Invicti

Testing Site Sızma Testleri

Sonuç Raporu

Ahmet Sabri MERT

02.09.2022

1.

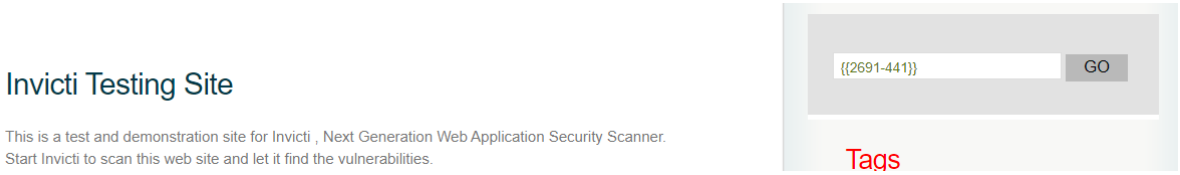
Bulgu Adı	Server-Side Template Injection (SSTI) Zafiyeti
Bulgu Seviyesi	Kritik
Risk/Etki	Yetkisiz Erişim
Bulgu Sebebi	Uygulama Geliştirmedeki Eksiklikler/Hatalar

Bulgu açıklaması:

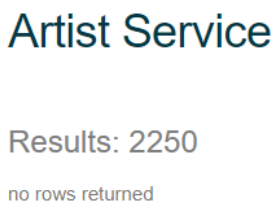
Yapılan testler sırasında bu sayfanın SSTI saldırılarına karşı savunmasız olduğu tespit edilmiştir. Saldırgan, template engine ifadeleri olarak değerlendirilebilecek verileri enjekte edebilir. Böylelikle bir sistemi keyfi bir sistem komutunu yürütmesi için kandırabilir. SSTI bulunmasına kanıt olarak örneğin ana sayfada bulunan input kısmına {{2691-441}} payloadı girildiğinde işlemin sonucu result olarak görülmektedir.

Kanıt urlsi:

http://php.testsparker.com/artist.php?id=%7B%7B2691-441%7D%7D+



Resim 1. Payload girişi



Resim 2. Başarılı bir şekilde sonuç alma

Çözüm önerileri:

- Kullanıcıların sağladığı verilere güvenilmemeli ve bunlar doğrudan şablona eklenmemelidir. Bunun yerine, kullanıcı tarafından kontrol edilen parametreler şablona şablon parametreleri olarak iletilmelidir.
- Meta karakter girişi engellenebilir.

2.

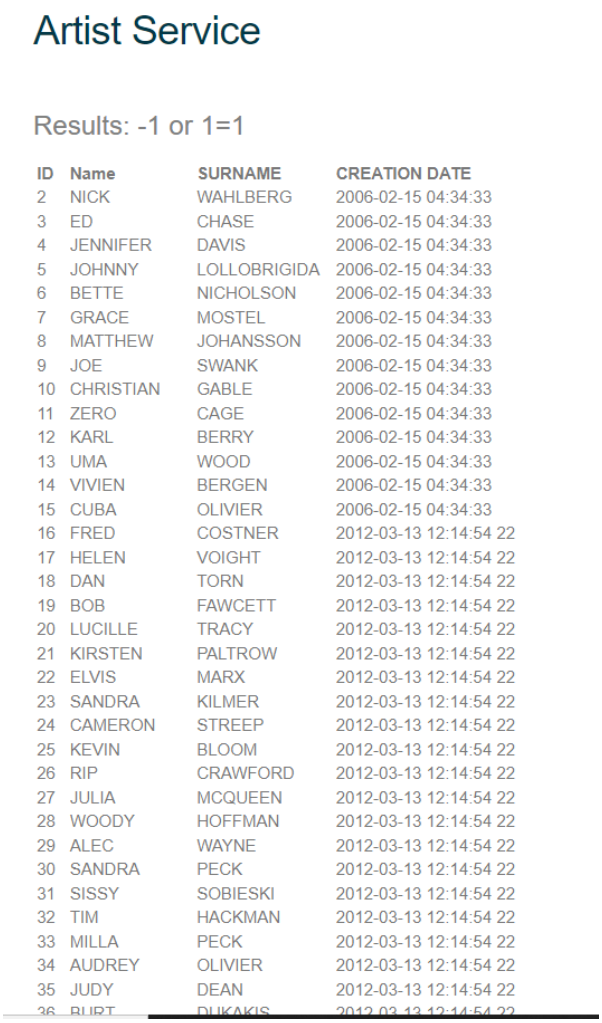
Bulgu Adı	Boolean Based SQL Injection Zafiyeti
Bulgu Seviyesi	Kritik
Risk/Etki	Yetkisiz Erişim, Bilgi İfşası
Bulgu Sebebi	Uygulama Geliştirmedeki Eksiklikler/Hatalar

