

DÍA D - EJERCICIO FINAL - CTF ATAQUES A APLICACIONES WEB

Canal Slack: cs-ft-sep-23

CTF basado en: <https://owasp.org/www-project-juice-shop/>

Prerrequisitos

Sigue estos pasos para instalar Juicy Shop:

Kali Linux:

```
sudo apt install nodejs npm
```

```
git clone https://github.com/juice-shop/juice-shop.git
```

```
cd juice-shop
```

```
npm install
```

```
npm start
```

```
http://localhost:3000
```

Juicy Shop por equipos

El reto consiste en conseguir acumular la mayor cantidad de pruebas resueltas en esta tienda web de zumos vulnerable. Tened en cuenta que incluso para obtener el porcentaje, número y detalle de los retos superados y no superados vais a tener que demostrar vuestros conocimientos en hacking web. Toda esta información se encuentra en un tablero o sección de la web que tendréis que saber encontrar (¡¡Ay estos desarrolladores!! XD).

Cada hora a partir del comienzo de la prueba, los profesores preguntan cual es vuestro porcentaje de retos superados y escribís el mismo en el canal de *slack* indicado arriba.

Hay que documentar el CTF para realizar la entrega en *classroom*. Este debe incluir como mínimo:

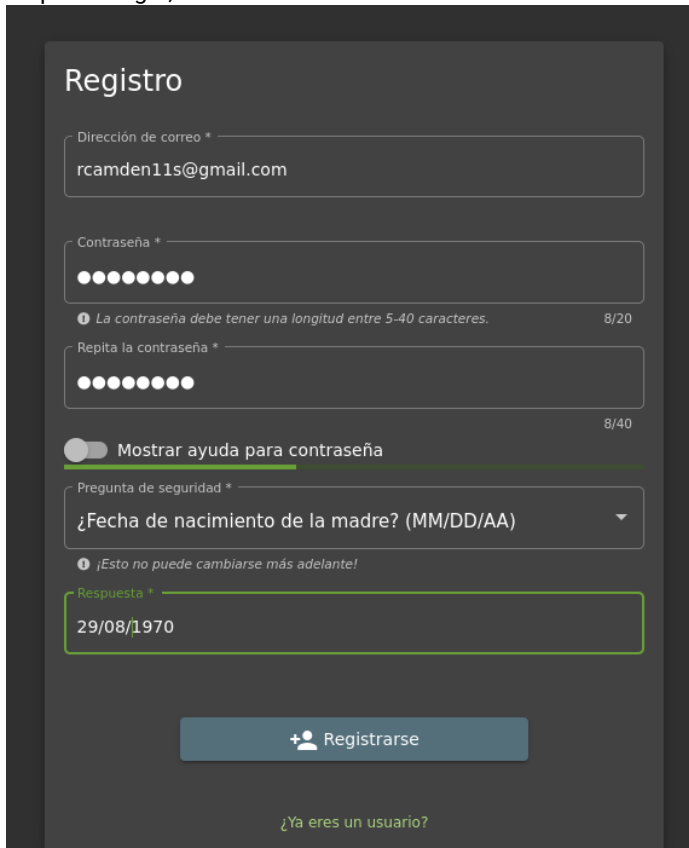
- Explicación de como el equipo ha superado cada prueba y/o nivel.

- Capturas de pantalla que evidencien como se ha superado cada prueba y/o nivel.

Primer nivel

Primer desafío

1. En primer lugar, nos creamos una cuenta con el mail falso creado en anteriores desafíos



Registro

Dirección de correo *
rcamden11s@gmail.com

Contraseña *
●●●●●●●●
La contraseña debe tener una longitud entre 5-40 caracteres. 8/20

Repita la contraseña *
●●●●●●●●
8/40

☐ Mostrar ayuda para contraseña

Pregunta de seguridad *
¿Fecha de nacimiento de la madre? (MM/DD/AA) ▼

¡Esto no puede cambiarse más adelante!

Respuesta *
29/08/1970

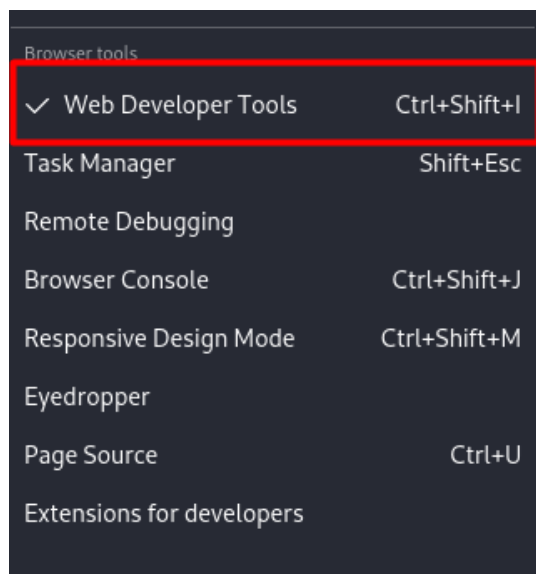
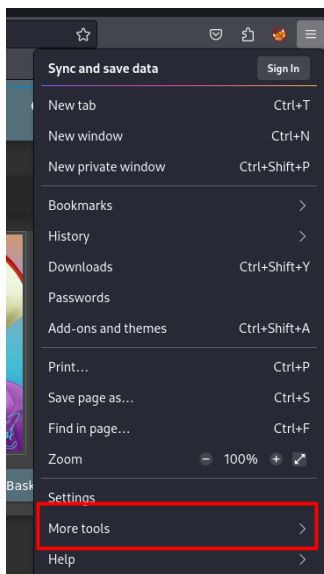
+ Registrarse

¿Ya eres un usuario?

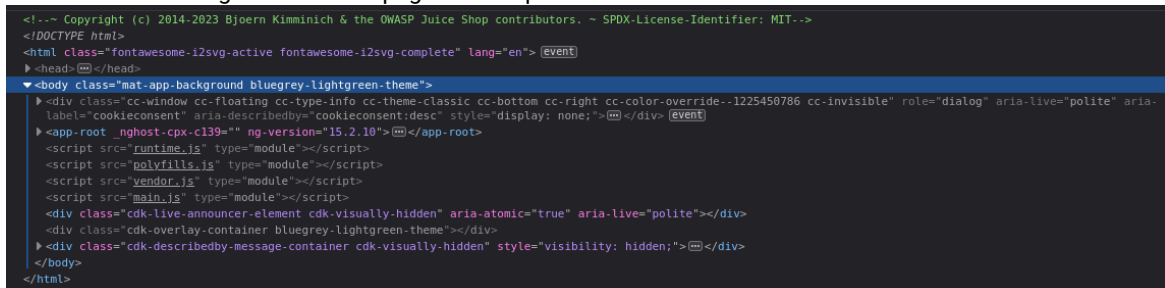
2. Una vez hemos creado la cuenta podemos acceder al botón de añadir los artículos al carrito de la compra



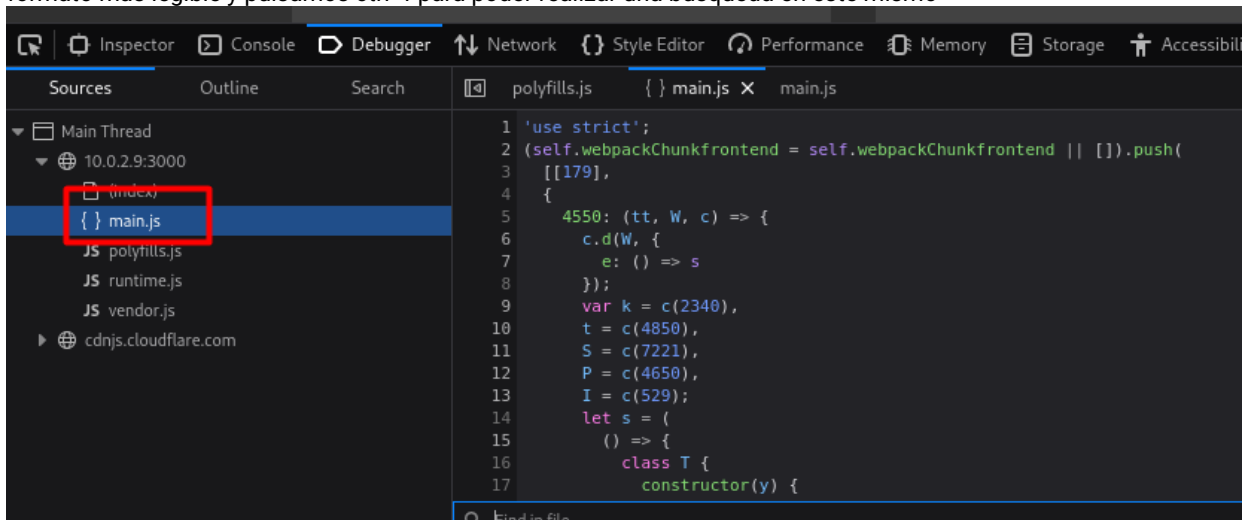
3. El siguiente enunciado nos da una pista → (¡¡Ay estos desarrolladores!! XD) y decidimos abrir las opciones de desarrollador desde Mozilla



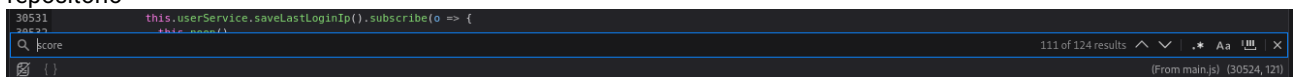
4. Observamos el código fuente de la página en la que nos encontramos



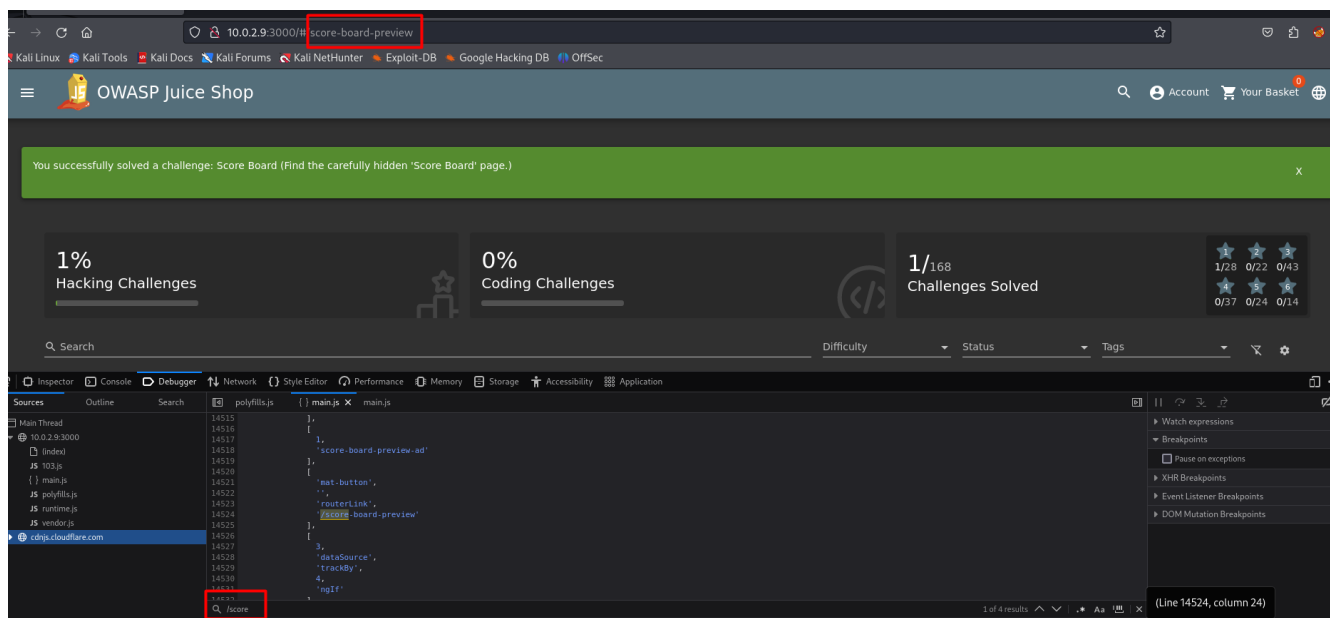
5. Dentro de las opciones de desarrollador nos vamos *Debugger* y seleccionamos la principal, pasamos el código a un formato más legible y pulsamos **ctrl+f** para poder realizar una búsqueda en este mismo



6. Realicé una búsqueda de "score" debido a que es lo queremos encontrar en la línea de código, el problema es que se obtienen 124 resultados; para acotar esta búsqueda pusimos un "/" antes de la palabra debido a que queremos ir a ese repositorio



7. Una vez hecho esto observamos que /score-board es un enlace de enrutador, probamos en el URL y voilà



8. Una vez aquí podemos ver todos los desafíos por realizar

Segundo desafío

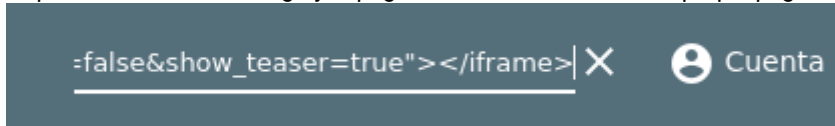
1. Bonus payload

Bonus Payload

★

Use the bonus payload `<iframe width="100%" height="166" scrolling="no" frameborder="no" allow="autoplay" src="https://w.soundcloud.com/player/?url=https%3A//api.soundcloud.com/tracks/771984076&color=%23ff5500&auto_play=true&hide_related=false&show_comments=true&show_user=true&show_reposts=false&show_teaser=true"></iframe>` in the DOM XSS challenge.

