UoEo NISM Group 3
MEETING

AGENDA

Date of meeting: 26 January 2022
Venue: Zoom
https://us02web.zoom.us/j/9025746143?pwd=Mndxa1kyR3I5NkVDQ1VmMDJ0emZtdz09
Meeting ID: 902 574 6143
Passcode: PT10
Time: 9pm HK / 4pm Yemen
Members: Jonathan, Jun, Haseeb
Required:

Items:

1. Review of last meeting minutes
2. Executive summary planning
3. Vulnerability scanning tools
4. Sections of the assignment
5. A.O.B.

MINUTES

Date of meeting: 17 January 2022
Venue: Zoom
https://us02web.zoom.us/j/9025746143?pwd=Mndxa1kyR3I5NkVDQ1VmMDJ0emZtdz09
Meeting ID: 902 574 6143
Passcode: PT10
Time: 9pm HK / 4pm Yemen
Members: Jonathan, Jun, Haseeb
Apologies:
Minutes:
Required:

Item:	**Time:**	**Details:**	**Who:**	**Action:**	**When:**
1. Review of last meeting minutes					
2. Executive summary planning		2000 words / Worth 40% Deadline 14 February Executive summary of the completed evaluation based on the design document in Unit 6			
3. Vulnerability scanning tools selection		Tools to use: Kali Linux, ZAP, Nmap, SQLmap, Burp suite, Nikto		Jun- ZAP, Nmap Haseeb- Burp suite, Nikto Jon- SQL map, Knockpy	Unit 10
4. Sections		A **brief summary of the work carried out** (tools used (with justifications - (i.e. why did you choose a specific			

		tool), tests carried out, summarised results). Justifications should use academic sources for support. **Summary findings** – presented in an easy-to-understand, non-technical manner (supported by graphics and charts as appropriate). A **discussion of any vulnerabilities** discovered and explanations of why expected vulnerabilities were not detected. **Conclusions and recommendations -** i.e. how the site owner could improve the site security – with justifications. Recommendations should be ordered by business priority. Note that the executive summary should organise any recommendations in order of the priority to the business' commercial needs. The organisation is particularly interested in how well they meet current security standards (including the new GDPR directive) and expect to see any mitigations required to meet such standards clearly called out as important business requirements. This is NOT a penetration testing exercise. The main purpose is to test your hypothesis (that is the vulnerabilities you identified in part 1) by using vulnerability scanning tools to scan a website/ application and produce a list of potential/ discovered vulnerabilities.			

		This list should then be compared to your theoretical list and any differences should be enumerated and possible explanations for the differences (between your theoretical list and the vulnerability scan) explained. Marks will be given for a demonstration of understanding of how the tools work; how vulnerabilities are detected and the most (cost) effective mitigations to be deployed.			
5. A.O.B.		For scanning: To pass WAF refresh the browser for captcha (No response then it will be blocked) Possibly use proxy / proxy chains Meeto discuss Team Debate later		Next meeting on 2 Feb Can message through Signal for support/ideas/etc.	Wed 2 Feb