SOP - distributed pentesting

- Everyone gets 1 user with credits or currency equivalent on their account
- Everyone works in ZAP in protected mode
- Everyone gets burp suite file
- Everyone gets assigned 1 endpoint
- Everyone delivers a checklist of what they tested for that feature
- If a second user is needed for IDOR testing for example, a new user can always be made themselves
- Nobody can change the scope they are assigned, DO NOT GO OUTSIDE OF YOUR SCOPE
- If you are unsure what your scope is, contact Wesley or Brandon
- If you are unsure of what to test specifically, contact Wesley or Brandon
- In case of any doubt you can not fix yourself, call Wesley or Brandon. Rather one call too much than one too little
- You will usually test according to the web app checklist (full and summary), the OWASP web security testing guide and the OWASP top 10 or API top 10 unless otherwise specified. You can find these checklists under the folder “Standard Operating Procedures”
- You will report on ANY finding, no matter how small or how low the impact. Just mark it well, the client can decide the final actions.
- In case of a bug, you will use the bug template found under “Standard Operating Procedures”
- We attempt to deliver much more than just a scan and exploit. We attempt to produce work that our client can pass to their QA team or developer team and they can repeat. This means you have to make a checklist with everything you tested per feature. It can be short and concise but make sure you have some trial of what was tested so Wesley or Brandon can create the best possible documentation.
- Note down any oddities as well, for example if the documentation is not correct or you get an unexpexted error message
- NO INVASE TESTS ON PRODUCTION UNLESS OTHERWISE SPECIFIED
- You can use production to see what features look like and should work like but do not hack on production!
- Use all the documentation you have to you disposal, this includes API documentation
- Focus on coverage + heavy impact. Make sure you coverage is wide and if you think you need to investigate further, ask a senior and they will ask the client if they want to spend budget on testing this.
- Our company values are accuracy, repeatability and maintainability so keep that in mind in your everyday work
- You can request a copy of the full documentation from a senior after signing off on an additional NDA.
- If you have an problem at all, call a senior, don’t spend hours on end staying blocked
- If you need a license but we did not provide you one, contact a senior
- You are to fill in the template for timekeeping accurately and truthfully at all times. We will not check up on your every move but if it becomes a problem, we need to talk.
- You must be present at 3 out of 7 weekly stand-up meetings. Invites will follow and I will try to send it different hours to account for everyone but let me know if you can’t make it at least 3 of 7 days
- Stand-ups are led by Wesley or Brandon, in case they can’t, they will make sure a replacement has been assigned and informed
- Stand-up meetings will last a maximum of 15 minutes. Limit your points to
- What you are working on
- How many hours you have spent and left
- Any problem you incurred but don’t wait ‘till the standup to talk to use about problems if they block you. We have an open door policy and if I do not answer, Brandon will or we will call you back ASAP!

- Anything you need from someone like a short meeting or a license for a tool
- let us know if you won't work for the due. You can be sick or on holiday, that is all perfectly normal but we just like to know ASAP so we can plan accordingly. We are often asked to act fast and it's good to know who can be on call.
- We will not have continues pentesting work for you. We try to give you as many of our hours as possible and more will come up in the future but for now, other tasks can be done by you and found by contacting Wesley or Brandon
- Every task will have a SOP (Standard Operating Procedure), for example course requirements document. You have to follow these, contact a senior about a possible exemption or risk not getting paid until all requirements have been met.
- All tasks will have a set budget, not a set amount of hours. Sometimes it might be in hours but usually it will be a lump sum and we ask you for an estimation to plan our releases around that.
- Examples for jobs are programming, course creation, content creation, template creation, writing out procedures and more…
- DO NOT STORE ANY DATA ON PERSONAL DEVICES. USE A GOOGLE DRIVE FOLDER OR SOMETHING IN THE CLOUD. No PoC = No Pay (PoC can be simple checklist of tests done), even if your computer crashes!
- Keep it safe, password protect documentation, do not talk about any of this to your friends and family without prior permission, even if you trust them and stay safe online. Make sure you are not the victim of an exploit before you start exploiting.
- Preferable use a fresh VM (as a matter of sandbox) or docker image and persist your storage while also backing it up to cloud. You can then deliver the full VM which would really help.
- Always hand over all documentation and things you made during the project while we report. Make sure you include python scripts, bash scripts, docker images, data you used for testing (like SQLi attack vectors), ... The more, the better.
- Keep track of the test data you used to test for certain things, of the commands you executed and the logic you tested. Keep track of you ZAP project and/or burp project and make sure to also deliver that deliverable to a senior so they can process it.
- RATE LIMIT YOUR REQUESTS TO 5 REQUEST PER SECOND ON NON-AUTHENTICATION ENDPOINTS
- RATE LIMIT YOUR REQUESTS TO 1 REQUEST PER MINUTE ON AUTHENTACTION ENDPOINTS. Those are not a lot of tests but you get banned easily. Make sure you make those few automated tests you have count.
- As for automated scanners, use them if you think they will make a difference on your endpoint but make sure you use free version or ask a senior for a license
- NEVER EVER EVER EVER EVER USE PIRATED VERSIONS OF SOFTWARE. ASK A SENIOR WHAT YOU NEED.
- 2 People per project MIGHT get the tasks to run automated scanners. ALWAYS RUN THESE BOTH AUTHENTICATED AND UNAUTHENTICADED.

If you are unsure of how to authenticate with these tools, contact a senior at the slightest doubt. This has to be right or it is useless.

- The following vulnerability scanners are required
- OWASP ZAP – Web and API (less so) - FREE
- Burp suite PRO – Web and API (less so) – 400$/year, ask a senior
- Ready API – API – 700$/y, ask a senior
- Nmap – Network – FREE
- Neuralegion – Web and API – 90$/mo, ask a senior
- KNOXSS – XSS – Costs ???, Ask senior, Tests based on PoC principle and reduces false positives and thus also wasted time a lot
- Nikto – Old but gold vuln scanner for web – FREE
- Nuclei – By project discory, will test for CVEs – FREE, template based.
- Masscan – Only in network tests – Free, harder to configure since you can't test only top 1000 used ports , you have to specify all you want to test in the 1 command, TIP: do it 1 time, put them in an env variable and grab that whenever you need it.
- Linkfinder & secretfinder – JS analysis – FREE, works on regex so can mix a lot, you are required to still analyse JS and:

o Do-obfuscate it

o Analyse it for new unexplored endpoints

o Analyse it for new unexplored parameters

o Analyse it for sneaky comments

o Analyse it for Business logic

o Analyse it for new API keys, make sure they are supposed to be private though and not just public which would explain why they are in the JS. For example, Google API keys for are supposed to be public. Read their docs.

- We do NOT accept or run the following scanners
- Metasploit – Network – If you run this, ALWAYS MAKE SURE YOUR SCRIPTS FIT YOUR TARGET. For example, never scan a windows machine with a script that uses linux commands. That a recipe for disaster and script kiddies.
- Nessus – Overpriced garbage, can hardly a single on of my labs
- XSShunter – XSS only - Does not work well, if you do use it, MAKE SURE TO ALSO TEST POST PARAMs
- SQLmap – You can use this to refine an attack you already found but never blindly run a tool on all endpoints, most of them do not even query anything. Also, make sure to test for NoSQL while you are at it.

Read and understood

(Sign name, date and signature)