USAID | GEORGIA
FROM THE AMERICAN PEOPLE

USAID ENERGY PROGRAM

UPGRADING PLMS/GCAP SOFTWARE

FINAL REPORT

USAID ENERGY PROGRAM

16 November 2020

This publication was produced for review by the United States Agency for International Development. It was prepared by Deloitte Consulting LLP. The author's views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States Government.

UPGRADING PLMS/GCAP SOFTWARE

FINAL REPORT

USAID ENERGY PROGRAM

CONTRACT NUMBER: AID-OAA-I-13-00018

DELOITTE CONSULTING LLP

USAID | GEORGIA

USAID CONTRACTING OFFICER'S

REPRESENTATIVE: NICHOLAS OKRESHIDZE

AUTHOR(S): GEORGIAN RESOURCE DEVELOPMENT

SERVICE (GRDS)

LANGUAGE: ENGLISH

16 NOVEMBER 2020

DATA

Reviewed by:	Ivane Pirveli
Practice Area:	Strategic Advisory Assistance to the Government of Georgia to Increase Energy Security
Key Words:	Cyber Security, Parallel Market Software, Generation and Consumption Nomination Planning

ACRONYMS

DAP	Day Ahead Planning
GCAP	Generation and Consumption Nomination Planning
GOG	Government of Georgia
GRDS	Georgian Resource Development Service
GSE	Georgian State Electrosystem
OWASP	Open Web Application Security Project
PHP	Hypertext Preprocessor
PLMS	Parallel Market Software
SoW	Scope of Work
SQL	Structured Query Language
USAID	United States Agency for International Development

CONTENTS

EXECUTIVE SUMMARY

This reports provides description of works which were undertaken by Georgian Resource Development Service LLC (GRDS) in upgrading and moving two applications – Parallel Market Software (PLMS) and Generation and Consumption Nomination and Planning (GCAP that is part of Parallel Market software) to a different platform. Both software belong to Georgian State Electrosystem (GSE) and is used to increase energy stakeholder capacity and provide tools for assessment of impact of new competitive electricity market to the market players.

BACKGROUND

The objective of USAID's Energy Program is to support Georgia's efforts to facilitate increased investment in power generation capacity to increase national energy security, facilitate economic growth, and enhance national sovereignty. The project will have a significant impact on the energy market reform efforts of the Government of Georgia (GoG) to comply with the country's obligations under the Energy Community Treaty. The project investment objectives will be achieved through the provision of technical assistance to a variety of stakeholders in the energy sector.

The goal of this program is to enhance Georgia's energy security through improved legal and regulatory framework and increased investments in the energy sector. The ultimate expected outcome of this program is an energy legal and regulatory framework that complies with European Union requirements and encourages competitive energy trade and private sector investments.

Under Task 5 of the Program, Strategic Advisory Assistance to the GoG to increase Energy Security, inter alia, USAID Energy Program helps GoG, on as need basis, to address issues of strategic energy infrastructure operation.

GSE requested assistance to USAID Energy Program with upgrading and moving two applications – PLMS and GCAP to a different platform. GSE does not have a development environment for these applications and for that moment production application was offline.

In order to assist GSE with this task, Deloitte subcontracted GRDS, the developer of PLMS who also integrated it with GCAP under prior USAID funded contract.

METHODOLOGY

Both, PLMS and GCAP required upgrades to mitigate operational system and programming platform vulnerabilities and to comply with basic cyber security requirements for web applications. Once upgraded, both applications must meet new information security policies applicable to GSE. Specifically, the performed tasks on a higher level included:

- Migration of applications to the New Linux 18.4 Platform;
- Work on upgrade and development of platform to Hypertext Preprocessor (PHP) 7.

Both applications should comply with the requirements of the Open Web Application Security Project (OWASP) Top 10 2017 and pass the analysis through Nessus software without critical error.

Functional upgrades of the software including testing and cleaning errors, as well as intensive support were required by GSE.

