Fortify Audit Workbench

CWE Top 25 2021

Webview

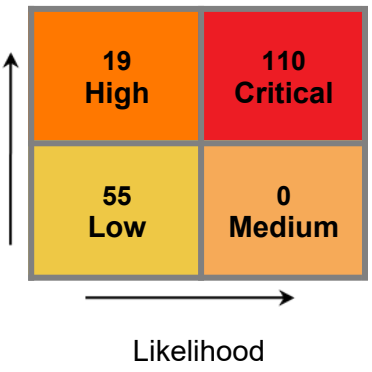
Table of Contents

Executive Summary

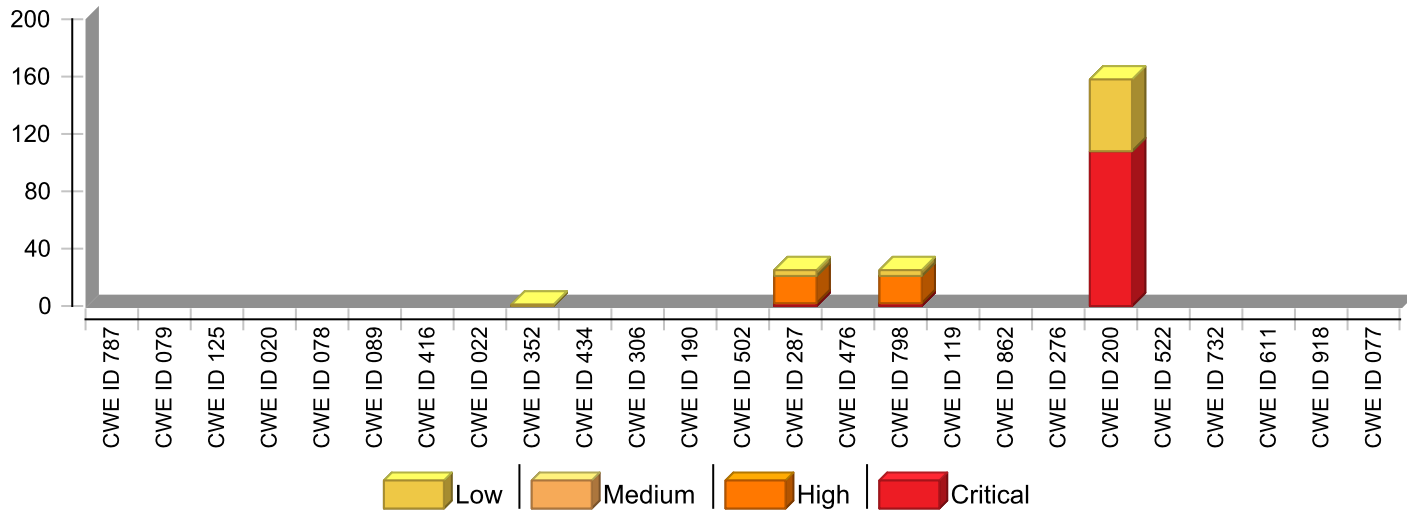
「2021 CWE Top 25 Most Dangerous Software Errors」列舉了軟體中可能導致嚴重弱點的最廣泛和最嚴重的弱點 (如「國家弱點資料庫」所示)。這些弱點經常出現，通常易於尋找與利用。這些錯誤經常可讓攻擊者完全接管軟體、竊取資料或讓軟體完全停止運作，因此這些錯誤非常危險。此清單是 CWE 團隊將啟發式公式與資料驅動方法搭配使用的結果，資料驅動方法採用常見弱點和暴露 (CVE)、國家弱點資料庫 (NVD) 和常見弱點評分系統 (CVSS)。由於 CWE 分類法的階層性質，Fortify 將前 25 個項目子項的所有 CWE ID 視為項目上下文的一部分，因為階層中包含 "CHILD-OF" 關係。如果僅使用此前 25 名清單來確定稽核工作的優先順序，請謹慎行事，因為所分析的軟體可能與用來定義前 25 名的啟發式方法假設不符。例如，這些弱點中的許多弱點與類 C 語言有關，而且所分析的軟體可能不在 C 系列語言之內，因此，許多 CWE 不在範圍之內。

Project Name:	Webview
Project Version:	
SCA:	Results Present
WebInspect:	Results Not Present
WebInspect Agent:	Results Not Present
Other:	Results Not Present
Remediation Effort (Hrs):	9.8

Issues by Priority



Issues by CWE Top 25 2021 Categories



* The detailed sections following the Executive Summary contain specifics.

Project Description

This section provides an overview of the Fortify scan engines used for this project, as well as the project meta-information.

SCA

Date of Last Analysis:	2022年11月15日 下午8:12	**Engine Version:**	21.2.3.0005
Host Name:	880PC0631	**Certification:**	VALID
Number of Files:	585	**Lines of Code:**	22,486

Rulepack Name	Rulepack Version
Fortify 安全編碼規則、社群、雲端	2022.1.1.0007
Fortify 安全編碼規則、社群、通用	2022.1.1.0007
Fortify 安全編碼規則、核心、JavaScript	2022.1.1.0007
Fortify 安全編碼規則、核心、通用	2022.1.1.0007
Fortify 安全編碼規則、延伸、配置	2022.1.1.0007
Fortify 安全編碼規則、延伸、內容	2022.1.1.0007
Fortify 安全編碼規則、延伸、JavaScript	2022.1.1.0007

Issue Breakdown

The following table summarizes the number of issues identified across the different CWE Top 25 2021 categories and broken down by Fortify Priority Order.

	Fortify Priority				Total Issues	Effort (hrs)
	Critical	High	Medium	Low		
[1] CWE ID 787	0	0	0	0	0	0.0
[2] CWE ID 079	0	0	0	0	0	0.0
[3] CWE ID 125	0	0	0	0	0	0.0
[4] CWE ID 020	0	0	0	0	0	0.0
[5] CWE ID 078	0	0	0	0	0	0.0
[6] CWE ID 089	0	0	0	0	0	0.0
[7] CWE ID 416	0	0	0	0	0	0.0
[8] CWE ID 022	0	0	0	0	0	0.0
[9] CWE ID 352	0	0	0	1	1	0.3
[10] CWE ID 434	0	0	0	0	0	0.0
[11] CWE ID 306	0	0	0	0	0	0.0
[12] CWE ID 190	0	0	0	0	0	0.0
[13] CWE ID 502	0	0	0	0	0	0.0
[14] CWE ID 287	2	19	0	4	25	2.2
[15] CWE ID 476	0	0	0	0	0	0.0
[16] CWE ID 798	2	19	0	4	25	2.2
[17] CWE ID 119	0	0	0	0	0	0.0
[18] CWE ID 862	0	0	0	0	0	0.0
[19] CWE ID 276	0	0	0	0	0	0.0
[20] CWE ID 200	108	0	0	50	158	7.5
[21] CWE ID 522	0	0	0	0	0	0.0
[22] CWE ID 732	0	0	0	0	0	0.0
[23] CWE ID 611	0	0	0	0	0	0.0
[24] CWE ID 918	0	0	0	0	0	0.0
[25] CWE ID 077	0	0	0	0	0	0.0

NOTE:
1. Reported issues in the above table may violate more than one CWE Top 25 2021 category. As such, the same issue may appear in more than one row. The total number of unique vulnerabilities are reported in the Executive Summary table.
2. For the same reason, the Project-level remediation effort total shown in the Executive Summary removes the effect of any duplication and may be smaller than the sum of the remediation effort per individual category.
3. Similarly, the remediation effort per external category is not intended to equal the sum of the remediation effort from the issue details section since individual files may contain issues in multiple Fortify priorities or audit folders.

Issue Details

Below is an enumeration of all issues found in the project. The issues are organized by CWE Top 25 2021, Fortify Priority Order, and vulnerability category. The issues are then further broken down by the package, namespace, or location in which they occur. Issues reported at the same line number with the same category originate from different taint sources.

