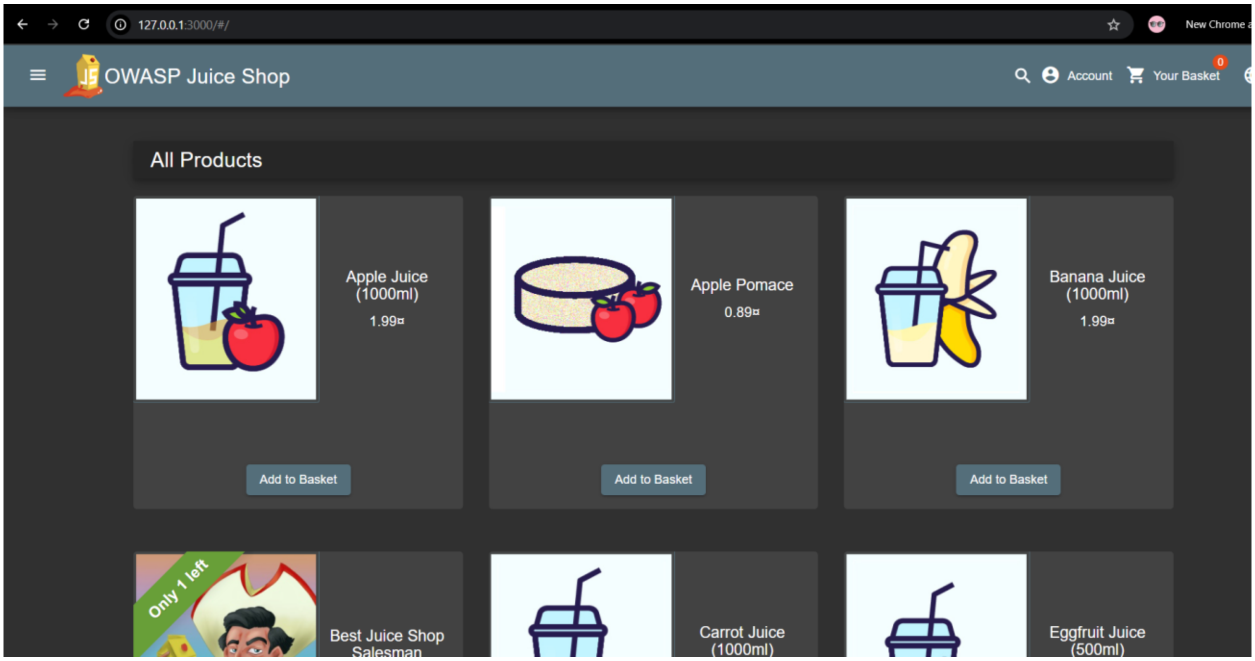
OWASP Juice Shop:



Attack Report:

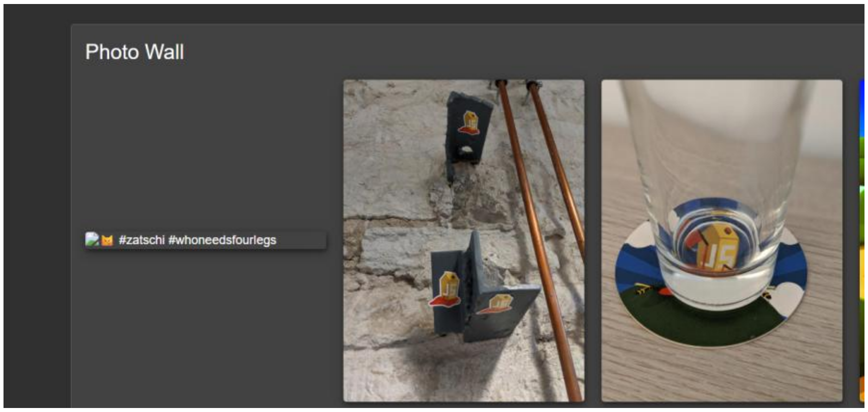
Practical Applications/Implementations in Daily Life of this Lab:

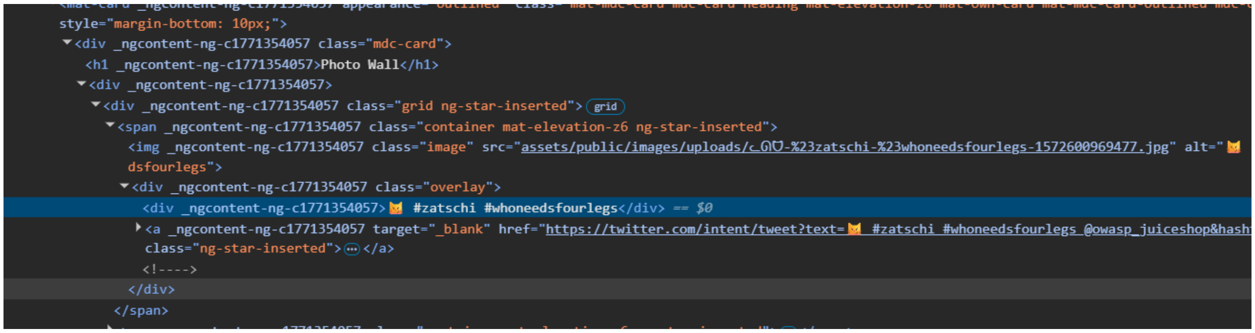
These labs demonstrate actual issues that might arise on websites. They aid in increasing our awareness of how hackers can execute malicious code, fool individuals into clicking on malicious links, or access personal data. Gaining this knowledge enables security teams and developers to address issues early and protect their customers.

