IDOR

What is an IDOR?

In this room, you're going to learn what an IDOR vulnerability is, what they look like, how to find them and a practical task exploiting a real case scenario.

What is an IDOR?
IDOR stands for Insecure Direct Object Reference and is a type of access control vulnerability.

This type of vulnerability can occur when a web server receives user-supplied input to retrieve objects (files, data, documents), too much trust has been placed on the input data, and it is not validated on the server-side to confirm the requested object belongs to the user requesting it.
****

Answer the questions below:

What does IDOR stand for?
Answer: Insecure Direct Object Reference
****

An IDOR Example

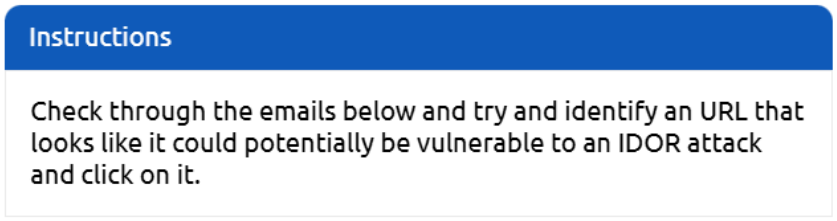
Imagine you've just signed up for an online service, and you want to change your profile information. The link you click on goes to http://online-service.thm/profile?user_id=1305, and you can see your information.

Curiosity gets the better of you, and you try changing the user_id value to 1000 instead (http://online-service.thm/profile?user_id=1000), and to your surprise, you can now see another user's information. You've now discovered an IDOR vulnerability! Ideally, there should be a check on the website to confirm that the user information belongs to the user logged requesting it.

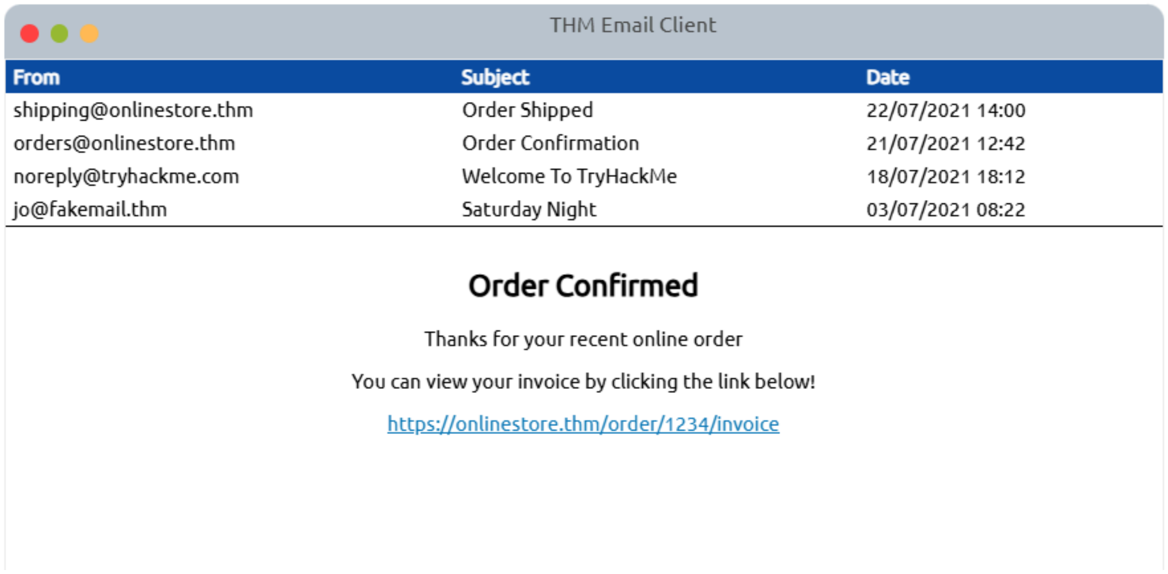
Using what you've learnt above, click on the View Site button and try to receive a flag by discovering and exploiting an IDOR vulnerability.
****

Answer the questions below:

What is the Flag from the IDOR example website?


Instructions

Check through the emails below and try and identify an URL that looks like it could potentially be vulnerable to an IDOR attack and click on it.


