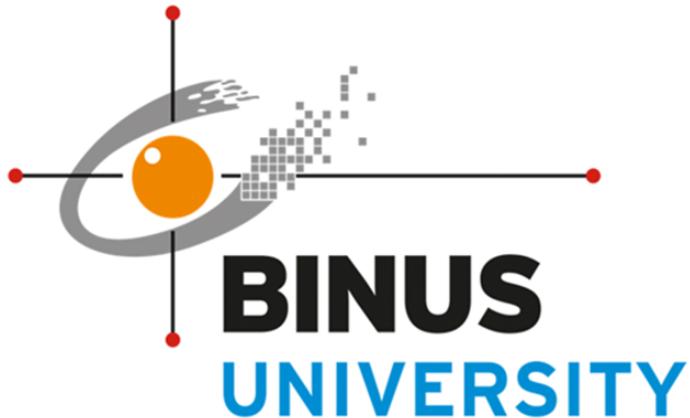


REPORT

SECURE PROGRAMMING



JAJAN SNACK WEBSITE APPLICATION

Disusun Oleh:

Kelompok 1

Arjuna Accha Dipa 2301865735

Eric Kurniawan 2301860072

Wilson Nugrah 2301858976

Delvin Nicholas 2301852581

Christian 2301881682

UNIVERSITAS BINA NUSANTARA

JAKARTA

2022

DAFTAR ISI

DAFTAR ISI	1
BAB 1. Pendahuluan	2
BAB 2. Teknik Secure Programming Laravel	8
BAB 3. Penetration Testing dengan TOP 10 OWASP	10

BAB 1

Pendahuluan

Link Source Code Github JajanSnack : <https://github.com/vantasm/JajanSnack>

JajanSnack merupakan sebuah aplikasi berbasis website yang menyediakan layanan berupa marketplace yang menjual berbagai jenis snack yang dapat dibeli dengan mudah oleh customer. Snack yang biasa dijual pada JajanSnack merupakan snack yang jarang ditemukan di supermarket pada umumnya. Selain jarang ditemukan, snack-snack tersebut merupakan snack import yang *limited* maupun *special edition*. Selain snack-snack import yang ada, JajanSnack juga menyediakan snack-snack buatan asli Indonesia yang akan tersedia di marketplace kami. Dengan menyediakan berbagai snack tersebut, maka akan dapat membantu meningkatkan UMKM yang menjual berbagai snack-snack khas Indonesia.

Contoh dari snack-snack import yang dijual di JajanSnack :

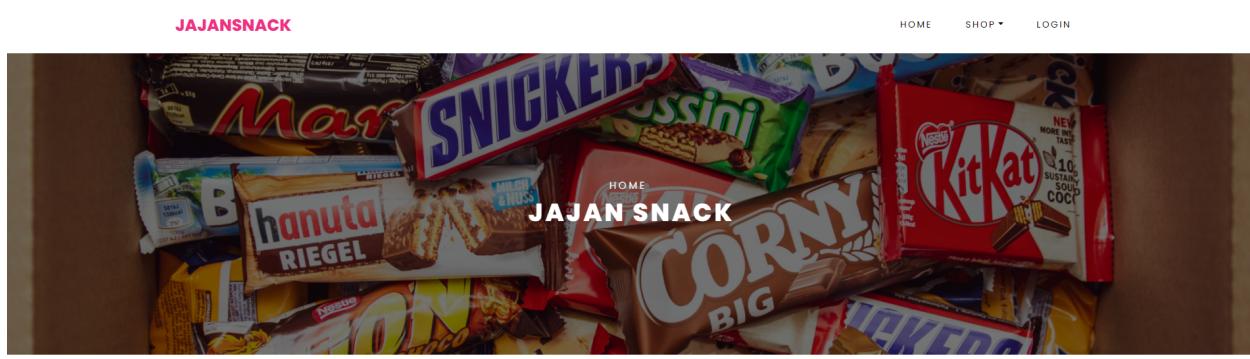


Contoh dari snack-snack khas Indonesia yang dijual di JajanSnack :



