

1

01/10/24

Hafaidh Mohamed BTS-SIO2

SOMMAIRE

PORTAINER DOCKER	3
DATABASE SERVER	5
Activité 1	8
ACTIVITÉ 2	

PORTAINER DOCKER

Tout d'abord nous devons créer un stack comme c'est expliqué dans l'activité, avec le nom mutilidae une fois cela fait nous devons installer le fichier mutillidae-dockerhub sur github. Dans le dossier nous allons retrouver un fichier au nom de docker-compose.yml qu'on doit ajouter dans le stack.



Une fois fini vous devez déployer le projet cela prendra du temps c'est normal.



Le projet déployer vous devriez avoir cela :

Stacks				(administrateur 🗸
Stacks				Q Search X	move + Add stack 🔲 🚦
Name↓↑ Filter ♥	Type↓↑	Control	Created↓↑	Updated↓↑	Ownership↓↑
📄 mutilidae	Compose	Total	2024-10-01 14:21:21 by administrateur	2024-10-01 14:23:44 by administrateur	⊗ administrators
					Items per page 10 🗸

€	Containers			Q S						•
	Name↓↑	State↓↑ Filter 🍸	Quick Actions	Stack↓↑	Image↓↑		Created↓↑	IP Address↓↑	Published Ports↓↑	Ownersh
		running		mutilidae			2024-10-01 14:21:21	172.20.0.2		🗞 admir
		running		mutilidae			2024-10-01 14:23:39	172.20.0.3		🗞 admir
		running		mutilidae			2024-10-01 14:23:39	172.19.0.2		🗞 admir
		running		mutilidae			2024-10-01 14:23:40	172.19.0.3		🗞 admir
		running		mutilidae			2024-10-01 14:23:40	172.20.0.4		🗞 admir
•									Itoma par paga	10

N'oublier pas d'enlever les ip et laisser les port sur l'editor :

	Stack C Editor
This s	tack will be deployed using docker compose .
You ca	an get more information about Compose file format in the official documentation.
 Det 	fine or paste the content of your docker compose file here
1	<pre># Documentation: https://github.com/compose-spec/compose-spec/blob/master/spec.md</pre>
2	<pre># Purpose: Build local containers for the Mutillidae environment</pre>
	version, 12.7
	services:
	database:
	container_name: database
	<pre>image: docker.io/webpwnized/mutillidae:database</pre>
	networks:
	- datanet
	databasa admin.
	udlabdse_ddmin:
	depends on:
	- database
	image: docker.io/webpwnized/mutillidae:database admin
	ports:
	- 81:80
	networks:
	- datanet
	# IP 127.0.0.1 is for mutillidae.localhost or www.mutillidae.localhost
	# IP 127.0.0.1 is for cors.mutilliiidae.localhost

DATABASE SERVER

Maintenant vous devez taper votre ip du serveur sur le navigateur cela vous ramènera sur une page comme celle-ci :

The database server at database appears to be offline.

- 1. Click here to attempt to setup the database. Sometimes this works.
- 2. Be sure the username and password to MySQL is the same as configured in includes/database-config.inc
- Be aware that MySQL disables password authentication for root user upon installation or update in some systems. This may happen even for a minor update. Please check the username and password to MySQL is the same as configured in includes/databaseconfig.inc
- 4. A video is available to help reset MySQL root password
- 5. Check the error message below for more hints
- 6. If you think this message is a false-positive, you can opt-out of these warnings below

Database Diagnostics Information

Database Error message:

Database host: database Database post: 3306 Database username: root Database password: mutillidae Database name: mutillidae

IP resolved from database hostname: 172.20.0.2

Ping database results:

PING database (172.20.0.2) 56(84) bytes of data. 64 bytes from database.mutilidae_datanet (172.20.0.2): icmp_seq=1 ttl=64 time=0.218 ms

--- database ping statistics ---1 packets transmitted, 1 received, 0% packet loss, time 0ms rtt min/avg/max/mdev = 0.218/0.218/0.218/0.000 ms

Traceroute database results:

Vous devriez cliquer sur Click Here pour accéder au site web OWASP Mutillidae II.



