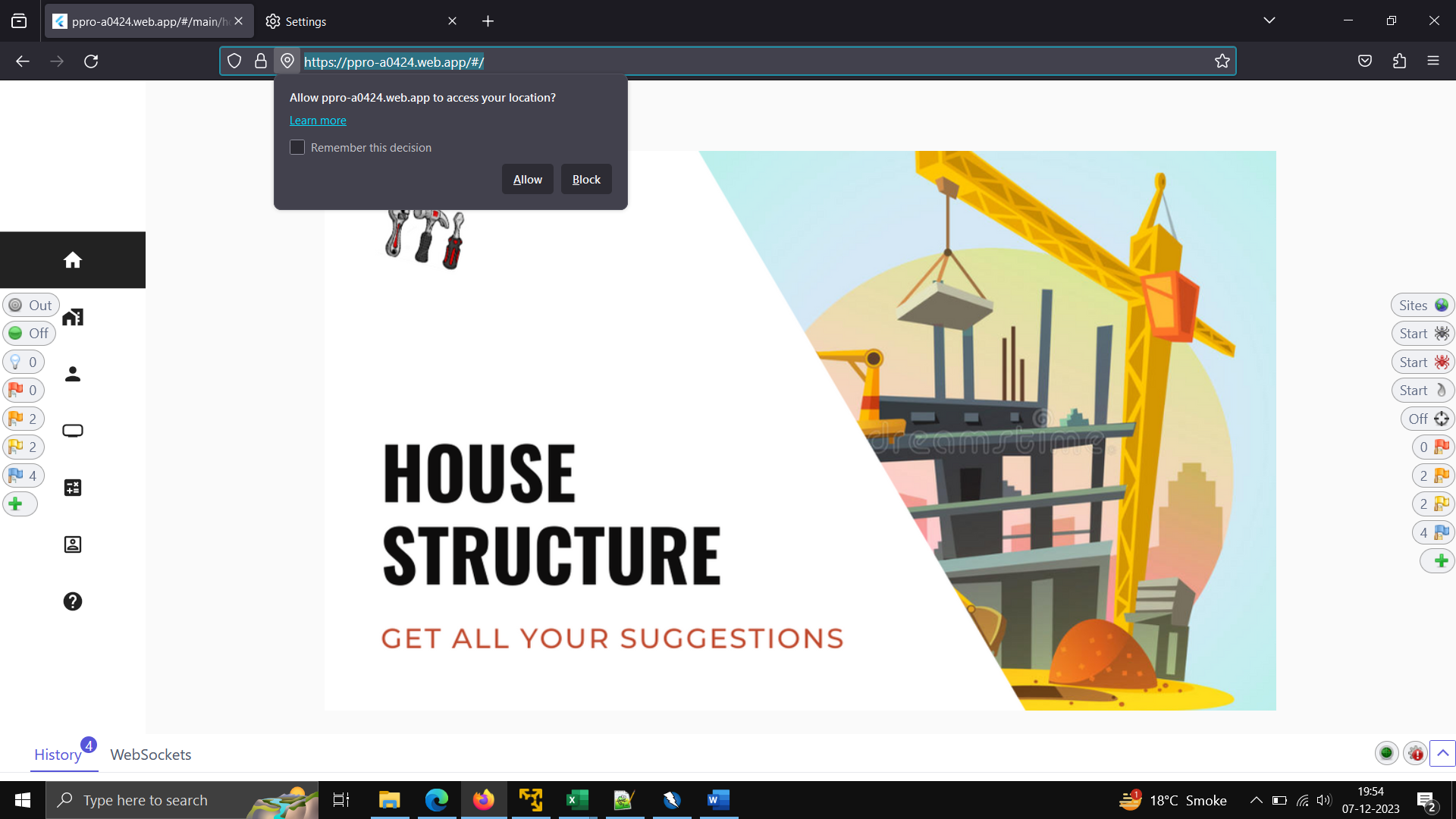
**SSCBS**

**MAYANK CHOPRA**

**ROLLNO -23719**

**ASSIGNMENT FOR ZAP PROXY**

**Target Website - >** [**https://ppro-a0424.web.app/#/**](https://ppro-a0424.web.app/#/)



**Attacks Encountered ->**

**Content Security Policy (CSP) Header Not Set**

**Description - >**

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.

