

IDOR

Görev 1 IDOR nedir?

Bu odada, IDOR güvenlik açığının ne olduğunu, neye benzediğini, nasıl bulunacağını ve gerçek bir senaryodan yararlanarak pratik bir görevi öğreneceksiniz.

IDOR nedir?

IDOR, Güvensiz Doğrudan Nesne Referansı anlamına gelir ve bir tür erişim kontrolü güvenlik açığıdır.

Bu tür bir güvenlik açığı, bir web sunucusu nesneleri (dosyalar, veriler, belgeler) almak için kullanıcı tarafından sağlanan girdiyi aldığı anda, girdi verilerine çok fazla güvenildiğinde ve istenen nesnenin onu isteyen kullanıcıya ait olduğunu doğrulamak için sunucu tarafında doğrulanmadığında ortaya çıkabilir.

.soru

IDOR ne anlama geliyor?


⇒ **Insecure Direct Object Reference**

Görev 2 Bir IDOR Örneği

Bir çevrimiçi hizmete yeni kaydolduğunuzu ve profil bilgilerinizi değiştirmek istediğinizi düşünün. Tıkladığınız bağlantı http://online-service.thm/profile?user_id=1305 adresine gidiyor ve bilgilerinizi görebiliyorsunuz.

Merakınızı yenemeyip user_id değerini 1000 olarak değiştirmeyi denediniz (http://online-service.thm/profile?user_id=1000) ve sürpriz bir şekilde artık başka bir kullanıcının bilgilerini görebiliyorsunuz. Artık bir IDOR güvenlik açığı keşfettiniz! İdeal olarak, kullanıcı bilgilerinin talep eden kullanıcıya ait olduğunu doğrulamak için web sitesinde bir kontrol olmalıdır.

Yukarıda öğrendiklerinizi kullanarak Siteyi Görüntüle düğmesine tıklayın ve bir IDOR açığını keşfedip kullanarak bir bayrak almaya çalışın.

 IDOR Example

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

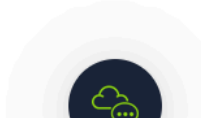
From	Subject	Date
shipping@onlinestore.thm	Order Shipped	22/07/2021 14:00
orders@onlinestore.thm	Order Confirmation	21/07/2021 12:42
noreply@tryhackme.com	Welcome To TryHackMe	18/07/2021 18:12
jo@fakemail.thm	Saturday Night	03/07/2021 08:22

Order Confirmed

Thanks for your recent online order

You can view your invoice by clicking the link below!

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





IDOR Example



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/1000/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}



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

.soru

IDOR örnek web sitesindeki Bayrak nedir?

⇒ **THM{IDOR-VULN-FOUND}**

Görev 3 Kodlanmış ID'lerdeki IDOR'ları Bulma

Kodlanmış Kimlikler (**Encoded IDs**)

Veri gönderme, sorgu dizeleri veya çerezler yoluyla sayfadan sayfaya veri aktarırken, web geliştiricileri genellikle önce ham veriyi alır ve kodlar. Kodlama, alıcı web sunucusunun içeriği anlayabilmesini sağlar. Kodlama, ikili verileri

genellikle a-z, A-Z, 0-9 ve dolgu için = karakterini kullanarak bir ASCII dizesine dönüştürür. Web'deki en yaygın kodlama tekniği base64 kodlamasıdır ve genellikle fark edilmesi oldukça kolaydır. Dizenin kodunu çözmek için <https://www.base64decode.org/> gibi web sitelerini kullanabilir, ardından verileri düzenleyebilir ve <https://www.base64encode.org/> kullanarak yeniden kodlayabilir ve ardından yanıtta bir değişiklik olup olmadığını görmek için web isteğini yeniden gönderebilirsiniz.

Bu sürecin grafiksel bir örneği olarak aşağıdaki resme bakın:



.soru

Web siteleri tarafından kullanılan yaygın kodlama türü nedir?

⇒ **base64**

Görev 4 Karışık Kimliklerde IDOR'ları Bulma

Karma Kimlikler (Hashed IDs)

Karma kimliklerle uğraşmak kodlanmış olanlardan biraz daha karmaşıktır, ancak tamsayı değerinin karma sürümü olmak gibi öngörülebilir bir model izleyebilirler. Örneğin, md5 hashing kullanılıyorsa 123 numaralı kimlik 202cb962ac59075b964b07152d234b70 olur.