Bulgu açıklaması:

Yapılan testler sırasında Boolean Based SQL Injection Zafiyeti tespit edilmiştir. Bu son derece yaygın bir güvenlik açığıdır ve başarılı bir şekilde kullanılmasının kritik sonuçları olabilir. Backend veritabanına, veritabanı bağlantı ayarlarına ve işletim sistemine bağlı olarak bir saldırgan, veritabanından rastgele veri okuma, güncelleme, silme ve temel işletim sisteminde komutları yürütme gibi saldırıları gerçekleştirebilir. Bu zafiyetin bulunmasına kanıt olarak ana sayfada bulunan input kısmına -1 or 1=1 payloadı girildiğinde veritabanında bulunan tüm "artist" kayıtları (id = 2 den id = 200'e kadar) görülebilmektedir.

Kanıt urlsi:

http://php.testsparker.com/artist.php?id=-1+or+1%3D1



Artist Service

Results: -1 or 1=1

ID	Name	SURNAME	CREATION DATE
2	NICK	WAHLBERG	2006-02-15 04:34:33
3	ED	CHASE	2006-02-15 04:34:33
4	JENNIFER	DAVIS	2006-02-15 04:34:33
5	JOHNNY	LOLLOBRIGIDA	2006-02-15 04:34:33
6	BETTE	NICHOLSON	2006-02-15 04:34:33
7	GRACE	MOSTEL	2006-02-15 04:34:33
8	MATTHEW	JOHANSSON	2006-02-15 04:34:33
9	JOE	SWANK	2006-02-15 04:34:33
10	CHRISTIAN	GABLE	2006-02-15 04:34:33
11	ZERO	CAGE	2006-02-15 04:34:33
12	KARL	BERRY	2006-02-15 04:34:33
13	UMA	WOOD	2006-02-15 04:34:33
14	VIVIEN	BERGEN	2006-02-15 04:34:33
15	CUBA	OLIVIER	2006-02-15 04:34:33
16	FRED	COSTNER	2012-03-13 12:14:54 22
17	HELEN	VOIGHT	2012-03-13 12:14:54 22
18	DAN	TORN	2012-03-13 12:14:54 22
19	BOB	FAWCETT	2012-03-13 12:14:54 22
20	LUCILLE	TRACY	2012-03-13 12:14:54 22
21	KIRSTEN	PALTROW	2012-03-13 12:14:54 22
22	ELVIS	MARX	2012-03-13 12:14:54 22
23	SANDRA	KILMER	2012-03-13 12:14:54 22
24	CAMERON	STREEP	2012-03-13 12:14:54 22
25	KEVIN	BLOOM	2012-03-13 12:14:54 22
26	RIP	CRAWFORD	2012-03-13 12:14:54 22
27	JULIA	MCQUEEN	2012-03-13 12:14:54 22
28	WOODY	HOFFMAN	2012-03-13 12:14:54 22
29	ALEC	WAYNE	2012-03-13 12:14:54 22
30	SANDRA	PECK	2012-03-13 12:14:54 22
31	SISSY	SOBIESKI	2012-03-13 12:14:54 22
32	TIM	HACKMAN	2012-03-13 12:14:54 22
33	MILLA	PECK	2012-03-13 12:14:54 22
34	AUDREY	OLIVIER	2012-03-13 12:14:54 22
35	JUDY	DEAN	2012-03-13 12:14:54 22
36	BURT	DUKAKIS	2012-03-13 12:14:54 22

Resim 3. SQL Injection sonucu elde edilen veriler

Çözüm önerileri:

- Kodun SQL Injectiona karşı korunmasının en iyi yolu parametreli sorgular (hazır ifadeler) kullanmaktır. Hemen hemen tüm modern diller bunun için yerleşik kütüphaneler sağlar. Mümkün olan her yerde, dinamik SQL sorguları oluşturulmamalıdır.

