Request Security Scan for App & aadReporting

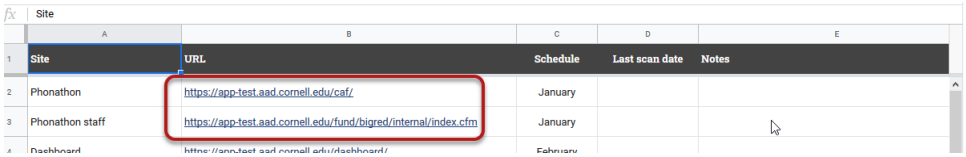
When your task is to set up and request a Security Scan for any of the Non-WordPress sites.

Scans happen every month except November

Web Dev Schedule https://docs.google.com/spreadsheets/d/1Ol1rg1LZ6FjlFvz8ViCSg83pBb-5sShzuyxmc_Hg_oU/edit#gid=0

Vulnerability scan schedule https://docs.google.com/spreadsheets/d/1ABb68I7LHtG2flh2CiMAMC_L45QUVfqP0bJfqkqW0NM/edit#gid=0
Security Scans archive: https://cornell.box.com/s/jeekdk83wpvrwe9daeu3aniyvlg9v70s

1. Check the “Vulnerability scan schedule” to see what’s on the list for the current month
2. Copy all the links listed for that month



Site	URL	Schedule	Last scan date	Notes
Phonathon	https://app-test.aad.cornell.edu/caf/	January		
Phonathon staff	https://app-test.aad.cornell.edu/fund/bigred/internal/index.cfm	January		
Dashboard	https://app-test.aad.cornell.edu/dashboard/	February		

NEW—The email port is changed from 25 to 999 within the ColdFusion admin for each instance on Media3 servers, both test and dev.

To set them back to 25 when ready, you can log into each instance and under the server settings there is a mail option. Once you click on that, you will see the mail port listed as 999. You can update this to 25 and click submit changes. You will need to do this to the other 2 CF instances as well. You may have to check your code too. If you specify server and port in your cfmail code, that will override the settings you are doing. Please let us know if you have any questions.

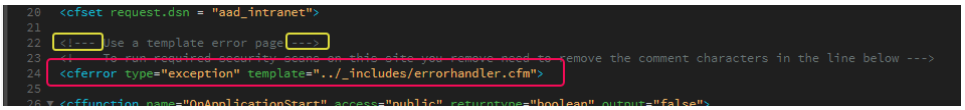
1. In the code, comment out any automatic emails so they won’t get sent.

```
<!--- <cfmail from="BRnewapp@cornell.edu" to="#sysdata.manager_email#...>blah</cfmail> --->
```

2. Check the .htaccess file to make sure that the itsoscan security office can access the sites.
   Remove the #(hashtag) in the “require shib-attr uid itsoscan” line to allow them to scan with Duo disabled.

```
1
2   # use Shibboleth to authenticate and authorize access
3       AuthType shibboleth
4
5   # valid-user is minimum require statement to restrict access
6   # BUT beware that this could allow in authenticated users from outside Cornell.
7   # not advisable. See below for better options
8       require valid-user
9
10  # Require Cornell employee
11      require shib-attr groups rg.cuniv.employee
12
13  # Require AAD staff
14      require shib-attr groups rg.aad.employee.staff AAD-Colleagues
15
16  # All IT security scan
17      require shib-attr uid itsoscan
18
19
20  #AuthType all
21  #Satisfy all
22  #ShibRequestSetting requireSession 1
23
24  # Disable DUO
25  #CUWA2FARequire CIT-2FA-Exempt
26
27  #AuthName Cornell
28  #require netid itsoscan lx58 djm6 tcd55
29  #require permit cit.security.cr.crrfull cit.security.cr.crrmodel aad.staff.all
30
31  #RewriteEngine On
32  #RewriteCond %{HTTPS} off
33  #RewriteRule ^(.*)$ https://%{SERVER_NAME}%{REQUEST_URI} [R=301,L]
34
```

3. To scan the Intranet you will need to remove the comment out commands, circled in yellow below, from the command on line 24 circled in red below.

4. 
```
<cfset request.dsn = "aad_intranet">

<!---Use a template error page--->
<!---To run required security scans on this site you remove need to remove the comment characters in the line below --->
<cferror type="exception" template="../_includes/errorhandler.cfm">

<cffunction name="OnApplicationStart" access="public" returntype="boolean" output="false">
```
5. **TURN OFF DEBUGGING** on the test servers to be scanned.
6. Send an email to security-services@cornell.edu requesting a scan.

   Please run a security scan on our test sites https://testspi.aad.cornell.edu/ and https://testconnect.aad.cornell.edu/ at your earliest convenience. We have prepared for it by confirming that "itsoscan" has permission, turning off notifications and disabling the automated emails.

7. Check the reports that come back for any issues more than low-level risk

8. When any issues are dealt with save the zipped scan reports in Cornell Box, aad-wsux, Security Scans folder. This folder should be locked down to aad-wsux team and Lisa Stensland (aad IT security contact).

Related articles

- Request Security Scan for App & aadReporting
- Security Scan Archive
- Use the Email Lookup tool on aadReporting
- Use Contribute with Mountain Duck
- Managing "My Tools"