

# DOCUMENTACIÓN PRUEBA DE INGRESO

Plataforma Juice Shop



Neith Altair Machuca  
Bernal



## índice

---

<b>1. Herramientas</b>	<b>2</b>
1.1. BurpSuite . . . . .	2
1.2. ExifTool . . . . .	2
1.3. Dirbuster . . . . .	2
1.4. ParrotOS . . . . .	2
<b>2. Documentación</b>	<b>3</b>
2.1. Nivel 1 . . . . .	3
2.2. Nivel 2 . . . . .	8
2.3. Nivel 3 . . . . .	13



## 1. Herramientas

Las herramientas utilizadas para la resolución de la prueba **Juice Shop** fueron:

- Chrome.
- BurpSuite.
- Dirbuster.
- ExifTool.
- Parrot OS.

### 1.1. BurpSuite

es una herramienta para realizar auditorías de seguridad a aplicaciones Web. Integra diferentes componentes de pentesting y funcionalidades para realizar las pruebas y permite combinar pruebas tanto automáticas como manuales. La herramienta Burp Suite está desarrollada y mantenida por la empresa PortSwigger.

### 1.2. ExifTool

ExifTool es un programa de software gratuito y de código abierto para leer, escribir y manipular imágenes, audio, video y metadatos.

### 1.3. Dirbuster

es una aplicación Java multi hilo diseñada para obtener por fuerza bruta los nombres de directorios y archivos en servidores Web.

### 1.4. ParrotOS

Parrot OS es una distribución GNU/Linux basada en Debian con un enfoque en la seguridad informática. Está diseñado para pruebas de penetración, evaluación y análisis de vulnerabilidades, análisis forense de computadoras, navegación web anónima, y practicar criptografía.



## 2. Documentación

### 2.1. Nivel 1

Una vez se accede a la página, se consulta información para entender el funcionamiento. Como procedimiento inicial, se realiza la ejecución de un DirBuster para obtener mediante fuerza bruta nombres de directorios y archivos en servidores Web.

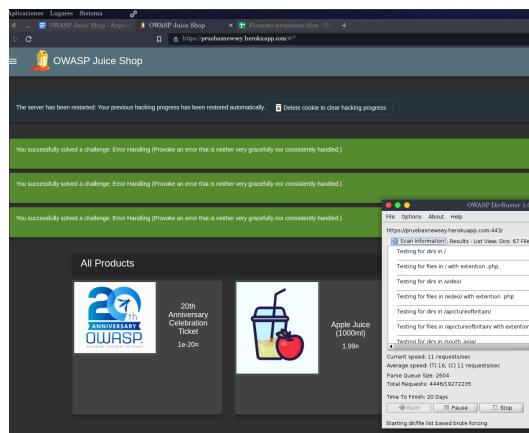


Imagen 1

Como se evidencia, mediante el uso de esta herramienta se resuelve el reto Handling Error. Al evidenciar que el proceso toma mucho tiempo se cancela y se procede a revisar el código HTML de la página, esta acción suele ser de ayuda y el paso principal en varios CTF.

The screenshot shows a browser window for the OWASP Juice Shop application. The URL in the address bar is 'https://pruebasenay.herokuapp.com/0/'. The main content area displays a large block of raw HTML code from a file named 'expresso2018.php'. The code includes various PHP statements, HTML structures, and CSS styles. The code is heavily obfuscated, making it difficult to read directly.

```
...  
time() * 1000);  
    time() * 1000);  
    $content = $this->getTemplate('error/error.html');  
    $content = str_replace($content, $this->app->view('error'), $content);  
    $content = str_replace($content, $this->localization->restore());  
    $content = str_replace($content, $this->dialog->render(),  
        str_replace($content, $this->dialog->render(),  
            str_replace($content, $this->dialog->render(),  
                str_replace($content, $this->dialog->render(),  
                    str_replace($content, $this->dialog->render(),  
                        str_replace($content, $this->dialog->render(),  
                            str_replace($content, $this->dialog->render(),  
                                str_replace($content, $this->dialog->render(),  
                                    str_replace($content, $this->dialog->render(),  
                                        str_replace($content, $this->dialog->render(),  
                                            str_replace($content, $this->dialog->render(),  
                                                str_replace($content, $this->dialog->render(),  
                                                    str_replace($content, $this->dialog->render(),  
                                                        str_replace($content, $this->dialog->render(),  
                                                            str_replace($content, $this->dialog->render(),  
                                                                str_replace($content, $this->dialog->render(),  
                                                                    str_replace($content, $this->dialog->render(),  
                                                                        str_replace($content, $this->dialog->render(),  
                                                                            str_replace($content, $this->dialog->render(),  
                                                                                str_replace($content, $this->dialog->render(),  
                                                                                    str_replace($content, $this->dialog->render(),  
                                                                                        str_replace($content, $this->dialog->render(),  
                                                                                            str_replace($content, $this->dialog->render(),  
                                                                                                str_replace($content, $this->dialog->render(),  
................................................................  
...
```

