**Information Leak**

**SEVERITY: LOW**

**VULN. CODE:** IN-LEAK

**AUTH. REQUIRED:**

**VULNERABILITY DESCRIPTION**

During the course of the activities, we found out that there are some sources of information leak. In the production servers, there should not be any disclosure of sensible information. Particularly, as suggested by best practices, custom pages and information about the usernames or passwords should be omitted. This type of vulnerability could allow a threat agent to obtain information on the technologies and logic being used by the application and the system by observing the verbose error messages.

During the analysis phase, header fields were detected that show the name of the software used and the relative versions.

|  |
| --- |
| **RESPONSE https://11.22.33.44/**  HTTP/1.1 200 OK  Cache-Control: no-cache  Cache-Control: no-store  Content-Language: it  Date: Fri, 17 May 2019 11:56:53 GMT  Expires: Thu, 01 Jan 1970 00:00:00 GMT  Pragma: no-cache  Server: nginx/1.4.6 (Ubuntu)  Connection: Close  Content-Length: 20405 |

**SUGGESTED SOLUTIONS**

It is advisable to remove any source of information leaks, limiting the verbosity of information, or set up access controls on web paths and applications, limiting the disclosure of information to unauthorized personnel.

The fields in the response headers that often represent the subject of information leaks are “X-Powered-By”, “X-AspNet-Version”, “Server”, etc. They are not necessary for the proper functioning of the application, nor are they useful for users who connect to them correctly, but they are an excellent source of information for a threat agent regarding the composition of the system. For this reason, they should be disabled in any case.

**REFERENCES**

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

**REF 37 – projects.webappsec.org/Information-Leakage**

**REF 38 – cwe.mitre.org/data/definitions/200.html**