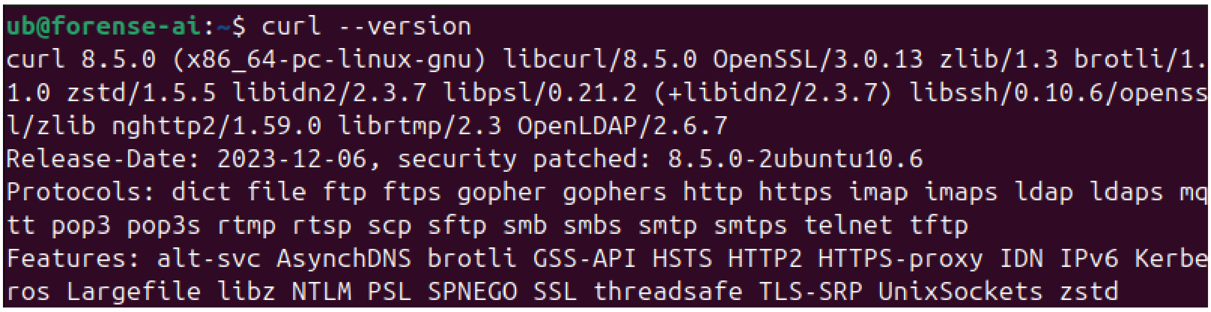
Preparación del entorno

Comprobar curl

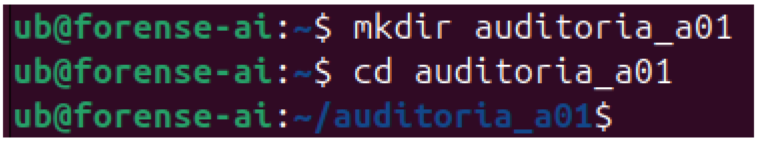
- curl --version



```
ub@forense-ai:~$ curl --version
curl 8.5.0 (x86_64-pc-linux-gnu) libcurl/8.5.0 OpenSSL/3.0.13 zlib/1.3 brotli/1.
1.0 zstd/1.5.5 libidn2/2.3.7 libpsl/0.21.2 (+libidn2/2.3.7) libssh/0.10.6/openss
l/zlib nghttp2/1.59.0 librtmp/2.3 OpenLDAP/2.6.7
Release-Date: 2023-12-06, security patched: 8.5.0-2ubuntu10.6
Protocols: dict file ftp ftps gopher gophers http https imap imaps ldap ldaps mq
tt pop3 pop3s rtmp rtsp scp sftp smb smbs smtp smtps telnet tftp
Features: alt-svc AsynchDNS brotli GSS-API HSTS HTTP2 HTTPS-proxy IDN IPv6 Kerbe
ros Largefile libz NTLM PSL SPNEGO SSL threadsafe TLS-SRP UnixSockets zstd
```

Crear carpeta de trabajo

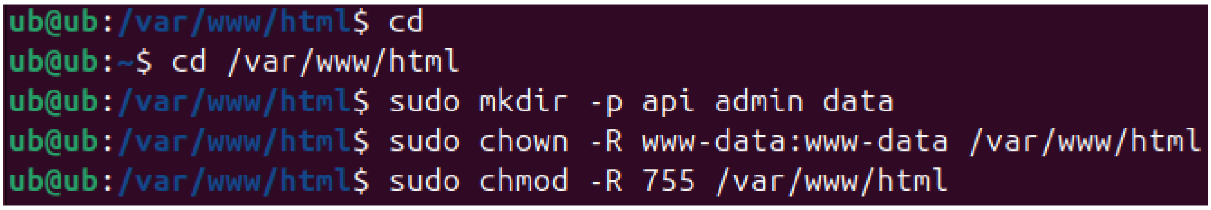
- mkdir auditoria_a01
- cd auditoria_a01



```
ub@forense-ai:~$ mkdir auditoria_a01
ub@forense-ai:~$ cd auditoria_a01
ub@forense-ai:~/auditoria_a01$
```

Nota: Cree un entorno dentro de /var/www/html

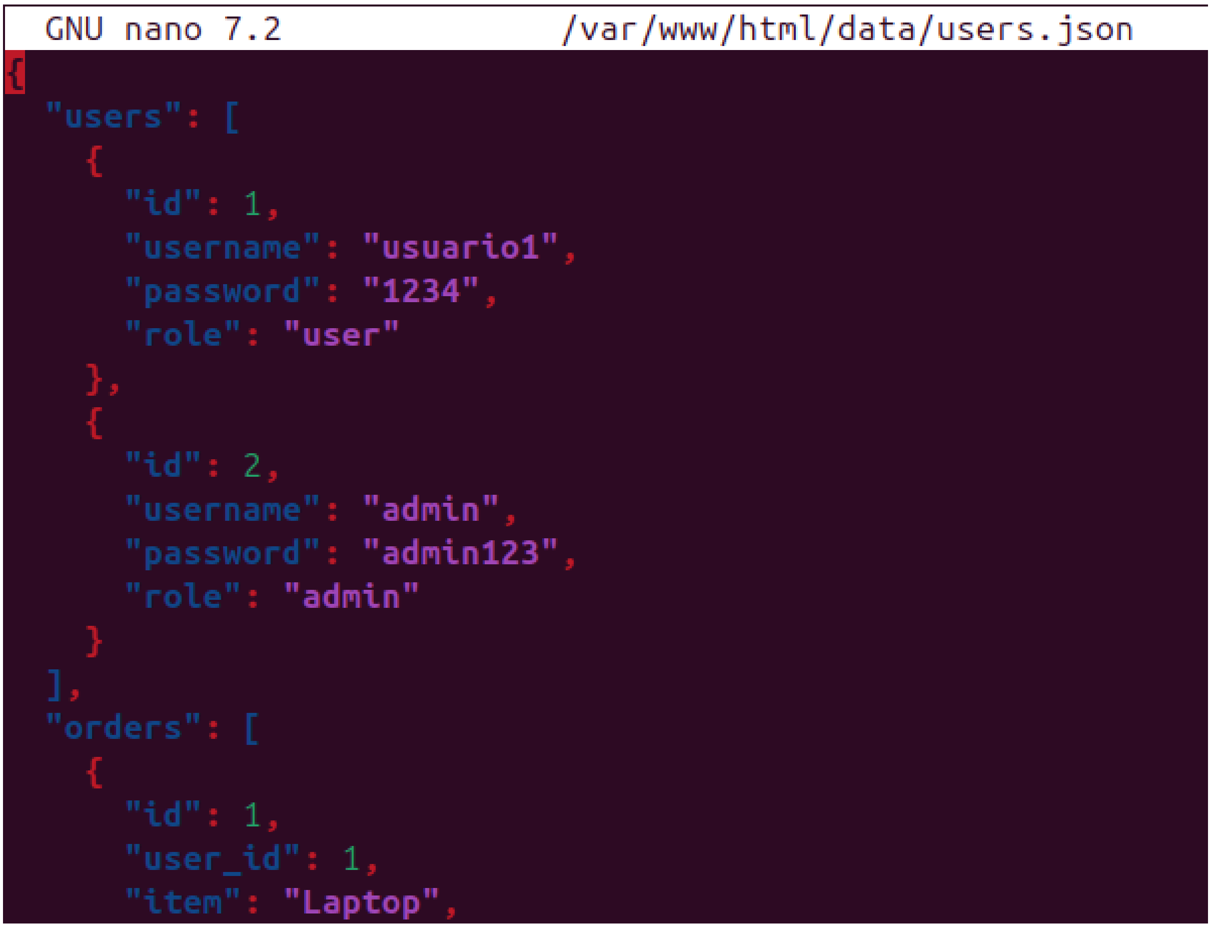
- cd /var/www/html
- sudo mkdir -p api admin data
- sudo chown -R www-data:www-data /var/www/html
- sudo chmod -R 755 /var/www/html



```
ub@ub:/var/www/html$ cd
ub@ub:~$ cd /var/www/html
ub@ub:/var/www/html$ sudo mkdir -p api admin data
ub@ub:/var/www/html$ sudo chown -R www-data:www-data /var/www/html
ub@ub:/var/www/html$ sudo chmod -R 755 /var/www/html
```

