

Praktikum Keamanan Jaringan
A05 Security Misconfiguration



Dosen Pengampu :
Ferry Astika Saputra, ST, M.Sc.

Nama: Saifudin
NRP: 3122640042

KELAS D4 LJ TI B
JURUSAN D4 TEKNIK INFORMATIKA
POLITEKNIK ELEKTRONIKA NEGERI SURABAYA
2023

TUGAS PRAKTIKUM KEMAMAN JARINGAN

Tugas 1

Resume apnic modul A05 Security Misconfiguration

Pengerjaan

Security Misconfiguratio adalah kerentanan yang paling umum terjadi dalam daftar kerentanan keamanan. Biasanya kesalahan terjadi ketika konfigurasi default digunakan tanpa memperhatikan kebutuhan khusus dari website

Berikut adalah beberapa contoh Security Misconfiguration yang berhasil diidentifikasi pada website OWASP Juice Shop:

A. Error Handling

memunculkan error, tetapi error yang ditampilkan tidak secara bagus dan konsisten.

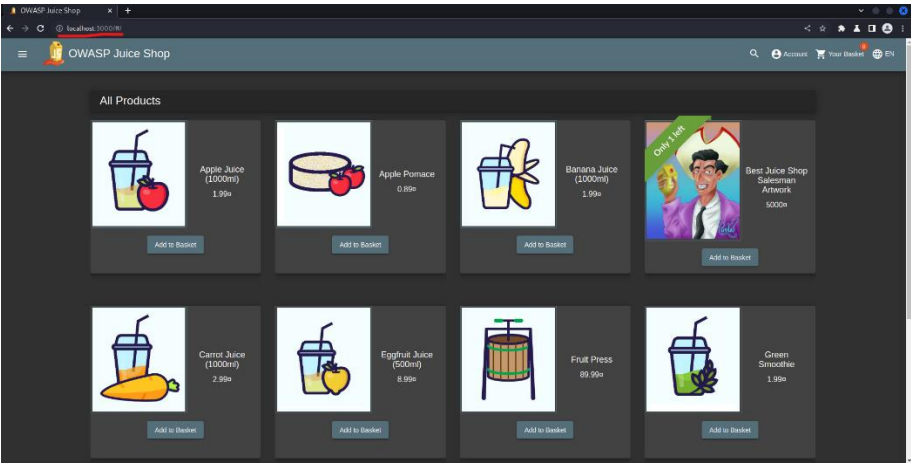
Nyalakan Burp Suite terlebih dahulu

Burp Suite Community Edition v2023.1.2 - Temporary Project										
Burp Project Intruder Repeater Window Help										
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn										
Intercept HTTP history WebSockets history Proxy settings										
Filter: Hiding CSS, image and general binary content										
#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	
3	http://cdnjs.cloudflare.com	GET	/ajax/libs/cookieconsent/2/3.1.0/cookiec...			200	21790	script	js	
8	http://cdnjs.cloudflare.com	GET	/ajax/libs/jquery/2.2.4/jquery.min.js			200	86561	script	js	
1	http://localhost:3000	GET	/			200	2425	HTML		
4	http://localhost:3000	GET	/main.js			304	365	script	js	
5	http://localhost:3000	GET	/vendor.js			304	366	script	js	
6	http://localhost:3000	GET	/polyfills.js			304	364	script	js	
7	http://localhost:3000	GET	/runtime.js			304	363	script	js	
10	http://localhost:3000	GET	/rest/admin/application-configuration			304	278			
11	http://localhost:3000	GET	/assets/i18n/en.json			304	364	script	json	
12	http://localhost:3000	GET	/socket.io/?EIO=4&transport=polling&t...	✓		200	232	JSON	io/	
13	http://localhost:3000	GET	/rest/admin/application-version			304	276			
14	http://localhost:3000	GET	/rest/admin/application-configuration			304	278			

Request

Response

Selanjutnya buka browser dan pergi ke halaman utama website OWASP Juice Shop



Buka kembali Burp Suite maka akan muncul request baru yaitu `/rest/product/search`

Burp Suite Community Edition v2023.12 - Temporary Project										
Burp	Project	Intruder	Repeater	Window	Help					
Dashboard	Target	Proxy	Intruder	Repeater	Sequencer	Decoder	Comparer	Logger	Extensions	Learn
Intercept	HTTP history	WebSockets history	Proxy settings							
Filter: Hiding CSS, image and general binary content										
#	Host ^	Method	URL	Params	Edited	Status	Length	MIMEtype	Extension	
64	http://localhost:3000	GET	/rest/user/whoami			304	275			
65	http://localhost:3000	GET	/rest/admin/application-configuration			304	278			
66	http://localhost:3000	GET	/api/Challenges/?name=Score%20Board	✓		304	277			
67	http://localhost:3000	GET	/api/Quantities/			304	278			
68	http://localhost:3000	GET	/rest/products/search?q=	✓		304	278			
70	http://localhost:3000	POST	/socket.io/?EIO=4&transport=polling&t...	✓		200	121	text	io/	
71	http://localhost:3000	GET	/socket.io/?EIO=4&transport=polling&t...	✓		200	168	JSON	io/	
72	http://localhost:3000	GET	/socket.io/?EIO=4&transport=websocket...	✓		101	129	io/	io/	
85	http://localhost:3000	GET	/socket.io/?EIO=4&transport=polling&t...	✓		200	136	text	io/	
86	http://localhost:3000	GET	/font-mfizz.woff			304	364		woff	
87	http://localhost:3000	GET	/api/Quantities/			304	278			
88	http://localhost:3000	GET	/rest/products/search?q=	✓		304	278			

