Fortify Audit Workbench

Developer Workbook

202506031508

Table of Contents

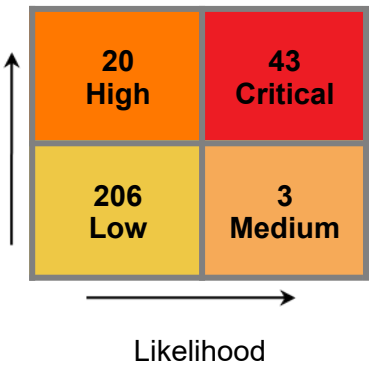
Executive Summary

This workbook is intended to provide all necessary details and information for a developer to understand and remediate the different issues discovered during the 202506031508 project audit. The information contained in this workbook is targeted at project managers and developers.

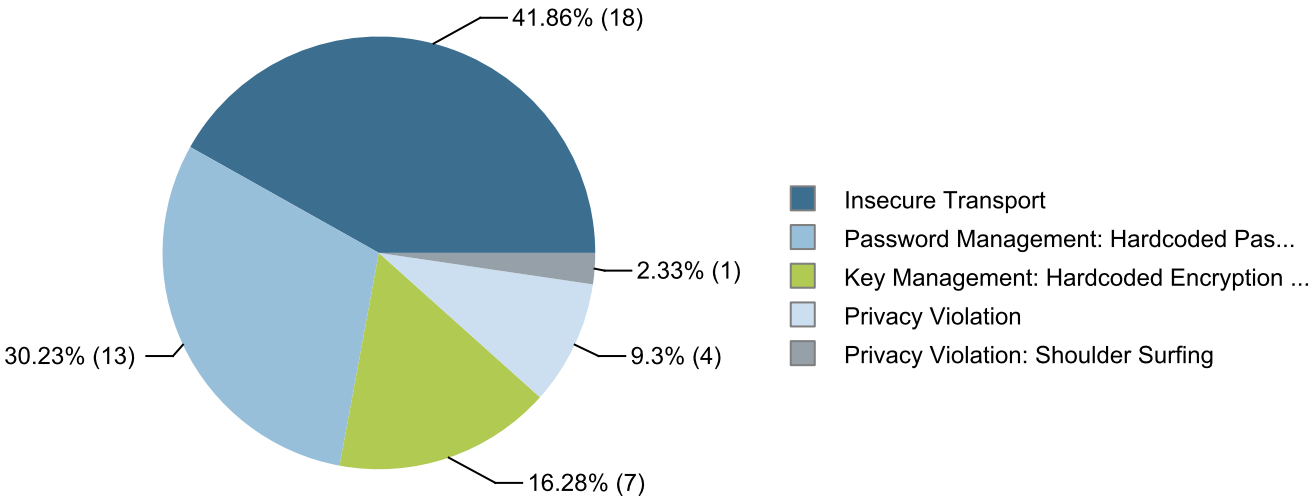
This section provides an overview of the issues uncovered during analysis.

Project Name:	202506031508
Project Version:	
SCA:	Results Present
WebInspect:	Results Not Present
WebInspect Agent:	Results Not Present
Other:	Results Not Present

Issues by Priority



Top Ten Critical Categories



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:	2025年6月3日 下午4:36	**Engine Version:**	22.1.0.0166
Host Name:	HPFortify15	**Certification:**	VALID
Number of Files:	16,042	**Lines of Code:**	430,511

Rulepack Name	Rulepack Version
Fortify 安全編碼規則、社群、Cloud	2025.2.1.0001
Fortify 安全編碼規則、社群、PHP	2025.2.1.0001
Fortify 安全編碼規則、社群、Universal	2025.2.1.0001
Fortify 安全編碼規則、核心、Android	2025.2.1.0001
Fortify 安全編碼規則、核心、Annotations	2025.2.1.0001
Fortify 安全編碼規則、核心、Cloud	2025.2.1.0001
Fortify 安全編碼規則、核心、.NET	2025.2.1.0001
Fortify 安全編碼規則、核心、Java	2025.2.1.0001
Fortify 安全編碼規則、核心、JavaScript	2025.2.1.0001
Fortify 安全編碼規則、核心、PHP	2025.2.1.0001
Fortify 安全編碼規則、核心、Python	2025.2.1.0001
Fortify 安全編碼規則、核心、SQL	2025.2.1.0001
Fortify 安全編碼規則、核心、Universal	2025.2.1.0001
Fortify 安全編碼規則、延伸、配置	2025.2.1.0001
Fortify 安全編碼規則、延伸、內容	2025.2.1.0001
Fortify 安全編碼規則、延伸、.NET	2025.2.1.0001
Fortify 安全編碼規則、延伸、Java	2025.2.1.0001
Fortify 安全編碼規則、延伸、JavaScript	2025.2.1.0001
Fortify 安全編碼規則、延伸、JSP	2025.2.1.0001
Fortify 安全編碼規則、延伸、SQL	2025.2.1.0001

Issue Breakdown by Fortify Categories

The following table depicts a summary of all issues grouped vertically by Fortify Category. For each category, the total number of issues is shown by Fortify Priority Order, including information about the number of audited issues.

