# Elazığ Ticaret ve Sanayi Odası

## Sızma Testleri Ve Güvenlik Denetimi Ön Raporu

**Grup-3**

---


**Bu araştırma**
**Doç. Dr. Fatih Özkaynak**
**gözetiminde, Fırat Üniversitesi Teknoloji Fakültesi**
**Yazılım Mühendisliği öğrencileri tarafından yapılmıştır**

**Ağustos-2022**

# Grup Üyeleri

Grup 3

**Analiz Ekibi**

Buğra Can Kuş (200541305)
Muhammet Onur AKPOLAT (195542009)
Tahsin Başar Paksoy (180541019)
Tunahan Gökçimen (185541005)

**Test Ekibi**

Alper Ragıb Budak (185541028)
Ferhat Karaboğa (185541033)
Zeki Muzaffer Akın (185541058)
Zeynep Geyik (195541075)

**Dokümantasyon**

Batuhan Berk Topal (185541047)
Bünyamin Kiremit (180542012)
Halil İbrahim Karabulut (185541044)
Hebun Sünbül (180541009)
Mustafa Akaydın (180541035)
Şahika Ercan (185541009)

**Sunum Ekibi**

Ahmet Sezer Alaca (180541061)
Ayşenur Bilgiç (185541040)
Nurcan Duman (180542018)

## İçindekiler

## Özet

Bu dokümanda Fırat Üniversitesi Teknoloji Fakültesi Yazılım Mühendisliği Bölümü Bilgi Sistemleri Ve Güvenliği dersini alan öğrencilerin Elazığ Ticaret Ve Sanayi Odası için gerçekleştirdikleri sızma testinin raporu bulunmaktadır.
Bu sızma testi yapılırken Nessus, Nmap, Wireshark, Maltego, HostedScan, Fierce ve Netsparker sızma testi araçları kullanılmıştır. Her araç için detaylı analiz işlemi yapılıp açıklamaları ile birlikte detaylı bir sonuç raporu hazırlanmıştır.

**Genel Sızma Testi Metodolojisi:**


**Sızma testi metodolojisi 5 aşamaya ayrılabilir.**

- **Planlama ve Keşif:**

  Amaç hedef sistem hakkında olabildiğince bilgi toplamaktır. Bu bilgiler firma hakkında olabildiği gibi firma çalışanları hakkında da olabilir. Bunun için internet siteleri haber grupları e-posta listeleri, gazete haberleri vb. hedef sisteme gönderilecek çeşitli paketlerin analizi yardımcı olacaktır.

- **Zafiyet Tarama:**

  Bu sürecin amacı belirlenen hedef sistemlerdeki açıklıkların ortaya çıkarılmasıdır. Bunun için sunucu servislerdeki bannerlar ilk aşamada

kullanılabilir. Ek olarak birden fazla zayıflık tarama aracı ile bu sistemler ayrı ayrı taranarak oluşabilecek false positive oranı düşürülmeye çalışılır. Bu aşamada hedef sisteme zarar vermeyecek taramalar gerçekleştirilir. Zayıflık tarama sonuçları mutlaka uzman gözler tarafından tekrar tekrar incelenmeli, olduğu gibi rapora yazılmamalıdır.

- **Erişim Elde Etme:**

  Sızma sürecinde amaç sisteme bir şekilde giriş hakkı elde etmektir. Bu süreçten sonra sistemdeki kullanıcının haklarının arttırılması hedeflenmektedir. Linux sistemlerde çekirdek(kernel) versiyonunun incelenerek priv escalation zafiyetlerinin belirlenmesi ve varsa kullanılarak root haklarına erişilmesi en klasik hak yükseltme adımlarından biridir.

- **Erişimleri Koruma:**

  Sisteme girildiğinin başkaları tarafından belirlenmemesi için bazı önlemler alınmasında fayda vardır. bunlar giriş loglarının silinmesi, çalıştırılan ek proseslerin saklı olması, dışarıya erişim açılacaksa gizli kanalların kullanılması(covert channel), backdoor, rootkit yerleştirilmesi vs.

