

WhiteHat School 1기

SSRF 문제 Write-up

Team: 과부화

Writer: 정진교

문제분석

Lab: Basic SSRF against another back-end system

APPRENTICE

LAB

Not solved



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

To solve the lab, use the stock check functionality to scan the internal `192.168.0.X` range for an admin interface on port 8080, then use it to delete the user `carlos`.



ACCESS THE LAB

저번 문제인 Basic SSRF against another the local server에 이어 비슷한 결의 문제인 Basic SSRF against another back-end system 문제를 들고 왔다. 문제 내용은 살짝 다르다. 백엔드 시스템의 개인 ip를 찾아내야 하기 때문이다.

서버 측 요청 위조로 자주 발생하는 유형은 애플리케이션 서버가 사용자가 직접 연결할 수 없는 다른 백엔드 시스템과 상호 작용할 수 있는 경우이다.

이러한 시스템에는 라우팅할 수 없는 개인 IP 주소가 있는 경우가 많다.


백엔드 시스템은 일반적으로 네트워크 토폴로지로 보호되기 때문에 보안 상태가 취약한 경우가 많다.





많은 경우 내부 백엔드 시스템에는 시스템과 상호 작용할 수 있는 모든 사람이 인증 없이 액세스할 수 있는 민감한 기능이 포함되어 있다.

이번 문제는 내부 백엔드 시스템에서 접근하여 사용자를 삭제하는 것이다.

저번 문제와 똑같이 내부 재고 시스템 기능을 사용하여 192.168.0.X 범위내에서 포트 8080 admin계정에 접속하여 사용자 carlos를 삭제해야 한다.

문제풀이

WE LIKE TO
SHOP 

			
Hologram Stand In ★★★★★ \$0.92	Caution Sign ★★★☆☆ \$0.20	Cheshire Cat Grin ★★★☆☆ \$16.75	Packaway Carport ★★★★★ \$24.12
View details	View details	View details	View details

저번 문제와 달라진 건 상품 종류밖에 없고, View details를 눌러 확인해보니

Description:

Do you ever have one of those days where nothing looks right, and you just don't feel like going to the ball? Never fear, Hologram Stand In is here.

There are times when you can't say no to that important invite, you need to show your face to the right people. But, we all have off days and know we won't be showing the right face if we turn up feeling like a sack of potatoes.

We spend time with our customers when they are having their best days, with 360-degree hologram mapping, and typical response recordings you shall go to the ball. Our experts are on hand throughout the evening enabling them to project you into the correct settings. We will also program polite excuses to leave the room should your hologram not be able to respond appropriately to a given set of questions.

With your Hologram Stand In you never need to worry about all those stressful high expectations again. You will look just as fresh and amazing at the end of the night as you do at the start. Put your best dress on, smile and we will do the rest. Full money back guarantee if your night is not a huge success*.

*Judged by whether you manage to pull it off.

London

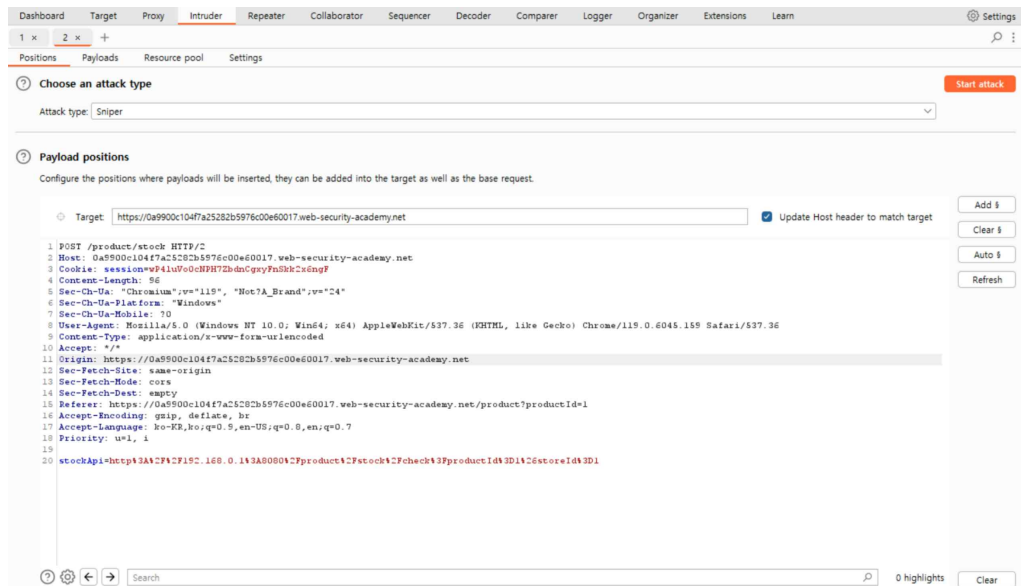
똑같이 Check stock이라는 버튼이 존재했다.