Lab 01: Missing Encoding

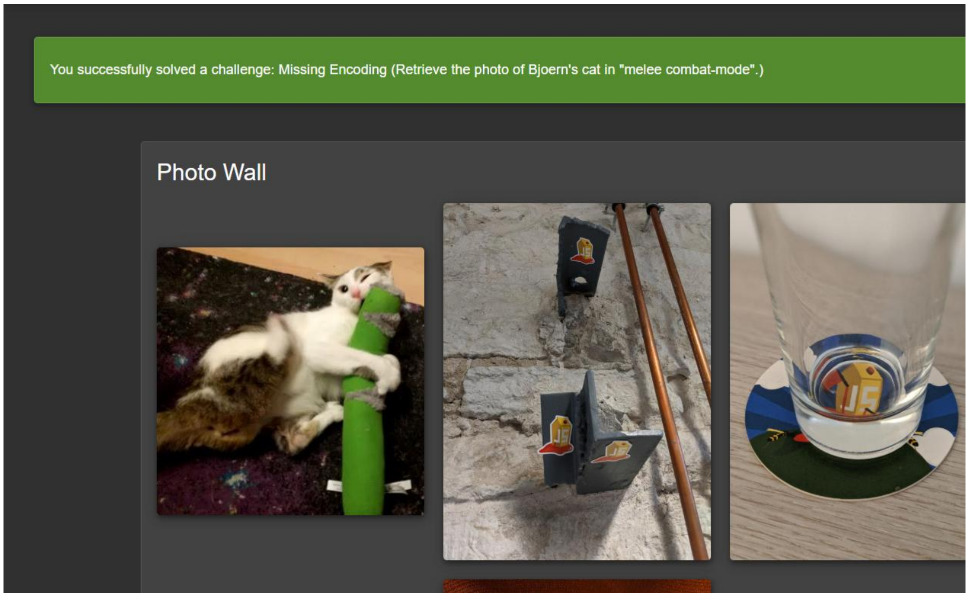
When I opened the Photo Wall site, I saw that one picture was not loading. I checked the code using Inspector tool pre-bult in browsers and discovered a # in the picture link. I found that # should be typed as %23 by using the (encoder-decoder website: meyerweb.com/eric/tools/dencoder/). That means, the site was not properly encoded, which was prevnting the image from loading.

The image failed to load, and the browser could not be able to interpret input as code. Missing encoding (CWE-116) is risky because it allows attackers to run malicious code or steal user data because a website fails to process special symbols correctly.





```
<mat-card _ngcontent-ng-c1771354057 appearance="outlined" class="mat-mdc-card mdc-card heading mat-elevation-z6 mat-own-card mat-mdc-card-outlined mdc-c
style="margin-bottom: 10px;">
 ▼<div _ngcontent-ng-c1771354057 class="mdc-card">
    <h1 _ngcontent-ng-c1771354057>Photo Wall</h1>
   ▼<div _ngcontent-ng-c1771354057>
     ▼<div _ngcontent-ng-c1771354057 class="grid ng-star-inserted"> grid
       ▼<span _ngcontent-ng-c1771354057 class="container mat-elevation-z6 ng-star-inserted">
          <img _ngcontent-ng-c1771354057 class="image" src="assets/public/images/uploads/ᓚᘏᗢ-%23zatschi-%23whoneedsfourlegs-1572600969477.jpg" alt="😼
          dsfourlegs">
         ▼<div _ngcontent-ng-c1771354057 class="overlay">
            <div _ngcontent-ng-c1771354057>😼 #zatschi #whoneedsfourlegs</div> == $0
           ▶<a _ngcontent-ng-c1771354057 target="_blank" href="https://twitter.com/intent/tweet?text=😼 #zatschi #whoneedsfourlegs @owasp_juiceshop&hash
            class="ng-star-inserted">⋯</a>
            <!---->
          </div>
        </span>
```



You successfully solved a challenge: Missing Encoding (Retrieve the photo of Bjoern's cat in "melee combat-mode".)

