

Burp Suite Community Edition

Manual Report

IT Support Chatbot project -Burp Suite vulnerability assessment report

Site: <https://sec.cse.csusb.edu/team1>

Manual report by: Vamsi Krishna Bandaru

Objective

- To identify and analyze potential vulnerabilities in the chatbot system using Burp Suite Community Edition

Methodology

- **Approach:**
 - Intercept and analyze HTTP request and responses
 - Test for common vulnerabilities like SQL injection and security misconfigurations

Findings

- **Overview Table:**

Vulnerability	Severity	Description	Recommendation
Cross-Origin WebSocket Hijacking (CSWSH)	Low	Server blocks unauthorized WebSocket connections.	Maintain configuration. Test for bypass.
Improper Origin Validation	Medium	Server relies on expected origins.	Enhance origin verification with tokens.
Security Misconfiguration	Low	Default WebSocket settings permit insecurity.	Audit and update WebSocket settings.

Burp Suite screenshots

- Request and response in repeater after modifications

The screenshot displays the Burp Suite Repeater interface. On the left, the 'Request' tab is active, showing a GET request to `/team1/_store/stream HTTP/1.1`. The request body contains headers and a body with a JavaScript payload. A red arrow points to the 'Send' button, labeled '2. click here after modifications'. Another red arrow points to the 'Modified request' label. On the right, the 'Response' tab is active, showing an HTTP 403 Forbidden response from TornadoServer/6.4.1. The response body contains the message 'Cross origin websockets not allowed'.

HTTP requests

- List of HTTP requests captured while intercepting IT Support Chatbot

The screenshot displays the Burp Suite HTTP history interface. The table lists captured HTTP requests, including details such as Host, Method, URL, Params, Status code, Length, MIME type, Extension, Title, Notes, TLS, IP, Cookies, Time, Listener port, and Start response time. The table is filtered to show only HTTP requests. The first few rows show requests to `http://localhost:5001` with various methods (GET, POST) and URLs (e.g., `/team1/_store/stream`, `/team1/_store/host-config`). The table is sorted by Time, showing a sequence of requests from 13:09:17 to 14:20:47.

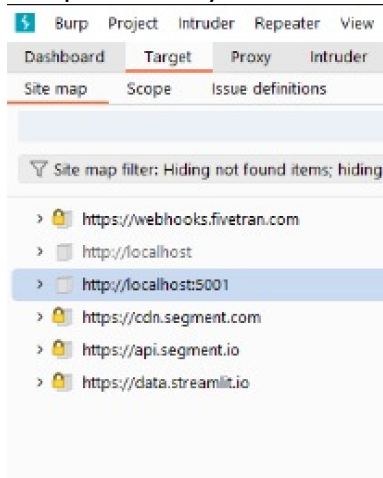
Target Tab and Sitemap

- Sitemap Analysis

Endpoint	Method	Description
/webhooks.fivetran.com	POST	Handles incoming webhooks from Fivetran
/localhost:5001	GET	Local development server endpoint
/cdn.segment.com	GET	Retrieves static assets for Segment integration
/api.segment.io	POST	API endpoint for Segment data collection
/data.streamlit.io	GET	Accesses data hosted on Streamlit's servers

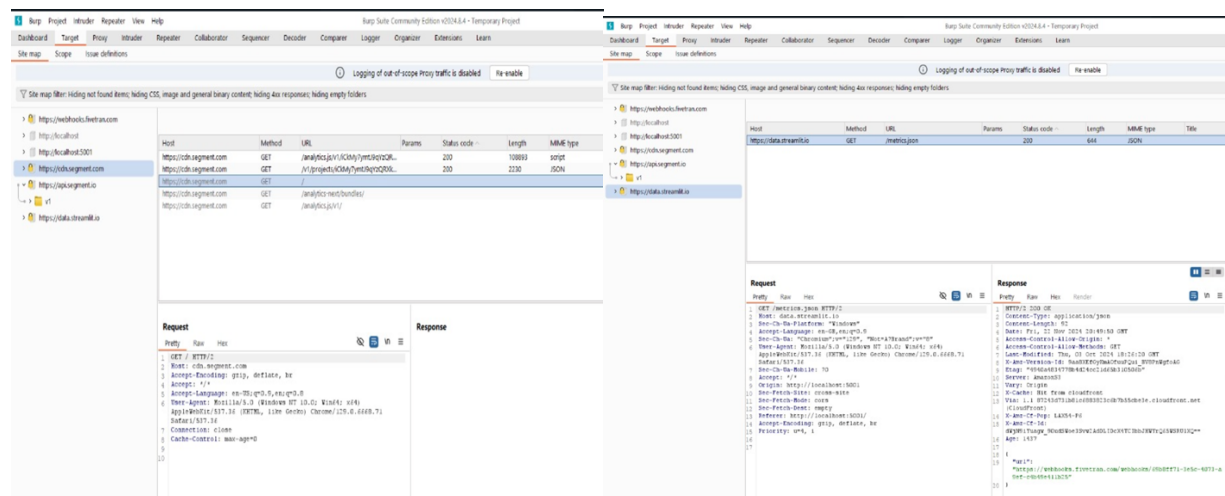
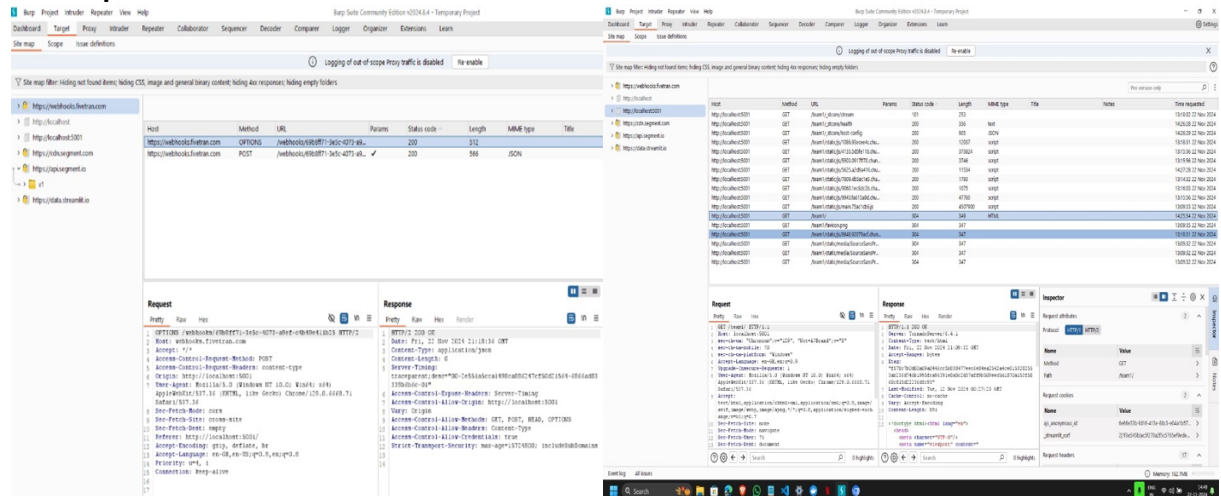
Sitemap screenshots