Imagen 2



Se revisan las fuentes de la página y se identifica el archivo main-es2018.js, en él se revisan los path contenidos y se obtiene el app-score-board.

```

var Logines_Sistema = {
    ...
};

var OWASP_Juice_Shop = Aspire;
var OWASP_Juice_Shop = {
    ...
};

var FormatoPropuestoXlsx = {
    ...
};

$(document).ready(function() {
    ...
});

```

The code block shows the contents of the main-es2018.js file. It includes imports for Logines\_Sistema, OWASP\_Juice\_Shop, and FormatoPropuestoXlsx. The OWASP\_Juice\_Shop object has properties like 'name' and 'version'. There are several methods defined, including 'loadDeckup', 'restoreDeckup', 'showDeckup', 'showDeckupReset', 'checkDeckup', 'getDeckup', 'checkDeckupReset', and 'checkDeckupTranslate'. The 'checkDeckup' method contains a large JSON object representing the app-score-board.

Imagen 3

Para la solución de los próximos niveles se realiza la configuración del proxy y la herramienta BurpSusite.

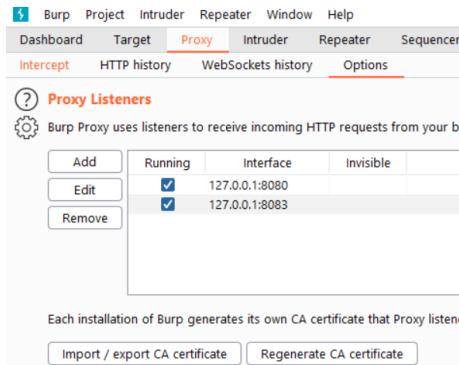


Imagen 4

La solución del nivel Zero Stars, se hace uso de la herramienta BurpSuit donde se intercepta el feedback enviado y se reemplaza el valor de rating por 0.

En Privacy Policy, solo es necesario realizar el proceso de registro y acceder a la política de privacidad de la página. En la flag Repetitive Registration se



The screenshot shows a browser's developer tools Network tab. A POST request to the URL `http://localhost:8080/api/authenticate` is selected. The request body contains a large JSON object representing user registration data, including fields like `username`, `password`, `repeatPassword`, `email`, `mobileNumber`, and `captcha`. The response status is 200 OK.

Imagen 5

identifica como pista el DRY (Dont Repit Yourself), para esta solución se realiza el registro de un nuevo usuario y se evidencia error al comparar el campo Password con Repeat Password, como se evidencia en la captura se puede enviar una contraseña diferente en el primer campo y no realiza la correcta validación.

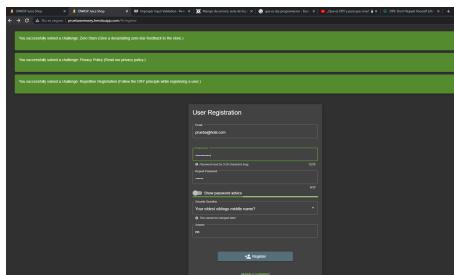


Imagen 6

En Missing code, se revisa la información de la flag, la cual dirige a photo Wall, allí se evidencia que una de las imágenes no carga de manera correcta, se revisa código HTML y se evidencia la incorrecta implementación del carácter HASH en la ruta de la imagen, la representación de esta caracter en una URL es /23, por lo que se reemplaza por los HASH y se logra ver la imagen del gato.

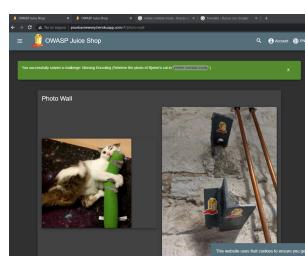


Imagen 7



Para solucionar Confidential Document se usa como orientación el Code Snippet de la flag, se accede al directorio /ftp y allí se pueden observar múltiples directorios y archivos, como acquisitions.md el cual da solución a la flag.



Imagen 8

La solución de Bully chatbot, es el reiterado envío de la palabra coupon al chat, para acceder a este chat es necesario estar logueado en la página.