[1] CWE ID 787

CWE-787 用於識別「超出範圍的寫入」弱點。

發生這些弱點的原因是，「軟體在預期緩衝區的結尾之後或開頭之前寫入資料」。

No Issues

[2] CWE ID 079

CWE-79 用於識別「在產生網頁期間不正確地抵消輸入 ('Cross-site Scripting')」弱點。

發生這些弱點的原因是，「軟體在將使用者可以控制的輸入置於用做為其他使用者提供之網頁的輸出中之前，未抵消或不正確地抵消該輸入」。

No Issues

[3] CWE ID 125

CWE-125 用於識別「超出範圍的讀取」弱點。

發生這些弱點的原因是，「軟體在預期緩衝區的結尾之後或開頭之前讀取資料」。

No Issues

[4] CWE ID 020

CWE-20 用於識別「不正確的輸入驗證」弱點。

發生這些弱點的原因是，「產品沒有驗證或不正確地驗證可影響程式之控制流或資料流的輸入」。

No Issues

[5] CWE ID 078

CWE-78 用於識別「不正確地抵消 OS 指令中使用的特殊元素 ('OS Command Injection')」弱點。

發生這些弱點的原因是，「軟體使用源自上游元件之受外部影響的輸入來構建全部或部分 OS 指令，但是未抵消或不正確地抵消特殊元素，這些特殊元素會在將預期的 OS 指令傳送至下游元件時修改預期的 OS 指令」。

No Issues

[6] CWE ID 089

CWE-89 用於識別「不正確地抵消 SQL 指令中使用的特殊元素 ('SQL Injection')」弱點。

發生這些弱點的原因是，「軟體使用源自上游元件之受外部影響的輸入來構建全部或部分 SQL 指令，但是未抵消或不正確地抵消特殊元素，這些特殊元素會在將預期的 SQL 指令傳送至下游元件時修改預期的 OS 指令」。

No Issues

[7] CWE ID 416

CWE-416 用於識別「釋出後使用」弱點。

發生這些弱點的原因是，「參照已釋出的記憶體，可能會導致程式當機、使用非預期的值，或是執行程式碼」。

No Issues

[8] CWE ID 022

CWE-22 用於識別「不正確地將路徑名稱限制到受限制的目錄 ('Path Traversal')」弱點。

發生這些弱點的原因是，「軟體使用外部輸入來構建旨在識別受限制父系目錄下之檔案或目錄的路徑名稱，但是軟體未正確抵消路徑名稱內的特殊元素，這些特殊元素會導致路徑名稱解析為受限制目錄之外的位置」。

No Issues

[9] CWE ID 352

CWE-352 用於識別「Cross-Site Request Forgery (CSRF)」弱點。

發生這些弱點的原因是，「Web 應用程式未能或無法充分確認形式良好、有效、一致的要求是否由提交要求的使用者有意提供」。

Cross-Site Request Forgery ***Remediation Effort(Hrs): 0.3***		**Low**
Package: utilities		
Location	**Analysis Info**	**Analyzer**
utilities/axios.js:263	**Sink:** AssignmentStatement **Enclosing Method:** download() **Source:**	SCA

[10] CWE ID 434

CWE-434 用於識別「未限制危險類型之檔案的上傳」弱點。

發生這些弱點的原因是，「軟體允許攻擊者上傳或傳輸危險類型的檔案，這些檔案可在產品環境中自動進行處理」。

No Issues

[11] CWE ID 306

CWE-306 用於識別「缺少關鍵函數驗證」弱點。

發生這些弱點的原因是，「該軟體未對需要證明使用者身分或消耗大量資源的功能執行任何驗證。」

No Issues

[12] CWE ID 190

CWE-190 用於識別「整數溢位或環繞」弱點。

發生這些弱點的原因是，「若邏輯假設產生的值始終大於原始值，則軟體執行的計算會產生整數溢位或環繞。如此會在將計算用於資源管理或執行控制時引入其他弱點」。

No Issues

[13] CWE ID 502

CWE-502 用於識別「還原序列化不可信賴的資料」弱點。

發生這些弱點的原因是，「應用程式對不可信賴的資料執行還原序列化，但未充分確認產生的資料是否有效」。

No Issues

[14] CWE ID 287

CWE-287 用於識別「不正確的驗證」弱點。

發生這些弱點的原因是，「動作執行者宣稱擁有指定的身分時，軟體未驗證或未充分地驗證宣稱是否屬實」。

Key Management: Hardcoded Encryption Key *Remediation Effort(Hrs): 0.2*		Critical
Package: utilities		
Location	**Analysis Info**	**Analyzer**
utilities/CipherUtil.js:121	**Enclosing Method:** () **Source:**	SCA

Password Management: Hardcoded Password *Remediation Effort(Hrs): 0.2*		Critical
Package: proto.Login		
Location	**Analysis Info**	**Analyzer**
proto/Login/login.js:48	**Sink:** FieldAccess: password **Enclosing Method:** Login() **Source:**	SCA

Password Management: Empty Password *Remediation Effort(Hrs): 0.4*		High
Package: pages.A00800_NonMemberRegister		
Location	**Analysis Info**	**Analyzer**
pages/A00800_NonMemberRegister/A00800.js:66	**Sink:** FieldAccess: password **Enclosing Method:** A00800() **Source:**	SCA
pages/A00800_NonMemberRegister/A00800.js:67	**Sink:** FieldAccess: passwordConfirm **Enclosing Method:** A00800() **Source:**	SCA
Package: pages.T00400_CardLessSetting		
Location	**Analysis Info**	**Analyzer**
pages/T00400_CardLessSetting/T004001.js:26	**Sink:** FieldAccess: withdrawPwd **Enclosing Method:** CardLessATM() **Source:**	SCA
pages/T00400_CardLessSetting/T004001.js:27	**Sink:** FieldAccess: withdrawPwdCheck **Enclosing Method:** CardLessATM() **Source:**	SCA

Password Management: Hardcoded Password *Remediation Effort(Hrs): 0.9*		High
Package: utilities		
Location	**Analysis Info**	**Analyzer**
utilities/validation.js:7	**Sink:** FieldAccess: passwordRequired **Enclosing Method:** ~file_function() **Source:**	SCA

[14] CWE ID 287

CWE-287 用於識別「不正確的驗證」弱點。

發生這些弱點的原因是，「動作執行者宣稱擁有指定的身分時，軟體未驗證或未充分地驗證宣稱是否屬實」。

Password Management: Hardcoded Password ***Remediation Effort(Hrs): 0.9***		**High**
Package: utilities		
Location	**Analysis Info**	**Analyzer**
utilities/validation.js:8	**Sink:** FieldAccess: passwordIncludeEnglishAndNumber **Enclosing Method:** ~file_function() **Source:**	SCA
utilities/validation.js:9	**Sink:** FieldAccess: passwordCannotBeTheSameAsId **Enclosing Method:** ~file_function() **Source:**	SCA
utilities/validation.js:10	**Sink:** FieldAccess: passwordWrongLength **Enclosing Method:** ~file_function() **Source:**	SCA
utilities/validation.js:11	**Sink:** FieldAccess: passwordCannotSameCharacter **Enclosing Method:** ~file_function() **Source:**	SCA
utilities/validation.js:12	**Sink:** FieldAccess: passwordCannotConsecutive **Enclosing Method:** ~file_function() **Source:**	SCA
utilities/validation.js:13	**Sink:** FieldAccess: passwordCannotIncludesROCID **Enclosing Method:** ~file_function() **Source:**	SCA
utilities/validation.js:14	**Sink:** FieldAccess: passwordCannotSameBetweenOld **Enclosing Method:** ~file_function() **Source:**	SCA
utilities/validation.js:17	**Sink:** FieldAccess: confirmPasswordRequired **Enclosing Method:** ~file_function() **Source:**	SCA
utilities/validation.js:18	**Sink:** FieldAccess: confirmPasswordNotMatching **Enclosing Method:** ~file_function() **Source:**	SCA
utilities/validation.js:72	**Sink:** FieldAccess: withdrawPasswordRequired **Enclosing Method:** ~file_function() **Source:**	SCA
utilities/validation.js:73	**Sink:** FieldAccess: withdrawPasswordLength **Enclosing Method:** ~file_function() **Source:**	SCA
utilities/validation.js:74	**Sink:** FieldAccess: withdrawPasswordNumberOnly **Enclosing Method:** ~file_function() **Source:**	SCA
utilities/validation.js:77	**Sink:** FieldAccess: confirmWithdrawPasswordRequired **Enclosing Method:** ~file_function() **Source:**	SCA
utilities/validation.js:78	**Sink:** FieldAccess: confirmWithdrawPasswordNotMatching **Enclosing Method:** ~file_function() **Source:**	SCA

[14] CWE ID 287

CWE-287 用於識別「不正確的驗證」弱點。

發生這些弱點的原因是，「動作執行者宣稱擁有指定的身分時，軟體未驗證或未充分地驗證宣稱是否屬實」。

Password Management: Null Password *Remediation Effort(Hrs): 0.6*		Low
Package: pages.A00700_RegularPwdModify		
Location	**Analysis Info**	**Analyzer**
pages/A00700_RegularPwdModify/A00700.js:81	**Sink:** VariableAccess: changePwdResponse **Enclosing Method:** onSubmit() **Source:**	SCA
pages/A00700_RegularPwdModify/index.js:79	**Sink:** VariableAccess: changePwdResponse **Enclosing Method:** onSubmit() **Source:**	SCA
Package: pages.D00400_CardLessWithDrawChgPwd		
Location	**Analysis Info**	**Analyzer**
pages/D00400_CardLessWithDrawChgPwd/index.js:69	**Sink:** VariableAccess: changePwdResponse **Enclosing Method:** changePwdHandler() **Source:**	SCA
Package: pages.T00900_PwdModify		
Location	**Analysis Info**	**Analyzer**
pages/T00900_PwdModify/index.js:74	**Sink:** VariableAccess: changePwdResponse **Enclosing Method:** handlePasswordModify() **Source:**	SCA