Maintenant vous allez installer BurpSuite :





Une fois installer vous tomber sur une page comme celle-ci :

Activité 1

Travail à faire 1 :

Q1. Créer un compte permettant de vous authentifier sur la plate-forme.

	e owa	SP Mutillidae II:	Keep Calı	m and Pwn On	
	Version: 2.11.17	Security Level: 0 (Hosed)	Hints: Enabled	Logged In User: Jean 📝	
	Home Logout Tog	gle Hints Toggle Security Enfo	orce TLS Reset DB \	/iew Log View Captured Data	
₩ Hints	and Videos				
		TIP: C	Click <i>Hint and Video</i> on each page	DS	
What Should I Do?	🥞 Help Me!				
Listing of vulnerabilit	ies 🕞 Video Tuto	orials			

Q2. Utiliser une méthode de votre choix afin de découvrir les noms des champs login et mot de passe du formulaire d'authentification.

Ouvrez BurpSuite et créez un projet temporaire.

Dans l'onglet Proxy, assurez-vous que l'interception est désactivée (Intercept is off).

n'oubliez pas d'activer votre proxy dans les paramètre de votre navigateur ou dans les paramètres de linux.

Maintenant vous allez sur le site web OWASP et vous allez mettre vos identifiant rentre au par avant attention il ne faut pas se login :

Please sign-in

Maintenant vous activez Intercept is on pour recevoir les requêtes. puis vous faites login.

Q3. Positionner le niveau de sécurité du code à 0 (Hosed) :

Intercept HTT	P history	WebSockets history (Proxy	settings							
Interce	pt on	→ Forward V	Drop			Request to	http://172.16.61.4:80 🖉	Open I	prowser	() 1
Time	Туре	Direction	Host	Method	URL			Status code	I	ength
16:26:47 1 Oct 2024	HTTP	→ Request	172.16.61.4	GET	http://172.16.61.4	1/index.php?do=to	ggle-security&page=login			
16:26:50 1 Oct 2024	HTTP	→ Request	172.16.61.4	GET	http://172.16.61.4	l/index.php?do=lo	gout			
Request					~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	9 m =	Inspector		±÷€) × (
Pretty Raw	Hex				Q.	🔛 W =				
1 GET /index.p	inp (do=togg)	le-security&page=login.pnp	HIIP/1.1				Request attributes		2	× .
3 User-Agent: 4 Accept:	Mozilla/5.(0 (X11; Ubuntu; Linux x86_6	i4; rv:130.0) Gecko/2010	00101 Firefox/130.0	(0+Ym] */* 0-(. 8	Request query parameters	;	2	~
5 Accept - Langu	age: fr,fr ling: gzip.	-FR; q=0.8, en - US; q=0.5, en; q= deflate. br	0.3	(op)::mage/ping/image/s			Request body parameters		0	~
7 Connection: 8 Cookie: PHPS	keep-alive ESSID=22pq	3dmsafi50d3vjrd60vmqdu; shq	whints=0; phpMyAdmin=e2	2412861ab904c73ffc50d3	o3480344e; pma	a_lang=fr	Request cookies		4	~
9 Upgrade-Inse 10 Priority: u= 11	cure-Reques 0, i	sts: 1					Request headers		9	~
(?) (‡) (►)	Search				Q	0 highlights				

Comme on le voit, le niveau de sécurité a été modifié.

Allez dans les paramètres de sécurité et changez le niveau de sécurité à **un niveau supérieur** (par exemple, **niveau 1 ou 2**). Ce niveau active des mesures de protection contre les attaques SQLi.

