Engage 6.5.7 Pentest - overview fixed security items

ADO Item	SCoE ID	Description
Bug 414078: Security | Broken access control: tables professional roles	SCoE Pentest 6.4: Intake ID 2239, Finding no 76575 - Improper authorization	For caregiver role an extensive analysis has been exected on the authorized database tables (backend types). Conclusion: read rights are ok (access is needed to a large set of tables to run the application), but there is a list of tables that should be read only for caregivers. The following tables are now being defined as read-only: CarePrograms CareProgramsPerDepartment CentralOrganizationsIndex CentralParticipantsIndex CentralPatientsIndex Comps.Consent.DataCategories Comps.Consent.DataExchanges Comps.Consent.DefaultsApplyTo Comps.Consent.HealthCareInterventions Comps.Consent.Texts Comps.Consent.TextsSet Comps.Consent.Types Comps.Content.SubItems Comps.Devices.Devices Comps.Devices.DeviceAssignments Comps.Devices.Models Comps.Devices.ModelTypes Comps.Devices.Statuses Comps.Organizations.IdentifierCategories Comps.Protocols.EvaluatedMedFacts Comps.Protocols.EvaluatedRuleInstances Comps.Workflow.ScheduleDefinitions ContentItems DataRecordStaging DataRecordStagingIdentifier DelayedCalls Engage.DataVal.MeasurementRuleConditions Engage.DataVal.ReflexiveActions Engage.DataVal.Rules ExternalLinks KoppeltaalLocalActivityDefinitionAdditions ArchetypesPerMeasurementSet MeasurementSets MeasurementSetsPerCareProgram MedicalCodesPerMeasurementSet SAC.Workflow.BaseActivityDefinitions SAC.Workflow.BaseFunctions ServiceProviders SMD.Units.Dimensions SMD.Units.Units SMD.Units.UnitSystems SMD.Units.UnitSystemUnits
Bug 442059: [Security] Add content check on file upload	SCoE Pentest 6.5.3: Intake ID 2630 - Finding No 86202 Unrestricted file upload.	If a file upload functionality within an application allows the user to upload any file without any restriction on the file type, the server becomes vulnerable to unrestricted file upload. Uploaded files may pose a significant risk if not verified and handled correctly. Attacker can upload malware/plant backdoor via this file upload feature. Resolution: apply check whether extension matches with the content of the uploaded file. Allowed extensions for upload: jpg|jpeg|png|gif|pdf|doc|txt|rtf|docx|ppt|pptx|pps|ppsx|odt|xls|xlsx| csv|mp3|m4a|ogg|wav|mp4|m4v|mov|wmv|avi|mpg|ogv|3gp|3g2|p12|zip|xml Uploading of files can be checked from Documents tab (e.g. available in patient portal and provider portal) The content check is, by default, supported for these extensions: pdf, png, jpg, jpeg, mp4, rtf, pptx, docx, xlsx, odt, gif, wmv, wav, exe, msi, ogg.

Bug 442729: Security | Engage contains multiple .js.map files that can be downloaded by anyone	N/A, internal Engage finding	.js.map files can be downloaded from server by anyone (no need to be logged in)
Bug 442733: Security | SAML: replay attack possible	N/A, internal Engage finding	SAML assertion in SAML authentication flow could be used multiple times (as long the token did not expire). From now on, token can only be used once. Instructions for Engage SAML flow will be shared per e-mail to SCoE.
Bug 442735: Security | Brute force password guessing attack possible	N/A, internal Engage finding	The OAuth2 interface of the platform is not using the brute force detector (BFD) properly so that an attacker can perform a brute force attack by guessing all possible passwords. The brute force detector must slow down this attack so that it becomes useless to the attacker. Endpoint for changing password: https://singleinstance-externalpentest.vitalhealthsoftware.com/OAuth2/Comps/ChangePassword