Alasan kami ingin mengembangkan JajanSnack menjadi salah satu marketplace snack terbesar di Indonesia adalah dapat dilihat bahwa Snack merupakan makanan pendamping yang sering sekali dikonsumsi oleh masyarakat Indonesia. Namun, tidak semua supermarket yang ada di Indonesia yang menyediakan snack-snack Import yang biasanya sulit didapatkan. Hal itu kami jadikan sebagai sebuah peluang untuk mengembangkan JajanSnack yang akan dapat membantu orang-orang yang ingin membeli snack import maupun snack khas Indonesia dengan mudah dan cepat.

Contoh tampilan Home website JajanSnack :



The screenshot shows the homepage of JajanSnack. At the top, there is a navigation bar with links for HOME, SHOP (with a dropdown arrow), and LOGIN. Below the navigation bar is a large image of various snack packages, including Mars, Snickers, Riegel, KitKat, and Corny. Overlaid on this image is the text "JAJAN SNACK". Below the image, the section title "Best Products" is displayed in bold black font. A subtitle "Selected randomly based on the rating of the products" follows. At the bottom of the screenshot, there are four small horizontal banners, each showing a 20% discount offer on different snack products.

Best Products

Selected randomly based on the rating of the products

20% 

20% 

20% 

20% 

Gambar di atas merupakan contoh tampilan halaman utama pada website JajanSnack yang berisikan berbagai jenis snack dengan tampilan snack dan harga dari snack tersebut. Pada bagian halaman utama juga terdapat menu lainnya yakni shop yang berisikan list-list dari snack secara keseluruhan dan bisa dibrowse oleh customer. Selain itu juga terdapat menu Login bagi calon customer untuk memudahkan proses transaksi dengan melakukan login akun pada JajanSnack.

Contoh tampilan login website JajanSnack :

The screenshot shows a login form titled "Login". It has two input fields: "E-Mail Address" and "Password". Below the password field is a checkbox labeled "Remember Me". At the bottom are two buttons: a pink "Login" button and a blue "Forgot Your Password?" link. Below the buttons is a link "Not registered yet? Register Now". The top navigation bar includes links for "HOME", "SHOP ▾", and "LOGIN".

Berikut tampilan login pada website JajanSnack bagian Login yang digunakan pengguna JajanSnack untuk masuk dengan akun yang telah dibuat pada page register. Pada login page, pengguna akan diminta untuk memasukkan email address dan password agar bisa login ke website JajanSnack. Pada login page juga tersedia fitur Forgot password yang dapat digunakan oleh pengguna JajanSnack untuk melakukan reset password apabila pengguna ingin mengganti password dari akun tersebut. Serta jika pengguna belum pernah membuat akun, maka terdapat fitur Register now yang akan mengarahkan pengguna ke register page untuk membuat akun baru.

Contoh tampilan register website JajanSnack :

The screenshot shows a registration form titled "Register". It has five input fields: "Name", "E-Mail Address", "Address", "Password", and "Confirm Password". At the bottom is a pink "Register" button. The top navigation bar includes links for "HOME", "SHOP ▾", and "LOGIN".

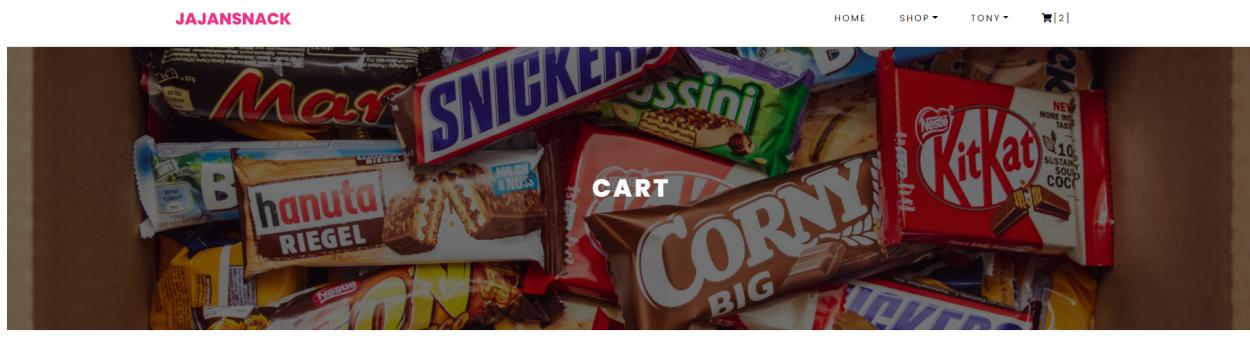
Tampilan register page akan berisikan data-data yang harus diisi oleh calon pengguna seperti nama, e-mail address, address, password dan confirm password. Setelah itu calon pengguna hanya perlu menekan register untuk membuat akun baru pada website JajanSnack.