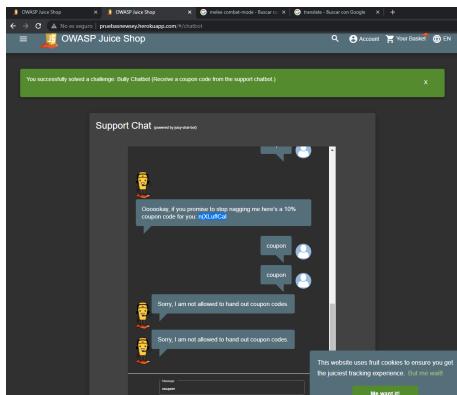


Imagen 9

DOM XSS la explotación de la vulnerabilidad XSS se realiza ejecutando el comando anexado en la flag en la barra de búsqueda, de igual forma se ejecuta el mismo comando para la flag Bonus Payload.

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

Listing 1: Script para explotación de XSS



```
<iframe width="100%" height="166" scrolling="no" frameborder="0" 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>
```

Listing 2: Script Bonus Payload

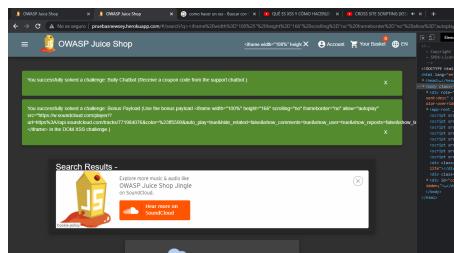


Imagen 10

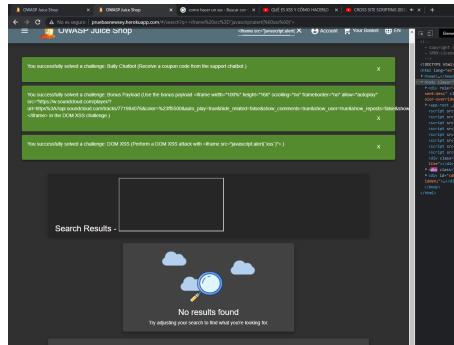


Imagen 11

En Exposed Metrics, se sigue la pista brindada por la página para encontrar el path [pruebasnewsey.herokuapp.com/metrics](http://pruebasnewsey.herokuapp.com/metrics).

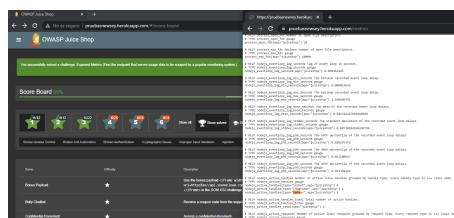


Imagen 12

Para Outdated Allowlist se inspecciona el archivo main-es2018.js buscando la palabra redirect, se encuentra un match con el path redirect?to=https://blockchain.info/address/1AbKfqvw9psQ4



el cual redirige a una billetera bitcoin.

```
POST /login HTTP/1.1
Host: pruebanewsey.herokuapp.com
Content-Length: 36
Accept: application/json, text/plain, */*
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9eyJzdGF0dXMiOiJzdWNjZWluZmliZGF0YSIiLCJpZCI6MjAxMjE1LkZjR4YtUmCMISinbWp0U1jBZQ1phI1taImRlHV4ZPvaUv1joi1ivibGFsfkxvZ1IuXAlO1T1Dw3QKcHgkqfCmVnB7PCQKQ1i1yB0iL7A3LT1T1DAw3QjGcYU1jIj1OE2EMycnfTMxHjMsInW4cc1eATTyHxEM1TE2MTo.77urDkrat3jaZ1OrhHfvkhlnseGCZ1iyICX2-M6BtELVahnfF17iFzrhNvDfPgHtCh_Wk
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.102 Safari/537.36
Origin: http://pruebanewsey.herokuapp.com
Referer: http://pruebanewsey.herokuapp.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.8
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dissmiss; eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9eyJzdGF0dXMiOiJzdWNjZWluZmliZGF0YSIiLCJpZCI6MjAxMjE1LkZjR4YtUmCMISinbWp0U1jBZQ1phI1taImRlHV4ZPvaUv1joi1ivibGFsfkxvZ1IuXAlO1T1Dw3QKcHgkqfCmVnB7PCQKQ1i1yB0iL7A3LT1T1DAw3QjGcYU1jIj1OE2EMycnfTMxHjMsInW4cc1eATTyHxEM1TE2MTo.77urDkrat3jaZ1OrhHfvkhlnseGCZ1iyICX2-M6BtELVahnfF17iFzrhNvDfPgHtCh_Wk
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 36
{"email": "admin or 1=1 -- ", "password": "admin"}
```

