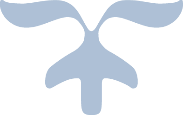


**kết quả đánh giá bảo mật**

**MISA JSC**



18 tHÁNG 4, 2023

Công ty cổ phần misa

N03-T1 Ngoại Giao Đoàn, Khu Ngoại giao đoàn, Xuân Tảo, Bắc Từ Liêm, Hà Nội

I, Nội dung

[1. Thông tin bảo mật 2](#_Toc130734743)

[1.1 Thông tin khách hàng 2](#_Toc130734744)

[1.2 Thông tin bên đánh giá 3](#_Toc130734745)

[1.2.1 Tài liệu và thành viên liên quan 3](#_Toc130734746)

[1.2.2 Quy trình và quy định liên quan 4](#_Toc130734747)

[A, Quy trình kiểm thử bảo mật 4](#_Toc130734748)

[B, Quy định phân loại mức độ lỗ hổng theo CVSS 3.1 5](#_Toc130734749)

[C, Checklist 5](#_Toc130734750)

[2 Báo cáo đánh giá bảo mật 6](#_Toc130734751)

[2.1 Thống kê lỗ hổng đã phát hiện 6](#_Toc130734752)

[2.2 Báo cáo lỗ hổng chi tiết 7](#_Toc130734753)

[2.2.1 Danh sách lỗ hổng 7](#_Toc130734754)

[2.2.2 Chi tiết lỗ hổng 7](#_Toc130734755)

[[EMIS-TB-01] broken access control 7](#_Toc130734756)

[3 Danh sách vị trí đã kiểm tra 8](#_Toc130734757)

II, Danh sách bảng

[Bảng 1: Thông tin dự án 2](#_Toc130734758)

[Bảng 2: Bản báo cáo 3](#_Toc130734759)

[Bảng 3: Phân loại lỗ hổng theo CVSS 3.1 5](#_Toc130734760)

[Bảng 4: Checklist OWASP 5](#_Toc130734761)

[Bảng 5: Thống kê lỗ hổng 6](#_Toc130734762)

# Thông tin bảo mật

## 1.1 Thông tin dự án

|  |  |  |  |
| --- | --- | --- | --- |
| **DỰ ÁN** | | | |
| **Tên dự án** | AMIS Quản lý tài sản | **Mã dự án** | QLTSv2 |
| **Sản phẩm** | WEB APPLICATON | | |
| **Phạm vi trong đánh giá** | https://testqltsapp.misa.vn | | |
| **Ngoài phạm vi** | https://api.livechatinc.com  https://qltshelp.misa.vn  https://cdn.livechatinc.com  https://testqltsapp.misacdn.net | | |
| **Tài khoản cung cấp** | Username: admin  Password: 12345678@Abc | | |

Bảng 1: Thông tin dự án

## 1.2 Thông tin bên đánh giá

### 1.2.1 Tài liệu và thành viên liên quan

|  |  |  |
| --- | --- | --- |
| **BẢN BÁO CÁO** | | |
| **Phiên bản báo cáo** | 1.0 | |
| **Thời gian thực hiện đánh giá** | 12/04/23 | Đến 18/4/2023 |
| **Phương thức đánh giá** | GRAYBOX | |
| **Thành viên thực hiện đánh giá** | ĐẶNG XUÂN HOÀNG | |
| **Thành viên phê duyệt báo cáo** | BÙI ĐỨC TRƯỜNG | |