Category	Fortify Priority (audited/total)				Total Issues
	Critical	High	Medium	Low	
Credential Management: Hardcoded API Credentials	0	0 / 2	0	0	0 / 2
Cross-Site Request Forgery	0	0	0	0 / 5	0 / 5
Cross-Site Scripting: Self	0	0	0	0 / 8	0 / 8
Dynamic Code Evaluation: Code Injection	0	0 / 2	0	0	0 / 2
Hardcoded Domain in HTML	0	0	0	0 / 1	0 / 1
Insecure Randomness	0	0 / 7	0	0	0 / 7
Insecure Transport	0 / 18	0	0	0	0 / 18
Insecure Transport: External Link	0	0	0 / 3	0	0 / 3
Key Management: Hardcoded Encryption Key	0 / 7	0	0	0	0 / 7
Key Management: Null Encryption Key	0	0	0	0 / 1	0 / 1
Password Management: Empty Password	0	0 / 3	0	0	0 / 3
Password Management: Hardcoded Password	0 / 13	0 / 3	0	0	0 / 16
Password Management: Null Password	0	0	0	0 / 7	0 / 7
Password Management: Password in Comment	0	0	0	0 / 61	0 / 61
Path Manipulation	0	0 / 2	0	0	0 / 2
Poor Error Handling: Empty Catch Block	0	0	0	0 / 96	0 / 96
Poor Logging Practice: Use of a System Output Stream	0	0	0	0 / 10	0 / 10
Privacy Violation	0 / 4	0	0	0	0 / 4
Privacy Violation: Shoulder Surfing	0 / 1	0	0	0	0 / 1
Race Condition	0	0 / 1	0	0	0 / 1
System Information Leak: External	0	0	0	0 / 1	0 / 1
System Information Leak: Internal	0	0	0	0 / 5	0 / 5
Weak Cryptographic Hash	0	0	0	0 / 11	0 / 11

Results Outline

Credential Management: Hardcoded API Credentials (2 issues)

Abstract

硬式編碼的 API 認證會導致無法輕易修正系統的安全性問題。

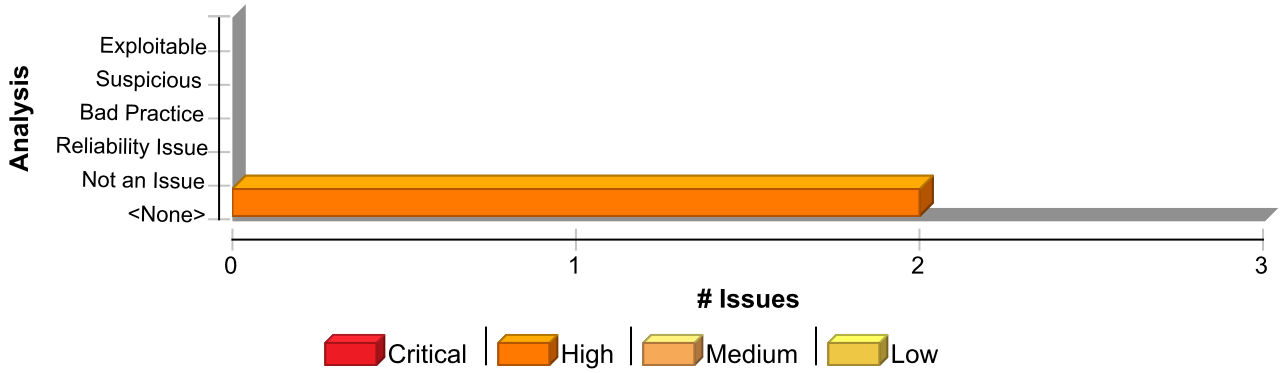
Explanation

切勿對認證進行硬式編碼，包括使用者名稱、密碼、API 金鑰、API 機密和 API 權杖。所有的專案開發人員不僅可以看到硬式編碼的認證，要更新這些內容也極為困難。程式碼進入生產階段後，除非修補軟體，否則無法變更認證。如果認證遭到破解，組織必須在安全性和系統可用性之間做出選擇。

Recommendation

請確定 API 認證是從僅在執行階段環境中可用的組態設定檔案或從環境變數載入。

Issue Summary



Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Credential Management: Hardcoded API Credentials	2	0	0	2
Total	**2**	**0**	**0**	**2**

Credential Management: Hardcoded API Credentials	**High**
Package: .venv.lib.python3.13.site-packages.bleak	
.venv/lib/python3.13/site-packages/bleak/uuids.py, line 723 (Credential Management: Hardcoded API Credentials)	**High**

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Sink Details

File: .venv/lib/python3.13/site-packages/bleak/uuids.py:723
Taint Flags:

Credential Management: Hardcoded API Credentials — High

Package: .venv.lib.python3.13.site-packages.bleak

.venv/lib/python3.13/site-packages/bleak/uuids.py, line 723 (Credential Management: Hardcoded API Credentials) — High

```
720  0x2BB2: "Advertising Constant Tone Extension PHY",
721  0x2BB3: "Bearer Provider Name",
722  0x2BB4: "Bearer UCI",
723  0x2BB5: "Bearer Technology",
724  0x2BB6: "Bearer URI Schemes Supported List",
725  0x2BB7: "Bearer Signal Strength",
726  0x2BB8: "Bearer Signal Strength Reporting Interval",
```

Package: frontend.node_modules.@ant-design.icons-angular.fesm2022

frontend/node_modules/@ant-design/icons-angular/fesm2022/ant-design-icons-angular-icons.mjs.map, line 1 (Credential Management: Hardcoded API Credentials) — High