`stockApi=http://192.168.0.1:8080/admin`

POST 요청에서 하단에 보면 저번 문제와 같은 stockApi의 url이 있다.

문제에서 알려준 `http://192.168.0.1:8080/admin` url을 입력한다.

그리고 위의 '1'부분을 드래그하고, add를 눌러 payload 공격을 수행할 부분을 지정한다.



저번 문제와 다르게 서버 IP가 특정되지 않았으므로 알맞는

서버 IP 범위를 찾아야 한다.

Proxy를 이용해 나온 값들을 Intruder로 넘겨준다.

Burp Suite Intruder는 웹 애플리케이션을 대상으로 사용자 정의 공격을 할 수 있는 자동화 도구다. 간단한 공격부터 복잡한 공격까지 다양한 공격 형태를 지원한다.

이 기능은 보통 무차별 대입공격(Brute Force)에 많이 사용이 된다.

Payload settings [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: ☒ Sequential ☐ Random

From:

To:

Step:

How many:

Payload 탭에서 type을 Numbers로 설정하고 옵션에서

1부터 255까지 1씩 커지도록 설정한다.

Attack Save Columns 2. Intruder attack of https://0a9900c104f7a25282b5976c00e60017.web-security-academy.net - Temp...

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request ^	Payload	Status code	Error	Timeout	Length	Comment
0		400	<input type="checkbox"/>	<input type="checkbox"/>	141	
1	1	400	<input type="checkbox"/>	<input type="checkbox"/>	141	
2	2	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
3	3	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
4	4	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
5	5	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
6	6	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
7	7	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
8	8	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
9	9	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
10	10	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
11	11	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	

15 of 255

이렇게 결과들이 쭉쭉 나열되게 된다.

Request	Payload	Status co... ^	Error	Timeout	Length	Comment
124	124	200	<input type="checkbox"/>	<input type="checkbox"/>	3274	
0		400	<input type="checkbox"/>	<input type="checkbox"/>	141	
1	1	400	<input type="checkbox"/>	<input type="checkbox"/>	141	
2	2	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
3	3	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
4	4	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
5	5	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
6	6	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
7	7	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
8	8	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
9	9	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
10	10	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	

공격이 끝나고, status 값이 다른 payload를 찾을 수 있다. 여기서는 '124'가 된다.

`stockApi=http://192.168.0.124:8080/admin`

stockApi 값을 http://192,168.0.X:8080/admin에서 status 값이 다른 payload인 124를 넣어서 수정한 뒤 프록시를 사용하면

결과

London

▼

Check stock

WebSecurity Academy

Basic SSRF against another back-end system

LAB

Not solved

Back to lab description >>

[Home](#) | [Admin panel](#) | [My account](#)

Users

wiener - [Delete](#)
carlos - [Delete](#)

저번 문제와 똑같은 admin 페이지에 접속이 되게 된다.

이 이후의 과정은 Basic SSRF against the local server 문제와 같다.