- **Analiz ve Raporlama:**
  Raporlar bir testin müşteri açısından en önemli kısmıdır. Raporlar ne kadar açık ve detaylı olursa müşterinin riski değerlendirmesi ve açıklıkları gidermesi de o kadar kolay olur.
  Testler esnasında çıkan kritik güvenlik açıklarının belgelenerek sözlü olarak anında bildirilmesi test yapan takımın görevlerindendir. Bildirimin ardından açıklığın açıklığın hızlıca giderilmesi için çözüm önerilerinin de birlikte sunulması gerekir.

# Gerçekleştirilen Güvenlik Testleri Ve Sonuçları

## Netsparker Tarama Sonucu raporu:

https://www.elazigtso.org.tr/

**Tarama süresi** : 19.08.2022 13:43:30 (UTC+03:00)
**Tarama Süresi** : 00:05:49:03

**Toplam İstek** : 10.866
**Ortalama Hız** : 0,5 r/s

Risk seviyesi:
**ORTA**

KESİNLİKLER

| 17 | 5 | 0 | 0 | 3 | 7 | 6 | 1 |
|---|---|---|---|---|---|---|---|
| TANIMLANMIŞ | ONAYLANMIŞ | KRİTİK | YÜKSEK | ORTA | DÜŞÜK | EN İYİ PRATİK | BİLGİ |

### Tanımlanan Güvenlik Açıkları

| | |
|---|---|
| kritik | 0 |
| Yüksek | 0 |
| Orta | 3 |
| Düşük | 7 |
| En iyi pratik | 6 |
| Bilgi | 1 |
| **TOPLAM** | **17** |

### Onaylanmış Güvenlik Açıkları

| | |
|---|---|
| kritik | 0 |
| Yüksek | 0 |
| Orta | 1 |
| Düşük | 4 |
| En iyi pratik | 0 |
| Bilgi | 0 |
| **TOPLAM** | **5** |

## 1. HTTPS Üzerinden Etkin Karma İçerik

ORTA 1 ONAYLANMIŞ 1

Netsparker, bir HTTPS sayfasında HTTP üzerinden etkin bir içeriğin yüklendiğini tespit etti.HTTPS sayfası, normal, açık metin HTTP aracılığıyla alınan komut dosyaları veya stil sayfaları gibi etkin içerik içeriyor ise, bağlantı yalnızca kısmen şifrelenir. Şifrelenmemiş içeriğe koklayıcılar erişebilir.

### Çözüm

Karışık içerik sorunlarına karşı savunmak için iki teknoloji vardır:

1. HTTP Strict Transport Security (HSTS), kullanıcı hataları (80 numaralı bağlantı noktasından web sitenize erişme girişimi) ve uygulama hataları karşısında bile güvenli kaynak alımını zorlayan bir mekanizmadır.
2. İçerik Güvenliği Politikası (CSP), üçüncü taraf web sitelerinden güvenli olmayan kaynak alımını engellemek için kullanılabilir.

Son olarak, kullanıcının hangi protokole bağlı olduğuna bağlı olarak, kullanıcının tarayıcısının HTTP veya HTTPS'yi uygun şekilde otomatik olarak seçmesini sağlamak için "protokol göreli URLleri" kullanabilirsiniz.

## 2. HTTP Sıkı Aktarım Güvenliği (HSTS) Politikası Etkin Değil

ORTA 1

Netsparker, HTTP Katı Aktarım Güvenliği (HSTS) ilkesinin etkinleştirilmediğini belirledi.
Hedef web sitesi yalnızca HTTPS'den değil, aynı zamanda HTTP'den de sunuluyor ve HSTS politika uygulamasından yoksun.

### Çözüm

Web sunucunuzu HTTP isteklerini HTTPS'ye yönlendirecek şekilde yapılandırın.

## 3. Güncel Olmayan Sürüm (jQuery)

ORTA 1

Netsparker, hedef web sitesinin jQuery kullanıldığını belirledi ve güncel olmadığını tespit etti.
Bu, yazılımın eski bir sürümü olduğundan saldırılara açık olabilir.

### Bilinen Bazı Güvenlik Açıkları

**jQuery Web Sayfası Oluşturma Sırasında Girdinin Uygunsuz Nötralizasyonu ('Siteler Arası Komut Dosyası Çalıştırma') Güvenlik Açığı**

3.0.0'dan önceki jQuery, dataType seçeneği olmadan bir etki alanları arası Ajax isteği gerçekleştirildiğinde ve metin/javascript yanıtlarının yürütülmesine neden olduğunda Siteler Arası Komut Dosyası Çalıştırma (XSS) saldırılarına karşı savunmasızdır.