- sudo nano /var/www/html/data/users.json

```
{
  "users": [
    {
      "id": 1,
      "username": "usuario1",
      "password": "1234",
      "role": "user"
    },
    {
      "id": 2,
      "username": "admin",
      "password": "admin123",
      "role": "admin"
    }
  ],
  "orders": [
    {
      "id": 1,
      "user_id": 1,
      "item": "Laptop",
      "status": "ACTIVE"
    },
    {
      "id": 2,
      "user_id": 2,
      "item": "Servidor",
      "status": "ACTIVE"
    }
  ]
}
```

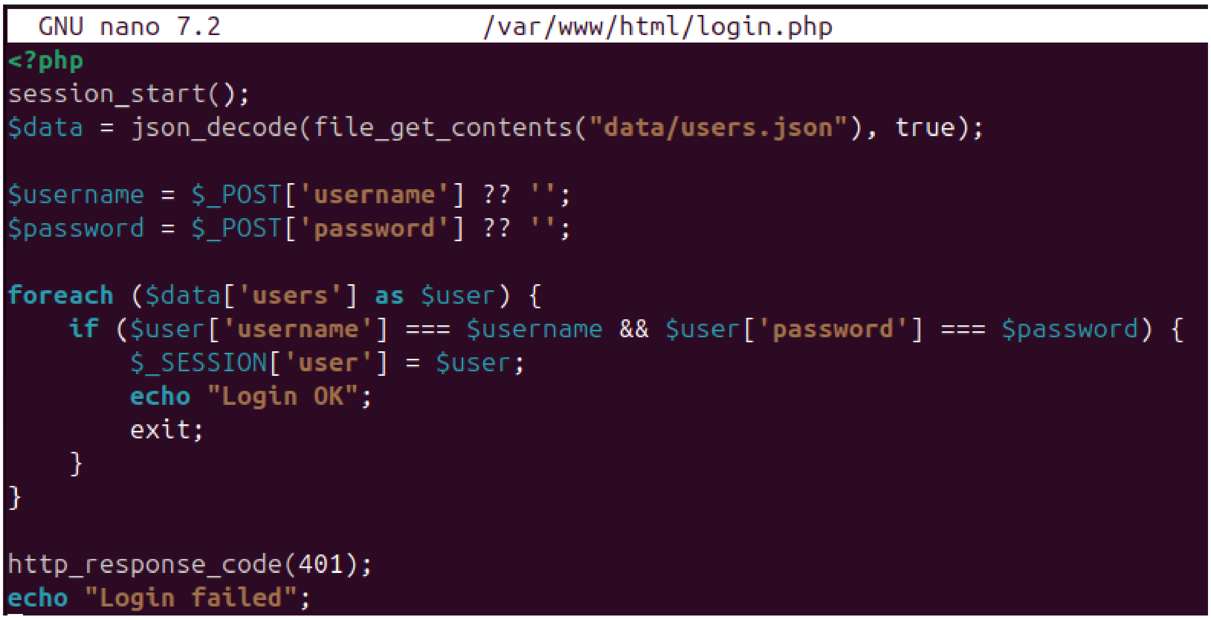


```
  GNU nano 7.2                    /var/www/html/data/users.json
{
  "users": [
    {
      "id": 1,
      "username": "usuario1",
      "password": "1234",
      "role": "user"
    },
    {
      "id": 2,
      "username": "admin",
      "password": "admin123",
      "role": "admin"
    }
  ],
  "orders": [
    {
      "id": 1,
      "user_id": 1,
      "item": "Laptop",
```

- sudo nano /var/www/html/login.php

```
<?php
session_start();
$data = json_decode(file_get_contents("data/users.json"), true);
```

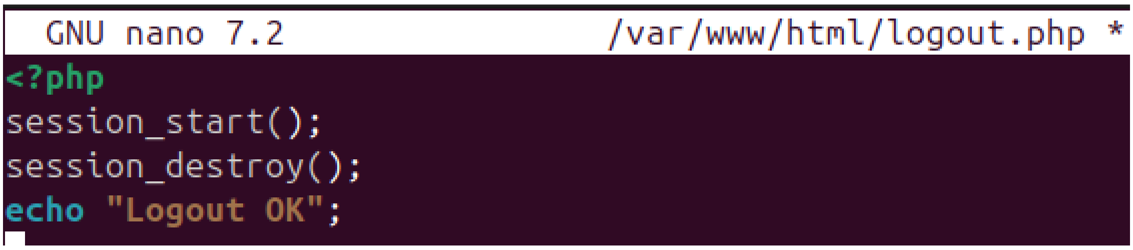
```
$username = $_POST['username'] ?? '';
$password = $_POST['password'] ?? '';

foreach ($data['users'] as $user) {
    if ($user['username'] === $username && $user['password'] === $password) {
        $_SESSION['user'] = $user;
        echo "Login OK";
        exit;
    }
}

http_response_code(401);
echo "Login failed";
```



```
  GNU nano 7.2                    /var/www/html/login.php
<?php
session_start();
$data = json_decode(file_get_contents("data/users.json"), true);

$username = $_POST['username'] ?? '';
$password = $_POST['password'] ?? '';

foreach ($data['users'] as $user) {
    if ($user['username'] === $username && $user['password'] === $password) {
        $_SESSION['user'] = $user;
        echo "Login OK";
        exit;
    }
}

http_response_code(401);
echo "Login failed";
```

- sudo nano /var/www/html/logout.php

```
<?php
session_start();
session_destroy();
echo "Logout OK";
```