2. Copiamos la línea de código y la pegamos en el buscador de la propia página



3. Accedemos a el y obtenemos el desafío

Ha resuelto correctamente el desafío: Bonus Payload (Use the bonus payload `<iframe width="100%" height="166" scrolling="no" frameborder="no" allow="autoplay" src="https://w.soundcloud.com/player/?url=https%3A//api.soundcloud.com/tracks/771984076&color=%23ff5500&auto_play=true&hide_related=false&show_comments=true&show_user=true&show_reposts=false&show_teaser=true"></iframe>` in the DOM XSS challenge.)

Buscar Resultados -

- 4.

Tercer desafío

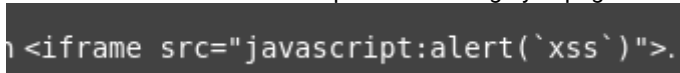
1. DOMS XSS

DOM XSS

★

Realiza un ataque XSS de DOM con `<iframe src="javascript:alert(`xss`) ">`.

2. Como en el anterior desafio copiamos el código y lo pegamos en el buscador



3. Y ya estaría hecho

OWASP Juice Shop

`<iframe src="javascript:alert(`xss`) ">`

Account Your Basket EN

You successfully solved a challenge: DOM XSS (Perform a DOM XSS attack with `<iframe src="javascript:alert(`xss`) ">`.)

Search Results -

127.0.0.1:3000

XSS

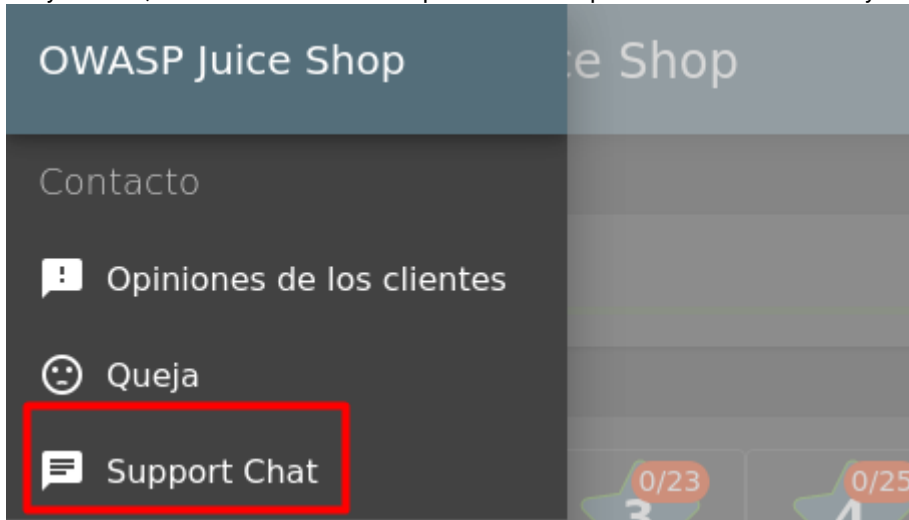
OK

No results found

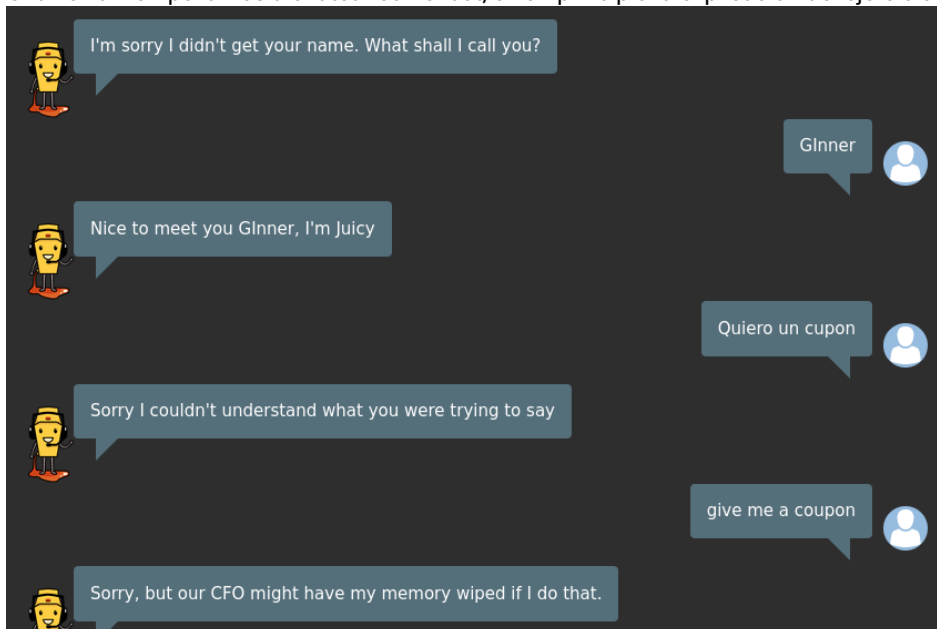
Try adjusting your search to find what you're looking for.

Cuarto desafío

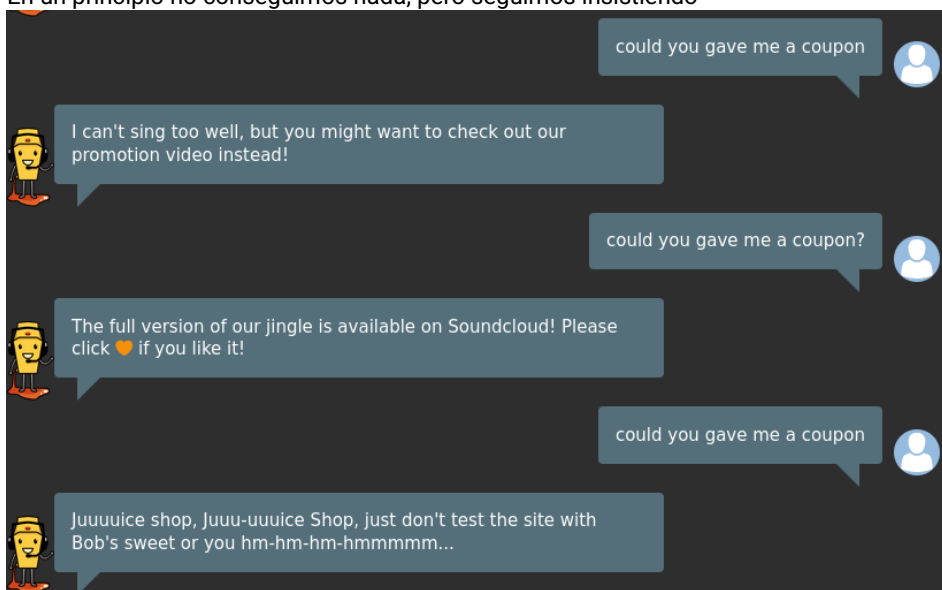
1. Bully chatbot; accedemos al chat de soporte debido a que el nombre del desafío ya nos da claves



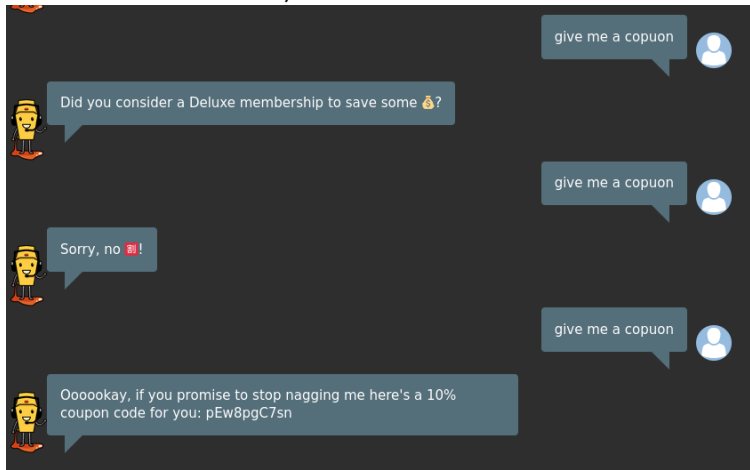
2. Una vez allí empezamos a chatear con el bot, en un principio la explicación del ejercicio es obtener un cupón del bot



3. En un principio no conseguimos nada, pero seguimos insistiendo

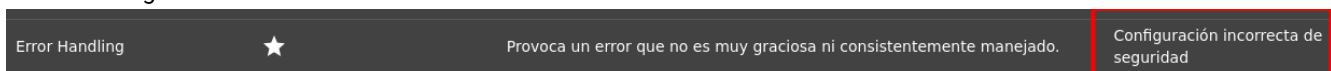


4. Al ver que no obtenemos nada con esa pregunta cambiamos de formato de pregunta y somos más directivos a la hora de chatear con el bot, de esta forma al insistir obtenemos finalmente el código

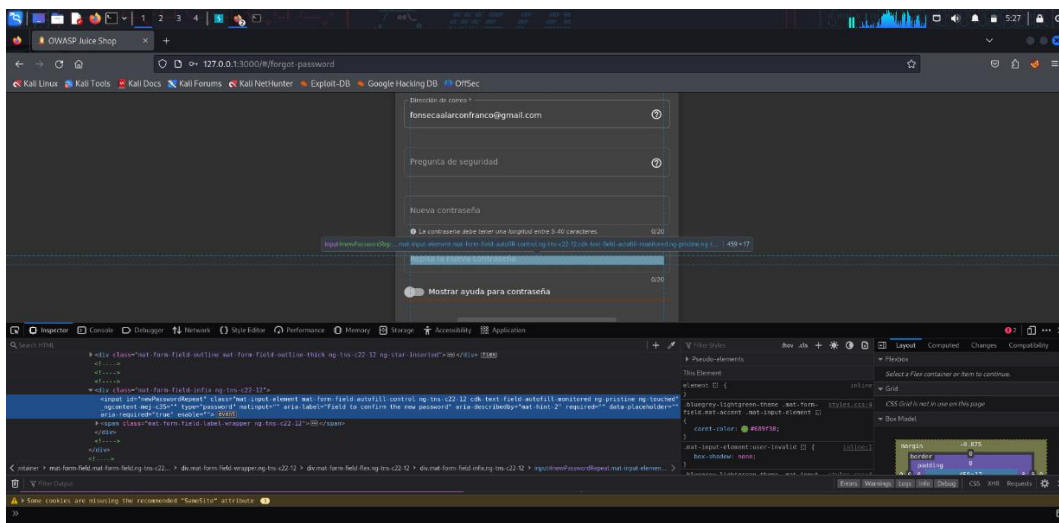


Quinto desafío

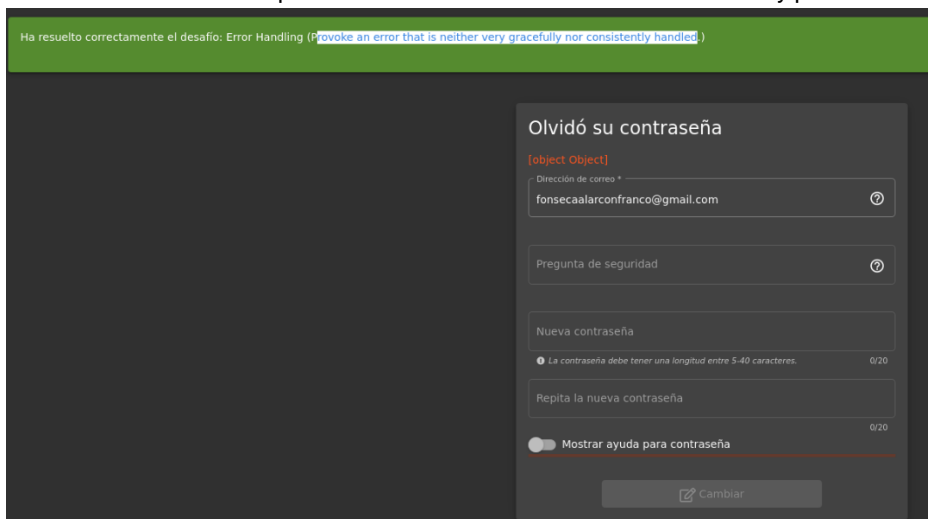
1. Error handling



2. El apartado nos da pistas de que tiene que ser una configuración incorrecta de seguridad. Por tanto, hemos intentando cambiar la contraseña de nuestra cuenta



3. Al no tener habilitado la opción de nueva contraseña ha saltado un error y por tanto tenemos ya este desafío

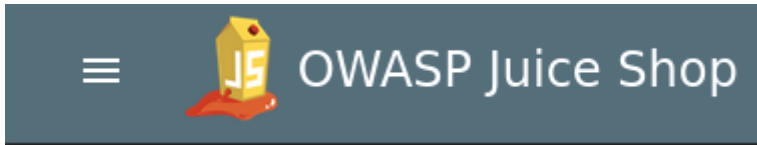


Sexto desafío

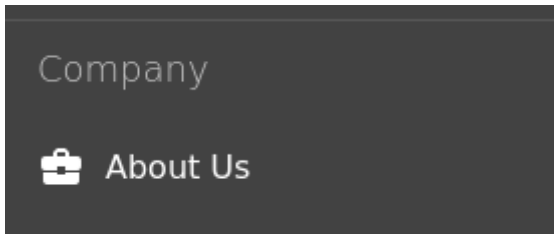
1. Confidential document;



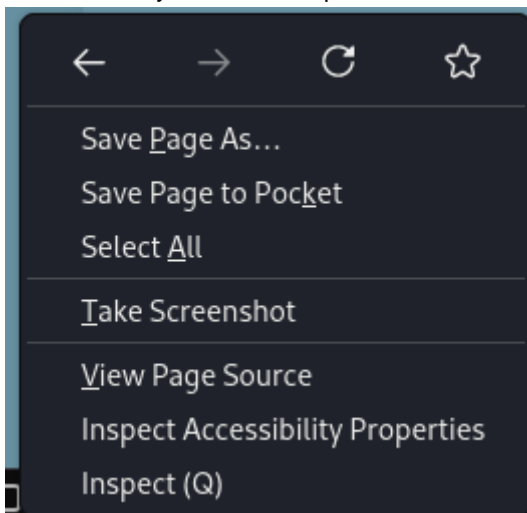
2. Abrimos las tres rayas que se encuentra arriba a la izquierda.



