Parse HTML Reponses

- Determining parameters that affect content.
- Comparing dynamic content.
- Comparisons that don't require manual intervention.

Parse HTML Reponses

- HTML Comments
  - `<!-- ServerInfo: BAYPPLOGU2A07 2005.08.30.21.29.11 Live1 ExclusiveNew LocVer:0 -->`
  - `<!-- ServerInfo: BAYPPLOGU2B01 2005.08.30.21.29.11 Live1 ExclusiveNew LocVer:0 -->`
  - `<!-- ServerInfo: BAYPPLOGU3B07 2005.08.30.21.29.11 Live1 ExclusiveNew LocVer:0 -->`

Parse HTML Reponses

- Other HTML elements
  - `<META name="DateInSecsSinceEpoch" content="1134594211">`
  - `<META name="DateInSecsSinceEpoch" content="1134594292">`
- Different anchor (<a>) content
- Ad banner constructs

Parse HTML Reponses

- Timestamps
  - `Wednesday, December 14 2005: 15:50:51`
  - `Page generated in: 0.0013 seconds`
  - `Page generated in 0.325261 seconds`
  - `Updated: 12:48 PM PST`
  - `GENERATED: Wednesday, 14-Dec-2005 20:07:07 GMT`

Complex Queries

- Handling large record sets.
- Handling unknown data types.
- Problems with GROUP BY and ORDER BY

Countermeasures

Countermeasures

- These attacks rely on normal SQL injection attack vectors.
  - Create queries with bound parameters
  - Use stored procedures where possible
    - Don't use string concatenation to build it!
  - Perform strong input validation
- Most important to reduce access privileges for the application's database connection!

Questions

Addition Information

- Data-mining with SQL Injection and Inference, David Litchfield
  www.ngssoftware.com/papers/sqlinference.pdf
- Absinthe: SQL injection automation (tool & slides)
  www.0x90.org/releases/absinthe/
- (more) Advanced SQL Injection, Chris Anley
  www.ngssoftware.com/papers/more_advanced_sql_injection.pdf
- Advanced SQL Injection in SQL Server Applications, Chris Anley
  www.ngssoftware.com/papers/advanced_sql_injection.pdf
- Blind SQL Injection: Are your web applications vulnerable?, Kevin Spett
  www.spidynamics.com/assets/documents/Blind_SQLInjection.pdf

...and the movies of John Carpenter (www.theofficialjohncarpenter.com)