Contoh tampilan shop pada website JajanSnack :

The screenshot shows the homepage of JajanSnack. At the top, there is a large collage of various snack products. Below the collage are four circular icons representing different service features: "FREE SHIPPING" (truck icon), "BRAND NEW" (oven icon), "ORIGINAL" (award icon), and "SUPPORT" (person icon). Under each icon is a brief description: "ON ORDER OVER RP 50.000", "FRESH FROM THE OVEN", "QUALITY PRODUCTS", and "100% REPLIED CHAT". The main navigation bar includes links for "HOME", "SHOP ▾", and "LOGIN". Below the navigation, there is a secondary navigation bar with categories: "All", "Biscuits", "Chips", "Chocolate", and "Candy". The main content area displays a grid of snack products. The first row contains four items: "BOURBON DEMON SLAYER" (20% off, Rp 20.000 - Rp 16.000), "CHEETOS BAGEL & CHEESE" (20% off, Rp 30.000 - Rp 24.000), "CHITATO KERAK TELOR" (20% off, Rp 15.000 - Rp 12.000), and "DORITOS WASABI" (30% off, Rp 20.000 - Rp 14.000). The second row contains four items: "IRVINS TRIO" (20% off), "KitKat Premium" (20% off), and two bags of Lay's chips (20% off).

Gambar di atas merupakan tampilan dari salah satu menu pada Website JajanSnack yaitu Shop yang menyediakan list berupa snack apa saja yang bisa dibeli oleh pengguna. List berikut menyediakan nama-nama dari snack, gambar dari snack tersebut, serta harga dan potongan harga yang telah diberikan pada seluruh snack berikut.

Contoh tampilan Cart pada website JajanSnack :



Product name	Price	Quantity	Total
Bourbon Demon Slayer			
The "Petit" series, which was launched in 1996 from three types. To commemorate the 25th anniversary, a limited-time package product featuring the character			
		<input type="text" value="1"/>	

Product name	Price	Quantity	Total
Bourbon Demon Slayer			
The "Petit" series, which was launched in 1996 from three types. To commemorate the 25th anniversary, a limited-time package product featuring the character of the anime "Demon Slayer". The lineup includes "pillars" such as Sumijiro, Zeni, Inosuke, Purgatory Anjuro, Kocho Shinobu, and Yoshiyuki Tomioka, and demons such as Inouza.			
	<input type="text" value="Rp 16.000"/>	<input type="text" value="1"/>	<input type="text" value="Rp 20.000"/>
Cheetos Bagel & Cheese			
Sweet, and salty flavor packed into crunchy, cheesy snacks. CHEETOS® Bagel & Cheese Flavored Snacks are full of flavor and made with real cheese.			
	<input type="text" value="Rp 24.000"/>	<input type="text" value="1"/>	<input type="text" value="Rp 30.000"/>

The screenshot shows the JAJANSNACK website's cart page. At the top, there are navigation links for HOME, SHOP, and TONY, along with a shopping cart icon showing 2 items. The main content area is divided into three sections: a coupon code input field, a shipping and tax estimation form, and a cart summary table.