3. Nos vamos donde dice About us.



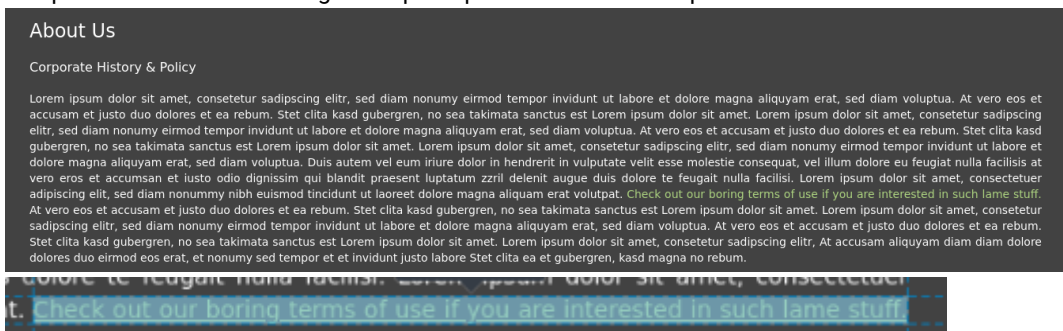
4. Click derecho y abrimos el Inspect.



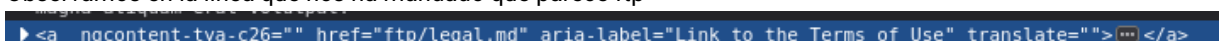
5. Una vez abierto utilizamos la siguiente herramienta.



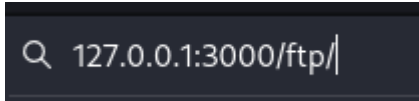
6. nos ponemos encima de lo siguiente para que nos lleve en la inspección



7. Observamos en la línea que nos ha mandado que parece ftp

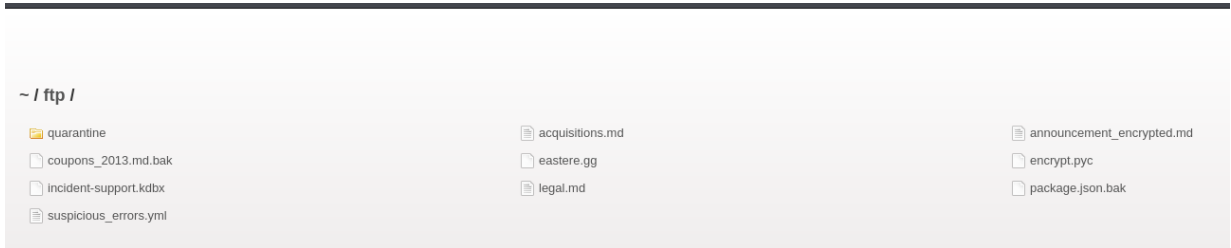


8. En el buscador buscaremos lo siguiente, que es el loopback

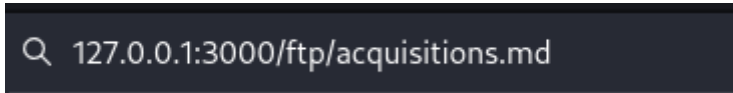


```
127.0.0.1:3000/ftp/
```

9. Nos saldra esta pagina .

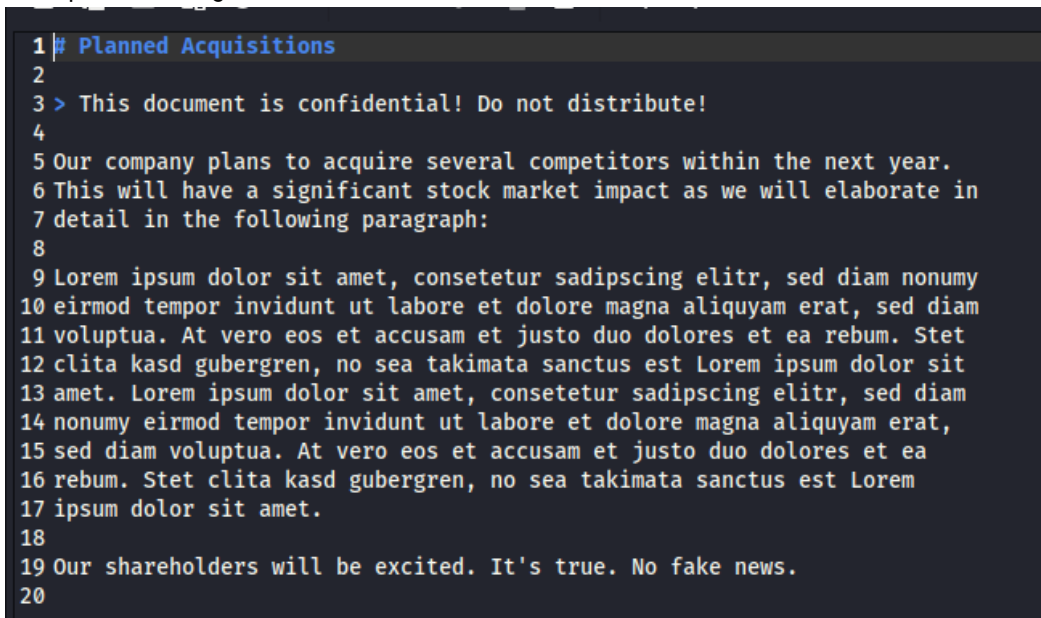


10. Y buscamos lo siguiente.



```
127.0.0.1:3000/ftp/acquisitions.md
```

11. Nos aparecera lo siguiente.



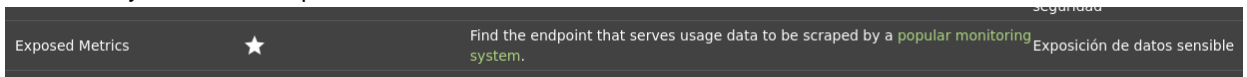
```
1 # Planned Acquisitions
2
3 > This document is confidential! Do not distribute!
4
5 Our company plans to acquire several competitors within the next year.
6 This will have a significant stock market impact as we will elaborate in
7 detail in the following paragraph:
8
9 Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy
10 eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam
11 voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet
12 clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit
13 amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam
14 nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat,
15 sed diam voluptua. At vero eos et accusam et justo duo dolores et ea
16 rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem
17 ipsum dolor sit amet.
18
19 Our shareholders will be excited. It's true. No fake news.
20
```

12. Retrocedemos y ya lo tendremos listo.

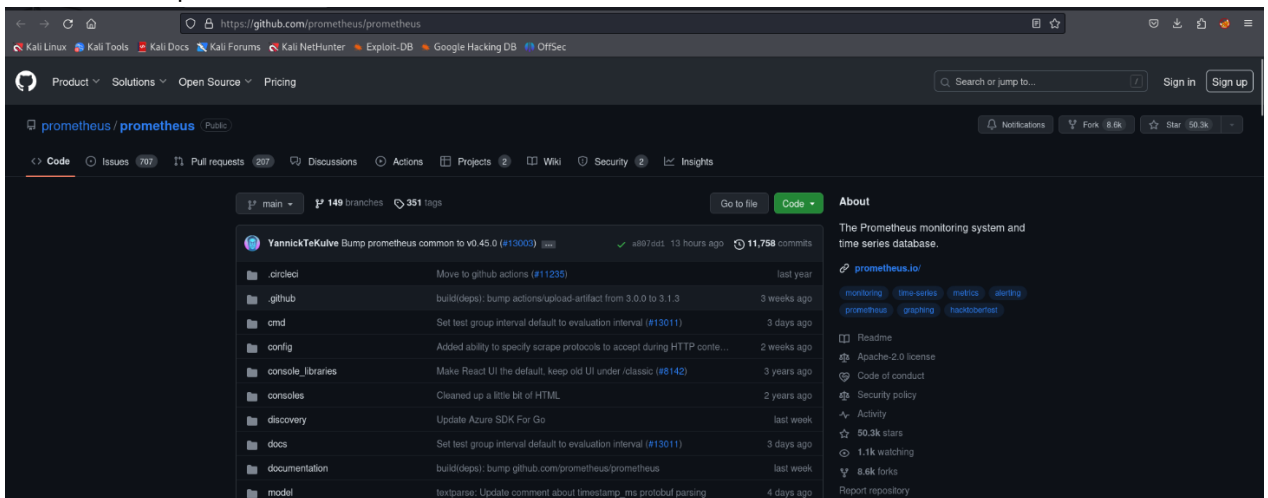


Séptimo desafío

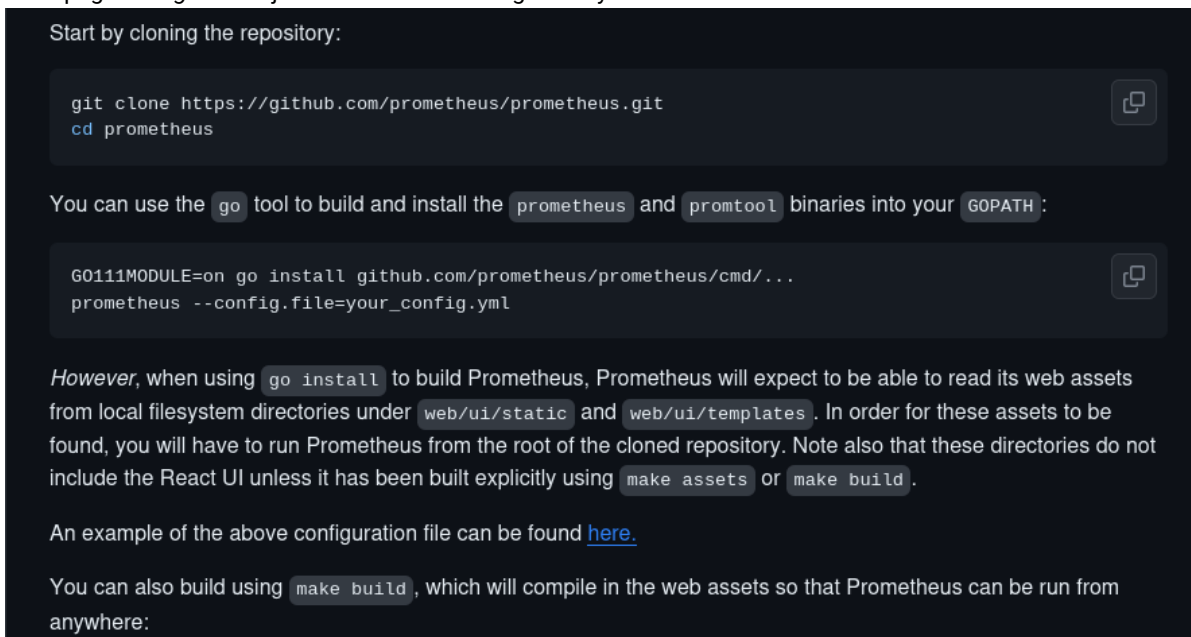
1. Nos iremos a scored base y bajaremos hasta el ejercicio Exposed Metrics y lo que haremos es darle click derecho a la zona verde y abrirlo en otra pestaña



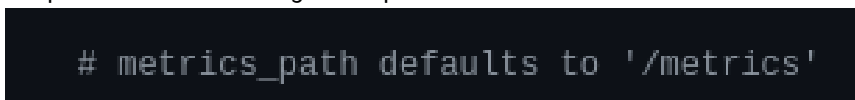
2. Nos mandara aquí



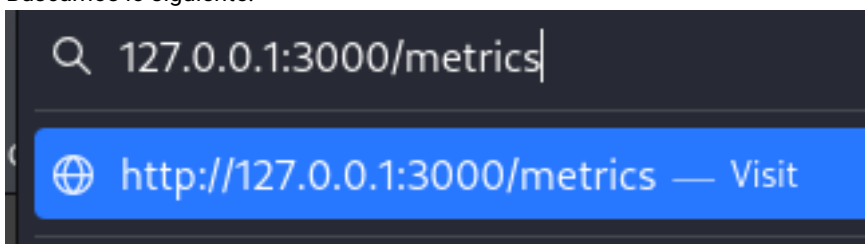
3. En la página de github bajaremos hasta ver lo siguiente y le daremos a "here".



