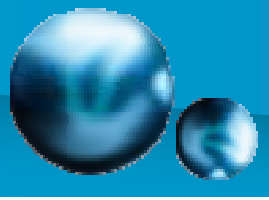
Web2.0 Secure Development Practice

Bruce Xia

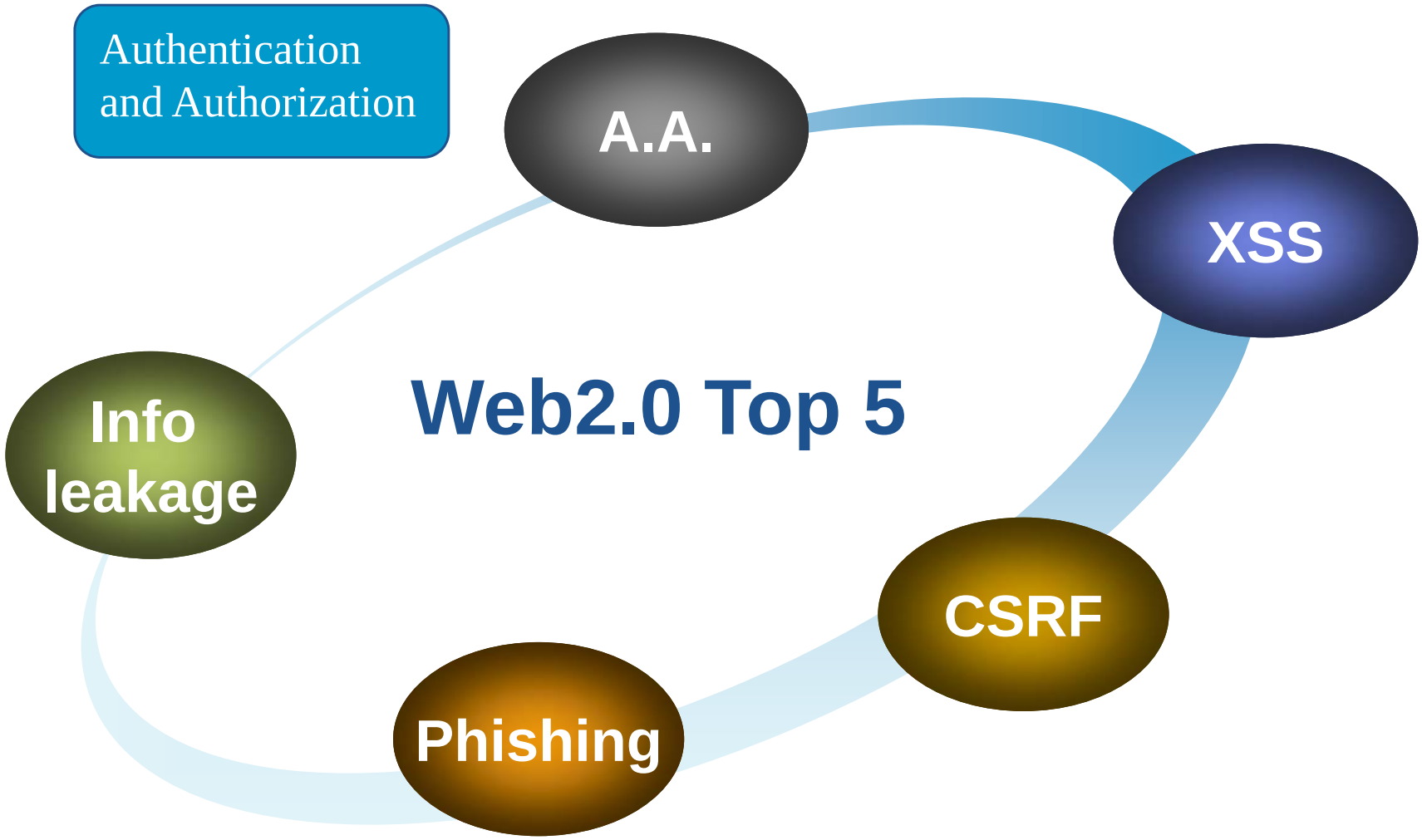
brucexym@gmail.com

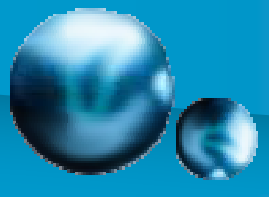


Agenda

- Background
- User Access Control
- Session Management
- Output Filtering
- Data Security and Misc

Background


Authentication
and Authorization
A.A.
XSS
Info
leakage
Web2.0 Top 5
CSRF
Phishing



Continue...