[15] CWE ID 476

CWE-476 用於識別「NULL 指標解除參照」弱點。

「當應用程式解除參照的指標預期為有效、卻是 NULL 時，會發生 NULL 指標解除參照，這通常會導致當機或結束。」

No Issues

[16] CWE ID 798

CWE-798 用於識別「使用硬式編碼的憑證」弱點。

發生這些弱點的原因是，「軟體包含硬式編碼的憑證 (例如密碼或加密金鑰)，軟體將這些憑證用於自己的輸入驗證、對外部元件的輸出通訊，或內部資料的加密」。

Key Management: Hardcoded Encryption Key *Remediation Effort(Hrs): 0.2*		Critical
Package: utilities		
Location	**Analysis Info**	**Analyzer**
utilities/CipherUtil.js:121	**Enclosing Method:** () **Source:**	SCA

Password Management: Hardcoded Password *Remediation Effort(Hrs): 0.2*		Critical
Package: proto.Login		
Location	**Analysis Info**	**Analyzer**
proto/Login/login.js:48	**Sink:** FieldAccess: password **Enclosing Method:** Login() **Source:**	SCA

Password Management: Empty Password *Remediation Effort(Hrs): 0.4*		High
Package: pages.A00800_NonMemberRegister		
Location	**Analysis Info**	**Analyzer**
pages/A00800_NonMemberRegister/A00800.js:66	**Sink:** FieldAccess: password **Enclosing Method:** A00800() **Source:**	SCA
pages/A00800_NonMemberRegister/A00800.js:67	**Sink:** FieldAccess: passwordConfirm **Enclosing Method:** A00800() **Source:**	SCA
Package: pages.T00400_CardLessSetting		
Location	**Analysis Info**	**Analyzer**
pages/T00400_CardLessSetting/T004001.js:26	**Sink:** FieldAccess: withdrawPwd **Enclosing Method:** CardLessATM() **Source:**	SCA
pages/T00400_CardLessSetting/T004001.js:27	**Sink:** FieldAccess: withdrawPwdCheck **Enclosing Method:** CardLessATM() **Source:**	SCA

Password Management: Hardcoded Password *Remediation Effort(Hrs): 0.9*		High
Package: utilities		
Location	**Analysis Info**	**Analyzer**
utilities/validation.js:7	**Sink:** FieldAccess: passwordRequired **Enclosing Method:** ~file_function() **Source:**	SCA

[16] CWE ID 798

CWE-798 用於識別「使用硬式編碼的憑證」弱點。

發生這些弱點的原因是，「軟體包含硬式編碼的憑證 (例如密碼或加密金鑰)，軟體將這些憑證用於自己的輸入驗證、對外部元件的輸出通訊，或內部資料的加密」。

Password Management: Hardcoded Password ***Remediation Effort(Hrs): 0.9***	**High**
Package: utilities	

Location	Analysis Info	Analyzer
utilities/validation.js:8	**Sink:** FieldAccess: passwordIncludeEnglishAndNumber **Enclosing Method:** ~file_function() **Source:**	SCA
utilities/validation.js:9	**Sink:** FieldAccess: passwordCannotBeTheSameAsId **Enclosing Method:** ~file_function() **Source:**	SCA
utilities/validation.js:10	**Sink:** FieldAccess: passwordWrongLength **Enclosing Method:** ~file_function() **Source:**	SCA
utilities/validation.js:11	**Sink:** FieldAccess: passwordCannotSameCharacter **Enclosing Method:** ~file_function() **Source:**	SCA
utilities/validation.js:12	**Sink:** FieldAccess: passwordCannotConsecutive **Enclosing Method:** ~file_function() **Source:**	SCA
utilities/validation.js:13	**Sink:** FieldAccess: passwordCannotIncludesROCID **Enclosing Method:** ~file_function() **Source:**	SCA
utilities/validation.js:14	**Sink:** FieldAccess: passwordCannotSameBetweenOld **Enclosing Method:** ~file_function() **Source:**	SCA
utilities/validation.js:17	**Sink:** FieldAccess: confirmPasswordRequired **Enclosing Method:** ~file_function() **Source:**	SCA
utilities/validation.js:18	**Sink:** FieldAccess: confirmPasswordNotMatching **Enclosing Method:** ~file_function() **Source:**	SCA
utilities/validation.js:72	**Sink:** FieldAccess: withdrawPasswordRequired **Enclosing Method:** ~file_function() **Source:**	SCA
utilities/validation.js:73	**Sink:** FieldAccess: withdrawPasswordLength **Enclosing Method:** ~file_function() **Source:**	SCA
utilities/validation.js:74	**Sink:** FieldAccess: withdrawPasswordNumberOnly **Enclosing Method:** ~file_function() **Source:**	SCA
utilities/validation.js:77	**Sink:** FieldAccess: confirmWithdrawPasswordRequired **Enclosing Method:** ~file_function() **Source:**	SCA
utilities/validation.js:78	**Sink:** FieldAccess: confirmWithdrawPasswordNotMatching **Enclosing Method:** ~file_function() **Source:**	SCA

[16] CWE ID 798

CWE-798 用於識別「使用硬式編碼的憑證」弱點。

發生這些弱點的原因是，「軟體包含硬式編碼的憑證 (例如密碼或加密金鑰)，軟體將這些憑證用於自己的輸入驗證、對外部元件的輸出通訊，或內部資料的加密」。

Password Management: Null Password ***Remediation Effort(Hrs): 0.6***	**Low**
Package: pages.A00700_RegularPwdModify	
Location	**Analysis Info**	**Analyzer**
pages/A00700_RegularPwdModify/A00700.js:81	**Sink:** VariableAccess: changePwdResponse **Enclosing Method:** onSubmit() **Source:**	SCA
pages/A00700_RegularPwdModify/index.js:79	**Sink:** VariableAccess: changePwdResponse **Enclosing Method:** onSubmit() **Source:**	SCA
Package: pages.D00400_CardLessWithDrawChgPwd		
Location	**Analysis Info**	**Analyzer**
pages/D00400_CardLessWithDrawChgPwd/index.js:69	**Sink:** VariableAccess: changePwdResponse **Enclosing Method:** changePwdHandler() **Source:**	SCA
Package: pages.T00900_PwdModify		
Location	**Analysis Info**	**Analyzer**
pages/T00900_PwdModify/index.js:74	**Sink:** VariableAccess: changePwdResponse **Enclosing Method:** handlePasswordModify() **Source:**	SCA