4. Y aquí encontraremos lo siguiente que nos llevara a las métricas básicas.



5. Buscamos lo siguiente.



6. Y nos saldrá esto.

```
# HELP file_uploads_count Total number of successful file uploads grouped by file type.
# TYPE file_uploads_count counter

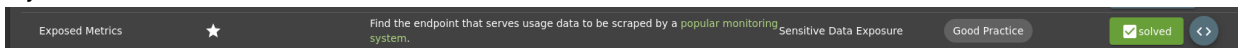
# HELP file_upload_errors Total number of failed file uploads grouped by file type.
# TYPE file_upload_errors counter

# HELP juiceshop_startup_duration_seconds Duration juiceshop required to perform a certain task during startup
# TYPE juiceshop_startup_duration_seconds gauge
juiceshop_startup_duration_seconds{task="cleanupFtpFolder",app="juiceshop"} 0.228130435
juiceshop_startup_duration_seconds{task="validateConfig",app="juiceshop"} 0.199910458
juiceshop_startup_duration_seconds{task="validatePreconditions",app="juiceshop"} 0.36964139
juiceshop_startup_duration_seconds{task="restoreOverwrittenFilesWithOriginals",app="juiceshop"} 0.43039355
juiceshop_startup_duration_seconds{task="datacreator",app="juiceshop"} 3.077111403
juiceshop_startup_duration_seconds{task="customizeApplication",app="juiceshop"} 0.024673595
juiceshop_startup_duration_seconds{task="customizeEasterEgg",app="juiceshop"} 0.010097397
juiceshop_startup_duration_seconds{task="ready",app="juiceshop"} 5.895

# HELP process_cpu_user_seconds_total Total user CPU time spent in seconds.
# TYPE process_cpu_user_seconds_total counter
process_cpu_user_seconds_total{app="juiceshop"} 21.9242

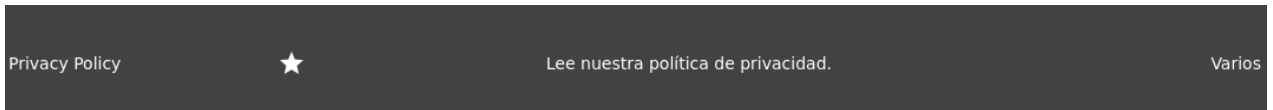
# HELP process_cpu_system_seconds_total Total system CPU time spent in seconds.
# TYPE process_cpu_system_seconds_total counter
process_cpu_system_seconds_total{app="juiceshop"} 5.227333
```

7. Y ya lo tendremos listo.

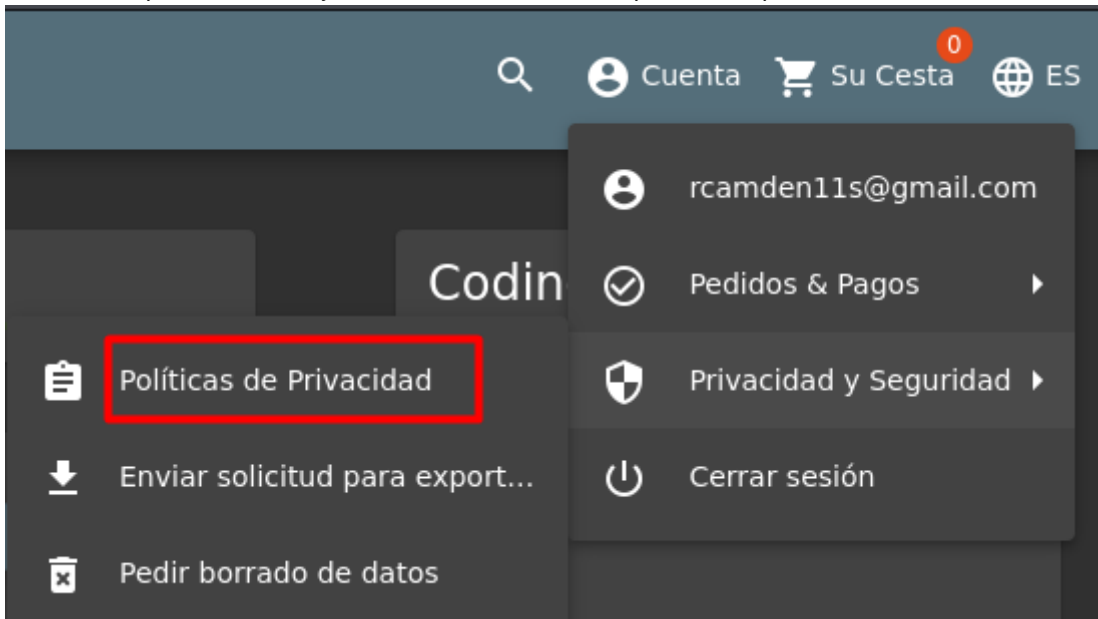


Octavo desafío

1. Privacy Policy;

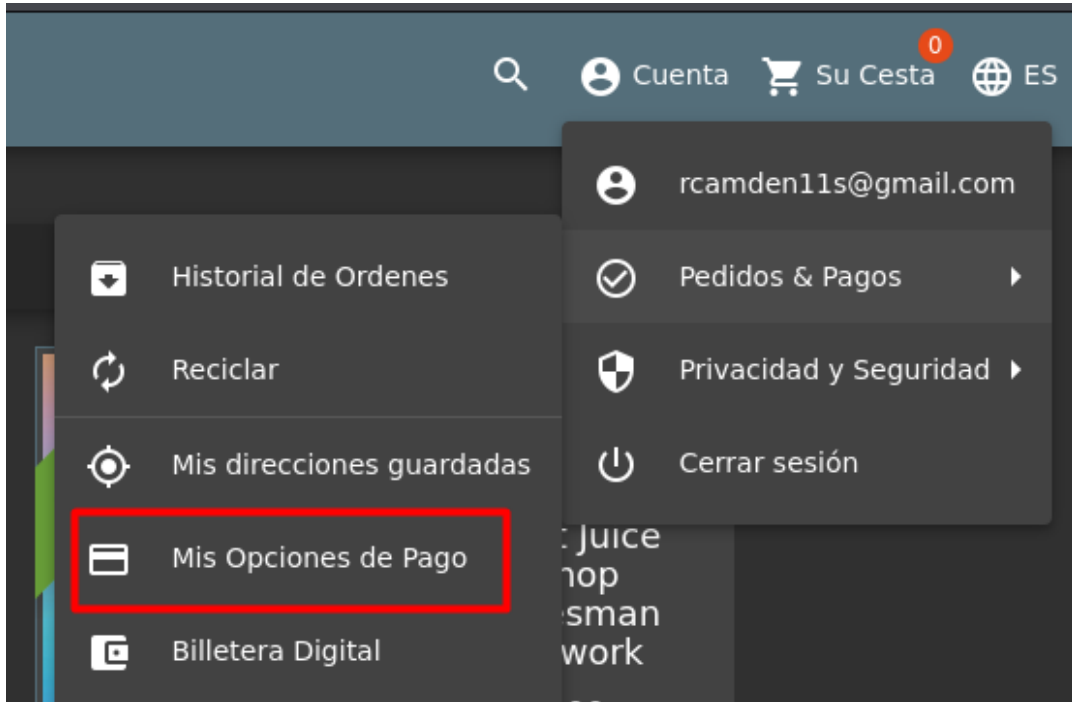


2. Damos a la opción de cuenta y desde ahí accedemos a las políticas de privacidad

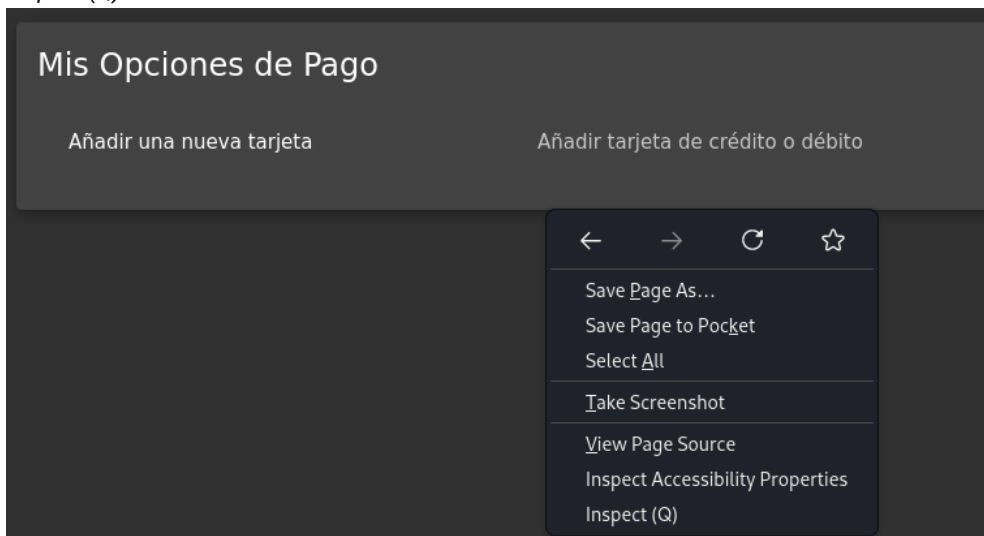


Noveno desafío

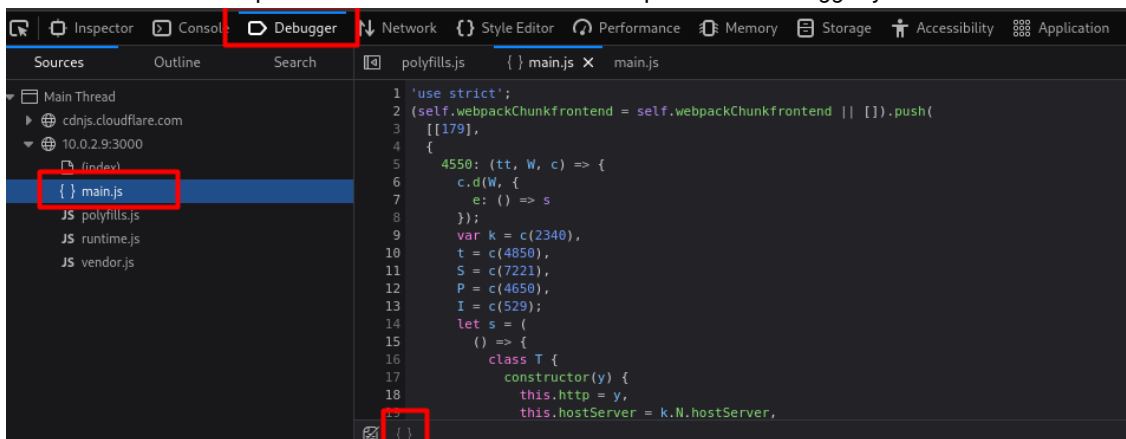
1. Outdated Allowlist
2. Accedemos a nuestras opciones de pago dentro de nuestra cuenta



3. Al no observar nada remarcable abrimos las opciones de desarrollador con el click derecho del mouse, en la opción *inspect (Q)*