- Background
- User Access Control
- Session Management
- Output Filtering
- Data Security

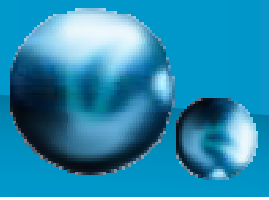
Access Control (1)

帐号设置

个人资料 | 修改头像 | 绑定手机 | 隐私设置 | 个性设置 | 应用授权 | 我的微币

帐号设置

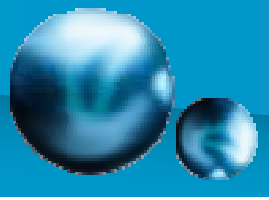
个人资料 | 修改头像 | 绑定手机 | 隐私设置 | 个性设置 | 应用授权 | 管理站点用户



Access Control (2)

```
var userID = GetCurrentUserID;
if (userID == 1000001 || userID == 1001)  // for system-admin and super-admin
{
    AjaxDisplay ( "ManagerSiteUsers" );
}
else
{
    AjaxDisplay ( "MyPoints" );
}
```

- Hiding UI is not a secure way to do authentication.
- Do not use Javascript/VBscript to determine actions only.
  - Do not depend on client side control



Access Control (3)

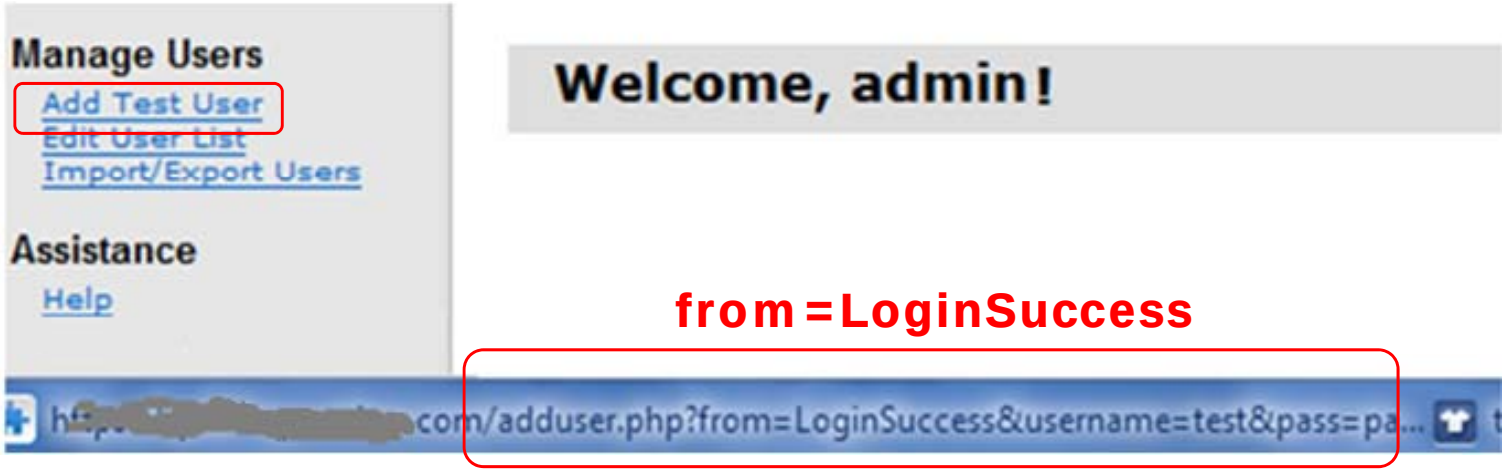
http://www.xxxx.com/mblog/delete.php?userID=98522&blogID=5843258546&rnd=0.6626736132893711

```
//delete mblog after verify user account
String RequestUserID = request.getParameter("userID");
String CurrentLoginID = session.getTokenKeyValue("userID");
if (CurrentLoginID.equalsIgnoreCase(RequestUserID))
{
    DeleteMBlog(request.getParameter("blogID"));
    AjaxRefresh("mblogStatus","mblogList","Homepage");
})
```

- Did not check if the resource is belong to the specific user.
  - Always check data ownership

