**SUMMITSECURITIES POC**

|  |  |
| --- | --- |
| Title: Directory Enumeration | |
| Description: | |
| it includes internal login pages. | |
| Affected Resources | Severity |
| https://www.summitsecurities.net/ | **Critical** |
| Impact | |
| Can Lead to critical information leakage. | |
| Recommendation | |
| Add the file in robot.txt in disallow state, check access for specific user | |
| Tool Used | References |
| DirBuster |  |
| POC | |
|  | |

|  |  |
| --- | --- |
| Title: Found Open Ports | |
| Description: | |
| Open Ports are revealing the Service Version that the server is running On. | |
| Affected Resources | Severity |
| https://www.summitsecurities.net/ | **High** |
| Impact | |
| The attacker can use this version for finding exploits (pentesting using Metasploit) | |
| Recommendation | |
| Please the in Production that the relevant ports are required, keep the server up to date | |
| Tool Used | References |
| NMAP | [WSTG - Latest | OWASP Foundation](https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/01-Information_Gathering/04-Enumerate_Applications_on_Webserver) |
| POC | |
|  | |

**NESSUS SCAN-**

|  |  |
| --- | --- |
| Title: Outdated Version Found | |
| Description: | |
| TLS and SSH version are outdated | |
| Affected Resources | Severity |
| https://www.summitsecurities.net/ | **HIGH** |
| Impact | |
| The Version are vulnerable to exploits | |
| Recommendation | |
| Please update to Latest Version | |
| Tool Used | References |
| Nessus | [A06 Vulnerable and Outdated Components - OWASP Top 10:2021](https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/) |
| POC | |
|  | |

