

Vulnerabilities 101

Task 1 Introduction (Görev 1 Giriş)

Siber güvenlik günümüz dünyasında büyük bir iş. Gazetelerde duyduğumuz hack'ler, güvenlik açıklarından yararlanmaktan kaynaklanıyor. Bu odada, güvenlik açığının tam olarak ne olduğunu, güvenlik açığı türlerini ve sızma testi çabalarımızda başarı için bunlardan nasıl yararlanabileceğimizi açıklayacağız.

Sızma testinin büyük bir kısmı, karşılaştığınız her durum için gerekli becerileri ve kaynakları bilmektir. Bu oda size, özellikle güvenlik açıklarını araştırırken gerekli olan bazı kaynakları tanıtacaktır:

- Güvenlik açıkları nelerdir
- Neden öğrenmeye değer olduklarını
- Güvenlik açıkları nasıl derecelendirilir?
- Güvenlik açığı araştırması için veri tabanları
- ACKme'nin katılımında güvenlik açığı araştırmasının nasıl kullanıldığını gösteren bir vitrin

Soru ⇒ Bu görevi okuyun!

Cevap ⇒ **Cevap Gerekmemektedir.**

Task 2 Introduction to Vulnerabilities (Görev 2 Güvenlik Açıklarına Giriş)

Siber güvenlikte bir güvenlik açığı, bir sistemin veya uygulamanın tasarımında, uygulanmasında veya davranışlarında bir zayıflık veya kusur olarak tanımlanır. Bir saldırgan, yetkisiz bilgilere erişim sağlamak veya yetkisiz eylemler gerçekleştirmek için bu zayıflıklardan yararlanabilir. "Güvenlik açığı" teriminin siber güvenlik

kuruluşları tarafından birçok tanımı bulunmaktadır. Ancak, bunların hepsi arasında çok az farklılık vardır.

Örneğin, NIST bir güvenlik açığını "bir tehdit kaynağı tarafından istismar edilebilecek veya tetiklenebilecek bir bilgi sistemindeki, sistem güvenlik prosedürlerindeki, iç kontrollerdeki veya uygulamadaki zayıflık" olarak tanımlar.

Güvenlik açıkları, bir uygulamanın kötü tasarımı veya bir kullanıcının amaçlanan eylemleri gözden kaçırmaması gibi birçok faktörden kaynaklanabilir.

Çeşitli güvenlik açığı türlerini daha sonraki bir odada tartışmaya devam edeceğiz. Ancak şimdilik, tartışmasız beş ana güvenlik açığı kategorisi olduğunu bilmeliyiz:

Vulnerability (Güvenlik Açığı)	Description (Açıklama)
Operating System (İşletim Sistemi)	Bu tür güvenlik açıkları İşletim Sistemlerinde (OS) bulunur ve genellikle ayrıcalıkların artmasına neden olur.
(Mis)Configuration-based ((Yanlış) Yapılandırma tabanlı)	Bu tür güvenlik açıkları, yanlış yapılandırılmış bir uygulama veya hizmetten kaynaklanır. Örneğin, müşteri bilgilerini ifşa eden bir web sitesi.
Weak or Default Credentials (Zayıf veya Varsayılan Kimlik Bilgileri)	Kimlik doğrulama unsuruna sahip olan uygulamalar ve hizmetler, yüklendiklerinde varsayılan kimlik bilgileriyle birlikte gelirler. Örneğin, bir yönetici panosu "admin" kullanıcı adı ve parolasına sahip olabilir. Bunların bir saldırgan tarafından tahmin edilmesi kolaydır.
Application Logic (Uygulama Mantığı)	Bu güvenlik açıkları kötü tasarlanmış uygulamaların bir sonucudur. Örneğin, bir saldırganın bir kullanıcıyı taklit edebilmesine neden olabilecek kötü uygulanmış kimlik doğrulama mekanizmaları.
Human-Factor (İnsan Faktörü)	İnsan Faktörü güvenlik açıkları, insan davranışlarından yararlanan güvenlik açıklarıdır. Örneğin, ortalama e-postaları insanları kandırarak meşru olduklarına inandırmak için tasarlanmıştır.