**Etkilenen Sürümler**
1.8.0 ila 2.2.4

**jQuery Web Sayfası Oluşturma Sırasında Girdinin Uygunsuz Nötralizasyonu ('Siteler Arası Komut Dosyası Çalıştırma') Güvenlik Açığı**

1.0.3'ten büyük veya buna eşit ve 3.5.0'dan önceki jQuery sürümlerinde, <option> güvenilmeyen kaynaklardan - sterilize ettikten sonra bile - jQuery'nin DOM işleme yöntemlerinden birine (yani .html(), .append() ve diğerleri) öğeler güvenilmeyen kodu çalıştırabilir. Bu sorun, jQuery 3.5.0'da düzeltilmiştir.

**Etkilenen Sürümler**
1.9.0 ila 3.4.1

### Çözüm

Lütfen jQuery kurulumunuzu en son kararlı sürüme yükseltin.

## 4. [Olası] Tarayıcı Sekmelerinde Gezinerek Kimlik Avı

DÜŞÜK 1

Netsparker, tarayıcı sekmelerinde gezinerek olası kimlik avını belirledi, ancak güvenlik açığını doğrulayamadı. Etiketli normal href'lere sahip açık pencereler, *window.opener.location'ı* değiştirebilir ve ana web sayfasını farklı bir kaynakta olsa bile başka bir şeyle değiştirebilir.

### Çözüm

- *Sayfaların window.opener'ı* kötüye kullanmasını önlemek rel=noopeneriçin bağlantılara ekleyin . Bu, sayfanın Chrome ve Opera tarayıcılarında *window.opener* özelliğine erişememesini sağlar .

- Daha eski tarayıcılar ve Firefox'ta, Yönlendiren başlığını ek olarak devre dışı bırakan ekleyebilirsiniz .rel=noreferrer

## 5. Çerez Yalnızca HttpOnly Olarak İşaretlenmemiş

DÜŞÜK 1 ONAYLANMIŞ 1

Netsparker, HTTPOnly olarak işaretlenmemiş bir çerez tanımladı.
HTTPOnly tanımlama bilgileri, istemci tarafı komut dosyaları tarafından okunamaz, bu nedenle bir tanımlama bilgisini HTTPOnly olarak işaretlemek, siteler arası komut dosyası çalıştırma saldırılarına karşı ek bir koruma katmanı sağlayabilir.

### Yapılacak İşlemler

1. Çözüm için çareye bakın.
2. Uygulama tarafından kullanılan tüm tanımlama bilgilerini HTTPOnly olarak işaretlemeyi düşünün. ( *Bu değişikliklerden sonra javascript kodu çerezleri okuyamayacaktır.* )

### Çözüm

Tanımlama bilgisini HTTPOnly olarak işaretleyin. Bu, XSS'ye karşı ekstra bir savunma katmanı olacaktır. Ancak bu bir gümüş kurşun değildir ve sistemi siteler arası komut dosyası çalıştırma saldırılarına karşı korumayacaktır. Saldırgan, HTTPOnly korumasını atlamak için XSS Tüneli gibi bir araç kullanabilir.

## 6. Çerez Güvenli Olarak İşaretlenmedi

DÜŞÜK 1 ONAYLANMIŞ 1

Netsparker, güvenli olarak işaretlenmeyen ve HTTPS üzerinden aktarılan bir tanımlama bilgisi belirledi.

Bu, çerezin trafiği başarıyla kesip şifresini çözebilen bir saldırgan tarafından veya başarılı bir ortadaki adam saldırısını takiben potansiyel olarak çalınabileceği anlamına gelir.

### Yapılacak İşlemler

1. Çözüm için çareye bakın.
2. Uygulama içinde kullanılan tüm çerezleri güvenli olarak işaretleyin. *(Çerez, kimlik doğrulama ile ilgili değilse veya herhangi bir kişisel bilgi içermiyorsa, onu güvenli olarak işaretlemeniz gerekmez.)*

### Çözüm

Uygulama içinde kullanılan tüm çerezleri güvenli olarak işaretleyin.

