

2. Voice acting allows you to improve your understanding of English on a spoken level.

3. You get a better grasp of grammar. Subtitles are frequently present in games these days, allowing you to see exactly how the word is written.

4. All games are different.

So, the Games are a super powerful and multipurpose tool. We are sure that everyone can choose a game that will help in learning English.

References

1. English while playing: can you learn English with computer games. URL: <https://ternopil.cx.ua/anhlijska-hraiuchys-chy-mozhna-vyvchyty-anhlijsku-z-komp-iuternymy-ihramy/> (Last accessed 18.04.2024).

2. How to upgrade your English to level 80 using computer games. URL: <https://greenforest.com.ua/journal/read/yak-prokachati-anglijsku-do-80-lvl-za-dopomogoyu-kompyuternih-igor> (Last accessed 18.04.2024).

3. Yulia Kulina. How computer games can help teenagers to improve their English. URL: <https://lse.ua/article/yak-kompyuterni-igri-mozhut-dopomogti-pidlitku-pokrashiti-anglijsku/> (Last accessed 18.04.2024).

4. Tymur Solod. How games can improve the level of English for work in game development. Experience and life hacks of a specialist. URL: <https://gamedev.dou.ua/blogs/how-to-improve-your-english-through-video-games/> (Last accessed 18.04.2024).

*Halatenko Daria,
Faculty of Information Technology,
course 2, group 16, specialty Information System and Technologies,
State University of Trade and Economics,
Kyiv, Ukraine
Scientific supervisor: Savchuk Tetiana,
Lecturer of the Department of
Modern European Languages, SUTE*

WEB APPLICATIONS SECURITY

Over a long period of development, web applications have become much more complex than just content sites. More and more complex web applications appear on the network every day, offering new solutions for consumer requirements in various market sectors. Web applications have

become the most convenient and effective means of presenting information and providing services in the network. Companies from various market sectors continue to create web applications to promote their goods and services online, carving out their niches in the digital space. Mobile tools and web technologies have topped this list for a long time. Because digital services are so important, they need to be protected to keep sensitive information safe. The development of web technologies continues at a rapid pace, but it also brings certain security risks. Ensuring the protection of large amounts of diverse information is a complex task, and carelessness can lead to wasted resources and enforcement issues.

Web applications, like any other software, may contain errors and defects for various reasons. This may be due to human factors, as software developers can make mistakes. Also, they usually use external libraries, which can also have their drawbacks. Even large open source projects like the Linux kernel can contain a significant number of bugs, which is normal. There are now many different attacks that hack or steal data from web applications. They do this because of various program vulnerabilities. A secure web application is one that can remain operational even during attacks and ensures data security. In addition, flaws in security mechanisms can adversely affect other important application features, such as accessibility. Failure to protect the application from DoS or DDoS attacks may result in temporary unavailability of the application. This is becoming a particularly serious problem as these types of attacks are becoming more common, even among large IT companies. For example, in 2015, Chinese hackers attacked GitHub, causing a 10-minute interruption in the operation of the platform. During the attack, traffic peaked at 1.35 terabytes per second. GitHub could not run for more than 8 minutes. In terms of scale, it was one of the most notorious DDoS attacks in history. Therefore, even companies with huge resources and reputation cannot guarantee complete protection against all attacks. However, it is important to have the appropriate protection measures in place to minimize risks and prevent most potential threats.

Organizations should consider several best practices to ensure that their web applications are fully secure:

- Security Shift to the Left (DevSecOps): Integrating security practices early in the software development lifecycle ensures that security concerns are considered from the outset. This allows you to identify and fix potential vulnerabilities at an early stage, reducing the risk of a security breach;

- Data encryption: Encrypted data that is transmitted between the user and the server, as well as stored on the server, is protected from unauthorized access. Use HTTPS for secure data transfer;

- Authentication and session management: Ensure user logins are secure and secure sessions are maintained. Use authentication mechanisms such as two-factor authentication and manage sessions to prevent session ID theft;

- Security configuration and patch management: Maintain up-to-date security configurations and promptly apply patches to software and infrastructure. Update software and patches regularly to prevent exploits of known vulnerabilities;

- Monitoring and response: Provide continuous security monitoring to detect potential threats and unusual activity. Establish alert and incident response systems to quickly respond to potential threats.

Therefore, the development of web technologies and the spread of web applications have become not only important, but also integral parts of the digital ecosystem. However, along with these new opportunities, the threat to information security is also growing. Ensuring the security of web applications is becoming a top priority for organizations of any size and industry. Integrating security practices early in software development, encrypting data, managing authentication and sessions effectively, setting up security configurations, and responding promptly to potential threats are all essential steps to secure web applications. Applying these best practices will help organizations minimize the risks of security breaches and maintain consumer trust in the digital environment.

References

1. Боскін О. О. Безпека веб-додатків та хакерські атаки. *Вісник Херсонського національного технічного університету*. 2023. № 3 (86). С. 83-92.

2. Яремчук К. П., Воскобойников Д. І., Мелкозьорова О. А. Сучасні загрози та способи забезпечення безпеки веб-застосунків. *Комп'ютерні науки та Кібербезпека*. 2022. №2. С. 28-34.

3. Abusaimh, Mohammad Shkoukani Hesham, Mohammad Shkoukani. Survey of web application and internet security threats. *International journal of computer science and network security*. 2012. С. 67-76.

4. Web Application Security: Risks, Technologies and Best Practices URL: <https://www.cycognito.com/learn/application-security/web-application-security.php> (Last accessed 21.03.2024).

5. Web Application Security: The Ultimate Guide. URL: <https://www.codica.com/blog/web-application-security/> (Last accessed 13.04.2024).