specifieke beveiligingsscenario's.

De gedetailleerde analyse van kwetsbaarheden binnen elke webapplicatie draagt bij aan een begrip van de specifieke beveiligingsuitdagingen waarmee deze applicaties worden geconfronteerd. Dit vormt de basis voor gerichte verbeteringen en maatregelen om de algehele beveiliging te versterken.

In het samenvattend rapport worden niet alleen de bevindingen, kwetsbaarheden en de geselecteerde penetratietesttools gedocumenteerd, maar ook praktische aanbevelingen voor het verbeteren van de beveiliging. Deze conclusies en aanbevelingen vormen gezamenlijk een waardevolle bijdrage aan de ontwikkeling van effectieve strategieën voor het waarborgen van de beveiliging van diverse webapplicaties. Het onderzoek biedt niet alleen inzicht in de huidige beveiligingsstatus, maar stelt ook organisaties in staat om proactief stappen te ondernemen ter versterking van hun beveiligingsinfrastructuur.

## Referenties

Abu-Dabaseh, F., & Alshammari, E. (2018). Automated Penetration Testing: An Overview. *Computer Science & Information Technology*. https://doi.org/10.5121/csit.2018.80610

Albahar, M., Alansari, D., & Jurcut, A. (2022). An Empirical Comparison of Pen-Testing Tools for Detecting Web App Vulnerabilities. *Electronics*, *11*(19), 2991. https://doi.org/10.3390/electronics11192991

Deng, G., Liu, Y., Mayoral-Vilches, V., Liu, P., Li, Y., Xu, Y., Zhang, T., Liu, Y., Pinzger, M., & Rass, S. (2023). PentestGPT: An LLM-empowered Automatic Penetration Testing Tool. https://doi.org/10.48550/ARXIV.2308.06782

K, N., A, A., ravichandran, C., Varshini K B, B. S., & P, C. (2019). Web Application Penetration Testing. *International Journal of Innovative Technology and Exploring Engineering*, *8*(10), 1029–1035. https://doi.org/10.35940/ijitee.j9173.0881019

Stuttard, D., & Pinto, M. (2011). *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws*. John Wiley & Sons Inc.