Bir siber güvenlik araştırmacısı olarak, uygulamaları ve sistemleri değerlendiriyor olacaksınız - günlük hayatta bu hedeflere karşı güvenlik açıklarını kullanacaksınız, bu nedenle bu keşif ve istismar sürecine aşina olmak çok önemlidir.

Sorular

Soru ⇒ Bir saldırgan, sistem hesabının izinlerini "kullanıcı"dan "yönetici"ye yükseltebildi. Bu ne tür bir güvenlik açığıdır?

Cevap ⇒ **Operating System**

Soru ⇒ Kimlik doğrulamak için çerezleri kullanarak bir oturum açma panelini atlamayı başardınız. Bu ne tür bir güvenlik açığıdır?

Cevap ⇒ **Application Logic**

Task 3 Scoring Vulnerabilities (CVSS & VPR) (Görev 3 Zafiyetlerin Puanlanması (CVSS & VPR))

Zafiyet yönetimi, bir kuruluşun karşılaştığı tehditlerin (zafiyetlerin) değerlendirilmesi, sınıflandırılması ve nihayetinde giderilmesi sürecidir.

Bir ağ veya bilgisayar sistemindeki her bir güvenlik açığını yamamak ve gidermek tartışmasız imkansızdır ve bazen kaynak israfına neden olur.

Sonuçta, güvenlik açıklarının yalnızca yaklaşık %2'si istismar edilebilmektedir (Kenna security., 2020). Bunun yerine, tüm mesele en tehlikeli güvenlik açıklarını ele almak ve bir saldırı vektörünün bir sistemi istismar etmek için kullanılma olasılığını azaltmaktır.

Güvenlik açığı puanlaması bu noktada devreye girer. Güvenlik açığı puanlaması, güvenlik açığı yönetiminde hayati bir rol oynar ve bir güvenlik açığının bir ağ veya bilgisayar sistemi üzerindeki potansiyel riskini ve etkisini belirlemek için kullanılır. Örneğin, popüler Ortak Güvenlik Açığı Puanlama Sistemi (CVSS) bir güvenlik açığına özelliklerine, kullanılabilirliğine ve yeniden üretilebilirliğine göre puan verir.

Elbette, BT dünyasında her zaman olduğu gibi, hiçbir zaman tek bir çerçeve veya önerilen fikir yoktur. Şimdi en yaygın çerçevelerden ikisini inceleyelim ve nasıl farklılaştıklarını analiz edelim.

Ortak Güvenlik Açığı Puanlama Sistemi

İlk olarak 2005 yılında tanıtılan Ortak Güvenlik Açığı Puanlama Sistemi (veya CVSS), güvenlik açığı puanlaması için çok popüler bir çerçevedir ve üç ana yinelemesi vardır. Mevcut versiyon CVSSv3.1'dir (4.0 versiyonu şu anda taslak halindedir) ve bir puan esasen aşağıdaki faktörlerden bazıları (ancak çok daha fazlası) tarafından belirlenir:

1. Güvenlik açığından faydalanmak ne kadar kolay?

2. Bunun için açıklar var mı?
3. Bu güvenlik açığı CIA üçlüsünü nasıl etkiliyor?

Aslında, o kadar çok değişken vardır ki, bu çerçeveyi kullanarak puanı hesaplamak için bir hesap makinesi kullanmanız gerekir. Bir güvenlik açığına, atanan puana bağlı olarak bir sınıflandırma (beş üzerinden) verilir. Niteliksel Önem Derecesi Ölçeğini ve puan aralıklarını aşağıdaki tabloya yerleştirdim.

Rating	Score
None	0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

Ancak CVSS sihirli bir değnek değildir. CVSS'in bazı avantaj ve dezavantajlarını aşağıdaki tabloda inceleyelim:

<u>CVSS'in Avantajları</u>	<u>CVSS'in Dezavantajları</u>
CVSS uzun zamandır kullanılıyor.	CVSS hiçbir zaman güvenlik açıklarının önceliklendirilmesine yardımcı olmak için tasarlanmadı, bunun yerine sadece bir önem derecesi atadı.
CVSS kuruluşlar arasında popülerdir.	CVSS, güvenlik açıklarını ağırlıklı olarak bir istismarın mevcut olmasına göre değerlendirir. Bununla birlikte, tüm güvenlik açıklarının yalnızca %20'sinin bir istismarı mevcuttur (Tenable., 2020) .
CVSS, benimsenmesi ücretsiz bir çerçevedir ve NIST gibi kuruluşlar tarafından tavsiye edilmektedir.	Güvenlik açıkları, istismarlar gibi yeni gelişmeler bulunabilmesine rağmen, değerlendirmeden sonra puanlamayı nadiren değiştirir.