**ZAP Vulnerabilities-**

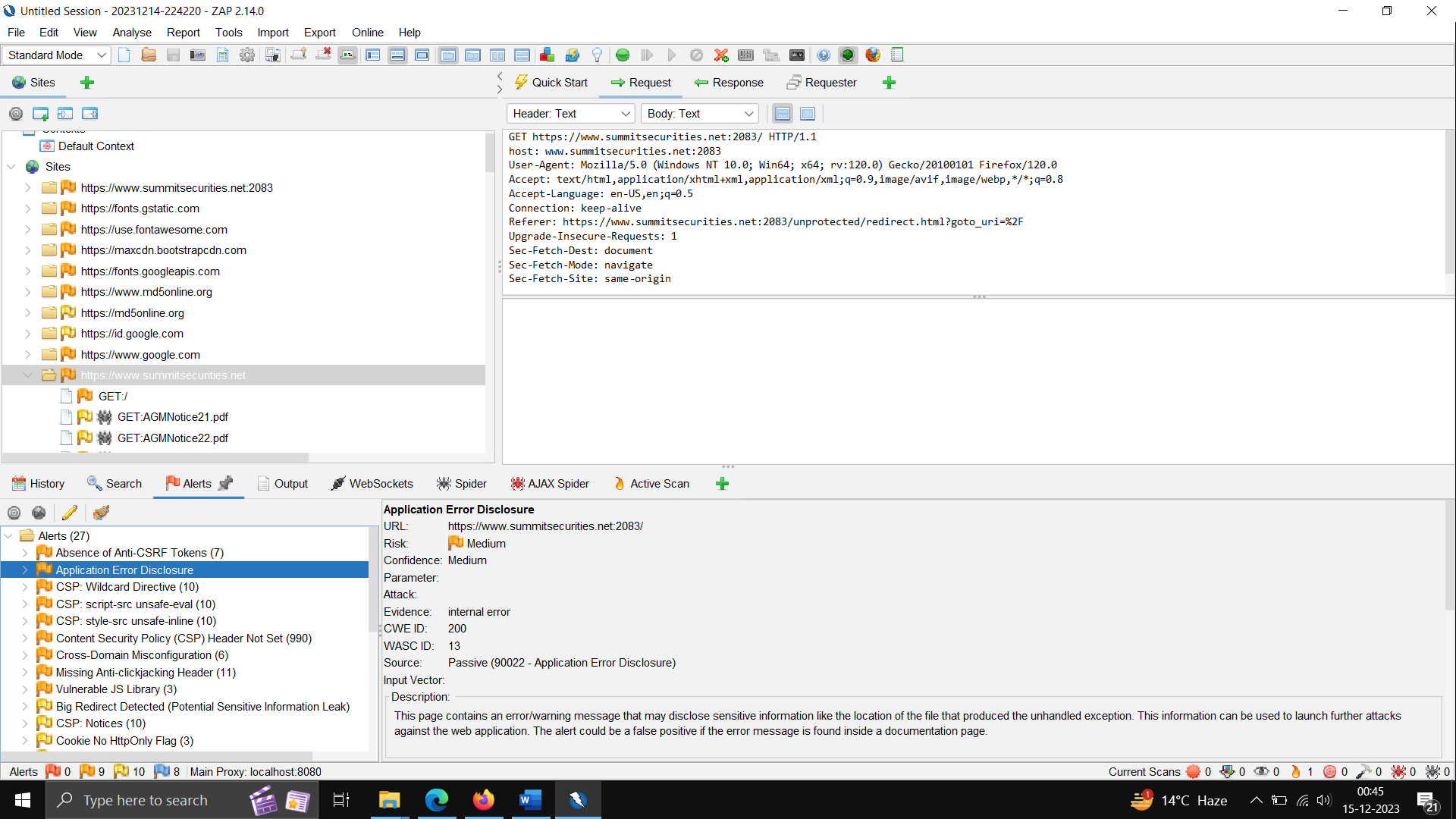
Request/Response –

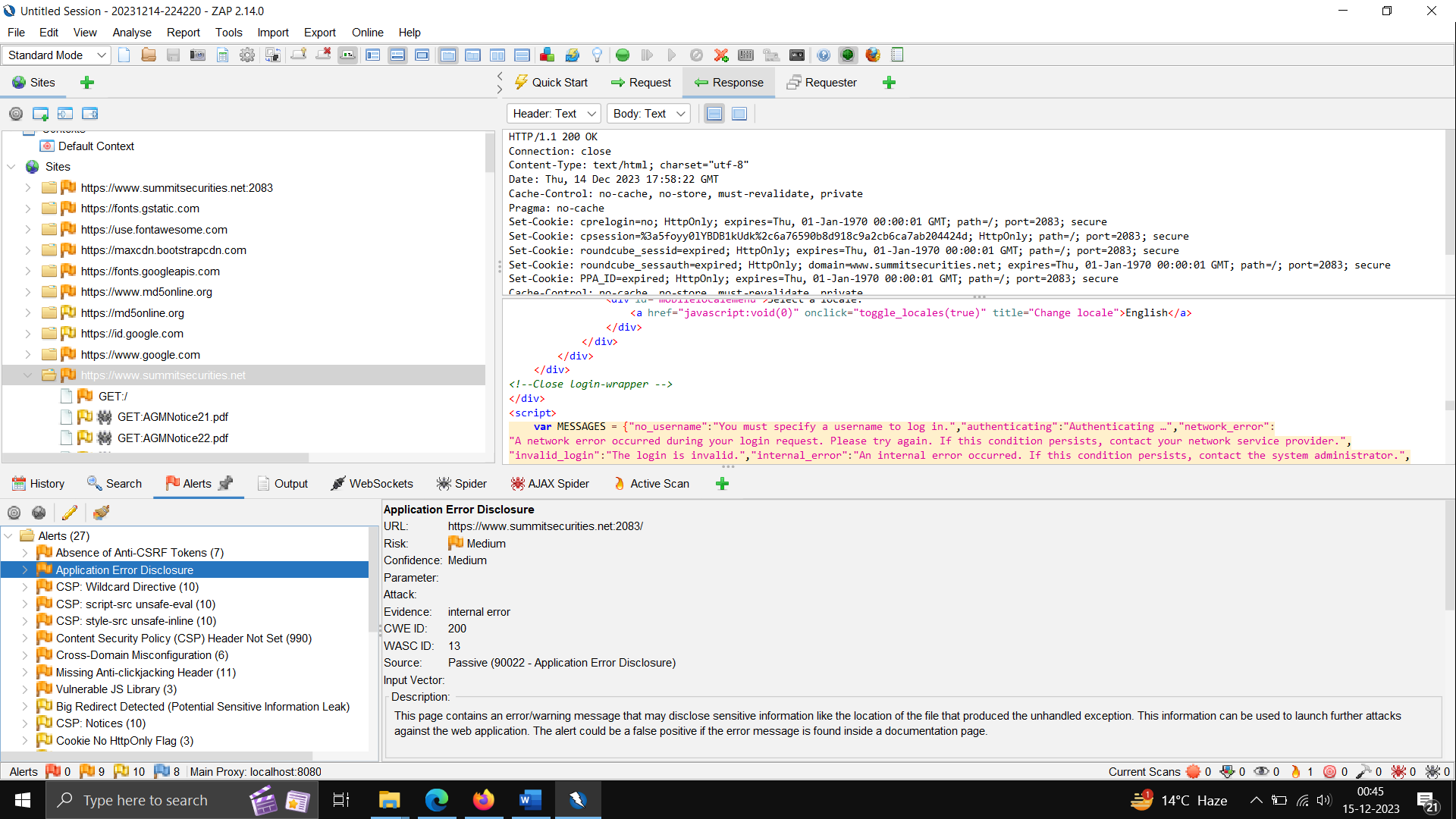
**Description** – This Page contains an error/warning that may disclose sensitive information