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Sink Details

File: frontend/node_modules/@ant-design/icons-angular/fesm2022/ant-design-icons-angular-icons.mjs.map:1
Taint Flags:

```
1 [Too long 833611 chars line truncated to 3500 ones]{"version":3,"file":"ant-design-icons-
angular-icons.mjs","sources":["../../../src/icons/outline/AccountBookOutline.ts","../../../src/
icons/fill/AccountBookFill.ts","../../../src/icons/outline/AlertOutline.ts","../../../src/
icons/outline/AimOutline.ts","../../../src/icons/outline/AlibabaOutline.ts","../../../src/
icons/fill/AlertFill.ts","../../../src/icons/outline/AlignCenterOutline.ts","../../../src/
icons/twotone/AlertTwoTone.ts","../../../src/icons/fill/AlipayCircleFill.ts","../../../src/
icons/fill/AlipaySquareFill.ts","../../../src/icons/outline/AlipayCircleOutline.ts","../../../
src/icons/outline/AlignRightOutline.ts","../../../src/icons/fill/
AmazonSquareFill.ts","../../../src/icons/outline/AlipayOutline.ts","../../../src/icons/outline/
ApiOutline.ts","../../../src/icons/outline/AliwangwangOutline.ts","../../../src/icons/outline/
AmazonOutline.ts","../../../src/icons/fill/AndroidFill.ts","../../../src/icons/outline/
AntCloudOutline.ts","../../../src/icons/fill/AppleFill.ts","../../../src/icons/fill/
AmazonCircleFill.ts","../../../src/icons/outline/AppstoreOutline.ts","../../../src/icons/
outline/AppstoreAddOutline.ts","../../../src/icons/outline/AppleOutline.ts","../../../src/
icons/outline/AreaChartOutline.ts","../../../src/icons/twotone/AppstoreTwoTone.ts","../../../
src/icons/fill/AppstoreFill.ts","../../../src/icons/outline/ArrowRightOutline.ts","../../../
src/icons/outline/AudioMutedOutline.ts","../../../src/icons/outline/
ArrowsAltOutline.ts","../../../src/icons/outline/BackwardOutline.ts","../../../src/icons/
outline/AuditOutline.ts","../../../src/icons/outline/BarChartOutline.ts","../../../src/icons/
fill/BankFill.ts","../../../src/icons/outline/AudioOutline.ts","../../../src/icons/twotone/
AudioTwoTone.ts","../../../src/icons/outline/BankOutline.ts","../../../src/icons/fill/
BackwardFill.ts","../../../src/icons/outline/BarsOutline.ts","../../../src/icons/outline/
ArrowLeftOutline.ts","../../../src/icons/outline/ArrowUpOutline.ts","../../../src/icons/
twotone/BankTwoTone.ts","../../../src/icons/outline/BellOutline.ts","../../../src/icons/fill/
AudioFill.ts","../../../src/icons/outline/BoldOutline.ts","../../../src/icons/outline/
BehanceOutline.ts","../../../src/icons/fill/BehanceCircleFill.ts","../../../src/icons/outline/
AliyunOutline.ts","../../../src/icons/fill/BehanceSquareFill.ts","../../../src/icons/twotone/
AccountBookTwoTone.ts","../../../src/icons/fill/AliwangwangFill.ts","../../../src/icons/
outline/ArrowDownOutline.ts","../../../src/icons/outline/BehanceSquareOutline.ts","../../../
src/icons/outline/ApartmentOutline.ts","../../../src/icons/outline/BlockOutline.ts","../../../
src/icons/outline/BorderOuterOutline.ts","../../../src/icons/outline/
```

Credential Management: Hardcoded API Credentials	High
Package: frontend.node_modules.@ant-design.icons-angular.fesm2022	
frontend/node_modules/@ant-design/icons-angular/fesm2022/ant-design-icons-angular-icons.mjs.map, line 1 (Credential Management: Hardcoded API Credentials)	High

```
BarcodeOutline.ts","../../../src/icons/twotone/BookTwoTone.ts","../../../src/icons/outline/
BorderHorizontalOutline.ts","../../../src/icons/outline/BorderVerticleOutline.ts","../../../
src/icons/outline/BorderlessTableOutline.ts","../../../src/icons/outline/
BorderOutline.ts","../../../src/icons/outline/BorderInnerOutline.ts","../../../src/icons/
outline/BorderTopOutline.ts","../../../src/icons/outline/BgColorsOutline.ts","../../../src/
icons/fill/BoxPlotFill.ts","../../../src/icons/outline/BorderLeftOutline.ts","../../../src/
icons/outline/BranchesOutline.ts","../../../src/icons/twotone/BoxPlotTwoTone.ts","../../../src/
icons/outline/BoxPlotOutline.ts","../../../src/icons/fill/BookFill.ts","../../../src/icons/
fill/BuildFill.ts","../../../src/icons/fill/BulbFill.ts","../../../src/icons/outline/
BugOutline.t
2
3 undefined
4 undefined
5 undefined
6 undefined
7 undefined
```

Cross-Site Request Forgery (5 issues)

Abstract

HTTP 要求必須包含特定使用者密碼，以避免攻擊者作出未經授權的要求。

Explanation

防禦跨網站偽造要求 (CSRF) 弱點會在以下情況中出現： 1. Web 應用程式使用了階段作業 cookie。 2. 應用程式在回應 HTTP 要求時，沒有驗證該要求是否經使用者同意產生。 nonce 是與訊息一起傳送的加密隨機值，用於防止重複進行的攻擊。如果要求不包含其來源的證明，則負責處理要求的程式碼將容易受到 CSRF 的攻擊 (除非它不改變應用程式的狀態)。這代表使用工作階段 Cookie 的 Web 應用程式必須特別留意，以確保攻擊者沒辦法傳遞假造的要求去欺騙使用者。想像若 Web 應用程式允許管理人員如下建立新帳戶：

```
  var req = new XMLHttpRequest();
  req.open("POST", "/new_user", true);
  body = addToPost(body, new_username);
  body = addToPost(body, new_passwd);
  req.send(body);
```

攻擊者可能會建立一個包含下列程式碼的惡意網站。

```
  var req = new XMLHttpRequest();
  req.open("POST", "http://www.example.com/new_user", true);
  body = addToPost(body, "attacker");
  body = addToPost(body, "haha");
  req.send(body);
```

