ZAP Scanning Report

Site: http://localhost:8080

[redacted]

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	0
Low	1
Informational	1

Alerts

Name	Risk Level	Number of Instances
Cookie without SameSite Attribute	Low	2
Loosely Scoped Cookie	Informational	3

Alert Detail

Low	Cookie without SameSite Attribute
Description	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
URL	http://localhost:8080/login
Method	GET
Attack	
Evidence	Set-Cookie: JSESSIONID
URL	http://localhost:8080/robots.txt
Method	GET
Attack	
Evidence	Set-Cookie: JSESSIONID
Instances	2
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site
CWE Id	1275
WASC Id	13
Plugin Id	10054

Informational	Loosely Scoped Cookie
	Cookies can be scoped by domain or path. This check is only concerned with domain scope. The domain scope applied to a cookie determines which domains can access it. For

Description	example, a cookie can be scoped strictly to a subdomain e.g. www.nottrusted.com, or loosely scoped to a parent domain e.g. nottrusted.com. In the latter case, any subdomain of nottrusted.com can access the cookie. Loosely scoped cookies are common in mega-applications like google.com and live.com. Cookies set from a subdomain like app.foo.bar are transmitted only to that domain by the browser. However, cookies scoped to a parent-level domain may be transmitted to the parent, or any subdomain of the parent.
URL	http://localhost:8080/login
Method	GET
Attack	
Evidence	
URL	http://localhost:8080/login
Method	GET
Attack	
Evidence	
URL	http://localhost:8080/robots.txt
Method	GET
Attack	
Evidence	
Instances	3
Solution	Always scope cookies to a FQDN (Fully Qualified Domain Name).
Reference	https://tools.ietf.org/html/rfc6265#section-4.1 https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html http://code.google.com/p/browsersec/wiki/Part2#Same-origin_policy_for_cookies
CWE Id	565
WASC Id	15
Plugin Id	90033