Gelişmiş Pentest Sızma Testi Hizmeti

Güvenlik Test Hizmetleri

NETAŞ

2024

Sızma Testi, sistemler üzerinde insan, mantıksal ve kodlama hatalarından kaynaklanan zafiyetlerin tespit edilmesi ve tespit edilen bu zafiyetlerin bilinen tüm yollar denenerek istismar edilmesiyle sistemlere yetkisiz erişim sağlanması şeklinde gerçekleştirilen güvenlik denetimine verilen isimdir.

Amaç, güvenlik zafiyetini bulmakla yetinmeyip, bulunan açıklığı istismar ederek, sistemlerde erişimler elde etmek ve bunun kanıtlanması; söz konusu güvenlik açıklıklarının kötü niyetli kişiler tarafından istismar edilmeden önce tespit edilerek, bertaraf edilmesi ve sistemlerin daha güvenli hale getirilmesidir.

www.netas.com.tr

Sızma Testi Hizmetlerimiz

- Web ve Mobil Uygulama Sızma Testleri
- Dahili ve Harici Ağ Sızma Testleri
- Kablosuz Ağ Sızma Testleri
- IoT, Kiosk, ATM Sızma Testleri
- Cloud, Docker Sızma Testleri
- API/Endpoint Client Sızma Testleri
- Red Team ve Sosyal Mühendislik Testleri
- DDoS Saldırı Simülasyon Testleri

NETAS

Sızma Testi Hizmetine Neden İhtiyaç Var?

- Saldırganların (Hacker) sahip olduğu motivasyon, bilişim uzmanlarının sahip olduğu motivasyonun üstündedir. Bu sebeple saldırıya dayalı bir güvenlik bakış açısı olmadan yapılan güvenlik değerlendirmelerinin eksik kalması
- Dünyada artan siber saldırılar ve kritik veri sızıntıları ile kurumların yaşadığı prestij ve maddi kayıplar
- DDoS saldırıları ile Kritik sistemlerde yaşanan Hizmet kesintileri
- Kurum personellerinin yetkinlik/farkındalık eksiklikleri
- Regülasyonlar gereği Kurumların Sızma Testi Hizmeti alım zorunluluğu, ISO 27001, PCI DSS, BDDK, EPDK, HIPAA
- Web ve Mobil Uygulama geliştirme aşamalarında, Ağ altyapısı ve Sunucu Sistemlerin canlı ortamlara alınmadan önceki son aşamalarında Sızma Testleri ''Zaruri proje adımlarından birisi'' haline gelmiş olması.

NETAS

Sızma Testi Sonrası Hangi Çıktıları Sağlıyoruz?

- Kurumun yetkili kullanıcılarının bilerek ya da bilmeden yapabilecekleri zararlı aktivitelerin tespiti
- Kötü niyetli diğer kullanıcıların (hacker) iç ve dış ağ üzerinden gerçekleştirilebileceği saldırılara karşı kurumun güvenlik seviyesinin ölçülmesi
- İnternet üzerinden kurum hakkında elde edilebilien hassas bilgilerin tespiti ile istihbarat bilgi paylaşımı
- Ele geçirilen sistemler üzerinden daha kritik bilgilere ulaşılıp ulaşılmadığının tespiti
- Sosyal Mühendislik Saldırılarına karşı kurum çalışanlarının farkındalığının ölçülmesi
- Kurumun, Regülasyonlara göre Güvenlik uyumluluk durumunun ölçülmesi
- Sızma Testi Raporlarını, Teknik ve Yönetim raporu olarak 2 farklı bölümde sunuyoruz.

NETAS

www.netas.com.tr

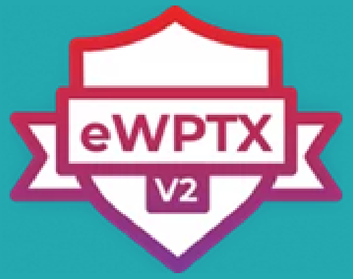
Ekip Uzmanlık Sertifikalarımız

Çeşitli yetkinliklere, geçmişe ve konusundaki uluslararası sertifikasyonlara sahip araştırmacıları sürece dahil ediyoruz.

GPEN
(GIAC Penetration Tester)

OSCP
(Offensive Security Certified Professional)

Red Team
(Certified Red Team Operator**)**



eWPTX v2
(Web Application Penetration Tester)

eMAPT
(Mobile Application Penetration Tester)

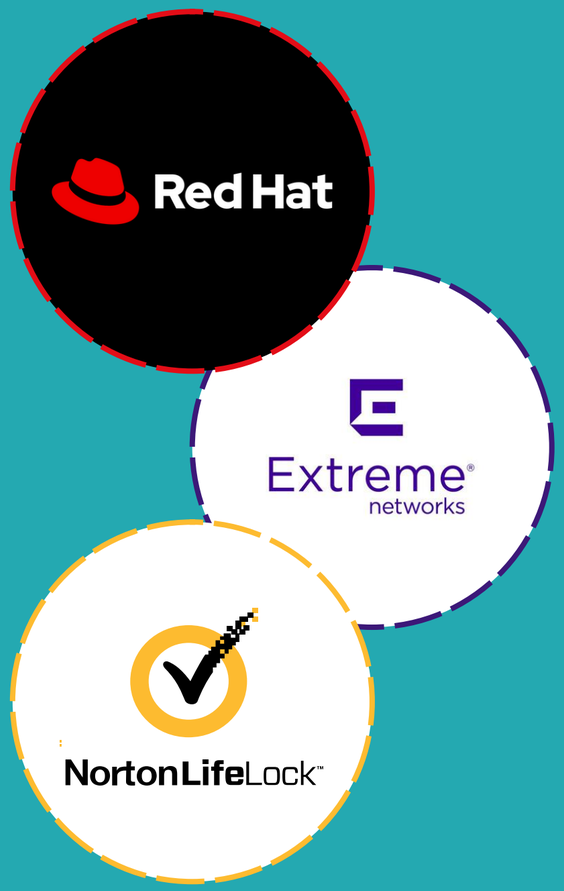
CEH
(Certified Ethical Hacker)