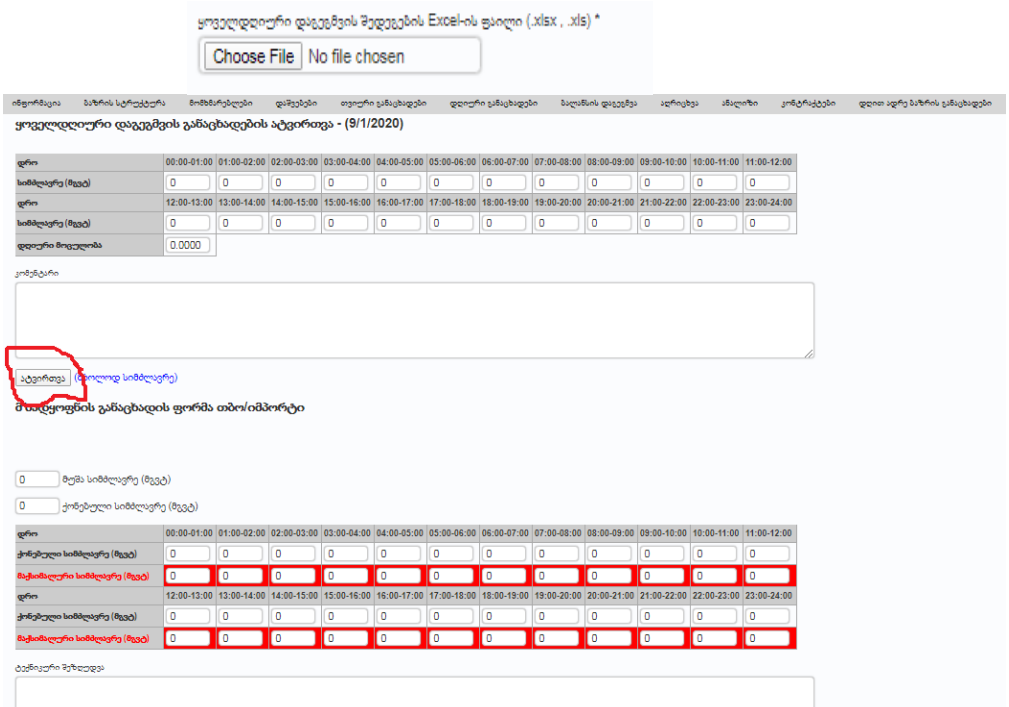
I. Specific Activities

Phase 1

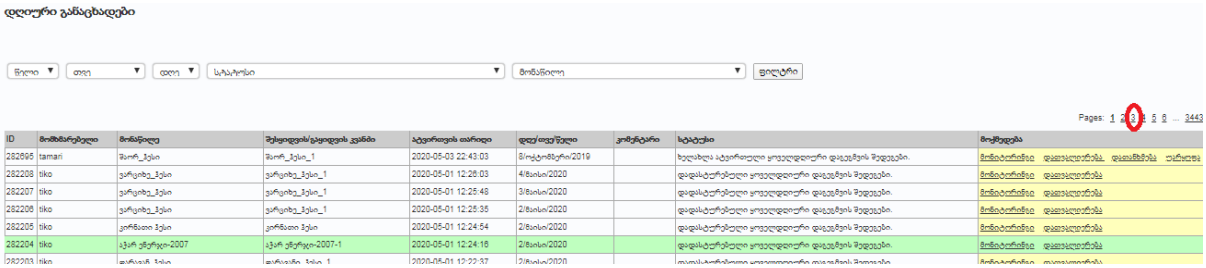
Security Measures

1. Migration PLMS and GCAP (part of Parallel Market software) with minor additions (agreed with GSE) to the new Linux 18.4 platform. Once the process is complete, GSE will either setup a development/test environment for GCAP; or run the application on production servers and test it;
2. Upgrade of development platform to PHP 7;
3. Update software and data security taking into account basic requirements of OWASP Top 10. Once software upgrade is complete, the developer will do a regression testing. Bug fixes will be done in Phase 2;
4. Software installation;
5. The software must pass the analysis through Nessus software without critical errors/high vulnerabilities which will also prove compliance with OWASP 10;
6. Functional upgrades. While there is no formalized test cycle or testing scenarios, those will be prepared during the development phase:

a) Development of Excel upload tool for user / administrator in daily reserve notifications.