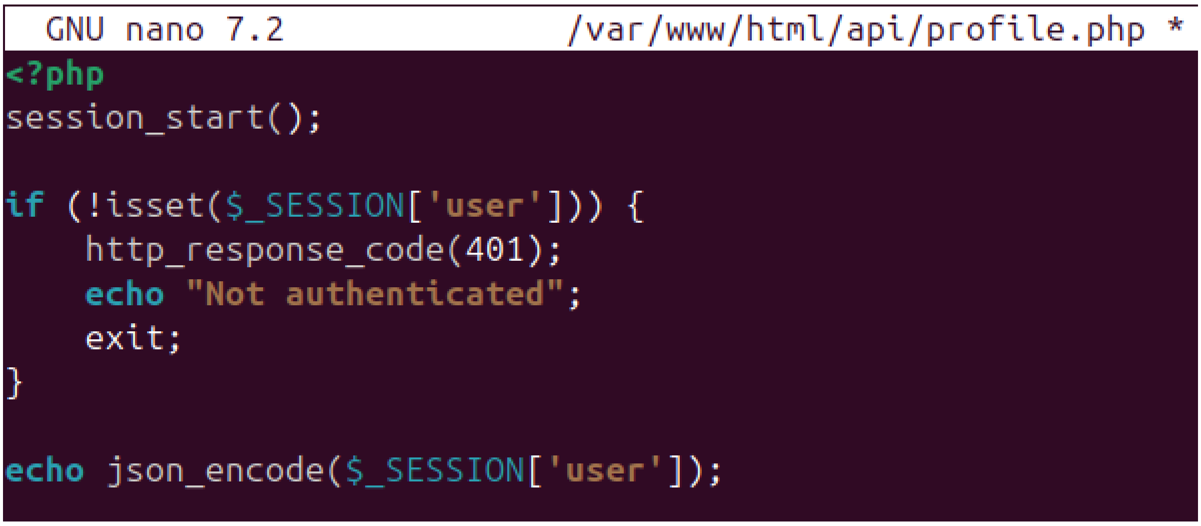


```
  GNU nano 7.2                 /var/www/html/logout.php *
<?php
session_start();
session_destroy();
echo "Logout OK";
```

- sudo nano /var/www/html/api/profile.php

```
<?php
session_start();
```

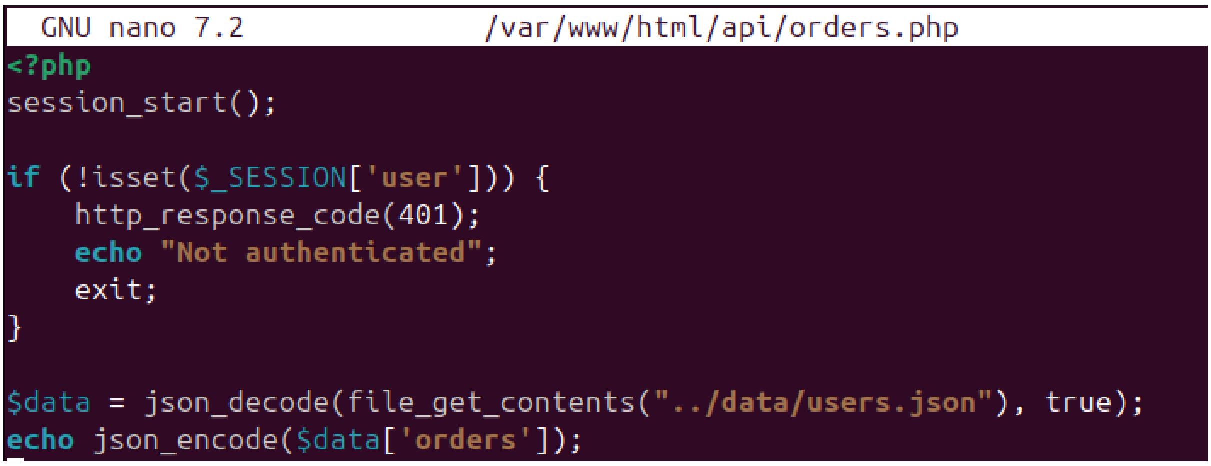
```
if (!isset($_SESSION['user'])) {
    http_response_code(401);
    echo "Not authenticated";
    exit;
}

echo json_encode($_SESSION['user']);
```



```
  GNU nano 7.2                    /var/www/html/api/profile.php *
<?php
session_start();

if (!isset($_SESSION['user'])) {
    http_response_code(401);
    echo "Not authenticated";
    exit;
}

echo json_encode($_SESSION['user']);
```

- sudo nano /var/www/html/api/orders.php

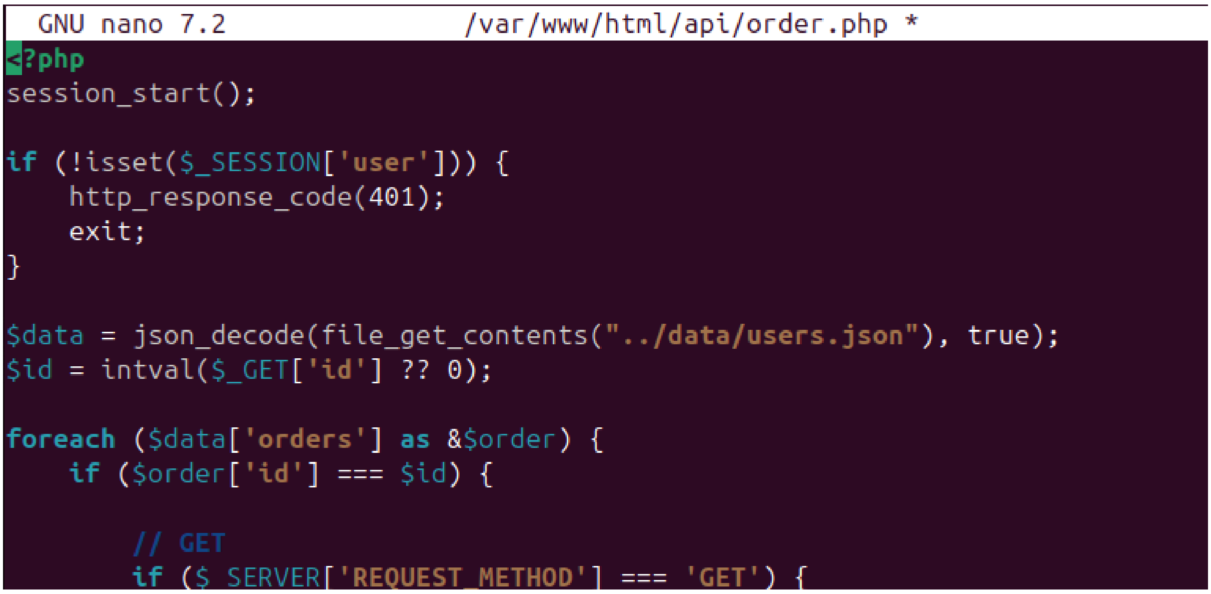
```
<?php
session_start();

if (!isset($_SESSION['user'])) {
    http_response_code(401);
    echo "Not authenticated";
    exit;
}

$data = json_decode(file_get_contents("../data/users.json"), true);
echo json_encode($data['orders']);
```



```
  GNU nano 7.2                    /var/www/html/api/orders.php
<?php
session_start();

if (!isset($_SESSION['user'])) {
    http_response_code(401);
    echo "Not authenticated";
    exit;
}

$data = json_decode(file_get_contents("../data/users.json"), true);
echo json_encode($data['orders']);
```