Photo Wall

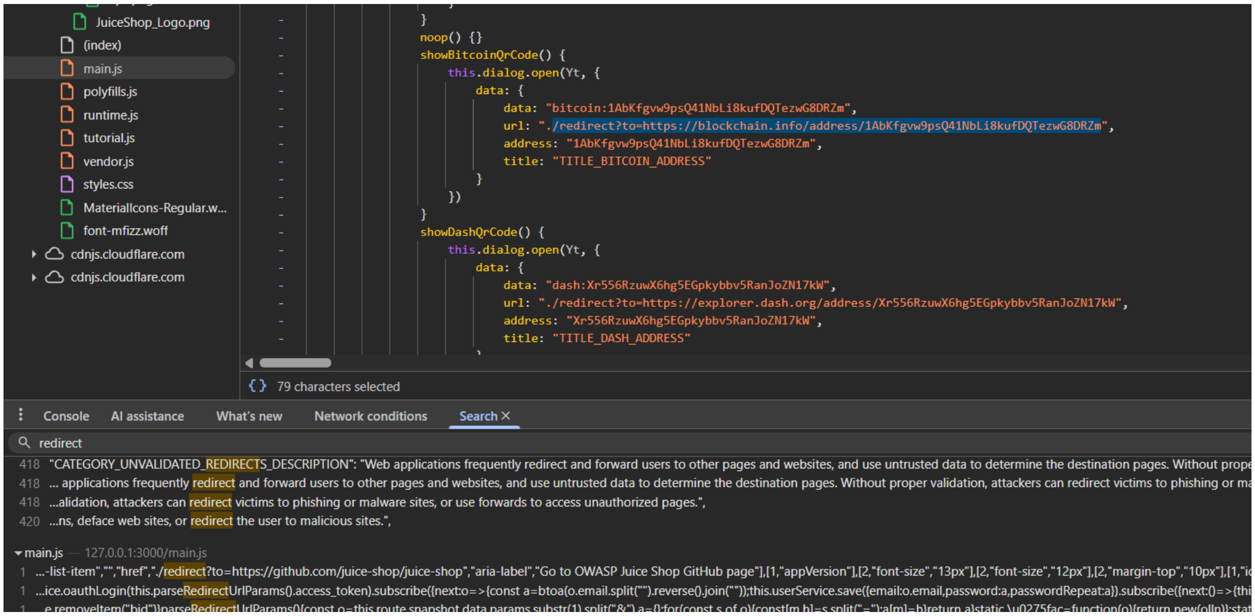
References:

https://www.youtube.com/watch?v=W7Bt2AmYtao

https://cwe.mitre.org/data/definitions/116.html

Lab 02: Outdated Allowlist [Redirection]

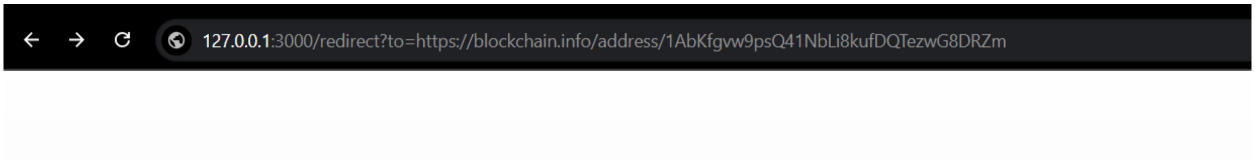
I looked at the code using Inspector tool pre-built in web browser [to see the source code] and discovered a redirect link in main.js. I then added the URL of Blockchain.info found in main.js after [http://127.0.0.1:3000/ - the website of OWASP juice shop] in the browser. And then upon opening it, I was redirected to blockchain.com. This is harmful, hackers can use it to direct users to malicious websites where they have uploaded malicious code if the user by mistakenly download it, then it might be possible that they could be hacked.



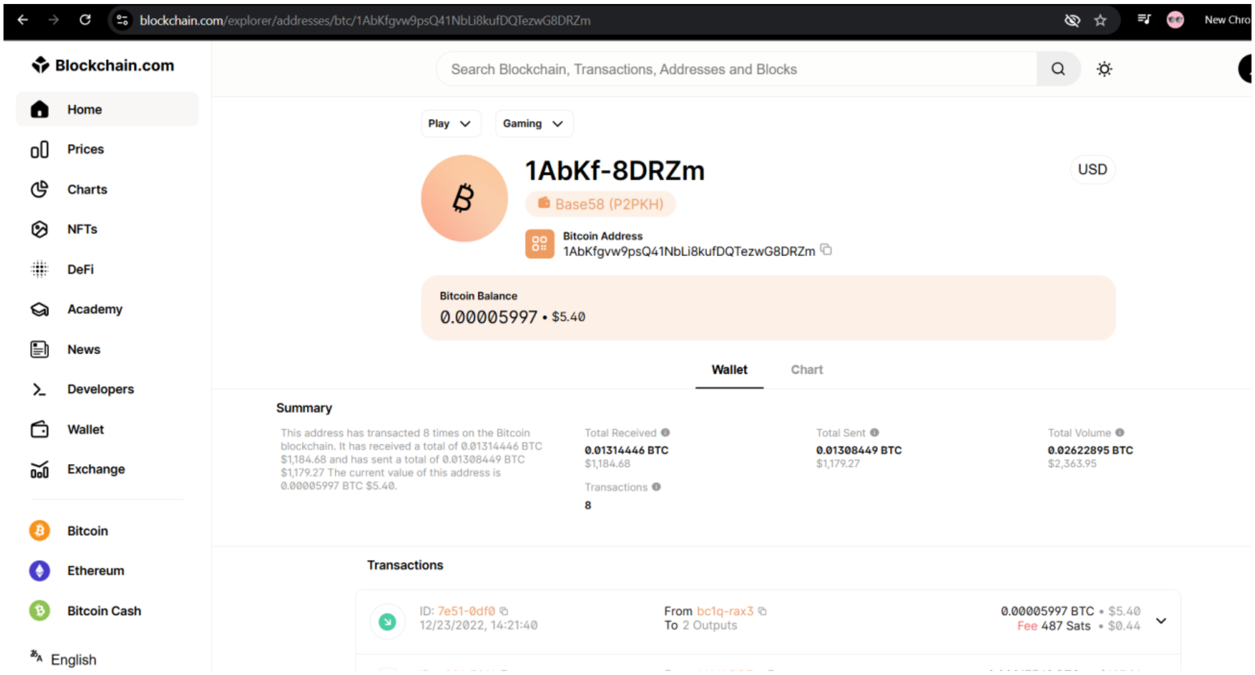
```
}
noop() {}
showBitcoinQrCode() {
    this.dialog.open(Yt, {
        data: {
            data: "bitcoin:1AbKfgvw9psQ41NbLi8kufDQTezwG8DRZm",
            url: "./redirect?to=https://blockchain.info/address/1AbKfgvw9psQ41NbLi8kufDQTezwG8DRZm",
            address: "1AbKfgvw9psQ41NbLi8kufDQTezwG8DRZm",
            title: "TITLE_BITCOIN_ADDRESS"
        }
    })
}
showDashQrCode() {
    this.dialog.open(Yt, {
        data: {
            data: "dash:Xr556RzuwX6hg5EGpkybbv5RanJoZN17kW",
            url: "./redirect?to=https://explorer.dash.org/address/Xr556RzuwX6hg5EGpkybbv5RanJoZN17kW",
            address: "Xr556RzuwX6hg5EGpkybbv5RanJoZN17kW",
            title: "TITLE_DASH_ADDRESS"
```