Imagen 13

## 2.2. Nivel 2

Se da inicio al nivel 2 resolviendo la flag Login Admin, en esta flag se hace nuevamente uso de la herramienta BurpSuite para identificar los datos enviados al momento de Login como admin.

```
1 {   email   :   admin   or 1=1 -- ,   password   :   admin   }
```

Listing 3: Inyección SQL

```
POST /login HTTP/1.1
Host: pruebanewsey.herokuapp.com
Content-Length: 36
Accept: application/json, text/plain, */*
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9eyJzdGF0dXMiOiJzdWNjZWluZmliZGF0YSIiLCJpZCI6MjAxMjE1LkZjR4YtUmCMISinbWp0U1jBZQ1phI1taImRlHV4ZPvaUv1joi1ivibGFsfkxvZ1IuXAlO1T1Dw3QKcHgkqfCmVnB7PCQKQ1i1yB0iL7A3LT1T1DAw3QjGcYU1jIj1OE2EMycnfTMxHjMsInW4cc1eATTyHxEM1TE2MTo.77urDkrat3jaZ1OrhHfvkhlnseGCZ1iyICX2-M6BtELVahnfF17iFzrhNvDfPgHtCh_Wk
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.102 Safari/537.36
Origin: http://pruebanewsey.herokuapp.com
Referer: http://pruebanewsey.herokuapp.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.8
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dissmiss; eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9eyJzdGF0dXMiOiJzdWNjZWluZmliZGF0YSIiLCJpZCI6MjAxMjE1LkZjR4YtUmCMISinbWp0U1jBZQ1phI1taImRlHV4ZPvaUv1joi1ivibGFsfkxvZ1IuXAlO1T1Dw3QKcHgkqfCmVnB7PCQKQ1i1yB0iL7A3LT1T1DAw3QjGcYU1jIj1OE2EMycnfTMxHjMsInW4cc1eATTyHxEM1TE2MTo.77urDkrat3jaZ1OrhHfvkhlnseGCZ1iyICX2-M6BtELVahnfF17iFzrhNvDfPgHtCh_Wk
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 36
{"email": "admin or 1=1 -- ", "password": "admin"}
```

Imagen 14

En el nivel Security Policy se consultan buenas practicas donde se identifica la recomendación de leer el archivo security.txt de las páginas, se insertan posibles rutas y se encuentra el archivo en ./well-known/security.txt.