b) Development of option submitting daily notification for multiple days or ability to copy / paste.



c) Development of password change function. Rules for setting passwords (e.g. number of characters, number of upper- and lower-case characters, use of digits and special characters) are outlined in the GSE's corporate information security policy. GSE will provide separate guidance to the developer.

   a. Users should be able to change their own passwords;
   b. Administrator based on written request of a user could terminate the password requirement;
   c. While terminating / adding new user, administrator should be able to create temporary password.

Phase 2

7. Clean "bugs"

8. PLMS and GCAP go-live, follow-up intensive support. GSE and the developer will prepare a plan to remediate potential vulnerabilities (medium and low) identified during the Nessus scan.

Item#	Deliverable	Estimated Due Date after Kick-off
1	1.1. Upgrade of PLMS and GCAP to PHP 7 programming language. 1.2. Migrate PLMS and GCAP to the new Linux 18.4 operating system 1.3. Update software and data security taking into account the basic requirements of OWASP Top 10	September 15, 2020
2	Passing Nessus software analysis, Software Installation	
3	Functional Upgrade. Interim report outlining the work that has been performed to complete Deliverables 1-3.	
4	PLMS and GCAP go-live. High, medium and low- level issues identified in Phase 2 and remediated. Interim report outlining the work that has been performed to complete this deliverable.	October 15, 2020
5	Follow-up intensive support. Final report (7 pages) outlining work performed for Deliverables 1-4 as well as on post-software launching support.	November 15, 2020

RESULTS ILLUSTRATING THE WORKS CONDUCTED UNDER ITEM #1

For increasing the level of cyber security for both applications we have made following steps:

1. Upgraded PHP 5.6 to the latest stable version PHP 7.4. PHP 7 offers better security improvements compared to PHP 5, including a filtered un-serialized function and a set of functions to easily get cryptographically secure random numbers
2. Upgraded PHP code security to be protected from the risks mentioned in OWASP Top 10. It includes:
   a. Injection;
   b. Broken Authentication;
   c. Sensitive Data Exposure;
   d. XML External Entities (XXE);
   e. Broken Access control;
   f. Security misconfigurations;
   g. Cross Site Scripting (XSS);
   h. Insecure Deserialization;

i. Using Components with known vulnerabilities;
j. Insufficient logging and monitoring.

Read more here: https://owasp.org/www-project-top-ten/

3. Created an Structured Query Language (SQL) Builder tool to be used for requesting data from Database without risk of SQL Injection by the end user;
4. Upgraded the user password encryption algorithm from MD5 to Bcrypt, which is more secure nowadays;
5. Implemented password management functionality for administrator users to be able to manage participant user's lost passwords securely;
6. Made the connection protocol with server more secure, using Secure Socket Layer Certificate;
7. Used `X-Frame-Options: DENY` option to prevent the application content being used in a frame and using on other domain;
8. Used `X-XSS-Protection` for pages to stop loading when they detect Cross-Site Scripting (XSS) attacks;
9. Configured session cookies to be used only when SSL connection was created with server and httpS protocol is used;
10. Closed access to the app source files with direct link, even if the direct location will be predicted, they can be used only by own apps;
11. Removed vulnerable and unused files from the application directory.

RESULTS ILLUSTRATING WORKS CONDUCTED UNDER ITEM #2

A cyber security check was carried out through the Nessus software (according to the Scope of Work (SoW) and agreement with the GSE), which showed no errors.