- Uygulama kodlarının gözden geçirilerek parametreler ve http başlığındaki diğer alanlar vasıtası ile yollanan her türlü bilginin kullanılmadan önce zararlı karakterlerden filtrelenmesi önerilmektedir.

- Uygulamalardaki bütün girdi noktalarından gelen değişkenler girdi kontrolüne sokulmalı ve bu girdilerdeki bütün meta karakterlerin filtrelenmesi önerilmektedir.

3.

Bulgu Adı	Güncel Olmayan PHP Sürümü
Bulgu Seviyesi	Kritik
Risk/Etki	Kod enjeksiyonu, Arabellek aşımı vs.
Bulgu Sebebi	Eski sürüm yazılım kullanımı

Bulgu açıklaması:

Yapılan testler sırasında güncel olmayan PHP 5.2.6 sürümünün kullanıldığı tespit edilmiştir. Bu sürüm eski bir sürüm olduğu için saldırılara açık olabilir. Aşağıdaki adreste PHP 5.2.6 sürümünün zafiyetleri yer almaktadır. Web sitesi, eski sürüm kullanılmaya devam edildiği sürece bu saldırılar tarafından tehdit altındadır.

https://www.cvedetails.com/vulnerability-list/vendor_id-74/product_id-128/version_id-404989/PHP-PHP-5.2.6.html

Çözüm önerileri:

- PHP en son sürüme yükseltilmelidir.

4.

Bulgu Adı	Güncel Olmayan Apache Sürümü
Bulgu Seviyesi	Kritik
Risk/Etki	Hatalı giriş, hatalı kimlik doğrulama vs.
Bulgu Sebebi	Eski sürüm yazılım kullanımı

Bulgu açıklaması:

Yapılan testler sırasında güncel olmayan Apache 2.2.8 sürümünün kullanıldığı tespit edilmiştir. Bu sürüm eski bir sürüm olduğu için saldırılara açık olabilir. Aşağıdaki adreste PHP 2.2.8 sürümünün zafiyetleri yer almaktadır. Web sitesi, eski sürüm kullanılmaya devam edildiği sürece bu saldırılar tarafından tehdit altındadır.

https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-66/version_id-416233/Apache-Http-Server-2.2.8.html

Çözüm önerileri:

- Apache en son sürüme yükseltilmelidir.

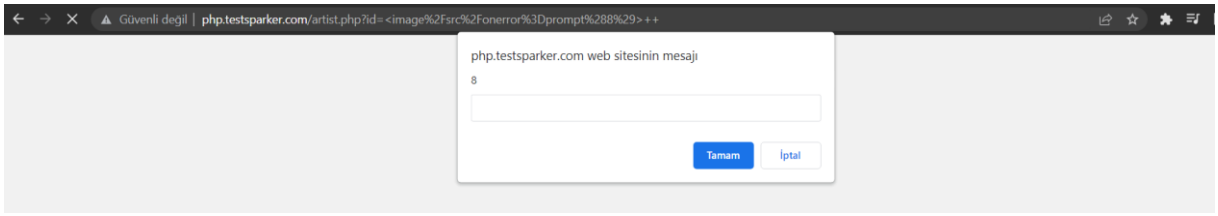
5.

Bulgu Adı	Cross-site Scripting (XSS) Zafiyeti
Bulgu Seviyesi	Yüksek
Risk/Etki	Yetkisiz Erişim
Bulgu Sebebi	Uygulama Geliştirmedeki Eksiklikler/Hatalar

Bulgu açıklaması:

Yapılan testler sırasında Cross-site Scripting (XSS) Zafiyeti tespit edilmiştir. XSS zafiyeti, saldırganların site üzerinde diğer kullanıcılara istemci tarafında çalışmak üzere kod gönderip kötü amaçlarla çalıştırmalarına imkân tanımaktadır.

XSS zafiyetleri uygulamalarda dışarıdan alınan bilgiler için yeterli girdi ve çıktı denetimini yapılmadığı durumlarda ortaya çıkar ve art niyetli kullanıcı istediği gibi javascript kodu çalıştırarak hedef aldığı kişilere ait oturum bilgilerini çalabilir ve browserlarını istediği gibi yönlendirebilir. Örnek olarak ana sayfadaki input kısmına <image/src/onerror=prompt(8)> payloadı girilerek XSS çalıştırılır ve aşağıdaki gibi bir görüntü ile karşılaşılır.