9

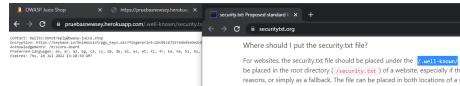


Imagen 15

Para solucionar Admin Section se acude de nuevo al documento main-es2018.js y se realiza búsqueda de la palabra admin, identificando el path /administration.

```
Page   Elapsed   |   app   polyfills.js  main-es2018.js  vendor-es2018.js  tutorial-es2018.js  main-es2018.js
x  App   pruebarenewy.herokuapp.com  110904  n.nicI, "value", 100); 110905  n.nicI, "button", 25); 110906  n.nicI, "checkbox", 25); 110907  n.nicI, "radio", 25); 110908  n.nicI, "text", 25); 110909  n.nicI, "password", 25); 110910  n.nicI, "file", 25); 110911  n.nicI, "color", 25); 110912  n.nicI, "date", 25); 110913  n.nicI, "time", 25); 110914  n.nicI, "month", 25); 110915  n.nicI, "weekend", 25); 110916  n.nicI, "year", 25); 110917  n.nicI, "button", 25); 110918  n.nicI, "checkbox", 25); 110919  n.nicI, "radio", 25); 110920  n.nicI, "text", 25); 110921  n.nicI, "password", 25); 110922  n.nicI, "file", 25); 110923  n.nicI, "color", 25); 110924  n.nicI, "date", 25); 110925  n.nicI, "time", 25); 110926  n.nicI, "month", 25); 110927  n.nicI, "weekend", 25); 110928  n.nicI, "year", 25); 110929  n.nicI, "button", 25); 110930  n.nicI, "checkbox", 25); 110931  n.nicI, "radio", 25); 110932  n.nicI, "text", 25); 110933  n.nicI, "password", 25); 110934  n.nicI, "file", 25); 110935  n.nicI, "color", 25); 110936  n.nicI, "date", 25); 110937  n.nicI, "time", 25); 110938  n.nicI, "month", 25); 110939  n.nicI, "weekend", 25); 110940  n.nicI, "year", 25); 110941  n.nicI, "button", 25); 110942  n.nicI, "checkbox", 25); 110943  n.nicI, "radio", 25); 110944  n.nicI, "text", 25); 110945  n.nicI, "password", 25); 110946  n.nicI, "file", 25); 110947  n.nicI, "color", 25); 110948  n.nicI, "date", 25); 110949  n.nicI, "time", 25); 110950  n.nicI, "month", 25); 110951  n.nicI, "weekend", 25); 110952  n.nicI, "year", 25); 110953  const ps = require('ps'); 110954  const psList = ps.list(); 110955  const psList = psList.filter(psItem => psItem.pid === 1); 110956  const psList = psList[0]; 110957  const psList = psList.addresses; 110958  const psList = psList[0]; 110959  const psList = psList.addresses; 110960  const psList = psList[0]; 110961  const psList = psList.addresses; 110962  const psList = psList[0]; 110963  const psList = psList.addresses; 110964  const psList = psList[0]; 110965  const psList = psList.addresses; 110966  const psList = psList[0]; 110967  const psList = psList.addresses; 110968  const psList = psList[0]; 110969  const psList = psList.addresses; 110970  const psList = psList[0]; 110971  const psList = psList.addresses; 110972  const psList = psList[0]; 110973  const psList = psList.addresses; 110974  const psList = psList[0]; 110975  const psList = psList.addresses; 110976  const psList = psList[0]; 110977  const psList = psList.addresses; 110978  const psList = psList[0]; 110979  const psList = psList.addresses; 110980  const psList = psList[0]; 110981  const psList = psList.addresses; 110982  const psList = psList[0]; 110983  const psList = psList.addresses; 110984  const psList = psList[0]; 110985  const psList = psList.addresses;
```

Imagen 16

Para Meta Geo Stalking, se siguen las pistas que brinda la página, al llamarse Meta, se interpreta que trata de obtener los metadatos de la imagen, se descarga y con la herramienta exiftool se obtienen los metadatos. En esta información está la latitud y longitud de donde fue tomada, se realiza la búsqueda en maps para identificar el lugar y responder la pregunta de seguridad.



```
17
a favorite-hiking-place.png
exittool favorite-hiking-place.png
[1]: exittool favorite-hiking-place.png
exittool Version Number : 12.16
File Name : favorite-hiking-place.png
File Owner : 
File Group : 
File Size : 651 KB
File Modification Date/Time : 2021-07-27 04:01:42+01:00
File Access Date/Time : 2021-07-27 04:01:43+01:00
File Inode Change Date/Time : 2021-07-27 04:01:55+01:00
File Permissions : rwxr--r--
File Type : JPEG
File Type Extension : png
FILE Type : Image/png
Image Width : 3779
Image Height : 3779
Bit Depth : 8
Color Type : RGB
Compression : deflate/inflate
Filter : Adaptive
Interlace : Noninterlaced
Pixel Order : Little Endian (Intel, II)
Resolution Unit : Inches
YCbCr Positioning : Centered
GPS CD/Cr Positioning : 
GPS Map Datum : WGS-84
GPS Latitude Ref : North
GPS Longitude Ref : West
GPS Map Datum : WGS-84
Thumbnail Offset : 233
Thumbnail Length : 4531
sRGB Rendering : Perceptual
Image : 
Pixels Per Unit X : 3779
Pixels Per Unit Y : 3779
Image Units : pixels
Image Size : 471x627
Megapixels : 0.295
Image Color Space : (Binary data 4531 bytes, use -b option to extract)
GPS Latitude : 36 deg 57' 31.38" N
GPS Longitude : 84 deg 20' 53.58" W
GPS Position : 36 deg 57' 31.38" N, 84 deg 20' 53.58" W
```

Imagen 17

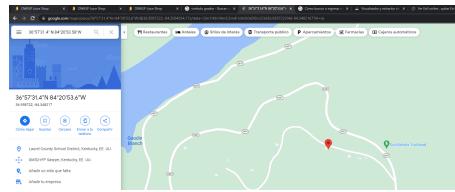


Imagen 18

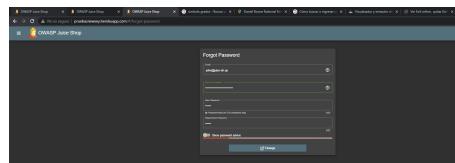


Imagen 19

En Visual Geo stalking se realiza el mismo proceso al anterior, sin identificar ubicación, al ver los pixeles de la imagen se realiza Zoom en busca de pistas y se evidencia un aviso en la ventana ITsec, el cual permite dar respuesta a la pregunta de seguridad de Emma.



