Information Leakage

Laurie Williams
williams@csc.ncsu.edu

What Do Attackers Want?

• Architecture details
  – Network topology
  – Application, database, and web and server details

• Application implementation details
  – Classes
  – Files and their layout
  – Database tables, field names

• Confidential data
Leak Sources

- Error message
- Comments and other clues
- Plain sight
- Physical media

Error Message Information Leakage

**CWE-209: Information Exposure Through an Error Message**

<table>
<thead>
<tr>
<th>Summary</th>
<th>Weakness Prevalence</th>
<th>Remediation Cost</th>
<th>Attack Frequency</th>
<th>Consequences</th>
<th>Ease of Detection</th>
<th>Attacker Awareness</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>High</td>
<td>Low</td>
<td>Often</td>
<td>Data loss</td>
<td>Easy</td>
<td>High</td>
</tr>
</tbody>
</table>

- **Condition:** If you use chatty error messages, then they could disclose secrets to any attacker who dares to misuse your software.
- **Consequences:** The secrets could cover a wide range of valuable data, including personally identifiable information (PII), authentication credentials, and server configuration. Sometimes, they might seem like harmless secrets that are convenient for your users and administrators, such as the full installation path of your software. Even these little secrets can greatly simplify a more concerted attack that yields much bigger rewards.

http://cwe.mitre.org/top25/#CWE-209
Gathering info for SQL Injection

The following was returned when placing an apostrophe into the username filed of a login page:

Verbose error message:

An Error Has Occurred.

In the first error statement a syntax error is reported. The error message reveals the query parameters that are used in the SQL query: username and password. This leaked information is the missing link for an attacker to begin to construct SQL Injection attacks against the site.

http://www.webappsec.org/projects/threat/classes/information_leakage.shtml

Narrowing down the errors

- Don’t say what’s wrong when dealing with sensitive data.

Sign in to Gmail with your Google Account
Username: lauriewilliams
Password: ********

Sign In

Stay signed in

The username or password you entered is incorrect. [2]

Sign in to Gmail with your Google Account
Username: lauriewilliams
Password: ********

Sign In

Your User ID or Password has been entered incorrectly (passwords are case sensitive). (MessageNumber 13)

Sign In

Incorrect userid/incorrect password

Sign In

Your User ID and/or Password are invalid.

Correct userid/incorrect password
Prevention and Mitigation

- Ensure that error messages only contain minimal information that are useful to their intended audience, and nobody else. The messages need to strike the balance between being too cryptic and not being cryptic enough. They should not necessarily reveal the methods that were used to determine the error. Such detailed information can help an attacker craft another attack that now will pass through the validation filters.
- If errors must be tracked in some detail, capture them in log messages - but consider what could occur if the log messages can be viewed by attackers.
- Handle exceptions internally and do not display errors containing potentially sensitive information to a user.
- Create default error pages or messages that do not leak any information.

Video

- http://www.youtube.com/watch?v=PB7hW1qTSqs&feature=related
Source of Leak

• Error message
• Comments and other clues
• Plain sight
• Physical media

Information Leakage via Comments

• Provides host IP Address

Using nmap an attacker could send a few packets at your application server using the command, nmap -v -p 80 192.168.1.100 and identify the following:

Interesting ports on 192.168.10.132:
PORT    STATE SERVICE   VERSION
80/tcp   open     http    Apache httpd 1.3.37

The attacker has now identified your Apache version and can now search for vulnerabilities affecting that version of Apache.

http://projects.webappsec.org/Information-Leakage
Google hacking

- Find Microsoft Excel files that contain login names and passwords
  - "login: " "password: " filetype:xls
- Locate passwords in plain text found in exposed log files
  - "your password is" filetype:log
- Discover insecure instances of the phpMyAdmin database frontend
  - "Welcome to phpMyAdmin" "Create new database"
  - intitle:PhpMyAdmin "Welcome to phpMyAdmin" running on as root"
- Find human resources web sites from the internal intranet which are accessible to external users
  - intitle:intranet inurl:intranet +intext:"human resources"
- Search for private contact lists that have been synced up from PDA’s or cell phones
  - contacts ext:wml

http://johnny.ihackstuff.com
http://netsecurity.about.com/od/perimetersecurity/a/4_leakage.htmll

Source of Leak

- Error message
- Comments and other clues
- Plain sight
- Physical media
Confidential data in plain sight

- Protect from the casual observer

Now I search for vulnerabilities for these versions!
Testing for Information Leakage

- Identify error conditions that are not likely to occur during normal usage and trigger them. For example, run the program under low memory conditions, run with insufficient privileges or permissions, interrupt a transaction before it is completed, or disable connectivity to basic network services such as DNS.
- Determine if the application provides information that could be used to attack the system.

Source of Leak

- Error message
- Comments and other clues
- Plain sight
- Physical media

http://cwe.mitre.org/top25/#CWE-209
Physical media

- USB Drives
- Printing … etc

HIPAA Breach Data

**Table 1**

<table>
<thead>
<tr>
<th>Breach Count Type/Location</th>
<th>Theft</th>
<th>Unauthorized Access/Disclosure</th>
<th>Loss</th>
<th>Hacking/IT Incident</th>
<th>Improper Disposal</th>
<th>Unknown</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper</td>
<td>27</td>
<td>46</td>
<td>13</td>
<td></td>
<td>20</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Laptop</td>
<td>07</td>
<td>5</td>
<td>4</td>
<td></td>
<td>1</td>
<td>97</td>
<td></td>
</tr>
<tr>
<td>Computer</td>
<td>51</td>
<td>10</td>
<td>4</td>
<td>10</td>
<td>1</td>
<td>36</td>
<td></td>
</tr>
<tr>
<td>Other Portable Electronic Device</td>
<td>40</td>
<td>2</td>
<td>25</td>
<td></td>
<td>1</td>
<td>68</td>
<td></td>
</tr>
<tr>
<td>Network Server</td>
<td>16</td>
<td>18</td>
<td>1</td>
<td>21</td>
<td>1</td>
<td>57</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>4</td>
<td>7</td>
<td>11</td>
<td></td>
<td>1</td>
<td>1</td>
<td>24</td>
</tr>
<tr>
<td>Email</td>
<td>2</td>
<td>6</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electronic Medical Record</td>
<td>4</td>
<td>4</td>
<td>1</td>
<td></td>
<td>1</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>X-ray film</td>
<td>3</td>
<td></td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backup tape</td>
<td>1</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compact Disc</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hard drive</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>235</strong></td>
<td><strong>98</strong></td>
<td><strong>62</strong></td>
<td><strong>35</strong></td>
<td><strong>23</strong></td>
<td><strong>6</strong></td>
<td><strong>2</strong></td>
</tr>
</tbody>
</table>

What do do …

• Organization security policies
• Not making printing easy
• Notifying “someone” when a copy of a file is made
• ....