### 3.1.3 检测到目标站点存在javascript框架库漏洞

|  |  |
| --- | --- |
| **URL** | http://192.168.17.117/r/cms/jquery.js |
| **请求方式** | GET |
| **问题参数** |  |
| **判断标准** | 1、在访问URL中匹配到存在漏洞的javascript框架库版本信息，则认为存在漏洞； 2、访问当前URL，在请求的响应内容中匹配到存在漏洞的javascript框架库版本信息，则认为存在漏洞； 3、访问当前URL，计算请求的响应hash值，如果和存在漏洞的javascript框架库hash值一致，则认为存在漏洞。 |
| **判断详情** | 1、请求URL：http://192.168.17.117/r/cms/jquery.js；  2、在响应内容中查找到javascript框架库：jquery，版本：1.10.2；  3、漏洞参考链接：https://www.cvedetails.com/cve/CVE-2015-9251/。 |
| **请求&响应** | **GET /r/cms/jquery.js HTTP/1.1** **Accept-Language**: zh-cn,en-us;q=0.7,en;q=0.3 **Accept-Encoding**: gzip,deflate **Accept**: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8 **User-Agent**: Mozilla/5.0 (Windows NT 6.1; rv:33.0) Gecko/20100101 Firefox/33.0 **Accept-Charset**: GBK,utf-8;q=0.7,\*;q=0.3 **Host**: 192.168.17.117 **cookie**: \_site\_id\_cookie=1;JSESSIONID=0E53A518DB91D00D2FEDC601BAEFFCE4 **Referer**: http://192.168.17.117/ |

### 3.1.10 检测到目标源码中可能存在用户名或者密码信息泄露

|  |  |
| --- | --- |
| **URL** | http://192.168.17.117/r/cms/front.js |
| **请求方式** | GET |
| **问题参数** |  |
| **判断标准** | 根据原始请求的响应内容进行判断，如果响应内容中出现疑似用户名或者密码相关的信息，则认为存在漏洞。 |
| **判断详情** | 1、请求URL：http://192.168.17.117/r/cms/front.js；  2、在响应头及响应内容中匹配到 username:username。 |
| **请求&响应** | **GET /r/cms/front.js HTTP/1.1** **Accept-Language**: zh-cn,en-us;q=0.7,en;q=0.3 **Accept-Encoding**: gzip,deflate **Accept**: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8 **User-Agent**: Mozilla/5.0 (Windows NT 6.1; rv:33.0) Gecko/20100101 Firefox/33.0 **Accept-Charset**: GBK,utf-8;q=0.7,\*;q=0.3 **Host**: 192.168.17.117 **cookie**: \_site\_id\_cookie=1;JSESSIONID=0E53A518DB91D00D2FEDC601BAEFFCE4 **Referer**: http://192.168.17.117/ |