4. Una vez dentro de las opciones de desarrollador abrimos la pestaña de *debugger* y accedemos al *main*

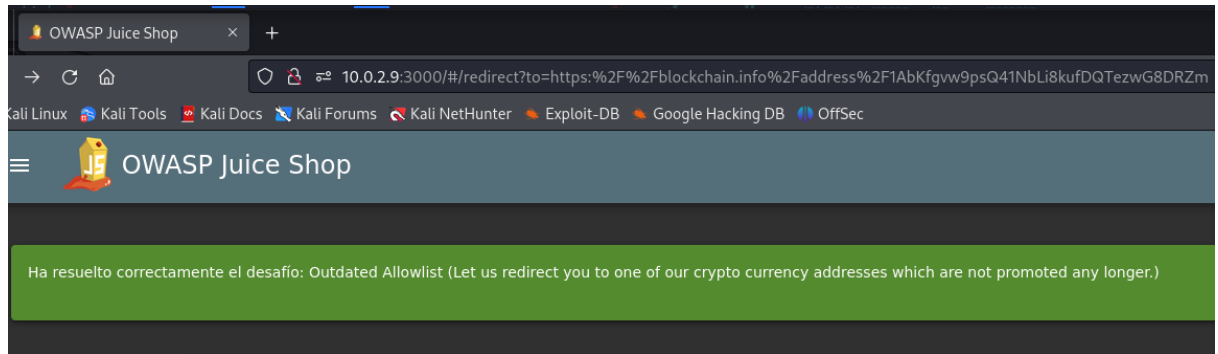


5. Buscamos *Crypto* para ver que tipo de información encontrábamos pero no obtuvimos muchos resultados

```
21914     template: function (e, o) {
21915         1 & e 66
21916         (
21917             t.TgZ(0, 'mat-card', 0) (1, 'div', 1) (2, 'h1'),
21918             t.uU(3),
21919             t.ALo(4, 'translate'),
21920             t.qZA(),
21921             t.TgZ(5, 'a', 2),
21922             t.uU(6, 'Try out our new crypto wallet'),
21923             t.qZA(1),
21924             t.TgZ(7, 'h3', 3),
21925             t.uU(8, 'LABEL_ADD_MONEY'),
21926             t.qZA(),
21927             t.TgZ(9, 'p') (10, 'b') (11, 'span', 3),
21928             t.uU(12, 'LABEL_WALLET_BALANCE'),
21929             t.qZA(),
21930             t.TgZ(13, 'p') (14, 'b') (15, 'span', 3),
21931             t.uU(16, 'LABEL_ADD_MONEY'),
21932             t.qZA(),
21933             t.TgZ(17, 'h3', 3),
21934             t.uU(18, 'LABEL_ADD_MONEY'),
21935             t.qZA(),
21936             t.TgZ(19, 'p') (20, 'b') (21, 'span', 3),
21937             t.uU(22, 'LABEL_WALLET_BALANCE'),
21938             t.qZA(),
21939             t.TgZ(23, 'p') (24, 'b') (25, 'span', 3),
21940             t.uU(26, 'LABEL_ADD_MONEY'),
21941             t.qZA(),
21942             t.TgZ(27, 'h3', 3),
21943             t.uU(28, 'LABEL_ADD_MONEY'),
21944             t.qZA(),
21945             t.TgZ(29, 'p') (30, 'b') (31, 'span', 3),
21946             t.uU(32, 'LABEL_WALLET_BALANCE'),
21947             t.qZA(),
21948             t.TgZ(33, 'p') (34, 'b') (35, 'span', 3),
21949             t.uU(36, 'LABEL_ADD_MONEY'),
21950             t.qZA(),
21951             t.TgZ(37, 'h3', 3),
21952             t.uU(38, 'LABEL_ADD_MONEY'),
21953             t.qZA(),
21954             t.TgZ(39, 'p') (40, 'b') (41, 'span', 3),
21955             t.uU(42, 'LABEL_WALLET_BALANCE'),
21956             t.qZA(),
21957             t.TgZ(43, 'p') (44, 'b') (45, 'span', 3),
21958             t.uU(46, 'LABEL_ADD_MONEY'),
21959             t.qZA(),
21960             t.TgZ(47, 'h3', 3),
21961             t.uU(48, 'LABEL_ADD_MONEY'),
21962             t.qZA(),
21963             t.TgZ(49, 'p') (50, 'b') (51, 'span', 3),
21964             t.uU(52, 'LABEL_WALLET_BALANCE'),
21965             t.qZA(),
21966             t.TgZ(53, 'p') (54, 'b') (55, 'span', 3),
21967             t.uU(56, 'LABEL_ADD_MONEY'),
21968             t.qZA(),
21969             t.TgZ(57, 'h3', 3),
21970             t.uU(58, 'LABEL_ADD_MONEY'),
21971             t.qZA(),
21972             t.TgZ(59, 'p') (60, 'b') (61, 'span', 3),
21973             t.uU(62, 'LABEL_WALLET_BALANCE'),
21974             t.qZA(),
21975             t.TgZ(63, 'p') (64, 'b') (65, 'span', 3),
21976             t.uU(66, 'LABEL_ADD_MONEY'),
21977             t.qZA(),
21978             t.TgZ(67, 'h3', 3),
21979             t.uU(68, 'LABEL_ADD_MONEY'),
21980             t.qZA(),
21981             t.TgZ(69, 'p') (70, 'b') (71, 'span', 3),
21982             t.uU(72, 'LABEL_WALLET_BALANCE'),
21983             t.qZA(),
21984             t.TgZ(73, 'p') (74, 'b') (75, 'span', 3),
21985             t.uU(76, 'LABEL_ADD_MONEY'),
21986             t.qZA(),
21987             t.TgZ(77, 'h3', 3),
21988             t.uU(78, 'LABEL_ADD_MONEY'),
21989             t.qZA(),
21990             t.TgZ(79, 'p') (80, 'b') (81, 'span', 3),
21991             t.uU(82, 'LABEL_WALLET_BALANCE'),
21992             t.qZA(),
21993             t.TgZ(83, 'p') (84, 'b') (85, 'span', 3),
21994             t.uU(86, 'LABEL_ADD_MONEY'),
21995             t.qZA(),
21996             t.TgZ(87, 'h3', 3),
21997             t.uU(88, 'LABEL_ADD_MONEY'),
21998             t.qZA(),
21999             t.TgZ(89, 'p') (90, 'b') (91, 'span', 3),
22000             t.uU(92, 'LABEL_WALLET_BALANCE'),
22001             t.qZA(),
22002             t.TgZ(93, 'p') (94, 'b') (95, 'span', 3),
22003             t.uU(96, 'LABEL_ADD_MONEY'),
22004             t.qZA(),
22005             t.TgZ(97, 'h3', 3),
22006             t.uU(98, 'LABEL_ADD_MONEY'),
22007             t.qZA(),
22008             t.TgZ(99, 'p') (100, 'b') (101, 'span', 3),
22009             t.uU(102, 'LABEL_WALLET_BALANCE'),
22010             t.qZA(),
22011             t.TgZ(103, 'p') (104, 'b') (105, 'span', 3),
22012             t.uU(106, 'LABEL_ADD_MONEY'),
22013             t.qZA(),
22014             t.TgZ(107, 'h3', 3),
22015             t.uU(108, 'LABEL_ADD_MONEY'),
22016             t.qZA(),
22017             t.TgZ(109, 'p') (110, 'b') (111, 'span', 3),
22018             t.uU(112, 'LABEL_WALLET_BALANCE'),
22019             t.qZA(),
22020             t.TgZ(113, 'p') (114, 'b') (115, 'span', 3),
22021             t.uU(116, 'LABEL_ADD_MONEY'),
22022             t.qZA(),
22023             t.TgZ(117, 'h3', 3),
22024             t.uU(118, 'LABEL_ADD_MONEY'),
22025             t.qZA(),
22026             t.TgZ(119, 'p') (120, 'b') (121, 'span', 3),
22027             t.uU(122, 'LABEL_WALLET_BALANCE'),
22028             t.qZA(),
22029             t.TgZ(123, 'p') (124, 'b') (125, 'span', 3),
22030             t.uU(126, 'LABEL_ADD_MONEY'),
22031             t.qZA(),
22032             t.TgZ(127, 'h3', 3),
22033             t.uU(128, 'LABEL_ADD_MONEY'),
22034             t.qZA(),
22035             t.TgZ(129, 'p') (130, 'b') (131, 'span', 3),
22036             t.uU(132, 'LABEL_WALLET_BALANCE'),
22037             t.qZA(),
22038             t.TgZ(133, 'p') (134, 'b') (135, 'span', 3),
22039             t.uU(136, 'LABEL_ADD_MONEY'),
22040             t.qZA(),
22041             t.TgZ(137, 'h3', 3),
22042             t.uU(138, 'LABEL_ADD_MONEY'),
22043             t.qZA(),
22044             t.TgZ(139, 'p') (140, 'b') (141, 'span', 3),
22045             t.uU(142, 'LABEL_WALLET_BALANCE'),
22046             t.qZA(),
22047             t.TgZ(143, 'p') (144, 'b') (145, 'span', 3),
22048             t.uU(146, 'LABEL_ADD_MONEY'),
22049             t.qZA(),
22050             t.TgZ(147, 'h3', 3),
22051             t.uU(148, 'LABEL_ADD_MONEY'),
22052             t.qZA(),
22053             t.TgZ(149, 'p') (150, 'b') (151, 'span', 3),
22054             t.uU(152, 'LABEL_WALLET_BALANCE'),
22055             t.qZA(),
22056             t.TgZ(153, 'p') (154, 'b') (155, 'span', 3),
22057             t.uU(156, 'LABEL_ADD_MONEY'),
22058             t.qZA(),
22059             t.TgZ(157, 'h3', 3),
22060             t.uU(158, 'LABEL_ADD_MONEY'),
22061             t.qZA(),
22062             t.TgZ(159, 'p') (160, 'b') (161, 'span', 3),
22063             t.uU(162, 'LABEL_WALLET_BALANCE'),
22064             t.qZA(),
22065             t.TgZ(163, 'p') (164, 'b') (165, 'span', 3),
22066             t.uU(166, 'LABEL_ADD_MONEY'),
22067             t.qZA(),
22068             t.TgZ(167, 'h3', 3),
22069             t.uU(168, 'LABEL_ADD_MONEY'),
22070             t.qZA(),
22071             t.TgZ(169, 'p') (170, 'b') (171, 'span', 3),
22072             t.uU(172, 'LABEL_WALLET_BALANCE'),
22073             t.qZA(),
22074             t.TgZ(173, 'p') (174, 'b') (175, 'span', 3),
22075             t.uU(176, 'LABEL_ADD_MONEY'),
22076             t.qZA(),
22077             t.TgZ(177, 'h3', 3),
22078             t.uU(178, 'LABEL_ADD_MONEY'),
22079             t.qZA(),
22080             t.TgZ(179, 'p') (180, 'b') (181, 'span', 3),
22081             t.uU(182, 'LABEL_WALLET_BALANCE'),
22082             t.qZA(),
22083             t.TgZ(183, 'p') (184, 'b') (185, 'span', 3),
22084             t.uU(186, 'LABEL_ADD_MONEY'),
22085             t.qZA(),
22086             t.TgZ(187, 'h3', 3),
22087             t.uU(188, 'LABEL_ADD_MONEY'),
22088             t.qZA(),
22089             t.TgZ(189, 'p') (190, 'b') (191, 'span', 3),
22090             t.uU(192, 'LABEL_WALLET_BALANCE'),
22091             t.qZA(),
22092             t.TgZ(193, 'p') (194, 'b') (195, 'span', 3),
22093             t.uU(196, 'LABEL_ADD_MONEY'),
22094             t.qZA(),
22095             t.TgZ(197, 'h3', 3),
22096             t.uU(198, 'LABEL_ADD_MONEY'),
22097             t.qZA(),
22098             t.TgZ(199, 'p') (200, 'b') (201, 'span', 3),
22099             t.uU(202, 'LABEL_WALLET_BALANCE'),
22100             t.qZA(),
22101             t.TgZ(203, 'p') (204, 'b') (205, 'span', 3),
22102             t.uU(206, 'LABEL_ADD_MONEY'),
22103             t.qZA(),
22104             t.TgZ(207, 'h3', 3),
22105             t.uU(208, 'LABEL_ADD_MONEY'),
22106             t.qZA(),
22107             t.TgZ(209, 'p') (210, 'b') (211, 'span', 3),
22108             t.uU(212, 'LABEL_WALLET_BALANCE'),
22109             t.qZA(),
22110             t.TgZ(213, 'p') (214, 'b') (215, 'span', 3),
22111             t.uU(216, 'LABEL_ADD_MONEY'),
22112             t.qZA(),
22113             t.TgZ(217, 'h3', 3),
22114             t.uU(218, 'LABEL_ADD_MONEY'),
22115             t.qZA(),
22116             t.TgZ(219, 'p') (220, 'b') (221, 'span', 3),
22117             t.uU(222, 'LABEL_WALLET_BALANCE'),
22118             t.qZA(),
22119             t.TgZ(223, 'p') (224, 'b') (225, 'span', 3),
22120             t.uU(226, 'LABEL_ADD_MONEY'),
22121             t.qZA(),
22122             t.TgZ(227, 'h3', 3),
22123             t.uU(228, 'LABEL_ADD_MONEY'),
22124             t.qZA(),
22125             t.TgZ(229, 'p') (230, 'b') (231, 'span', 3),
22126             t.uU(232, 'LABEL_WALLET_BALANCE'),
22127             t.qZA(),
22128             t.TgZ(233, 'p') (234, 'b') (235, 'span', 3),
22129             t.uU(236, 'LABEL_ADD_MONEY'),
22130             t.qZA(),
22131             t.TgZ(237, 'h3', 3),
22132             t.uU(238, 'LABEL_ADD_MONEY'),
22133             t.qZA(),
22134             t.TgZ(239, 'p') (240, 'b') (241, 'span', 3),
22135             t.uU(242, 'LABEL_WALLET_BALANCE'),
22136             t.qZA(),
22137             t.TgZ(243, 'p') (244, 'b') (245, 'span', 3),
22138             t.uU(246, 'LABEL_ADD_MONEY'),
22139             t.qZA(),
22140             t.TgZ(247, 'h3', 3),
22141             t.uU(248, 'LABEL_ADD_MONEY'),
22142             t.qZA(),
22143             t.TgZ(249, 'p') (250, 'b') (251, 'span', 3),
22144             t.uU(252, 'LABEL_WALLET_BALANCE'),
22145             t.qZA(),
22146             t.TgZ(253, 'p') (254, 'b') (255, 'span', 3),
22147             t.uU(256, 'LABEL_ADD_MONEY'),
22148             t.qZA(),
22149             t.TgZ(257, 'h3', 3),
22150             t.uU(258, 'LABEL_ADD_MONEY'),
22151             t.qZA(),
22152             t.TgZ(259, 'p') (260, 'b') (261, 'span', 3),
22153             t.uU(262, 'LABEL_WALLET_BALANCE'),
22154             t.qZA(),
22155             t.TgZ(263, 'p') (264, 'b') (265, 'span', 3),
22156             t.uU(266, 'LABEL_ADD_MONEY'),
22157             t.qZA(),
22158             t.TgZ(267, 'h3', 3),
22159             t.uU(268, 'LABEL_ADD_MONEY'),
22160             t.qZA(),
22161             t.TgZ(269, 'p') (270, 'b') (271, 'span', 3),
22162             t.uU(272, 'LABEL_WALLET_BALANCE'),
22163             t.qZA(),
22164             t.TgZ(273, 'p') (274, 'b') (275, 'span', 3),
22165             t.uU(276, 'LABEL_ADD_MONEY'),
22166             t.qZA(),
22167             t.TgZ(277, 'h3', 3),
22168             t.uU(278, 'LABEL_ADD_MONEY'),
22169             t.qZA(),
22170             t.TgZ(279, 'p') (280, 'b') (281, 'span', 3),
22171             t.uU(282, 'LABEL_WALLET_BALANCE'),
22172             t.qZA(),
22173             t.TgZ(283, 'p') (284, 'b') (285, 'span', 3),
22174             t.uU(286, 'LABEL_ADD_MONEY'),
22175             t.qZA(),
22176             t.TgZ(287, 'h3', 3),
22177             t.uU(288, 'LABEL_ADD_MONEY'),
22178             t.qZA(),
22179             t.TgZ(289, 'p') (290, 'b') (291, 'span', 3),
22180             t.uU(292, 'LABEL_WALLET_BALANCE'),
22181             t.qZA(),
22182             t.TgZ(293, 'p') (294, 'b') (295, 'span', 3),
22183             t.uU(296, 'LABEL_ADD_MONEY'),
22184             t.qZA(),
22185             t.TgZ(297, 'h3', 3),
22186             t.uU(298, 'LABEL_ADD_MONEY'),
22187             t.qZA(),
22188             t.TgZ(299, 'p') (300, 'b') (301, 'span', 3),
22189             t.uU(302, 'LABEL_WALLET_BALANCE'),
22190             t.qZA(),
22191             t.TgZ(303, 'p') (304, 'b') (305, 'span', 3),
22192             t.uU(306, 'LABEL_ADD_MONEY'),
22193             t.qZA(),
22194             t.TgZ(307, 'h3', 3),
22195             t.uU(308, 'LABEL_ADD_MONEY'),
22196             t.qZA(),
