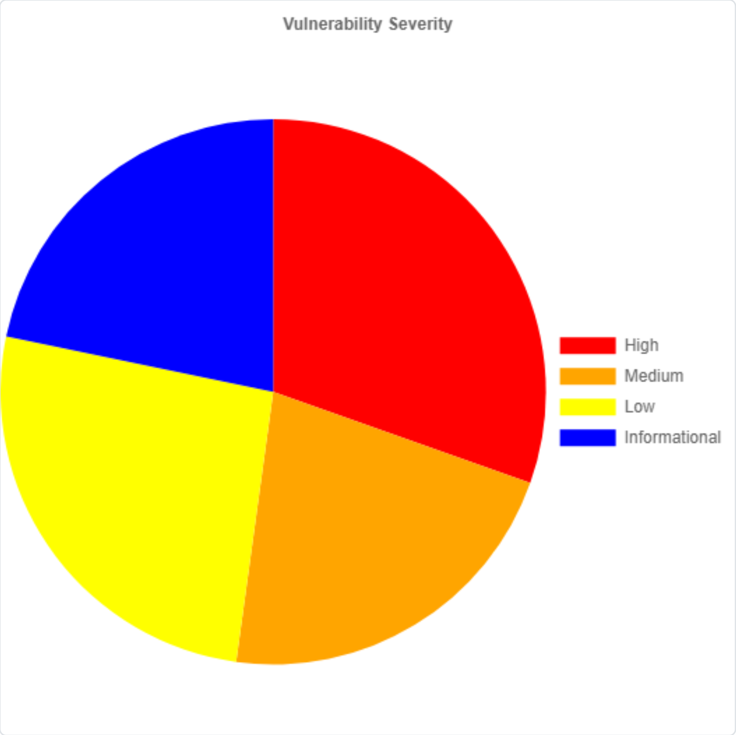
ZAP Scanning Report - imigrasi.go.id

Generated on Thu, 9 Feb 2023 21:19:20

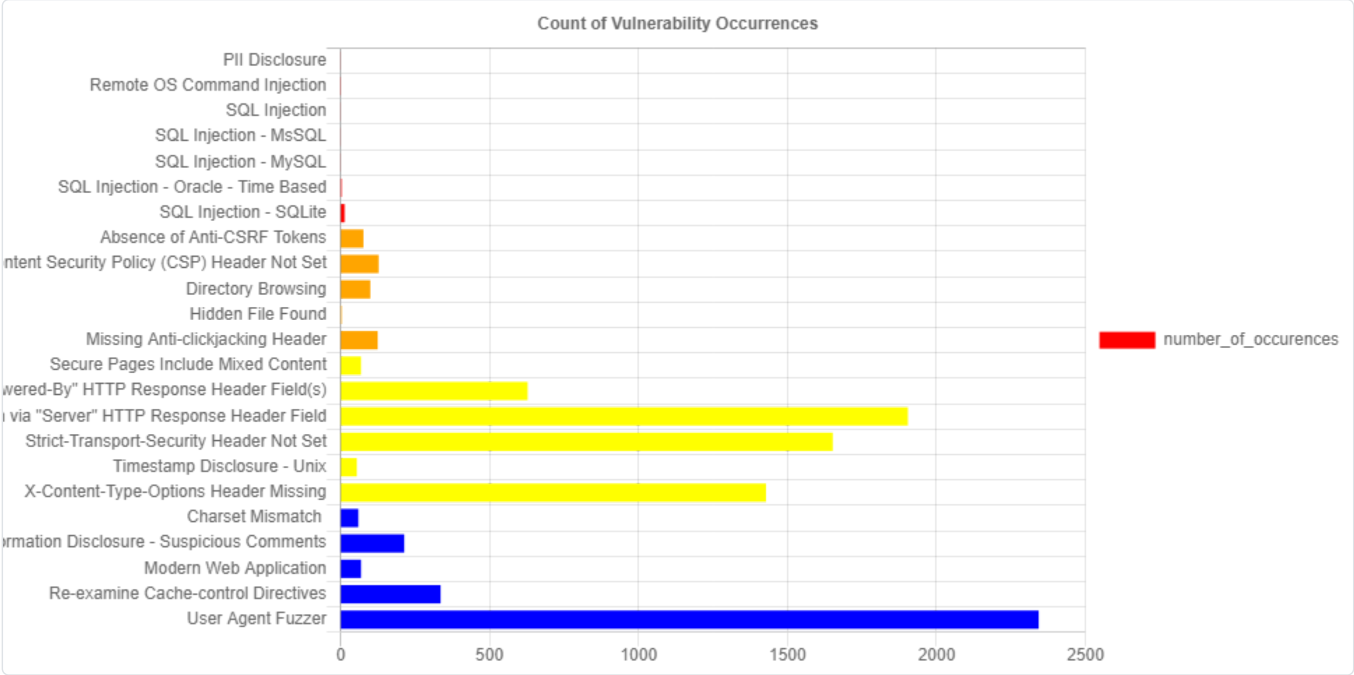
Most Severe Alert

High



Most Common Bug

User Agent Fuzzer (2343)



Vulnerability Impact

#	Name	Impact

1	PII Disclosure	The response contains Personally Identifiable Information, such as CC number, SSN and similar sensitive data.
2	Remote OS Command Injection [1] [2]	Attack technique used for unauthorized execution of operating system commands. This attack is possible when an application accepts untrusted input to build operating system commands in an insecure manner involving improper data sanitization, and/or improper calling of external programs.
3	SQL Injection [1]	SQL injection may be possible
4	SQL Injection - MsSQL [1]	SQL injection may be possible
5	SQL Injection - MySQL [1]	SQL injection may be possible
6	SQL Injection - Oracle - Time Based [1]	SQL injection may be possible
7	SQL Injection - SQLite [1]	SQL injection may be possible
8	Absence of Anti-CSRF Tokens [1] [2]	No Anti-CSRF tokens were found in a HTML submission form.
9	Content Security Policy (CSP) Header Not Set [1] [2] [3] [4] [5] [6] [7]	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
10	Directory Browsing [1] [2]	It is possible to view the directory listing. Directory listing may reveal hidden scripts, include files, backup source files, etc. which can be accessed to read sensitive information.
11	Hidden File Found [1]	A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.
12	Missing Anti-clickjacking Header [1]	The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.
13	Secure Pages Include Mixed Content [1]	The page includes mixed content, that is content accessed via HTTP instead of HTTPS.
14	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) [1] [2]	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
15	Server Leaks Version Information via "Server" HTTP Response Header Field [1] [2] [3] [4]	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
16	Strict-Transport-Security Header Not Set [1] [2] [3] [4] [5]	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
17	Timestamp Disclosure - Unix [1]	A timestamp was disclosed by the application/web server - Unix
18	X-Content-Type-Options Header Missing [1] [2]	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
19	Charset Mismatch [1]	This check identifies responses where the HTTP Content-Type header declares a charset different from the charset defined by the body of the HTML or XML. When there's a charset mismatch between the HTTP

		header and content body Web browsers can be forced into an undesirable content-sniffing mode to determine the content's correct character set.
20	Information Disclosure - Suspicious Comments	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
21	Modern Web Application	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
22	Re-examine Cache-control Directives [1] [2] [3]	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
23	User Agent Fuzzer [1]	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

Vulnerability Descriptions