

Paper 46-28

Big Brother for SAS/IntrNet® Security and Tracking Agent

Yadong Zhang, Oxford Health Plans, Trumbull, CT
 Muhammad Khan, Oxford Health Plans, Trumbull, CT
 Kevin Smith, Oxford Health Plans, Trumbull, CT

ABSTRACT

With all the new laws that enforce the protection of the personnel information, security for web application has become mission critical. Since the operating system or the web server only enforces the security for SAS/IntrNet, we implemented a security and tracking agent – “The BIG Brother”. This was accomplished by creating a user validation and a user activity database. Some basic JavaScript were also incorporated to validate the data parameters in the form.

INTRODUCTION

Like most programmers, we hate the userid/password screen, and like most considerable people, we don't want to over-burden our users. With this philosophy, the SAS/IntrNet application was designed to be user friendly, no ID / password restrictions. After deploying some applications in our company, our users are pretty happy about the ease of use, but we also ran into the security concerns from upper management. To address these concerns we decided to develop a validation and tracking agent.

FORM DESIGN

Figure one is a sample form for our applications. Some features I would like to point out.

1. The form use JavaScript for preliminary data quality check. If user enters non-conforming parameters, a friendly reminder will be prompted.
2. The form requires a User ID field. The field serves two purposes:
 - ❖ Use for user validation
 - ❖ Use as email address to send notification
3. Hidden field `_apps`, stores name for this application
4. Hidden filed `_appsgpr`, stores name for the application group Allows you to access remote files using the FTP protocol

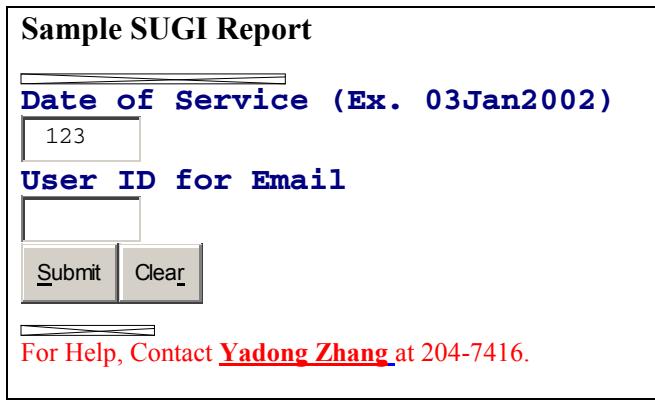


Figure I: Form

```

<HTML><HEAD>
<TITLE> Provider Report </TITLE>

1.
<SCRIPT language="JavaScript">
function checkchars(form)
{
var max=9
  if (form.dos.value.length !=9)
    {
      alert("Please input the required 9 characters for
the Start Date!")
      form.dos.focus()
      return false
    }
}
</SCRIPT>
</HEAD>

<BODY TEXT="00008B" text=#0000a0>

<H1>Sample SUGI Report
<HR color=darkblue SIZE="5" width="23%"
align=left></H1>

<FORM onsubmit="return checkchars(this)" action="/cgi-
bin/sasweb/broker" method=post>

<P><B>Date of Service (Ex. 03Jan2002) </B></P>
<P><INPUT name=dos size=9 ></P>
2.
<P><B>User ID for Email </b></p>
<P><INPUT name=userid size=9 ></P>

<INPUT type=submit value=Submit >
<INPUT type=reset value=Clear >

<INPUT name=_SERVICE type=hidden value=default>
3.
<INPUT name=_PROGRAM type=hidden
value=finance.prv_pw.sas>
4.
<INPUT name=_apps type=hidden value=PROVIDER>
<INPUT name=_appsgpr type=hidden value=finance>
...

```

Figure II: Actual HTML

PASSWORD DATABASE

After some painful consideration, we reached the conclusion that the password database is too difficult to maintain. Instead, a user-list database can server the same purpose.

Sample layout.

userid	Role	Apps	appsgrp
Yzhang	Dev	All	all

userid: one user can have more than one entry

Role: Either Dev or User

Apps: Application name user has privilege to run

Appsgrp: Application group name user has privilege to run

THE BIG BROTHER

The control program first wrote an entry to the tracking database. It then cross-references to see if the user ID entered has privilege to run the specified report. If the answer is yes, the program will then call the macro pass, which kicks off another SAS program to create the report and send the email notification when the job has been completed. If it fails, the program will call macro fail to remind the user of the security enforcement put into place.

```
%macro pass;
%* Launch mail program ;
systask command "sas /finance/provider.sas -set dos
&dos -set userid &userid" nowait;

data _null_ ;
file _webout;
put '<HTML>';
put '<BODY BGCOLOR=#FFFFFF'
TEXT="#000000" LINK="#0000FF" '@;
put 'VLINK="#8000080" ALINK="#FF0000"> ';
put '<H1>Provider Application</H1>';
put '<HR>';
put '<P><b> Hi ' userid ', please wait for email
notification </b></P>';
put '<P><b> For report for' &dos ' </b></P>';
put '</BODY>';
put '</HTML>';
run;
%mend;
```

Marco Pass

```
%macro fail;
data _null_ ;
file _webout;
put '<HTML>';
put '<BODY BGCOLOR=#FFFFFF'
TEXT="#000000" LINK="#0000FF" '@;
put 'VLINK="#8000080" ALINK="#FF0000"> ';
put '<H1>Provider Application</H1>';
put '<HR>';
put '<P><b> Sorry ' userid ', you are not authorized to
run this report </b></P>';
put '<P><b> Please contact the administrator </b></P>';
put '</BODY>';
put '</HTML>';
run;
%mend;
```

Macro Fail

```
1.
data c;
date=today();
user="&userid";
...
run;
2.
proc append base=pass.track data=c;
run;
3.
Data a;
set pass.userlist;
if userid=upcase("&userid");
if class='DEV' or apps='ALL' or appsgrp='All' or
appsgrp="&_appsgrp" or apps="&_apps";
run;
data b;
if nn=0 then
call execute(%fail);
else
call execute(%pass);
set a nobs=nn;
stop;
run;
```

Control Program

Acknowledgement

The author would like to thank his colleagues of Health Care Economics department, which gave him the opportunity to prepare this paper. Special thanks go to Lori Hendra on helping with the Javascript.

CONTACT INFORMATION

Your comments and questions are valued and encouraged.
Contact the author at:

Yadong Zhang
Oxford Health Plans
48 Monroe Tpk
Trumbull, CT 06611
Email: yzhang@oxhp.com

SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration.

Other brand and product names are trademarks of their respective companies.