Coupon Code
Enter your coupon code if you have one
Coupon code:
Apply Coupon

Estimate shipping and tax
Enter your destination to get a shipping estimate
Country:
State/Province:
Zip/Postal Code:
Estimate

Cart Totals

Subtotal	Rp 50.000
Delivery	Rp 0
Discount	Rp 0
TOTAL	Rp 50.000

Proceed to Checkout

Ketiga gambar di atas merupakan tampilan menu cart pada website JajanSnack dimana pengguna dapat melihat daftar barang apa saja yang sudah dimasukkan ke cart untuk selanjutnya dilanjutkan ke dalam proses transaksi dan checkout snack seperti gambar diatas.

Pada bagian *Check out cart* , pengguna dapat memasukkan coupon code jika memiliki, Lokasi pengiriman serta total dari biaya yang harus dikeluarkan untuk transaksi tersebut.

BAB 2

Teknik Secure Programming Laravel

1. Penggunaan hashing pada Password

Hashing pada password sangat penting yang dimana password merupakan data penting sehingga diperlukan proteksi lebih dengan menggunakan hash.

```
protected function create(array $data)
{
    return User::create([
        'name' => $data['name'],
        'email' => $data['email'],
        'address' => $data['address'],
        'password' => Hash::make($data['password']),
    ]);
}
```

2. Penggunaan Validation pada Data

Function validation berguna untuk melakukan validasi data-data yang perlu dimasukkan oleh user, seperti name, email, address dan password yang harus “string” sehingga user tidak dapat memasukkan type lain seperti int atau special characters.

```
protected function validator(array $data)
{
    return Validator::make($data, [
        'name' => ['required', 'string', 'max:255'],
        'email' => ['required', 'string', 'email', 'max:255', 'unique:users'],
        'address' => ['required', 'string', 'max:255'],
        'password' => ['required', 'string', 'min:8', 'confirmed'],
    ]);
}
```

3. Penggunaan CSRF Token

CSRF Token merupakan sebuah random string yang di generate setiap kali halaman form muncul yang biasanya disisipkan sebagai headers, atau form data, atau query string. Dengan adanya CSRF Token, maka akan dapat mencegah serangan CSRF.

CSRF merupakan salah satu teknik hacking yang dilakukan dengan cara mengeksekusi perintah yang seharusnya tidak diizinkan, tetapi output yang dihasilkan sesuai dengan yang seharusnya.

```
        '',
        $.ajaxSetup({
            headers: {
                'X-CSRF-TOKEN': $('meta[name="csrf-token"]').attr('content')
            }
        });
    
```

4. Penggunaan Form untuk menghindari manipulasi URL User ID

Penggunaan Form dalam situasi ini bertujuan untuk menghindari GET Request yang dimana jika digunakan, maka user id akan dijadikan sebagai parameter dan bisa diganti. Dengan menggunakan form, kita dapat menggunakan POST Method sehingga tidak dapat memanipulasi URL user id.

```
<a href="/wishlist/{{Auth::user()->id}}/{{$product->id}}" class="heart d-flex justify-content-center align-items-center">
    <span><i class="fas fa-heart"></i></span>
</a>
<form name="add-blog-post-form" id="add-blog-post-form" method="post" action="{{url('wishlist')}}">
    @csrf
    <input type="hidden" value="{{{$product->id}}}" name="product_id" id="product_id" readonly>
    <input type="hidden" value="{{Auth::user()->id}}" name="user_id" id="user_id" readonly>
    <button type="submit" class="btn btn-primary">
        <span><i class="fas fa-heart"></i></span>
    </button>
</form>
```

5. Menggunakan unique string untuk menghindari brute-force directory url

Brute-force directory url pada umumnya terjadi dengan menggunakan dirbuster ataupun gobuster untuk mendapatkan directory yang terdapat pada website dapat dicegah dengan menggunakan unique string. Penyerangan pada umumnya dilakukan dengan menggunakan wordlist umum yang telah tersedia, sehingga solusi untuk mengatasinya adalah dengan membuat directory baru dengan string yang sulit untuk didapatkan wordlist pada umumnya.

```
@if (Auth::user()->isadmin)
    <a class="dropdown-item" href="/M3ADM1N">Admin</a>
@endif
```