[17] CWE ID 119

CWE-119 用於識別「不正確地限制記憶體緩衝區範圍內的作業」弱點。

發生這些弱點的原因是，「軟體在記憶體緩衝區上執行作業，但可以讀取或寫入緩衝區預期範圍之外的記憶體位置」。

No Issues

[18] CWE ID 862

CWE-862 用於識別「缺少授權」弱點。

發生這些弱點的原因是，「當動作執行者嘗試存取資源或執行某項動作時，該軟體未執行授權檢查」。

No Issues

[19] CWE ID 276

CWE-276 用於識別「不正確的預設權限」弱點。

發生這些弱點的原因是，「產品在安裝時，為物件設定了錯誤權限，進而使其向非預期的動作執行者公開」。

No Issues

[20] CWE ID 200

CWE-200 用於識別「將敏感資訊洩漏給未經授權的動作執行者」弱點。

發生這些弱點的原因是「產品將敏感資訊洩漏給未明確授權存取該資訊的動作執行者。」

Privacy Violation *Remediation Effort(Hrs): 4.3*		Critical
Package: assets.images.icons		
Location	**Analysis Info**	**Analyzer**
assets/images/icons/index.js :14	**Sink:** Assignment to textContent **Enclosing Method:** Icon() **Source:** Read PasswordInput **from** FingerPrint() **In** pages/FingerPrintLockSetting/index.js:168	SCA
assets/images/icons/index.js :14	**Sink:** Assignment to textContent **Enclosing Method:** Icon() **Source:** Read PasswordInput **from** OTPValidate() **In** pages/R00600_Adjustment/otpValidate.js:134	SCA
assets/images/icons/index.js :14	**Sink:** Assignment to textContent **Enclosing Method:** Icon() **Source:** Read PasswordInput **from** PwdModify() **In** pages/T00900_PwdModify/index.js:90	SCA
assets/images/icons/index.js :14	**Sink:** Assignment to textContent **Enclosing Method:** Icon() **Source:** Read PasswordInput **from** PwdModify() **In** pages/T00900_PwdModify/index.js:97	SCA
assets/images/icons/index.js :14	**Sink:** Assignment to textContent **Enclosing Method:** Icon() **Source:** Read PasswordInput **from** PwdModify() **In** pages/T00900_PwdModify/index.js:104	SCA
assets/images/icons/index.js :14	**Sink:** Assignment to textContent **Enclosing Method:** Icon() **Source:** Read PasswordInput **from** renderForm() **In** pages/D00400_CardLessWithDrawChgPwd/index.js:109	SCA
assets/images/icons/index.js :14	**Sink:** Assignment to textContent **Enclosing Method:** Icon() **Source:** Read PasswordInput **from** renderForm() **In** pages/D00400_CardLessWithDrawChgPwd/index.js:97	SCA
assets/images/icons/index.js :14	**Sink:** Assignment to textContent **Enclosing Method:** Icon() **Source:** Read PasswordInput **from** renderForm() **In** pages/D00400_CardLessWithDrawChgPwd/index.js:85	SCA
assets/images/icons/index.js :14	**Sink:** Assignment to textContent **Enclosing Method:** Icon() **Source:** Read PasswordInputField **from** renderPage() **In** pages/T00400_CardLessSetting/T004001.js:62	SCA
assets/images/icons/index.js :14	**Sink:** Assignment to textContent **Enclosing Method:** Icon() **Source:** Read PasswordInputField **from** renderPage() **In** pages/T00400_CardLessSetting/T004001.js:68	SCA
assets/images/icons/index.js :14	**Sink:** Assignment to textContent **Enclosing Method:** Icon() **Source:** Read PasswordInput **from** renderFormArea() **In** pages/BillPay/billPay_1.js:80	SCA

[20] CWE ID 200

CWE-200 用於識別「將敏感資訊洩漏給未經授權的動作執行者」弱點。

發生這些弱點的原因是「產品將敏感資訊洩漏給未明確授權存取該資訊的動作執行者。」

Privacy Violation *Remediation Effort(Hrs): 4.3*		Critical
Package: assets.images.icons		
Location	**Analysis Info**	**Analyzer**
assets/images/icons/index.js :14	**Sink:** Assignment to textContent **Enclosing Method:** Icon() **Source:** Read PasswordInput **from** RegularPwdModify( ) **In** pages/A00700_RegularPwdModify/A00700.js:189	SCA
assets/images/icons/index.js :14	**Sink:** Assignment to textContent **Enclosing Method:** Icon() **Source:** Read PasswordInput **from** RegularPwdModify( ) **In** pages/A00700_RegularPwdModify/A00700.js:196	SCA
assets/images/icons/index.js :14	**Sink:** Assignment to textContent **Enclosing Method:** Icon() **Source:** Read PasswordInput **from** RegularPwdModify( ) **In** pages/A00700_RegularPwdModify/A00700.js:203	SCA
assets/images/icons/index.js :14	**Sink:** Assignment to textContent **Enclosing Method:** Icon() **Source:** Read PasswordInput **from** RegularPwdModify( ) **In** pages/A00700_RegularPwdModify/index.js:146	SCA
assets/images/icons/index.js :14	**Sink:** Assignment to textContent **Enclosing Method:** Icon() **Source:** Read PasswordInput **from** RegularPwdModify( ) **In** pages/A00700_RegularPwdModify/index.js:153	SCA
assets/images/icons/index.js :14	**Sink:** Assignment to textContent **Enclosing Method:** Icon() **Source:** Read PasswordInput **from** RegularPwdModify( ) **In** pages/A00700_RegularPwdModify/index.js:160	SCA
assets/images/icons/index.js :14	**Sink:** Assignment to textContent **Enclosing Method:** Icon() **Source:** Read PasswordInput **from** Template() **In** st ories/components/PasswordInput.stories.jsx:41	SCA
assets/images/icons/index.js :14	**Sink:** Assignment to textContent **Enclosing Method:** Icon() **Source:** Read PasswordInput **from** SMSOTPactivate() **In** pages/SMSOTPactivate/index.js:176	SCA
assets/images/icons/index.js :14	**Sink:** Assignment to textContent **Enclosing Method:** Icon() **Source:** Read PasswordInput **from** renderPasswordAre a() **In** components/PasswordDrawer/index.js:119	SCA
assets/images/icons/index.js :14	**Sink:** Assignment to textContent **Enclosing Method:** Icon() **Source:** Read PasswordInput **from** PassWordArea() **In** pages/PatternLockSetting/index.js:166	SCA
assets/images/icons/index.js :14	**Sink:** Assignment to textContent **Enclosing Method:** Icon() **Source:** Read PasswordInput **from** ChangeUserName() **In** pages/T00800_ChangeUserName/index.js:102	SCA

[20] CWE ID 200

CWE-200 用於識別「將敏感資訊洩漏給未經授權的動作執行者」弱點。

發生這些弱點的原因是「產品將敏感資訊洩漏給未明確授權存取該資訊的動作執行者。」

Privacy Violation *Remediation Effort(Hrs): 4.3*		Critical
Package: assets.images.icons		
Location	**Analysis Info**	**Analyzer**
assets/images/icons/index.js :14	**Sink:** Assignment to textContent **Enclosing Method:** Icon() **Source:** Read PasswordInput **from** ChangeUserName() **In** pages/T00800_ChangeUserName/index.js:94	SCA
assets/images/icons/index.js :14	**Sink:** Assignment to textContent **Enclosing Method:** Icon() **Source:** Read PasswordInput **from** ChangeUserName() **In** pages/T00800_ChangeUserName/index.js:86	SCA
Package: components.Fields		
Location	**Analysis Info**	**Analyzer**
components/Fields/passwordInputField.js:37	**Sink:** Assignment to textContent **Enclosing Method:** PasswordInputField() **Source:** Read handleClickShowPassword **from** PasswordInputField() **In** components/Fields/passwordInputField.js:54	SCA
components/Fields/passwordInputField.js:37	**Sink:** Assignment to textContent **Enclosing Method:** PasswordInputField() **Source:** Read PasswordInputField **from** renderPage() **In** pages/T00400_CardLessSetting/T004001.js:62	SCA
components/Fields/passwordInputField.js:37	**Sink:** Assignment to textContent **Enclosing Method:** PasswordInputField() **Source:** Read PasswordInputField **from** renderPage() **In** pages/T00400_CardLessSetting/T004001.js:68	SCA
Package: components.PasswordInput		
Location	**Analysis Info**	**Analyzer**
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read PasswordInput **from** PassWordArea() **In** pages/PatternLockSetting/index.js:166	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read PasswordInput **from** renderPasswordArea() **In** components/PasswordDrawer/index.js:119	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read PasswordInput **from** PwdModify() **In** pages/T00900_PwdModify/index.js:90	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read PasswordInput **from** PwdModify() **In** pages/T00900_PwdModify/index.js:97	SCA

[20] CWE ID 200

CWE-200 用於識別「將敏感資訊洩漏給未經授權的動作執行者」弱點。

發生這些弱點的原因是「產品將敏感資訊洩漏給未明確授權存取該資訊的動作執行者。」

Privacy Violation *Remediation Effort(Hrs): 4.3*	Critical
Package: components.PasswordInput	

Location	Analysis Info	Analyzer
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read PasswordInput **from** FingerPrint() **In** pages/FingerPrintLockSetting/index.js:168	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read errors.password **from** PwdModify() **In** pages/T00900_PwdModify/index.js:95	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read PasswordInput **from** SMSOTPactivate() **In** pages/SMSOTPactivate/index.js:176	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read errors.newPasswordConfirm **from** renderForm() **In** pages/D00400_CardLessWithDrawChgPwd/index.js:116	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read errors.newPassword **from** PwdModify() **In** pages/T00900_PwdModify/index.js:102	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read errors.password **from** OTPValidate() **In** pages/R00600_Adjustment/otpValidate.js:139	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read errors.oldPassword **from** renderForm() **In** pages/D00400_CardLessWithDrawChgPwd/index.js:92	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read PasswordInput **from** renderForm() **In** pages/D00400_CardLessWithDrawChgPwd/index.js:109	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read PasswordInput **from** renderForm() **In** pages/D00400_CardLessWithDrawChgPwd/index.js:85	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read PasswordInput **from** renderForm() **In** pages/D00400_CardLessWithDrawChgPwd/index.js:97	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read errors.newPasswordCheck **from** PwdModify() **In** pages/T00900_PwdModify/index.js:109	SCA

