VegBank - Bug #919

Advanced IP system, user-specific filtering of data

11/27/2002 01:31 PM - Michael Lee

Status:	New	**Start date:**	11/27/2002
Priority:	Immediate	**Due date:**	
Assignee:	Michael Lee	**% Done:**	0%
Category:	IP	**Estimated time:**	0.00 hour
Target version:	3.0.0	**Spent time:**	0.00 hour
Bugzilla-Id:	919		

Description

Confidential plots (that is plot with plot.ConfidentialityStatus = 6) must not
be viewable in the system. Also not downloadable or queryable. They stay hidden.

The following are the rules for confientiality:
values valueDescription
0 Public
1 1 km radius
2 10 km radius
3 100 km radius
4 Location embargo
5 Public embargo on data
6 Full embargo on data

0 means that anyone can access all data belonging to the plot.
1-3 mean that latitude and longitude are "fuzzed" to some degree so that the
user doesn't know exactly where the plot is.
4 means that users can't access data from the place table for that plot, as well
as the lat/long. LocationNarrative and authorE, authorN, authorLocation in the
plot table should also be hidden.
5 and 6 mean that users can't access the plot at all - no attributes on any
tables.

RealLatitude and RealLongitude should ALWAYS be hidden from the user. Use
latitude and longitude instead.

Related issues:

Is duplicate of VegBank - Bug #866: [1353] Export provides ALL data except co...	**Closed**	**11/13/2002**
Blocks VegBank - Bug #1219: VegBank 1.0.2 model - implemented	**Resolved**	**11/21/2003**
Blocked by VegBank - Bug #841: Limit number of plots uploaded based on certif...	**Resolved**	**11/13/2002**
Blocked by VegBank - Bug #835: IP: form for embargo renewal and dropping	**Resolved**	**11/13/2002**
Blocked by VegBank - Bug #1610: lift VA Heritage data embargo	**Resolved**	**06/28/2004**

History

#1 - 01/09/2003 09:54 AM - John Harris

- Bug 866 has been marked as a duplicate of this bug. ***

#2 - 11/21/2003 09:24 PM - Michael Lee

not critical bug to be highlighted in red, but very important

#3 - 11/21/2003 10:20 PM - Michael Lee

One of the 5 major (critical on bugzilla so higlighted red) bugs:

We must implement the new intellectual property design so that plots with
current embargoes are not viewable. This will use changes made for version
1.0.2 vegbank model.

-----WHAT USERS SHOULD BE ABLE TO VIEW ----------

Changes in field usage: plot.confidentialityStatus may only contain 0-3 meaning no fuzzing of lat/long, or up to 100km of fuzzing. This is necessary, because there can only be one value in lat or long, so different users cannot each see views of the plot with coordinates fuzzed to different degree.

Whenever a user attempts to view or download a plot, or child of plot (orange, teal [not project], grey, and yellow tables in ERD), embargo.defaultStatus must be checked, where embargoStart is before now and embargoStop is after now (embargo stop date REQUIRED, ie it must expire). Currently the following values apply to defaultStatus:
0 Public
1 1 km radius
2 10 km radius
3 100 km radius
4 Location embargo
5 Public embargo on data
6 Full embargo on data

IF: 0-3, then all normally viewable fields (ie NOT realLatitude, confidentialityReason, embargo table), should be viewable.

IF: 4, then the following fields/tables should not be viewable:
plot.{fields:
realLatitude
realLongitude
locationAccuracy
confidentialityStatus
confidentialityReason
latitude
longitude
authorE
authorN
authorZone
authorDatum
authorLocation
locationNarrative
placementMethod (may contain loc info?)
}
place table {all fields}

IF:5
User may request permission to view this plot. I am not sure how the user finds out about the plot's existence. My worry is that this will be challenging to implement, if, for example, the query can see the plot, but the user can't. Perhaps certain views of plots for case 5 will be OK, others not. For example, the plot could be returned to the "list of plots matching your query" but detailed and summary views wouldn't be available. Others with technical know-how should comment on this. Users requesting permission is talked about below.

IF:6
Do not let users see this plot.