Herhangi bir eşleşme bulup bulamayacağımızı görmek için keşfedilen hash'leri <https://crackstation.net/> gibi bir web hizmetine (milyarlarca hash değer sonucundan oluşan bir veritabanına sahip) koymaya değer.

.soru

Kimlikleri karma hale getirmek için kullanılan yaygın algoritma nedir?

⇒ **md5**

Görev 5 Tahmin Edilemeyen ID'lerde IDOR'ları Bulma

Öngörülemeyen Kimlikler (Unpredictable IDs)

Kimlik yukarıdaki yöntemler kullanılarak tespit edilemiyorsa, IDOR tespiti için mükemmel bir yöntem iki hesap oluşturmak ve kimlik numaralarını aralarında değiştirmektir. Farklı bir hesaba oturum açmışken (veya hiç oturum açmamışken) diğer kullanıcıların içeriğini kimlik numaralarını kullanarak görüntüleyebiliyorsanız, geçerli bir IDOR güvenlik açığı buldunuz demektir.

.soru

Hesaplar arasındaki IDOR'ları kontrol etmek için oluşturmanız gereken minimum hesap sayısı nedir?

⇒ 2

Görev 6 IDOR'lar nerede bulunuyor

Nerede bulunuyorlar?

Hedeflediğiniz savunmasız uç nokta her zaman adres çubuğunda gördüğünüz bir şey olmayabilir. Tarayıcınızın bir AJAX isteği aracılığıyla yüklediği içerik veya bir JavaScript dosyasında referans olarak bulduğunuz bir şey olabilir.

Bazen uç noktalar, geliştirme sırasında kullanılmış ve üretime aktarılmış olabilecek referanssız bir parametreye sahip olabilir. Örneğin, /user/details adresine yapılan bir çağrının kullanıcı bilgilerinizi görüntülediğini fark edebilirsiniz (oturumunuz aracılığıyla kimliğiniz doğrulanmıştır). Ancak parametre madenciliği olarak bilinen bir saldırı yoluyla, diğer kullanıcıların bilgilerini görüntülemek için kullanabileceğiniz user_id adlı bir parametre keşfedersiniz, örneğin /user/details?user_id=123.

cevap gerekmemektedir.

Görev 7 Pratik Bir IDOR Örneği

Makineyi Başlat düğmesine basarak başlayın; başladıktan sonra aşağıdaki bağlantıya tıklayın ve yeni bir tarayıcı sekmesinde açın:

https://LAB_WEB_URL.p.thmlabs.com

Öncelikle oturum açmanız gerekir. Bunu yapmak için müşteri bölümüne tıklayın ve bir hesap oluşturun. Giriş yaptıktan sonra Hesabınız sekmesine tıklayın.

Hesabınız bölümü size kullanıcı adı, e-posta adresi ve şifre gibi bilgilerinizi değiştirme olanağı sunar. Kullanıcı adı ve e-posta alanlarının bilgilerinizle önceden doldurulmuş olduğunu göreceksiniz.

Hesabınız bölümü size kullanıcı adı, e-posta adresi ve şifre gibi bilgilerinizi değiştirme olanağı sunar. Kullanıcı adı ve e-posta alanlarının bilgilerinizle önceden doldurulmuş olduğunu göreceksiniz.

Bu sayfa kullanıcı kimliğinizi, kullanıcı adınızı ve e-posta adresinizi JSON biçiminde döndürür. Gösterilen kullanıcı bilgilerinin sorgu dizesinin id parametresinden alındığını yoldan görebiliriz (aşağıdaki resme bakın).

Status	Method	Domain	File	Indicator	Type	Transferred	Size	Headers	Cookies	Request	Response	Timings	Stack Trace	Security
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 (url)	json	363 B	51 B							
200	GET	10-10-210-133.p.thmlabs.com	favicon.ico	favicon:loader:gem:191 (img)	html	1.16 kB	2.14 kB							
200	GET	10-10-210-133.p.thmlabs.com	favicon.ico	onload:off.js:71 (img)	html	1.16 kB	2.14 kB							

Bu id parametresini başka bir kullanıcının id'si ile değiştirerek bir IDOR güvenlik açığı için test etmeyi deneyebilirsiniz. ID'si 1 ve 3 olan kullanıcıları seçmeyi deneyin ve ardından aşağıdaki soruları yanıtlayın.