- sudo nano /var/www/html/api/order.php

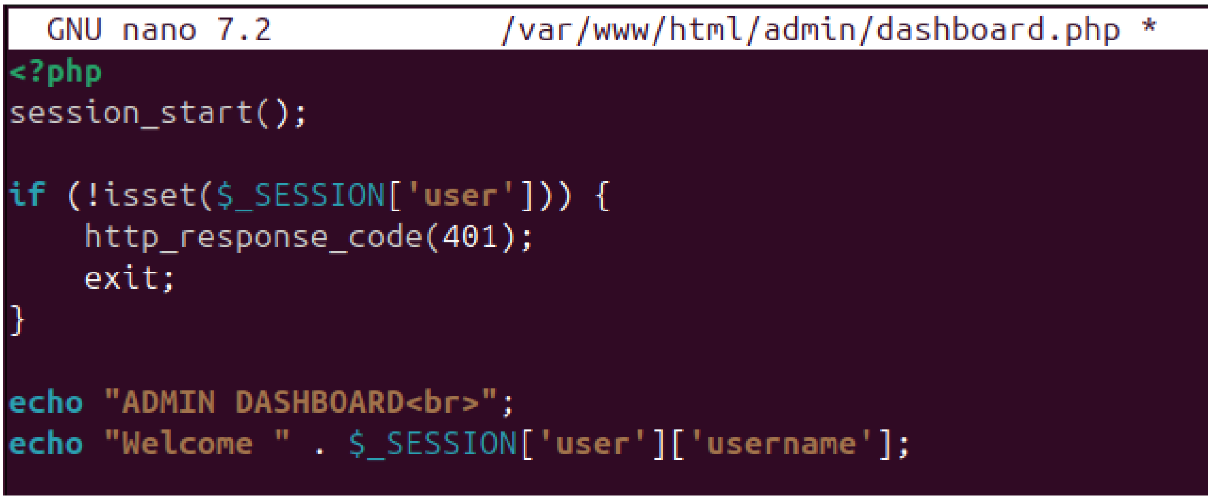
```php
<?php
session_start();

if (!isset($_SESSION['user'])) {
    http_response_code(401);
    exit;
}

$data = json_decode(file_get_contents("../data/users.json"), true);
$id = intval($_GET['id'] ?? 0);

foreach ($data['orders'] as &$order) {
    if ($order['id'] === $id) {

        // GET
        if ($_SERVER['REQUEST_METHOD'] === 'GET') {
            echo json_encode($order);
            exit;
        }

        // PUT
        if ($_SERVER['REQUEST_METHOD'] === 'PUT') {
            $input = json_decode(file_get_contents("php://input"), true);
            $order['status'] = $input['status'] ?? $order['status'];
            file_put_contents("../data/users.json", json_encode($data, JSON_PRETTY_PRINT));
            echo "Order updated";
            exit;
        }

        // DELETE
        if ($_SERVER['REQUEST_METHOD'] === 'DELETE') {
            $order['status'] = "DELETED";
            file_put_contents("../data/users.json", json_encode($data, JSON_PRETTY_PRINT));
            echo "Order deleted";
            exit;
        }
    }
}

http_response_code(404);
echo "Order not found";
```



```
  GNU nano 7.2                    /var/www/html/api/order.php *
<?php
session_start();

if (!isset($_SESSION['user'])) {
    http_response_code(401);
    exit;
}

$data = json_decode(file_get_contents("../data/users.json"), true);
$id = intval($_GET['id'] ?? 0);

foreach ($data['orders'] as &$order) {
    if ($order['id'] === $id) {

        // GET
        if ($_SERVER['REQUEST_METHOD'] === 'GET') {
```

- sudo nano /var/www/html/admin/dashboard.php

```
<?php
session_start();

if (!isset($_SESSION['user'])) {
    http_response_code(401);
    exit;
}

echo "ADMIN DASHBOARD<br>";
echo "Welcome " . $_SESSION['user']['username'];
```



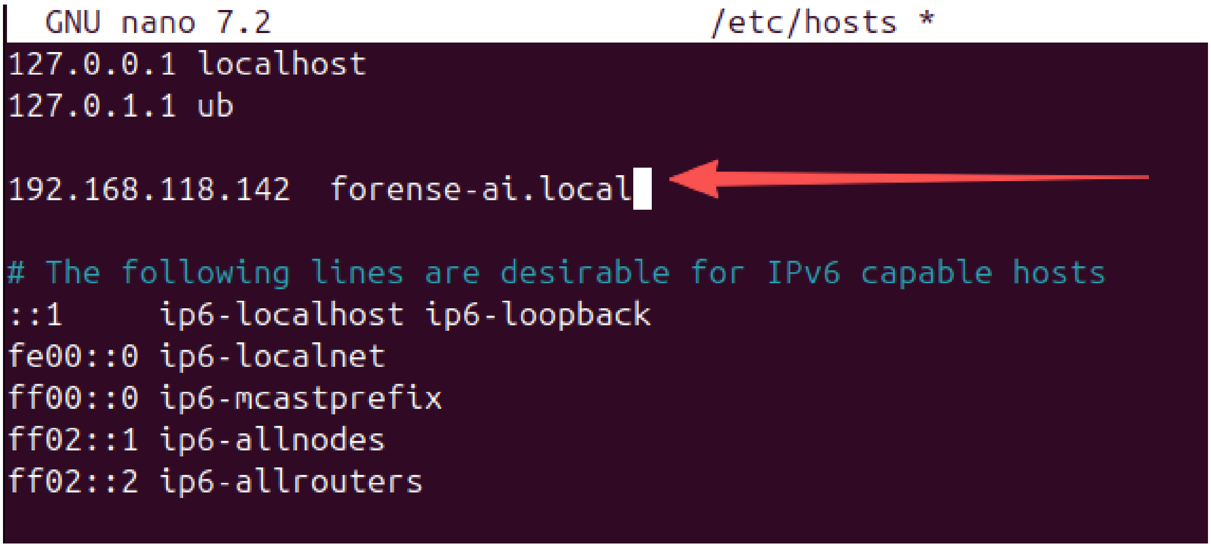
```
  GNU nano 7.2                 /var/www/html/admin/dashboard.php *
<?php
session_start();

if (!isset($_SESSION['user'])) {
    http_response_code(401);
    exit;
}

echo "ADMIN DASHBOARD<br>";
echo "Welcome " . $_SESSION['user']['username'];
```

Reiniciar Apache

- sudo systemctl restart apache2

Añade una línea a /etc/hosts: 192.168.118.142(IP) forense-ai.local

- sudo nano /etc/hosts



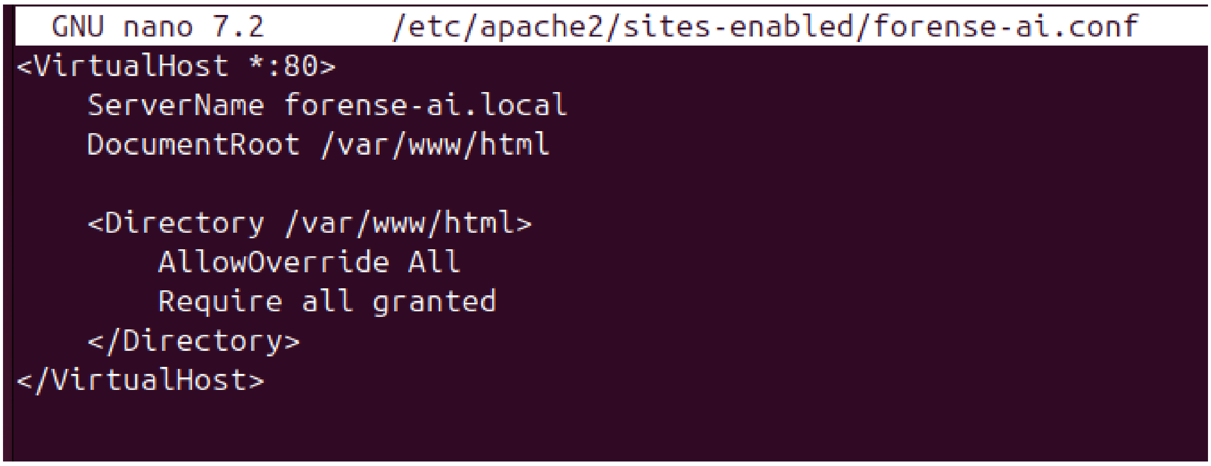
```
  GNU nano 7.2                          /etc/hosts *
127.0.0.1 localhost
127.0.1.1 ub

192.168.118.142  forense-ai.local

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Modificar VirtualHost

- sudo nano /etc/apache2/sites-enabled/forense-ai.conf

Reemplazar con el siguiente contenido:

```
<VirtualHost *:80>
  ServerName forense-ai.local
  DocumentRoot /var/www/html

  <Directory /var/www/html>
    AllowOverride All
    Require all granted
  </Directory>
</VirtualHost>
```



```
  GNU nano 7.2       /etc/apache2/sites-enabled/forense-ai.conf
<VirtualHost *:80>
    ServerName forense-ai.local
    DocumentRoot /var/www/html

    <Directory /var/www/html>
        AllowOverride All
        Require all granted
    </Directory>
</VirtualHost>
```

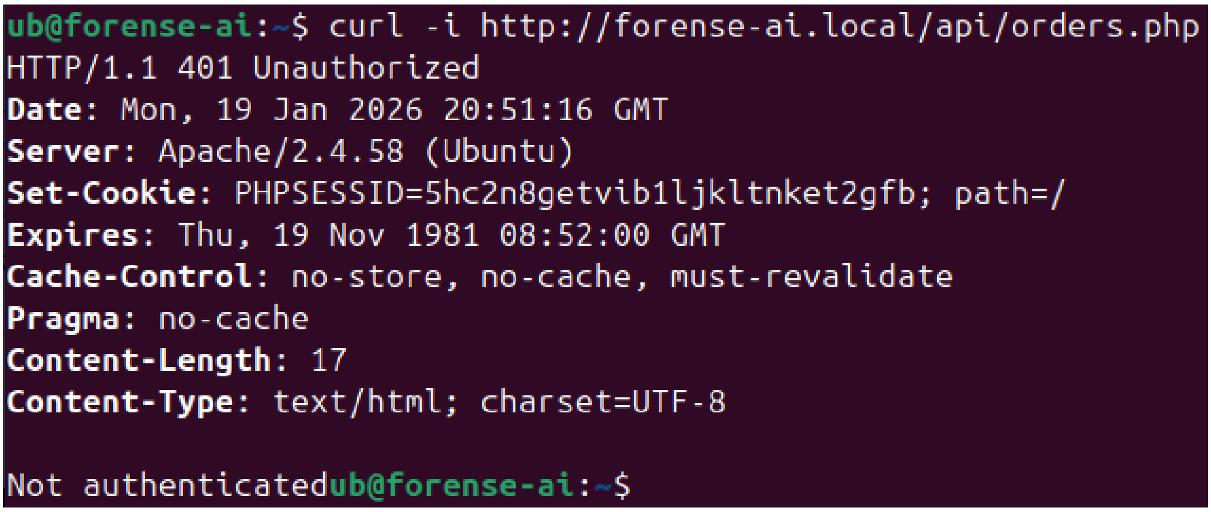
Reiniciar Apache

- sudo systemctl restart apache2

Reconocimiento pasivo (sin login)

Acceso a recursos protegidos sin autenticar

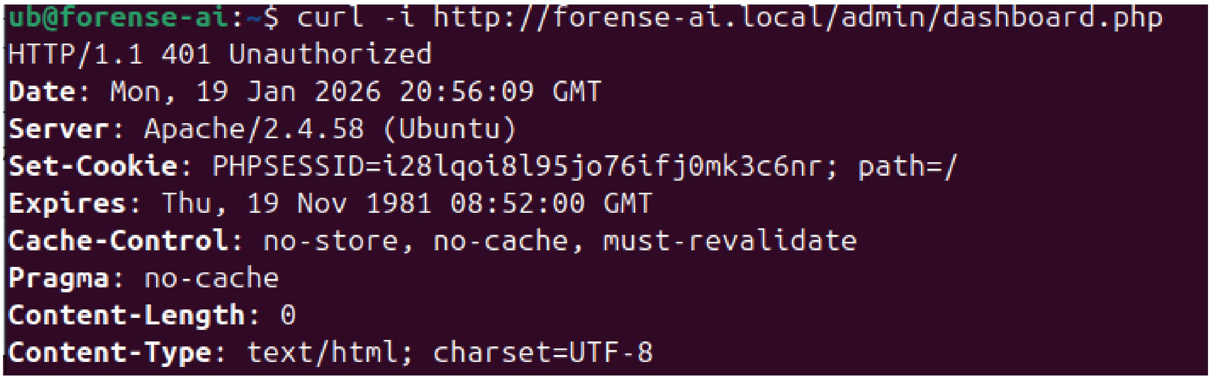
- curl -i http://forense-ai.local/api/orders.php



```
ub@forense-ai:~$ curl -i http://forense-ai.local/api/orders.php
HTTP/1.1 401 Unauthorized
Date: Mon, 19 Jan 2026 20:51:16 GMT
Server: Apache/2.4.58 (Ubuntu)
Set-Cookie: PHPSESSID=5hc2n8getvib1ljkltnket2gfb; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 17
Content-Type: text/html; charset=UTF-8

Not authenticatedub@forense-ai:~$
```

Intento directo a panel admin

- curl -i http://forense-ai.local/admin/dashboard.php

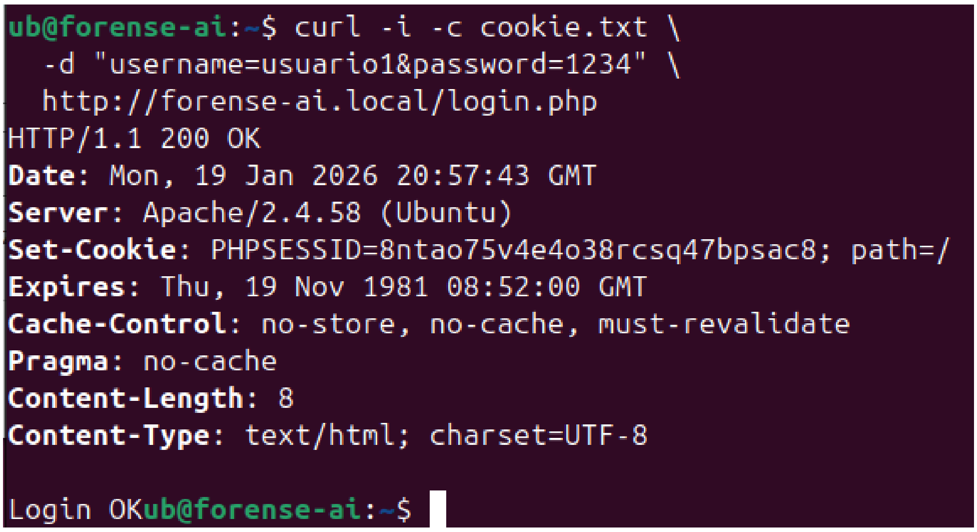