## 7. Güvensiz Çerçeve (Harici)

DÜŞÜK 1 ONAYLANMIŞ 1

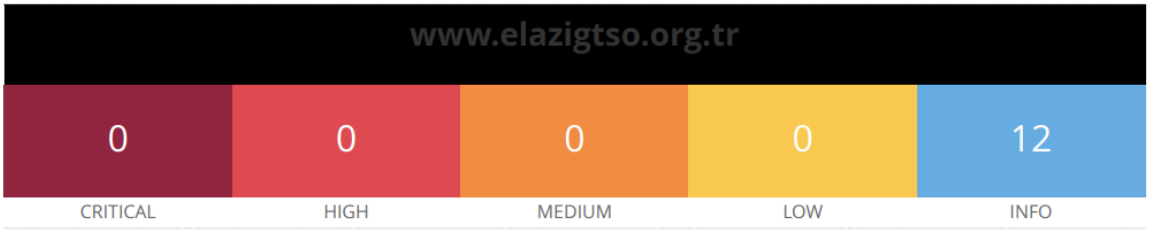
Netsparker, harici bir güvenli olmayan veya yanlış yapılandırılmış iframe belirledi. IFrame korumalı alanı, potansiyel olarak kötü amaçlı kodunun, onu gömen web sayfasına zarar vermesini kısıtlamak için bir çerçeve içindeki içerik için bir dizi ek kısıtlama sağlar.

### Çözüm

Satır içi çerçevede korumalı alan uygulama
<iframe korumalı alan src="framed-page-url"></iframe>

- 
- Güvenilmeyen içerik için, ve ve ve in sandbox özniteliklerini seamlesskullanmaktan kaçının.allow-top-navigationallow-popupsallow-scripts

**Nessus Tarama Sonu:**




Scan Information

| | |
|---|---|
| Start time: | Thu Aug 18 12:59:39 2022 |
| End time: | Thu Aug 18 13:16:18 2022 |

Host Information

| | |
|---|---|
| DNS Name: | www.elazigtso.org.tr |
| IP: | 94.73.147.29 |
| OS: | EthernetBoard OkiLAN 8100e |

Nessus kullanılarak yapılan tarama ve analizler sonucunda, herhangi bir risk veya açığa rastlanmadı.

**Nmap Tarama Sonucu:**

elazigtso.org.tr domainimizin ip adresini 94.73.147.29 olduğunu öğrendikten sonra -sV parametresi ile versiyon taraması yaparak testlere başladık