TSE B Seviye Onaylı Sızma Testi Firması

ITIL-F (Information Technologies Infrastructure Library**)**

NETAS

www.netas.com.tr



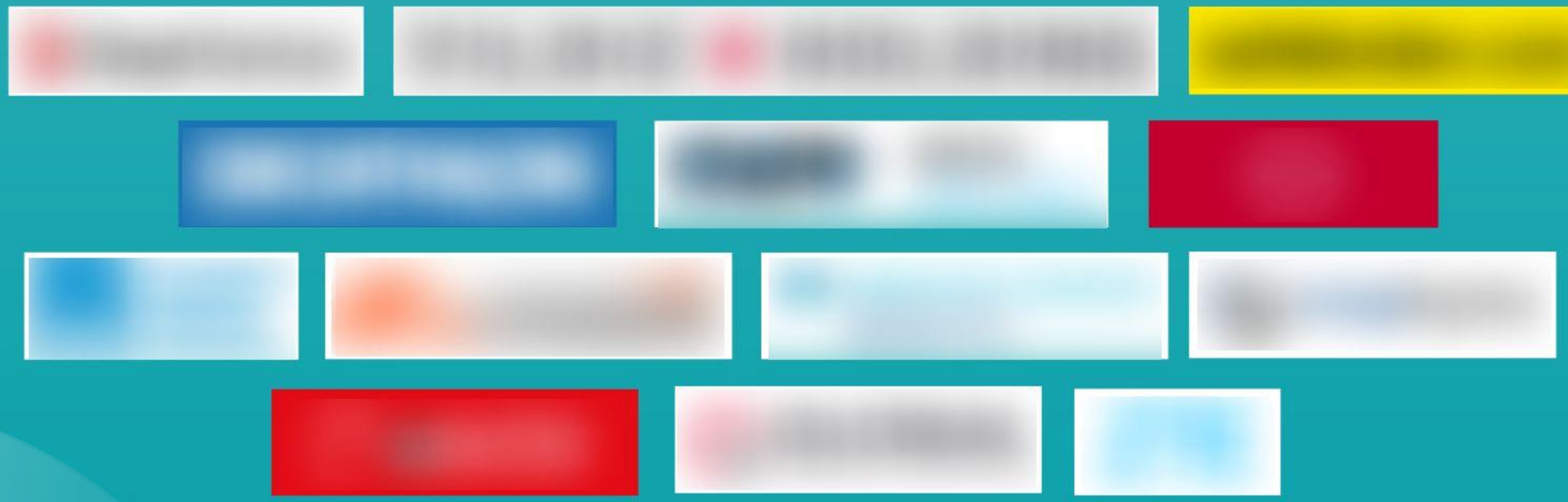
Zafiyet Keşiflerimiz

- **CVE-2022-2256: RedHat Keycloak Open Source Identity and Access Management** - Stored XSS Vulnerability
- **CVE-2020-18305: Extreme Networks Switch EXOS Chalet Web GUI** - Privilege Escalation Vulnerability
- **CVE-2019-18373: Norton App Lock** - Security Passcode/Pattern Lock Screen Bypass Vulnerability

NETAS

Referanslarımız

Güvenlik Zafiyet Test hizmetleri konusunda **sektörünün en büyük şirketleri** tarafından güveniliyoruz. NDA anlaşmaları gereği referans bilgileri yazılı olarak paylaşılamamaktadır. Netaş Satış temsilcinizden bilgi alabilirsiniz.



www.netas.com.tr

2016-2025 Sızma Testi Projelerimiz

- **Finans Sektörü** – Yurtiçi ve Yurtdışı tüm kurum BT Altyapısı, DDoS
- **Holding** – Yurtiçi ve Yurtdışı tüm kurum BT Altyapısı
- **E-Ticaret** – Tüm BT Altyapısı
- **Uluslararası Mağazacılık** – Web/Mobil Uygulamalar
- **Havacılık Lojistik Sektörü** – Tüm BT Altyapısı, DDoS, Sosyal Mühendislik
- **Otomotiv** – Web/Mobil Uygulamalar, Sosyal Mühendislik
- **Havacılık Sektörü** – Tüm BT Altyapısı, DDoS
- **Arge** – Web Uygulama
- **Birçok Çeşitli Sektörden Kurum –** Web/Mobil Uygulama
- **Sermaye Piyasası –** Tüm BT Altyapısı, DDoS
- **Telekom Sektörü –** Tüm BT Altyapısı, DDoS

NETAS

Sızma Testi Metodolojisi

Test Metodoloji ve Standartları

- OWASP Application Security Verification Standard (ASVS)
- OWASP Mobile Application Security Verification Standard (MASVS)
- OWASP Firmware Security Testing Methodology
- “OSSTMM” Open Source Security Testing Methodology Manual
- TS 13638, PCI Penetration testing, ISSAF, NIST SP800-115

Sızma Testi Metodolojisi

- **Otomatik araçların kaçırdığı güvenlik açıklarını ortaya çıkarmak için** kendi manuel araştırmalarımız ile **yaratıcı sızma testi yaklaşımları izliyoruz**.