[20] CWE ID 200

CWE-200 用於識別「將敏感資訊洩漏給未經授權的動作執行者」弱點。

發生這些弱點的原因是「產品將敏感資訊洩漏給未明確授權存取該資訊的動作執行者。」

Privacy Violation *Remediation Effort(Hrs): 4.3*		Critical
Package: components.PasswordInput		
Location	**Analysis Info**	**Analyzer**
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read errors.password **from** PassWordArea() **In** pages/PatternLockSetting/index.js:169	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read PasswordInput **from** RegularPwdModify() **In** pages/A00700_RegularPwdModify/A00700.js:189	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read PasswordInput **from** RegularPwdModify() **In** pages/A00700_RegularPwdModify/A00700.js:203	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read PasswordInput **from** RegularPwdModify() **In** pages/A00700_RegularPwdModify/A00700.js:196	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read PasswordDrawer **from** Template() **In** stories/components/PasswordDrawer.stories.js:19	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read PasswordInput **from** RegularPwdModify() **In** pages/A00700_RegularPwdModify/index.js:153	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read PasswordInput **from** RegularPwdModify() **In** pages/A00700_RegularPwdModify/index.js:146	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read PasswordInput **from** RegularPwdModify() **In** pages/A00700_RegularPwdModify/index.js:160	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read errors.newPassword **from** RegularPwdModify() **In** pages/A00700_RegularPwdModify/A00700.js:201	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read errors.newPassword **from** RegularPwdModify() **In** pages/A00700_RegularPwdModify/index.js:158	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read PassWordArea **from** PatternLockSetting() **In** pages/PatternLockSetting/index.js:225	SCA

[20] CWE ID 200

CWE-200 用於識別「將敏感資訊洩漏給未經授權的動作執行者」弱點。

發生這些弱點的原因是「產品將敏感資訊洩漏給未明確授權存取該資訊的動作執行者。」

Privacy Violation *Remediation Effort(Hrs): 4.3*	Critical
Package: components.PasswordInput	

Location	Analysis Info	Analyzer
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read PasswordInput **from** PwdModify() **In** pages/T00900_PwdModify/index.js:104	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read errors.password **from** SMSOTPactivate() **In** pages/SMSOTPactivate/index.js:181	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read PasswordInput **from** renderFormArea() **In** pages/BillPay/billPay_1.js:80	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read errors.password **from** renderFormArea() **In** pages/BillPay/billPay_1.js:83	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read errors.password **from** renderPasswordArea() **In** components/PasswordDrawer/index.js:123	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read PasswordDrawer **from** appTransactionAuth() **In** utilities/AppScriptProxy.js:557	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read errors.password **from** RegularPwdModify() **In** pages/A00700_RegularPwdModify/A00700.js:194	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read errors.password **from** RegularPwdModify() **In** pages/A00700_RegularPwdModify/index.js:151	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read PasswordInput **from** ChangeUserName() **In** pages/T00800_ChangeUserName/index.js:94	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read PasswordInput **from** ChangeUserName() **In** pages/T00800_ChangeUserName/index.js:86	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read PasswordInput **from** ChangeUserName() **In** pages/T00800_ChangeUserName/index.js:102	SCA

[20] CWE ID 200

CWE-200 用於識別「將敏感資訊洩漏給未經授權的動作執行者」弱點。

發生這些弱點的原因是「產品將敏感資訊洩漏給未明確授權存取該資訊的動作執行者。」

Privacy Violation *Remediation Effort(Hrs): 4.3*		Critical
Package: components.PasswordInput		
Location	**Analysis Info**	**Analyzer**
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read errors.newPassword **from** renderForm() **In** pages/D00400_CardLessWithDrawChgPwd/index.js:104	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read PasswordInput **from** Template() **In** stories/components/PasswordInput.stories.jsx:41	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read errors.password **from** FingerPrint() **In** pages/FingerPrintLockSetting/index.js:173	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read errors.newPasswordCheck **from** RegularPwdModify() **In** pages/A00700_RegularPwdModify/index.js:165	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read errors.newPasswordCheck **from** RegularPwdModify() **In** pages/A00700_RegularPwdModify/A00700.js:208	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read PasswordInput **from** OTPValidate() **In** pages/R00600_Adjustment/otpValidate.js:134	SCA
components/PasswordInput/index.js:39	**Sink:** Assignment to textContent **Enclosing Method:** renderControllerWithInput() **Source:** Read renderPasswordArea **from** PasswordDrawer() **In** components/PasswordDrawer/index.js:131	SCA
components/PasswordInput/index.js:81	**Sink:** Assignment to textContent **Enclosing Method:** PasswordInput() **Source:** Read PassWordArea **from** PatternLockSetting() **In** pages/PatternLockSetting/index.js:225	SCA
components/PasswordInput/index.js:81	**Sink:** Assignment to textContent **Enclosing Method:** PasswordInput() **Source:** Read PasswordInput **from** PwdModify() **In** pages/T00900_PwdModify/index.js:90	SCA
components/PasswordInput/index.js:81	**Sink:** Assignment to textContent **Enclosing Method:** PasswordInput() **Source:** Read PasswordInput **from** PwdModify() **In** pages/T00900_PwdModify/index.js:97	SCA

[20] CWE ID 200

CWE-200 用於識別「將敏感資訊洩漏給未經授權的動作執行者」弱點。

發生這些弱點的原因是「產品將敏感資訊洩漏給未明確授權存取該資訊的動作執行者。」

Privacy Violation *Remediation Effort(Hrs): 4.3*	Critical
Package: components.PasswordInput	

Location	Analysis Info	Analyzer
components/PasswordInput/index.js:81	**Sink:** Assignment to textContent **Enclosing Method:** PasswordInput() **Source:** Read PasswordInput **from** PwdModify() **In** pages/T00900_PwdModify/index.js:104	SCA
components/PasswordInput/index.js:81	**Sink:** Assignment to textContent **Enclosing Method:** PasswordInput() **Source:** Read PasswordInput **from** SMSOTPactivate() **In** pages/SMSOTPactivate/index.js:176	SCA
components/PasswordInput/index.js:81	**Sink:** Assignment to textContent **Enclosing Method:** PasswordInput() **Source:** Read renderPasswordArea **from** PasswordDrawer() **In** components/PasswordDrawer/index.js:131	SCA
components/PasswordInput/index.js:81	**Sink:** Assignment to textContent **Enclosing Method:** PasswordInput() **Source:** Read PasswordInput **from** PassWordArea() **In** pages/PatternLockSetting/index.js:166	SCA
components/PasswordInput/index.js:81	**Sink:** Assignment to textContent **Enclosing Method:** PasswordInput() **Source:** Read PasswordInput **from** RegularPwdModify() **In** pages/A00700_RegularPwdModify/index.js:146	SCA
components/PasswordInput/index.js:81	**Sink:** Assignment to textContent **Enclosing Method:** PasswordInput() **Source:** Read PasswordInput **from** RegularPwdModify() **In** pages/A00700_RegularPwdModify/A00700.js:203	SCA
components/PasswordInput/index.js:81	**Sink:** Assignment to textContent **Enclosing Method:** PasswordInput() **Source:** Read PasswordInput **from** RegularPwdModify() **In** pages/A00700_RegularPwdModify/index.js:160	SCA
components/PasswordInput/index.js:81	**Sink:** Assignment to textContent **Enclosing Method:** PasswordInput() **Source:** Read PasswordInput **from** RegularPwdModify() **In** pages/A00700_RegularPwdModify/index.js:153	SCA
components/PasswordInput/index.js:81	**Sink:** Assignment to textContent **Enclosing Method:** PasswordInput() **Source:** Read PasswordInput **from** RegularPwdModify() **In** pages/A00700_RegularPwdModify/A00700.js:196	SCA
components/PasswordInput/index.js:81	**Sink:** Assignment to textContent **Enclosing Method:** PasswordInput() **Source:** Read PasswordInput **from** RegularPwdModify() **In** pages/A00700_RegularPwdModify/A00700.js:189	SCA
components/PasswordInput/index.js:81	**Sink:** Assignment to textContent **Enclosing Method:** PasswordInput() **Source:** Read handleClickShowPassword **from** renderInput() **In** components/PasswordInput/index.js:76	SCA