Resim 4. XSS çalıştıktan sonra karşılaşılan ekran

Kanıt urlsi:

http://php.testsparker.com/artist.php?id=%3Cimage%2Fsrc%2Fonerror%3Dprompt%288%29%3E++

Çözüm önerileri:

- Kodlar gözden geçirilerek payload çalıştırılamayacak şekilde düzenlenmelidir.
- Meta karakterler filtrelenebilir.
- Kullanıcı girişi front-end ve back-end'de temizlenerek, kötü amaçlı kodun giriş göndermesi engellenebilir.

6.

Bulgu Adı	SVN Tespiti
Bulgu Seviyesi	Yüksek
Risk/Etki	Yetkisiz Erişim, Bilgi İfşası
Bulgu Sebebi	Uygulama Geliştirmedeki Eksiklikler/Hatalar

Bulgu açıklaması:

Yapılan testler sırasında bir SVN repository dosyası tespit edilmiştir. SVN repository dosyaları, SVN adreslerini, SVN kullanıcı adlarını ve tarih bilgilerini ifşa edebilir. Bu tür ifşaatlar doğrudan saldırı şansı vermese de, diğer güvenlik açıklarıyla birleştiğinde veya diğer bazı güvenlik açıklarından yararlanılması sırasında bir saldırgan için yararlı olabilir.

Kanıt urlsi:

http://php.testsparker.com/.svn/all-wcprops

Çözüm önerileri:

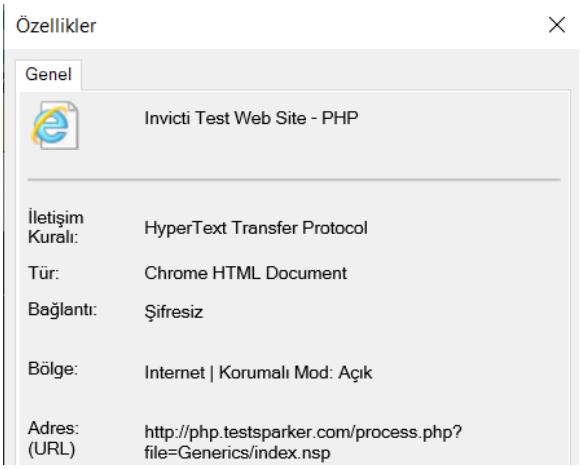
- SVN repository dosyaları üretim ortamlarında bırakılmamalıdır. Eğer bırakmak gerekiyorsa, bu dosyalara genel erişimi durdurmak için erişim kontrol mekanizmaları uygulanmalıdır.

7.

Bulgu Adı	Uygulanmamış SSL/TLS Zafiyeti
Bulgu Seviyesi	Orta
Risk/Etki	Bilgi İfşası
Bulgu Sebebi	Uygulama Geliştirmedeki Eksiklikler/Hatalar

Bulgu açıklaması:

Yapılan testler sırasında SSL/TLS'in uygulanmadığı tespit edilmiştir. Herhangi birinin veya onun kullanıcılarının ağ trafiğine müdahale edebilen bir saldırgan, sunucusuyla bu kişilerin arasında gelen ve giden tüm mesajları okuyabilir ve değiştirebilir. Bu, bir saldırganın şifreleri düz metin olarak görebileceği, web sitenizin görünümünü değiştirebileceği, kullanıcıyı diğer web sayfalarına yönlendirebileceği veya oturum bilgilerini çalabileceği anlamına gelir. Böylelikle sunucuya gönderilen hiçbir mesaj gizli kalmaz. Aşağıdaki resimde görüldüğü gibi bağlantı "Şifresiz" dir.



Resim 5. SSL/TLS eksikliği

Çözüm önerileri:

- Let's Encrypt sertifika yetkilisi tarafından sağlanan Certbot aracını kullanılarak SSL/TLS doğru şekilde uygulanmalıdır. Çoğu modern web sunucusu otomatik olarak yapılandırılabilir.

8.