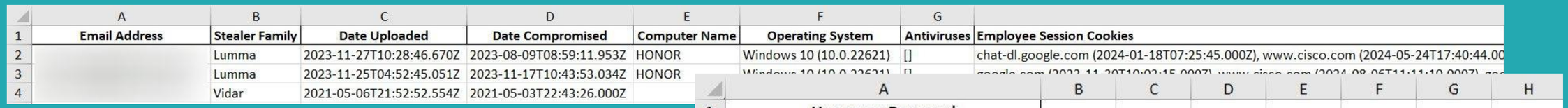
- **Uygulamalar üzerinde** tüm mimari, endpoint ve parametreleri tespit ederek, saldırı yüzeyini daha kapsamlı şekilde adresleyip, olası tüm saldırı senaryolarını ortaya çıkartmayı hedefliyoruz.

- **Kurumunuzun günlük iş operasyonlarındaki** her türlü etkiyi azaltmak için **tüm sızma testi sürecini kontrollü bir şekilde yürütüyoruz.**

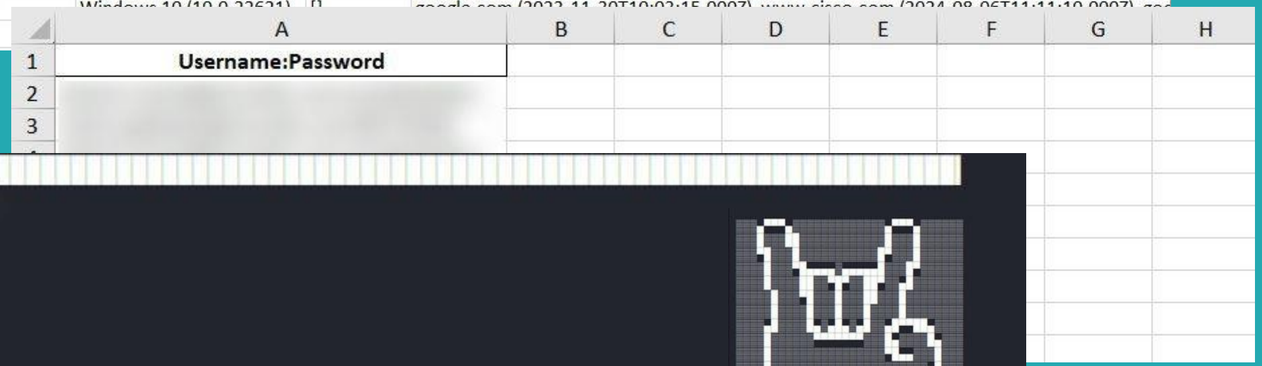
NETAS

Tehdit İstihbaratı Keşif Kapasitemiz

- Sızma testi sırasında, yalnızca güvenlik açıklarını belirlemenin ötesine geçerek **HudsonRock**, **IntelligenceX**, **COMB** ve **BreachDirectory** gibi siber tehdit istihbaratı kaynaklarını ve ihlal veritabanlarını kullanarak, **altyapınızla ilgili kimlik bilgilerinin tehlikeye atılıp atılmadığını da kontrol ediyor ve eyleme geçilebilir bilgiler sunuyoruz.**



	A	B	C	D	E	F	G	
1	Email Address	Stealer Family	Date Uploaded	Date Compromised	Computer Name	Operating System	Antiviruses	Employee Session Cookies
2		Lumma	2023-11-27T10:28:46.670Z	2023-08-09T08:59:11.953Z	HONOR	Windows 10 (10.0.22621)	[]	chat-dl.google.com (2024-01-18T07:25:45.000Z), www.cisco.com (2024-05-24T17:40:44.00
3		Lumma	2023-11-25T04:52:45.051Z	2023-11-17T10:43:53.034Z	HONOR			
4		Vidar	2021-05-06T21:52:52.554Z	2021-05-03T22:43:26.000Z				