**Impact ->**

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.

**Reference –**

**https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing\_Content\_Security\_Policy**

**Severity -MEDIUM**

**Solution –**

Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

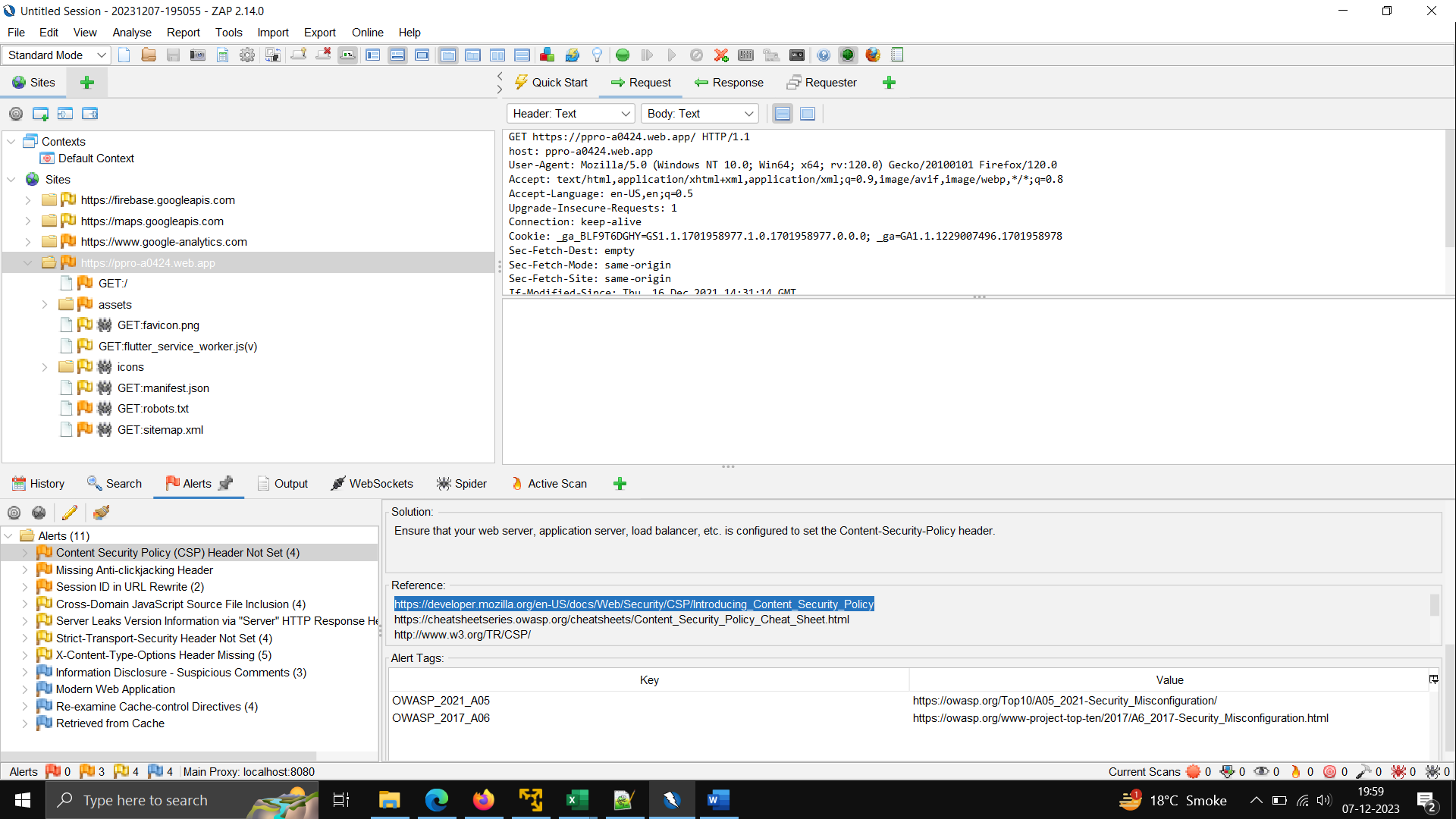
POC –

Step1 – Open Firefox browser and step the proxy, open the desired website