[20] CWE ID 200

CWE-200 用於識別「將敏感資訊洩漏給未經授權的動作執行者」弱點。

發生這些弱點的原因是「產品將敏感資訊洩漏給未明確授權存取該資訊的動作執行者。」

Privacy Violation *Remediation Effort(Hrs): 4.3*		Critical
Package: components.PasswordInput		
Location	**Analysis Info**	**Analyzer**
components/PasswordInput/index.js:81	**Sink:** Assignment to textContent **Enclosing Method:** PasswordInput() **Source:** Read PasswordDrawer **from** appTransactionAuth() **In** utilities/AppScriptProxy.js:557	SCA
components/PasswordInput/index.js:81	**Sink:** Assignment to textContent **Enclosing Method:** PasswordInput() **Source:** Read PasswordInput **from** renderForm() **In** pages/D00400_CardLessWithDrawChgPwd/index.js:109	SCA
components/PasswordInput/index.js:81	**Sink:** Assignment to textContent **Enclosing Method:** PasswordInput() **Source:** Read PasswordInput **from** renderForm() **In** pages/D00400_CardLessWithDrawChgPwd/index.js:97	SCA
components/PasswordInput/index.js:81	**Sink:** Assignment to textContent **Enclosing Method:** PasswordInput() **Source:** Read PasswordInput **from** renderForm() **In** pages/D00400_CardLessWithDrawChgPwd/index.js:85	SCA
components/PasswordInput/index.js:81	**Sink:** Assignment to textContent **Enclosing Method:** PasswordInput() **Source:** Read PasswordInput **from** OTPValidate() **In** pages/R00600_Adjustment/otpValidate.js:134	SCA
components/PasswordInput/index.js:81	**Sink:** Assignment to textContent **Enclosing Method:** PasswordInput() **Source:** Read PasswordDrawer **from** Template() **In** stories/components/PasswordDrawer.stories.js:19	SCA
components/PasswordInput/index.js:81	**Sink:** Assignment to textContent **Enclosing Method:** PasswordInput() **Source:** Read PasswordInput **from** renderPasswordArea() **In** components/PasswordDrawer/index.js:119	SCA
components/PasswordInput/index.js:81	**Sink:** Assignment to textContent **Enclosing Method:** PasswordInput() **Source:** Read PasswordInput **from** Template() **In** stories/components/PasswordInput.stories.jsx:41	SCA
components/PasswordInput/index.js:81	**Sink:** Assignment to textContent **Enclosing Method:** PasswordInput() **Source:** Read PasswordInput **from** ChangeUserName() **In** pages/T00800_ChangeUserName/index.js:86	SCA
components/PasswordInput/index.js:81	**Sink:** Assignment to textContent **Enclosing Method:** PasswordInput() **Source:** Read PasswordInput **from** ChangeUserName() **In** pages/T00800_ChangeUserName/index.js:94	SCA
components/PasswordInput/index.js:81	**Sink:** Assignment to textContent **Enclosing Method:** PasswordInput() **Source:** Read PasswordInput **from** ChangeUserName() **In** pages/T00800_ChangeUserName/index.js:102	SCA

[20] CWE ID 200

CWE-200 用於識別「將敏感資訊洩漏給未經授權的動作執行者」弱點。

發生這些弱點的原因是「產品將敏感資訊洩漏給未明確授權存取該資訊的動作執行者。」

Privacy Violation *Remediation Effort(Hrs): 4.3*		Critical
Package: components.PasswordInput		
Location	**Analysis Info**	**Analyzer**
components/PasswordInput/index.js:81	**Sink:** Assignment to textContent **Enclosing Method:** PasswordInput() **Source:** Read PasswordInput **from** renderFormArea() **In** pages/BillPay/billPay_1.js:80	SCA
components/PasswordInput/index.js:81	**Sink:** Assignment to textContent **Enclosing Method:** PasswordInput() **Source:** Read PasswordInput **from** FingerPrint() **In** pages/FingerPrintLockSetting/index.js:168	SCA
Package: pages.A00800_NonMemberRegister		
Location	**Analysis Info**	**Analyzer**
pages/A00800_NonMemberRegister/api.js:17	**Sink:** ~JS_Generic.log() **Enclosing Method:** memberRegister() **Source:** Read data.password **from** onSubmit() **In** pages/A00800_NonMemberRegister/A00800.js:137	SCA
Package: pages.BillPay		
Location	**Analysis Info**	**Analyzer**
pages/BillPay/billPay_1.js:78	**Sink:** Assignment to textContent **Enclosing Method:** renderFormArea() **Source:** Read PasswordInput.prototype **from** renderFormArea() **In** pages/BillPay/billPay_1.js:80	SCA
pages/BillPay/billPay_1.js:78	**Sink:** Assignment to textContent **Enclosing Method:** renderFormArea() **Source:** Read errors.password **from** renderFormArea() **In** pages/BillPay/billPay_1.js:83	SCA
pages/BillPay/billPay_1.js:78	**Sink:** Assignment to textContent **Enclosing Method:** renderFormArea() **Source:** Read handleClickShowPassword **from** renderInput() **In** components/PasswordInput/index.js:76	SCA
pages/BillPay/billPay_1.js:210	**Sink:** Assignment to textContent **Enclosing Method:** pageControll() **Source:** Read errors.password **from** renderFormArea() **In** pages/BillPay/billPay_1.js:83	SCA
pages/BillPay/billPay_1.js:210	**Sink:** Assignment to textContent **Enclosing Method:** pageControll() **Source:** Read PasswordInput.prototype **from** renderFormArea() **In** pages/BillPay/billPay_1.js:80	SCA
pages/BillPay/billPay_1.js:227	**Sink:** Assignment to textContent **Enclosing Method:** pageControll() **Source:** Read errors.password **from** renderFormArea() **In** pages/BillPay/billPay_1.js:83	SCA
pages/BillPay/billPay_1.js:227	**Sink:** Assignment to textContent **Enclosing Method:** pageControll() **Source:** Read PasswordInput.prototype **from** renderFormArea() **In** pages/BillPay/billPay_1.js:80	SCA

[20] CWE ID 200

CWE-200 用於識別「將敏感資訊洩漏給未經授權的動作執行者」弱點。

發生這些弱點的原因是「產品將敏感資訊洩漏給未明確授權存取該資訊的動作執行者。」

Privacy Violation *Remediation Effort(Hrs): 4.3*		Critical
Package: pages.T00900_PwdModify		
Location	**Analysis Info**	**Analyzer**
pages/T00900_PwdModify/index.js:50	**Sink:** Assignment to textContent **Enclosing Method:** setResultDialog() **Source:** Read handlePasswordModify **from** onSubmit() **In** pages/T00900_PwdModify/index.js:82	SCA
Package: utilities		
Location	**Analysis Info**	**Analyzer**
utilities/AppScriptProxy.js:79	**Sink:** ~JS_Generic.log() **Enclosing Method:** callAppJavaScript() **Source:** Read handlePasswordModify **from** onSubmit() **In** pages/T00900_PwdModify/index.js:82	SCA
System Information Leak: External ***Remediation Effort(Hrs): 1.7***		**Low**
Package: components.CreditCard		
Location	**Analysis Info**	**Analyzer**
components/CreditCard/index.jsx:51	**Sink:** Assignment to textContent **Enclosing Method:** AccountCard() **Source:** Read process.env **from** startFunc() **In** utilities/AppScriptProxy.js:167	SCA
Package: components.DepositPlanHeroSlide		
Location	**Analysis Info**	**Analyzer**
components/DepositPlanHeroSlide/index.jsx:81	**Sink:** Assignment to src **Enclosing Method:** DepositPlanHeroSlide() **Source:** Read process.env **from** imgSrc() **In** components/DepositPlanHeroSlide/index.jsx:44	SCA
Package: components.SuccessFailureAnimations		
Location	**Analysis Info**	**Analyzer**
components/SuccessFailureAnimations/index.js:45	**Sink:** Assignment to textContent **Enclosing Method:** renderSuccessInfo() **Source:** lambda(0) **from** lambda() **In** utilities/axios.js:237	SCA
components/SuccessFailureAnimations/index.js:51	**Sink:** Assignment to textContent **Enclosing Method:** renderErrorInfo() **Source:** lambda(0) **from** lambda() **In** utilities/axios.js:237	SCA

[20] CWE ID 200

CWE-200 用於識別「將敏感資訊洩漏給未經授權的動作執行者」弱點。

發生這些弱點的原因是「產品將敏感資訊洩漏給未明確授權存取該資訊的動作執行者。」

System Information Leak: External *Remediation Effort(Hrs): 1.7*	Low

Package: pages.B00300_Notice

Location	Analysis Info	Analyzer
pages/B00300_Notice/index.js :114	**Sink:** Assignment to textContent **Enclosing Method:** renderEditList() **Source:** Read process.env **from** userRequest() **In** u tilities/axios.js:180	SCA
pages/B00300_Notice/index.js :114	**Sink:** Assignment to textContent **Enclosing Method:** renderEditList() **Source:** Read process.env **from** userRequest() **In** u tilities/axios.js:180	SCA