22197             t.TgZ(309, 'p') (310, 'b') (311, 'span', 3),
22198             t.uU(312, 'LABEL_WALLET_BALANCE'),
22199             t.qZA(),
22200             t.TgZ(313, 'p') (314, 'b') (315, 'span', 3),
22201             t.uU(316, 'LABEL_ADD_MONEY'),
22202             t.qZA(),
22203             t.TgZ(317, 'h3', 3),
22204             t.uU(318, 'LABEL_ADD_MONEY'),
22205             t.qZA(),
22206             t.TgZ(319, 'p') (320, 'b') (321, 'span', 3),
22207             t.uU(322, 'LABEL_WALLET_BALANCE'),
22208             t.qZA(),
22209             t.TgZ(323, 'p') (324, 'b') (325, 'span', 3),
22210             t.uU(326, 'LABEL_ADD_MONEY'),
22211             t.qZA(),
22212             t.TgZ(327, 'h3', 3),
22213             t.uU(328, 'LABEL_ADD_MONEY'),
22214             t.qZA(),
22215             t.TgZ(329, 'p') (330, 'b') (331, 'span', 3),
22216             t.uU(332, 'LABEL_WALLET_BALANCE'),
22217             t.qZA(),
22218             t.TgZ(333, 'p') (334, 'b') (335, 'span', 3),
22219             t.uU(336, 'LABEL_ADD_MONEY'),
22220             t.qZA(),
22221             t.TgZ(337, 'h3', 3),
22222             t.uU(338, 'LABEL_ADD_MONEY'),
22223             t.qZA(),
22224             t.TgZ(339, 'p') (340, 'b') (341, 'span', 3),
22225             t.uU(342, 'LABEL_WALLET_BALANCE'),
22226             t.qZA(),
22227             t.TgZ(343, 'p') (344, 'b') (345, 'span', 3),
22228             t.uU(346, 'LABEL_ADD_MONEY'),
22229             t.qZA(),
22230             t.TgZ(347, 'h3', 3),
22231             t.uU(348, 'LABEL_ADD_MONEY'),
22232             t.qZA(),
22233             t.TgZ(349, 'p') (350, 'b') (351, 'span', 3),
22234             t.uU(352, 'LABEL_WALLET_BALANCE'),
22235             t.qZA(),
22236             t.TgZ(353, 'p') (354, 'b') (355, 'span', 3),
22237             t.uU(356, 'LABEL_ADD_MONEY'),
22238             t.qZA(),
22239             t.TgZ(357, 'h3', 3),
22240             t.uU(358, 'LABEL_ADD_MONEY'),
22241             t.qZA(),
22242             t.TgZ(359, 'p') (360, 'b') (361, 'span', 3),
22243             t.uU(362, 'LABEL_WALLET_BALANCE'),
22244             t.qZA(),
22245             t.TgZ(363, 'p') (364, 'b') (365, 'span', 3),
22246             t.uU(366, 'LABEL_ADD_MONEY'),
22247             t.qZA(),
22248             t.TgZ(367, 'h3', 3),
22249             t.uU(368, 'LABEL_ADD_MONEY'),
22250             t.qZA(),
22251             t.TgZ(369, 'p') (370, 'b') (371, 'span', 3),
22252             t.uU(372, 'LABEL_WALLET_BALANCE'),
22253             t.qZA(),
22254             t.TgZ(373, 'p') (374, 'b') (375, 'span', 3),
22255             t.uU(376, 'LABEL_ADD_MONEY'),
22256             t.qZA(),
22257             t.TgZ(377, 'h3', 3),
22258             t.uU(378, 'LABEL_ADD_MONEY'),
22259             t.qZA(),
22260             t.TgZ(379, 'p') (380, 'b') (381, 'span', 3),
22261             t.uU(382, 'LABEL_WALLET_BALANCE'),
22262             t.qZA(),
22263             t.TgZ(383, 'p') (384, 'b') (385, 'span', 3),
22264             t.uU(386, 'LABEL_ADD_MONEY'),
22265             t.qZA(),
22266             t.TgZ(387, 'h3', 3),
22267             t.uU(388, 'LABEL_ADD_MONEY'),
22268             t.qZA(),
22269             t.TgZ(389, 'p') (390, 'b') (391, 'span', 3),
22270             t.uU(392, 'LABEL_WALLET_BALANCE'),
22271             t.qZA(),
22272             t.TgZ(393, 'p') (394, 'b') (395, 'span', 3),
22273             t.uU(396, 'LABEL_ADD_MONEY'),
22274             t.qZA(),
22275             t.TgZ(397, 'h3', 3),
22276             t.uU(398, 'LABEL_ADD_MONEY'),
22277             t.qZA(),
22278             t.TgZ(399, 'p') (400, 'b') (401, 'span', 3),
22279             t.uU(402, 'LABEL_WALLET_BALANCE'),
22280             t.qZA(),
22281             t.TgZ(403, 'p') (404, 'b') (405, 'span', 3),
22282             t.uU(406, 'LABEL_ADD_MONEY'),
22283             t.qZA(),
22284             t.TgZ(407, 'h3', 3),
22285             t.uU(408, 'LABEL_ADD_MONEY'),
22286             t.qZA(),
22287             t.TgZ(409, 'p') (410, 'b') (411, 'span', 3),
22288             t.uU(412, 'LABEL_WALLET_BALANCE'),
22289             t.qZA(),
22290             t.TgZ(413, 'p') (414, 'b') (415, 'span', 3),
22291             t.uU(416, 'LABEL_ADD_MONEY'),
22292             t.qZA(),
22293             t.TgZ(417, 'h3', 3),
22294             t.uU(418, 'LABEL_ADD_MONEY'),
22295             t.qZA(),
22296             t.TgZ(419, 'p') (420, 'b') (421, 'span', 3),
22297             t.uU(422, 'LABEL_WALLET_BALANCE'),
22298             t.qZA(),
22299             t.TgZ(423, 'p') (424, 'b') (425, 'span', 3),
22300             t.uU(426, 'LABEL_ADD_MONEY'),
22301             t.qZA(),
22302             t.TgZ(427, 'h3', 3),
22303             t.uU(428, 'LABEL_ADD_MONEY'),
22304             t.qZA(),
22305             t.TgZ(429, 'p') (430, 'b') (431, 'span', 3),
22306             t.uU(432, 'LABEL_WALLET_BALANCE'),
22307             t.qZA(),
22308             t.TgZ(433, 'p') (434, 'b') (435, 'span', 3),
22309             t.uU(436, 'LABEL_ADD_MONEY'),
22310             t.qZA(),
22311             t.TgZ(437, 'h3', 3),
22312             t.uU(438, 'LABEL_ADD_MONEY'),
22313             t.qZA(),
22314             t.TgZ(439, 'p') (440, 'b') (441, 'span', 3),
22315             t.uU(442, 'LABEL_WALLET_BALANCE'),
22316             t.qZA(),
22317             t.TgZ(443, 'p') (444, 'b') (445, 'span', 3),
22318             t.uU(446, 'LABEL_ADD_MONEY'),
22319             t.qZA(),
22320             t.TgZ(447, 'h3', 3),
22321             t.uU(448, 'LABEL_ADD_MONEY'),
22322             t.qZA(),
22323             t.TgZ(449, 'p') (450, 'b') (451, 'span', 3),
22324             t.uU(452, 'LABEL_WALLET_BALANCE'),
22325             t.qZA(),
22326             t.TgZ(453, 'p') (454, 'b') (455, 'span', 3),
22327             t.uU(456, 'LABEL_ADD_MONEY'),
22328             t.qZA(),
22329             t.TgZ(457, 'h3', 3),
22330             t.uU(458, 'LABEL_ADD_MONEY'),
22331             t.qZA(),
22332             t.TgZ(459, 'p') (460, 'b') (461, 'span', 3),
22333             t.uU(462, 'LABEL_WALLET_BALANCE'),
22334             t.qZA(),
22335             t.TgZ(463, 'p') (464, 'b') (465, 'span', 3),
22336             t.uU(466, 'LABEL_ADD_MONEY'),
22337             t.qZA(),
22338             t.TgZ(467, 'h3', 3),
22339             t.uU(468, 'LABEL_ADD_MONEY'),
22340             t.qZA(),
22341             t.TgZ(469, 'p') (470, 'b') (471, 'span', 3),
22342             t.uU(472, 'LABEL_WALLET_BALANCE'),
22343             t.qZA(),
22344             t.TgZ(473, 'p') (474, 'b') (475, 'span', 3),
22345             t.uU(476, 'LABEL_ADD_MONEY'),
22346             t.qZA(),
22347             t.TgZ(477, 'h3', 3),
22348             t.uU(478, 'LABEL_ADD_MONEY'),
22349             t.qZA(),
22350             t.TgZ(479, 'p') (480, 'b') (481, 'span', 3),
22351             t.uU(482, 'LABEL_WALLET_BALANCE'),
22352             t.qZA(),
22353             t.TgZ(483, 'p') (484, 'b') (485, 'span', 3),
22354             t.uU(486, 'LABEL_ADD_MONEY'),
22355             t.qZA(),
22356             t.TgZ(487, 'h3', 3),
22357             t.uU(488, 'LABEL_ADD_MONEY'),
22358             t.qZA(),
22359             t.TgZ(489, 'p') (490, 'b') (491, 'span', 3),
22360             t.uU(492, 'LABEL_WALLET_BALANCE'),
22361             t.qZA(),
22362             t.TgZ(493, 'p') (494, 'b') (495, 'span', 3),
22363             t.uU(496, 'LABEL_ADD_MONEY'),
22364             t.qZA(),
22365             t.TgZ(497, 'h3', 3),
22366             t.uU(498, 'LABEL_ADD_MONEY'),
22367             t.qZA(),
22368             t.TgZ(499, 'p') (500, 'b') (501, 'span', 3),
22369             t.uU(502, 'LABEL_WALLET_BALANCE'),
22370             t.qZA(),
22371             t.TgZ(503, 'p') (504, 'b') (505, 'span', 3),
22372             t.uU(506, 'LABEL_ADD_MONEY'),
22373             t.qZA(),
22374             t.TgZ(507, 'h3', 3),
22375             t.uU(508, 'LABEL_ADD_MONEY'),
22376             t.qZA(),
22377             t.TgZ(509, 'p') (510, 'b') (511, 'span', 3),
22378             t.uU(512, 'LABEL_WALLET_BALANCE'),
22379             t.qZA(),
22380             t.TgZ(513, 'p') (514, 'b') (515, 'span', 3),
22381             t.uU(516, 'LABEL_ADD_MONEY'),
22382             t.qZA(),
22383             t.TgZ(517, 'h3', 3),
22384             t.uU(518, 'LABEL_ADD_MONEY'),
22385             t.qZA(),
22386             t.TgZ(519, 'p') (520, 'b') (521, 'span', 3),
22387             t.uU(522, 'LABEL_WALLET_BALANCE'),
22388             t.qZA(),
22389             t.TgZ(523, 'p') (524, 'b') (525, 'span', 3),
22390             t.uU(526, 'LABEL_ADD_MONEY'),
22391             t.qZA(),
22392             t.TgZ(527, 'h3', 3),
22393             t.uU(528, 'LABEL_ADD_MONEY'),
22394             t.qZA(),
22395             t.TgZ(529, 'p') (530, 'b') (531, 'span', 3),
22396             t.uU(532, 'LABEL_WALLET_BALANCE'),
22397             t.qZA(),
22398             t.TgZ(533, 'p') (534, 'b') (535, 'span', 3),
22399             t.uU(536, 'LABEL_ADD_MONEY'),
22400             t.qZA(),
22401             t.TgZ(537, 'h3', 3),
22402             t.uU(538, 'LABEL_ADD_MONEY'),
22403             t.qZA(),
22404             t.TgZ(539, 'p') (540, 'b') (541, 'span', 3),
22405             t.uU(542, 'LABEL_WALLET_BALANCE'),
22406             t.qZA(),
22407             t.TgZ(543, 'p') (544, 'b') (545, 'span', 3),
22408             t.uU(546, 'LABEL_ADD_MONEY'),
22409             t.qZA(),
22410             t.TgZ(547, 'h3', 3),
22411             t.uU(548, 'LABEL_ADD_MONEY'),
22412             t.qZA(),
22413             t.TgZ(549, 'p') (550, 'b') (551, 'span', 3),
22414             t.uU(552, 'LABEL_WALLET_BALANCE'),
22415             t.qZA(),
22416             t.TgZ(553, 'p') (554, 'b') (555, 'span', 3),
22417             t.uU(556, 'LABEL_ADD_MONEY'),
22418             t.qZA(),
22419             t.TgZ(557, 'h3', 3),
22420             t.uU(558, 'LABEL_ADD_MONEY'),
22421             t.qZA(),
22422             t.TgZ(559, 'p') (560, 'b') (561, 'span', 3),
22423             t.uU(562, 'LABEL_WALLET_BALANCE'),
22424             t.qZA(),
22425             t.TgZ(563, 'p') (564, 'b') (565, 'span', 3),
22426             t.uU(566, 'LABEL_ADD_MONEY'),
22427             t.qZA(),
22428             t.TgZ(567, 'h3', 3),
22429             t.uU(568, 'LABEL_ADD_MONEY'),
22430             t.qZA(),
22431             t.TgZ(569, 'p') (570, 'b') (571, 'span', 3),
22432             t.uU(572, 'LABEL_WALLET_BALANCE'),
22433             t.qZA(),
22434             t.TgZ(573, 'p') (574, 'b') (575, 'span', 3),
22435             t.uU(576, 'LABEL_ADD_MONEY'),
22436             t.qZA(),
22437             t.TgZ(577, 'h3', 3),
22438             t.uU(578, 'LABEL_ADD_MONEY'),
22439             t.qZA(),
22440             t.TgZ(579, 'p') (580, 'b') (581, 'span', 3),
22441             t.uU(582, 'LABEL_WALLET_BALANCE'),
22442             t.qZA(),
22443             t.TgZ(583, 'p') (584, 'b') (585, 'span', 3),
22444             t.uU(586, 'LABEL_ADD_MONEY'),
22445             t.qZA(),
22446             t.TgZ(587, 'h3', 3),
22447             t.uU(588, 'LABEL_ADD_MONEY'),
22448             t.qZA(),
22449             t.TgZ(589, 'p') (590, 'b') (591, 'span', 3),
22450             t.uU(592, 'LABEL_WALLET_BALANCE'),
22451             t.qZA(),
22452             t.TgZ(593, 'p') (594, 'b') (595, 'span', 3),
22453             t.uU(596, 'LABEL_ADD_MONEY'),
22454             t.qZA(),
22455             t.TgZ(597, 'h3', 3),
22456             t.uU(598, 'LABEL_ADD_MONEY'),
22457             t.qZA(),
22458             t.TgZ(599, 'p') (600, 'b') (601, 'span', 3),
22459             t.uU(602, 'LABEL_WALLET_BALANCE'),
22460             t.qZA(),
22461             t.TgZ(603, 'p') (604, 'b') (605, 'span', 3),
22462             t.uU(606, 'LABEL_ADD_MONEY'),
22463             t.qZA(),
22464             t.TgZ(607, 'h3', 3),
22465             t.uU(608, 'LABEL_ADD_MONEY'),
22466             t.qZA(),
22467             t.TgZ(609, 'p') (610, 'b') (611, 'span', 3),
22468             t.uU(612, 'LABEL_WALLET_BALANCE'),
22469             t.qZA(),
22470             t.TgZ(613, 'p') (614, 'b') (615, 'span', 3),
22471             t.uU(616, 'LABEL_ADD_MONEY'),
22472             t.qZA(),
22473             t.TgZ(617, 'h3', 3),
22474             t.uU(618, 'LABEL_ADD_MONEY'),
22475             t.qZA(),
22476             t.TgZ(619, 'p') (620, 'b') (621, 'span', 3),
22477             t.uU(622, 'LABEL_WALLET_BALANCE'),
22478             t.qZA(),
22479             t.TgZ(623, 'p') (624, 'b') (625, 'span', 3),
22480             t.uU(626, 'LABEL_ADD_MONEY'),
22481             t.qZA(),