Full reports automatically generated by this software are attached to this report. In addition, the main results are shown on Fig. 1 and 2.

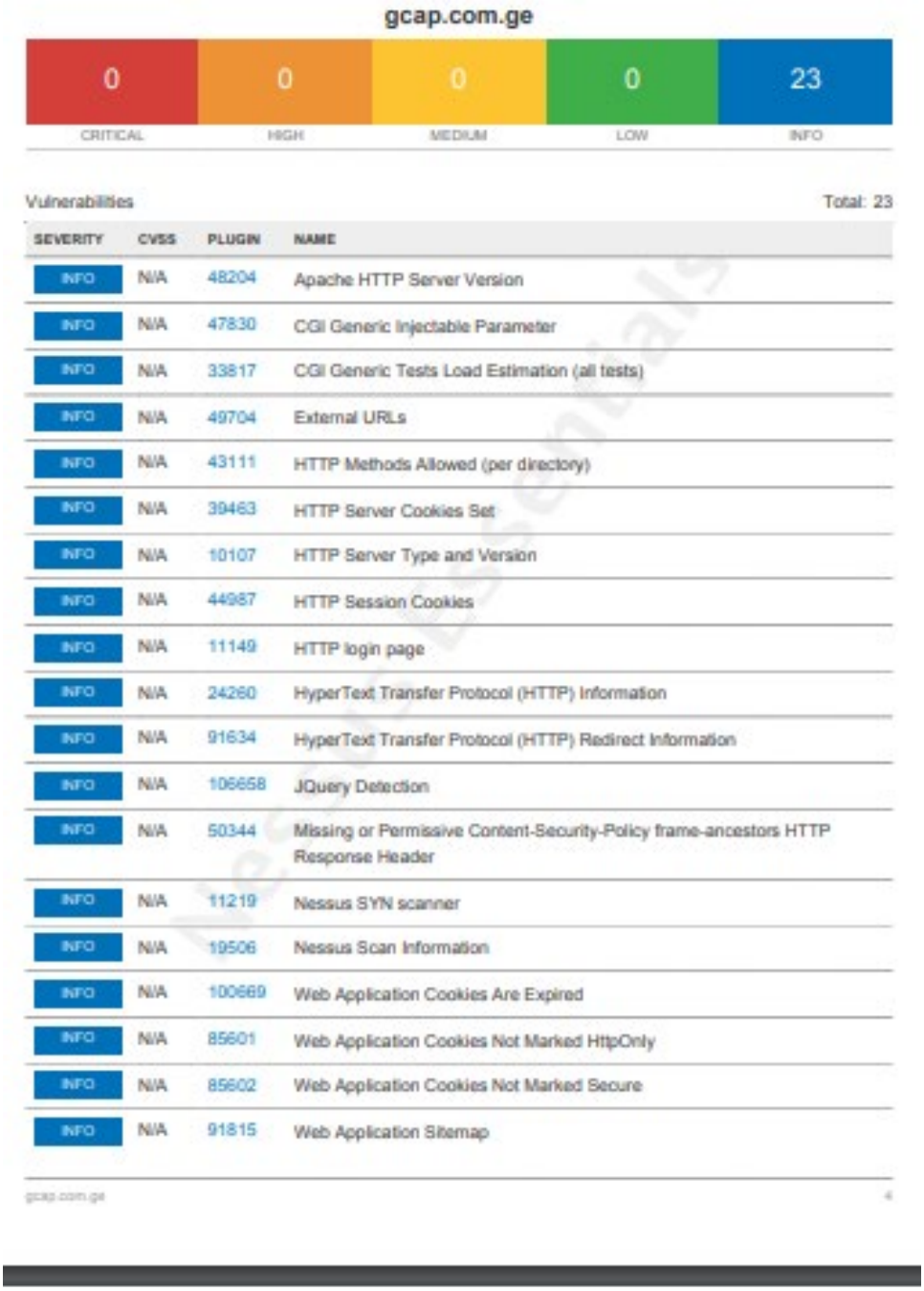
Figure 1

plms.com.ge

Vulnerabilities Total: 18

SEVERITY	CVSS	PLUGIN	NAME
INFO	N/A	47830	CGI Generic Injectable Parameter
INFO	N/A	39470	CGI Generic Tests Timeout
INFO	N/A	49704	External URLs
INFO	N/A	43111	HTTP Methods Allowed (per directory)
INFO	N/A	39463	HTTP Server Cookies Set
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	11149	HTTP login page
INFO	N/A	50344	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	100669	Web Application Cookies Are Expired
INFO	N/A	85602	Web Application Cookies Not Marked Secure
INFO	N/A	40773	Web Application Potentially Sensitive CGI Parameter Detection
INFO	N/A	91815	Web Application Sitemap
INFO	N/A	11032	Web Server Directory Enumeration
INFO	N/A	10386	Web Server No 404 Error Code Check
INFO	N/A	47863	Web Tests Session Expiration Errors
INFO	N/A	10662	Web mirroring

Figure 2



gcap.com.ge

0	0	0	0	23
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 23

SEVERITY	CVSS	PLUGIN	NAME
INFO	N/A	48204	Apache HTTP Server Version
INFO	N/A	47830	CGI Generic Injectable Parameter
INFO	N/A	33817	CGI Generic Tests Load Estimation (all tests)
INFO	N/A	49704	External URLs
INFO	N/A	43111	HTTP Methods Allowed (per directory)
INFO	N/A	39463	HTTP Server Cookies Set
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	44987	HTTP Session Cookies
INFO	N/A	11149	HTTP login page
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	91634	HyperText Transfer Protocol (HTTP) Redirect Information
INFO	N/A	106658	JQuery Detection
INFO	N/A	50344	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	100669	Web Application Cookies Are Expired
INFO	N/A	85601	Web Application Cookies Not Marked HttpOnly
INFO	N/A	85602	Web Application Cookies Not Marked Secure
INFO	N/A	91815	Web Application Sitemap

