

THM-IDOR（不安全的直接对象引用）-学习

本文相关的TryHackMe实验房间链接：<https://tryhackme.com/room/idor>

H2 概念

什么是IDOR

IDOR 代表不安全的直接对象引用，是访问控制漏洞的一种类型（IDOR越权漏洞，属于授权逻辑型漏洞）。

当 Web 服务器接收用户提供的输入来检索对象(文件、数据、文档)时，如果对用户输入数据的信任度过高，且在服务器端没有进行验证来确认"所请求的对象"是否属于"有权请求它的用户"，那么这种类型的漏洞就有可能发生:使你能够访问不应该拥有的文件、数据、文档等对象。

答题

Answer the questions below 回答下面的问题

What does IDOR stand for? IDOR 代表什么？

Insecure Direct Object Reference

Correct Answer 正确答案

H2 IDOR示例

假设你刚刚注册了一项在线服务，你现在想要更改你的个人资料信息，你点击的链接会进入 http://online-service.thm/profile?user_id=1305 页面，你可以看到你的个人资料信息。

你的好奇心占了上风，于是你尝试将 user_id 值更改为1000(http://online-service.thm/profile?user_id=1000)，令你惊讶的是，你现在可以看到ID为1000的用户的个人信息，你现在已经发现了一个 IDOR 漏洞！在理想情况下，网站上应该有一个检查机制，以确认某个ID相关的一些信息 只有当前所登录的 对应ID的用户才能访问。

答题

利用你上面学到的知识，点击查看TryHackMe网站在本页面所提供的站点按钮，通过发现和利用 IDOR 漏洞（修改url中的数值）来尝试接收一个标志。



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

Now you can view your order confirmation, which contains your details.


Try changing the URL below to view order number 1000 (press enter to load the new URL)

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

Order : 1234

Harry A Howe
97 Church Way
BRAISEWORTH
IP23 1HB

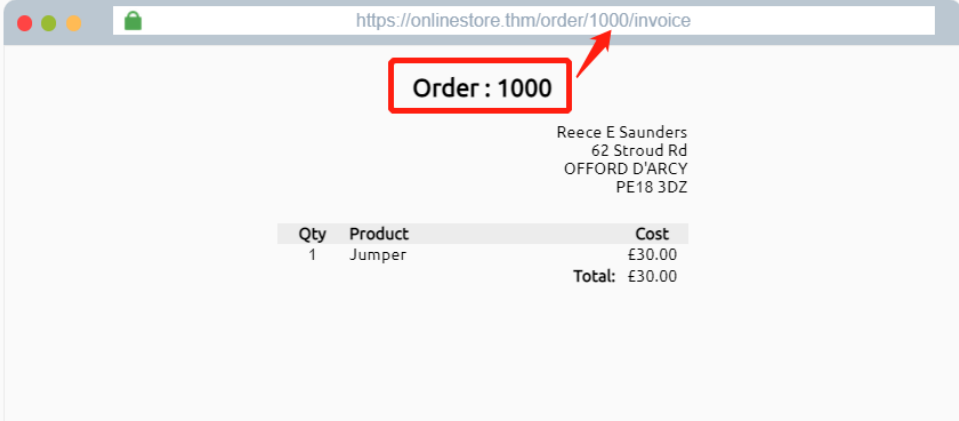
Qty	Product	Cost
1	T-Shirt	£12.30
1	Jeans	£19.99
Total:		£32.29