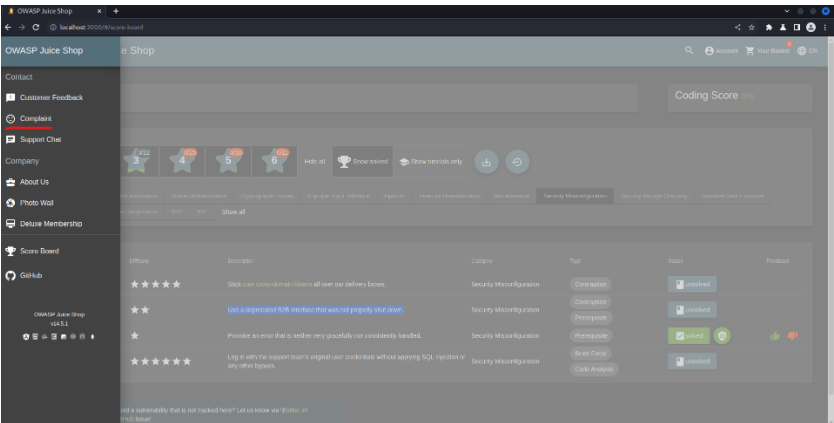
Masukkan payload /rest/product/search tadi ke repeater lalu ubah enpointnya menjadi text random lalu klik tombol send

[illegible]

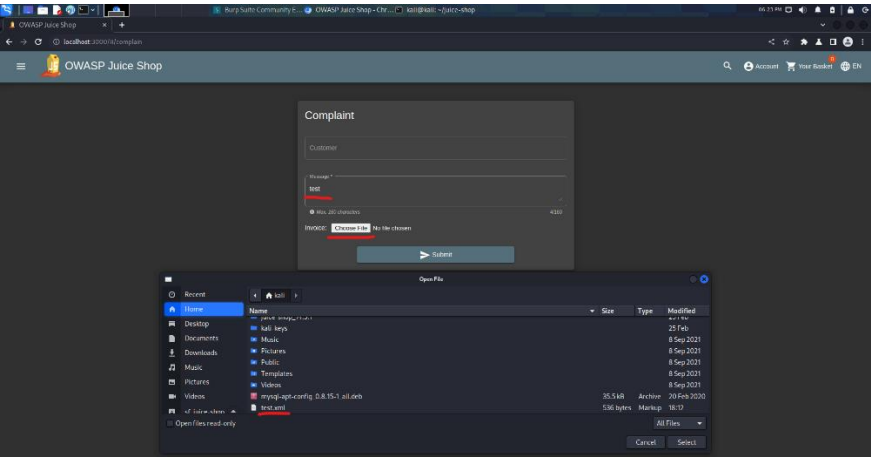
B. Deprecated Interface

Menggunakan antarmuka B2B usang yang tidak dimatikan dengan benar.

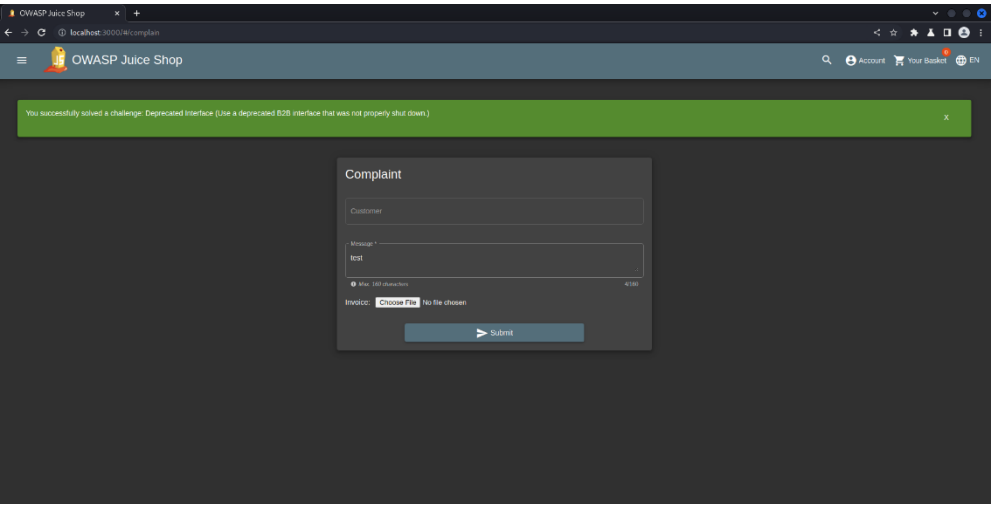
Pada halaman utama, klik tombol menu di pojok kiri atas untuk memunculkan sidebar. Setelah itu klik complaint



Setelah sudah masuk ke halaman complaint, isikan form yang ada, dan masukkan file dengan format xml



Setelah itu akan muncul challenge Deprecated Interface berhasil di selesaikan seperti ini



Jika kita lihat di proxy history pada burp suite, akan muncul error panjang seperti ini