gcap.com.ge 4

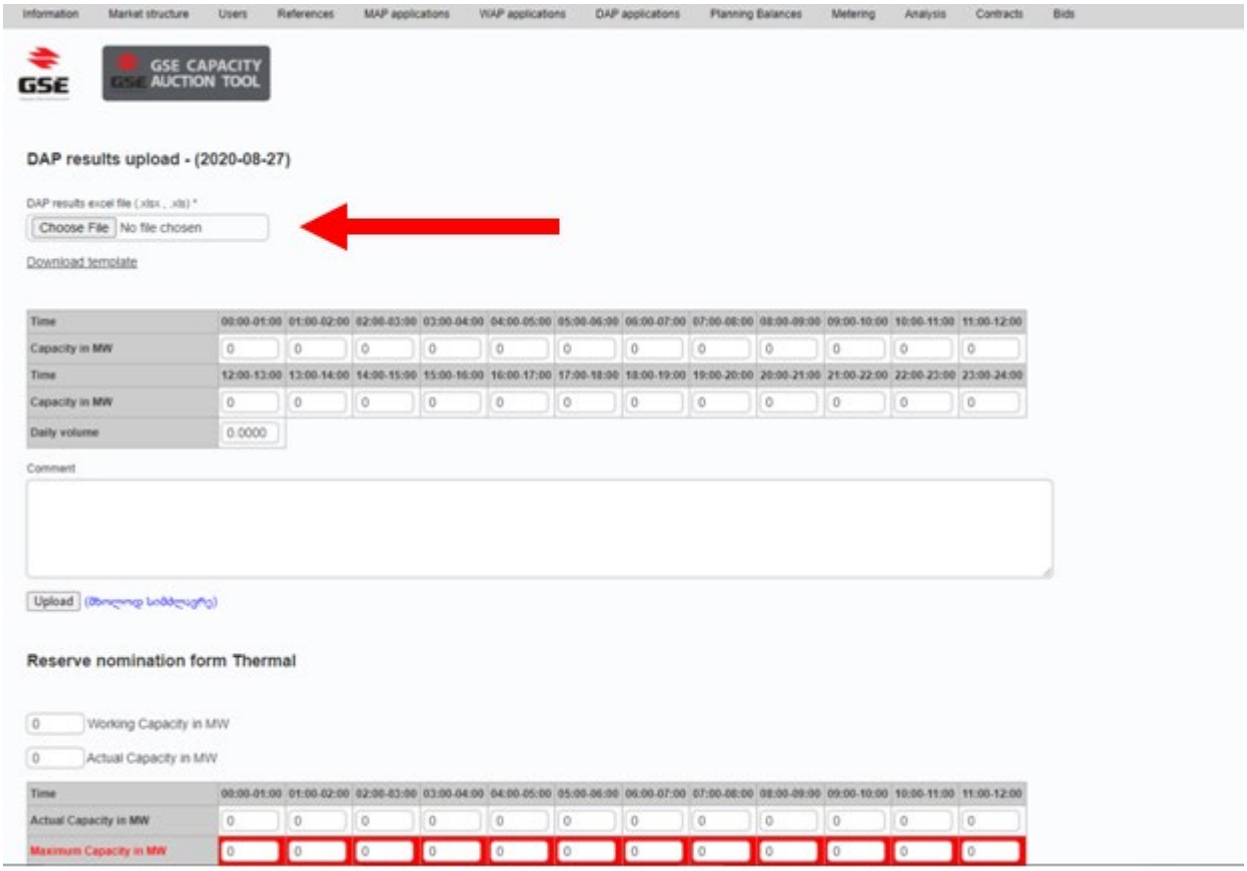
INFO	N/A	11032	Web Server Directory Enumeration
INFO	N/A	10386	Web Server No 404 Error Code Check
INFO	N/A	47863	Web Tests Session Expiration Errors
INFO	N/A	10662	Web mirroring

I. Changes in GCAP functionality (Item #3)

1. Possibility to upload Day Ahead Planning (DAP) applications via MS Excel for the nodes of generators marked as "Reserve"

Upload via Excel functionality was added (Fig.3).

Figure 3



2. Development of option submitting daily notification for multiple days or ability to copy / paste

After changes DAP applications can now be submitted for several days at the same time. While selecting date for which application is being submitted (DAP applications upload sub-menu), several days can be selected (Fig.4, 5).