**Impact** - Can reveal user access, software we are using that can be used for exploiting

**Severity** – MEDIUM

**Reference** - [Improper Error Handling | OWASP Foundation](https://owasp.org/www-community/Improper_Error_Handling)





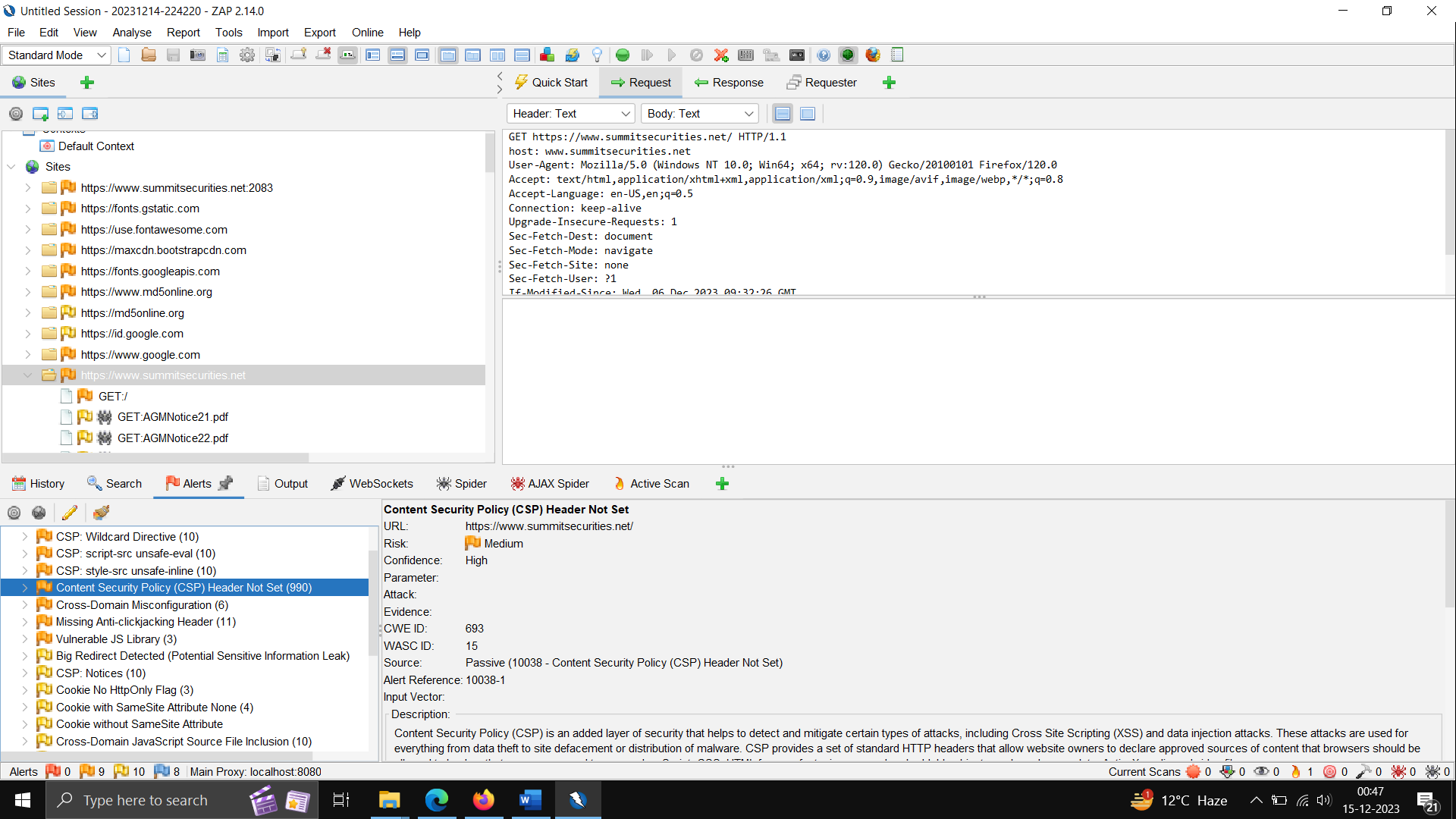