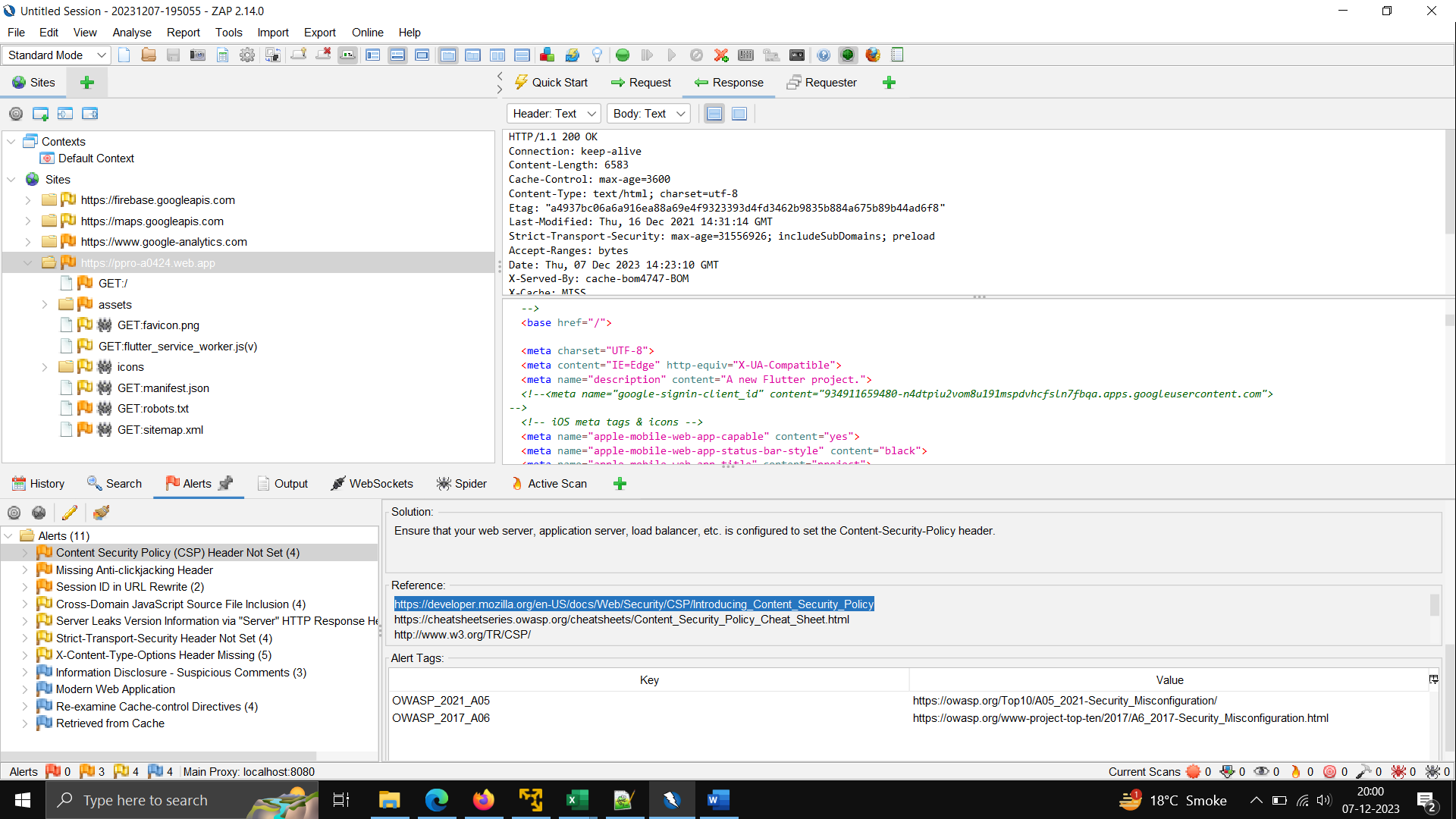
Step2 – Start the Zap Proxy, reload the website and click on selected target.

Step3 – Automatic Scan

Request->



Response ->



Second Attack ->**Session ID in URL Rewrite**

**Description ->**

URL rewrite is used to track user session ID. The session ID may be disclosed via cross-site referrer header. In addition, the session ID might be stored in browser history or server logs.