Access Control (4)

www.abc.com/adduser.php?from=LoginSuccess&username=xxxx&pass=xxxxx&type=1

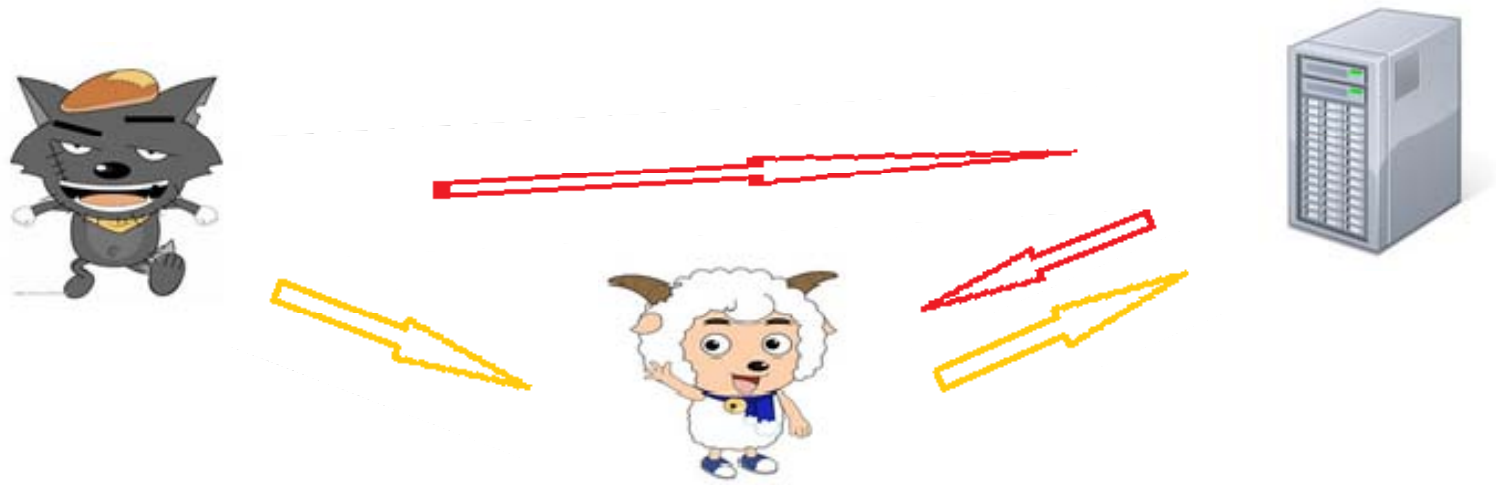


- HTTP request parameters in URL or in POST form data is easy to be modified.
  - Do not rely on any flag parameters

Access Control (5)

www.abc.com/adduser.php?from=LoginSuccess&username=xxxx&pass=xxxxx&type=1 &ticket=5sfde58fe84fe866

("from" was validated already in session)



- Critical operations and external published URLs is not protected
  - Protect critical operations (CSRF)

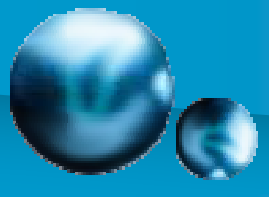
Access Control (6)

www.abc.com/adduser.php?from=LoginSuccess&username=xxxx&pass=xxxxx&type=1&ticket=5sfde58fe84fe866

Ticket = SHA(username+secureKey)

Ticket = SHA(username+secureKey+nonce)

- Add nonce or timestamp in important actions request.
  - Protect for replay attack

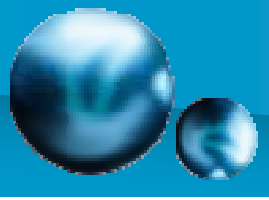


Continue...

- Background
- User Access Control
- Session Management
- Output Filtering
- Data Security and Misc

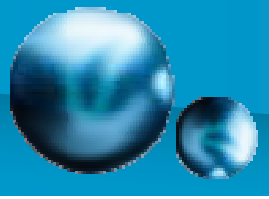
Session Management

- Clear sessions after login or logout
- Cookie management
  - Protect for cookie value that only used by server
  - Life time setting
  - “Secure" and “HttpOnly" flag
  - Domain name and path



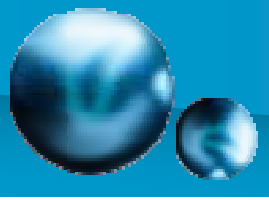
Continue...

- Background
- User Access Control
- Session Management
- Output Filtering
- Data Security and Misc



Output Filtering – XSS

- Filtering user data by APIs
  - Output **any** user data, filter with proper encoding API.
  - JSON data encoding method.
- Run code scan tool



Continue...