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 94.73.147.29 -sV
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-21 14:23 EDT
Nmap scan report for cpls24.srvpanel.com (94.73.147.29)
Host is up (0.013s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE VERSION
80/tcp  open  http    imunify360-webshield/1.18
443/tcp open  https   imunify360-webshield/1.18
```

Nmap ile yapılan tarama sonucunda 80 ve 443 portlarının açık olduğu bilgisine ulaştık. Firewall dolayısıyla diğer portların filtreli olduğunu ve erişimimizin olmadığını görüyoruz
-O parametresini kullanarak karşı tarafın işletim sisteminin linux 2.6.22 olduğunu öğreniyoruz.
Sitenin SSL sertifikasının 06.10.2022 tarihinde biteceğini, sertifikanın hosting hizmetinin de alındığı Natro'nun içerisinde bulunan Sectigo tarafından sağlandığını öğrendik

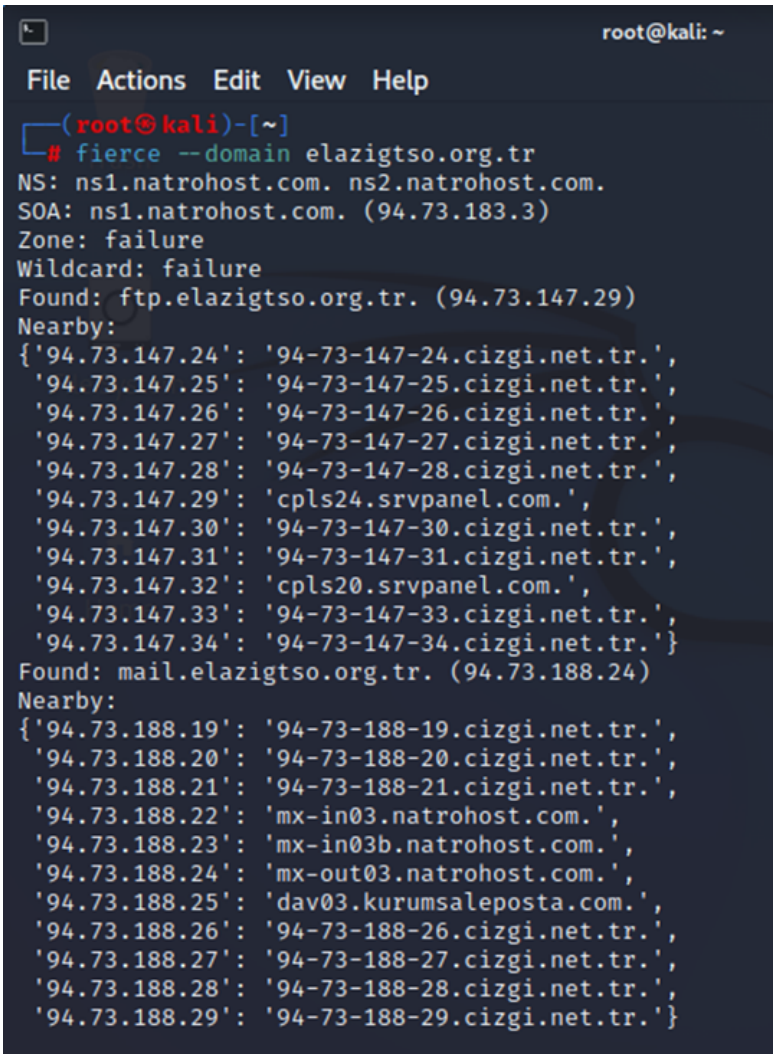
```
Nmap scan report for elazigtso.org.tr (94.73.147.29)
Host is up (0.13s latency).
rDNS record for 94.73.147.29: cpls24.srvpanel.com

PORT    STATE SERVICE
80/tcp  open  http
| http-litespeed-sourcecode-download:
| Litespeed Web Server Source Code Disclosure (CVE-2010-2333)
| /index.php source code:
|_<center> Access from  to  blocked due to malicious traffic. <br> Please try agai
n later. <br> If you feel this is an error please contact us. <br> <br> <br>  ip a
dresinden  'e zararl\xC4\xB1 eri\xC5\x9Fim tespit edilmi\xC5\x9F ve engellenmi\xC5
\x9Ftir. <br> L\xC3\xBCtfen daha sonra tekrar deneyiniz. <br> Bunun bir hata oldu\
xC4\x9Funu d\xC3\xBC\xC5\x9F\xC3\xBCn\xC3\xBCyorsan\xC4\xB1z bizimle ileti\xC5\x9F
ime ge\xC3\xA7ebilirsiniz.\x0D
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-majordomo2-dir-traversal: ERROR: Script execution failed (use -d to debug)
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-phpmyadmin-dir-traversal:
```