Req/Reponse –

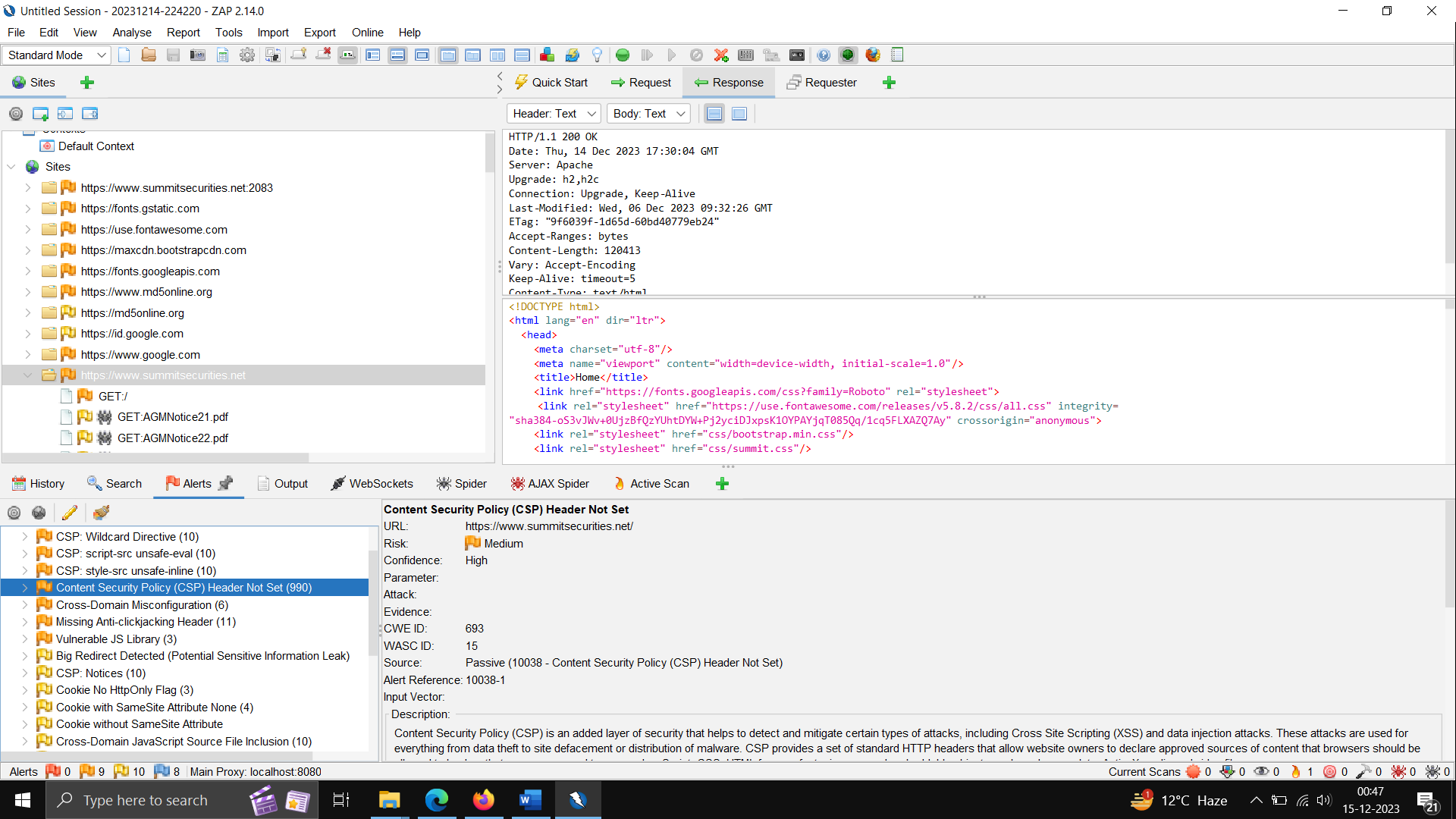
**Description** – By injecting the Content-Security-Policy (CSP) headers from the server, the browser is aware and capable of protecting the user from dynamic calls that will load content into the page currently being visited.