11

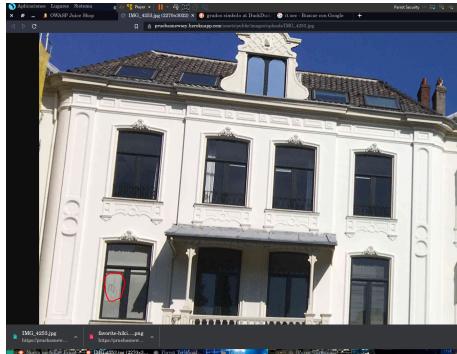


Imagen 20

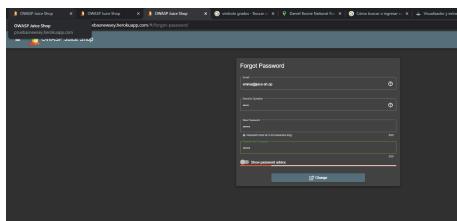


Imagen 21

Para View Basket, se realiza la inspección de la página web para lograr ver la canasta de otro usuario, se revisan los storage identificando que en el sessionstorage al modificar el Bid se puede acceder a la canasta de otro usuario.

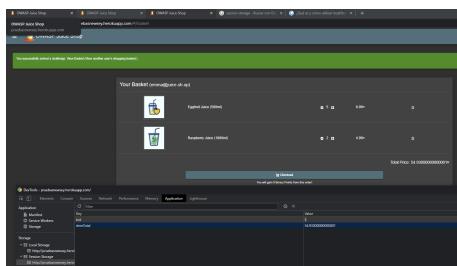


Imagen 22

La solucion de Login MC SafeSearch no se obtiene a traves de la inyeccion SQL, realizando busqueda relacionada a MC SafeSearch se identifica una cancion en youtube relacionada a la página, en esta cancion se habla sobre las contraseñas, al revisar la letra de la misma se obtiene la respuesta. Mr. N00dles, con BurpSuit



se puede realizar un ataque de fuerza bruta con las multiples variaciones que puede tener escribir la palabra.

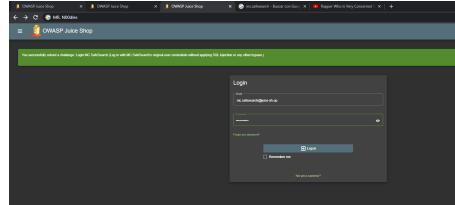


Imagen 23

Password strength por el nombre y las normas de no usar inyeccion SQL se deduce que se trata de un ataque de fuerza bruta al usuario admin. Se hace uso de la herramienta Burp Suit para realizar un intruder, de esta forma se agrega una lista de palabras y se ejecuta el ataque.

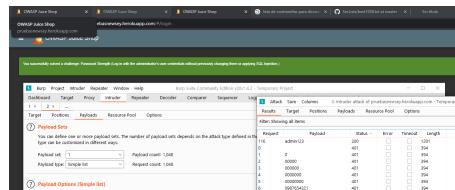


Imagen 24

En five Star Feedback, con los accesos de admin se pueden eliminar los feedback 5 estrellas.

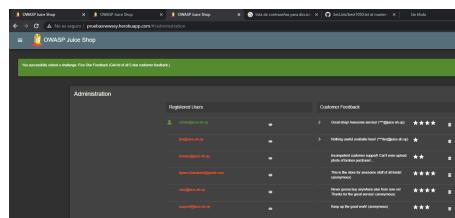


Imagen 25

Weird Crypto trata de informar una librería o algoritmo que no debería ser usado en la aplicación, en este caso al revisar las librerías se identifica la implementación del hash md5, algoritmo débil e inseguro para su uso.

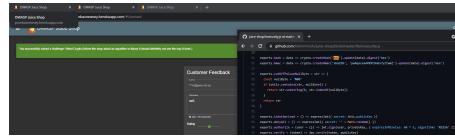


Imagen 26

### 2.3. Nivel 3

En admin registration se evidencia la categoría improper validation vulnerabilidad asociada a la duplicidad en los formularios. Se realiza registro de un nuevo usuario y se interceptan los datos JSON enviados y se agrega el valor “role”:admin, se evidencia una correcta respuesta del servidor y la solución de esta flag.