Package: pages.B00600_More

Location	Analysis Info	Analyzer
pages/B00600_More/B00600.js: 43	**Sink:** setItem() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** utilities/axi os.js:237	SCA

Package: pages.C00300_NtdDeposit.DepositPlus

Location	Analysis Info	Analyzer
pages/C00300_NtdDeposit/ Depo sitPlus/depositPlusDetail.js:85	**Sink:** Assignment to textContent **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** utilities/axi os.js:237	SCA
pages/C00300_NtdDeposit/ Depo sitPlus/depositPlusDetail.js:87	**Sink:** Assignment to textContent **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** utilities/axi os.js:237	SCA
pages/C00300_NtdDeposit/ Depo sitPlus/depositPlusDetail.js:88	**Sink:** Assignment to textContent **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** utilities/axi os.js:237	SCA

Package: pages.C00600_DepositPlan.components

Location	Analysis Info	Analyzer
pages/C00600_DepositPlan/ com ponents/HeroWithEdit.jsx:121	**Sink:** Assignment to src **Enclosing Method:** HeroWithEdit() **Source:** Read process.env **from** imgSrc() **In** pages/ C00600_DepositPlan/components/HeroWithEdit.jsx:31	SCA

Package: pages.C00700_CreditCard

Location	Analysis Info	Analyzer
pages/C00700_CreditCard/C007 00.jsx:57	**Sink:** Assignment to options.textContent **Enclosing Method:** functionAllList() **Source:** Read process.env **from** startFunc() **In** uti lities/AppScriptProxy.js:167	SCA

[20] CWE ID 200

CWE-200 用於識別「將敏感資訊洩漏給未經授權的動作執行者」弱點。

發生這些弱點的原因是「產品將敏感資訊洩漏給未明確授權存取該資訊的動作執行者。」

System Information Leak: External *Remediation Effort(Hrs): 1.7*	Low

Package: pages.C00700_CreditCard

Location	Analysis Info	Analyzer
pages/C00700_CreditCard/C00700.jsx:61	**Sink:** Assignment to textContent **Enclosing Method:** lambda() **Source:** Read process.env **from** startFunc() **In** utilities/AppScriptProxy.js:167	SCA
pages/C00700_CreditCard/C00700.jsx:89	**Sink:** Assignment to options.textContent **Enclosing Method:** handleMoreClick() **Source:** Read process.env **from** startFunc() **In** utilities/AppScriptProxy.js:167	SCA
pages/C00700_CreditCard/C00700.jsx:91	**Sink:** Assignment to textContent **Enclosing Method:** lambda() **Source:** Read process.env **from** startFunc() **In** utilities/AppScriptProxy.js:167	SCA

Package: pages.T00100_Profile

Location	Analysis Info	Analyzer
pages/T00100_Profile/T00100.js:226	**Sink:** Assignment to textContent **Enclosing Method:** T00100() **Source:** Read process.env **from** userRequest() **In** utilities/axios.js:180	SCA
pages/T00100_Profile/T00100.js:226	**Sink:** Assignment to textContent **Enclosing Method:** T00100() **Source:** Read process.env **from** userRequest() **In** utilities/axios.js:180	SCA
pages/T00100_Profile/T00100.js:226	**Sink:** Assignment to textContent **Enclosing Method:** T00100() **Source:** lambda(0) **from** lambda() **In** utilities/axios.js:237	SCA
pages/T00100_Profile/index.js:182	**Sink:** Assignment to textContent **Enclosing Method:** Profile() **Source:** Read process.env **from** userRequest() **In** utilities/axios.js:180	SCA
pages/T00100_Profile/index.js:182	**Sink:** Assignment to textContent **Enclosing Method:** Profile() **Source:** Read process.env **from** userRequest() **In** utilities/axios.js:180	SCA

Package: proto.Login

Location	Analysis Info	Analyzer
proto/Login/DoGetToken.js:27	**Sink:** ~JS_Generic.confirm() **Enclosing Method:** getKey() **Source:** lambda(0) **from** lambda() **In** utilities/axios.js:237	SCA
proto/Login/HandShake.js:42	**Sink:** setItem() **Enclosing Method:** handshake() **Source:** lambda(0) **from** lambda() **In** utilities/axios.js:237	SCA

[20] CWE ID 200

CWE-200 用於識別「將敏感資訊洩漏給未經授權的動作執行者」弱點。

發生這些弱點的原因是「產品將敏感資訊洩漏給未明確授權存取該資訊的動作執行者。」

System Information Leak: External *Remediation Effort(Hrs): 1.7*		Low
Package: proto.Login		
Location	**Analysis Info**	**Analyzer**
proto/Login/HandShake.js:45	**Sink:** alert() **Enclosing Method:** handshake() **Source:** lambda(0) **from** lambda() **In** utilities/axios.js:237	SCA
proto/Login/login.api.js:22	**Sink:** ~JS_Generic.confirm() **Enclosing Method:** login() **Source:** lambda(0) **from** lambda() **In** utilities/axios.js:237	SCA
proto/Login/login.api.js:32	**Sink:** alert() **Enclosing Method:** login() **Source:** lambda(0) **from** lambda() **In** utilities/axios.js:237	SCA
proto/Login/login.api.js:33	**Sink:** alert() **Enclosing Method:** login() **Source:** lambda(0) **from** lambda() **In** utilities/axios.js:237	SCA

System Information Leak: Internal *Remediation Effort(Hrs): 1.8*		Low
Package: pages.A00400_Provisioning		
Location	**Analysis Info**	**Analyzer**
pages/A00400_Provisioning/index.js:36	**Sink:** ~JS_Generic.log() **Enclosing Method:** triggerProvide() **Source:** lambda(0) **from** lambda() **In** utilities/axios.js:237	SCA
Package: pages.A00600_RegularBasicInformation		
Location	**Analysis Info**	**Analyzer**
pages/A00600_RegularBasicInformation/index.js:76	**Sink:** ~JS_Generic.log() **Enclosing Method:** getJobsCode() **Source:** lambda(0) **from** lambda() **In** utilities/axios.js:237	SCA
Package: pages.D00100_NtdTransfer		
Location	**Analysis Info**	**Analyzer**
pages/D00100_NtdTransfer/D00100_1.js:74	**Sink:** ~JS_Generic.log() **Enclosing Method:** onConfirm() **Source:** lambda(0) **from** lambda() **In** utilities/axios.js:237	SCA
pages/D00100_NtdTransfer/D00100_2.js:56	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** utilities/axios.js:237	SCA

[20] CWE ID 200

CWE-200 用於識別「將敏感資訊洩漏給未經授權的動作執行者」弱點。

發生這些弱點的原因是「產品將敏感資訊洩漏給未明確授權存取該資訊的動作執行者。」

System Information Leak: Internal *Remediation Effort(Hrs): 1.8*	Low

Package: pages.D00300_CardLessATM

Location	Analysis Info	Analyzer
pages/D00300_CardLessATM/D00300_1.js:88	**Sink:** ~JS_Generic.log() **Enclosing Method:** fetchAccountSummary() **Source:** lambda(0) **from** lambda() **In** utilities/axios.js:237	SCA
pages/D00300_CardLessATM/D00300_1.js:119	**Sink:** ~JS_Generic.log() **Enclosing Method:** requestCardlessWithdrawApply() **Source:** lambda(0) **from** lambda() **In** utilities/axios.js:237	SCA

Package: pages.D00700_ForeignCurrencyTransfer

Location	Analysis Info	Analyzer
pages/D00700_ForeignCurrencyTransfer/index.js:59	**Sink:** ~JS_Generic.log() **Enclosing Method:** getForeignCurrencyAccounts() **Source:** lambda(0) **from** lambda() **In** utilities/axios.js:237	SCA
pages/D00700_ForeignCurrencyTransfer/index.js:70	**Sink:** ~JS_Generic.log() **Enclosing Method:** getForeignCurrencyAccounts() **Source:** lambda(0) **from** lambda() **In** utilities/axios.js:237	SCA
pages/D00700_ForeignCurrencyTransfer/index.js:86	**Sink:** ~JS_Generic.log() **Enclosing Method:** getTransTypeOptions() **Source:** lambda(0) **from** lambda() **In** utilities/axios.js:237	SCA

Package: pages.ForeignCurrencyPriceSetting

Location	Analysis Info	Analyzer
pages/ForeignCurrencyPriceSetting/index.js:66	**Sink:** ~JS_Generic.log() **Enclosing Method:** getCurrencyInfo() **Source:** lambda(0) **from** lambda() **In** utilities/axios.js:237	SCA
pages/ForeignCurrencyPriceSetting/index.js:81	**Sink:** ~JS_Generic.log() **Enclosing Method:** getAllPriceNotifications() **Source:** lambda(0) **from** lambda() **In** utilities/axios.js:237	SCA