如果 example.com 管理員在網站上的有效階段作業期間造訪惡意頁面，則會在不知不覺中為攻擊者建立帳戶。這就是 CSRF 攻擊。這樣是有可能的，因為應用程式無法確定要求的來源。因此不論是使用者建立的或是由攻擊者建立的偽造操作，都會被視為合法的操作。攻擊者不會看到假造的要求所產生的網頁，所以這種攻擊技術只有對修改應用程式狀態的要求有用。 在 URL 中傳送階段作業識別碼而非當作 Cookie 的應用程式不會有 CSRF 問題，因為攻擊者沒有辦法存取階段作業識別碼做為假造的要求。

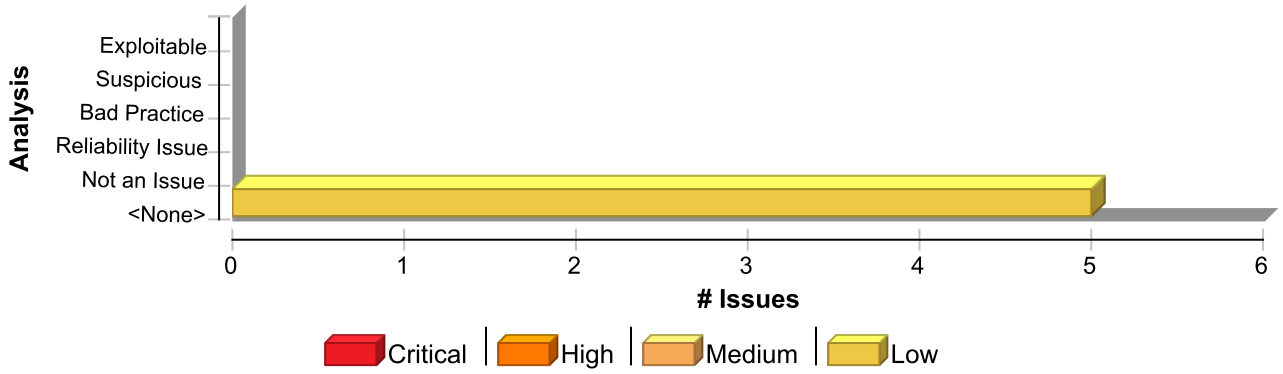
Recommendation

使用階段作業 Cookie 的應用程式必須包含每個發佈表單的一部分資訊，以供後端程式碼用來驗證要求的來源。其中一種方法是包含一個隨機要求識別碼或 nonce，如下所示：

```
  RequestBuilder rb = new RequestBuilder(RequestBuilder.POST, "/new_user");
  body = addToPost(body, new_username);
  body = addToPost(body, new_passwd);
  body = addToPost(body, request_id);
  rb.sendRequest(body, new NewAccountCallback(callback));
```

之後後端邏輯就能夠在處理其他的表單資料前，先驗證要求識別碼。如果可能，各伺服器要求應具備唯一的要求識別碼，而非讓特定工作階段的所有要求共用要求識別碼。就階段作業識別碼而言，攻擊者如果愈難猜出要求識別碼，就愈難發起一次成功的 CSRF 攻擊。權杖應無法輕易猜出，且其受保護的方式應與保護工作階段權杖的方式相同 (例如使用 SSLv3)。 其他減緩技術包括： **架構保護：**大多數現代 Web 應用程式架構都內嵌 CSRF 保護，且會自動包括並驗證 CSRF 權杖。 **使用挑戰/回應控制項：**強制客戶回應伺服器傳送的挑戰是針對 CSRF 的強大防禦措施。可用於此用途的一些挑戰有：CAPTCHA、密碼重新驗證和一次性權杖。 **檢查 HTTP Referer/Origin 表頭：**攻擊者將無法在執行 CSRF 攻擊時欺騙這些表頭。因此，這些表頭將成為防止 CSRF 攻擊的有用方式。 **對階段作業 Cookie 進行雙重提交：**除了傳送實際的階段作業識別碼 Cookie 外，還以隱藏表單值的形式傳送階段作業 ID Cookie，這是針對 CSRF 攻擊的良好保護方式。伺服器會先檢查這兩個值，確保其完全相同，然後再處理其餘的表單資料。若攻擊者代表使用者提交表單，將無法根據相同來源策略修改階段作業 ID Cookie 值。 **限制階段作業存留期：**若使用 CSRF 攻擊存取受保護的資源，只有在作為攻擊一部分而傳送的階段作業 ID 在伺服器上仍有效時，攻擊才有效。限制階段作業存留期會降低攻擊成功的可能。 XSS 攻擊會破解此處描述的技術。有效的 CSRF 減緩措施包括 XSS 減緩技術。

Issue Summary



Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Cross-Site Request Forgery	5	0	0	5
Total	**5**	**0**	**0**	**5**

Cross-Site Request Forgery — Low

Package: .src.app.features.contact

frontend/src/app/features/contact/contact.component.html, line 69 (Cross-Site Request Forgery) — Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Content)

Sink Details

File: frontend/src/app/features/contact/contact.component.html:69
Taint Flags:

```
66  <mat-card-subtitle>憚怠神隙乩 ″ 讌曝 <mat-card-subtitle>
67  </mat-card-header>
68  <mat-card-content>
69  <form [formGroup]="contactForm" (ngSubmit)="onSubmit()" class="contact__form-content">
70  <!-- 憫 -->
71  <mat-form-field appearance="outline" class="contact__field">
72  <mat-label>憫 * </mat-label>
```

Package: .src.app.shared.components.login-modal

frontend/src/app/shared/components/login-modal/login-modal.component.html, line 13 (Cross-Site Request Forgery) — Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Content)

