Ethical Hacking Report

Ethical Hacking F/618/5213 **AC 3.2:** Execute a series of ethical hacking attacks based upon the plan. **AC 3.3:** Report on the results of the attacks.			
Learner Name	O. Folarin	**Tutor Name**	Shamim Khan

Scenario

As Pentest Ground's Ethical Hacker, you have prepared an Ethical Hacking Project Management Plan to identify and assess vulnerabilities in their URL, https://pentest-ground.com:81/. It is now time to carry out the ethical hacking activities outlined in the plan and document the findings in a report. Alongside this, you must use project management software to monitor and track the progress of the project, against the original plan.

***Task 3)** Using https://pentest-tools.com/ execute **at least two** ethical hacking attacks outlined in your "Ethical Hacking Project Management Plan" and upload the results PDFs (3.2).*

***Task 4**) Complete this "Ethical Hacking Report (EH 3.3)" to document the findings (3.3).*

Complete the fields below ensuring you are clear and concise with your answers to ensure your Ethical Hacking Report is legible for your tutor to assess and IQA to review.

Action/attack 1	
Evidence of attack being executed (3.2)	*(upload results PDF)*
Was it successful? (3.3)	Network vulnerability scan was successful with just one medium risk level reported. Scan took 1 minute 22 seconds with all possible 10 tests performed.
Any vulnerabilities identified? If yes, what were they? (3.3)	Yes, one vulnerability was found and was categorized as medium risk. It was from the first vulnerability scan of jQuery on port 81 that was performed. It says the passing HTML contains elements from untrusted sources which can be manipulated by cybercriminals to execute untrusted codes.
Action/attack 2	
Evidence of attack being executed (3.2)	*(upload results PDF)*
Was it successful? (3.3)	Website vulnerability scan was successful with 3 medium risks and 5 low risks level reported. Scan took 15 seconds with all possible 19 test performed.
Any vulnerabilities identified? If yes, what were they? (3.3)	Yes 8 vulnerabilities were found with 3 categorized as medium risk and 5 categorized as medium risk. Insecurities were found in the cookies settings and a scan on a server-side software 'jQuery' reveals that passing HTML contains elements from untrusted sources which can be manipulated by cybercriminals to execute untrusted codes. The 4 out of 5 low risk consists of missing 'HTTPS' security headers after each response. Security headers of the following are found

	missing; X-Content-Type-Options, Referrer-Policy, Strict-Transport-Security, and Content-Security-Policy. The 5th low risk highlights all the server software and technology tools and requests for them to be validated manually.
Action/attack 3	
Evidence of attack being executed (3.2)	*(upload results PDF)*
Was it successful? (3.3)	
Any vulnerabilities identified? If yes, what were they? (3.3)	