{ } 79 characters selected

```
redirect
418  "CATEGORY_UNVALIDATED_REDIRECTS_DESCRIPTION": "Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without prope
418  ... applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or ma
418  ...alidation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.",
420  ...ns, deface web sites, or redirect the user to malicious sites.",

main.js — 127.0.0.1:3000/main.js
1  ...-list-item","","href","./redirect?to=https://github.com/juice-shop/juice-shop","aria-label","Go to OWASP Juice Shop GitHub page"],[1,"appVersion"],[2,"font-size","13px"],[2,"font-size","12px"],[2,"margin-top","10px"],[1,"ic
1  ...ice.oauthLogin(this.parseRedirectUrlParams().access_token).subscribe({next:o=>{const a=btoa(o.email.split("").reverse().join(""));this.userService.save({email:o.email,password:a,passwordRepeat:a}).subscribe({next:()=>{thi
1  ...e.removeItem("bid")}parseRedirectUrlParams(){const o=this.route.snapshot.data.params.substr(1).split("&"),a={};for(const s of o){const[m,h]=s.split("=");a[m]=h}return a}static \u0275fac=function(o){return new(o||n)};stat
```



127.0.0.1:3000/redirect?to=https://blockchain.info/address/1AbKfgvw9psQ41NbLi8kufDQTezwG8DRZm



1AbKf-8DRZm

Base58 (P2PKH)

Bitcoin Address
1AbKfgvw9psQ41NbLi8kufDQTezwG8DRZm

Bitcoin Balance
0.00005997 • $5.40

Summary

This address has transacted 8 times on the Bitcoin blockchain. It has received a total of 0.01314446 BTC $1,184.68 and has sent a total of 0.01308449 BTC $1,179.27 The current value of this address is 0.00005997 BTC $5.40.

Total Received
0.01314446 BTC
$1,184.68

Transactions
8

Total Sent
0.01308449 BTC
$1,179.27

Total Volume
0.02622895 BTC
$2,363.95

Transactions

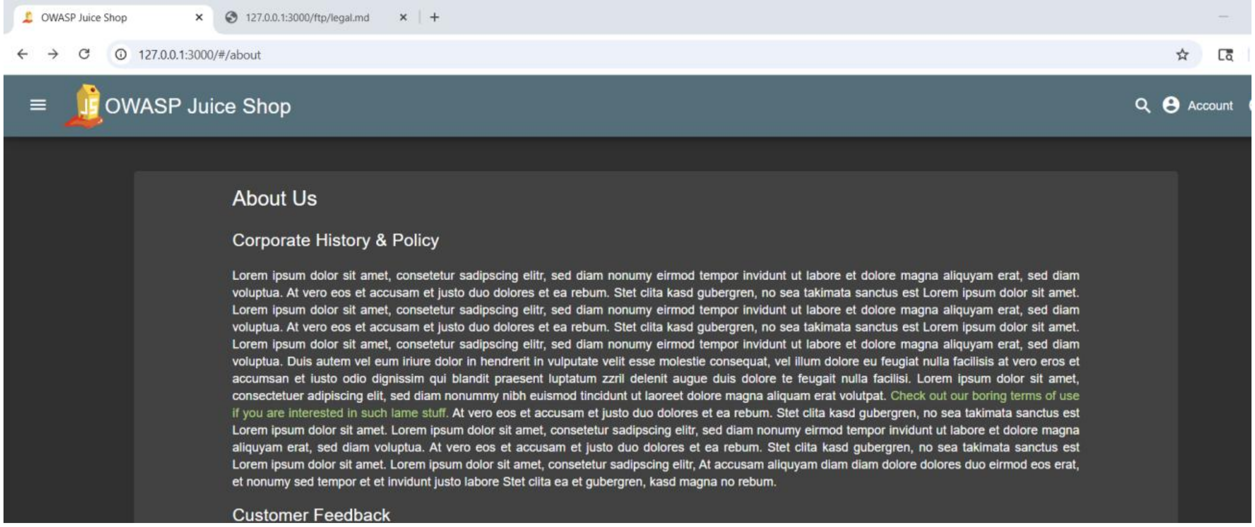
ID: 7e51-0df0
12/23/2022, 14:21:40
From bc1q-rax3
To 2 Outputs
0.00005997 BTC • $5.40
Fee 487 Sats • $0.44

References:

https://www.youtube.com/watch?v=TEdZAXuTfpk

Lab 03: Confidential Document Exposure

I scrolled to the About Us page from the OWASP Dashboard and then clicked on the green link["Check out our boring terms of use if you are interested in such lame stuff. "]. It loaded /ftp/legal.md in new tab. I have captured on these all in Burp. After that, I tried /ftp and examined it in Burp Suite. It responded 200 Ok, then I further scrolled to the response provided by server. I found the name of file "acquisitions.md". I opened /ftp/acquisitions.md. There were other additional files also might contain confidential private data. These files shouldn't be available to the public, this is dangerous.

