Issued 1/17/17

McDonald's Vulnerability Allows Hackers to Steal Users' Passwords

If you registered for an account on McDonald's website to get free burgers, you might actually get your account hacked, as a vulnerability could allow an attacker to steal your password quite easily. Specifically, Dutch independent software engineer Tijme Gommers discovered a security flaw in McDonald's website that can be exploited by cybercriminals to access user data, including password stored into cookies.

McDonald's website can save user information in cookies whenever they check the option to remember their usernames and passwords, so those who didn't use this option are supposed to be secure. The security researcher explains in a lengthy and technical blog post how the vulnerability exposes users and what type of information can be stolen by hackers. "By abusing an insecure cryptographic storage vulnerability and a reflected server cross-site-scripting vulnerability it is possible to steal and decrypt the password from a McDonald's user. Besides that, other personal details like the user's name, address [and] contact details can be stolen too," he says. What's worse is that, according to the security expert,

McDonald's has already been informed about the vulnerability, but the company never responded, choosing instead to ignore it and not release a patch. The security hole is still there and because no response was offered, Tijme Gommers decided to disclose it, hoping that once it makes the headlines, McDonald's would pay a little bit more attention to it and release a patch. In the meantime, registered users of

McDonald's portal should avoid saving their usernames and passwords on the website, and at the same time, avoid setting the same password for other accounts for other services. There's a good chance that cybercriminals would attempt to exploit other accounts as well, so using different passwords is an effective way to prevent that from happening.