Bulgu Adı	Ayarlanmamış İçerik Güvenliği Politikası (CSP) Başlığı Zafiyeti
Bulgu Seviyesi	Orta
Risk/Etki	Yetkisiz İşlem, Bilgi İfşası
Bulgu Sebebi	Uygulama Geliştirmedeki Eksiklikler/Hatalar

Bulgu açıklaması:

OWASP ZAP aracı kullanılarak yapılan taramada web sitesinde Ayarlanmamış İçerik Güvenliği Politikası (CSP) Başlığı Zafiyeti tespit edilmiştir. CSP, XSS ve veri enjeksiyon saldırıları dahil olmak üzere belirli saldırı türlerini algılamaya ve azaltmaya yardımcı olan ek bir güvenlik katmanıdır. CSP, web sitesi sahiplerinin, tarayıcıların o sayfada yüklemesine izin verilmesi gereken onaylı içerik kaynaklarını beyan etmesine olanak tanıyan bir dizi standart HTTP başlığı sağlar. Kapsanan türler JavaScript, CSS, HTML çerçeveleri, yazı tipleri, resimler ve Java uygulamaları gibi gömülebilir nesnelerdir.

Çözüm önerileri:

- Web sunucusunun, uygulama sunucusunun, yük dengeleyicisinin vb. en iyi tarayıcı desteğini elde etmek için İçerik Güvenliği Politikası başlığını ayarlayacak şekilde yapılandırıldığından emin olunmalıdır.

9.

Bulgu Adı	Eksik Anti-Clickjacking Başlığı Zafiyeti
Bulgu Seviyesi	Orta
Risk/Etki	Bilgi İfşası
Bulgu Sebebi	Uygulama Geliştirmedeki Eksiklikler/Hatalar

Bulgu açıklaması:

OWASP ZAP aracı kullanılarak yapılan taramada web sitesinde Eksik Anti-Clickjacking Başlığı Zafiyeti tespit edilmiştir. Clickjacking, kullanıcının görünmeyen veya başka bir öğe olarak gizlenmiş bir web sayfası öğesini tıklaması için kandıran bir saldırıdır. Bu, kullanıcıların farkında olmadan kötü amaçlı yazılım indirmesine, kötü amaçlı web sayfalarını ziyaret etmesine, kimlik bilgileri veya hassas bilgiler sağlamasına, para transfer etmesine veya çevrimiçi ürün satın almasına neden olabilir.

Çözüm önerileri:

- Modern Web tarayıcıları, CSP ve X-Frame-Options HTTP başlıklarını destekler. Site/uygulama tarafından döndürülen tüm web sayfalarında bunlardan birinin ayarlandığından emin olunmalıdır.
- Sayfanın yalnızca sunucudaki sayfalar tarafından çerçevelenmesi bekleniyorsa SAMEORIGIN kullanılacaktır aksi takdirde sayfanın çerçevelenmesi hiç beklenmiyorsa DENY kullanılmalıdır. Alternatif olarak, CSP'nin "frame-ancestors" yönergesinin uygulanması düşünülebilir.

10.

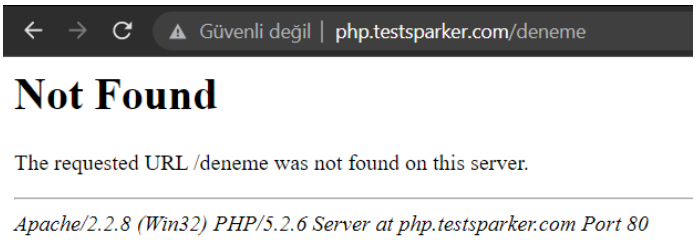
Bulgu Adı	PHP ve Apache Sürüm İfşası
Bulgu Seviyesi	Düşük
Risk/Etki	Bilgi İfşası
Bulgu Sebebi	Uygulama Geliştirmedeki Eksiklikler/Hatalar

Bulgu açıklaması:

Yapılan testler sırasında hedef web sunucunun HTTP responseunda PHP ve Apache sürüm ifşası olduğu tespit edilmiştir. Bu bilgi, bir saldırganın kullanılan sistemler hakkında daha iyi bir anlayış kazanmasına ve potansiyel olarak PHP ve Apache'nin belirli bir sürümünü hedefleyen başka saldırılar geliştirmesine yardımcı olabilir.

Kanıt urlsi:

https://php.testsparker.com/deneme



Resim 6. PHP ve Apache sürüm ifşası

Çözüm önerileri:

- HTTP responseunun SERVER başlığından bilgi sızıntısını önlemek için web sunucusu yapılandırılmalıdır.