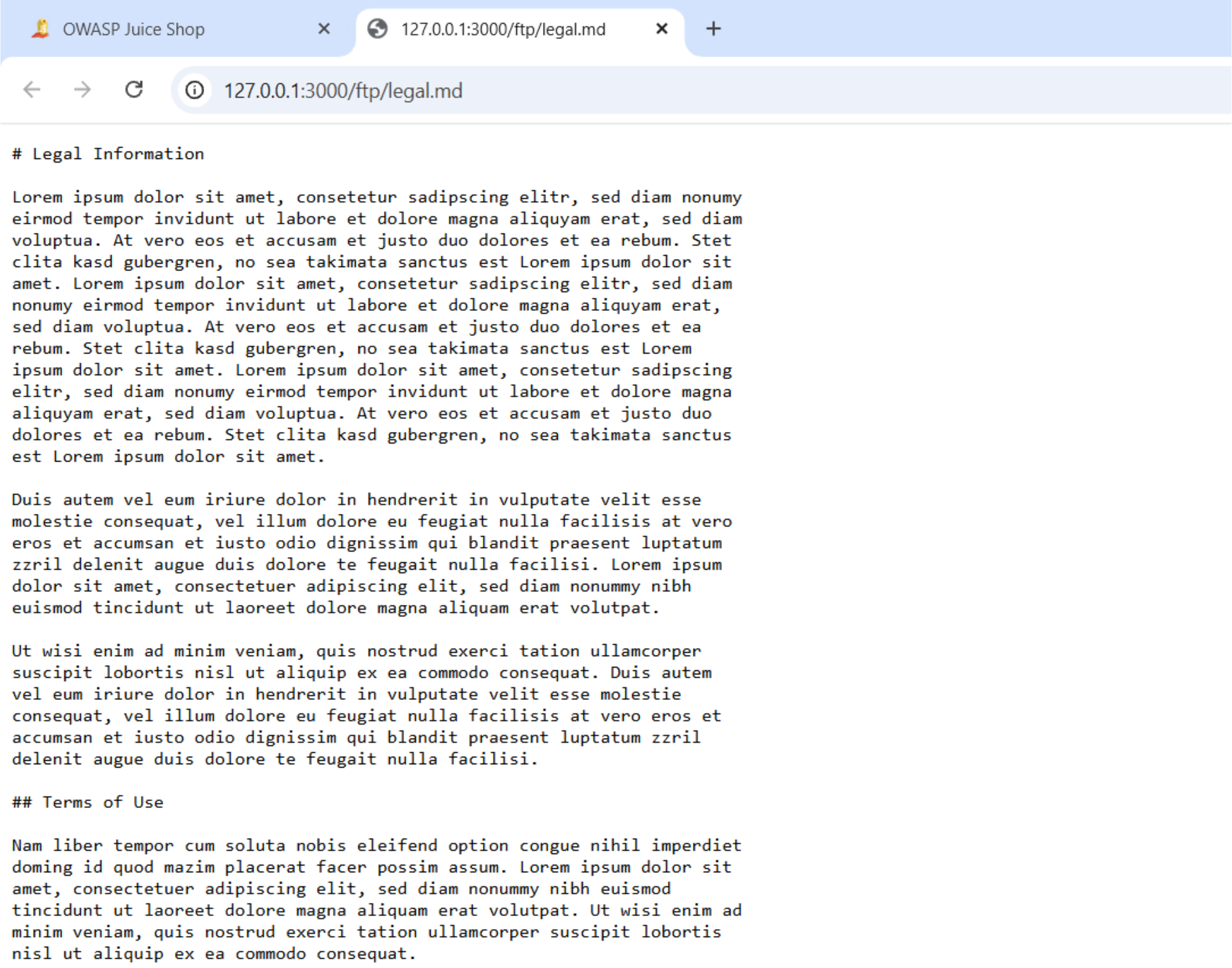


About Us

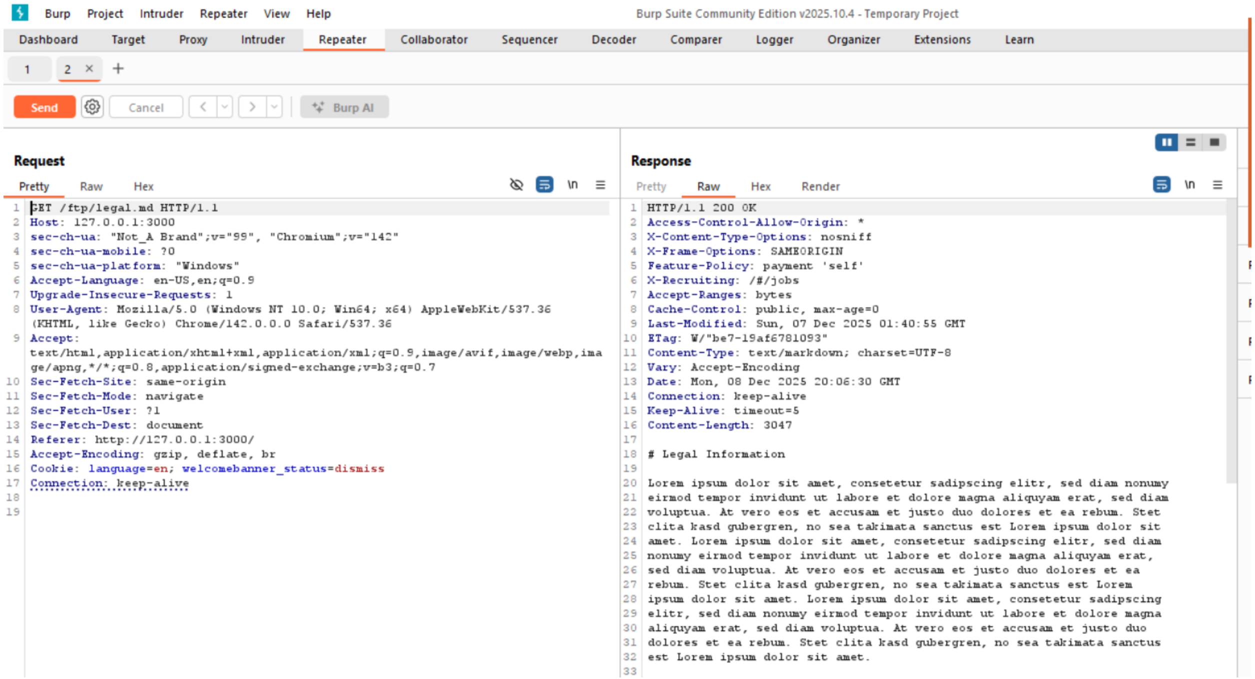
Corporate History & Policy

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. 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, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Check out our boring terms of use if you are interested in such lame stuff. 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, At accusam aliquyam diam diam dolore dolores duo eirmod eos erat, et nonumy sed tempor et et invidunt justo labore Stet clita ea et gubergren, kasd magna no rebum.

Customer Feedback