Acme IT Support

Customer Signup

Already have an account? [Login here.](#)

Customer Signup

Username:

deneme1

Email Address:

deneme1@gmail.com

Password:

Confirm Password:

Signup

Acme IT Support

[Home](#)
[News](#)
[Contact](#)
[Customers](#)

Dashboard

Support Tickets

Your Account

Logout

Username

Current Username:

deneme1

Inspector

Console

Debugger

Network

Style Editor

Performance

Memory

Storage

Accessibility

Application

Filter URLs

All

HTML

CSS

JS

XHR

Fonts

Images

Media

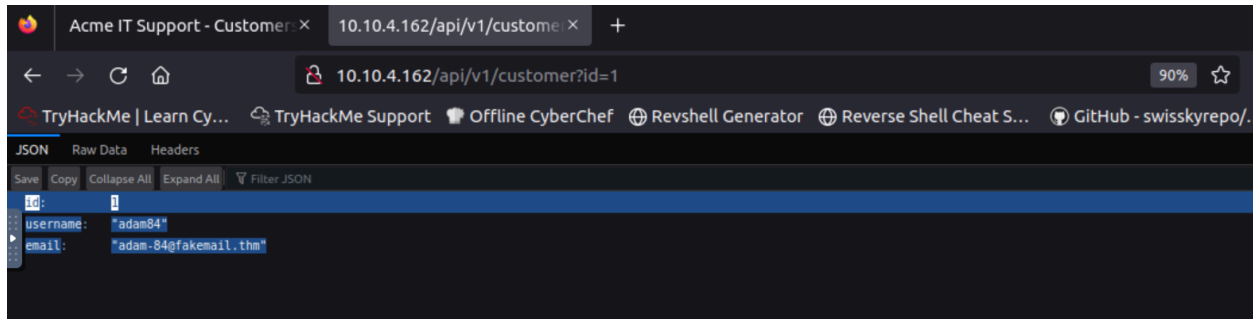
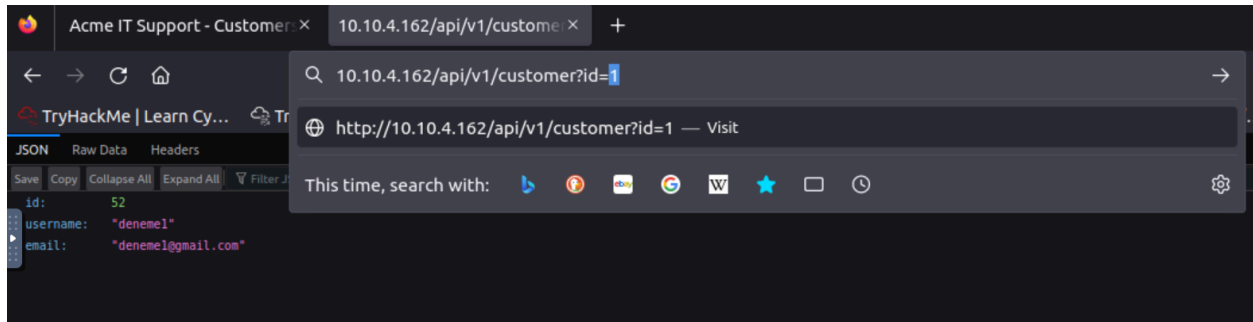
WS

Other

Disable Cache

No Throttling

Status	Method	Domain	File	Initiator	Type	Transferred	Size	0 ms	640 ms
200	GET	10.10.4.162	jquery.min.js	script	js	cached	0 B	0 ms	
200	GET	10.10.4.162	bootstrap.min.js	script	js	cached	0 B	0 ms	
200	GET	10.10.4.162	site.js	script	js	cached	408 B	0 ms	
200	GET	10.10.4.162	customerid=52	jquery.min.js:2 (xhr)	json	370 B	58 B	16 ms	



.soru

Kullanıcı kimliği 1 için kullanıcı adı nedir?

⇒ adam84

.soru

Kullanıcı kimliği 3 için e-posta adresi nedir?

⇒ j@fakemail.thm