 IDOR Example

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}



Answer the questions below 回答下面的问题

What is the Flag from the IDOR example website? IDOR 示例网站的标志是什么？

THM{IDOR-VULN-FOUND}

Correct Answer 正确答案

H2 在编码后的IDs中寻找IDOR漏洞

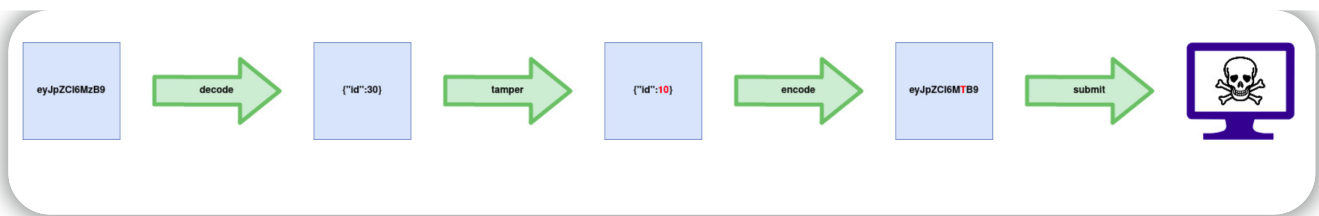
编码过的IDs (Encoded IDs)

将数据从一个页面传递到另一个页面，或者发布数据、查询字符串或 cookie 的时候，网页开发人员通常会首先获取原始数据并对其进行编码处理，编码能确保接收到信息的web服务器能够理解收到的内容（不经过编码处理的数据 是web服务器理解不了的）。

编码技术通常使用 `a-z`, `A-Z`, `0-9` and `=` 字符进行填充，将二进制数据更改为 ASCII 字符串形式。Web 上最常用的编码技术是 base64 编码，这种编辑方式通常很容易识别。

你可以使用像 <https://www.base64decode.org/> 的网站来解码base64字符串，然后重新编辑数据并使用 <https://www.base64encode.org/> 网站再重新进行一次base64编码，然后重新提交 Web 请求，看看响应消息中是否有变化。

下图是解码并重新编码过程的一个图形示例:



答题

Answer the questions below 回答下面的问题

What is a common type of encoding used by websites? 网站常用的编码方式是什么?

base64

Correct Answer 正确答案

H2 在hash加密的IDs中寻找IDOR漏洞

哈希加密过的IDs (Hashed IDs)

处理哈希加密之后的ID 要比 处理编码后的ID稍微复杂一些，但它们可能遵循一种可预测的模式，例如整数值的hash版本，例如，如果使用 md5散列(哈希)算法，ID 号123将变成 202cb962ac59075b964b07152d234b70 。

你可以将你发现的哈希值放入在线网站，如 <https://crackstation.net/> (它有一个数十亿散列值结果的数据库) 看看能不能找到匹配的。

答题

Answer the questions below 回答下面的问题

What is a common algorithm used for hashing IDs? 哈希加密ID的常用算法是什么?

md5

Correct Answer 正确答案

H2 在不可预测的ID中寻找IDOR漏洞

不可预测的IDs

如果使用上述方法无法检测到 Id，那么检测IDOR漏洞的一个很好的方法是创建两个帐户并交换它们的 Id 号。

如果你可以直接使用其他用户的 ID 号查看其他用户的内容，同时仍然在使用 "非此ID对应的帐户" 登录(或者根本没有登录)，那么你就发现了一个IDOR 漏洞。

答题

What is the minimum number of accounts you need to create to check for IDORs between accounts? 你需要创建多少个帐户来检查帐户之间是否存在 IDOR 漏洞?

2

Correct Answer 正确答案

H2 IDOR漏洞一般位于哪里？

你所针对的易受攻击的点 可能并不总是你在地址栏中看到的東西，它可以是浏览器通过 AJAX 请求加载的内容，也可以是 JavaScript 文件中引用的内容。

有时，易受攻击的点可能有一个未引用的参数，这个参数在开发期间可能有用，并被推到生产环境中。

例如，你可能会注意到显示用户信息时调用的是 `/user/details`（通过你的会话验证），但是，通过名为参数挖掘的攻击，也许能够发现一个名为 `user_id` 的未引用参数，你可以使用该参数显示其他用户的信息，如 `/user/details?user_id=123`。

H2 一个实际的IDOR示例

打开TryHackMe网站在该知识点页面 提供的链接。

首先你需要登录，为此，单击客户部分并创建一个帐户。登录后，单击“你的帐户”选项卡。

Your Account 部分允许你更改用户名、电子邮件地址和密码等信息。你会注意到用户名和电子邮件字段预先填写了你注册账户时填的信息。

我们先调查一下这些信息是如何预先填写的，如果打开浏览器开发人员工具（F12），选择网络（network）选项卡，然后刷新页面，你将看到一个对端点的调用，路径为 `/api/v1/customer?id={user_id}`。

