Glossary of Terms

Burp Suite	: Software used to manually test web application security using the intercept proxy method.
Clickjacking	: An attack technique where a user is tricked into clicking a disguised web element for the attacker's benefit.
CSP	: A security policy that specifies the content sources allowed to be loaded by the browser.
CSRF	: An attack where an authenticated user is forced to perform an unauthorized action on a website.
XSS	: A malicious script injection attack into a web page.
CVSS	: An international standard for assessing the severity of a vulnerability.
DSR	: A research method that produces practical artifacts to solve specific problems.
DDoS	: An attack that floods a network or server, causing the service to be disrupted or unavailable.
ETag	: An HTTP header used for timestamp-based cache validation.
HTTP Headers	: A security policy that forces browsers to use only HTTPS
connections.	
HSTS	: A security policy that forces browsers to use only HTTPS connections.
IP	: A series of unique numbers used to identify a device on the internet network.

IT	: A general term for any technology that helps humans create, modify, store, communicate, and/or disseminate information.
Nessus	: A vulnerability scanning tool that detects security holes in systems and applications.
Nmap	: A network scanning tool to detect active services, open ports, and service versions.
OWASP ZAP	: Open-source software for automatically and manually testing web application security.
VA	: The systematic process of identifying, classifying, and evaluating vulnerabilities in a system.
WPScan	: A specialized tool for scanning security vulnerabilities on the WordPress platform.