GİRDİ/ÇIKTI DENETİMİ 1

Alp, kendisi de kullanıcısı olduğu hedef uygulamaya özel yazdığı Javascript kodu göndererek başka bir uygulama kullanıcısının veya daha kötüsü yönetici kullanıcısının oturum id, kullanıcı adı, şifre gibi bilgilerini kendi sitesine yönlendirmek suretiyle çalabilir...

KRİTİK	HANGİ ÖNLEM?
4	* kara liste * beyaz liste * normalizasyon * doğru kodlama

SANS Top 25	MITRE CWE	OWASP ASVS
4	79	5.15

sourceflake.com

GİRDİ/ÇIKTI DENETİMİ 2

Deniz, hedef uygulamaya SQL komut parçaları göndererek uygulama veritabanından hassas bir çok veriyi çalabilir, hatta veritabanında komutlar çalıştırarak dahili ağa sızabilir...

ACİL	HANGİ ÖNLEM?
5	* doğru kodlama * prepared statement * stored procedure

SANS Top 25	MITRE CWE	OWASP ASVS
1	89	5.10

sourceflake.com

GİRDİ/ÇIKTI DENETİMİ 3

Özay, kara liste girdi denetimi stratejisi kullanılan hedef uygulamadaki kontrolleri, saldırı payload'ları üzerinde bir veya birden fazla kere URL encode, HTML encode transformasyon teknikleri uygulayarak atlatabilir...

ACİL	HANGİ ÖNLEM?
5	* kara liste * beyaz liste * normalizasyon * doğru kodlama

SANS Top 25	MITRE CWE	OWASP ASVS
10	807	N/A

sourceflake.com

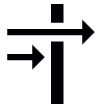
GİRDİ/ÇIKTI DENETİMİ 4

Can, XML gönderebildiği hedefindeki uygulamaya, XML DTD (Document Type Definition) standardının özelliklerini kullanıp kendi ürettiği XML dosyasını yükleyerek sunucuda istediği komutu çalıştırabilir, hassas sunucu dosyalarını görüntüleyebilir...

ACİL	HANGİ ÖNLEM?
5	* XML file size control * DTD kısmının işlenmemesi * DTD içindeki değişkenlerin silinmesi

SANS Top 25	MITRE CWE	OWASP ASVS
N/A	611	5.14

sourceflake.com



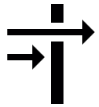
YETKİLENDİRME 1

Bedirhan, kullandığı hedef uygulamaya giden HTTP GET veya HTTP POST istekler içinde varolan parametre değerlerini değiştirerek başka kullanıcıların verilerini görebilmekte veya değiştirebilmektedir...

ACİL	HANGİ ÖNLEM?
5	* parametre sahiplik kontrolü * parametre şifreleme * HTML hidden parametreler

SANS Top 25	MITRE CWE	OWASP ASVS
15	863	4.4

sourceflake.com



YETKİLENDİRME 2

Caner, kullandığı hedef uygulamaya giden özellikle HTTP POST istekler içindeki parametrelere ek yeni parametre isimleri ve değerleri göndererek değiştirmesi yasak olan bilgilerini değiştirebilir. Örneğin kendini yönetici yapabilir veya kota miktarını arttırabilir.

ACİL	HANGİ ÖNLEM?
5	* parametre beyaz listeleri * parametre kara listeleri * parametre sahiplik kontrolü

SANS Top 25	MITRE CWE	OWASP ASVS
N/A	915	5.16

sourceflake.com

OTURUM YÖNETİMİ 1

Şenol, havalimanında bir kullanıcının kendi hesabından çıkış (logout) işlemini yapmadığı bir KIOSK web uygulamasında tarayıcının adres kısmına Javascript yazarak elde ettiği oturum bilgisini kullanarak kullanıcıymış gibi hedef uygulamaya girebilmektedir...

YÜKSEK	HANGİ ÖNLEM?
3	* oturum zaman aşımı * HTTPS kullanımı * httponly cookie'ler

SANS Top 25	MITRE CWE	OWASP ASVS
N/A	613	3.3

sourceflake.com

OTURUM YÖNETİMİ 2

Ayşe, kullanıcısı olduğu web uygulamasını kullanırken tarayıcısında başka bir tab'da Mehmet'nin sitesini açtığında, Mehmet'in yazdığı Javascript kodları Ayşe'nin haberi olmadan web uygulamasına sahte istekler gönderebilmektedir...