此页面以 JSON 格式返回你的用户 ID、用户名和电子邮件地址。我们可以从路径中看到，所显示的用户信息来自查询字符串的 `id` 参数(见下图)

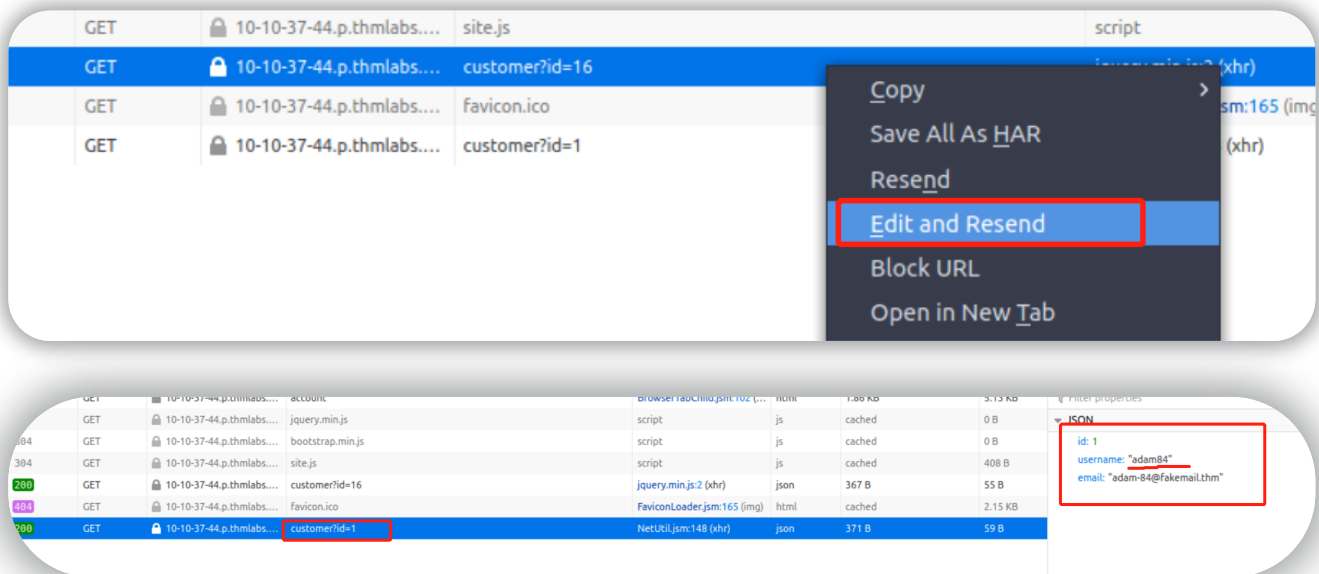
Status	Method	Domain	File	Initiator	Type	Transferred	Size	Headers	Cookies	Request	Response
200	GET	10-10-210-133.p.thmlabs.com	account	document	html	1.86 kB	5.13 kB				
200	GET	pro.fontawesome.com	all.css	stylesheet	css	32.06 kB	166.57 kB				
200	GET	10-10-210-133.p.thmlabs.com	bootstrap.min.css	stylesheet	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	olite.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	id: 13 username: "adam" email: "adam@test.com"			
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				