	A	B	C	D	E	F	G	H
1	Username:Password							
2								
3								

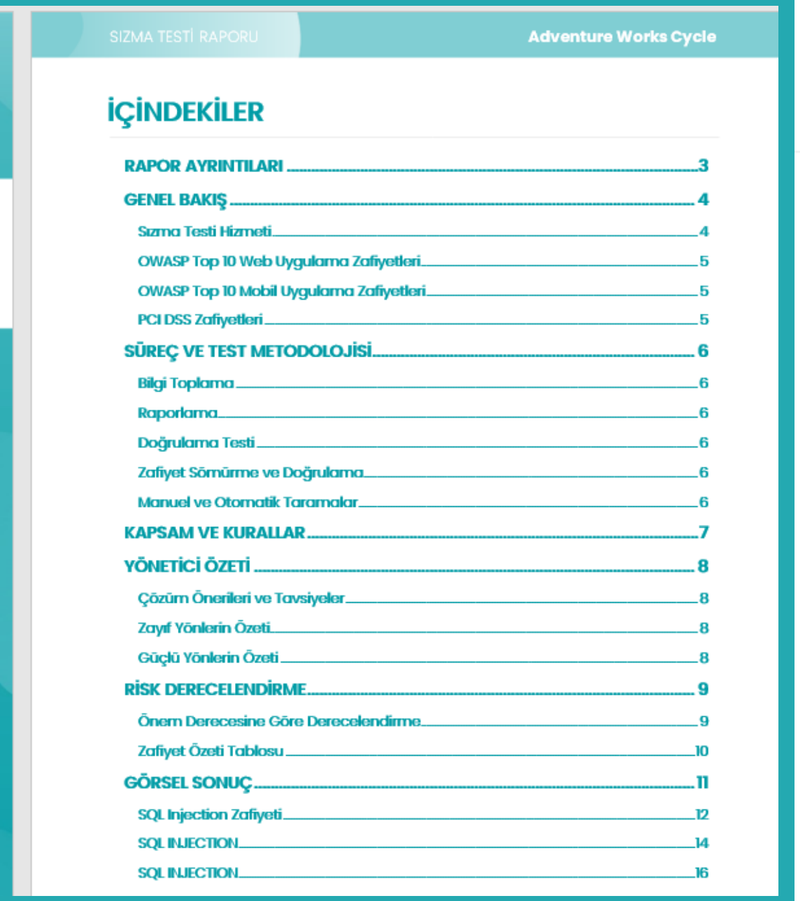
```
Processing:  70%|
Querying HudsonRock for

── Entry ──
Stealer Family: Vidar
Date Uploaded: 2021-05-06T21:52:52.554Z
Date Compromised: 2021-05-03T22:43:26.000Z
Computer Name:
```

NETAS

Rapor Çıktıları

www.netas.com.tr

Sızma testi sonucu paylaşılan güvenlik açığı bulgularının **geçerli**, **yeniden tekrarlanabilir**, **kaliteli** ve **aksiyon alınabilir** çıktılardan oluşmasını sağlıyoruz.



Rapor Çıktıları

Zafiyet Özeti Tablosu

Güvenlik denetimi sonucunda tespit edilen bulgular bu bölümde sınıflandırılarak görsel olarak sunulmaktadır.

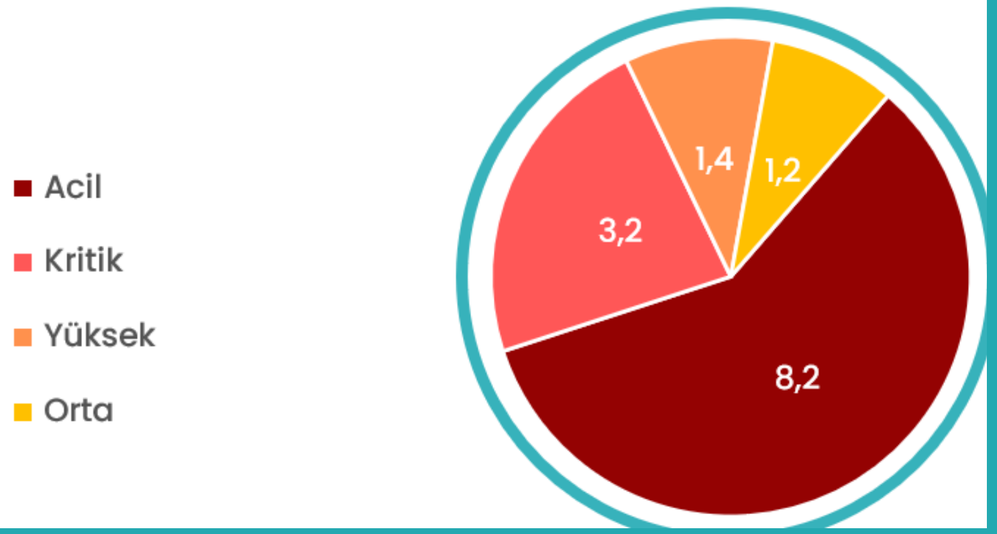
3	3	3	3	3
⚠ ACİL RİSK	⚠ KRİTİK RİSK	⚠ YÜKSEK RİSK	⚠ ORTA RİSK	DÜŞÜK RİSK

Her bir risk düzeyinde aşağıdaki güvenlik açıkları bulunmuştur. Toplam güvenlik açıklarının risk düzeyini belirlemede bir faktör olmadığını bilmek önemlidir. Risk seviyesi, bulunan güvenlik açıklarının ciddiyetine bağlıdır.

Zafiyet No – Zafiyet Adı ve Özeti	Skor	Risk Seviyesi
A1 - SQL INJECTION Use parameterized queries (also known as prepared statements) for all database queries.		⚠ ACİL
K1 - SQL INJECTION Use parameterized queries (also known as prepared statements) for all database queries.		⚠ KRİTİK
Y1 - SQL INJECTION Use parameterized queries (also known as prepared statements) for all database queries.		⚠ YÜKSEK

GÖRSEL SONUÇ

venlik Denetlemesi sonucunda tespit edilen bulgular bu bölümde sınıflandırılarak görsel olarak ulmuştur. Kapsam dahilinde Test edilen sistemlerde bulunan zafiyetlerin risk seviyesine göre ğılımı Şekil 1'de, zafiyet tipine göre sayısal dağılımı Şekil-2'de gösterilmiştir.