Sink Details

File: frontend/src/app/shared/components/login-modal/login-modal.component.html:13
Taint Flags:

Cross-Site Request Forgery — Low

Package: .src.app.shared.components.login-modal

frontend/src/app/shared/components/login-modal/login-modal.component.html, line 13 (Cross-Site Request Forgery) — Low

```
10  </button>
11  </header>
12
13  <form class="login-form" (ngSubmit)="onSubmit()" #loginForm="ngForm">
14  <div class="login-form__group">
15  <label for="username" class="login-form__label">□ □ □□□</label>
16  <input
```

Package: <none>

test_complete_workflow.html, line 526 (Cross-Site Request Forgery) — Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: go()
File: test_complete_workflow.html:526
Taint Flags:

```
523
524  try {
525  const response = await fetch(`${API_BASE}/bluetooth/devices/${deviceId}/cast`, {
526  method: 'POST',
527  headers: {
528  'Content-Type': 'application/json'
529  },
```

test_complete_workflow.html, line 578 (Cross-Site Request Forgery) — Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: go()
File: test_complete_workflow.html:578
Taint Flags:

```
575  for (const device of devices) {
576  try {
577  const response = await fetch(`${API_BASE}/bluetooth/devices/${device.id}/cast`, {
578  method: 'POST',
579  headers: {
```

Cross-Site Request Forgery — Low

Package: <none>

test_complete_workflow.html, line 578 (Cross-Site Request Forgery) — Low

```
580  'Content-Type': 'application/json'
581  },
```

Package: frontend.node_modules.needle.test.files

frontend/node_modules/needle/test/files/Appalachia.html, line 564 (Cross-Site Request Forgery) — Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Content)

Sink Details

File: frontend/node_modules/needle/test/files/Appalachia.html:564
Taint Flags:

```
561  <div><a href="https://wayback.archive-it.org/3259/20160318141818/http://www.arc.gov/
index.asp"><img src="County%20Economic%20Status%20in%20Appalachia,%20FY%202004%20-
%20Appalachian%20Regional%20Commission_files/top.jpg" style="width:1024px;height:124px;"
alt="Link to ARC home page." border="0"></a></div>
562 <!--BeginNoIndex-->
563  <div class="searchbar">
564  <form action="/3259/20160318141818/http://www.arc.gov/search.asp" method="GET"><div
class="searcharc">Search ARC</div>
565 <input type="text" size="10" name="KEYWORDS" class="searchbox">
566 <input class="searchgo" type="submit" value="Go">
567 </form> </div><!--EndNoIndex-->
```

Cross-Site Scripting: Self (8 issues)

Abstract

傳送未經驗證的資料至網路瀏覽器，會導致瀏覽器執行惡意的程式碼。

Explanation

Cross-Site Scripting (XSS) 弱點會在以下情況中出現： 1.資料從一個不可信賴的來源進入 Web 應用程式。在自我 XSS 的案例中，會從文字方塊或可從 DOM 控制的其他值來讀取資料，並以用戶端程式碼回寫到頁面中。 2.未經驗證且包含在動態內容中的資料將傳送給某個網頁使用者。在自我 XSS 的案例中，惡意內容會做為 DOM (Document Object Model，文件物件模型) 修改的一部分執行。 在自我 XSS 的案例中，惡意內容是以 JavaScript 片段，或瀏覽器執行的其他程式碼類型的形式出現。由於自我 XSS 主要是對自己的攻擊，所以常被認為不重要，但如果可能發生下列任一情況，則應視為標準 XSS 弱點來處理： - 在您的網站上識別出「跨網站偽造要求」弱點。 - 社交工程攻擊可能說服某個使用者攻擊自己的帳戶，進而危及其階段作業。 **範例 1：**請考慮使用 HTML 表單：

```
<div id="myDiv">
  Employee ID: <input type="text" id="eid"><br>
  ...
  <button>Show results</button>
</div>
<div id="resultsDiv">
  ...
</div>
```

以下的 jQuery 程式碼片段會從文字方塊讀取員工識別碼，並顯示給使用者。

```
$(document).ready(function(){
  $("#myDiv").on("click", "button", function(){
    var eid = $("#eid").val();
    $("resultsDiv").append(eid);
    ...
  });
});
```

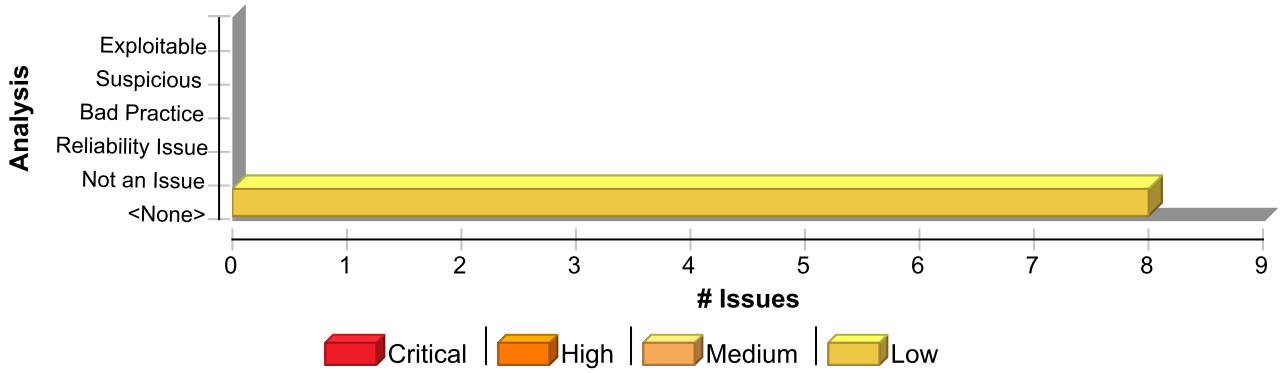
如果文字輸入中的員工識別碼 (識別碼為 eid) 只包含標準英數字元，這些程式碼便會正確地運作。如果 eid 中有包含中繼或來源程式碼中的值，那麼在使用者按一下按鈕後，程式碼就會被新增至 DOM 供瀏覽器執行。如果攻擊者可以說動使用者將惡意內容輸入文字輸入中，那麼這就只是 DOM 型 XSS。