OWASP 2013 OWASP 2010 OWASP 2007 Web Services	Back See Help Me!								
Others 🕨		Pass	word in	correct					
Labs 🕨	ſ	PI	ease si	gn-in					
Documentation 🕨		Username							
Resources 🕨		Password							
Donate			Login						
Want to Help?		Dont have an a	ccount?	Please register here					
Con	sole 🕞 Débogueur † Réseau -{} Éditeur de style 🛛 Performances	🕄 🕀 Mémoire 🗄 Stockage 🕇 Ac	essibilité	888 Applications					D
Rechercher dans le HTML						🔅 🛈 🖹	Mise en page	Calculé Mo	difications C
html PUBLIC "-/<br <html> event défilable</html>	//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/1999/	REC-html401-19991224/loose.dtd">		élément III { }					
<pre> <head> </head> <</br></pre>	n="true"> débordement						Sélectionnez un cor continuer.		
<pre><table class="main-tal</th><th>ble-frame">mm (débordement)</table></pre>			html !!! {	<u>global-s</u> if taboma vero	tyles.css:3				
<pre>div id="colorbox" cl;</pre>	ass="" style="display: none; padding-bottom: 42px; padding-right:				<u></u> ,			tilisée sur la page	

	//`				
	Ve	rsi	on: 2.11.17	Security L	evel: 0 (
	Home Logi	n/R	tegister Toggl	e Hints Toggl	le Securi
OWASP 2017	A1 - Injection (SQL)	▶			
OWASP 2013	A1 - Injection (Other)	۲			
OWASP 2010	A2 - Broken Authentication and Session Management	►	Authe	ntication Bypass	•
OWASP 2007		_	Privi	iege Escalation	•
	A3 - Sensitive Data Exposure			-	
Web Services		_	Userna	me Enumeration	•
Others	A4 - XML External Entities		ISONA	Vab Takan (1347)	
	A5 - Broken Access Control		120N V	veo Token (J w I)	

Vous devez vous dériger vers **OWASP 2017** pour accéder **A2-Broken Auth....** Puis **Username Enumeration** puis **LookUp user.**

Cela fait vous tombez sur une page comme celle-ci :

W	s-user-account	
	View the <u>WSDL</u> for the service. Click on an operation name to view it's details.	
	<u>getUser</u>	
	<u>createUser</u>	

Maintenant vous allez sur Burp Suite pour activer Intercept off en on. Comme ce screen :

Burp Project	Intruaer	кереаter	view негр										
Dashboard	Target	Proxy	Intruder	Repeater	Collaborator	Sequencer	Decoder	Comparer	Logger	Organizer	Extensions	Learn	Wsdler
Intercept	HTTP histor	y Web:	Sockets history	(i) Pr	oxy settings								
@ Int	ercept on		> Forward		Drop								
Time	Т	ype		Direction		Host			Method	URL			
								F					

Une fois que le Intercept est en on vous devez cliquer sur L'URL "WSDL" de la page précédente attention vous devez avoir votre proxy bien activé si cela ne fonctionnera pas :

View the <u>WSDL</u> for the service. Click on an operation name to view it's details.

Très bien, maintenant vous allez sur Burp Suite :

Burp Project Intrude	Repeater	View Help												
Dashboard Target	Proxy	Intruder	Repeater	Collaborator	Sequencer	Decoder	Comparer	Logger	Organizer	Extensions	Learn	Wsdler		Settings
Intercept HTTP his	ory Web	Sockets history	O Pro	xy settings										
③ Intercept on → Forward ✓ Drop Request to http://17216.61.4:80 Ø ⊕ Open browser ③										er 🤉 :				
Time	Туре	0	Direction		Host			Method	URL				Status code	Length
16:31:08 8 Oct 2024	HTTP		→ Request		172.16.61.4			GET	http://17	2.16.61.4/webserv	ices/soap/	ws-user-account.php?wsdl		