NETAS

Rapor Çıktıları

M1	Open Redirect	MEDIUM ⚠
Vuln. Type(s)	Insecure Redirect	
Access Point(s)	External	
Attacker Profile	Anonymous	

H1	Stealing OAuth Tokens via an Insecure Open Redirect	HIGH ⚠
Vuln. Type(s)	Insecure Redirect	
Access Point(s)	External	
Attacker Profile	Anonymous	

NETAS

Rapor Çıktıları

www.netas.com.tr

01 Stored Cross-site Scripting (XSS) – Leads to Account Takeover

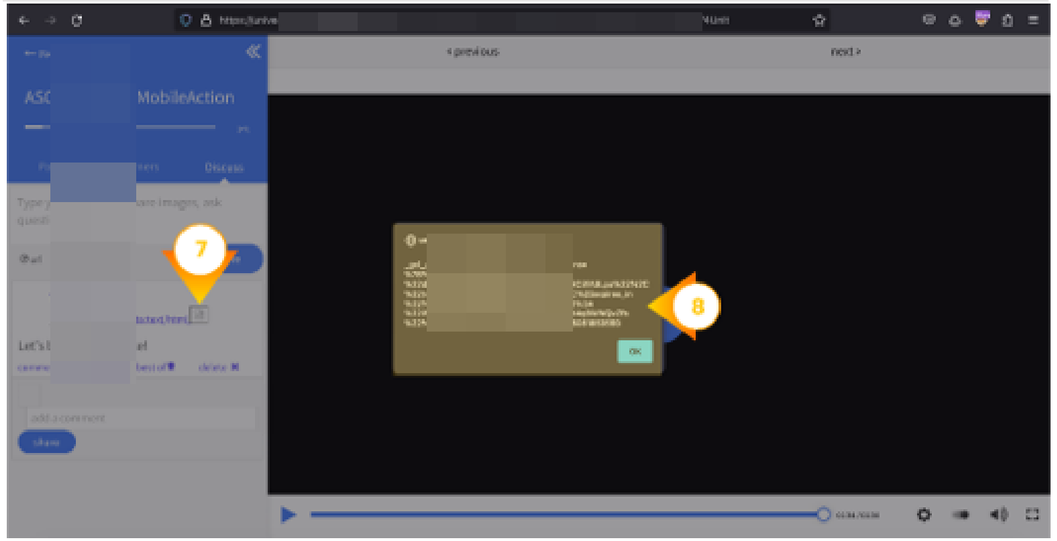
CRITICAL

Vuln. Type(s)	Insufficient Input Validation
Access Point(s)	External
Attacker Profile	Anonymous
Affected Host(s)	**POST** https://university.xxxxxxxxxxxxxxxx/api/posts
Affected Parameter(s)	data{context}
Impact(s)	Execute Malicious JavaScript Code, Cookie Stealing, Account Takeover
Description	The xxxxxxxxxxxxxxxxx LMS application https://www.xxxxxxxxxxxxx/blog/ is affected by a **Stored XSS** in the **data{context}** parameter. This when we inject the JavaScript code **feed:data:text/html,<img src=x onerror=alert(1)><b>** and it is stored and executed in the response page were viewed by the users, the vulnerable page will show the current cookie value in an alert box. **What is Stored cross-site scripting?** Stored cross-site scripting (also known as second-order or persistent XSS) arises when an application receives data from an untrusted source and includes that data within its later HTTP responses in an unsafe way. In terms of exploitability, the key difference between reflected and stored XSS is that a stored XSS vulnerability enables attacks that are self-contained within the application itself.
Detail(s)	The server reads data directly from the HTTP request and reflects it back in the HTTP response. The payload **feed:data:text/html,<img src=x onerror=alert(1)><b>** was submitted in the **data{context}** parameter. Payload is copied from a request and echoed into the application's immediate response in an unsafe way.

Proof(s)
LearnWorlds LMS application contains a stored XSS vulnerability in the Course Discussion function. A victim user can views all discussions after they are posted. XSS will be executed when ever any legit user visits Discuss tab.

"**Inspector**" allows view the fully decoded values of parameters, cookies, or a substring that we've selected

feed:data:text/html,<img src=x onerror=alert(document.cookie)>



Remediation(s)	• Contact with vendor for security mitigations.
Reference(s)	• https://owasp.org/www-community/attacks/xss/ • https://portswigger.net/web-security/cross-site-scripting • How to prevent XSS? (https://portswigger.net/web-security/cross-site-scripting/preventing)

www.netas.com.tr

DoS/DDoS Dağıtık Hizmet Dışı Bırakma Saldırı Simülasyonları

- **Volumetrik:** UDP-ICMP bandwidth, Tcp Syn, Ack, Psh+Ack, Rst Flood, DNS, NTP, SNMP, Portmap, Netbios, RIPv1 Amplification Saldırı testleri
- **DNS Saldırıları:** DNS Flood, DNS Amplification
- **Uygulama Katmanı:** Http, Https GET/POST Flood
- **Sistem Kaynak Tüketimi :** Ping of Death, Slow read, Sock stress, Tcp Syn-Fin, Rst Flood saldırı teknikleri ile Sunucu, Firewall, Load Balancer gibi aktif sistemlerin kaynak tüketimine yönelik saldırılar
- **BotNet:** Yüzlerdce farklı IP kaynağı kullanarak ICMP, UDP, TCP, http Flood saldırı teknikleri ile bot net saldırı simulasyonu testi.
- **Kuruma Özel:** Kurumunuz uygulama, sunucu ve güvenlik sistemlerinize uygun karşılıklı belirleyeceğimiz senaryolar ve özel atak tipleri oluşturarak yapılan özel saldırı testleri