Recommendation

防止 XSS 的解決方法是：確保在需要的位置進行驗證，並設定相關屬性以防止漏洞。 由於 XSS 弱點會在應用程式在它的輸出中包含惡意資料時出現，所以合理方法就是，在資料離開應用程式之前馬上驗證資料 (如果是 DOM 型，會在轉譯之前馬上驗證)。然而，由於 Web 應用程式經常會為了產生動態內容而包含複雜且難以理解的程式碼，所以此方法容易遺漏錯誤 (遺漏驗證)。降低此風險的有效方法即為執行 XSS 輸入驗證。Web 應用程式必須驗證所有輸入以防止出現其他弱點 (如 SQL Injection)，因此比較簡單的方法就是，加強應用程式現有的輸入驗證機制，納入 XSS 檢查。儘管有一定的作用，但是 XSS 的輸入驗證並不能取代嚴格的輸出驗證。應用程式可能會透過共用資料存放區或者其他信賴的來源接受輸入，而該資料存放區可能會從未執行適當輸入驗證的來源接受輸入。因此，應用程式不能間接依賴此資料或任何其他資料的安全性。這代表杜絕 XSS 弱點的最佳方法就是，驗證所有進入應用程式的資料，以及所有離開應用程式並傳送到使用者的資料。 驗證 XSS 最安全的方法，是建立一個安全字元的允許清單，只允許清單上的字元可以出現在 HTTP 內容，並僅接受由經過檢驗的集合中字元組成的輸入。例如，有效的使用者名稱可能僅包含英數字元，或電話號碼可能僅包含數字 0-9。然而，這種解決方式在 Web 應用程式中經常是不可行的，因為很多字元對瀏覽器來說都具有特殊意義，將這些字元編碼之後，必須將它們視為有效輸入。例如，一個網站設計公告欄就必須接受來自於使用者的 HTML 片段。 更具彈性但安全性較低的方法是實作拒絕清單，能在使用輸入前選擇性地拒絕或避開可能有危險的字元。若要建立這類名單，首先必須了解那些對網頁瀏覽器來說有特殊意義的字元集。雖然 HTML 標準會定義具有特殊意義的字元，但是許多網頁瀏覽器會嘗試修正 HTML 中的常見錯誤，而且在特定環境中可能會將其他字元視為有特殊意義。這就是為什麼我們不建議使用拒絕清單做為預防 XSS 的方式。Carnegie Mellon 大學軟體工程學院 (Software Engineering Institute) 下的 CERT(R) 合作中心

(CERT(R) Coordination Center) 提供了在各種環境中具有特殊意義的字元資訊 [1]： 在區塊等級元素的內容中 (位於文字段落中間)： -「<」是特殊字元，因為它會引入標籤。 -「&」是特殊字元，因為它會引入字元實體。 -「>」是特殊字元，因為某些瀏覽器將其視為特殊字元，會假設該頁面的作者想加入開頭的「<」，卻不小心遺漏掉了。 以下原則適用於屬性值： - 在以雙引號括住的屬性值中，雙引號之所以特殊，是因為它們標記了屬性值的結尾。 - 在以單引號結尾的屬性值中，單引號是特殊字元，因為它們標記了屬性值的結尾。 - 在沒有任何引號的屬性值中，空格字元 (例如空格和定位字元) 也是特殊字元。 -「&」和特定屬性一起使用時會變成特殊字元，因為它會引入字元實體。 舉例來說，在 URL 中，搜索引擎可能會在結果頁面提供一個連結，讓使用者可以按一下該連結來重新執行搜尋。這個方法可以運用在編寫 URL 中的搜尋查詢，此動作會引導出其他特殊字元： - 空格、定位字元和換行符號都是特殊字元，因為它們標記了 URL 的結尾。 -「&」為特殊字元，因為它會引入字元實體或分隔 CGI 參數。 - 非 ASCII 字元 (就是所有在 ISO-8859-1 編碼表中大於 127 的字元) 不允許出現在 URL 中，所以它們在此內容中被視為特殊字元。 - 每當伺服器端程式碼對以 HTTP 逸出序列編碼的參數進行解碼時，就必須從輸入中篩選 "%" 符號。例如，對於諸如「%68%65%6C%6C%6F」的輸入，必須篩選「%」，才能在網頁上顯示「hello」。 在 的正文中： - 將文字直接插入原有指令碼標籤時，必須篩選分號、括號、中括號以及換行字元。 伺服器端 Script： - 如果伺服器端指令碼將輸入中的任何驚嘆號字元 (!) 轉換為輸出中的雙引號字元 (")，則可能需要進行更多篩選。 其他可能性： - 若攻擊者提交 UTF-7 的要求，特殊字元「<」會顯示為「+ADw-」，並且可能會避開篩選。如果輸出包含在沒有明確指定編碼格式的頁面中，某些瀏覽器會嘗試以智慧方式來根據內容識別編碼 (在此情況下為 UTF-7)。 在您確定在應用程式中針對 XSS 攻擊執行驗證的正確要點，以及驗證時要考慮的特殊字元後，那麼下一個挑戰就是決定驗證過程中處理特殊字元的方法。如果應用程式將某些特殊字元認定為無效輸入，那麼您可以拒絕任何包含這些被視為無效特殊字元的輸入。第二種選擇是以篩選方式移除特殊字元。然而，篩選所產生的副作用在於會改變篩選內容的顯示樣貌。但是在需要完整顯示輸入內容時，這種情況是無法接受的。 如果必須接受包含特殊字元的輸入，並將其準確顯示出來，驗證動作一定要編碼所有特殊字元，以移除特殊字元代表的意義。官方 HTML 規格 [2] 提供了特殊字元對應的 ISO 8859-1 編碼值完整清單。 很多應用程式伺服器都試圖避免應用程式出現 Cross-site scripting 弱點，方法是為負責設定某個特定 HTTP 回應內容的函數提供各種實作，以驗證是否存在進行 Cross-site scripting 攻擊的字元。請勿依賴執行應用程式的伺服器來確保應用程式的安全性。對於任何開發的應用程式，無法保證在其存留期內將在哪些應用程式伺服器上執行。隨著標準和已知盜取方式不斷地演變，無法保證應用程式伺服器會繼續保持同步。