- End points analyzed



- Endpoint: /webhooks.fivetran.com, /localhost:5001, /cdn.segment.com, /api.segment.io, /data.streamlit.io
- **/webhooks.fivetran.com**: 200 OK status. Proper handling of data sent to the endpoint
- **/localhost:5001**: 200 OK. The server is running correctly and serving the content as expected during local testing
- **/cdn.segment.com**: 200 OK. Static assets scripts, stylesheets were retrieved successfully, suggesting no issues with content delivery
- **/api.segment.io**: 200 OK status. The API endpoint successfully handled the request, likely returning data related to user tracking, analytics
- **/data.streamlit.io**: 200 OK status. Confirms that the data hosted on Streamlit's platform was successfully accessed

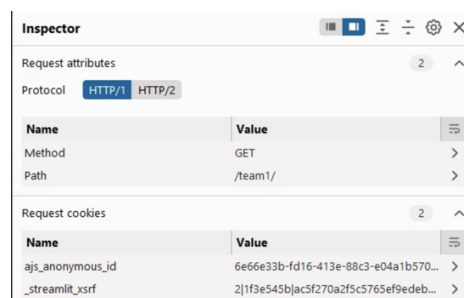
Sitemap screenshots:



Dash board inspector

- **Request Headers:** "Connection: keep-alive" header keeps the connection open for multiple requests, improving network performance by reusing the same connection
- **Response Headers:** "vary: Accept-Encoding" the response may change based on the client's Accept-Encoding, typically to handle compressed formats like gzip or deflate

Screenshots of inspector



Request headers			Response headers		
Name	Value		Name	Value	
Host	localhost:5001	>	Server	TornadoServer/6.4.1	>
sec-ch-ua	"Chromium";v="129", "Not=A?Brand"...	>	Content-Type	text/html	>
sec-ch-ua-mobile	?0	>	Date	Fri, 22 Nov 2024 21:09:32 GMT	>
sec-ch-ua-platform	"Windows"	>	Accept-Ranges	bytes	>
Accept-Language	en-GB,en;q=0.9	>	Etag	"f578c7b0d00a09a0446cc5b838477e..."	>
Upgrade-Insecure-Requests	1	>	Last-Modified	Tue, 12 Nov 2024 00:27:23 GMT	>
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64...	>	Cache-Control	no-cache	>
Accept	text/html,application/xhtml+xml,application/javascript;q=0.9,*/*;q=0.8	>	Vary	Accept-Encoding	>
Sec-Fetch-Site	none	>	Content-Length	891	>
Sec-Fetch-Mode	navigate	>			
Sec-Fetch-User	?1	>			
Sec-Fetch-Dest	document	>			
Accept-Encoding	gzip, deflate, br	>			
Cookie	ajs_anonymous_id=6e66e33b-fd16-4...	>			
If-None-Match	"2c06f1bb433d252a1eb544504956de..."	>			
If-Modified-Since	Tue, 01 Oct 2024 21:34:20 GMT	>			
Connection	keep-alive	>			

Conclusion

- **HTTP Headers**
 - "Connection: keep-alive" enhances performance but may pose security risks if not managed
 - "Vary: Accept-Encoding" optimizes caching but could lead to cache poisoning if misconfigured
- **Sitemap Endpoints**
 - /webhooks.fivetran.com, /localhost:5001, /cdn.segment.com, /api.segment.io, /data.streamlit.io were accessible, indicating functional responses
- **WebSocket Security Testing**
 - The server blocks WebSocket connections from unauthorized origins, preventing CSWSH, with strong protections against header modifications like Origin, Sec-WebSocket-Key, and Sec-WebSocket-Protocol