Güvenlik Açığı Öncelik Derecelendirmesi (VPR)

VPR çerçevesi, güvenlik açığı yönetiminde çok daha modern bir çerçevedir - güvenlik açığı yönetimi için bir endüstri çözümleri sağlayıcısı olan Tenable tarafından geliştirilmiştir. Bu çerçevenin risk odaklı olduğu düşünülmektedir; yani

güvenlik açıklarına, etki gibi faktörlerden ziyade (CVSS'de olduğu gibi) bir güvenlik açığının kuruluşun kendisi için oluşturduğu riske odaklanan bir puan verilir.

CVSS'den farklı olarak, VPR puanlaması bir güvenlik açığının alaka düzeyini dikkate alır. Örneğin, bir güvenlik açığı kuruluş için geçerli değilse (yani, güvenlik açığı olan yazılımı kullanmıyorlarsa), bu güvenlik açığıyla ilgili hiçbir risk dikkate alınmaz. VPR'nin puanlaması da oldukça dinamiktir; bir güvenlik açığının oluşturabileceği risk, yaşlandıkça neredeyse her gün değişebilir.

VPR, CVSS ile benzer bir puanlama aralığı kullanır ve ben de bunu aşağıdaki tabloya ekledim. Bununla birlikte, iki önemli fark, VPR'nin "Hiçbiri/Bilgilendirici" kategorisine sahip olmaması ve VPR'nin farklı bir puanlama yöntemi kullanması nedeniyle, aynı güvenlik açığı VPR kullanıldığında CVSS kullanıldığında olduğundan farklı bir puana sahip olacaktır.

Rating	Score
Low	0.0 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

VPR çerçevesini kullanmanın bazı avantaj ve dezavantajlarını aşağıdaki tabloda özetleyelim.

<u>VPR'nin Avantajları</u>	<u>Disadvantages of VPR</u>
VPR, gerçek dünyaya uygun modern bir çerçevedir.	VPR, diğer bazı güvenlik açığı yönetim çerçeveleri gibi açık kaynaklı değildir.
VPR, riski hesaplarken 150'den fazla faktörü göz önünde bulundurur.	VPR yalnızca ticari bir platform dışında benimsenebilir.
VPR risk odaklıdır ve kuruluşlar tarafından güvenlik açıklarının yamalanmasına öncelik verilmesine yardımcı olmak için kullanılır.	VPR, CVSS'in yaptığı ölçüde CIA üçlüsünü dikkate almaz; yani verilerin gizliliği, bütünlüğü ve kullanılabilirliğine yönelik risk, VPR kullanılırken güvenlik açıklarının puanlanmasında büyük bir faktör oynamaz.

Puanlamalar nihai değildir ve çok dinamikdir, yani bir güvenlik açığına verilmesi gereken öncelik, güvenlik açığı yaşlandıkça değişebilir.	Kasıtlı olarak boş bırakılmıştır.
--	-----------------------------------

Sorular

Soru ⇒ CVSS'in ilk yinelemesi hangi yıl yayınlandı?

Cevap ⇒ 2005

Soru ⇒ Güvenlik açığını bir kuruluş için oluşturduğu riske göre değerlendirmek isteseydiniz, hangi çerçeveyi kullanırdınız?

Not: Burada kısaltmayı arıyoruz.

Cevap ⇒ VPR

Soru ⇒ Ücretsiz ve açık kaynaklı bir çerçeve kullanmak isteseydiniz, bu hangi çerçeve olurdu?

Not: Burada kısaltmayı arıyoruz.

Cevap ⇒ CVSS

Task 4 Vulnerability Databases (Görev 4 Güvenlik Açığı Veritabanları)

Siber güvenlik yolculuğunuz boyunca sık sık çok sayıda farklı uygulama ve hizmetle karşılaşacaksınız. Örneğin, bir CMS'nin hepsi aynı amaca sahip olsa da, genellikle çok farklı tasarım ve davranışlara (ve dolayısıyla potansiyel olarak farklı güvenlik açıklarına) sahiptir.