(see next comments on users requesting permission to view and how to consider a user's special permission that may exist)

#4 - 11/21/2003 10:26 PM - Michael Lee

---- THE PLOT IS CONFIDENTIAL TO SOME DEGREE BUT THE USER HAS PERMISSION

IF a plot is not viewable to a user, or only to a lesser degree (embargo.defaultStatus>0), then the user may have special permission from the plot owner to view the plot anyway. This would be found in userPermission table corresponding to the usr_id of the user and the embargo_id of the embargo. If the current date is between the permissionStart and permissionStop, then their permission value is userPermission.permissionStatus, not embargo.defaultStatus. See above for what this means. 0-6.

For 0, we may want to allow the user to download the realLatitude and realLongitude- some business rule may need to exist for this. If the user is assigned permission of 1-3 (1,10,100 km radius fuzzing), then this value should match plot.confidentialityStatus. Then they can see lat&long. If the user's permission is 4, then the same fields that are hidden above in case 4 should be hidden now. Case 5 and 6 seem absurd. This shouldn't be a valid value for

userPermission.permissionStatus (see next comment).

#5 - 11/21/2003 10:33 PM - Michael Lee

--------- OK so a user wants to request permission, how does this happen?

We need a form that we can link to when a user is denied permission to viewing a plot (defaultStatus=4,5). Business rules not yet in existence need to deal with cases where the defaultStatus=1-3 and user wants to know exact coordinates. In theory, they should be able to use the same form.

The form would state the plot(s) the user would like to view that a particular plot owner has embargoed. Initially, this form could be filled out once per plot, but better would be once per plot owner. The form would show the plot the user wanted to see, the owner's name, and allow the user to fill in information about him/herself [basic stuff we can send from the user's party info] and why they want to see the plot. They would press submit and we'd send an email to the plot owner (as determined in table:UserRecordOwner, find the owner of the plot record), which would state that a user has requested permission to see their plot #XXX and why. It would also have a link to a page where the user could login, then grant permission to the first user.

the form where the owner gives permission would be much like the administrative pending tasks for mailman on hyperion's mailing lists. The plot owner could either accept/reject/accept at a different level than the owner requested, or discard (in case of abuse of this, in which case cc to dba). The plot owner would optionally stop date of the permission and any notes that they wanted to record about this permission granting. All this info, along with teh current date for permission start go into a new record in user_permission table for the user and embargo in question.

#6 - 11/21/2003 10:34 PM - Michael Lee

Bob, please read through this bug and my long-winded descriptions and then, if OK, please pass along to Mark.

#7 - 11/22/2003 12:22 AM - Michael Lee

bug 835 = form for owner to provide permission

#8 - 11/22/2003 12:24 AM - Michael Lee

the thing that is high priority here is ensuring that embargoed plots cannot be viewed. Building forms to request and grant permission are lower priority (835)

#9 - 07/27/2004 11:46 AM - Michael Lee

fuzzing of lat/long according to new rules listed on the wiki has been implemented in VegBranch

#10 - 01/18/2005 05:08 PM - Michael Lee

we could initially have an all-or-nothing embargo whereby plots exist in VegBank, but are completely unaccessible (by anyone) until we build tools to selectively get around the embargo. We would do this by using SQLStore and database views (SQL) to create a list of "ok" data to show, and only these tables would be referenced in SQLStore.

#11 - 01/20/2005 11:41 PM - Michael Lee

All-or-nothing embargo now complete through our standard view. Plots that are completely embargoed (level 6) cannot be viewed through our standard views. This has holes in that there are places (plot-query and download most notably) where the plots can be viewed in part, and in the case of download, completely accessed.

This bug is now in PMark's court to test when the download feature (most importantly) and plot-query use either the same SQLStore as everything else, or use the SQL-views I created to accomplish this.

#12 - 01/20/2005 11:42 PM - Michael Lee

example plot that is embargoed on aldo:

http://aldo.vegbank.org/get/std/observation/8896

compare to vegbank:
http://vegbank.org/get/std/observation/8896

the rest of the views could probably use a little QA to make sure I didn't break anything with my monkeying around with the SQL

#13 - 01/31/2005 11:35 AM - Michael Lee

simple system is mostly done, and put into a new bug 1925

#14 - 03/27/2013 02:15 PM - Redmine Admin

Original Bugzilla ID was 919