Bảng 2: Bản báo cáo

### 1.2.2 Quy trình và quy định liên quan

#### A, Quy trình kiểm thử bảo mật

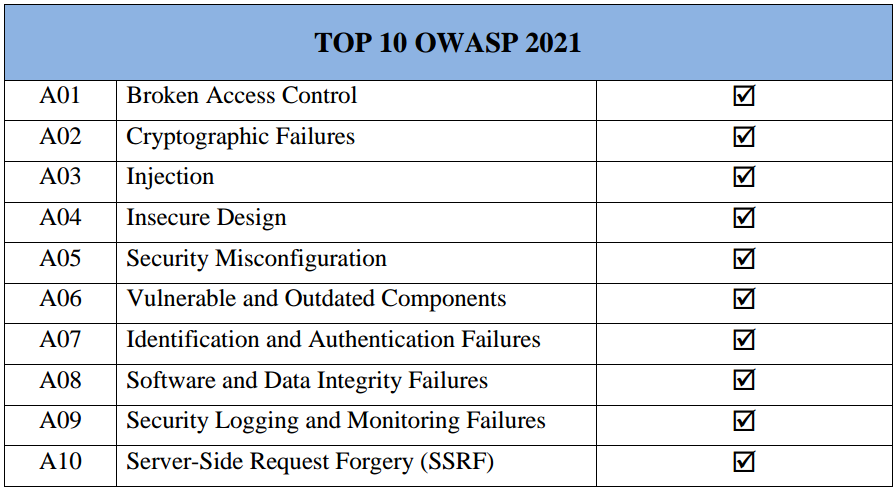


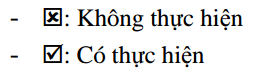
#### B, Quy định phân loại mức độ lỗ hổng theo CVSS 3.1

|  |  |  |
| --- | --- | --- |
| **Điểm CVSS 3.1** | **Mức độ lỗ hổng** | **Mô tả** |
| 10-9 | Nguy hiểm - Critical |  |
| 8.9-7 | Cao - High |  |
| 6.9-4 | Trung bình - Medium |  |
| 3.9-0.1 | Thấp - Low |  |
| 0 | None |  |

Bảng 3: Phân loại lỗ hổng theo CVSS 3.1

#### C, Checklist

Bảng 4: Checklist OWASP



# 2 Báo cáo đánh giá bảo mật

## 2.1 Thống kê lỗ hổng đã phát hiện

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **KẾT QUẢ CHUNG** | | | | |
| **Sản phẩm** | Số lỗ hổng theo mức độ | | | |
| Nghiêm trọng | Cao | Trung Bình | Thấp |
|  | 1 | 0 | 1 | 0 |
| **Tổng sô lỗ hổng** | 2 | | | |

Bảng 5: Thống kê lỗ hổng

## 2.2 Báo cáo lỗ hổng chi tiết

### 2.2.1 Danh sách lỗ hổng

|  |  |  |  |
| --- | --- | --- | --- |
| **MÃ** | **TÊN** | **MỨC ĐỘ** | **TRẠNG THÁI** |
| **QLTSv2-01** | SQL Injection | Nghiêm trọng |  |
| **QLTSv2-02** | Cross-site Scripting | Trung bình |  |

### 2.2.2 Chi tiết lỗ hổng

## [QLTSv2-01] SQL Injection

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **A, Mức độ nghiêm trọng**: Nghiêm trọng   |  |  | | --- | --- | | **ĐIỂM CVSS** | | | **9** | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H |   **B, Mô tả** :   * SQL Injection là một kỹ thuật lợi dụng những lỗ hổng về câu truy vấn của các ứng dụng. Được thực hiện bằng cách chèn thêm một đoạn SQL để làm sai lệnh đi câu truy vấn ban đầu, từ đó có thể khai thác dữ liệu từ database.   **C, Ảnh hưởng:**   * Bỏ qua cơ chế xác thực​ * Khai thác cơ sở dữ liệu​ * Leo thang đặc quyền​   **D, Vị trí lỗ hổng:**   |  |  |  | | --- | --- | --- | | **STT** | **URL** | **Ghi chú** | | **1** | <https://testqltsapp.misa.vn/fa/api/fixedassetlist/pagingfixedassetlist> | Vị trí tham số “Sort” |   **E, Các bước tái tạo lỗ hổng:**   * Tại Danh sách tài sản cố định, thực hiện nhập ký tự bất kỳ vào các ô lọc. * Bắt chặn request ở hình trên, tại vị trí tham số “Sort”, thêm đoạn payload (select\*from(select(sleep(5)))a) và gửi đi. Sau khi gửi request, phản hồi trả về kết quả sau 5s, bằng với thời gian được set trong cú pháp sleep. * Tiến hành khai thác sâu hơn để tìm tên database, tại vị trí tham số “Sort”, truyền thêm đoạn payload như hình dưới. * Kết quả phản hồi trả về sau 5s, khẳng định tên database có dạng q\* * Sau nhiều lần thử, tìm ra tên database là qlts\_demov2\_asset   **F, Tài liệu tham khảo**:   * https://cheatsheetseries.owasp.org/cheatsheets/SQL\_Injection\_Prevention\_Cheat\_Sheet.html * https://cwe.mitre.org/data/definitions/89.html * https://cheatsheetseries.owasp.org/cheatsheets/DotNet\_Security\_Cheat\_Sheet.html#sql-injection   **J, Các biện pháp phòng chống**:   * Kiểm soát dữ liệu từ người dùng phát hiện và loại bỏ các kí tự, cú pháp liên quan đến SQL query . Sử dụng MISA Library​ * Sử dụng Parameterized Queries thay vì cộng chuỗi để tạo SQL , không execute string (EXEC(@query)) trong stored procdures .​ * Không trả exception,message lỗi trực tiếp về cho phía client.​ * Lưu các thông tin nhảy cảm như password, CCCD ... ở dạng mã hóa 1 chiều * Phân quyền rõ ràng trong DB,Backup dữ liệu thường xuyên.​ |