Neyse ki internette her türlü yazılım, işletim sistemi ve daha fazlası için güvenlik açıklarını takip eden kaynaklar var! Bu oda, bilgi güvenliği yolculuğumuzda keşfedilen uygulamalar için mevcut güvenlik açıklarını aramak için kullanabileceğimiz iki veritabanını, özellikle aşağıdaki web sitelerini sergileyecektir:

1. NVD (National Vulnerability Database). (NVD (Ulusal Güvenlik Açığı Veritabanı))
2. Exploit-DB

Bu iki kaynağa geçmeden önce, bazı temel anahtar terimleri aynı şekilde anladığımızdan emin olalım:

<u>Terim</u>	<u>Tanım</u>
Vulnerability (Güvenlik Açığı)	Güvenlik açığı, bir sistem veya uygulamanın tasarım, uygulama veya davranışlarındaki bir zayıflık veya kusur olarak tanımlanır.
Exploit (İstismar)	Bir istismar, bir sistem veya uygulamadaki bir güvenlik açığını kullanan bir eylem veya davranış gibi bir şeydir.
Proof of Concept (PoC) (Kavram Kanıtı (PoC))	PoC, genellikle bir güvenlik açığının istismarını gösteren bir teknik veya araçtır.

NVD – National Vulnerability Database

Ulusal Güvenlik Açığı Veritabanı, kamuya açık olarak kategorize edilmiş tüm güvenlik açıklarını listeleyen bir web sitesidir. Siber güvenlikte, güvenlik açıkları "Ortak Güvenlik Açıkları ve Maruziyetler" (veya kısaca CVE) altında sınıflandırılır.

Bu CVE'ler CVE-YEAR-IDNUMBER biçimlendirmesine sahiptir. Örneğin, ünlü kötü amaçlı yazılım WannaCry'ın kullandığı güvenlik açığı CVE-2017-0144 idi.

NVD, kategoriye ve gönderildiği aya göre filtreler kullanarak onaylanmış tüm CVE'leri görmenizi sağlar. Örneğin, Ağustos ayına gireli üç gün oldu; bu veritabanına şimdiden 223 yeni CVE gönderildi.

VULNERABILITIES

August 2021

Below is a list of CVEs for the selected month.

NOTE: The CVEs shown below have a **release date** in the year and month chosen. The CVE ID may show a year value that does not match the release date, however, the release date will fall within the chosen year and month.

223 entries found for August 2021

CVE-2021-32066	CVE-2017-18113	CVE-2021-35477	CVE-2021-34556	CVE-2021-3351	CVE-2021-24371
CVE-2021-24425	CVE-2021-24428	CVE-2021-24430	CVE-2021-24443	CVE-2021-24444	CVE-2021-24448
CVE-2021-24450	CVE-2021-24455	CVE-2021-24456	CVE-2021-24457	CVE-2021-24458	CVE-2021-24459
CVE-2021-24460	CVE-2021-24461	CVE-2021-24462	CVE-2021-24463	CVE-2021-24464	CVE-2021-24468
CVE-2021-24470	CVE-2021-24472	CVE-2021-24473	CVE-2021-24474	CVE-2021-24476	CVE-2021-24477
CVE-2021-24478	CVE-2021-24479	CVE-2021-24480	CVE-2021-24481	CVE-2021-24483	CVE-2021-24484
CVE-2021-24488	CVE-2021-24492	CVE-2021-24496	CVE-2021-24498	CVE-2021-24503	CVE-2021-24504
CVE-2021-33526	CVE-2021-33527	CVE-2021-34574	CVE-2021-34575	CVE-2021-37165	CVE-2021-37216
CVE-2021-20332	CVE-2021-37160	CVE-2021-37161	CVE-2021-37162	CVE-2021-37163	CVE-2021-37164




Bu web sitesi yeni güvenlik açıklarını takip etmeye yardımcı olsa da, belirli bir uygulama veya senaryo için güvenlik açıklarını ararken harika değildir.