6. Escape string untuk mengatasi XSS

Pada umumnya XSS dapat dilakukan pada elemen html yang tidak di sanitasi. Selain itu, XSS akan menjalankan script ketika user masuk ke halaman yang memiliki script sehingga akan langsung tereksekusi dari *client side*. Salah satu tindakan yang kami lakukan untuk mencegah hal tersebut adalah menggunakan double bracket untuk melakukan *escape string* yang bertujuan untuk mencegah terjadinya eksekusi script. Alasannya adalah ketika hacker berhasil mengganti nama produk kita dengan sebuah script, otomatis semua user yang menggunakan website tersebut dan mengakses halaman tersebut akan terkena *script injection* yang dilakukan oleh hacker tersebut.

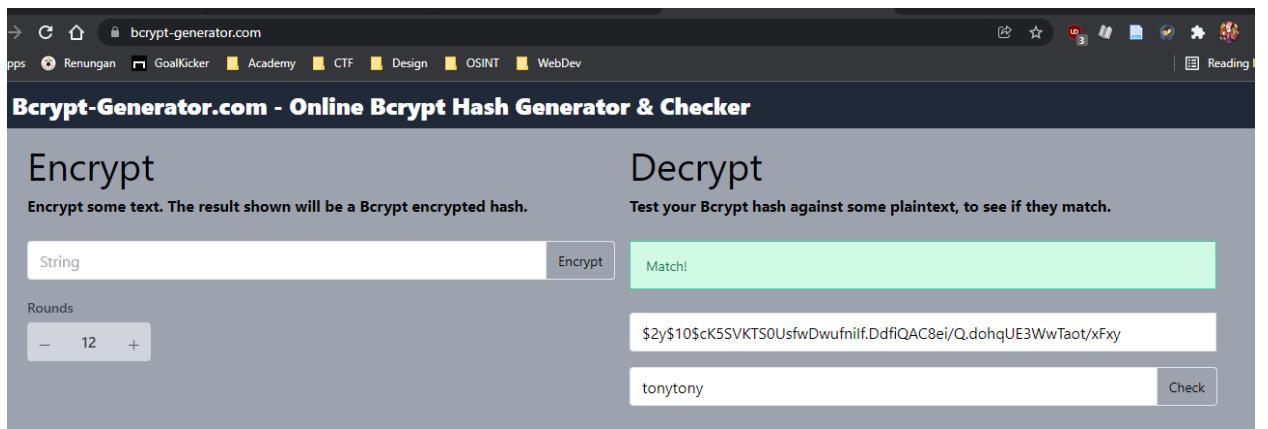
```
<h3>{{ $product->name }}</h3>
```

Bab 3

Penetration Testing dengan TOP 10 OWASP

1. Weak Cryptographic

Enkripsi password menggunakan enkripsi BCrypt ketika menggunakan framework login bawaan dari Laravel, dan dapat nilai hashingnya dapat dengan mudah di-decrypt.



2. SQL Injection pada halaman login

Serangan SQL Injection pada halaman login menggunakan wordlist dari repository ‘payloadbox/sql-injection-payload-list’ tidak berhasil menembus halaman login. Semua respon yang didapat mengarahkan kembali ke halaman login, dan tidak menuju ke halaman home sebagaimana jika berhasil login.

Attack Save Columns
Results Positions Payloads Resource Pool Options

Filter: Showing all items

Request ^	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			302	<input type="checkbox"/>	<input type="checkbox"/>	1528	
1	";"	";"	302	<input type="checkbox"/>	<input type="checkbox"/>	1528	
2	" "	" "	302	<input type="checkbox"/>	<input type="checkbox"/>	1528	
3	"&"	"&"	302	<input type="checkbox"/>	<input type="checkbox"/>	1528	
4	"\\"	"\\"	302	<input type="checkbox"/>	<input type="checkbox"/>	1528	
5	"%"	"%"	302	<input type="checkbox"/>	<input type="checkbox"/>	1528	
6	" or ";"	" or ";"	302	<input type="checkbox"/>	<input type="checkbox"/>	1528	...

