${FINDING\_NAME}  
**Dread Score Summary                                                         STATUS:** CONFIRMED

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | **Risk Rating** | | | | MODERATE | | | | | Damage Potential | Reproducibility | Exploitability | Affected Users | | Discoverability | Total | Remediation Effort | | 3 | 4 | 5 | ${CRI\_AFEC} | | 4 | ${CRI\_TTL} | MEDIUM | |

**Summary of Finding**  
${CRITICAL\_SUMMARY}  
**Proof of Concept**  
${CRITICAL\_PROOF}  
**Recommendations**  
It is best business practice that any cookies that are sent (set-cookie) over an SSL connection to explicitly state secure on them. As such, make sure that sensitive cookies, which are sent over an encrypted connection to the server, are set with the "secure" attribute.
References
? http://www.owasp.org/index.php/Authentication\_Cheat\_Sheet#Secure\_Flag
? http://www.owasp.org/index.php/Testing\_for\_cookies\_attributes\_%28OWASP-SM-002%29
? http://cwe.mitre.org/data/definitions/614.html
? http://capec.mitre.org/data/definitions/102.html