```
SF:DDoS\x20atak\x20tespit\x20edilmi\xc5\x9f\x20ve\x20engellenmi\xc5\x9ftir
SF:\.\x20<br>\x20L\xc3\xbctfen\x20daha\x20sonra\x20tekrar\x20deneyiniz\.\x
SF:20<br>\x20Bunun\x20bir\x20hata\x20oldu\xc4\x9funu\x20d\xc3\xbc\xc5\x9f\
SF:xc3\xbcn\xc3\xbcyorsan\xc4\xb1z\x20bizimle\x20ileti\xc5\x9fime\x20ge\xc
SF:3\xa7ebilirsiniz\.\r\n")%r(HTTPOptions,1F8,"HTTP/1\.1\x20200\x20OK\r\nC
SF:ontent-Length:\x20351\r\nConnection:\x20Close\r\nCache-Control:\x20no-c
SF:ache\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nX-Frame-Options
SF::\x20SAMEORIGIN\r\n\r\n<center>\x20Access\x20from\x20\x20to\x20\x20bloc
SF:ked\x20due\x20to\x20a\x20DDoS\x20attack\.\x20<br>\x20Please\x20try\x20a
```

Nmap aracılığı ile testlerimize devam ederken güvenlik duvarı tarafından fark edilip engellenmiş bulunmaktayız. Üç farklı ekip üyemizin farklı bilgisayar ve IP adresi üzerinden yaptığı testlerin tamamına engelleyen bir güvenlik duvarı ile karşı karşıya olduğumuz için beklediğimiz türde bir sonuç elde edemedik.

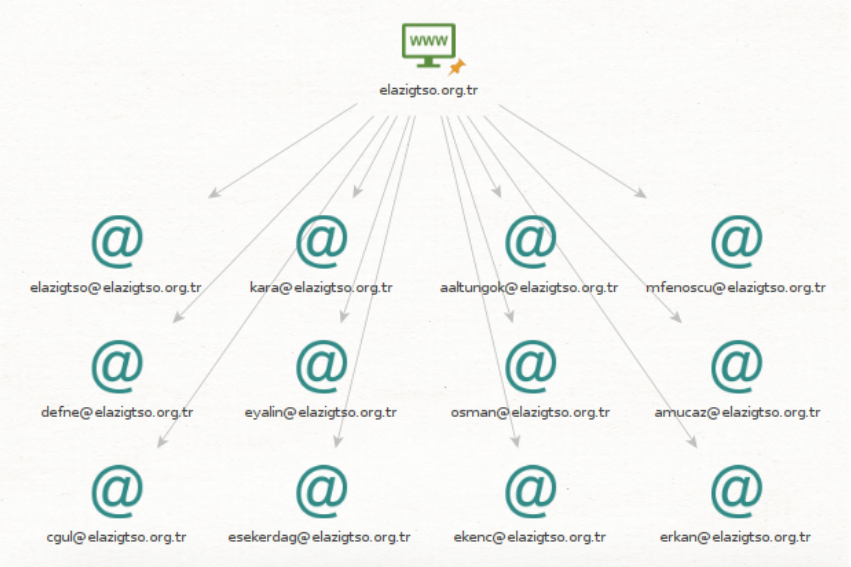
**Fierce Araştırması**




Fierce tarafında yaptığımız araştırmalarda Hosting hizmetinin Natro tarafından sağlandığını görüyoruz.
Natro, cPanel içerisinde bulunan birçok özelliği bloklaması ile bilinmektedir. Sebebi ise bunları kendilerine yük olarak görmeleri ve diğer özellikleri de kullanıcılara para ile satmak istemeleri.
Örneğin cPanel üzerinde “phpmailer” kütüphanesinin çalışmasına izin verilmiyor. Ayrıca cPanel içerisinde ücretsiz olarak bulunan SSL Sertifikasını engelleyerek kullanıcılara SSL Sertifikası satıyorlar.

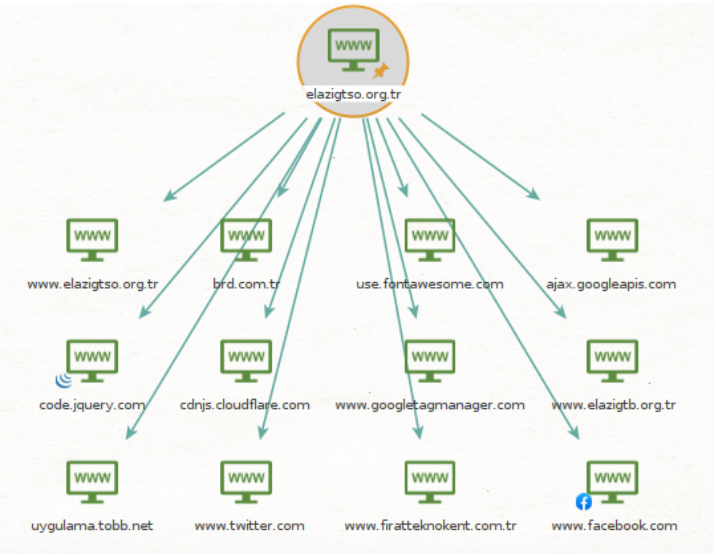
Bu sebeplerden dolayı hosting hizmetinin alındığı firmanın değiştirilmesi tavsiye edilmektedir.

**Maltego Analizi:**
Maltego ile yapılan taramalar sonucunda elazigtso.org.tr adresine kayıtlı 12 adet mail bulunmaktadır. Bu maillere ise mail.elazigtso.org.tr adresinden ulaşılabilmektedir.




Ofise yapılan fiziksel ziyaretlerde internet şifresinin direkt verilmesi ofis çalışanlarının sosyal mühendisliğe müsait olduğunu göstermektedir. Bu, yazılımsal veya donanımsal açıklardan daha riskli bir açıktır. Bulunan maillere Phishing saldırısı yapılarak çalışanların linke tıklaması sonucu firmadan oldukça önemli veriler çalınabilir.

Bu konuda firmanın çalışanlarına eğitim veya seminer ile bilgi vermesi tavsiye edilmektedir.




Web sitesinde SEO çalışması olarak sadece temel Google Tag Manager kullanıldığı gözükmektedir. Bu firmaya Google aramalarında öne çıkma konusunda yardımcı olsa da daha verimli ve etkili çalışan çözümler kullanılması tavsiye edilir.