Exploit-DB

Exploit-DB, hackerlar olarak bir değerlendirme sırasında çok daha yararlı bulacağımız bir kaynaktır. Exploit-DB, yazılım ve uygulamalar için yazılım veya uygulamanın adı, yazarı ve sürümü altında saklanan açıkları tutar.

Exploit-DB'yi belirli bir güvenlik açığından yararlanmak için kullanılan kod parçacıklarını (Kavram Kanıtı olarak bilinir) aramak için kullanabiliriz.

EXPLOIT
DATABASE
























☐ Verified ☐ Has App

▼ Filters

↕ Reset All

Show 15

Search:

Date	D	A	V	Title	Type	Platform	Author
2021-08-03				Hotel Management System 1.0 - Cross-Site Scripting (XSS) Arbitrary File Upload Remote Code Execution (RCE)	WebApps	PHP	Merbin Russel
2021-08-02				Panasonic Sanyo CCTV Network Camera 2.03-0x - 'Disable Authentication / Change Password' CSRF	WebApps	Hardware	LiquidWorm
2021-08-02				Online Hotel Reservation System 1.0 - 'Multiple' Cross-site scripting (XSS)	WebApps	PHP	Mohammad Koochaki
2021-08-02				Neo4j 3.4.18 - RMI based Remote Code Execution (RCE)	Remote	Java	Christopher Ellis
2021-08-02				Men Salon Management System 1.0 - SQL Injection Authentication Bypass	WebApps	PHP	Akshay Khanna
2021-07-29				Oracle Fatwire 6.3 - Multiple Vulnerabilities	WebApps	Multiple	J. Francisco Bolivar
2021-07-29				CloverDX 5.9.0 - Cross-Site Request Forgery (CSRF) to Remote Code Execution (RCE)	WebApps	Java	niebardzo
2021-07-29				Care2x Integrated Hospital Info System 2.7 - 'Multiple' SQL Injection	WebApps	PHP	securityforeveryone.com
2021-07-29				IntelliChoice eFORCE Software Suite 2.5.9 - Username Enumeration	WebApps	ASPX	LiquidWorm
2021-07-29				Longjing Technology BEMS API 1.21 - Remote Arbitrary File Download	WebApps	Hardware	LiquidWorm
2021-07-29				Denver IP Camera SHO-110 - Unauthenticated Snapshot	WebApps	Hardware	Ivan Nikolsky

Sorular

Soru ⇒ NVD'yi kullanarak, Temmuz 2021'de kaç CVE yayınlandı (İpucu ⇒ "Arama Türü "nü Gelişmiş olarak değiştirin, uygun Yayın Tarihi Aralığını belirtin ve Ara düğmesine basın.)?

Cevap ⇒ 1554

Soru ⇒ Exploit-DB'nin yazarı kimdir?

Cevap ⇒ Offsec

Task 5 An Example of Finding a Vulnerability (Görev 5 Bir Güvenlik Açığı Bulma Örneği)

Bu görevde, küçük bir güvenlik açığı bulma sürecini göstereceğim ve güvenlik açığı veritabanlarında biraz araştırma yaparak sonuçta çok daha değerli bir güvenlik açığı ve istismara yol açacağım.


Bir değerlendirme boyunca, sonuç almak için genellikle birden fazla güvenlik açığını birleştirirsiniz. Örneğin, bu görevde, bir uygulamanın sürümünü bulmak için "Sürüm İfşası" güvenlik açığından yararlanacağız. Bu sürümle, belirli bir sürümle çalışan herhangi bir istismarı aramak için Exploit-DB'yi kullanabiliriz.

Uygulamalar ve yazılımlar genellikle bir sürüm numarasına sahiptir. Bu bilgi genellikle iyi niyetle bırakılır; örneğin, yazar yazılımın birden fazla sürümünü ve benzerlerini destekleyebilir. Ya da bazen, kasıtsız olarak bırakılır.


Örneğin, aşağıdaki ekran görüntüsünde bu uygulamanın adının ve sürüm numarasının "Apache Tomcat 9.0.17" olduğunu görebiliriz

[Home](#) [Documentation](#) [Configuration](#) [Examples](#) [Wiki](#) [Mailing Lists](#) [Find Help](#)

Apache Tomcat/9.0.17



If you're seeing this, you've successfully installed Tomcat. Congratulations!