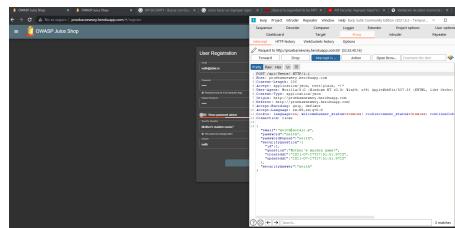


Imagen 27

PaybackTime se resuelve de una manera similar, se intercepta el tráfico generado al enviar un nuevo artículo a la canasta, en este caso se cambia el valor en la cantidad a negativo, de forma que al pagar la aplicación quedaría debiendo al usuario.

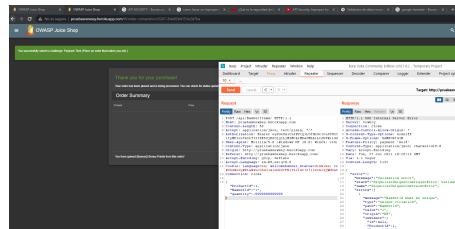


Imagen 28

En DeluxeFraud se realiza inspeccionando el código HTML, se habilita el botón de la billetera virtual y se intercepta el tráfico para cambiar los valores enviados.



The screenshot shows the OWASP ZAP interface with two panes. The left pane, titled 'Request', displays a POST request to '/rest/review-ownership' with various headers and a payload containing a SQL injection query. The right pane, titled 'Response', shows the server's response with status code 200 OK, content type application/json, and a JSON object indicating a successful update.

Imagen 29

Para acceder a los usuarios de Jim y Bender, se realiza una inyección SQL sencilla, acompañando los email con ‘– para anular el resto de la consulta realizada.

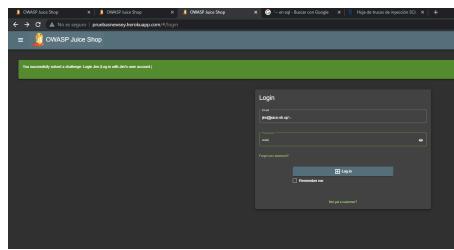


Imagen 30

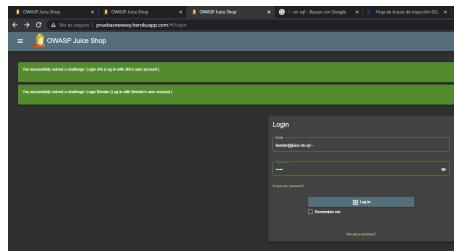


Imagen 31

Para establecer una nueva contraseña del usuario Jim, se inicia sesión en su perfil y se busca información en la cuenta que de pistas de quién es y cuál era el nombre de su hermano mayor (Samuel).



The screenshot shows the Burp Suite interface with the "Response" tab selected. The response body contains JSON data:

```
HTTP/1.1 201 Created
Content-Type: application/json; charset=UTF-8
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS
Access-Control-Max-Age: 3600
X-Frame-Options: SAMEORIGIN
P3P: CP="NOI ADM DEV PSAi COMa DSPi CURa TAIa"
X-RateLimit-Limit: 100
X-RateLimit-Remaining: 99
X-RateLimit-Reset: 1477949400
X-XSS-Protection: 1; mode=block
Content-Length: 249
Date: Mon, 19 Jun 2017 17:38:49 GMT
Vary: Accept-Encoding
Content-Type: application/json; charset=UTF-8
{
    "success": true,
    "msg": "Your password has been successfully changed.",
    "new_password": "pruebasnewyorkjuicesshop"
}
```

Imagen 32

Para CAPTCHA bypass se genera un ataque de fuerza bruta con Burpsuit para poder realizar el envío de 10 feedbacks en 10 segundos.

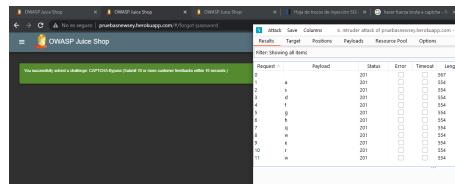


Imagen 33

Para encontrar la mascota favorita de Bjoern, se realiza busqueda en sus redes sociales, identificando en instagram el nombre de su gata. Se agrega este nombre en la respuesta y se logra cambiar la contraseña.