11.

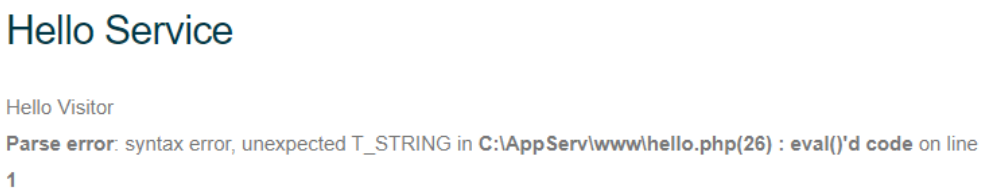
Bulgu Adı	Programlama Hata Mesajı
Bulgu Seviyesi	Düşük
Risk/Etki	Bilgi İfşası
Bulgu Sebebi	Uygulama Geliştirmedeki Eksiklikler/Hatalar

Bulgu açıklaması:

Yapılan testler sırasında web sitesinde programlama hata mesajlarının olduğu gözlemlenmiştir. Hata mesajı hassas bilgileri ifşa edebilir ve bu bilgiler bir saldırgan tarafından yeni saldırılar düzenlemek veya saldırı yüzeyini genişletmek için kullanılabilir. Kaynak kodu, yığın izleme vb. veriler ifşa edilebilir.

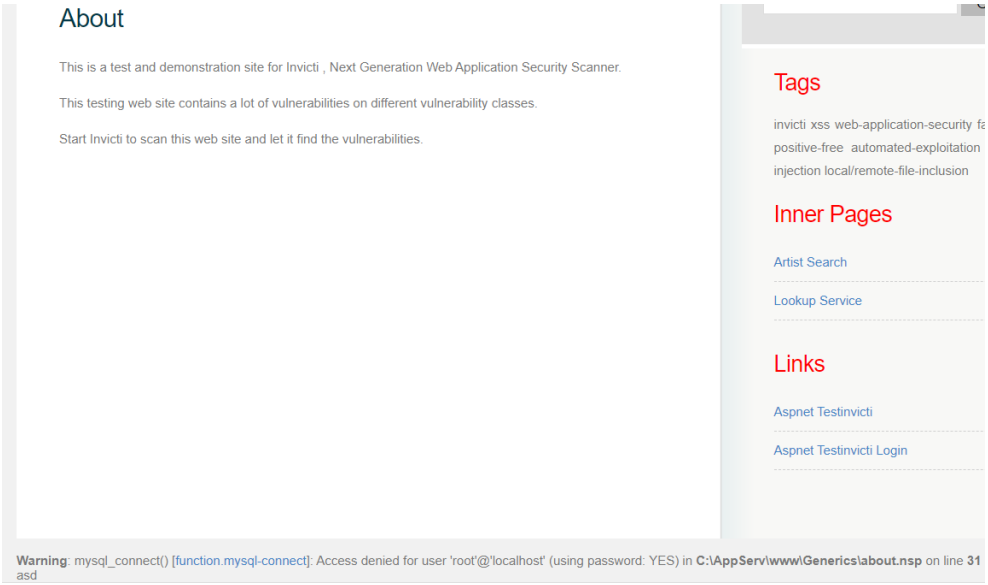
Kanıt urlleri:

http://php.testsparker.com/hello.php?name=hello.php



Resim 7. Programlama hata mesajı (1)

http://php.testsparker.com/process.php?file=Generics/about.nsp



Resim 8. Programlama hata mesajı (2)

Çözüm önerileri:

- Üretim ortamlarında hata mesajları verilmemelidir.
- Bir referans numarasıyla hata mesajları backend deposuna kaydedilmelidir. Örneğin bir kayıt, metin dosyası veya veritabanı gibi, ardından bu numarayı ve kullanıcıya statik, kullanıcı dostu bir hata mesajı gösterilebilir.

12.

Web sitesinin güvenliği için kişisel öneri:

Kullanıcı girişi kısmında Captcha (Güvenlik karakteri) kullanılması önerilmektedir. Captcha, her oturum açma aşamasında rastgele karakterler çıkartılarak bunun kullanıcı tarafından girilmesi işlemidir. Bu yöntem saldırganların sistem üzerinde erişim elde edememeleri için uygulanan ek bir güvenlik önlemidir.