Request Response

Prev Raw Hex Render ⌂ ↻ ⌂ ⌂

```

Content-Type: text/html; charset=UTF-8
Set-Cookie: JSESSIONID=10000000000000000000000000000000; path=/; sameSite=lax
eyJpdiI6IiwhocI1K2Zqc1lURkE4OG2uakJUNEEEPStisInhbHVL1jola0hnVVpCNU7YbDfONrWnRdJ7TRIVStLTyTQzhtS2N9WlovcGsyVEV3bWVoVOZCMjB0aS9FZ3FQWHotCOURuL1ZGZ2l0VE1WRV1L
JPSORKSGtaea3Bndj2U1V1cMIVU2XVXNRP10MGdwOXZGymh3Yzil2CJY1Wt0i1yZDZgdMDAxZDmByjz12jNMtCzTMxZDYYymMC2TjJ1TJnMsUz3MgszNTy0gVmMOTYwNTMCODe4Oti1iwidg
FnijoIn0V3d; expires=Tue, 18-Jan-2022 08:16:33 GMT; Max-Age=7200; path=/; httpOnly; sameSite=lax
<!DOCTYPE html>
<html>
  <head>
    <meta charset="UTF-8" />
    <meta http-equiv="refresh" content="0;url='http://127.0.0.1:8000/login'" />
  </head>
  <body>
    Redirecting to <a href="http://127.0.0.1:8000/login">
      http://127.0.0.1:8000/login
    </a>
  </body>
</html>
```

0 matches

3. IDOR pada cart page

Pada cart page, website akan mengirimkan parameter user id kepada CartController untuk menampilkan page cart sesuai dengan user yang login atau yang melakukan request pada saat itu. Untuk melihat hal ini, diperlukan 2 akun, yang pertama ada akun bernama “Tony” yang tidak memiliki item di cartnya dengan user id 1 pada database.

The screenshot shows the JAJANSNACK website with a navigation bar at the top. The cart icon indicates 0 items. Below the navigation, there is a pink header bar with columns for Product name, Price, Quantity, and Total. A large circular button with an upward arrow is centered on the page. At the bottom, there are links for JajanSnack, Menu, Help, and Have a Questions?.

Kemudian ada akun bernama “Mantap” dengan cart yang berisi 2 item dengan user id 2 pada database.

The screenshot shows the JAJANSNACK website with a navigation bar at the top. The cart icon indicates 2 items. Below the navigation, there is a pink header bar with columns for Product name, Price, Quantity, and Total. Two items are listed: Cheetos Bagel & Cheese and Lays Grilled Cheese and Tomato Soup. Each item has a delete icon (X) and a quantity input field set to 1. The total price for each item is displayed as Rp 24.000 and Rp 20.000 respectively. A horizontal scrollbar is visible at the bottom of the cart area.

Kemudian saya akan menggunakan user Tony dan mencoba mengakses cart Mantap dengan mengganti parameter menggunakan burp suite.