Issue Summary



Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Cross-Site Scripting: Self	8	0	0	8
Total	**8**	**0**	**0**	**8**

Cross-Site Scripting: Self	**Low**
Package: .src.app.shared.components.modals	
frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts, line 206 (Cross-Site Scripting: Self)	**Low**
Issue Details	

Cross-Site Scripting: Self — Low

Package: .src.app.shared.components.modals

frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts, line 206 (Cross-Site Scripting: Self) — Low

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: Read textarea_20.value
From: onchange
File: frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts:80

```
77  <mat-form-field *ngSwitchCase="'text'" appearance="outline">
78  <mat-label>文字內容</mat-label>
79  <textarea matInput
80  [(ngModel)]="settings.data"
81  rows="3"
82  placeholder="輸入文字內容"
83  (input)="onContentChange()"></textarea>
```

Sink Details

Sink: Assignment to p_72.innerHTML
Enclosing Method: ~file_function()
File: frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts:206
Taint Flags: SELF_XSS, WEB

```
203  </div>
204
205  <div class="preview-info">
206  <p><strong>內容：</strong> {{ getPreviewText() }}</p>
207  <p><strong>大小：</strong> {{ settings.size }}x{{ settings.size }}px</p>
208  <p><strong>錯誤修正：</strong> {{ getErrorCorrectionText() }}</p>
209  <p><strong>邊距：</strong> {{ settings.margin }}px</p>
```

frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts, line 206 (Cross-Site Scripting: Self) — Low

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: Read input_30.value
From: onchange
File: frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts:108

```
105  <div *ngSwitchCase="'wifi'" class="wifi-settings">
106  <mat-form-field appearance="outline">
```

Cross-Site Scripting: Self — Low

Package: .src.app.shared.components.modals

frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts, line 206 (Cross-Site Scripting: Self) — Low

```
107   <mat-label>WiFi名稱 (SSID)</mat-label>
108   <input matInput [(ngModel)]="wifiSSID" (input)="onWifiChange()">
109   </mat-form-field>
110   <mat-form-field appearance="outline">
111   <mat-label>密碼</mat-label>
```

Sink Details

Sink: Assignment to p_72.innerHTML
Enclosing Method: ~file_function()
File: frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts:206
Taint Flags: CONCATENATED, SELF_XSS, WEB

```
203   </div>
204
205   <div class="preview-info">
206   <p><strong>內容：</strong> {{ getPreviewText() }}</p>
207   <p><strong>大小：</strong> {{ settings.size }}x{{ settings.size }}px</p>
208   <p><strong>錯誤修正：</strong> {{ getErrorCorrectionText() }}</p>
209   <p><strong>邊距：</strong> {{ settings.margin }}px</p>
```

frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts, line 156 (Cross-Site Scripting: Self) — Low

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: Read input_53.value
From: onchange
File: frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts:155

```
152   <div class="setting-item">
153   <label>背景色</label>
154   <div class="color-picker">
155   <input
type="color" [(ngModel)]="settings.backgroundColor" (input)="onSettingChange()'
156   <span>{{ settings.backgroundColor }}</span>
157   </div>
158   </div>
```

Sink Details

Cross-Site Scripting: Self — Low

Package: .src.app.shared.components.modals

frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts, line 156 (Cross-Site Scripting: Self) — Low

Sink: Assignment to span_54.innerHTML
Enclosing Method: ~file_function()
File: frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts:156
Taint Flags: SELF_XSS, WEB

```
153  <label>背景色</label>
154  <div class="color-picker">
155  <input type="color" [(ngModel)]="settings.backgroundColor" (input)="onSettingChange()">
156  <span>{{ settings.backgroundColor }}</span>
157  </div>
158  </div>
159
```

frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts, line 206 (Cross-Site Scripting: Self) — Low

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: Read input_23.value
From: onchange
File: frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts:90

```
87  <mat-form-field *ngSwitchCase="'phone'" appearance="outline">
88  <mat-label>電話號碼</mat-label>
89  <input matInput
90  [(ngModel)]="phoneNumber"
91  placeholder="+886-912-345-678"
92  (input)="onPhoneChange()">
93  </mat-form-field>
```