NETAS

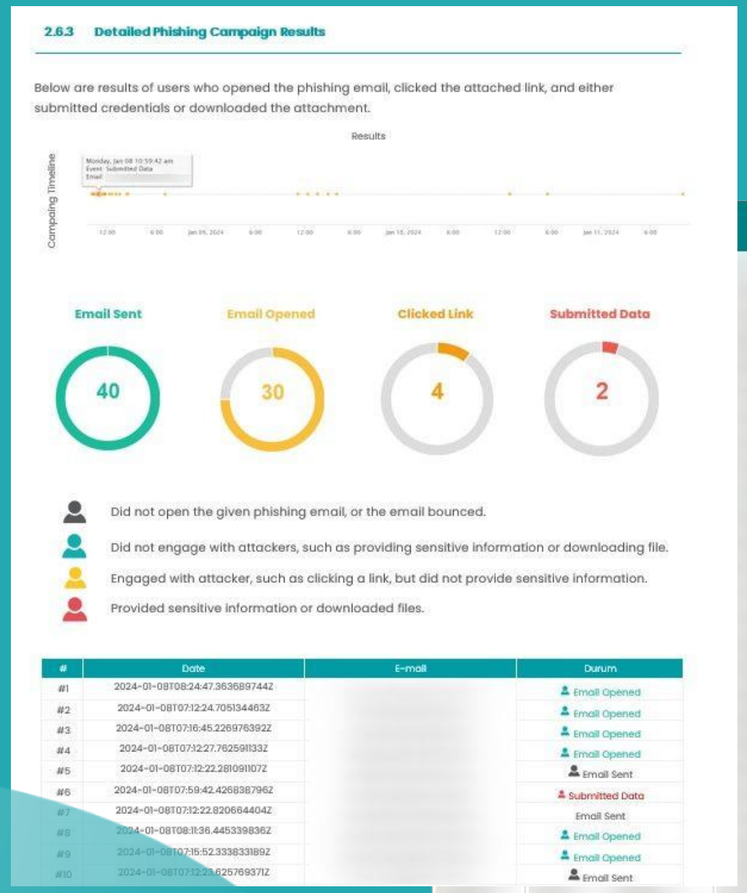
www.netas.com.tr

Gelişmiş Saldırı Simülasyonları

- Hedefli E-mail Oltalama (Phishing) Saldırıları
- Vishing (Voice Phishing) Saldırıları
- Red Teaming

Sosyal Mühendislik Testi Rapor Çıktıları

www.netas.com.tr



2.6.3 Detailed Phishing Campaign Results

Below are results of users who opened the phishing email, clicked the attached link, and either submitted credentials or downloaded the attachment.

Results

Campaign Timeline

Monday, Jan 08 10:59:42 am
Event: Submitted Data
Email:

12:00 6:00 Jan 09, 2024 6:00 12:00 6:00 Jan 10, 2024 6:00 12:00 6:00 Jan 11, 2024 6:00

Email Sent	Email Opened	Clicked Link	Submitted Data
40	30	4	2

Did not open the given phishing email, or the email bounced.

Did not engage with attackers, such as providing sensitive information or downloading file.

Engaged with attacker, such as clicking a link, but did not provide sensitive information.

Provided sensitive information or downloaded files.