Request to http://127.0.0.1:8000

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex ⌂ ⌂ IN INSPECTOR

```

1 POST /cart HTTP/1.1
2 Host: 127.0.0.1:8000
3 Content-Length: 57
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="95", ";Not A Brand";v="95"
6 sec-ch-ua-mobile: 70
7 sec-ch-ua-platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36
10 Origin: http://127.0.0.1:8000
11 Content-Type: application/x-www-form-urlencoded
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Dest: document
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Feature: -easement
18 Referer: http://127.0.0.1:8000/
19 Accept-Encoding: gzip, deflate
20 Accept-Language: en-US,en;q=0.9
21 Cookie: XSRF-TOKEN=eyJpdjI6Ix3YEElRjh1NW5LwA0PZFAeMoxBSoE9PSIisInZhbHV1IjoiaThicGxhBn0WhlSkw5VhrzZHN0VnJqYkdGQoQNHk10U3YwJfINnVhd0d2UzvQJM0N1pGTH1CdzFnRF1EWFDiUHh1SFpEK1FWs2dHNG5oeUREVEhgbkN2algbqVUJUJUcxtHNU2a1swhDV3NEVWTnhcCc5eV23TFeiLCJtYW10i11yUyHsQwG1CYTQyHDVmMjJyMaPhu1UmjHxOTg2MeExNxex01hMDriODYOYZYwNGM0NcQ0NTQ3NTEmh21ividGFni1jo1n043D; jajansnack_session=eyJpdjI6ImVxQaUJNExVIM3EWBdFMWdPdFu30Cc9PSIisInZhbHV1IjoiaUHirTU2NTGRGN2ModmRFT1FWS1NgdnJUhnJW0U00WeW9QJUHN3K1V2HHwldho201aAvgNmhl1QmOTHIQUWtXSFFBcDK02ZgvQKZ0cUJHvxBjaXJ4VFY31HnyV3Rcupw0h5RGW1ShFaJpUSeHqZfc1cG80aX1PMcvSKCp0qUY1LCJtYW10i1k0WHSyQ3NDKmHGTwMaH3NWhNQ3NaJhRaQ3MTh1ZmE3NCM502hYd9jWNTsYt2sPh0TiwHsh21ividGFni1jo1n043D
22 Connection: close
23 _token=otBvdUMr508G21311ITQnhd5KuJiJmQBV3h48ya2n&user_id=1

```

Saya mengganti \$user_id tersebut menjadi 2.

Request to http://127.0.0.1:8000

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex ⌂ ⌂ IN INSPECTOR

```

1 POST /cart HTTP/1.1
2 Host: 127.0.0.1:8000
3 Content-Length: 57
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="95", ";Not A Brand";v="95"
6 sec-ch-ua-mobile: 70
7 sec-ch-ua-platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://127.0.0.1:8000
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?2
16 Sec-Fetch-Dest: document
17 Sec-Fetch-Feature: -easement
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Cookie: XSRF-TOKEN=eyJpdjI6Ix3YEElRjh1NW5LwA0PZFAeMoxBSoE9PSIisInZhbHV1IjoiaUralZKQ3R1SkRjWjdWVvcnNUUsYTfKvMpN3RodGO0YnA3V1szEDhuDvB3VnlRbCY4NGFwdvENsUvMaK0Elbk12AhSvElleWhBSFd0hUFuR1Vta1ZPR2SyGhKsXJWV7YtWU74TtNBw0xp01VFBrlQ1FGwsls1M1N4NVBDROFNSOY1LCJtYW10i1jMjV1ZjEvTTAcTW3hJAM0T1aNTd1HGQ13MTV2ajA3Yzc4MTR1Ysh1Nm2hNvFjYVWh2au4M71j2DU5MaYv1ividGFni1jo1n043D; jajansnack_session=eyJpdjI6I1dGcl1UmagYTF6aWtCc1vQhNQhVqUhc9PSIisInZhbHV1IjoiaM0hWWFna31E60ryUctSYK2WSTivQWQ5UHFQU3RCQtd1UzFccUntamhJQCNZQ19EMWRhQjFXRehWhtB1uHh1Y1daRTgzbE11L3U1R1FpVxFiTn2rZTF3Vn2YWG8sSkRqd2gwSDFT0EsoYkNTM1piUW2tQz2aWHFvaJNNcGiveVi1LCJtYW10i1jk2jdiMDkyMj1h2T1zHTNaNWF1NGNhZjPmYq1MsN1NcQzM1x2WM5YtH42TM3MhNzD2hZjMzD1hYsc3HWY4I1ividGFni1jo1n043D
21 Connection: close
22 _token=otBvdUMr508G21311ITQnhd5KuJiJmQBV3h48ya2n&user_id=2

```

Ketika saya forward, user Tony akan memiliki isi cart dari Mantap.