THM Email Client

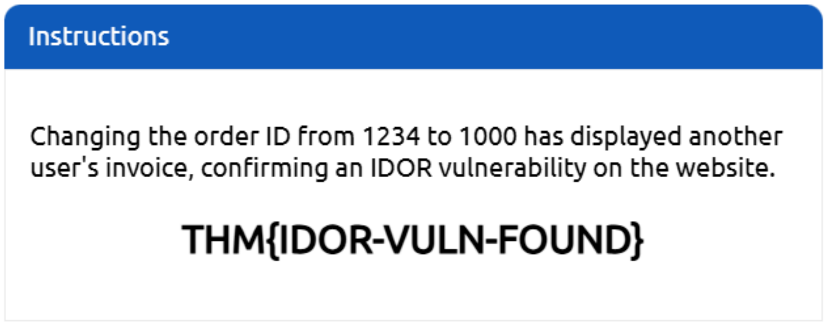
From	Subject	Date
shipping@onlinestore.thm	Order Shipped	22/07/2021 14:00
orders@onlinestore.thm	Order Confirmation	21/07/2021 12:42
noreply@tryhackme.com	Welcome To TryHackMe	18/07/2021 18:12
jo@fakemail.thm	Saturday Night	03/07/2021 08:22

Order Confirmed

Thanks for your recent online order

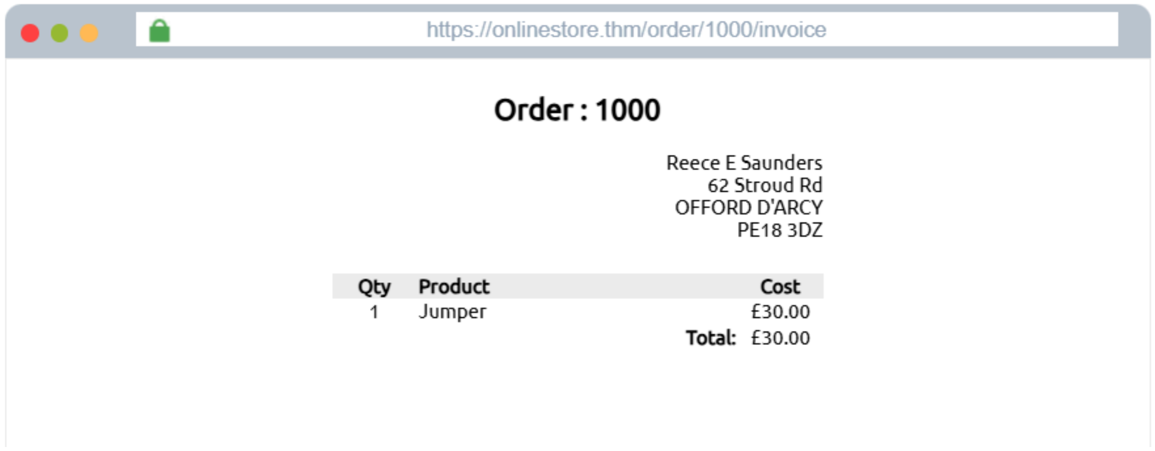
You can view your invoice by clicking the link below!

https://onlinestore.thm/order/1234/invoice


Instructions

Changing the order ID from 1234 to 1000 has displayed another user's invoice, confirming an IDOR vulnerability on the website.

THM{IDOR-VULN-FOUND}


https://onlinestore.thm/order/1000/invoice

Order : 1000

Reece E Saunders
62 Stroud Rd
OFFORD D'ARCY
PE18 3DZ

Qty	Product	Cost
1	Jumper	£30.00
	Total:	£30.00

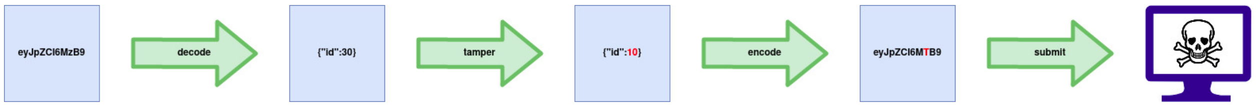
Answer: THM{IDOR-VULN-FOUND}
****

Finding IDORs in Encoded IDs

Encoded IDs

When passing data from page to page either by post data, query strings, or cookies, web developers will often first take the raw data and encode it. Encoding ensures that the receiving web server will be able to understand the contents. Encoding changes binary data into an ASCII string commonly using the a-z, A-Z, 0-9 and = character for padding. The most common encoding technique on the web is base64 encoding and can usually be pretty easy to spot. You can use websites like https://www.base64decode.org/ to decode the string, then edit the data and re-encode it again using https://www.base64encode.org/ and then resubmit the web request to see if there is a change in the response.

See the image below as a graphical example of this process:



****

Answer the questions below:

What is a common type of encoding used by websites?

Answer: base64
****

Finding IDORs in Hashed IDs

Hashed IDs

Hashed IDs are a little bit more complicated to deal with than encoded ones, but they may follow a predictable pattern, such as being the hashed version of the integer value. For example, the ID number 123 would become 202cb962ac59075b964b07152d234b70 if md5 hashing were in use.