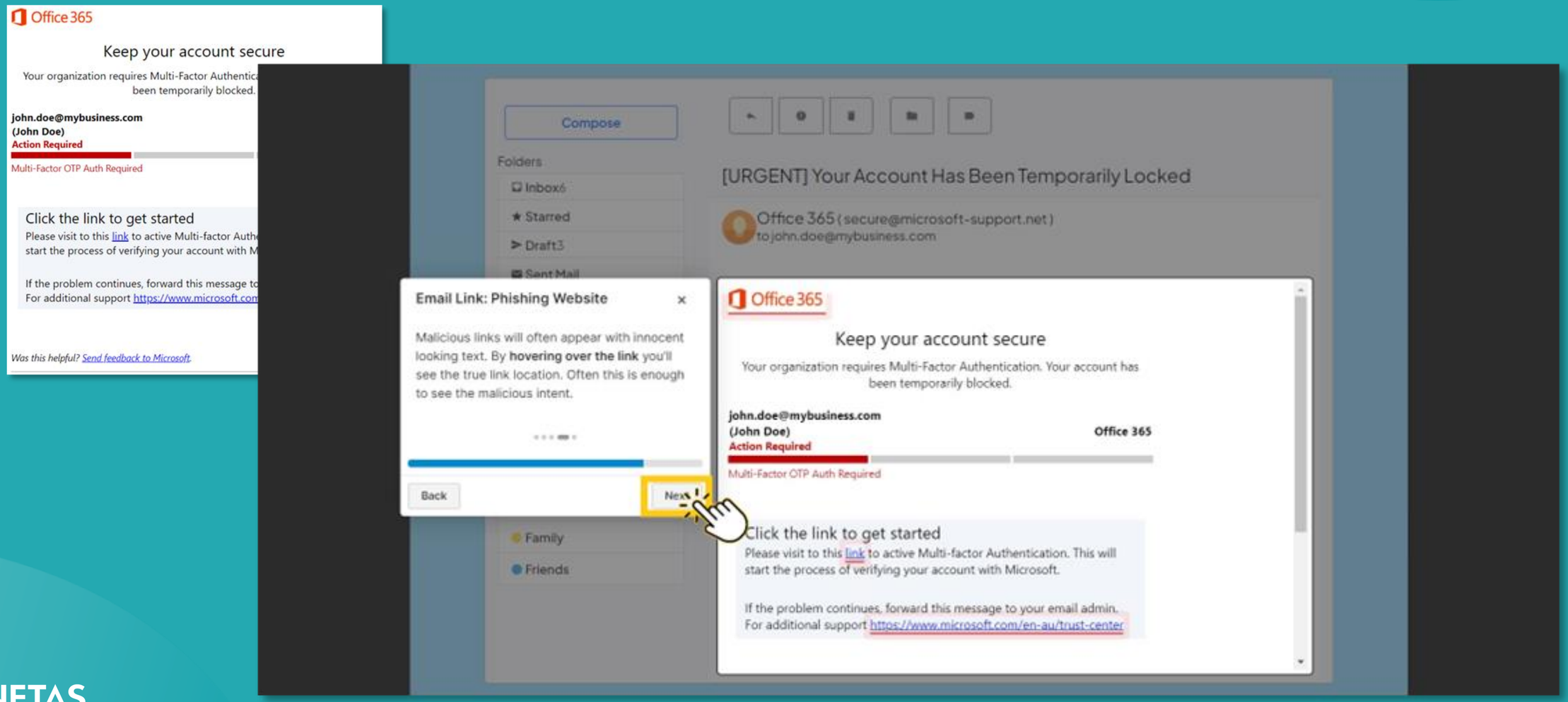
#	Date	E-mail	Durum
#1	2024-01-08T08:24:47.3636897442		Email Opened
#2	2024-01-08T07:12:24.7051344632		Email Opened
#3	2024-01-08T07:16:45.2269763922		Email Opened
#4	2024-01-08T07:12:27.7625911332		Email Opened
#5	2024-01-08T07:12:22.2810911072		Email Sent
#6	2024-01-08T07:59:42.4268387962		Submitted Data
#7	2024-01-08T07:12:22.8206644042		Email Sent
#8	2024-01-08T08:11:36.4453398362		Email Opened
#9	2024-01-08T07:15:52.3338331892		Email Opened
#10	2024-01-08T07:12:23.6257693712		Email Sent

Email	Status	IP Address	Latitude	Longitude	Send Date	Last Activity
	Email Opened				2024-01-08T07:12:21.208685585Z	2024-01-08T08:24:47.363689744Z
	Email Opened				2024-01-08T07:12:21.476948622Z	2024-01-08T07:12:24.705134463Z
	Email Opened				2024-01-08T07:12:21.742554875Z	2024-01-08T07:16:45.226976392Z
	Email Opened				2024-01-08T07:12:22.016699464Z	2024-01-08T07:12:27.762591133Z
	Email Sent				2024-01-08T07:12:22.2810911072	2024-01-08T07:12:22.2810911072
	Submitted Data				2024-01-08T07:12:22.548076175Z	2024-01-08T07:59:42.426838796Z
	Email Sent				2024-01-08T07:12:22.820664404Z	2024-01-08T07:12:22.820664404Z
	Email Opened				2024-01-08T07:12:23.087952643Z	2024-01-08T08:11:36.445339836Z
	Email Opened				2024-01-08T07:12:23.3583624192	2024-01-08T07:15:52.3338331892
	Email Sent				2024-01-08T07:12:23.6257693712	2024-01-08T07:12:23.6257693712
	Email Sent				2024-01-08T07:12:23.892374563Z	2024-01-08T07:12:23.892374563Z
	Email Opened				2024-01-08T07:12:24.1590890622	2024-01-08T10:33:30.398442898Z
	Email Opened				2024-01-08T07:12:24.434073995Z	2024-01-09T12:54:27.60544055Z
	Email Opened				2024-01-08T07:12:24.705546835Z	2024-01-08T08:01:05.522410526Z
	Clicked Link				2024-01-08T07:12:24.9820811052	2024-01-08T08:45:25.248393866Z
	Email Opened				2024-01-08T07:12:25.24757183Z	2024-01-08T07:19:03.578538399Z
	Email Sent				2024-01-08T07:12:25.5121428912	2024-01-08T07:12:25.5121428912
	Email Sent				2024-01-08T07:12:25.781084114Z	2024-01-08T07:12:25.781084114Z
	Email Opened				2024-01-08T07:12:26.0563701372	2024-01-09T08:10:21.074889163Z
	Email Opened				2024-01-08T07:12:26.3213661062	2024-01-10T14:30:35.564626094Z
	Email Opened				2024-01-08T07:12:26.58792756Z	2024-01-11T06:58:43.342236043Z
	Email Opened				2024-01-08T07:12:26.8534841952	2024-01-10T09:56:40.192888884Z
	Email Opened				2024-01-08T07:12:27.1336184142	2024-01-08T09:17:22.257396891Z
	Submitted Data				2024-01-08T07:12:27.4026536242	2024-01-08T07:34:03.746285866Z
	Email Sent				2024-01-08T07:12:27.7562319852	2024-01-08T07:12:27.7562319852
	Email Opened				2024-01-08T07:12:28.0421923342	2024-01-08T07:18:54.752395742Z
	Email Opened				2024-01-08T07:12:28.3107548672	2024-01-08T07:38:18.193982303Z

