Student.

Which attacks are possible on the web? How to prevent it?

🚮 Intent Interpreter

What are the common types of cyber attacks that can be launched against websites and web applications, and how can they be prevented or mitigated in a cloud computing environment?

Retriever

- [1] Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data...
- [2] Organizations should ensure that web applications employ secure coding practices, including input validation, output encoding...
- [3] When deploying web applications in a multi-tenant public cloud environment, it is critical to secure data at rest by using encryption and and to enforce stringent access controls. Preventive measures against cross-site scripting and SQL injection should be integrated...

Generative AI

Common types of cyber attacks that can be launched against websites and web applications include cross-site scripting (XSS), SQL injection, cross-site request forgery (CSRF)...

These can be prevented or mitigated in a cloud computing environment through HTTP anomaly analysis to detect attacks like XSS, SQL injection, and brute-force attacks and by ensuring proper configuration and security measures, such as...

∴Ontology Verifier

"validation result": "Pass",

"confidence score": 0.9,

"reasoning": "The answer correctly maps to several concepts within the cybersecurity ontology, including 'attack' and 'vulnerability', with specific examples such as 'SQL Injection' and 'Cross-site scripting (XSS)' which are types of attacks and vulnerabilities. The cloud computing environment context is also relevant, as these attacks can be launched against websites and web applications hosted in cloud environments, and prevention or mitigation strategies...