Figure 4

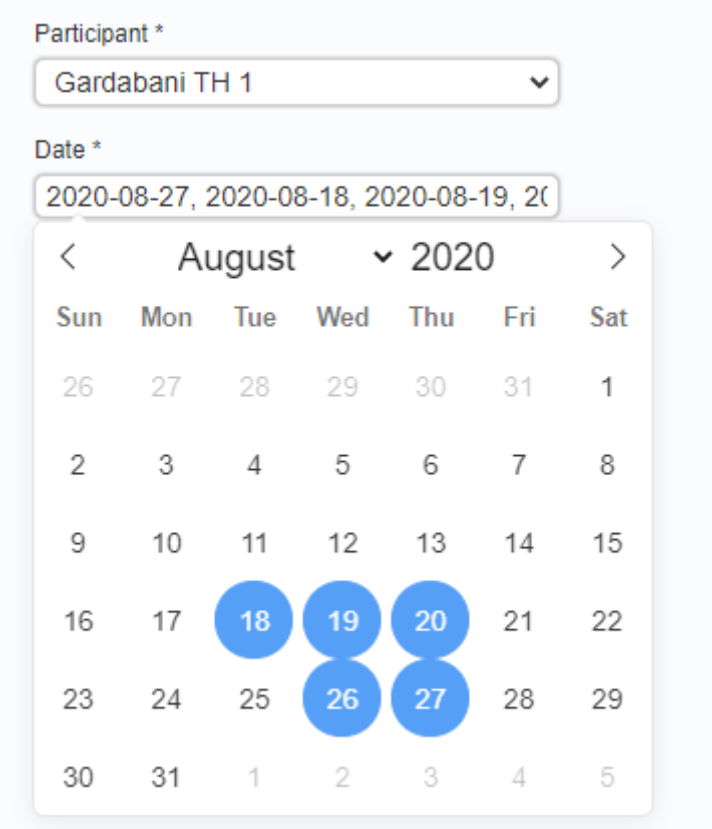
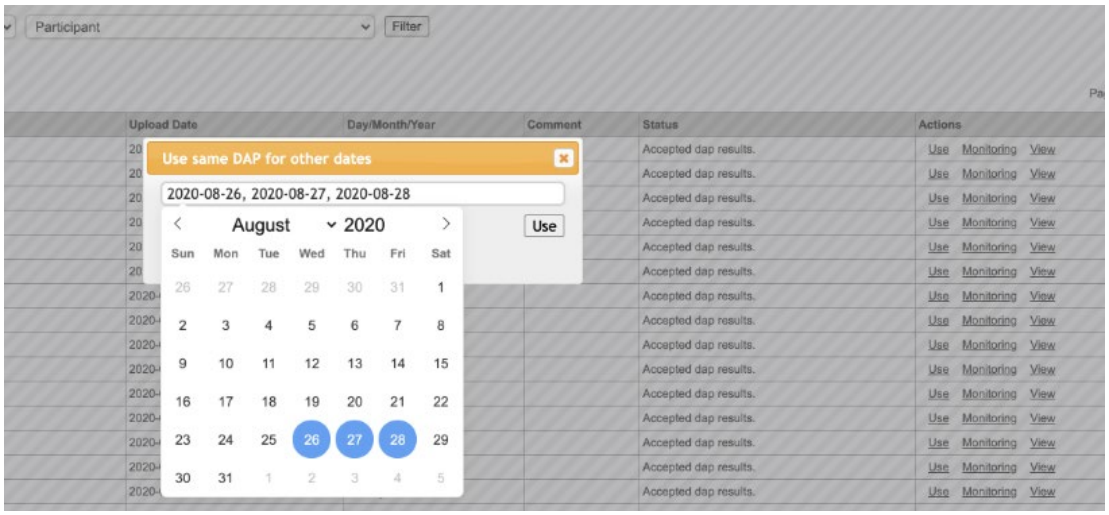


Figure 5

Moreover, already submitted application can be later used for another days. To do this user should go to DAP Applications sub-menu, find the application he wants to use, click on **"Use"** button from "Actions" column and select dates for which the applications with same data of selected application should be submitted (Fig.6).

Figure 6



Developed functionalities can be used by both Market Participants and System Operator.

In addition, the GSE requirement was taken into account and implemented, so that when accepting or rejecting applications, the user is returned to the page with the processed application.

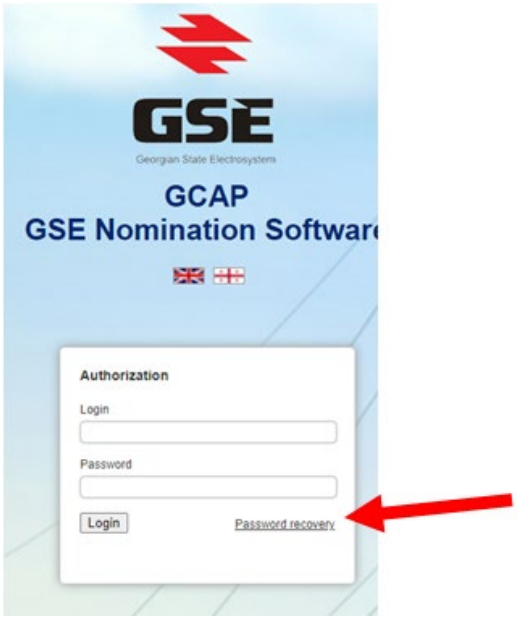
3. Development of password change functionality

All **NEW** passwords (old passwords are saved and can be changed to new ones) set should meet the following requirements.