YÜKSEK	HANGİ ÖNLEM?
3	* synchronizer token * SMS OTP * CAPTCHA

SANS Top 25	MITRE CWE	OWASP ASVS
12	352	4.13

sourceflake.com

KRİPTOGRAFİ 1

PCI-DSS, ISO27001, SOX güvenlik politikaları ve BDDK, BTK gibi regülasyon kurumları, veritabanlarında kullanıcı şifrelerinin, kredi kartı numaralarının, haberleşme bilgilerinin şifreli tutulmasını zorlamaktadırlar...

ACİL	HANGİ ÖNLEM?
5	* Base64 Encoding kullanılması * Veritabanının şifrelenmesi * İlgili alanların şifrelenmesi

SANS Top 25	MITRE CWE	OWASP ASVS
8	311	7.12

sourceflake.com

KRİPTOGRAFİ 2

Ahmet, hedef uygulamada bulduğu başka bir güvenlik açığı yolu ile çaldığı veritabanında şifreler tuzsuz MD5, SHA-1 gibi kriptografik hash algoritmaları kullanılarak tutulduğundan, uygulama kullanıcı şifrelerine rahatlıkla erişebilmektedir...

YÜKSEK	HANGİ ÖNLEM?
3	* Bcrypt kullanılması * Tuzlu hash kullanılması * SHA-2 kullanılması

SANS Top 25	MITRE CWE	OWASP ASVS
19,25	327,759	7.7

sourceflake.com

KRİPTOGRAFİ

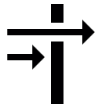
3

Metin, Starbacks'ta laptopunu açıp hedef uygulamayı kullanan müşteriler ile hedef uygulama sunucusu arasına girerek, kullanıcıların oturum id'lerini, kullanıcıların haberi olmadan çalabilmektedir.

ACİL	HANGİ ÖNLEM?
5	* HTTPS kullanımı * Websocket kullanılması * secure cookie attribute'u

SANS Top 25	MITRE CWE	OWASP ASVS
19	327	10.3

sourceflake.com



YETKİLENDİRME

3

Ömer, hedef uygulamanın gizli olduğu düşünülen yönetici arayüzüne /admin ile erişip, yöneticinin kullanıcı adı ve şifrelerine deneme yanılma saldırısı gerçekleştirebilir...

YÜKSEK	HANGİ ÖNLEM?
3	* IP kısıtlaması * CAPTCHA * Karmaşık yönetici URL'i

SANS Top 25	MITRE CWE	OWASP ASVS
6	862	2.32

sourceflake.com

DİZAYN 1

Murat, kaynak kod içerisinde gömülü yetkilendirme kodlarına, şifrelere veya hassas verilere uygulamayı decompile ederek erişebilmektedir...

ACİL	HANGİ ÖNLEM?
5	* Kod karmaşıklaştırma * Şifrelerin gömülü olmaması

SANS Top 25	MITRE CWE	OWASP ASVS
7	798	17.4

sourceflake.com

DİZAYN 2

Mesut, numerik olan HTTP parametrelerine maximum integer değerini göndererek uygulamada aritmetik algoritmaların beklenmeyen çok büyük negatif değerler üretmesini tetikleyebilmektedir...

YÜKSEK	HANGİ ÖNLEM?
3	* Unsigned int kullanılması * Tam sayı taşma kontolleri * String to Int cast yapılması

SANS Top 25	MITRE CWE	OWASP ASVS
24	190	N/A

sourceflake.com

KİMLİK DOĞRULAMA 1

Özer, hedef uygulamaya sahte IP değerleri ile HTTP X-Forwarded-For başlığı göndererek, kayıt bilgilerini geçersiz hale getirebilmekte veya daha kötüsü IP kısıtlama işlemlerini aşabilmektedir...

ACİL	HANGİ ÖNLEM?
5	* XFF'de ilk IP'nin kullanılması * XFF'nin LB'de silinmesi * XFF'de son IP'nin kullanılması

SANS Top 25	MITRE CWE	OWASP ASVS
N/A	348	11.3

sourceflake.com

KİMLİK DOĞRULAMA 2

Behruz, hedef uygulamanın zorunlu kıldığı ilk CAPTCHA değerini çözdükten sonra aynı değeri kullanarak kullanıcı adı ve şifreler için deneme-yanılma saldırıları yapabilmektedir...

KRİTİK	HANGİ ÖNLEM?
4	* Karmaşık CAPTCHA'lar * SMS OTP * CAPTCHA değerinin her kullanımda oturumdan silinmesi

SANS Top 25	MITRE CWE	OWASP ASVS
N/A	294	N/A

sourceflake.com

Güvenli Kod Geliştirme Eğitimleri

www.sourceflake.com