JAJANSNACK

HOME SHOP TONY [0]

Product name	Price	Quantity	Total
 Cheetos Bagel & Cheese Sweet, and salty flavor packed into crunchy, cheesy snacks. CHEETOS® Bagel & Cheese Flavored Snacks are full of flavor and made with real cheese.	Rp 24.000	1	Rp 24.000
 Lays Grilled Cheese and Tomato Soup Exciting new grilled cheese and tomato soup flavor.	Rp 20.000	1	Rp 20.000

4. XSS pada kolom input yang tersedia

Ketika saya melakukan XSS dengan menggunakan payload dari <https://book.hacktricks.xyz/pentesting-web/xss-cross-site-scripting> dan <https://portswigger.net/research/noscript-xss-filter-bypass> saya tidak menemukan efek atau dampak yang ditimbulkan dari script.

Contoh (script yang digunakan “”):

Back to Shop

Kitkat Peach Mint

4.7 ★★★★★

Rp 12.000

Kitkat mixed with peach and mint flavor

- +

49 available

Add to Cart

Hasil atau result:

Item(s) quantity must be below available quantity

Back to Shop

Kitkat Peach Mint

4.7 ★★★★★

Rp 12.000

Kitkat mixed with peach and mint flavor

- 1 +

49 available

Add to Cart

5. OWASP ZAP

http://127.0.0.1:8000 Scan Progress						
Progress		Response Chart				
Host:	http://127.0.0.1:8000					
	Strength	Progress	Elapsed	Reqs	Alerts	Status
Analysing			00:01.406	9		
Plugin						
Path Traversal	Medium		01:39.321	339	0	✓
Remote File Inclusion	Medium		01:00.609	220	0	✓
Source Code Disclosure - /WEB-INF folder	Medium		00:12.446	41	0	✓
External Redirect	Medium		00:30.955	117	0	✓
Server Side Include	Medium		00:28.147	88	0	✓
Cross Site Scripting (Reflected)	Medium		00:27.454	113	0	✓
Cross Site Scripting (Persistent) - Prime	Medium		00:11.090	22	0	✓
Cross Site Scripting (Persistent) - Spider	Medium		00:11.269	87	0	✓
Cross Site Scripting (Persistent)	Medium		00:08.407	0	0	✓
SQL Injection	Medium		01:32.709	610	0	✓
Server Side Code Injection	Medium		00:31.041	176	0	✓
Remote OS Command Injection	Medium		02:12.361	866	0	✓
Directory Browsing	Medium		00:15.231	87	0	✓
Buffer Overflow	Medium		00:12.030	22	0	✓
Format String Error	Medium		00:18.738	66	0	✓
CRLF Injection	Medium		00:29.135	154	0	✓
Parameter Tampering	Medium		00:36.468	157	0	✓
ELMAH Information Leak	Medium		00:00.138	1	0	✓
.htaccess Information Leak	Medium		00:02.279	9	1	✓
Script Active Scan Rules	Medium		00:00.001	0	0	✗
Cross Site Scripting (DOM Based)	Medium		00:00.211	0	0	✗
Advanced SQL Injection	Medium		18:39.042	5532	0	✓
SOAP Action Spoofing	Medium		00:00.400	0	0	✓
SOAP XML Injection	Medium		00:08.377	0	0	✓
Totals			29:36.696	8876	1	

Dengan menggunakan automated scan dari aplikasi OWASP ZAP, kami mendapati 1 vulnerability yaitu pada file htaccess dengan peringatan “.htaccess Information Leak”.

.htaccess Information Leak	
URL: http://127.0.0.1:8000/.htaccess	
Risk: Medium	
Confidence: Medium	
Parameter:	
Attack:	
Evidence: HTTP/1.1 200 OK	
CWE ID: 94	
WASC ID: 14	
Source: Active (40032 - .htaccess Information Leak)	
Description:	
htaccess files can be used to alter the configuration of the Apache Web Server software to enable/disable additional functionality and features that the Apache Web Server software has to offer.	
Other Info:	
Solution:	
Ensure the .htaccess file is not accessible.	
Reference:	
http://www.htaccess-guide.com/	
Alert Tags:	
Key	Va
OWASP 2021 A05	https://owasp.org/Top10/A05_2021-Security_Misconfiguration/