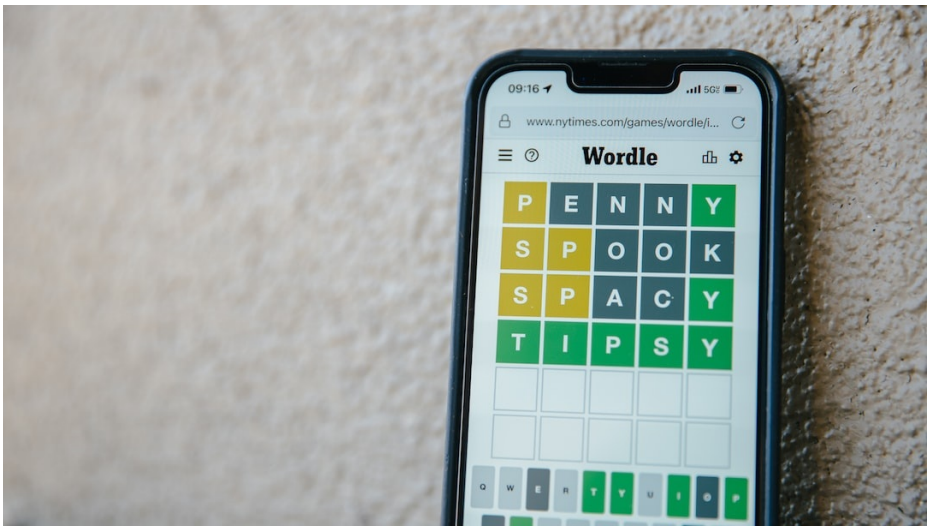
CyberSec Weekly

Wordle API Vulnerability Leaves it Open to Hacking

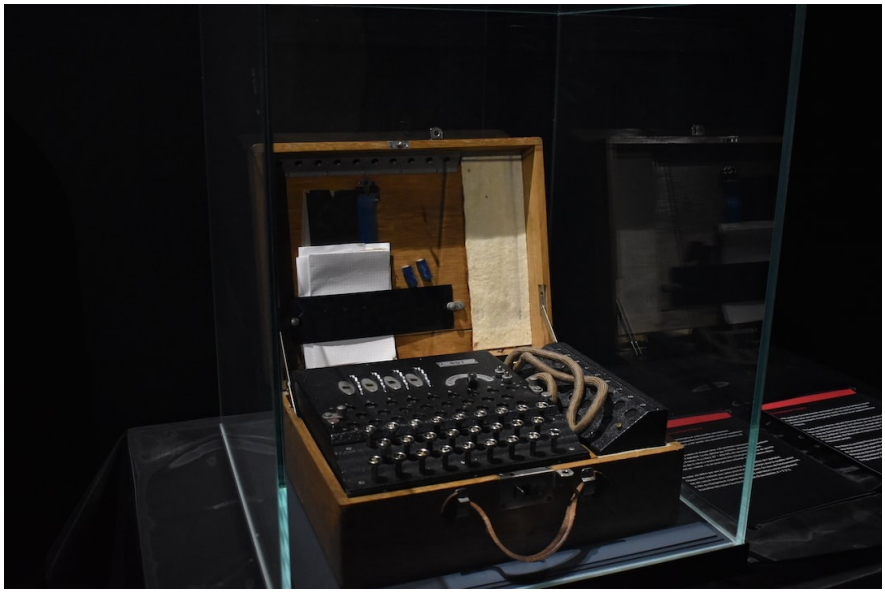
A security researcher has uncovered vulnerabilities in the New York Times-owned online game Wordle that not only reveal the solution to the daily word puzzle but also expose its application programming interface to potential hacking.



Detailed by David Thompson, a security researcher at Noname Security under the title of “Tomorrow’s Wordle is ‘PWNED!’,” the vulnerabilities were found using Google Chrome’s built-in developer tools. Thompson found the daily answer with the help of a JSON-formatted API.

To read full story…

Click Here



NIST Retires SHA-1

The SHA-1 algorithm, one of the first widely used methods of protecting electronic information, has reached the end of its useful life, according to security experts at the National Institute of Standards and Technology (NIST). The agency is now recommending that IT professionals replace SHA-1, in the limited situations where it is still used, with newer algorithms that are more secure.

“Modules that still use SHA-1 after 2030 will not be permitted for purchase by the federal government,” Celi said.

To read the full story…

Click Here

Why did the plastic surgeon apply for a software engineering job?

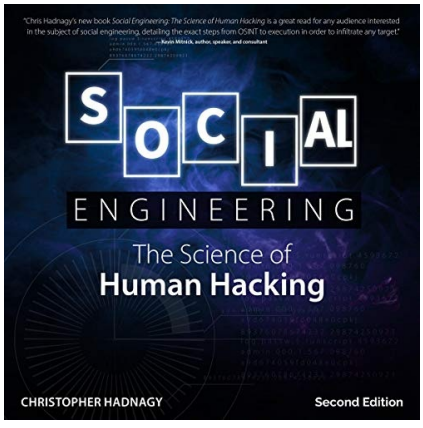
The company needed a back-end developer.

Hackers Plants Files to Frame Priest

hackers planted fake evidence on the computers of two Indian human rights activists that led to their arrest along with more than a dozen colleagues, has already become notorious worldwide. Now the tragedy and injustice of that case is coming further into focus: A forensics firm has found signs that the same hackers also planted evidence on the hard drive of another high-profile defendant in the case who later died in detention—as well as fresh clues that the hackers who fabricated that evidence were collaborating with the Pune City Police investigating him.

To read the full story…

Click Here



Social Engineering, Second Edition

Social Engineering: The Science of Human Hacking reveals the craftier side of the hacker's repertoire - why hack into something when you could just ask for access? Undetectable by firewalls and antivirus software, social engineering relies on human fault to gain access to sensitive spaces.

Click Here