Create a comparative table summarizing Web 1.0 to Web 5.0 based on the following parameters:

* Time Period: Approximate years when each phase was prominent.
* Content Type: Nature of content (static, dynamic etc.).
* User Interaction: Level and type of interaction supported.
* Technology Used: Major technologies associated with each phase (e.g., HTML, JavaScript, AI).
* Example Platforms: Applications or websites typical of each web phase.
* Security Concerns: Key security risks associated with the phase
* Attacks: Possible attacks

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Web Version | Time Period | Content Type | User Interaction | Technology Used | Example Platforms | Security Concerns | Attacks |
| Web 1.0 | 1990s - early 2000s | Static | Limited interaction, mostly read-only. | HTML, basic JavaScript | Early websites, GeoCities, AOL | The security is weak, lacking encryption, which makes the static content vulnerable to data theft. | SQL Injection, DNS Spoofing, Cross-site Scripting (XSS) |
| Web 2.0 | Mid 2000s - 2010s | Dynamic, User-Generated | Social media, sharing, comments, user collaboration | JavaScript, PHP, Flash | Facebook, YouTube, Twitter, Wikipedia | Privacy concerns, social engineering, data breaches | Phishing, Cross-Site Request Forgery (CSRF), DDoS attacks |
| Web 3.0 | Late 2010s - Present | Smart, Decentralized | Personalized content, blockchain-based, AI-driven | Blockchain, AI, Machine Learning, JSON | Ethereum, Bitcoin, AI assistants (Siri, Alexa) | Hacking of decentralized systems, data privacy issues | 51% Attack, Smart Contract Vulnerabilities, Phishing in Crypto |
| Web 4.0 | 2020s - Emerging | Intelligent, Context-Aware | AR/VR, IoT, self-learning systems | IoT, 5G, Big Data, Edge Computing | Smart homes, AR apps, autonomous vehicles | IoT security risks, data leakage, AI bias, privacy breaches | IoT Hacking, AR Spoofing, Deepfake Attacks |
| Web 5.0 | 2030s - Future (Speculative) | Emotionally Intelligent, Human-like | Brain-computer interfaces, VR immersion | AI, Quantum Computing, Brain-Computer Interface | Fully immersive VR worlds, AI-driven apps | Ethical issues, mind hacking, data security in AI-driven tech | Brain-hacking, Privacy breaches in emotional AI, Quantum attacks |