Students	Almog Franco, Raziel Shushan, Alon Bril, Netanel Hajbi, Ori Ronen	
Subject	Weakness Point(s)	Relevant Threats
Spoofing	Spoofing user credentials during login	Impersonation of a legitimate user
	Manipulating session tokens	Session hijacking
	Intercepting and modifying network traffic	Man-in-the-middle attack
Tampering	Tampering with customer data	Modifying customer details without proper authorization
	Altering customer records in the database	Unauthorized modifications to customer information
	Modifying search queries to manipulate results	Manipulating search results to hide or expose specific customer information
	Manipulating form data to bypass validation	Submitting unauthorized or malicious customer data
Repudiation	Repudiation of customer actions	Denying performing certain customer actions
	False claims of unauthorized access	Claiming not to have added/modified customer information
	Manipulating audit logs	Tampering with log entries to hide or manipulate customer actions
	Falsifying evidence of customer interactions	Fabricating or modifying evidence related to customer activities
Information Disclosure	Information leakage in error messages	Displaying sensitive customer data in error messages
	Revealing system details or implementation in errors	Disclosing application or infrastructure vulnerabilities in error messages
	Inadequate access controls on customer data	Unauthorized access to sensitive customer information
	Exposing customer details through insecure APIs	Leakage of customer data through insecure API endpoints
Denial of Service	Denial of service through excessive requests	Overwhelming the server with a high volume of customer creation/search requests
	Resource exhaustion through inefficient algorithms	Consuming excessive server resources through inefficient operations
	Exploiting application or infrastructure vulnerabilities	Launching DoS attacks targeting application or network vulnerabilities
	Disrupting service availability through spamming	Flooding the system with spam or fake customer requests
Elevation of Privilege	Unauthorized access to administrative features	Gaining administrative privileges without proper authorization
	Exploiting privilege escalation vulnerabilities	Elevating user privileges to gain unauthorized access
	Bypassing user role-based access controls	Accessing sensitive user profile information without proper authorization
	Exploiting insecure password reset mechanisms	Manipulating password reset process to gain unauthorized access