```
# 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, consectetuer adipiscing elit, sed diam nonummy 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, consectetuer adipiscing elit, sed diam nonummy 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.
```

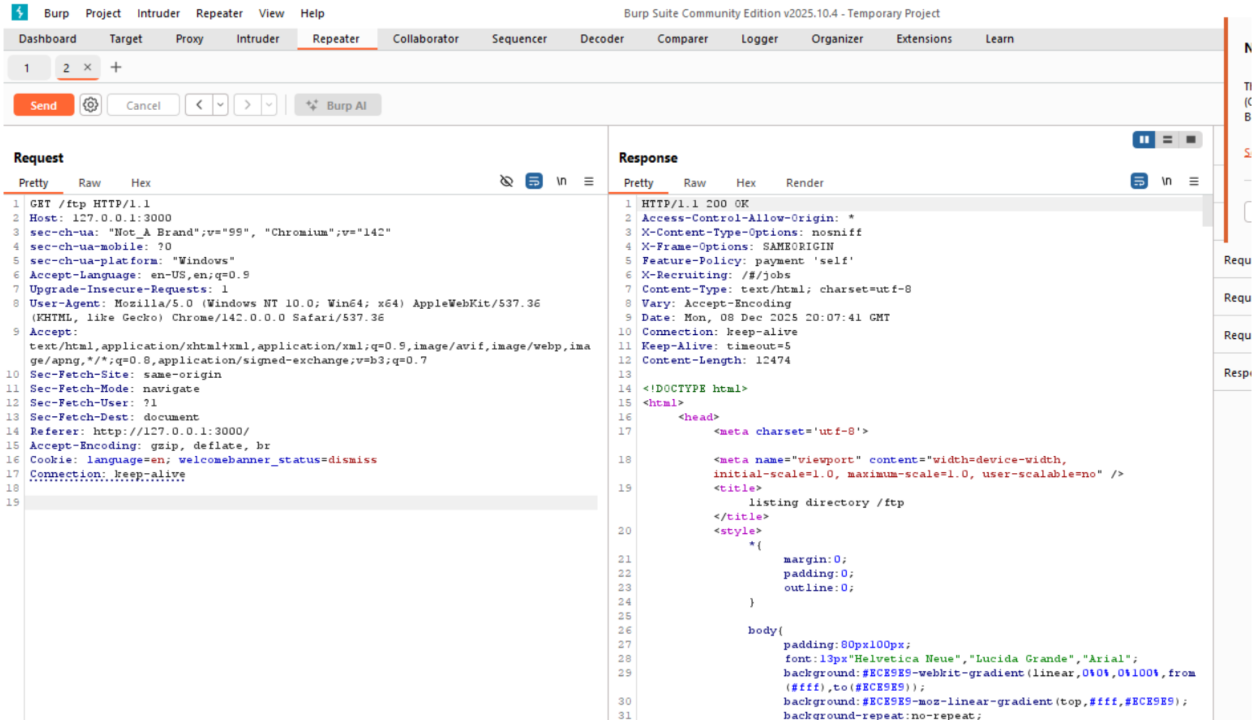


Request

```
GET /ftp/legal.md HTTP/1.1
Host: 127.0.0.1:3000
sec-ch-ua: "Not_A Brand";v="99", "Chromium";v="142"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
ge/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; welcomebanner_status=dismiss
Connection: keep-alive