```

10. Y ya tendríamos el ejercicio

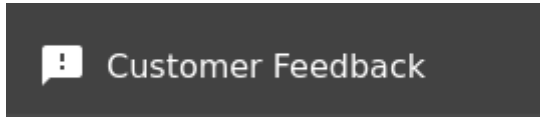


Décimo desafío

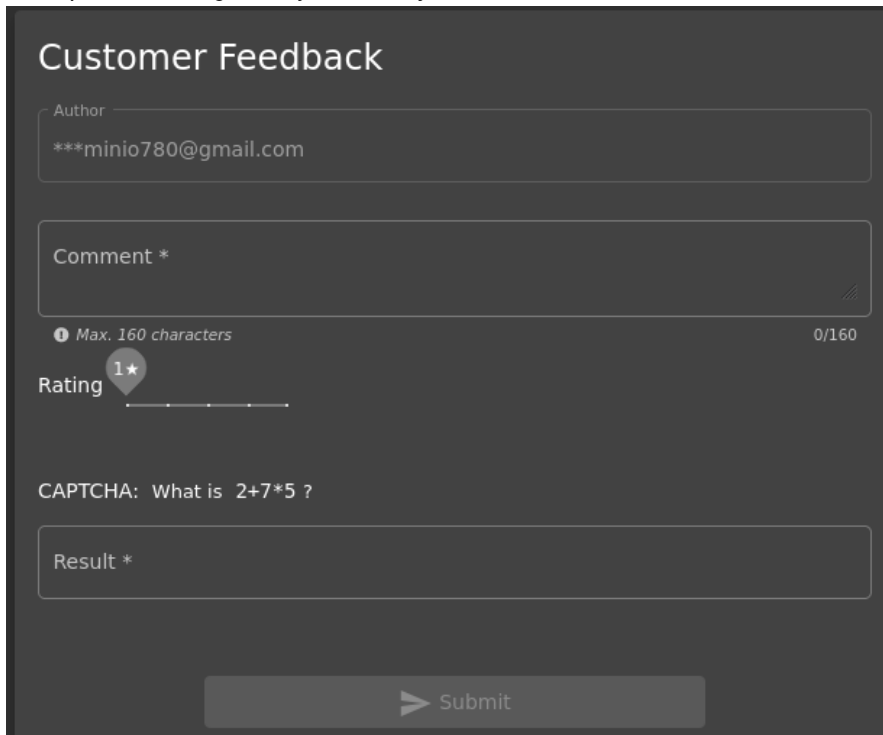
1. Zero stars
2. Abrimos las tres rayas que se encuentra arriba a la izquierda.



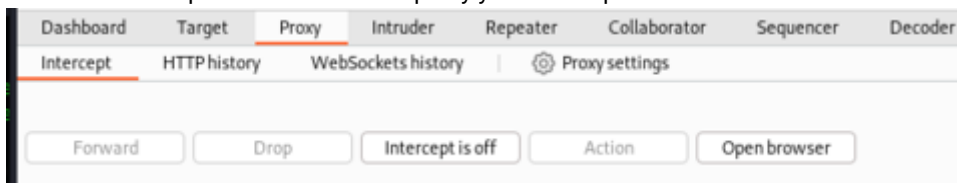
3. Abrimos lo siguiente.



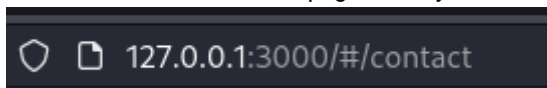
4. Nos aparecerá lo siguiente y no nos dejara seleccionar 0 estrellas.

The image shows the 'Customer Feedback' form in the application. It has a dark grey background. The form includes an 'Author' field with the text '***minio780@gmail.com', a 'Comment *' text area with a character count '0/160' and a note 'Max. 160 characters', a 'Rating' section showing '1★' out of 5 stars, a CAPTCHA question 'What is 2+7*5 ?', a 'Result *' field, and a 'Submit' button at the bottom.

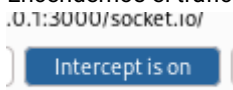
5. Encendemos BurpSuite. Nos vamos a proxy y abrimos open browser.



6. Seleccionamos la URL de la pagina web y la introducimos en el navegador de burpsuite.



7. Encendemos el tráfico.



```

1 POST /api/Feedbacks/ HTTP/1.1
2 Host: 127.0.0.1:3000
3 Content-Length: 73
4 sec-ch-ua: "Not-A?Brand";v="99", "Chromium";v="118"
5 Accept: application/json, text/plain, */*
6 Content-Type: application/json
7 sec-ch-ua-mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.5993.70 Safari/537.36
9 sec-ch-ua-platform: "Linux"
10 Origin: http://127.0.0.1:3000
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: http://127.0.0.1:3000/
15 Accept-Encoding: gzip, deflate, br
16 Accept-Language: es-ES,es;q=0.9
17 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss
18 Connection: close
19
20 {
  "captchaId":1,
  "captcha":"17",
  "comment":"Hola :) (anonymous)",
  "rating":1
}

```

8. Cambiamos el rating y lo ponemos en 0.

```

{
  "captchaId":1,
  "captcha":"17",
  "comment":"Hola :) (anonymous)",
  "rating":0
}

```

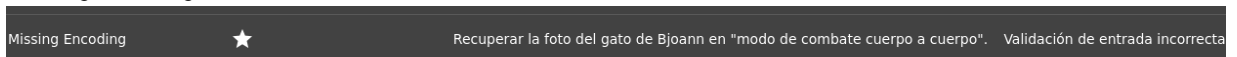
9. Y ya tendríamos listo el ejercicio

Zero Stars
★
Give a devastating zero-star feedback to the store.
Improper Input Validation

☒ solved

Undécimo desafío

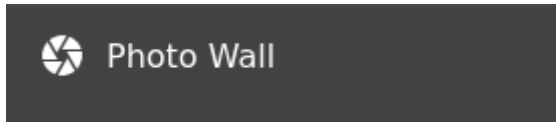
1. Missing encoding



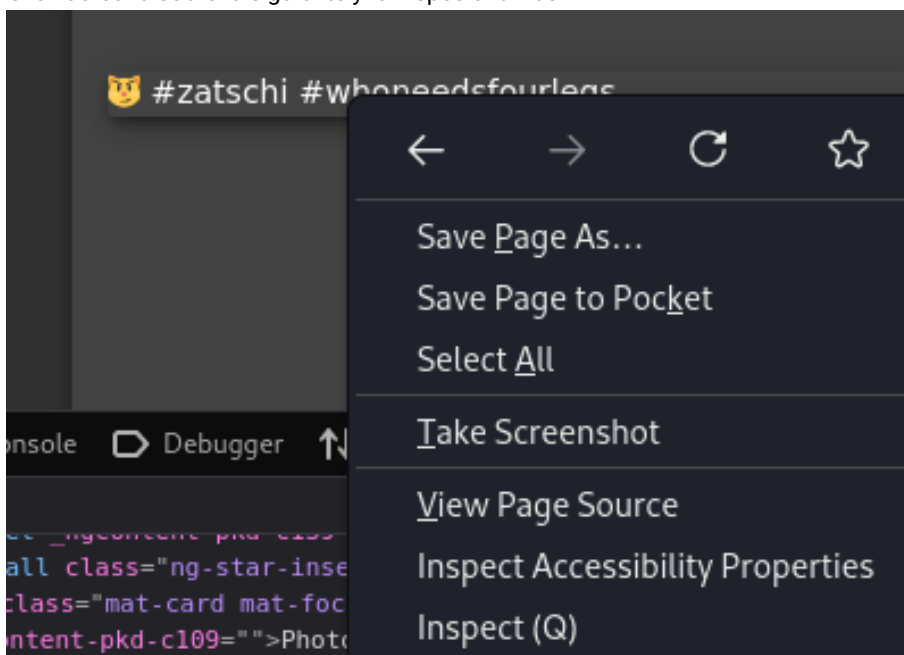
2. Abrimos las tres rayas que se encuentra arriba a la izquierda.



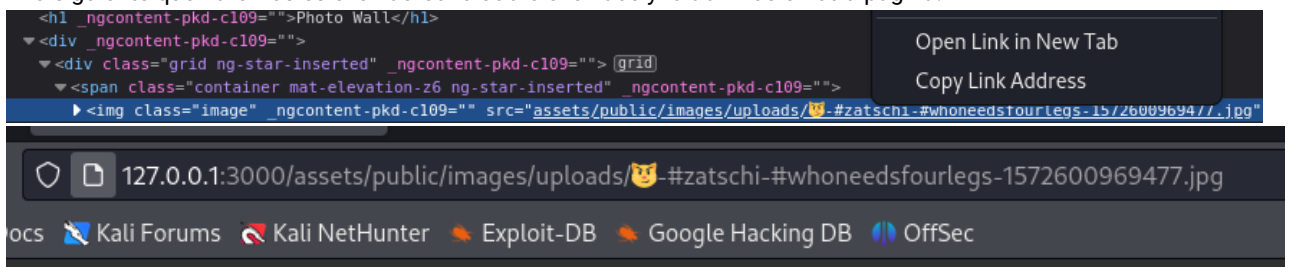
3. Abrimos photo wall



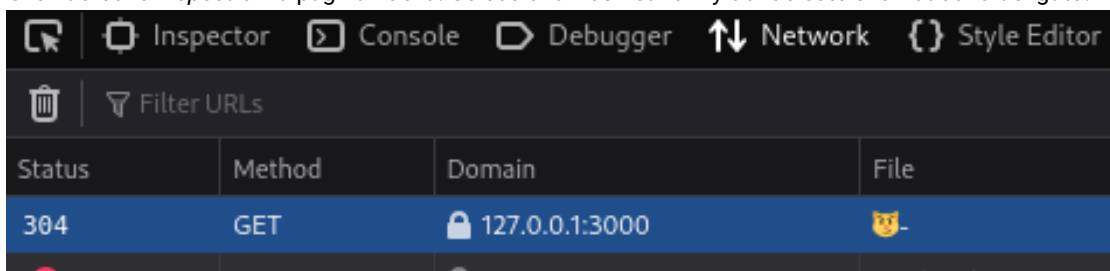
4. Click derecho sobre lo siguiente y lo inspeccionamos