Package: pages.L00100_Loan

Location	Analysis Info	Analyzer
pages/L00100_Loan/api.js:87	**Sink:** ~JS_Generic.log() **Enclosing Method:** getLoanSummary() **Source:** lambda(0) **from** lambda() **In** utilities/axios.js:237	SCA

[20] CWE ID 200

CWE-200 用於識別「將敏感資訊洩漏給未經授權的動作執行者」弱點。

發生這些弱點的原因是「產品將敏感資訊洩漏給未明確授權存取該資訊的動作執行者。」

System Information Leak: Internal *Remediation Effort(Hrs): 1.8*	Low

Package: pages.T00100_Profile

Location	Analysis Info	Analyzer
pages/T00100_Profile/T00100.js:100	**Sink:** ~JS_Generic.log() **Enclosing Method:** uploadAvatarImg() **Source:** lambda(0) **from** lambda() **In** utilities/axios.js:237	SCA
pages/T00100_Profile/T00100.js:121	**Sink:** ~JS_Generic.log() **Enclosing Method:** onSubmit() **Source:** lambda(0) **from** lambda() **In** utilities/axios.js:237	SCA
pages/T00100_Profile/index.js:78	**Sink:** ~JS_Generic.log() **Enclosing Method:** uploadAvatarImg() **Source:** lambda(0) **from** lambda() **In** utilities/axios.js:237	SCA
pages/T00100_Profile/index.js:110	**Sink:** ~JS_Generic.log() **Enclosing Method:** onSubmit() **Source:** lambda(0) **from** lambda() **In** utilities/axios.js:237	SCA

Package: pages.T00300_NonDesignatedTransfer

Location	Analysis Info	Analyzer
pages/T00300_NonDesignatedTransfer/T00300.js:61	**Sink:** ~JS_Generic.log() **Enclosing Method:** onFailure() **Source:** lambda(0) **from** lambda() **In** utilities/axios.js:237	SCA
pages/T00300_NonDesignatedTransfer/T00300.js:241	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** utilities/axios.js:237	SCA

Package: pages.T00700_BasicInformation

Location	Analysis Info	Analyzer
pages/T00700_BasicInformation/T00700.js:54	**Sink:** ~JS_Generic.log() **Enclosing Method:** fetchCountyList() **Source:** lambda(0) **from** lambda() **In** utilities/axios.js:237	SCA
pages/T00700_BasicInformation/T00700.js:54	**Sink:** ~JS_Generic.log() **Enclosing Method:** fetchCountyList() **Source:** lambda(0) **from** lambda() **In** utilities/axios.js:237	SCA

Package: utilities

Location	Analysis Info	Analyzer
utilities/AppScriptProxy.js:26	**Sink:** ~JS_Generic.log() **Enclosing Method:** callAppJavaScript() **Source:** Read process.env **from** shareMessageContent() **In** pages/M00100_Community/M00100.js:45	SCA

[20] CWE ID 200

CWE-200 用於識別「將敏感資訊洩漏給未經授權的動作執行者」弱點。

發生這些弱點的原因是「產品將敏感資訊洩漏給未明確授權存取該資訊的動作執行者。」

System Information Leak: Internal *Remediation Effort(Hrs): 1.8*	Low
Package: utilities	

Location	Analysis Info	Analyzer
utilities/AppScriptProxy.js: 26	**Sink:** ~JS_Generic.log() **Enclosing Method:** callAppJavaScript() **Source:** lambda(0) **from** lambda() **In** utilities/axios.js:237	SCA
utilities/AppScriptProxy.js: 538	**Sink:** ~JS_Generic.log() **Enclosing Method:** appTransactionAuth() **Source:** lambda(0) **from** lambda() **In** utilities/axios.js:237	SCA
utilities/axios.js:281	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** utilities/axios.js:280	SCA

[21] CWE ID 522

CWE-522 用於識別「憑證保護不足」弱點。

發生這些弱點的原因是，「產品會傳輸或儲存驗證憑證，但使用的方法不安全，容易受到未經授權的攔截和/或擷取。」

No Issues

[22] CWE ID 732

CWE-732 用於識別「為關鍵資源指定不正確的權限」弱點。

發生這些弱點的原因是，「軟體為安全關鍵資源指定權限時，所採用的方式允許非預期的動作執行者讀取或修改資源」。

No Issues

[23] CWE ID 611

CWE-611 用於識別「不正確地限制 XML 外部實體參照」弱點。

發生這些弱點的原因是，「軟體處理的 XML 文件可能包含具有 URI 的 XML 實體，而這些 URI 會解析為預期控制領域之外的文件，這導致產品將不正確的文件內嵌到其輸出中」。

No Issues

[24] CWE ID 918

CWE-918 用於識別「Server-Side Request Forgery (SSRF)」弱點。

發生這些弱點的原因是，「Web 伺服器從上游元件收到一個 URL 或類似要求，並擷取此 URL 的內容，但無法充分確保該要求會傳送至預期的目的地」。

No Issues

[25] CWE ID 077

CWE-77 用於識別「不正確地抵消指令中使用的特殊元素 (「Command Injection」)」弱點。

發生這些弱點的原因是，「軟體使用源自上游元件之受外部影響的輸入來構建全部或部分指令，但是未抵消或不正確地抵消特殊元素，這些特殊元素會在將預期的指令傳送至下游元件時修改預期的指令」。

No Issues

Description of Key Terminology

Likelihood and Impact

Likelihood
Likelihood is the probability that a vulnerability will be accurately identified and successfully exploited.

Impact
Impact is the potential damage an attacker could do to assets by successfully exploiting a vulnerability. This damage can be in the form of, but not limited to, financial loss, compliance violation, loss of brand reputation, and negative publicity.

Fortify Priority Order

Critical
Critical-priority issues have high impact and high likelihood. Critical-priority issues are easy to detect and exploit and result in large asset damage. These issues represent the highest security risk to the application. As such, they should be remediated immediately.

SQL Injection is an example of a critical issue.

High
High-priority issues have high impact and low likelihood. High-priority issues are often difficult to detect and exploit, but can result in large asset damage. These issues represent a high security risk to the application. High-priority issues should be remediated in the next scheduled patch release.

Password Management: Hardcoded Password is an example of a high issue.

Medium
Medium-priority issues have low impact and high likelihood. Medium-priority issues are easy to detect and exploit, but typically result in small asset damage. These issues represent a moderate security risk to the application. Medium-priority issues should be remediated in the next scheduled product update.

Path Manipulation is an example of a medium issue.

Low
Low-priority issues have low impact and low likelihood. Low-priority issues can be difficult to detect and exploit and typically result in small asset damage. These issues represent a minor security risk to the application. Low-priority issues should be remediated as time allows.

Dead Code is an example of a low issue.

Remediation Effort

The report provides remediation effort estimates. You can use these estimates to perform a relative comparison of projects and as a starting point for estimates specific to your organization. Remediation effort estimates are provided in the following report sections:

- Executive Summary
- Issue Breakdown
- Issue Details

To determine remediation effort for a collection of issues, Software Security Center weights each issue based on its category (“remediation constant”) and adds an overhead calculation based on the number of distinct

files which contain the set of issues. The formula used at each report level is the same:

- Remediation Effort (in mins) = SUM(remediation constant for each issue in the set) + 6 * Number of distinct files in that set of issues.

At the lowest level of detail, issues are grouped based on Fortify category and Fortify priority OR Fortify category and folder name, depending on report options. So, for example, the Issue Details section of the report might show the remediation effort for “SQL Injection, Critical” or “SQL Injection, MyFolder”.

At the Issue Breakdown level, remediation effort is shown at the level of each external (non-Fortify) category (such as “AC-3 Access Enforcement” in the case of NIST, or “A1 Unvalidated Input” in the case of OWASP Top10). Remediation effort is calculated for the set of all issues that fall into that external category (irrespective of Fortify priority or folder name). As an example, if there are two SQL injection vulnerabilities, one critical and one medium, within the same file, the file overhead is only included once.

At the Executive Summary level, all issues of that project which are mapped to the specified external category list (such as NIST or CWE) are used in the remediation effort calculation.

Fortify recommends that you treat the different levels of remediation effort as information relevant at that level only. You cannot add up remediation effort at a lower level and expect it to match the remediation effort at a higher level.

About Fortify Solutions

Fortify is the leader in end-to-end application security solutions with the flexibility of testing on-premise and on-demand to cover the entire software development lifecycle. Learn more at www.microfocus.com/solutions/application-security.