NETAS

Phishing Eğitim Modülleri

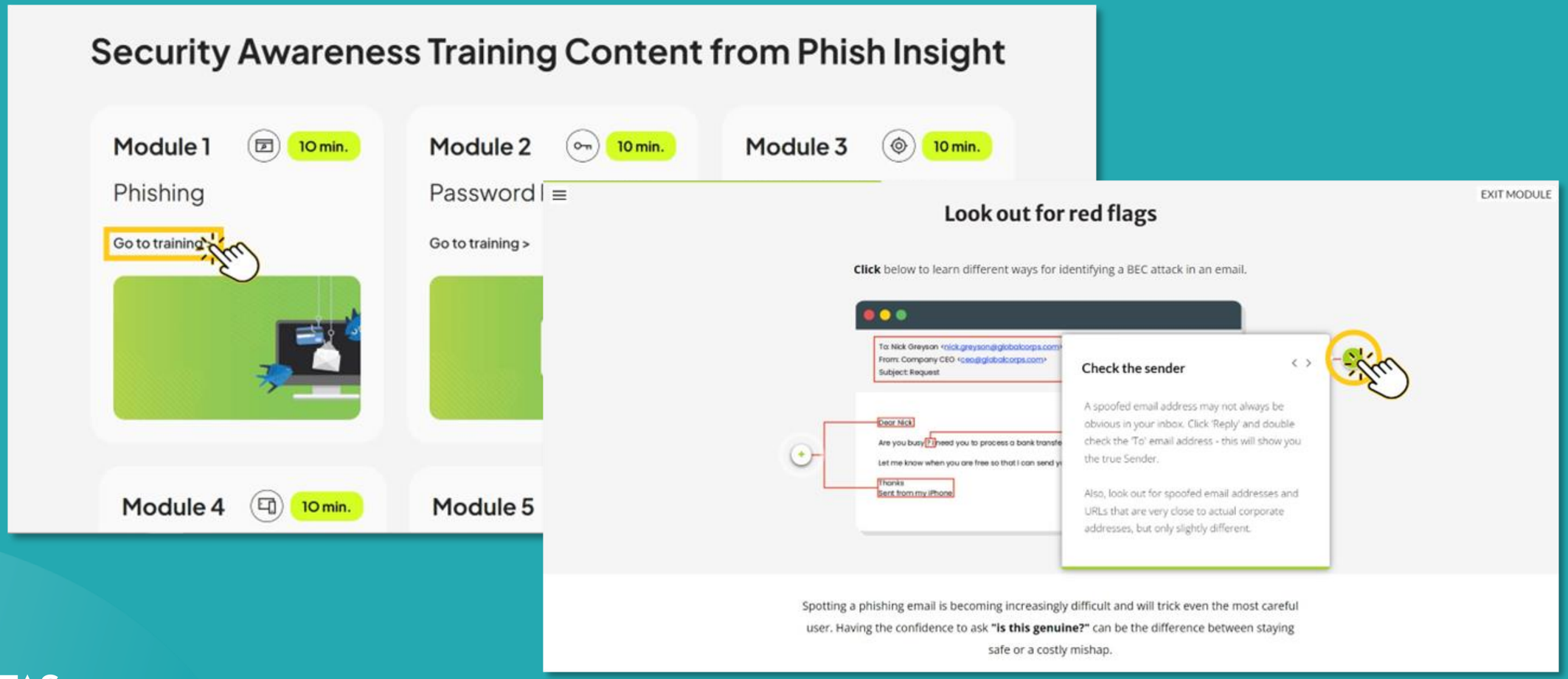
www.netas.com.tr



NETAS

Phishing Eğitim Modülleri

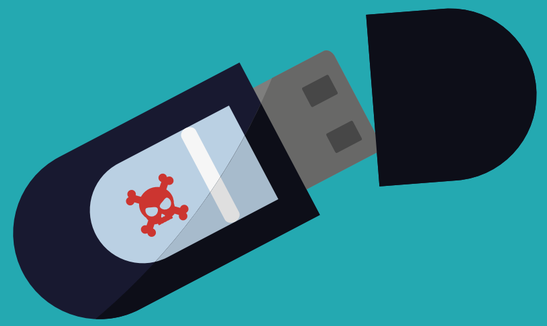
www.netas.com.tr



NETAS

Test Araçları

- Burp Suite Professional
- Nessus Professional, nuclei
- Metasploit
- sqlmap, gobuster, amass, nmap
- aircrack-ng, wifijammer, bettercap, mitm-proxy, tcpdump, responder, mimikatz, crackmapexec
- binwalk, QEMU, EMBA, TROMMEL
- Özel Script, Exploit ve Donanım araçları



Teşekkürler

NETAŞ

Security Testing Services