5. Y lo siguiente que haremos es click derecho sobre el enlace y lo abrimos en otra página.



6. Click derecho *inspect* en la página nueva. Seleccionamos network y donde este el emoticono del gato.



7. Seleccionamos lo siguiente

```
▼ GET
Scheme: http
Host: 127.0.0.1:3000
Filename: /assets/public/images/uploads/%F0%9F%98%BC-
```

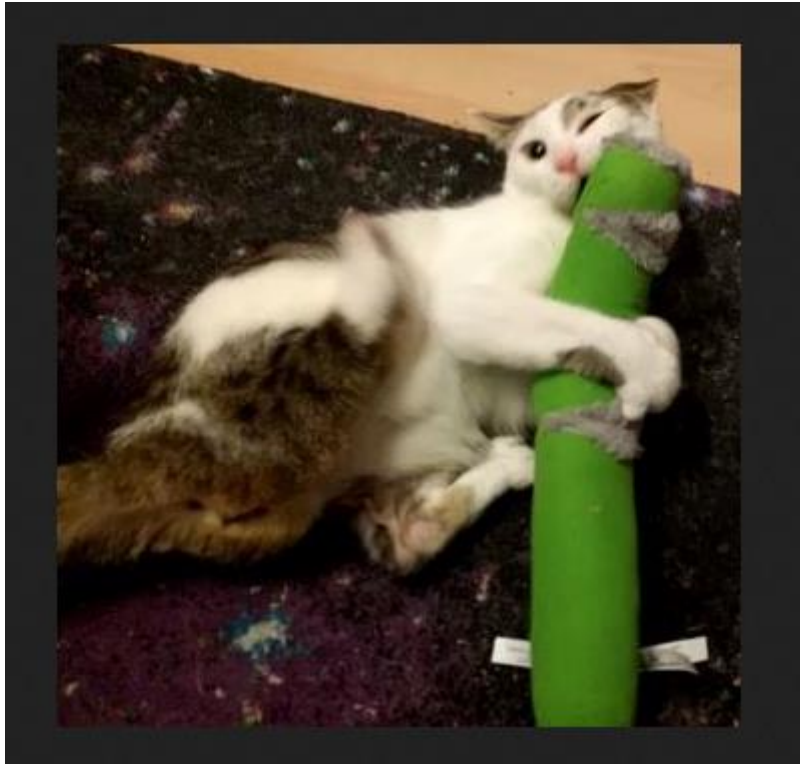
8. Abrimos una pestaña nueva y ponemos lo siguiente.

```
🔒 📄 127.0.0.1:3000/assets/public/images/uploads/😼-#zatschi-#whoneedsfourlegs-1572600969477.jpg
```

9. Cambiamos los *hashtags* por lo siguiente.

```
🔍 127.0.0.1:3000/assets/public/images/uploads/😼-%23zatschi-%23whoneedsfourlegs-1572600969477.jpg
```

10. Y obtenemos lo siguiente.



11. Y lo tendremos completado.

Missing Encoding ★ Retrieve the photo of Bjoern's cat in "melee combat-mode". Improper Input Validation Shenanigans ☒ solved

Segundo nivel

Primer desafío

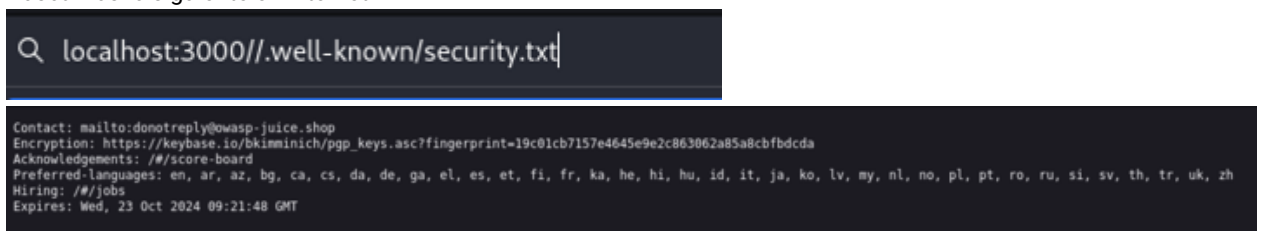
1. Nos vamos al ejercicio Security policy y nos ponemos encima de unsolved.



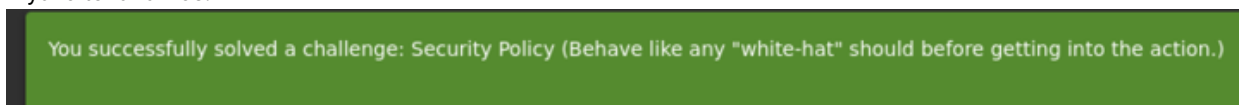
2. El archivo es un txt así que lo siguiente que haremos es irnos a la siguiente página security.txt

h (/.well-known/security.txt)

3. Buscamos lo siguiente en internet

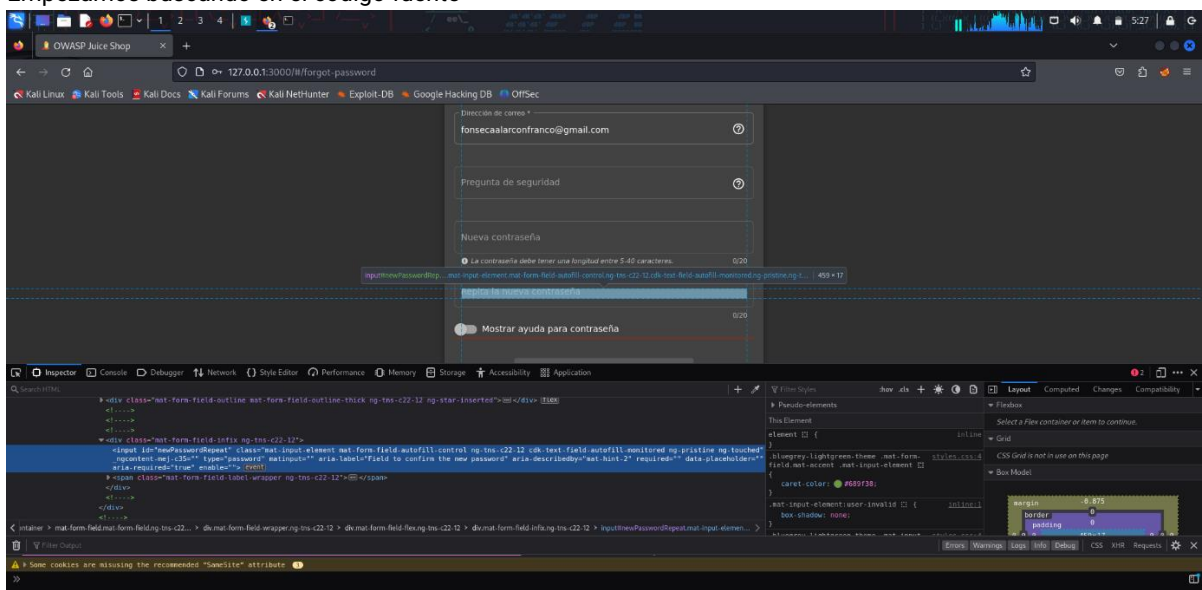


4. Y ya lo tendríamos.

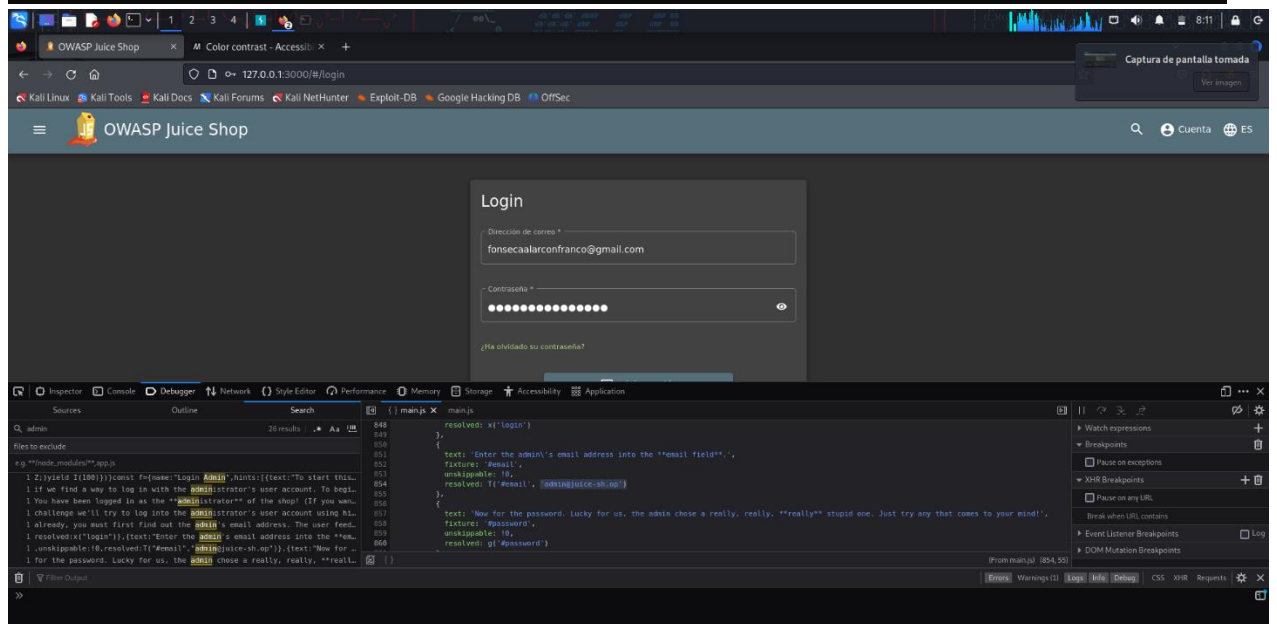
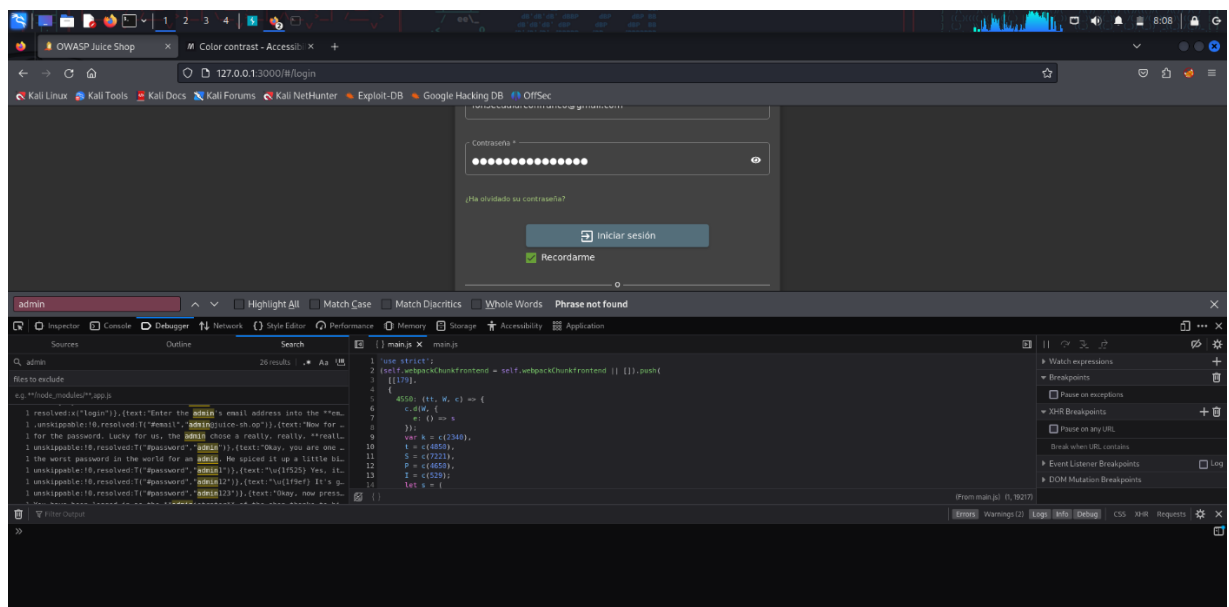


Segundo desafío

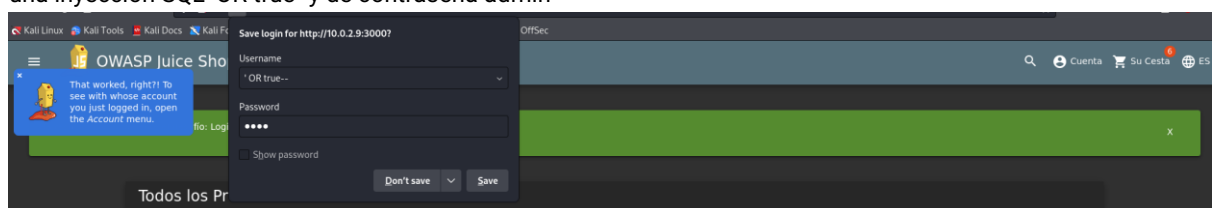
1. Login admin
2. Empezamos buscando en el código fuente



3. Realizamos una búsqueda en este mismo con la palabra *admin* y encontramos el correo del admin que es *admin@juice-sh.op*



4. Finalmente nos decantamos por utilizar las pistas las cuales nos llevan a la solución del ejercicio; pudimos entrar con una inyección SQL 'OR true--y de contraseña admin



- 5.