**Lack of protection mechanism in cookies**

**SEVERITY:** **MODERATE**

**VULN. CODE:** SCK-PROT

**AUTH. REQUIRED:**

**VULNERABILITY DESCRIPTION**

Following the Penetration Test, it was found that the session cookies generated by the application do not use the protection mechanisms defined by the standard (RFC 6265, April 2011), as the "HttpOnly" flag is not used and the "Secure" flag is not present. The absence of the "HttpOnly" flag allows access to the session cookie stored in the DOM by scripts such as Javascript or Flash. In the presence of malicious scripts, or in the presence of other vulnerabilities (e.g. Cross Site Scripting/XSS), the absence of this protection mechanism favors the theft of the session and allows a threat agent to impersonate a legitimate and authenticated user on the application. The absence of the "Secure" flag allows the use of a session cookie delivered through the HTTPS protocol, during HTTP browsing sessions (not encrypted), thus making it exposed to attacks of "eavesdropping".

The following box shows the extract of a server response containing the Set-Cookie directive.

|  |
| --- |
| **RESPONSE**  HTTP/1.1 302 Moved Temporarily  Date: Fri, 17 May 2019 11:54:24 GMT  Server: nginx/1.4.6 (Ubuntu)  Set-Cookie: JSESSIONID=EVRZTXc6Bzi1z7DBeXRY7-Q7.undefined; Path=/;  Content-Length: 0  Connection: Close |

**Box 4 – Set-Cookie, missing HttpOnly and Secure flag**

**SUGGESTED SOLUTIONS**

We recommend that you modify the application so that the HTTPOnly flags are added to the generated cookies. In case it is not possible to act on the application code, it is suggested to implement the session cookie protection measures through one of the systems used to expose the application services to users (web server, application server, reverse proxy, etc..).

**REFERENCES**

More information regarding the vulnerability and its possible solutions can be found on the following addresses:

**REF 14 – www.owasp.org/index.php/HttpOnly**

**REF 15 – www.owasp.org/index.php/Testing\_for\_cookies\_attributes\_(OWASP-SM-002)**