Authentication Security

Hui Zhu
Agenda

• Authentication Components
• Authentication Hacking
• Consideration for Authentication Security
• Principle for Authentication Security
• Case Study
Authentication components

- Login
- Logout
- Registration or Enrolment
- “Forget Password” Function
- “Reset Password” Function
- De-registration
Authentication Hacking

- Server-side Hacking
  - Authentication Bypass
  - Authentication Replay
  - Session Attack
  - Information Disclosure
  - Brute Force and Dictionary Attack
  - Denial of Service Attack
  - Business Logic Vulnerability
  - Miscellaneous Vulnerability
Authentication Hacking

• Client-side Hacking
  – Man-in-the-Middle Attack
  – Sniffing
  – Phishing Attack
  – Keystroke and Screen Logger
  – Password Disclosure
  – Denial-of-Service Attack
Authorization Bypass
(server-side)

Gain unauthorized access to the application without knowing password and/or username.

• Impact: High
• Levels of skills required: Medium
• Likelihood of Occurrence: High
Authentication Bypass (server-side)

strUsername = request.getParameter("username");
StrUserPassword = request.getParameter("password");
 strSQL = "select * from login where username=" + strUsername + " and password=" + strUserPassword;
db.setNType(0);
db.setStrQuery(strSQL);
db.run();
sqlRst = db.getSqlRst();
sqlRst.last();
intRowCount = sqlRst.getRow();
If (intRowCount <= 0) login=false;
else login=true;

• http://www.vulnerable.com/login.jsp?username=hack&password=1%20or%201=1
Authentication Bypass (server-side)

.NET forms authentication vulnerability
A standard forms authentication setup requires the presence of "web.config" to set the authentication method and login procedure. The presence of this file prevents access to certain files (.aspx files for example) unless authenticated.

Normal Request:
http://localhost/secure/somefile.aspx

Attacks:
http://localhost/secure\somefile.aspx (Mozilla)
http://localhost/secure%5Csomefile.aspx (IE)
Authentication Replay (Server-side)

Replay the victim’s authentication request by exploiting the caching feature provided by the browser.

- Impact: High
- Levels of skills required: Low
- Likelihood of Occurrence: High
Authentication Replay
(Server-side)
Authentication Replay
(Server-side)
Authentication Replay (Server-side)
Authentication Replay (Server-side)
Session Attack (server-side)

Take advantage of the weak session management to break into or hijack authenticated session

- Impact: High
- Levels of skills required: High
- Likelihood of Occurrence: Medium
Session Attack
(server-side)

- Cookie:
  timestamp=9894849323&UserID=dragon001&sessionkey=87928942
Information Disclosure (Server-side)

Discover sensitive information from weak authentication process

- Impact: Low
- Levels of skills required: Low
- Likelihood of Occurrence: High
Brute Force and Dictionary Attack (Server-side)

Gain unauthorized access by trying a large number of possibilities from dictionary or wordlist, or exhaustively working through all possible passwords

- Impact: Low
- Levels of skills required: Medium
- Likelihood of Occurrence: Low
Brute Force and Dictionary Attack (Server-side)
Denial-of-Service
(Server-side)

prevent legitimate user’s access, by exhausting various computing resource, such as network bandwidth, CPU time, memory, hard disk, etc

• Impact: High
• Levels of skills required: Medium
• Likelihood of Occurrence: Medium
Business Logic Vulnerability (Server-side)

Explore the weakness in the business logic design to gain unauthorized access

• Impact: High
• Levels of skills required: Medium
• Likelihood of Occurrence: Medium
Miscellaneous Vulnerabilities

CAPTCHAs - Completely Automated Public Turing test to tell Computers and Humans Apart

PWNTcha - http://sam.zoy.org/pwntcha/

Man-in-the-Middle Attack
(Client-side)

Attacker intercept, alter the traffic between two parties without either party knowing that the link between them has been compromised

- Impact: High
- Levels of skills required: High
- Likelihood of Occurrence: Low
Sniffing (Client-side)

Capture the user credentials from network traffic, proxy, caching, etc

- Impact: High
- Levels of skills required: High
- Likelihood of Occurrence: Medium
Phishing Attack  
(Client-side)

use 'spoofed' e-mails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers

• Impact: High
• Levels of skills required: High
• Likelihood of Occurrence: High
Dear client of the Citi,

As the Technical service of the Citibank have been currently updating the software, we kindly ask you to follow the reference given below to confirm your data, otherwise your access to the system may be blocked.


We are grateful for your cooperation.

A member of citigroup
Copyright © 2004 Citicorp
Phishing Attack (Client-side)
Key Logger, Screen Logger (Client-side)

Capture user keystroke, mouse click and screen to discover the username and password, even with the on-screen keyboard.

