Nowadays, the web application needs to support both standard and mobile Web apps. No matter what kind of application, it has to face two major basic security concerns. The first is user authentication security, the second is hacking and DDoS attacks.

For user authentication security, OAuth 2.0 (Open Authorization) is widely used in using a simple credential with a username and password. It is a federation protocol and aims at simplifying authorization and access to protected data by giving access to data while protecting the owner's account credentials. It allows a user with an account on one website (provider) to allow another website (subscriber) to access his or her data from the first website. Users can give out tokens instead of credentials. A token can grant access to a specific resource for a specific duration so resources can be shared with a third party without having to grant complete access to all the data. This is a far better solution than users sharing their usernames and passwords to access each other's data. On the other hand, this turns into another weakness of using OAuth. This authentication security technology is using authorization tokens. When this secret token was leaked or stolen from the device, other web services linked to it for authorization also was granted. (Lodderstedt, T., Ed., McGloin, M., and P. Hunt, 2013)

For hacking and DDoS attacks, Intrusion Detection Systems or Intrusion Prevent Systems can be tuned to show you the specific content within the packets. This can be used for uncovering intrusions such as exploitation attacks or compromised endpoint devices that are part of a botnet. When performing protocol analysis, it looks at the TCP and UDP payloads. The sensors can detect suspicious activity based on the signature defined in its database. Based on the analysis result, it can be used to change security systems or implement new and more effective controls. It can also be analyzed to identify bugs or network device configuration problems. The metrics can then be used for future risk assessments too. It can also block or resolve potential issues proactively and automatically. However, it also has potential weaknesses. The IP address can be spoofed. If an attacker is using a fake IP address, it makes the threat more difficult to detect and assess. In many cases, false positives are more frequent than actual threats. The signature update interval is also affecting the effectiveness and efficiency of the intrusion system. There is often a gap between the new signature database update and the new attack happened. Furthermore, hacking and attacks are turning to be being like human beings' behaviors. The detection by signature-based is not intelligent enough to distinguish the anomaly attacks. (checkpoint.com)

Reference:

Bertocci, V. & Campbell, B. 2022. *OAuth 2.0 Step-up Authentication Challenge Protocol.* Available: https://www.ietf.org/archive/id/draft-bertocci-oauth-step-up-authn-challenge-01.html [Accessed 9 Apr 2022]

Lodderstedt, T., Bradley, J., Labunets, A., and Fett, D. 2021. *OAuth 2.0 Security Best Current Practice.* Available: https://www.ietf.org/id/draft-ietf-oauth-security-topics-19.html [Accessed 9 Apr 2022]

Lodderstedt, T., Ed., McGloin, M., and P. Hunt. 2013. *OAuth 2.0 Threat Model and Security Considerations*. Available: https://www.rfc-editor.org/info/rfc6819 [Accesed 9 Apr 2022]

Checkpoint.com *Intrusion Detection System (IDS) Vs Intrusion Prevention System (IPS).* Available: https://www.checkpoint.com/cyber-hub/network-security/what-is-an-intrusion-detection-system-ids/ids-vs-ips/ [Accessed 9 Apr 2022]