```

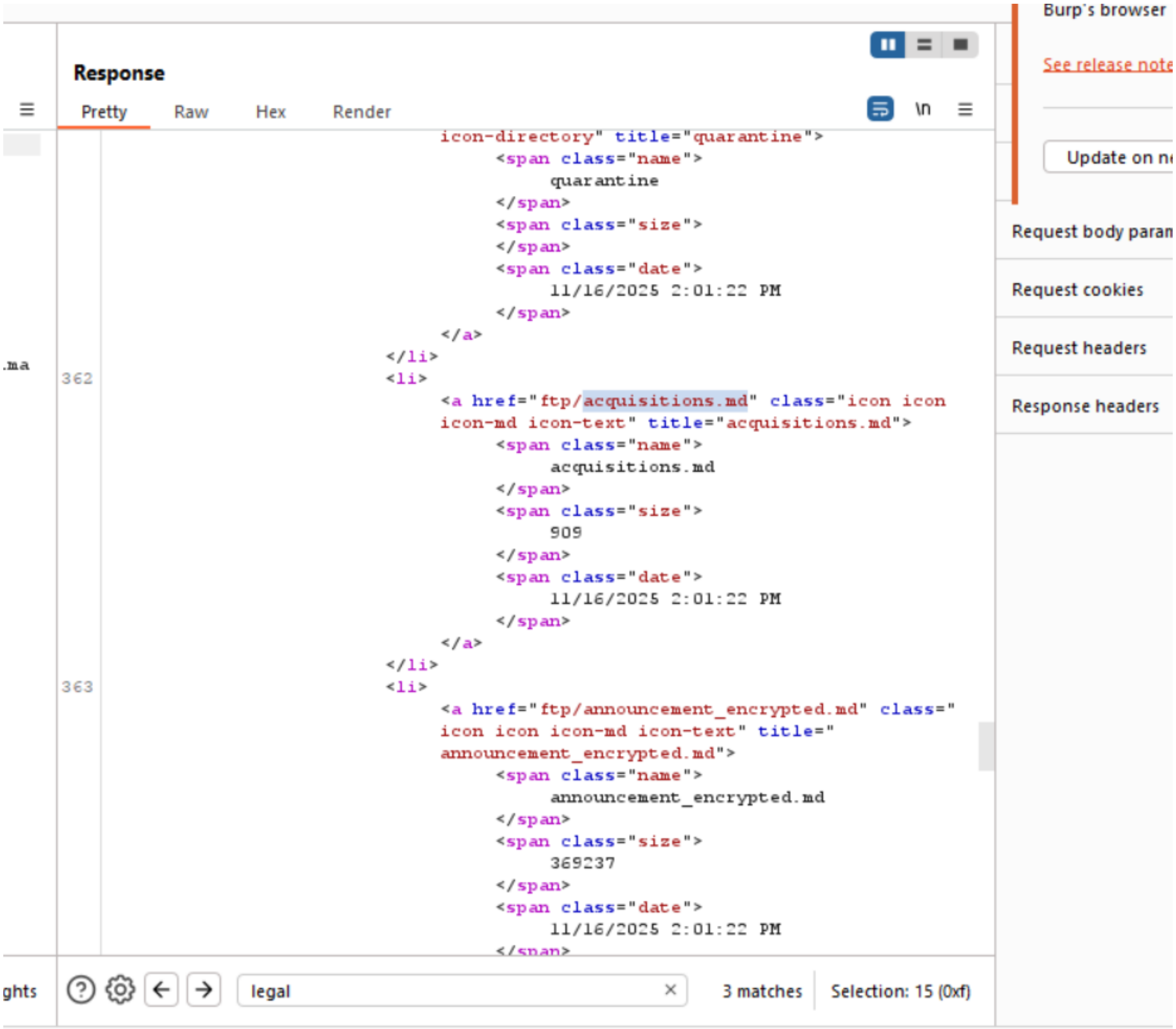
Response

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Sun, 07 Dec 2025 01:40:55 GMT
ETag: W/"be7-19af6781093"
Content-Type: text/markdown; charset=UTF-8
Vary: Accept-Encoding
Date: Mon, 08 Dec 2025 20:06:30 GMT
Connection: keep-alive
Keep-Alive: timeout=5
Content-Length: 3047