```
ub@forense-ai:~$ curl -i http://forense-ai.local/admin/dashboard.php
HTTP/1.1 401 Unauthorized
Date: Mon, 19 Jan 2026 20:56:09 GMT
Server: Apache/2.4.58 (Ubuntu)
Set-Cookie: PHPSESSID=i28lqoi8l95jo76ifj0mk3c6nr; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 0
Content-Type: text/html; charset=UTF-8
```

Autenticación y gestión de sesión

Login como usuario normal

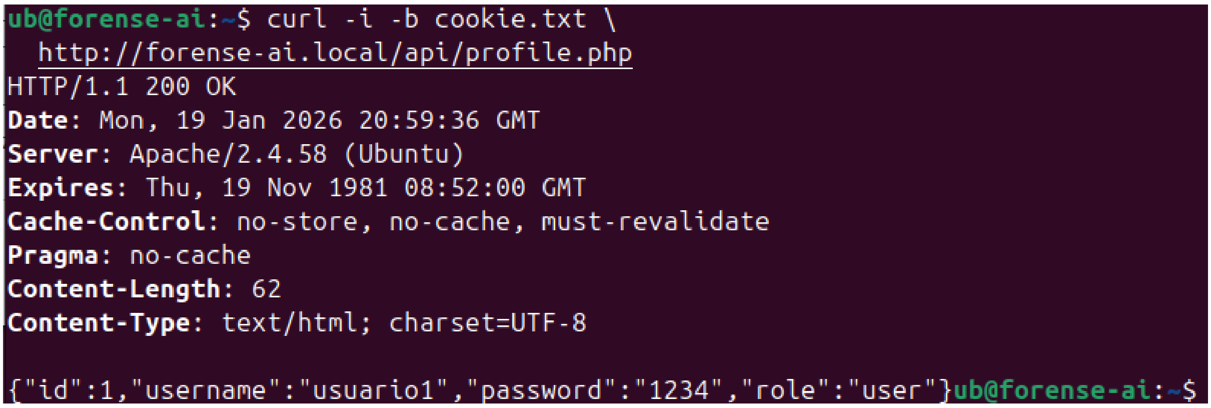
```
curl -i -c cookie.txt \
  -d "username=usuario1&password=1234" \
  http://forense-ai.local/login.php
```



```
ub@forense-ai:~$ curl -i -c cookie.txt \
  -d "username=usuario1&password=1234" \
  http://forense-ai.local/login.php
HTTP/1.1 200 OK
Date: Mon, 19 Jan 2026 20:57:43 GMT
Server: Apache/2.4.58 (Ubuntu)
Set-Cookie: PHPSESSID=8ntao75v4e4o38rcsq47bpsac8; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 8
Content-Type: text/html; charset=UTF-8

Login OKub@forense-ai:~$
```

Acceso autenticado

```
curl -i -b cookie.txt \
  http://forense-ai.local/api/profile.php
```



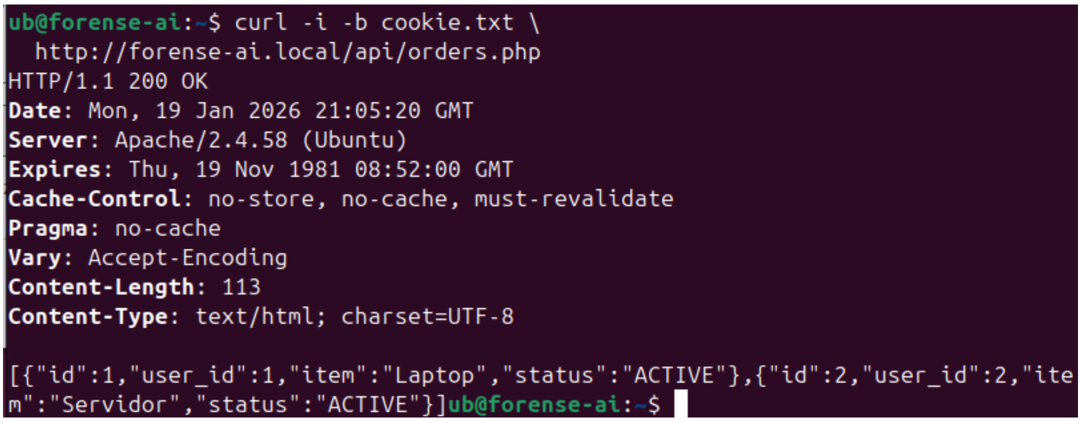
```
ub@forense-ai:~$ curl -i -b cookie.txt \
  http://forense-ai.local/api/profile.php
HTTP/1.1 200 OK
Date: Mon, 19 Jan 2026 20:59:36 GMT
Server: Apache/2.4.58 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 62
Content-Type: text/html; charset=UTF-8

{"id":1,"username":"usuario1","password":"1234","role":"user"}ub@forense-ai:~$
```

OWASP A01 en acción (Broken Access Control)

Verificar vulnerabilidad A01

Los usuarios normales pueden acceder a todos los pedidos

```
curl -i -b cookie.txt \
  http://forense-ai.local/api/orders.php
```

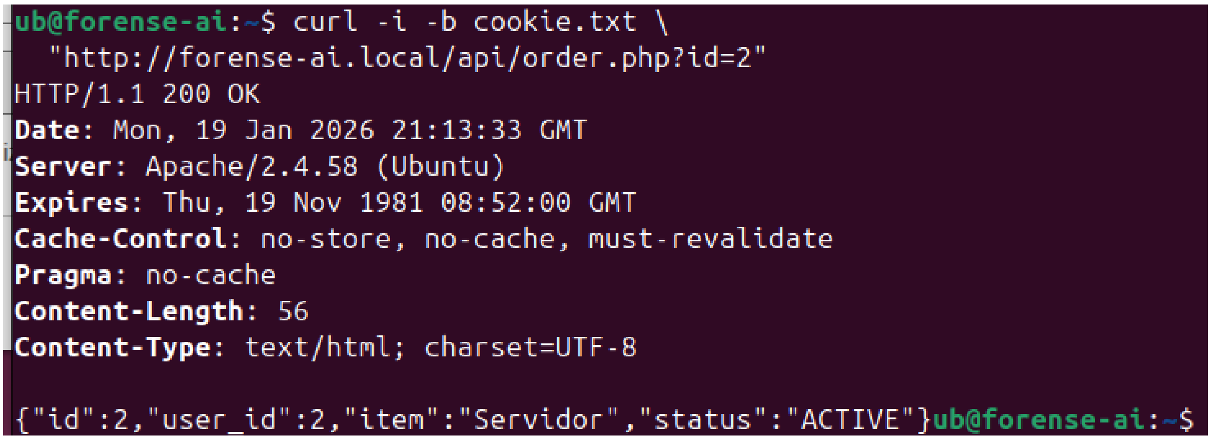


```
ub@forense-ai:~$ curl -i -b cookie.txt \
  http://forense-ai.local/api/orders.php
HTTP/1.1 200 OK
Date: Mon, 19 Jan 2026 21:05:20 GMT
Server: Apache/2.4.58 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 113
Content-Type: text/html; charset=UTF-8

[{"id":1,"user_id":1,"item":"Laptop","status":"ACTIVE"},{"id":2,"user_id":2,"ite
m":"Servidor","status":"ACTIVE"}]ub@forense-ai:~$
```

Verificar IDOR

Ver órdenes que no le pertenecen