## CUPP ve Brute Force ile WI-FI şifresinin kırılması:

ETSO ofisindeki çalışandan sosyal mühendislik yardımı ile alınan şifrenin sosyal mühendislik kullanılmadan ne kadar kolay kırılacağını test etmek için Common User Passwords Profiler (CUPP) isimli kişiye özel wordlist oluşturan python kodundan yardım alındı.

CUPP, içinde “Elazig, Ticaret, Sanayi, Odasi, ETSO, 2018, 2019, 2020, 2021, 2022” bulunan toplam 6863 farklı şifre oluşturdu. Firmanın güncel şifresi ise CUPP Wordlistinde 2743. sırada yer almakta. Donanım hızına ve doğru wordlist kullanımına bağlı olarak bu şifrenin yaklaşık 10 dakikada kırıldığı gözlemlenmiştir.

## Wireshark Ağ Analizi:

ETSO ofisine giden ekip üyeleri, girişte bulunan çalışana oldukça basit bir sosyal mühendislik yöntemi uygulayarak ağ şifresini almayı başarmıştır. Çalışanın şifreyi kolayca verme sebebinin ise ağı kullanmak için TC Kimlik No ve benzeri bilgilerin alındığı XLOG sistemi olduğu tahmin ediliyor.

Ancak ekip üyelerinin Wireshark programını giriş yapmadan denemesi üzerine XLOG sisteminin bir engelleme oluşturmadığını, ağın içerisindeki trafiğin giriş yapmadan izlenebildiği gözlemlenmiştir.

Ofiste XLOG sistemine herhangi bir bilgi vermeden ağı izlemeye devam eden ve Wireshark üzerinden takip eden ekip üyeleri, WI-FI ağına bağlanarak bir süre ağ üzerindeki veri akışını takip etti.

40 dakika süren Wireshark izlemesi sonucunda yaklaşık 90,000 veri paketi kontrol edildi.

WI-FI ağına bağlı olarak birbirleri ile iletişim kuran yazıcılar, modemler, routerlar, laptoplar, masaüstü bilgisayarlar, telefonlar ve yayın/projeksiyon cihazları olmak üzere toplamda 87 cihaz gözlemlendi.

Ofiste bulunan kişisel bilgisayarların büyük bir kısmının HP marka laptoplar oluşturuyor. Ofis içerisinde iletişim için Skype isimli uygulama, yazıcı markası olarak ise Kyocera tercih edilmekte. Modem ve router konusunda ise Tp-Link ve Cisco markaları göze çarpıyor.

## Sonuç:

Elazığ Ticaret Ve Sanayi Odası için gerçekleştirdiğimiz sızma testleri sonucunda tespit edilen hataları;

XLOG sisteminin bypass edilebilmesi.
Düşük performanslı hosting seçimi.
Çalışanların sosyal mühendisliğe müsait olması.
Harici ve güvenilir olmayan <iframe>.
Güncel olmayan jQuery sürümü.
Etkin olmayan HSTS ilkesi.
HTTPOnly olmayan çerez.
Zayıf WI-FI şifresi.

olarak listeleyebiliriz. Bu açıklardan ilk olarak XLOG sisteminde bulunan açığın düzeltilmesi tavsiye edilmektedir.