- Background
- User Access Control
- Session Management
- Output Filtering
- Data Security and Misc

Phishing and Data Security

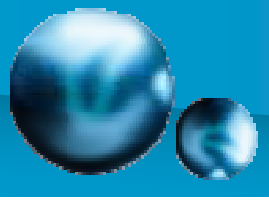
- URL Redirection
- Monitor unusual account activity
- HTTPS
  - Verify CN
  - Verify date validity
  - CRL query
- Save important data

Information Leakage

- POST method
- HTTP Trace
- Unify same message
- Personal information

Information leakage

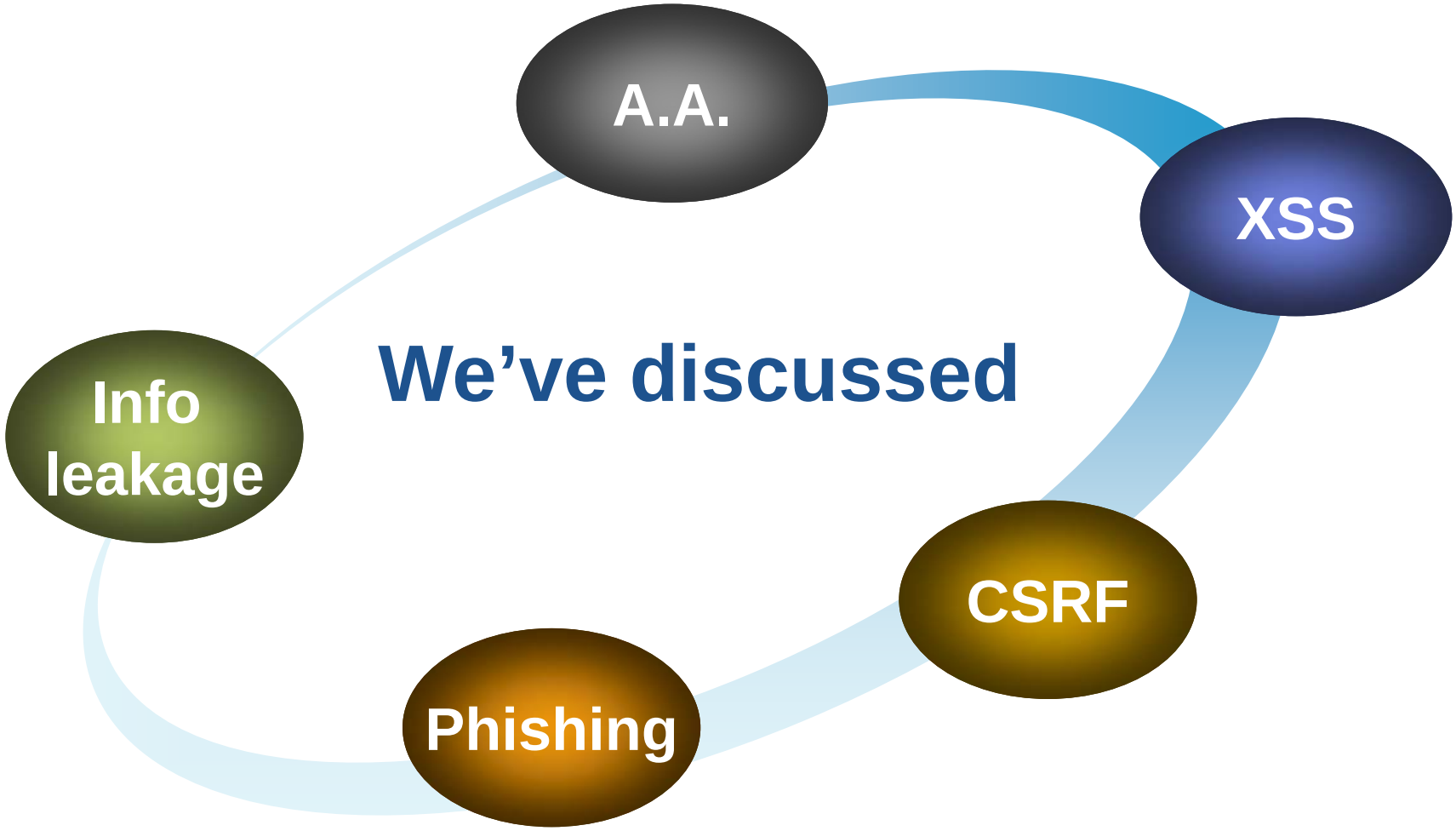
- Do not include any sensitive information in error message / exception content



Misc

- Use standard algorithms
- AES with hash
- DES, MD5
- Math.random and java.util.Random
- Page Charset

Summarize



Thank you!

brucexym@gmail.com