## [QLTSv2-02] Cross-site Scripting

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **A, Mức độ nghiêm trọng**: Trung bình   |  |  | | --- | --- | | **ĐIỂM CVSS** | | | **5.4** | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N |   **B, Mô tả** :   * XSS là một lỗi bảo mật cho phép người tấn công (Attacker, Hacker,…) chèn các đoạn script nguy hiểm vào trong source code (FE) của ứng dụng web. Nhằm thực thi các đoạn mã độc Javascript để chiếm phiên đăng nhập của người dùng và ăn cắp các thông tin nhạy căm được lưu phía client.   **C, Ảnh hưởng:**   * Đánh cắp dữ liệu của người dùng được lưu trên trình duyệt: Cookie của người dùng: session, token. Kẻ tấn công giả dạng người dùng, thực hiện bất kỳ hành động nào mà người dùng có thể thực hiện và truy cập vào bất kỳ dữ liệu nào của người dùng.   **D, Vị trí lỗ hổng:**   |  |  |  | | --- | --- | --- | | **STT** | **URL** | **Ghi chú** | | **1** | https://testqltsapp.misa.vn/fa/api/fixedassetcategory/getbyparams |  | | **2** | https://testqltsapp.misa.vn/fa/api/fixedassetricategory/getbyparams |  | | **3** | https://testqltsapp.misa.vn/fa/api/equipmentcategory/getbyparams |  | | **4** | https://testqltsapp.misa.vn/fa/api/ActivityDiary/GetActivityDiaries |  | | **5** | https://testqltsapp.misa.vn/fa/api/equipmentcategory/checkcountref |  | | **6** | … (diện rộng) |  |   **E, Các bước tái tạo lỗ hổng:**   * Tại **Danh mục → Loại tài sản**, truyền đoạn script <img src=0 onerror=alert(document.cookie)> vào các form input và lưu lại. * Sau khi lưu, màn hình trả về danh sách tài sản, chuyển sang chức năng **Nhật ký truy cập** → xuất hiện popup hiển thị thông cookie. * Tương tự tại vị trí **Danh mục → Loại tài sản hạ tầng đường bộ → Thêm loại tài sản,** tiến hành nhập payload vào các form input và lưu lại bản ghi.      * Sau khi lưu, danh sách loại tài sản đường bộ hiện ra, xuất hiện popup mang thông tin cookie. * Tắt popup quan sát thấy vị trí gây ra lỗi.      * Thực hiện tương tự tại **Danh mục -> Loại công cụ** cũng cho ra lỗi.        * Còn nhiều vị trí cũng bị lỗi XSS như **Nhật ký truy cập,** hay tại tính năng xóa bản ghi trong các danh mục.   **F, Tài liệu tham khảo**:   * https://cwe.mitre.org/data/definitions/79.html * https://portswigger.net/web-security/cross-site-scripting * https://cheatsheetseries.owasp.org/cheatsheets/DotNet\_Security\_Cheat\_Sheet.html#a7-cross-site-scripting-xss   **J, Các biện pháp phòng chống**:   * Kiểm soát dữ liệu đầu vào, phát hiện và loại bỏ các kí tự, cú pháp giúp thực thi mã trên trình duyệt. * Mã hóa dữ liệu đầu ra an toàn , tùy vào ngữ cảnh có thể kết hợp HTML, URL, Javascript , CSS encoding * Thiết lập Content Security Policy (CSP)​ * Sử dụng các tiêu đề phản hồi thích hợp: Content-type * Thiết lập cờ HTTPOnly và Secure Flag cho cookie. |