**Impact** – Cross Site Scripting ,increase in XSS (Cross-Site Scripting), clickjacking, and cross-site leak vulnerabilities.

**Severity** – MEDIUM

**Reference** - [Content Security Policy - OWASP Cheat Sheet Series](https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html)





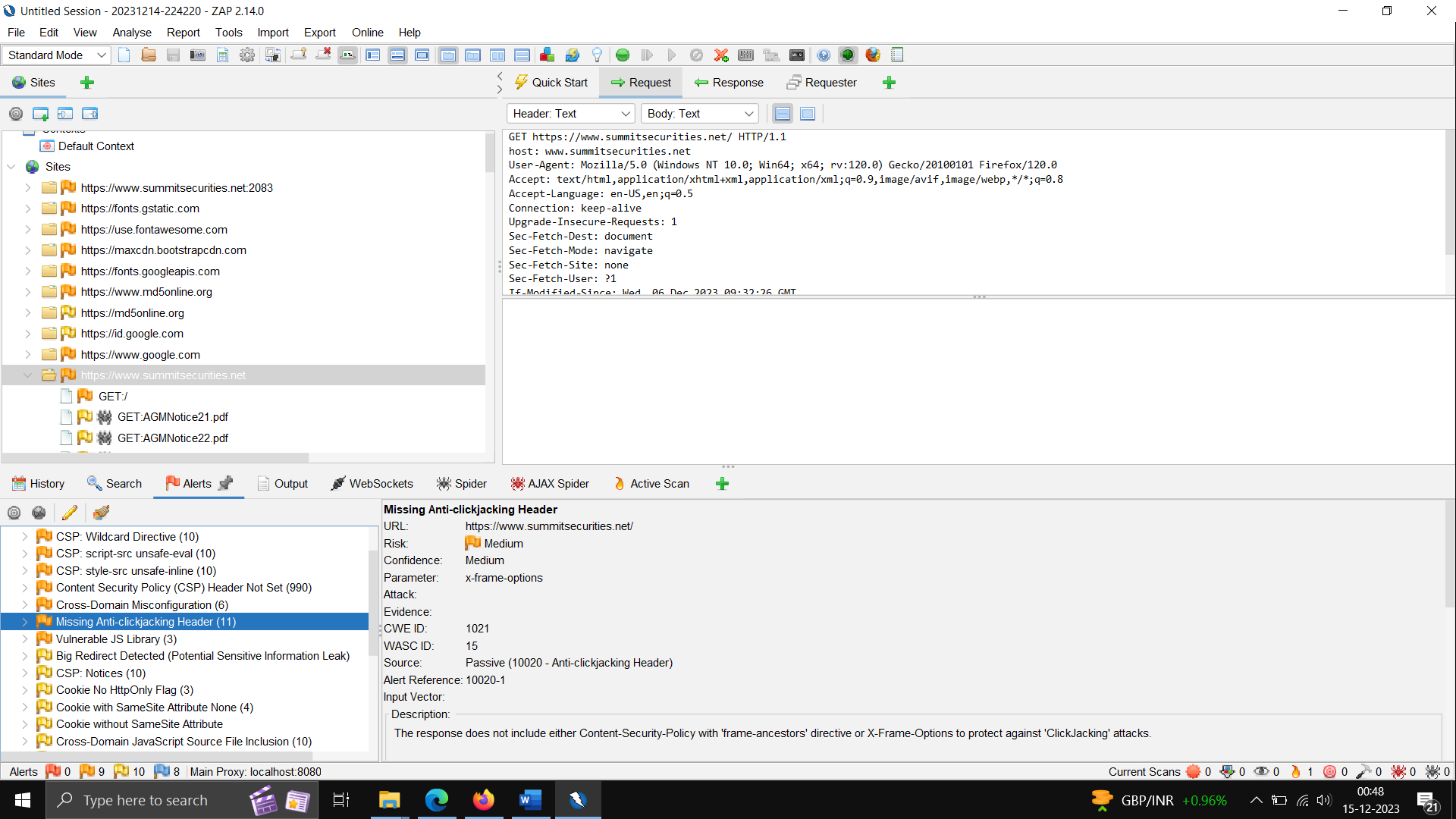
Req/reponse –

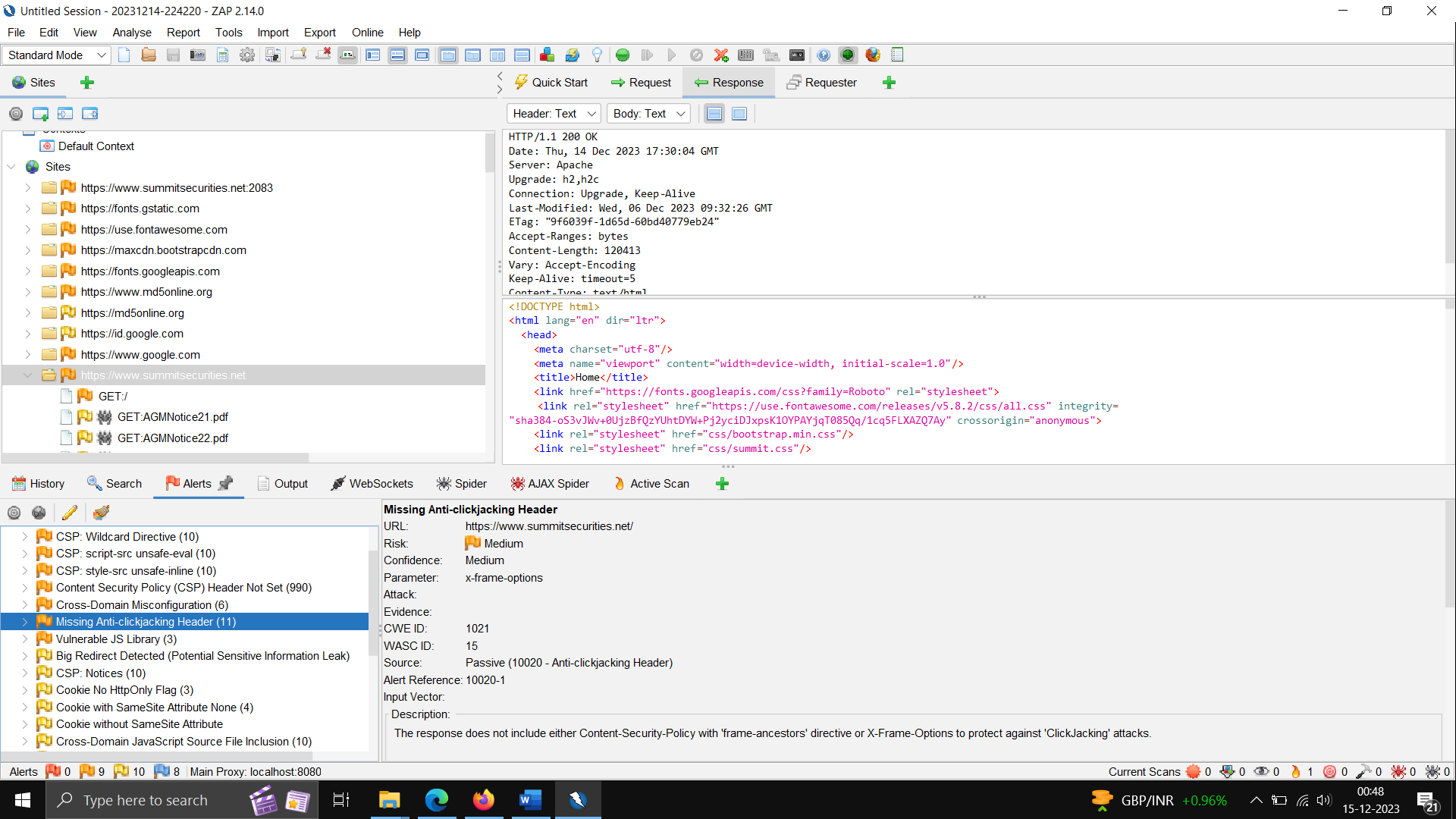
**Description** – he response does not include either Content-Security-Policy with ‘frame-ancestors’ directive or X-Frame-Options to protect against ‘ClickJacking’ attacks.