# 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.

```

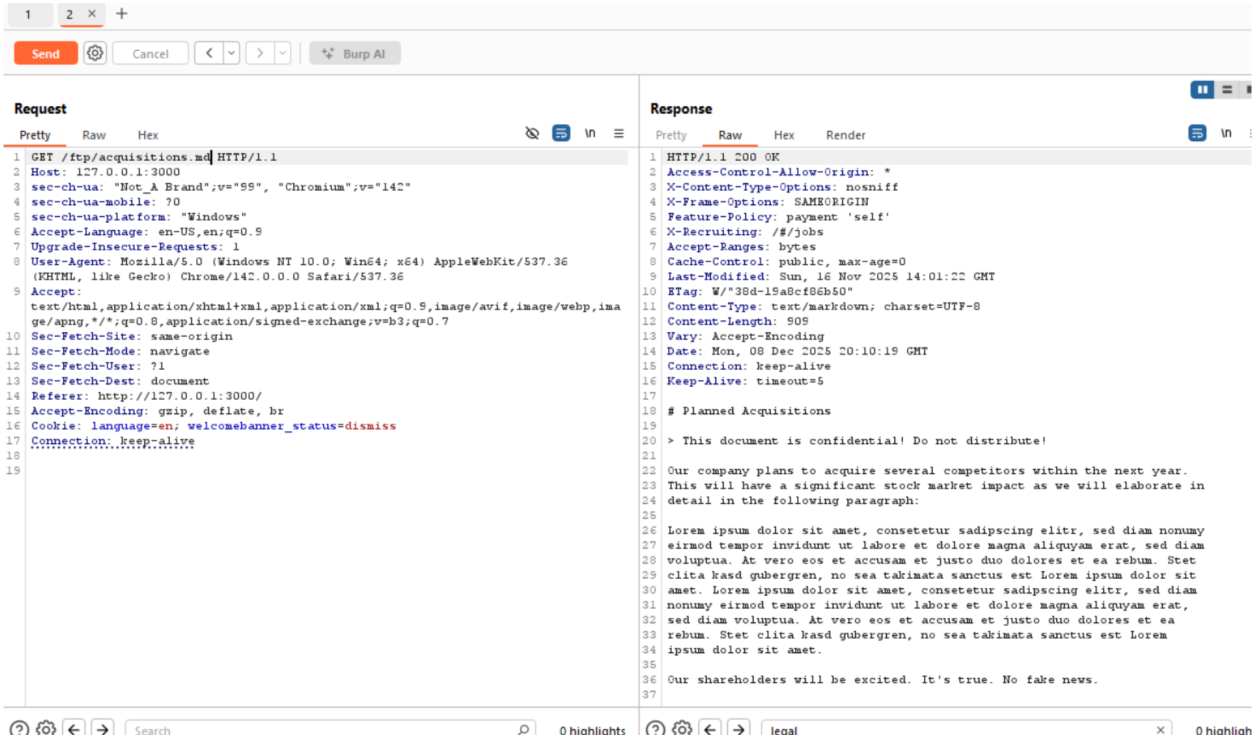


```
GET /ftp HTTP/1.1
Host: 127.0.0.1:3000
sec-ch-ua: "Not_A Brand";v="99", "Chromium";v="142"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
ge/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; welcomebanner_status=dismiss
Connection: keep-alive


```

```
HTTP/1.1 200 OK
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: Mon, 08 Dec 2025 20:07:41 GMT
Connection: keep-alive
Keep-Alive: timeout=5
Content-Length: 12474

<!DOCTYPE html>
<html>
    <head>
        <meta charset='utf-8'>

        <meta name="viewport" content="width=device-width,
        initial-scale=1.0, maximum-scale=1.0, user-scalable=no" />
        <title>
            listing directory /ftp
        </title>
        <style>
            *{
                margin:0;
                padding:0;
                outline:0;
            }

            body{
                padding:80px100px;
                font:13px"Helvetica Neue","Lucida Grande","Arial";
                background:#ECE9E9-webkit-gradient(linear,0%0%,0%100%,from
                (#fff),to(#ECE9E9));
                background:#ECE9E9-moz-linear-gradient(top,#fff,#ECE9E9);
                background-repeat:no-repeat;
```



```
                        icon-directory" title="quarantine">
                            <span class="name">
                                quarantine
                            </span>
                            <span class="size">
                            </span>
                            <span class="date">
                                11/16/2025 2:01:22 PM
                            </span>
                        </a>
                    </li>
                    <li>
                        <a href="ftp/acquisitions.md" class="icon icon
                        icon-md icon-text" title="acquisitions.md">
                            <span class="name">
                                acquisitions.md
                            </span>
                            <span class="size">
                                909
                            </span>
                            <span class="date">
                                11/16/2025 2:01:22 PM
                            </span>
                        </a>
                    </li>
                    <li>
                        <a href="ftp/announcement_encrypted.md" class="
                        icon icon icon-md icon-text" title="
                        announcement_encrypted.md">
                            <span class="name">
                                announcement_encrypted.md
                            </span>
                            <span class="size">
                                369237
                            </span>
                            <span class="date">
                                11/16/2025 2:01:22 PM
                            </span>
```



```
GET /ftp/acquisitions.md HTTP/1.1
Host: 127.0.0.1:3000
sec-ch-ua: "Not_A Brand";v="99", "Chromium";v="142"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
ge/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; welcomebanner_status=dismiss
Connection: keep-alive


```

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Sun, 16 Nov 2025 14:01:22 GMT
ETag: W/"38d-19a8cf86b50"
Content-Type: text/markdown; charset=UTF-8
Content-Length: 909
Vary: Accept-Encoding
Date: Mon, 08 Dec 2025 20:10:19 GMT
Connection: keep-alive
Keep-Alive: timeout=5

# Planned Acquisitions

> This document is confidential! Do not distribute!

Our company plans to acquire several competitors within the next year.
This will have a significant stock market impact as we will elaborate in
detail in the following paragraph:

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.

Our shareholders will be excited. It's true. No fake news.

```

References:

https://www.youtube.com/watch?v=Yi7OiMtzGXc