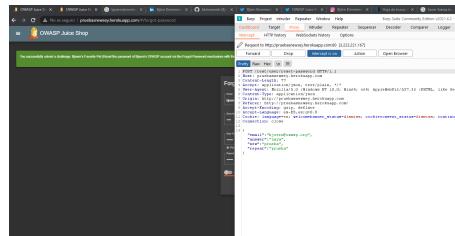


Imagen 34

Forged Feedback es de solución sencilla, se inicia sesión como un nuevo usuario y se genera un nuevo Feedback.



16

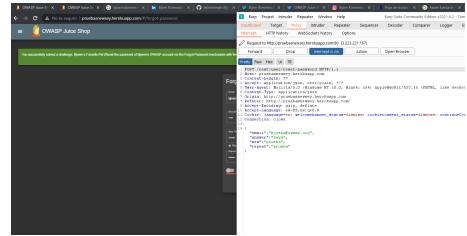


Imagen 35

En el ejercicio Login Amy, es necesario analizar muy bien la información contenida en la flag y los enlaces relacionados a ella, en este caso se encuentra un script en python donde se puede realizar el ataque de fuerza bruta de una manera rápida y efectiva. Solo fue necesario instalar los módulos importados y agregar la URL de la aplicación en la que se está trabajando.

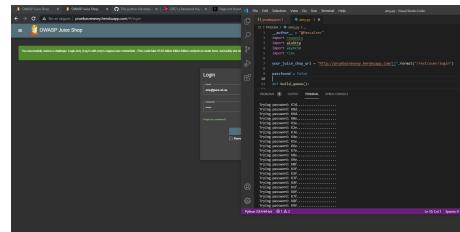


Imagen 36

Upload Size requiere de interceptar el archivo cargado, para poder cambiar los datos del mismo y así lograr cargar un archivo mayor a 100kb.

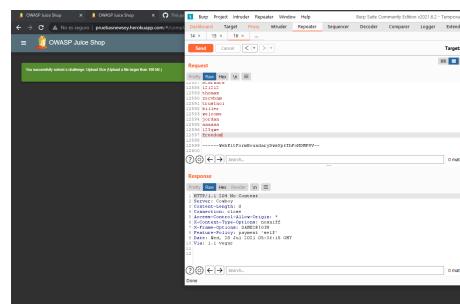


Imagen 37

Upload type es similar al anterior, pero en este caso se cambia la extensión del archivo.



17

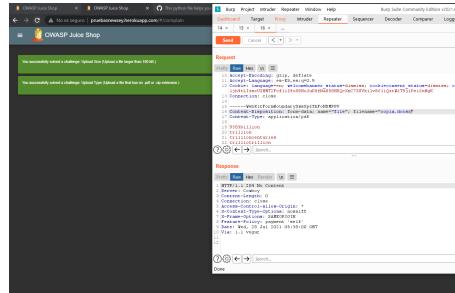


Imagen 38

La solución de Manipule Basket también se puede obtener interceptando el tráfico generado al agregar un artículo a la canasta, luego de varios intentos al agregar un nuevo “BasketId” y realizar la petición se supera el nivel.

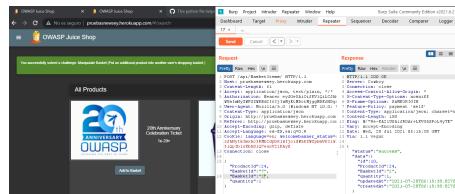


Imagen 39

Para superar Privacy Policy, se inspecciona el código HTML de la página identificando la clase “Hot” en determinados puntos, estos puntos se utilizan como PATH y se accede a una página.

```
"OWASP Juice Shop ("us", "we", or "our") operates the "
<span _ngcontent-c214 class="hot">http://pruebasnewsey.herokuapp.com</span> = $0
" website (the "Service")."
```

Imagen 40

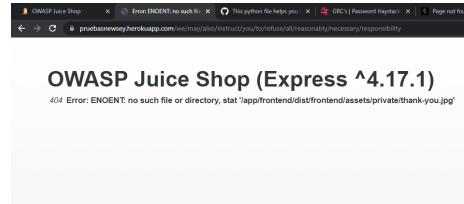


Imagen 41

Forged Review requiere de interceptar el tráfico al hacer una reseña de un producto, se cambia el valor de “author” por un correo diferente al utilizado para el envío.

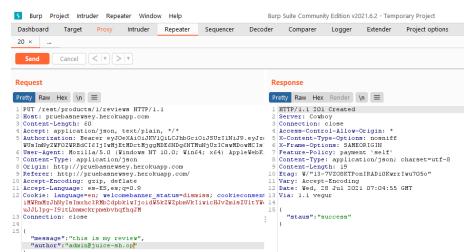


Imagen 42