**Impact -**Clickjacking is a serious threat to internet users as it can lead to unauthorized actions being taken on their behalf and can also expose sensitive data.

**Severity** – MEDIUM

**Reference** - [ZAP – Missing Anti-clickjacking Header (zaproxy.org)](https://www.zaproxy.org/docs/alerts/10020-1/)





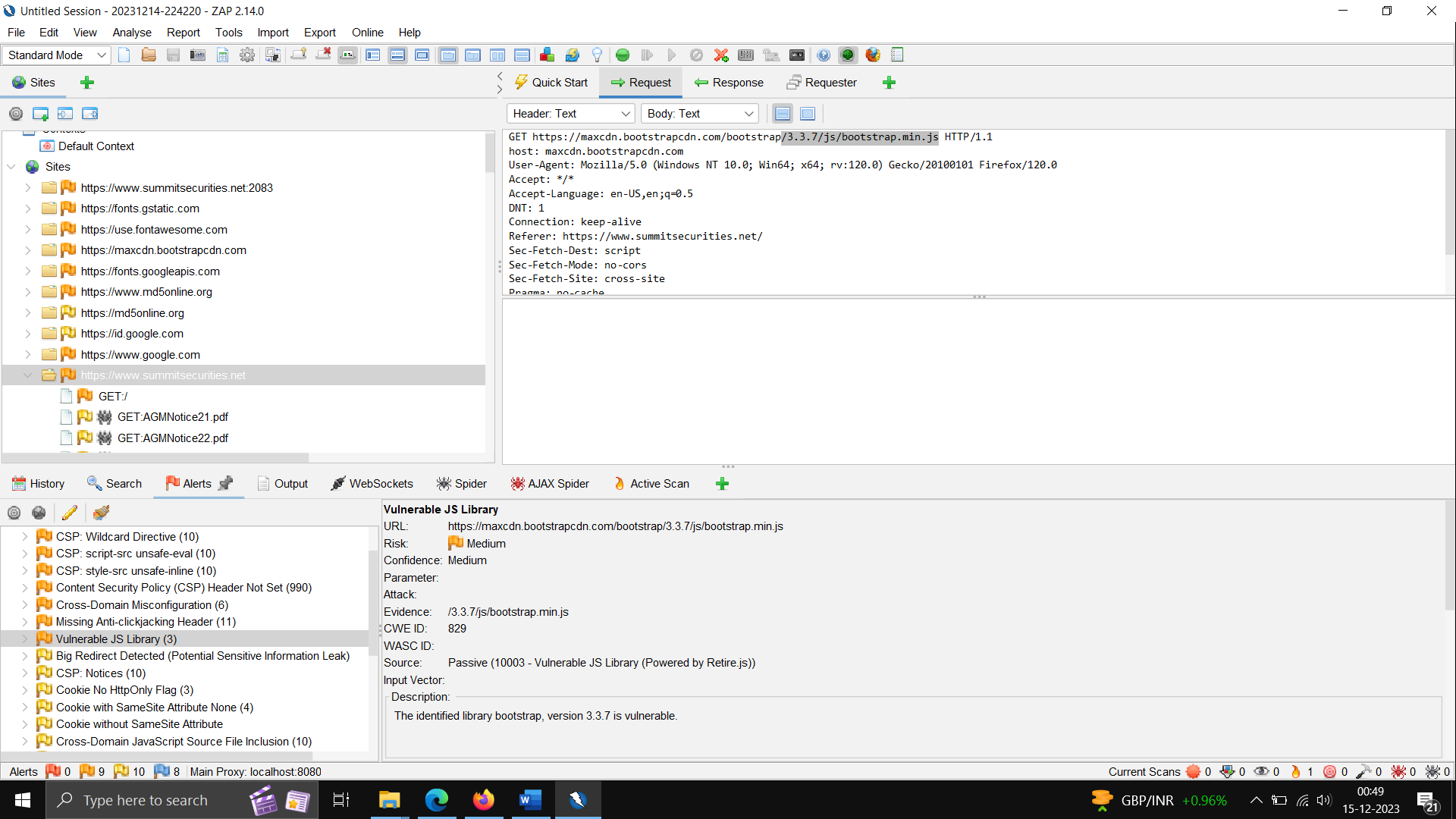
Req/Response –

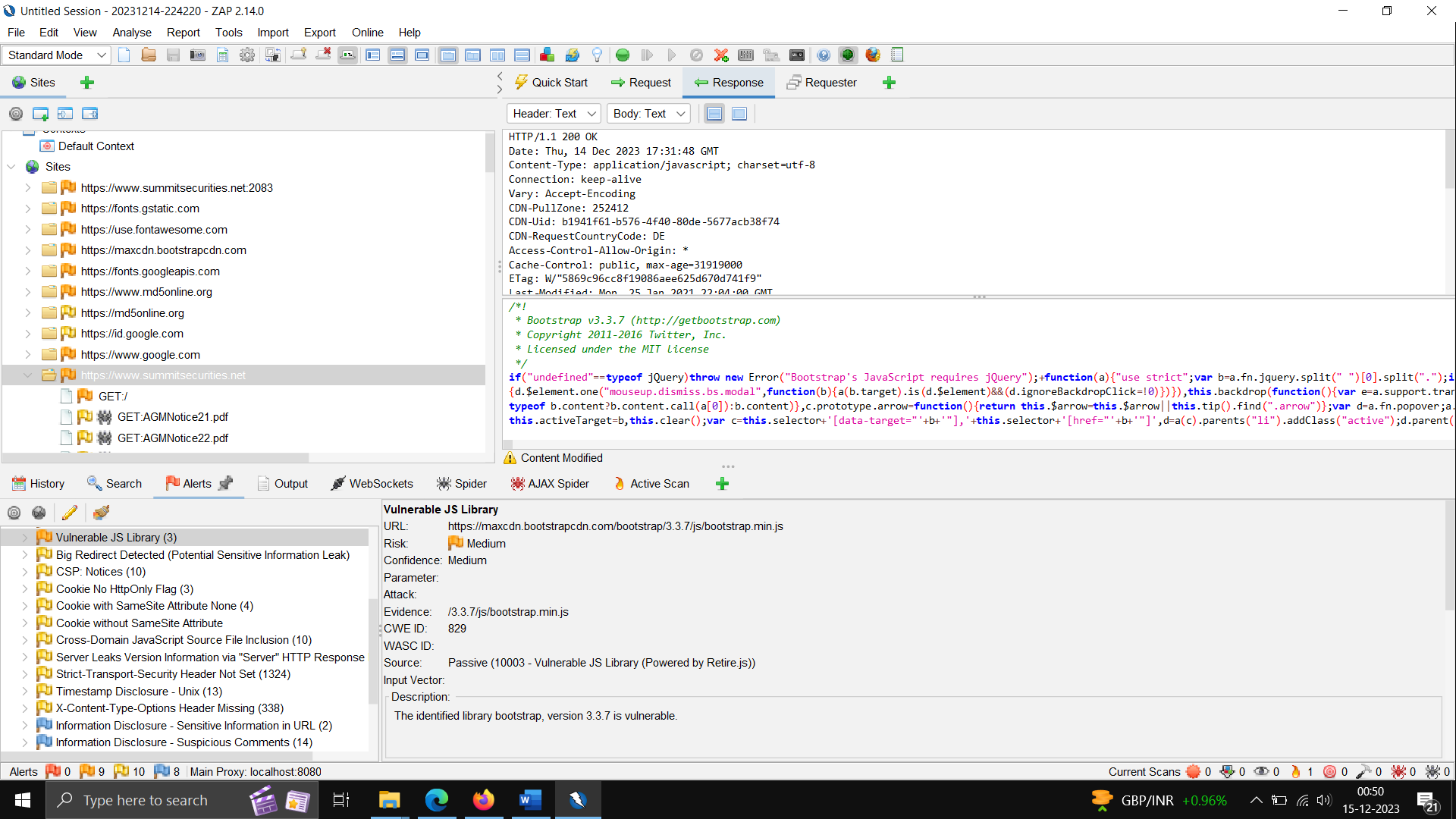
**Description** – Using outdated JS library.

**Impact** – Can be Used for executing malicious script.

**Severity** – MEDIUM

**Reference** - [A06 Vulnerable and Outdated Components - OWASP Top 10:2021](https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/)





BURPSUITE USECASE - login to <https://www.summitsecurities.net/webmail> and try longing, we can saying parameter are unencrypted.