It's worthwhile putting any discovered hashes through a web service such as https://crackstation.net/ (which has a database of billions of hash to value results) to see if we can find any matches.
****

Answer the questions below:

What is a common algorithm used for hashing IDs?
Answer: md5
****

Finding IDORs in Unpredictable IDs

Unpredictable IDs

If the ID cannot be detected using the above methods, an excellent method of IDOR detection is to create two accounts and swap the Id numbers between them. If you can view the other users' content using their ID number while still being logged in with a different account (or not logged in at all), you've found a valid IDOR vulnerability.
****

Answer the questions below:

What is the minimum number of accounts you need to create to check for IDORs between accounts?
Answer: 2
****

Where are IDORs Located

Where are they located?

The vulnerable endpoint you're targeting may not always be something you see in the address bar. It could be content your browser loads in via an AJAX request or something that you find referenced in a JavaScript file.

Sometimes endpoints could have an unreferenced parameter that may have been of some use during development and got pushed to production. For example, you may notice a call to /user/details displaying your user information (authenticated through your session). But through an attack known as parameter mining, you discover a parameter called user_id that you can use to display other users' information, for example, /user/details?user_id=123.
****

Answer the questions below:

Read the above:
No Answer Needed
****

A Practical IDOR Example

Begin by pressing the Start Machine button; once started, click the below link and open it in a new browser tab:

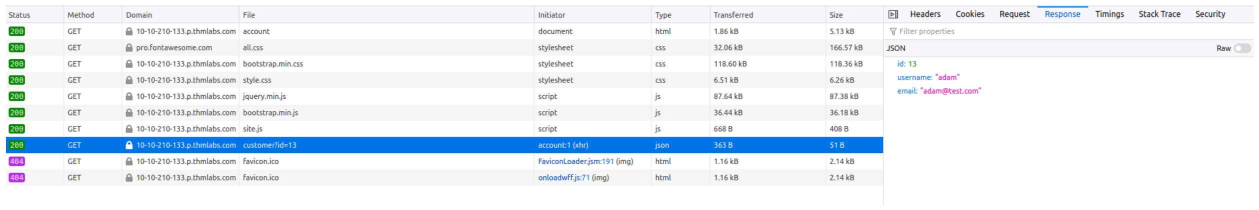
- https://LAB_WEB_URL.p.thmlabs.com

Firstly you'll need to log in. To do this, click on the customer's section and create an account. Once logged in, click on the Your Account tab.

The Your Account section gives you the ability to change your information such as username, email address and password. You'll notice the username and email fields pre-filled in with your information.

We'll start by investigating how this information gets pre-filled. If you open your browser developer tools, select the network tab and then refresh the page, you'll see a call to an endpoint with the path /api/v1/customer?id={user_id}.

This page returns in JSON format your user id, username and email address. We can see from the path that the user information shown is taken from the query string's id parameter (see below image).



Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	10-10-210-133.p.thmlabs.com	account	document	html	1.86 kB	5.13 kB
200	GET	pro.fontawesome.com	all.css	stylesheet	css	32.06 kB	166.57 kB
200	GET	10-10-210-133.p.thmlabs.com	bootstrap.min.css	stylesheet	css	118.60 kB	118.36 kB
200	GET	10-10-210-133.p.thmlabs.com	style.css	stylesheet	css	6.51 kB	6.26 kB
200	GET	10-10-210-133.p.thmlabs.com	jquery.min.js	script	js	87.64 kB	87.38 kB
200	GET	10-10-210-133.p.thmlabs.com	bootstrap.min.js	script	js	36.44 kB	36.18 kB
200	GET	10-10-210-133.p.thmlabs.com	site.js	script	js	668 B	408 B
200	GET	10-10-210-133.p.thmlabs.com	customer?id=13	account:1 (xhr)	json	363 B	51 B
404	GET	10-10-210-133.p.thmlabs.com	favicon.ico	FaviconLoader.jsm:191 (img)	html	1.16 kB	2.14 kB
404	GET	10-10-210-133.p.thmlabs.com	favicon.ico	onloadwff.js:71 (img)	html	1.16 kB	2.14 kB