Recommended Reading:
[Security Considerations How-To](#)
[Manager Application How-To](#)
[Clustering/Session Replication How-To](#)

[Server Status](#)
[Manager App](#)
[Host Manager](#)

Developer Quick Start
[Tomcat Setup](#) [Realms & AAA](#) [Examples](#) [Servlet Specifications](#)
[First Web Application](#) [JDBC DataSources](#) [Tomcat Versions](#)

Managing Tomcat
For security, access to the [manager webapp](#) is restricted. Users are defined in:
`$CATALINA_HOME/conf/tomcat-users.xml`
In Tomcat 9.0 access to the manager application is split between different users.
[Read more...](#)
[Release Notes](#)
[Changelog](#)
[Migration Guide](#)
[Security Notices](#)

Documentation
[Tomcat 9.0 Documentation](#)
[Tomcat 9.0 Configuration](#)
[Tomcat Wiki](#)
Find additional important configuration information in:
`$CATALINA_HOME/RUNNING.txt`
Developers may be interested in:
[Tomcat 9.0 Bug Database](#)
[Tomcat 9.0 JavaDocs](#)
[Tomcat 9.0 SVN Repository](#)

Getting Help
[FAQ and Mailing Lists](#)
The following mailing lists are available:

[tomcat-announce](#)
Important announcements, releases, security vulnerability notifications. (Low volume).

[tomcat-users](#)
User support and discussion

[taglibs-user](#)
User support and discussion for [Apache Taglibs](#)

[tomcat-dev](#)
Development mailing list, including commit messages

Elimizdeki bu bilgilerle, "Apache Tomcat 9.0.17" için geçerli olabilecek açıkları aramak için Exploit-DB'deki arama filtresini kullanalım.

The screenshot shows the Exploit-DB search results for 'Tomcat 9.0'. The search bar at the top right contains 'Tomcat 9.0'. Below the search bar, there are filters for 'Verified' and 'Has App'. The results table shows 5 entries, with the first three being marked as 'Not Verified' (red X) and the last two as 'Verified' (green checkmark). The table columns are Date, D, A, V, Title, Type, Platform, and Author.

Date	D	A	V	Title	Type	Platform	Author
2021-07-13			X	Apache Tomcat 9.0.0.M1 - Cross-Site Scripting (XSS)	WebApps	Multiple	Central InfoSec
2021-07-13			X	Apache Tomcat 9.0.0.M1 - Open Redirect	WebApps	Multiple	Central InfoSec
2020-01-08			X	Tomcat proprietaryEvaluate 9.0.0.M1 - Sandbox Escape	WebApps	Java	hantwister
2017-10-09			✓	Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2)	WebApps	JSP	intx0x80
2017-09-20			X	Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (1)	WebApps	Windows	xxlegend

Showing 1 to 5 of 5 entries (filtered from 44,305 total entries)

Harika! Exploit-DB'yi araştırdıktan sonra, uygulamanın bu özel sürümü için bizim için yararlı olabilecek toplam beş açık var.

Soru ⇒ Bu örnekte uygulamanın adını ve sürümünü bulmak için ne tür bir güvenlik açığı kullandık?

Cevap ⇒ **Version Disclosure**

Task 6 Showcase: Exploiting Ackme's Application (Görev 6 Vitrin: Ackme Uygulamasından Yararlanma)