- Password length should have at least 8 characters;
- Password should include at least 1 upper-case character;
- Password should include at least 1 lower-case character;
- Password should include at least 1 digit;
- Password should include at least 1 special character;

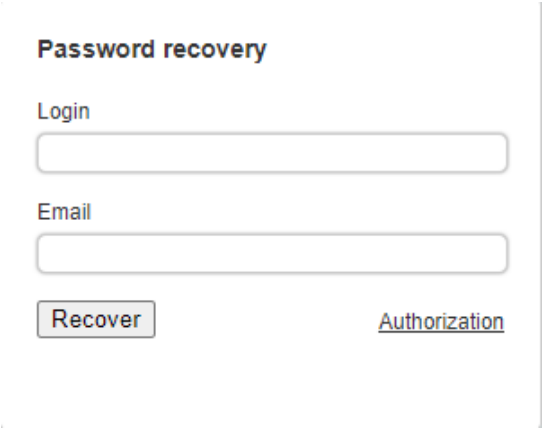
Password recovery mechanism has been implemented. From sign-in page, user can recover his password by going to “Password recovery” page (Fig.7).

Figure 7



Here, user should provide his login and email address (Fig.8).

Figure 8

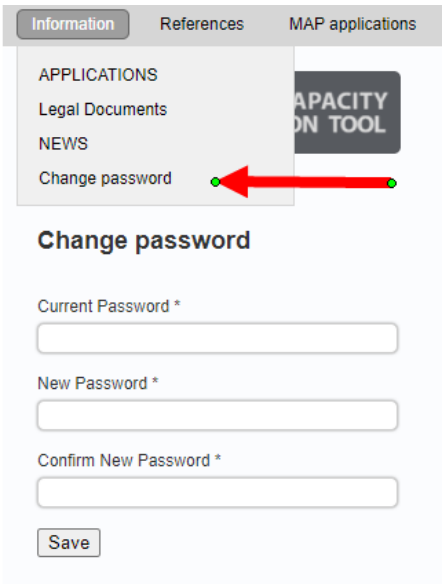


If verified, an e-mail with temporary password is sent to the user (Fig. 9).

Figure 9

User can then login with his username and temporary password. After which, password can be changed from password change sub-menu (Fig.10).

Figure 10



System operator can also reset password for Market Participant, after which an e-mail with new temporary password will be sent to participant's e-mail address. Password change functionality by System Operator has not been changed and can be used by the request of Market Participant.

RESULTS ILLUSTRATING THE WORKS CONDUCTED UNDER ITEMS #4 AND #5

1. The "clean bugs" process was completed (very minor changes) - GSE confirmed;
2. Joint testing of functionality with GSE completed - GSE confirmed;
3. All test calculations were carried out together with GSE to identify inaccuracies and needed adjustments. Everything functions correctly – GSE confirmed;
4. Outside the scope of the contract, at the request of GSE:
    - All historical data have been transferred by us to a new operating database – all required data is available;
    - We reconfigured the mail server in the GSE for sending and receiving emails, necessary for the operation of the software.

FINALLY, PLMS AND GCAP SOFTWARE ARE FULLY OPERATIONAL AND OPERATE ON A DAILY BASIS IN GSE

Thus, the contract work completely fulfilled.

USAID Energy Program

Deloitte Consulting Overseas Projects LLP

Address: 29 I. Chavchavadze Ave.,0179, Tbilisi, Georgia

Phone: +(995) 595 062505

E-mail: info@uep.ge