# 3 Danh sách vị trí đã kiểm tra

|  |  |
| --- | --- |
| **Domain** | **URI** |
| **https://testqltsapp.misa.vn/** | /  /approvereportv2  /assettransfer  /AssetTransfer/FixedAssetTransferOutUnitPopup  /auth/api/auth/addenvironment  /auth/api/auth/addenvironment?tenantId=9583ee42-e55f-11eb-bd5c-005056a68014  /auth/api/auth/login  /auth/api/licenseagreement/getlicenseagreement  /auth/api/tenant/gettenant  /auth/api/user/updatecacheclient  /BudgetCategory/Popup  /BusinessOption/Popup  /changeinformation  /changeinformationri  /ChangeInformationRI/PopupDetail  /Convert/PopupCancel  /Convert/PopupCancelRI  /Convert/PopupDetail  /Convert/PopupDetailRI  /ConvertFAToEQ/PopupDetail  /createreportv2  /dashboard  /DecisionProvide/Popup  /decrementfixedassetri  /DecrementFixedAssetRI/DecrementFixedAssetRIPopupDetail  /Department/Popup  /depreciationfixedasset  /DepreciationFixedAsset/PopupDetail  /depreciationfixedassetri  /DepreciationFixedAssetRI/DepreciationFixedAssetRIPopupDetail  /depreciationforbusiness  /DepreciationForBusiness/DepreciationForBusinessPopupDetail  /DetailV2  /dictionary  /elastic/api/SearchEquipment/SearchEQPaging  /elastic/api/searchfixedasset/doexporttemplatefa  /elastic/api/SearchFixedAsset/SearchFAPaging  /equipment/api/columnconfig/getcolumnconfig  /equipment/api/EquipmentDecrement/pagingEQDecrement  /equipment/api/EquipmentDistribution/GetPagingEQByVoucherId  /equipment/api/EquipmentDistribution/pagingEQDistribution  /equipment/api/EquipmentIncrement/PagingEQIncrement  /equipment/api/EquipmentInventory/GetPagingEQInventoryByVoucherID  /equipment/api/EquipmentInventory/pagingEQInventory  /equipment/api/EquipmentLedger/GetPagingEQByVoucherID  /equipment/api/equipmentlist/getequipmentsbydetail  /equipment/api/EquipmentList/pagingEquipmentList  /equipment/api/EquipmentTransfer/pagingEQTransfer  /equipmentdecrement  /EquipmentDecrement/EquipmentDecrementPopupDetail  /equipmentdistribution  /EquipmentDistribution/EquipmentDistributionPopupDetail  /equipmentincrement  /EquipmentIncrement/Popup  /equipmentinventory  /EquipmentInventory/ScannerPopupDetail  /equipmentlist  /EquipmentList/Detail  /EquipmentList/ExportEquipment  /EquipmentList/ImportEquipment  /equipmenttransfer  /EquipmentTransfer/PopupDetail  /fa/api/activitydiary  /fa/api/autoid/getbyobjectid  /fa/api/autoid/updateautoid  /fa/api/budgetchapter/getbudgetchapterbyid  /fa/api/budgetclause/getbudgetclausebyid  /fa/api/columnconfig/getcolumnconfig  /fa/api/columnconfig/getcolumnconfig?systemCode=search\_fixed\_asset  /fa/api/Dashboard/GetFAGeneral  /fa/api/Dashboard/GetSituationFACategory  /fa/api/dboption/getoptions  /fa/api/dboption/getoptionshownerversion  /fa/api/dboption/getoptionview  /fa/api/dboption/updateoptionworkyear  /fa/api/DecisionProvide/pagingv2  /fa/api/equipmentcategory/checkcountref  /fa/api/ExportTemplate/GetExportTemplate  /fa/api/exporttemplate/getexporttemplatedefault  /fa/api/fixedasset/checkworker  /fa/api/fixedasset/getfanotincrementpaging  /fa/api/FixedAsset/GetForChangeInfo  /fa/api/FixedAssetBuyingPlan/GetPagingFABuyingPlan  /fa/api/fixedassetcategory/checkcountref  /fa/api/FixedAssetCategory/FixedAssetCategory  /fa/api/fixedassetcategory/getbyparams  /fa/api/FixedAssetChangeInformation/GetPagingChangeInfomation  /fa/api/FixedAssetChangeInformation/GetPagingChangeInfomation  /fa/api/FixedAssetDecrement/pagingReducingAsset  /fa/api/FixedAssetDepreciation/pagingDepreciationFixedAsset  /fa/api/FixedAssetDepreciationDetail/PagingDepreciationFixedAssetDetail  /fa/api/FixedAssetExploitation/GetPagingFAExploitation  /fa/api/FixedAssetIncrement/GetPagingFAIncrement  /fa/api/FixedAssetInspectionReport/GetPagingFAInspection  /fa/api/fixedassetinventory/checkisinventory  /fa/api/FixedAssetInventory/GetPagingFAInventoryByVoucherID  /fa/api/FixedAssetInventory/pagingFixedAssetInventory  /fa/api/FixedAssetLedger/GetPagingFAByVoucherId  /fa/api/fixedassetlist/checkimporterror  /fa/api/fixedassetlist/getfixedassetsbydetail  /fa/api/fixedassetlist/pagingfixedassetlist  /fa/api/FixedAssetMaintenancePlan/GetPagingFAMaintenancePlan  /fa/api/FixedAssetQuota/GetFixedAssetQuotaByYear  /fa/api/FixedAssetRearrangement/GetFARearrangement  /fa/api/fixedassetrearrangement/getupdatetime  /fa/api/FixedAssetRequestProcess/GetPagingFAReceiptRecommend  /fa/api/FixedAssetRequestProcess/GetPagingRequestProcessDetail  /fa/api/FixedAssetRequestProvide/GetPagingFARequestProvide  /fa/api/FixedAssetRevaluation/pagingAssetRevaluation  /fa/api/fixedassetricategory/getbyparams  /fa/api/FixedAssetTransfer/pagingFixedAssetTransfer  /fa/api/FixedAssetUsing/GetPagingFAUsingDetail  /fa/api/netpromoterscore/getdatanps  /fa/api/notification/sumnotify  /fa/api/Position/pagingV2  /fa/api/Project  /fa/api/registerlicense/getdatasuman  /fa/api/RegisterLicense/GetHistoryCommitmentOrder  /fa/api/registerlicense/getsumannotice  /fa/api/reportlist/checkdata  /fa/api/role/GetRolePaging  /fa/api/sendandapprovereport/checkprocessreport  /fa/api/SendAndApproveReport/GetChildOrgNotSendReport  /fa/api/SendAndApproveReport/GetCreateReportByPeriod  /fa/api/sendandapprovereport/getcreatereportmaster  /fa/api/sendandapprovereport/getmainreviewreport  /fa/api/SendAndApproveReport/GetMasterReviewReport  /fa/api/SendAndApproveReport/GetSummaryReportDetail  /fa/api/sendandapprovereport/getsummaryreportmaster  /fa/api/user/getbyid  /fa/api/User/GetPagingUserAccount  /fa/api/Vendor  /fa/api/Vendor/pagingV2  /faep/api/FAEPDecision/GetPagingFAEPDecision  /faep/api/FAEPDecision/GetPagingFAEPDetail  /faep/api/FAEPManagement/GetPagingFAEPDetail  /faep/api/FAEPManagement/GetPagingFAEPManagement  /faep/api/FAEPResult/GetPagingFAEPDetail  /faep/api/FAEPResult/GetPagingFAEPResult  /faep/api/FAEPSolution/GetPagingFAEPDetail  /faep/api/FAEPSolution/GetPagingFAEPSolution  /fari/api/columnconfig/getcolumnconfig  /fari/api/DecrementFixedAssetRI/GetPagingFARIDecrement  /fari/api/FixedAssetRIChangeInformation/GetPagingFARIChangeInfo  /fari/api/FixedAssetRIDepreciation/GetPagingFARIDepreciation  /fari/api/FixedAssetRIIncrement/GetPagingFARIIncrement  /fari/api/FixedAssetRIInventory/GetPagingFARIInventory  /fari/api/FixedAssetRIList/pagingFixedAssetRIList  /fari/api/FixedAssetRIRevaluation/GetPagingFARIRevaluation  /fixedassetemploy  /FixedAssetEmploy/FixedAssetEmployPopupDetail  /fixedassetepdecision  /FixedAssetEPDecision/Popup  /fixedassetepmanagement  /FixedAssetEPManagement/Popup  /FixedAssetEPManagement/PopupDetail  /fixedassetepresult  /FixedAssetEPResult/Popup  /fixedassetepsolution  /FixedAssetEPSolution/Popup  /fixedassetexploitation  /FixedAssetExploitation/PopupBusiness  /FixedAssetExploitation/PopupRent  /FixedAssetExploitation/PopupVenture  /FixedAssetHealth/Popup  /fixedassetincrease  /FixedAssetIncrease/ChooseFixedAssetIncrease  /fixedassetinventory  /FixedAssetInventory/FixedAssetInventoryPopupDetail  /fixedassetlist  /FixedAssetList/ChangeBudget  /FixedAssetList/ChooseFixedAssetBycategory  /FixedAssetList/Detail  /FixedAssetList/ExchangeData  /FixedAssetList/ExportTemplateFA  /FixedAssetList/Group  /FixedAssetList/ImportFixedAsset  /FixedAssetList/PrintBarcodePopup  /fixedassetmaintenanceplan  /FixedAssetMaintenancePlan/Popup  /FixedAssetQuota/PopupAddFromFixedAssetCategory  /FixedAssetQuota/PopupAddType  /fixedassetrearrangement  /FixedAssetRearrangement/FixedAssetRearrangementPopup  /FixedAssetRearrangement/RequestRearrangementPopup  /fixedassetreassessment  /fixedassetriincrement  /FixedAssetRIIncrement/FixedAssetRIIncrementPopup  /fixedassetriinventory  /FixedAssetRIInventory/Popup  /fixedassetrilist  /FixedAssetRIList/ExportFixedAssetRI  /FixedAssetRIList/FixedAssetRIListDetail  /FixedAssetRIList/ImportFixedAssetRI  /fixedassetrireassessment  /FixedAssetRIReassessment/FixedAssetRIReassessmentPopupDetail  /home  /login  /Organization/Popup  /Organization/PopupUpdate  /planshopping  /PlanShopping/AutonomousShopping  /PlanShopping/CentralizedShopping  /PopupAcceptSubmitReport  /PopupApproveAndCreateReport  /PopupApproveAndSummaryReport  /PopupRequestReportCreatReport  /PopupRequestSubmitReport  /PopupV2  /position  /Position/Popup  /position?useLayout=0  /Project/Popup  /receiptrecommend  /ReceiptRecommend/ReceiptRecommendPopupDetail  /reducingasset  /ReducingAsset/PopupDetail  /report  /Report/ReportGenerate  /requestprovide  /RequestProvide/PopupDetail  /RoleManagement/PopupAddRole  /search  /searchequipment  /summaryreportv2  /UndoAcceptReportPopupV2  /UserManagement/Child  /UserManagement/PopupAddUser  /UserManagement/PopupChangePasswordUser  /vendor  /vendor/Popup |