- Impact: High
- Levels of skills required: High
- Likelihood of Occurrence: Medium
Key Logger, Screen Logger (Client-side)
Key Logger, Screen Logger (Client-side)
Password Discovery (Client-side)

Discover the password from browser cache, history list, memory in client’s PC

• Impact: High
• Levels of skills required: High
• Likelihood of Occurrence: Low
Password Discovery
(Client-side)
Password Discovery
(Client-side)
Password Discovery
(Client-side)

• For example, an online banking application stored the password in memory like the following:

```
FEFFFEFF75007600770078003100320033003400FEFFFEFF
```

• The password “uvwx1234” is encoded by Unicode and stored in memory with “FEFFFEFF” as delimiters. It is simple to search for FEFFFEFF to find the password.
Denial-of-Service Attack
(Client-side)

prevent legitimate users’ access to the web application, by sabotage the users’ computer

• Impact: High
• Levels of skills required: High
• Likelihood of Occurrence: Low
Consideration for Authentication Security

• Security requirement
• Risk assessment and/or threat modeling
• User acceptance
• Application performance
• Compatibility
• Cost of implementation
Principles for Authentication Security

- Proper input validation and output verification
- Always use “post” for form variable submission
- Non-cache and immediately expire all the web pages
- Manage user sessions and transaction sessions properly
- Use strong session management mechanism
Real World Case Study

```
login to citibank
with your card number and PIN

Card Number

Please use your mouse to enter your PIN

[8] [2] [4] [6] [0]
[5] [3] [9] [7] [1]

Clear

[ ] Remember my Card Number

Need Help?
Forgot your PIN?
```

Mar 8 2006

Copyright 2006 www.eBizSec.com
Real World Case Study
CookieRevolver

http://sourceforge.net/projects/cookie-revolver
CookieRevolver

The first time a system is used by a browser, this is the process:
- Browser gets a new machine-id cookie
- User authenticates with username/password
- User answers preset security question
- Browser gets a new certificate cookie
- User is redirected to the site main page

For most interaction with a CookieRevolver secured site, this is the process:
- Browser sends machine-id cookie
- User authenticates with username/password
- Browser sends and gets a new certificate cookie
- User is redirected to the site main page
Cookie Revolver

Cookie

- certtest001=EtDPWHDLhISEt5NxkqPZVmWFVWNZRkXHuYYcSOqJ27611qtyuYKA%2BknmKdAzxPcEsnaKJI8hFdFd%0D%0AZ00pOEeklxuiUCDSHe%2BqplKlY4inQdiZ%2F2VACue8DbL8rvQNgjpXnHqBOEo7f6%2BbTx3dALjmZ8G2%0D%0Aqv4EJa075Tt2Cg%2BwL74%3D;JSESSIONID=74D44E606788EF36AF174C2BBF7E7E92

- {machine='36d5c75f-a064-4ae3-86eb-b727f0e95ee0'(homepc),userName=test001,loginFailures='0',cert='id=8a8aac01-dd3e-4bd9-be5c-8ec8e39d6a05&userID=test001'}
## CookieRevolver

<table>
<thead>
<tr>
<th>Test Case</th>
<th>Impact</th>
<th>Risk rating</th>
<th>Finding</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Side</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication Bypass</td>
<td>N/A</td>
<td>N/A</td>
<td>No</td>
</tr>
<tr>
<td>Authentication Replay</td>
<td>N/A</td>
<td>N/A</td>
<td>No</td>
</tr>
<tr>
<td>Session Attack</td>
<td>N/A</td>
<td>N/A</td>
<td>No</td>
</tr>
<tr>
<td>Information Disclosure</td>
<td>N/A</td>
<td>N/A</td>
<td>No</td>
</tr>
<tr>
<td>Brute Force and Dictionary Attack</td>
<td>N/A</td>
<td>N/A</td>
<td>No</td>
</tr>
<tr>
<td>Denial-of-Service Attack</td>
<td>N/A</td>
<td>N/A</td>
<td>No</td>
</tr>
<tr>
<td>Business Logic Vulnerabilities</td>
<td>N/A</td>
<td>N/A</td>
<td>No</td>
</tr>
<tr>
<td><strong>Client Side</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Man-in-the-Middle Attack</td>
<td>Medium</td>
<td>Low</td>
<td>Vulnerable but difficult to explore</td>
</tr>
<tr>
<td>Sniffing</td>
<td>Medium</td>
<td>Low</td>
<td>Vulnerable but difficult to explore</td>
</tr>
<tr>
<td>Phishing Attack</td>
<td>Medium</td>
<td>Low</td>
<td>Vulnerable but difficult to explore</td>
</tr>
<tr>
<td>Key and screen Logger</td>
<td>Low</td>
<td>Low</td>
<td>Vulnerable but difficult to explore</td>
</tr>
<tr>
<td>Password Discovery</td>
<td>Low</td>
<td>Low</td>
<td>Vulnerable but difficult to explore</td>
</tr>
<tr>
<td>Denial-of-Service Attack</td>
<td>Low</td>
<td>Low</td>
<td>Vulnerable but can be fixed</td>
</tr>
</tbody>
</table>
Reference

- Directory traversal http://www.imperva.com/application_defense_center/glossary/directory_traversal.html
- Phishing http://www.antiphishing.org/
- Application Denial of Service (DoS) Attacks http://www.corsaire.com/
- Open Source Web Application Security Project (OWASP) http://www.owasp.org
- Dos and Don’ts of Client Authentication on the Web http://cookies.lcs.mit.edu
Reference

- Osk.exe - On-screen keyboard in Windows
- [http://www.mykeylogger.com/](http://www.mykeylogger.com/)
- **My Little Spy** is intended for recording a file of everything that is entered from the keyboard. My Little Spy works without being seen, and can be recalled by a combination of keys. My Little Spy records all email, chats conversations, instant messengers (ICQ, MSN, Yahoo, AIM ...), usernames and passwords, all keystrokes typed, in one word, everything. It records all text that has been on the clipboard (copy/paste), window titles and takes pictures of the screen as well.
• zhusec005@yahoo.com

• www.ebizsec.com