**Impact - >**

The Session Id can be used to login through unauthorize way.

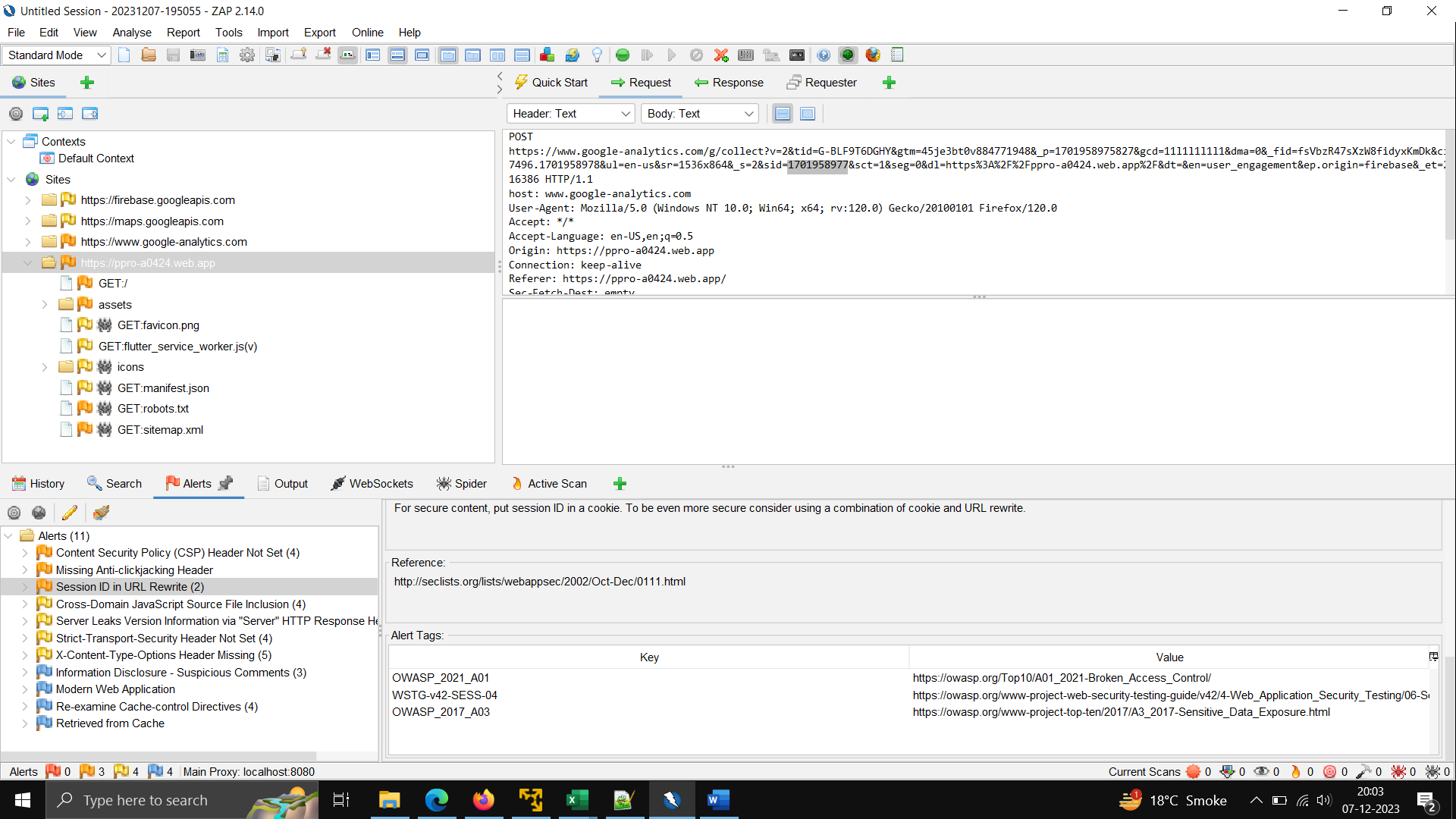
Reference-

<http://seclists.org/lists/webappsec/2002/Oct-Dec/0111.html>

**Severity -MEDIUM**

POC – same as above

Request - >



Response - >