```
curl -i -b cookie.txt \
  "http://forense-ai.local/api/order.php?id=2"
```

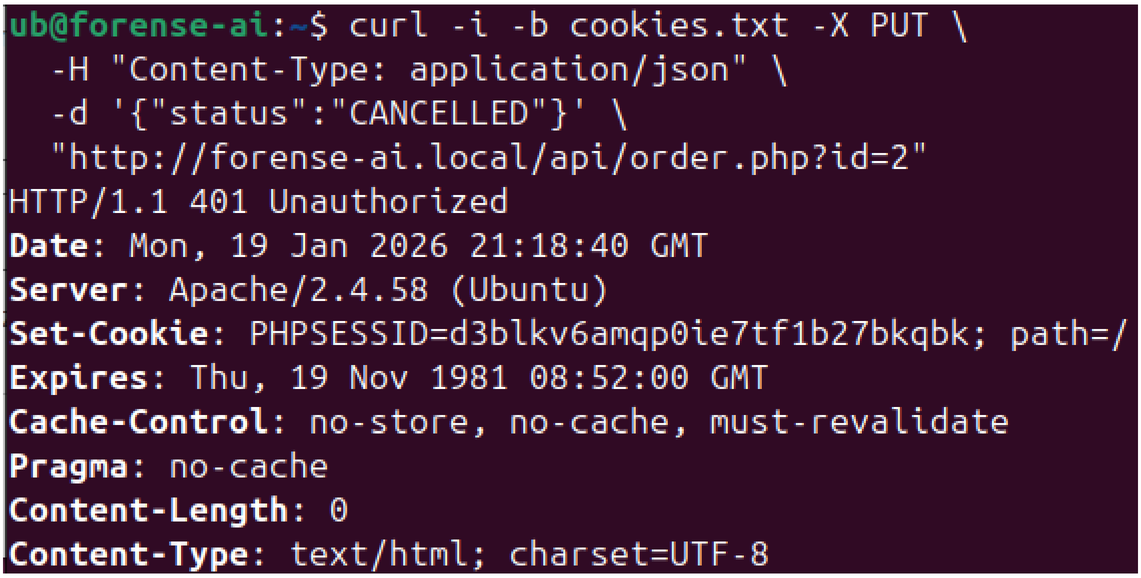


```
ub@forense-ai:~$ curl -i -b cookie.txt \
  "http://forense-ai.local/api/order.php?id=2"
HTTP/1.1 200 OK
Date: Mon, 19 Jan 2026 21:13:33 GMT
Server: Apache/2.4.58 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 56
Content-Type: text/html; charset=UTF-8

{"id":2,"user_id":2,"item":"Servidor","status":"ACTIVE"}ub@forense-ai:~$
```

Bypass por método HTTP (PUT / DELETE)

Intento de modificación

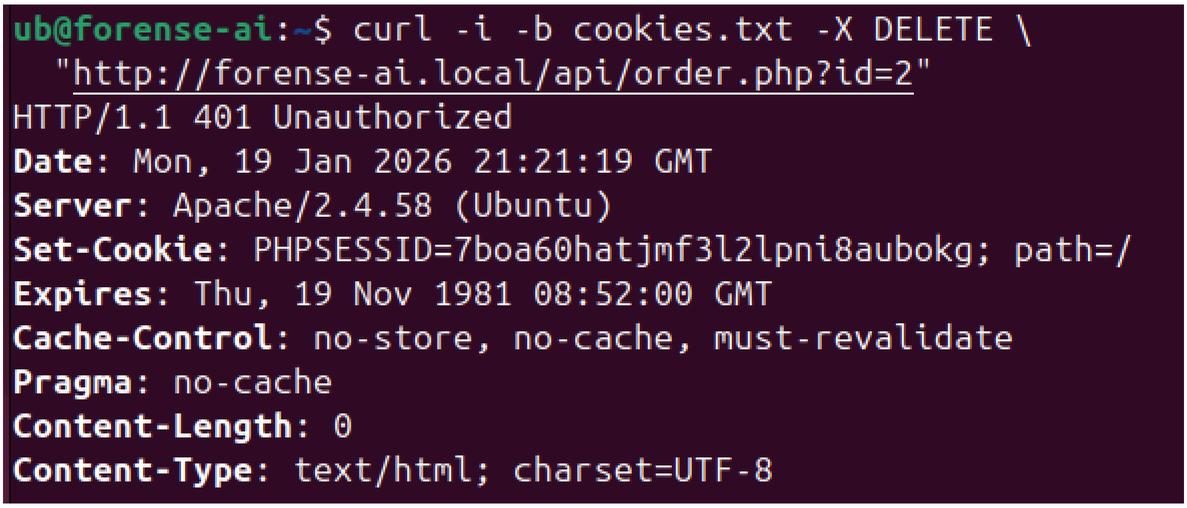
```
curl -i -b cookies.txt -X PUT \
  -H "Content-Type: application/json" \
  -d '{"status":"CANCELLED"}' \
  "http://forense-ai.local/api/order.php?id=2"
```



```
ub@forense-ai:~$ curl -i -b cookies.txt -X PUT \
  -H "Content-Type: application/json" \
  -d '{"status":"CANCELLED"}' \
  "http://forense-ai.local/api/order.php?id=2"
HTTP/1.1 401 Unauthorized
Date: Mon, 19 Jan 2026 21:18:40 GMT
Server: Apache/2.4.58 (Ubuntu)
Set-Cookie: PHPSESSID=d3blkv6amqp0ie7tf1b27bkqbk; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 0
Content-Type: text/html; charset=UTF-8
```

Intento de borrado

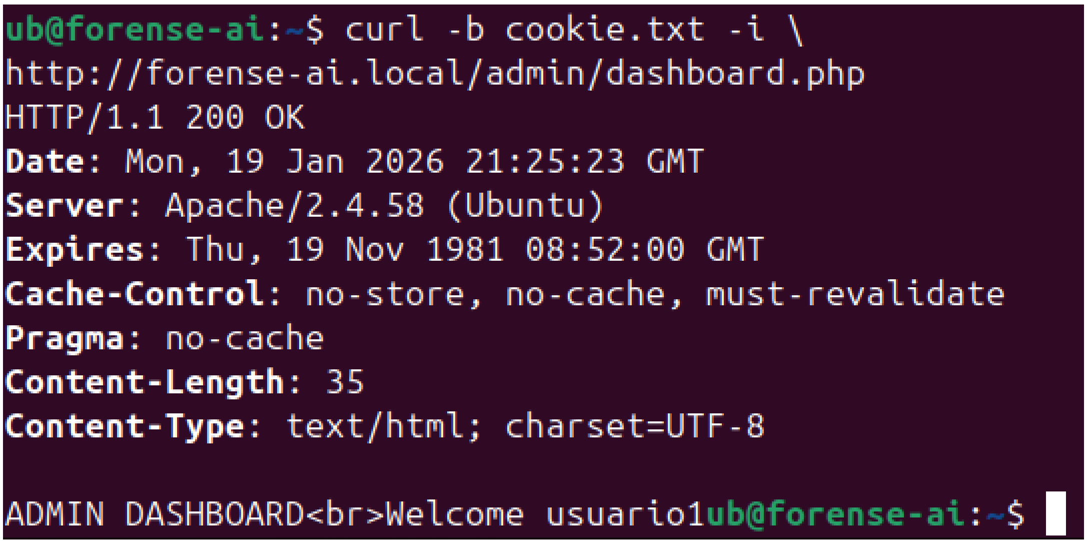
```
curl -i -b cookies.txt -X DELETE \
  "http://forense-ai.local/api/order.php?id=2"
```