你可以通过将 `id` 更改为另一个用户的 `id` 来测试这个 `id` 参数是否存在 IDOR 漏洞，尝试选择 ID 为1和3的用户，然后回答下面的问题。

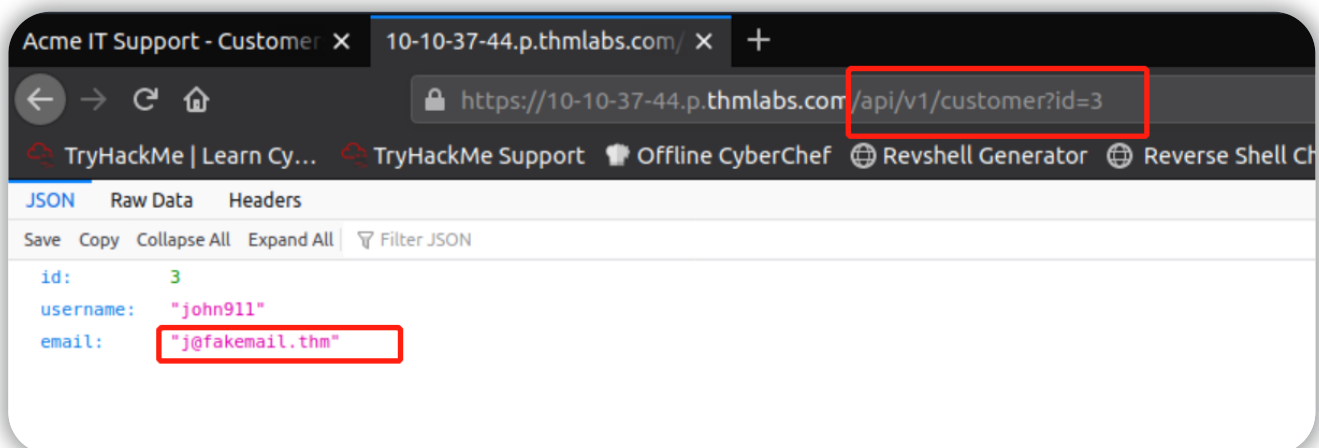
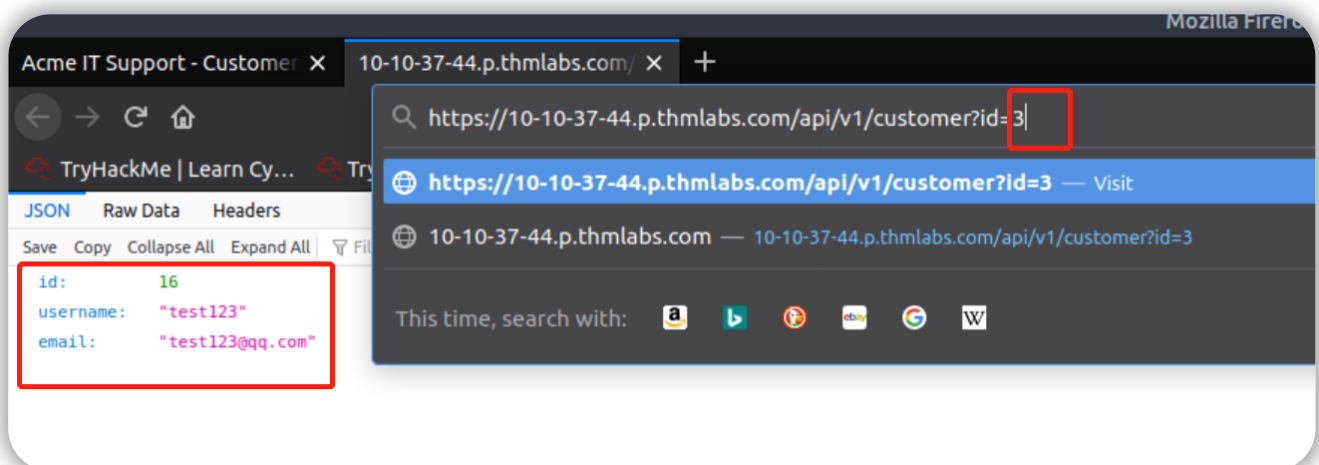
答题

建议使用火狐浏览器，使用TryHackMe网站提供的Attack Box即可。

选中有效记录修改并重新发送：



双击有效记录，进入对应的页面并直接修改url：



Answer the questions below 回答下面的问题

What is the username for user id 1? 用户 id 1 的用户名是什么?

adam84

Correct Answer 正确答案

What is the email address for user id 3? 用户 id3 的电子邮件地址是什么?

j@fakemail.thm

Correct Answer 正确答案