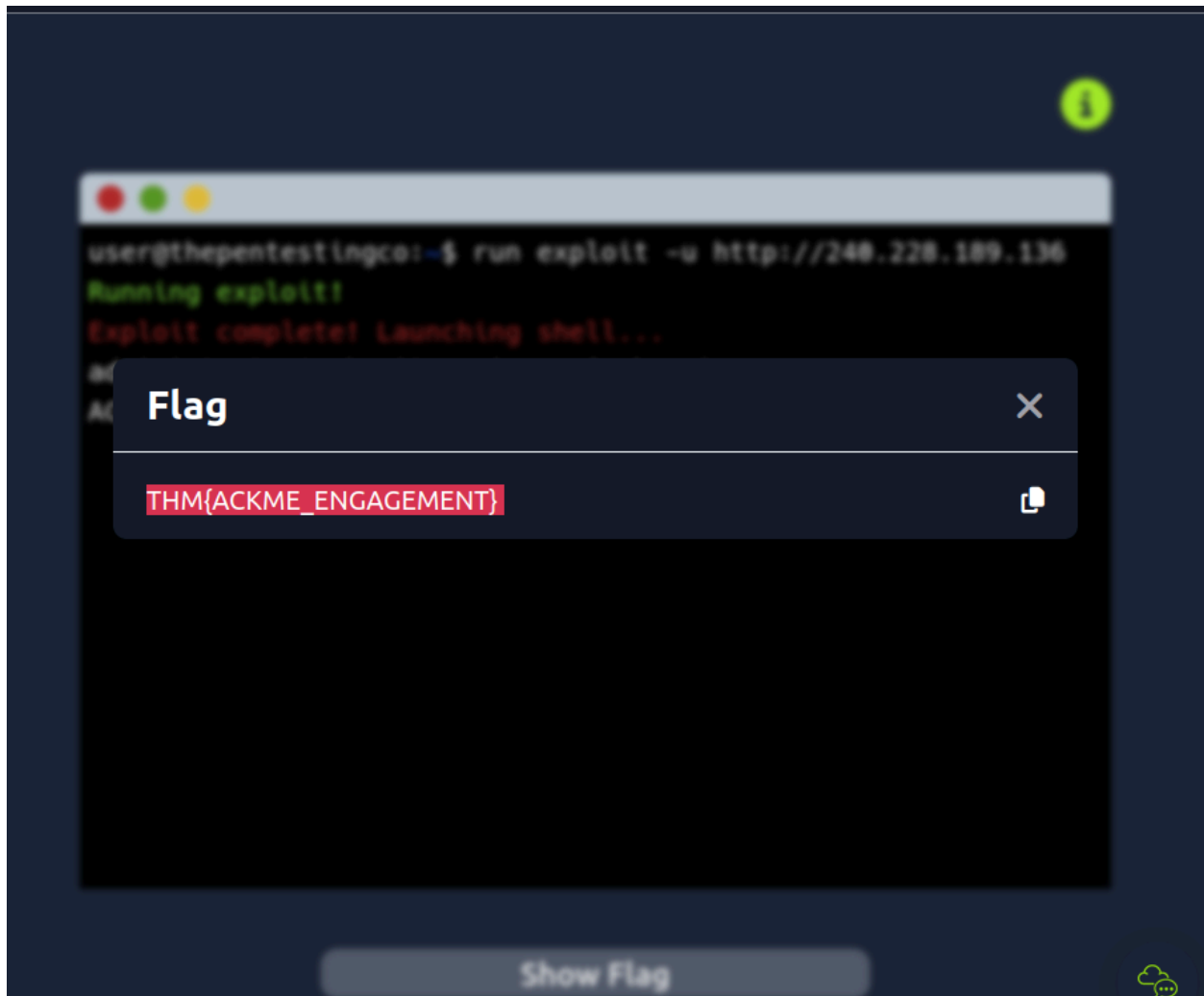
Jr. olarak işteki ilk haftanız. ThePentestingCo'da Sızma Test Uzmanı olarak ilk haftanız. İlk göreviniz için, şirket içinde bir Sızma Test Uzmanının gölgesi olacaksınız.

Bu göreve ekli siteyi dağıtın ve ACKme IT Service'in altyapısına karşı bir güvenlik açığından yararlanmak için Kıdemli Sızma Test Uzmanının attığı adımları izleyin.

Bir bayrağı geri almak için görevi tamamlayın.

Soru ⇒ Bir bayrağı almak için ACKme'nin uygulamasından sonuna kadar yararlanma vitrini ile birlikte izleyin. Bu bayrak nedir?

Cevap ⇒ **THM{ACKME_ENGAGEMENT}**



Task 7 Conclusion (Görev 7 Sonuç)

İyi işti! Sonuna kadar geldik. Bu oda, güvenlik açığı araştırmasına ve bunun gerektirdiği bazı beceri ve kaynaklara giriş niteliğinde olup, bu bilgileri pratik olarak uyguladığınız bir yer olmuştur.

Bu modüldeki ek odalar ile öğreniminize devam edin.

Soru ⇒ Bir sonraki modüle devam edin.

Cevap ⇒ **Cevap Gerekmemektedir.**