```
ub@forense-ai:~$ curl -i -b cookies.txt -X DELETE \
  "http://forense-ai.local/api/order.php?id=2"
HTTP/1.1 401 Unauthorized
Date: Mon, 19 Jan 2026 21:21:19 GMT
Server: Apache/2.4.58 (Ubuntu)
Set-Cookie: PHPSESSID=7boa60hatjmf3l2lpni8aubokg; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 0
Content-Type: text/html; charset=UTF-8
```

Acceso a funciones admin con usuario normal

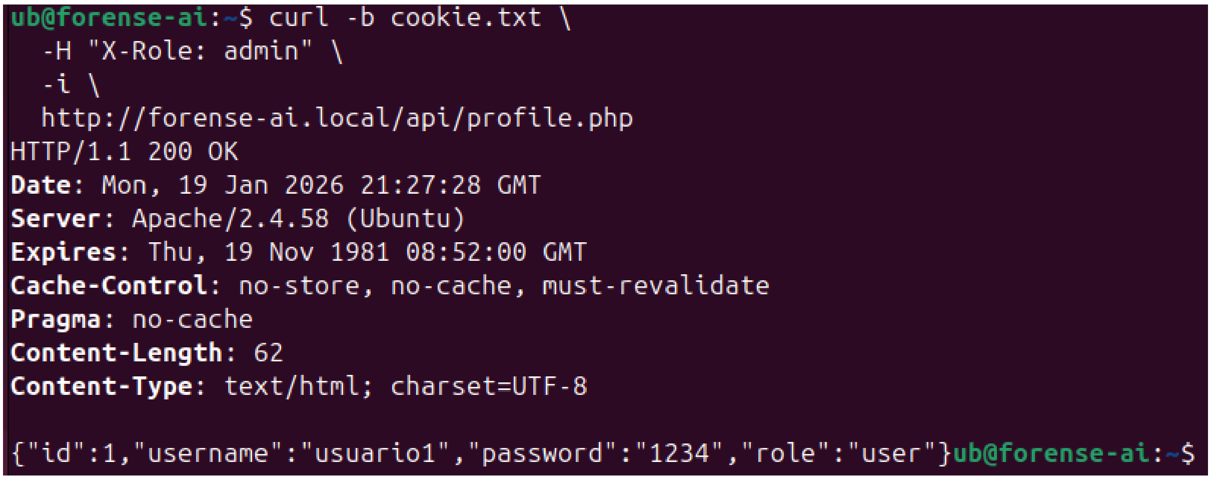
```
curl -b cookie.txt -i \
http://forense-ai.local/admin/dashboard.php
```



```
ub@forense-ai:~$ curl -b cookie.txt -i \
http://forense-ai.local/admin/dashboard.php
HTTP/1.1 200 OK
Date: Mon, 19 Jan 2026 21:25:23 GMT
Server: Apache/2.4.58 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 35
Content-Type: text/html; charset=UTF-8

ADMIN DASHBOARD<br>Welcome usuario1ub@forense-ai:~$
```

Headers manipulables (prueba de confianza indebida)

```
curl -b cookie.txt \
  -H "X-Role: admin" \
  -i \
  http://forense-ai.local/api/profile.php
```

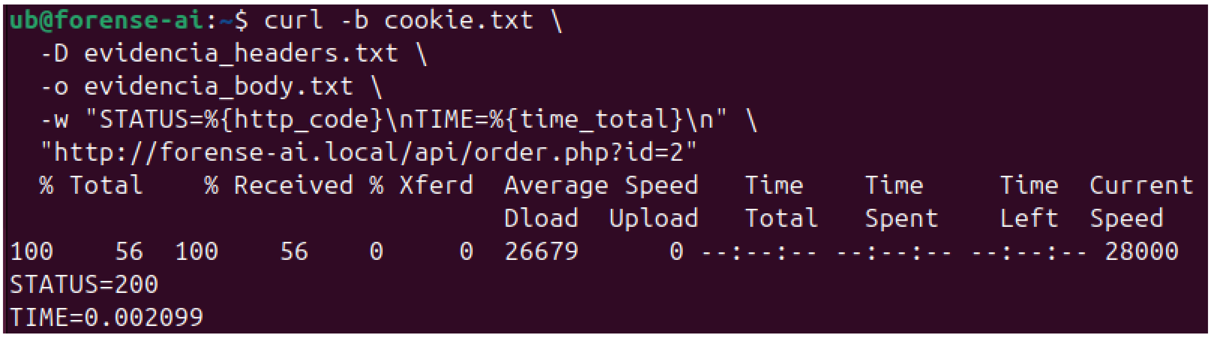


```
ub@forense-ai:~$ curl -b cookie.txt \
  -H "X-Role: admin" \
  -i \
  http://forense-ai.local/api/profile.php
HTTP/1.1 200 OK
Date: Mon, 19 Jan 2026 21:27:28 GMT
Server: Apache/2.4.58 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 62
Content-Type: text/html; charset=UTF-8

{"id":1,"username":"usuario1","password":"1234","role":"user"}ub@forense-ai:~$
```

Evidencias para informe

Guardar headers y cuerpo

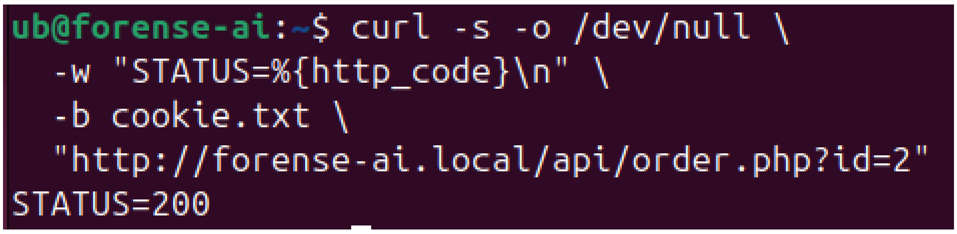
```
curl -b cookie.txt \
  -D evidencia_headers.txt \
  -o evidencia_body.txt \
  -w "STATUS=%{http_code}\nTIME=%{time_total}\n" \
  "http://forense-ai.local/api/order.php?id=2"
```



```
ub@forense-ai:~$ curl -b cookie.txt \
  -D evidencia_headers.txt \
  -o evidencia_body.txt \
  -w "STATUS=%{http_code}\nTIME=%{time_total}\n" \
  "http://forense-ai.local/api/order.php?id=2"
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    56  100    56    0     0  26679      0 --:--:-- --:--:-- --:--:-- 28000
STATUS=200
TIME=0.002099
```

Evidencia mínima reproducible

```
curl -s -o /dev/null \
  -w "STATUS=%{http_code}\n" \
  -b cookie.txt \
  "http://forense-ai.local/api/order.php?id=2"
```



```
ub@forense-ai:~$ curl -s -o /dev/null \
  -w "STATUS=%{http_code}\n" \
  -b cookie.txt \
  "http://forense-ai.local/api/order.php?id=2"
STATUS=200
```