bzyo Update README.md ... on Mar 25, 2021 History

..	
imgs	2 years ago
README.md	last year
worklist.txt	2 years ago

README.md

Vulnerability

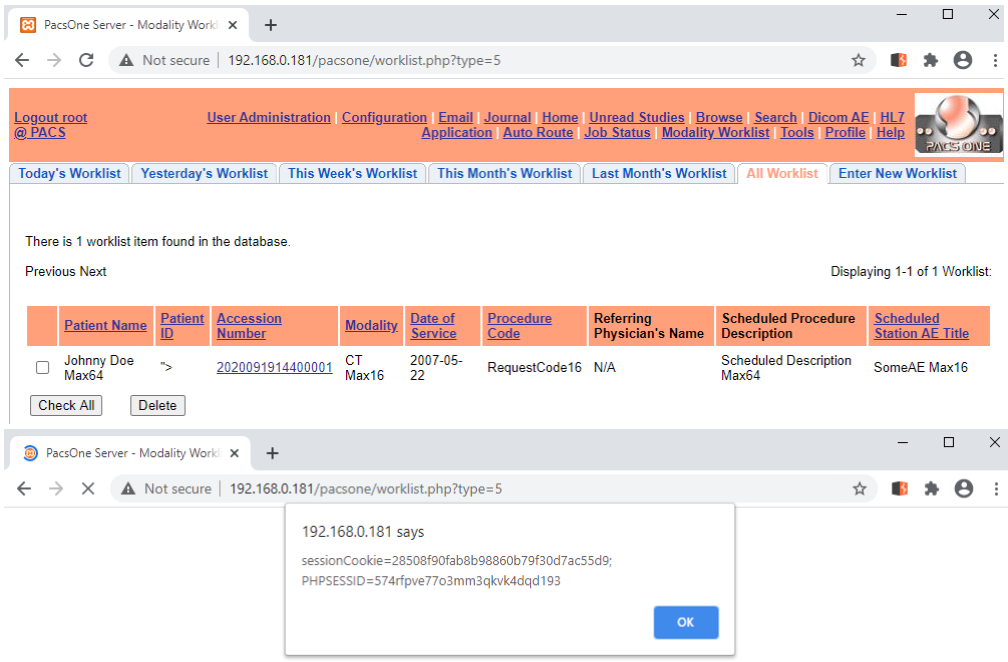
PacsOne Server 6.8.4 suffers from multiple authenticated stored XSS vulnerabilities.

Prerequisites

To successfully exploit these vulnerabilities, an attacker must be authenticated and have the ability to import a worklist

Exploit

Patient ID field is one of many that suffers from a stored XSS vulnerability
Example worklist.txt contains the vulnerable string "><script>alert(document.cookie)</script>



Timeline

05-07-20: Submitted incident through email, immediate response
05-21-20: Issue resolved
09-10-20: New version released
09-19-20: Submitted public disclosure

Reference

MITRE CVE-2020-12869

Disclaimer

Content is for educational and research purposes only. Author doesn't hold any responsibility over the misuse of the software, exploits or security findings contained herein and does not condone them whatsoever.