ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
<u>High</u>	0
<u>Medium</u>	1
<u>Low</u>	0
<u>Informational</u>	0

Alert Detail

Medium (Medium)	Format String Error
Description	A Format String error occurs when the submitted data of an input string is evaluated as a command by the application.
URL	http://localhost:8080/OTHER/core/other/proxy.pac/? apinonce=ZAP%25n%25s%25s%25n%25s%25n%25s%25
Method	GET
Parameter	apinonce
Attack	ZAP%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%
URL	http://localhost:8080/script.js/? apinonce=434650f8c2644ff1&v=ZAP%25n%25s%25s%25n%25s%25n%25s%25n%25s%
Method	GET
Parameter	v
Attack	ZAP%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%
URL	http://localhost:8080/script.js/? apinonce=ZAP%25n%25s%25s%25s%25s%25n%25s%25s%25n%25s%25s%25s%25s%25s%25s%25s%25s%25s%25s
Method	GET
Parameter	apinonce
Attack	ZAP%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%
Instances	3
Solution	Rewrite the background program using proper deletion of bad character strings. This will require a recompile of the background executable.
Other information	Potential Format String Error. The script closed the connection on a /%s
Reference	https://www.owasp.org/index.php/Format_string_attack
CWE Id	134
WASC Id	6
Source ID	1