¢,	Inspector 🔳 🗉 🛨 🐵 🗙	Request
Insp	Request attributes 2 ~	Pretty Raw Hex GET /vebservices/soap/ws-user-account.php?wsdl HTTP/1.1
oector	Request query parameters 1 ~	2 Host: 172.16.61.4 3 Upgrade-Insecure-Requests: 1 4 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36
	Request body parameters 0 ~	<pre>S Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8 6 Sec-CPC: 1 2 Accept: apnumant fr.FR fr</pre>
	Request cookies 7 ~	9 Refere: http://ll21.16.61.4/webservices/soap/ws-user-account.php 9 Accept-Encoding: gzip, deflate, br
lotes	Request headers 10 ~	<pre>10 Cookie: pmalang=fr: senu_lock=0: pmalser-1=ddM480j0mLBsxYhlT4fH26pcRSCpe3zakUTy3TsJvHX8et3UL6AX5j4430: portainer_api_key= eybh6ci3JUIIINIEINESCIGTKPXVD:9: eyb2CT6MsviAWL eshbMutoiJD2Caphale4JhdGV1ciIIIJV4UK05jEIN(biBI)ioIZOVFXVGCIIII/CAUEA 3dvcm20m2hbMLLCleH4i0jEBMj0MTg5OT0sImp0asI61j000Tc3MsVjLTg5ZjHHNDY3ZCLHj02LWE00WR12jZ1VWZkZCISILhdCf0MTcy0MB9DESNH0.kisp0003TuoIca82V0 PQMvDoSVetKvqTp0VIdDVKV; gorlla_csf= MTcy0MSMDESNHJDTRAWDKROUTbHkbH6qVILvVELucDZzbFZNY0dsVFdYRktUMnAyZDA5dmFXVkRMMLExTjFsNmQvMDLJZ289fFlx1pumP_fkIMjSnYvIJZYjNKJ238d-QJddp9are1 11 Connection: keep-alive 12 13 14 15 15 15 15 15 15 15 15 15 15 15 15 15</pre>
Eve	nt log (1) All issues	O Memory 167 8MB

Si la manipulation a bien fonctionné normalement vous devez tomber sur la même interface du screen au-dessus.

ACTIVITÉ 2

Travail à faire 1

Q1. Commencer par installer l'extension Wsdler en réalisant les manipulations décrites dans l'étape n°1. Puis, positionner le niveau de sécurité à 0.

WebSphere Portlet S		ជជជជា	— 17 Feb 2015	Low		Updated:	01 Nov 2
Wordlist Extractor		☆☆☆☆☆	— 20 Apr 2017	Low		·	
WordPress Scanner		☆☆☆☆☆☆		Low		Rating:	ជាជា
WS Security		****	— 10 Feb 2022	Medium		Popularity-	
WSDL Wizard		☆☆☆☆☆☆	— 01 Jul 2014	Low		Popularity.	
Wsdler	~	☆☆☆☆☆	— 01 Nov 2016	Low		Deinstel	
XChromeLogger Dec		<u> </u>	— 15 Dec 2021	Low		Reinstat	
XSS Cheatsheet		<u> </u>	— 17 Oct 2023	Low			
XSS Validator		☆☆☆☆☆	— 10 Feb 2022	High	Requires Bur		

Tester un exemple de requête et de réponse à l'aide d'un login non valide en réalisant les manipulations décrites dans l'étape n°2 (parse de la page wsdl, envoi au répéteur, génération de la réponse et envoi au comparateur).

Burp	Project	Intruder	Repeater	View Help					
Dashb	oard	Target	Proxy	Intruder	Repeater	Collaborato	r Sequencer	Decoder	Compare
1 ×	+								
Sen	d Ø	Canc	el 🤇 🖓) > v					
Reque	est							Response	
Pretty	Rav	/ Hex				Ø	🗊 \n 🗉		
1 GET use 2 Hos 3 Upg 4 Use (KF 5 Acc tex age 6 Sec 7 Acc 8 Ref 8 Ref 0 Coo 0 ddM por eyJ 1pb mdl LTk kG8 MTc YZE C40	<pre>Pretty Raw Hex</pre>								
Ready									

Securem .							
	#	Length	Data	Paste			
	1 1	1281	${\tt GET\/index.php?page=user-info.php\&username=admin\&password=jggut\&user-info-php-submit-button=View+Acc}$	Load			
				Remove			
				Clear			

Cela me fait une erreur quand j'essaye de l'envoyer à WSDLER