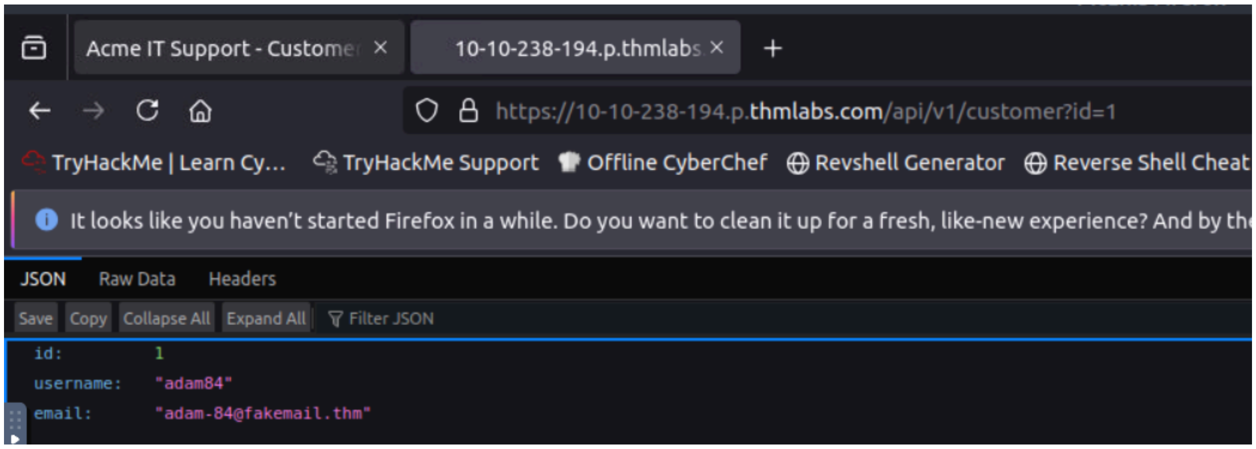
```
id: 13
username: "adam"
email: "adam@test.com"
```

You can try testing this id parameter for an IDOR vulnerability by changing the id to another user's id. Try selecting users with IDs 1 and 3 and then answer the questions below.

****

Answer the questions below:

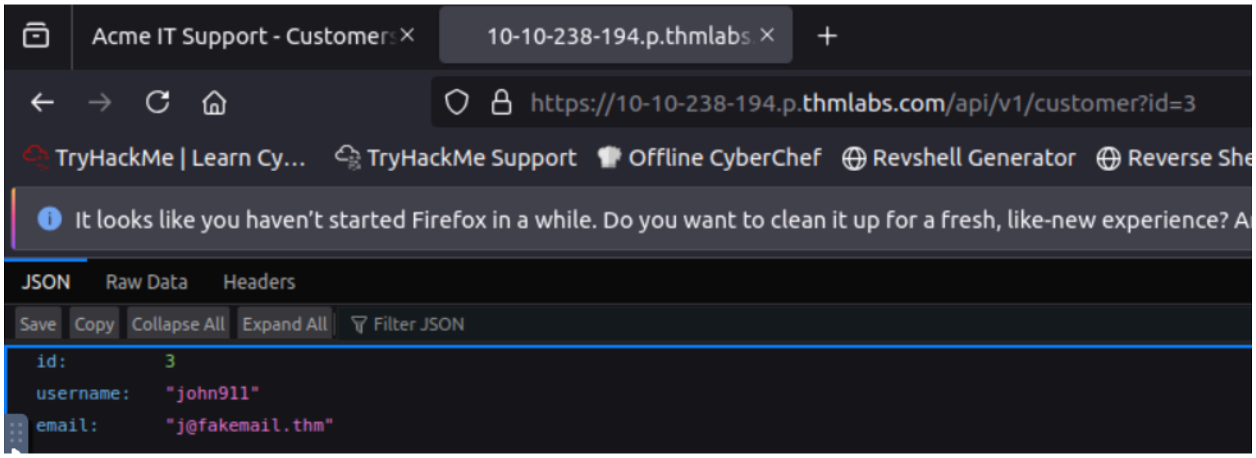
What is the username for user id 1?


Acme IT Support - Custome
10-10-238-194.p.thmlabs
https://10-10-238-194.p.thmlabs.com/api/v1/customer?id=1
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
Revshell Generator
Reverse Shell Cheat
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the
JSON
Raw Data
Headers
Save
Copy
Collapse All
Expand All
Filter JSON

```
id:         1
username:   "adam84"
email:      "adam-84@fakemail.thm"
```

Answer: adam84

What is the email address for user id 3?


Acme IT Support - Customer
10-10-238-194.p.thmlabs
https://10-10-238-194.p.thmlabs.com/api/v1/customer?id=3
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
Revshell Generator
Reverse She
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? A
JSON
Raw Data
Headers
Save
Copy
Collapse All
Expand All
Filter JSON

```
id:         3
username:   "john911"
email:      "j@fakemail.thm"
```

Answer: j@fakemail.thm