Sink Details

Sink: Assignment to p_72.innerHTML
Enclosing Method: ~file_function()
File: frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts:206
Taint Flags: CONCATENATED, SELF_XSS, WEB

```
203  </div>
204
205  <div class="preview-info">
206  <p><strong>內容：</strong> {{ getPreviewText() }}</p>
207  <p><strong>大小：</strong> {{ settings.size }}x{{ settings.size }}px</p>
208  <p><strong>錯誤修正：</strong> {{ getErrorCorrectionText() }}</p>
209  <p><strong>邊距：</strong> {{ settings.margin }}px</p>
```

Cross-Site Scripting: Self — Low

Package: .src.app.shared.components.modals

frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts, line 206 (Cross-Site Scripting: Self) — **Low**

frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts, line 147 (Cross-Site Scripting: Self) — **Low**

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: Read input_48.value
From: onchange
File: frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts:146

```
143   <div class="setting-item">
144   <label>前景色</label>
145   <div class="color-picker">
146   <input type="color" [(ngModel)]="settings.foregroundColor" (input)="onSettingChange()"
147   <span>{{ settings.foregroundColor }}</span>
148   </div>
149   </div>
```

Sink Details

Sink: Assignment to span_49.innerHTML
Enclosing Method: ~file_function()
File: frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts:147
Taint Flags: SELF_XSS, WEB

```
144   <label>前景色</label>
145   <div class="color-picker">
146   <input type="color" [(ngModel)]="settings.foregroundColor" (input)="onSettingChange()">
147   <span>{{ settings.foregroundColor }}</span>
148   </div>
149   </div>
150
```

frontend/src/app/shared/components/modals/color-picker-modal.component.ts, line 51 (Cross-Site Scripting: Self) — **Low**

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Cross-Site Scripting: Self — Low

Package: .src.app.shared.components.modals

frontend/src/app/shared/components/modals/color-picker-modal.component.ts, line 51 (Cross-Site Scripting: Self) — Low

Source: Read input_15.value
From: onchange
File: frontend/src/app/shared/components/modals/color-picker-modal.component.ts:48

```
45  <div class="custom-color-picker">
46  <input
47  type="color"
48  [(ngModel)]="customColor"
49  (input)="onCustomColorChange($event)"
50  class="color-input">
51  <div class="color-value">{{ customColor }}</div>
```

Sink Details

Sink: Assignment to div_16.innerHTML
Enclosing Method: ~file_function()
File: frontend/src/app/shared/components/modals/color-picker-modal.component.ts:51
Taint Flags: SELF_XSS, WEB

```
48  [(ngModel)]="customColor"
49  (input)="onCustomColorChange($event)"
50  class="color-input">
51  <div class="color-value">{{ customColor }}</div>
52  </div>
53  </div>
54
```

frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts, line 206 (Cross-Site Scripting: Self) — Low

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: Read input_17.value
From: onchange
File: frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts:71

```
68  <mat-form-field *ngSwitchCase="'url'" appearance="outline">
69  <mat-label>網址</mat-label>
70  <input matInput
71  [(ngModel)]="settings.data"
72  placeholder="https://example.com"
73  (input)="onContentChange()">
```

Cross-Site Scripting: Self — Low

Package: .src.app.shared.components.modals

frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts, line 206 (Cross-Site Scripting: Self) — Low

```
74  </mat-form-field>
```

Sink Details

Sink: Assignment to p_72.innerHTML
Enclosing Method: ~file_function()
File: frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts:206
Taint Flags: SELF_XSS, WEB

```
203  </div>
204
205  <div class="preview-info">
206  <p><strong>内容：</strong> {{ getPreviewText() }}</p>
207  <p><strong>大小：</strong> {{ settings.size }}x{{ settings.size }}px</p>
208  <p><strong>錯誤修正：</strong> {{ getErrorCorrectionText() }}</p>
209  <p><strong>邊距：</strong> {{ settings.margin }}px</p>
```

frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts, line 206 (Cross-Site Scripting: Self) — Low

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: Read input_26.value
From: onchange
File: frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts:99

```
96  <mat-form-field *ngSwitchCase="'email'" appearance="outline">
97  <mat-label>電子郵件</mat-label>
98  <input matInput
99  [(ngModel)]="emailAddress"
100  placeholder="example@email.com"
101  (input)="onEmailChange()">
102  </mat-form-field>
```

Sink Details

Sink: Assignment to p_72.innerHTML
Enclosing Method: ~file_function()
File: frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts:206
Taint Flags: CONCATENATED, SELF_XSS, WEB

```
203  </div>
204
205  <div class="preview-info">
```

Cross-Site Scripting: Self	Low

Package: .src.app.shared.components.modals

frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts, line 206 (Cross-Site Scripting: Self)	Low

```
206  <p><strong>内容：</strong> {{ getPreviewText() }}</p>
207  <p><strong>大小：</strong> {{ settings.size }}x{{ settings.size }}px</p>
208  <p><strong>錯誤修正：</strong> {{ getErrorCorrectionText() }}</p>
209  <p><strong>邊距：</strong> {{ settings.margin }}px</p>
```

Dynamic Code Evaluation: Code Injection (2 issues)

Abstract

在執行期間轉譯使用者所控制的指示，可讓攻擊者執行惡意的程式碼。

Explanation

許多現代的程式語言均允許動態轉譯來源指示。此功能可讓程式設計師根據使用者的輸入執行動態指示。程式碼插入弱點會在程式設計師錯誤地假設下列情況時發生：直接由使用者所提供的指示僅會執行無害的作業，例如對使用中的使用者物件進行簡單的計算或修改使用者的狀態。但是，若沒有適當的驗證，使用者可能會指定不是程式設計師想要執行的作業。 **範例 1：**在此典型的程式碼注入範例中，應用程式會實作基本的計算機，讓使用者指定要執行的指令。

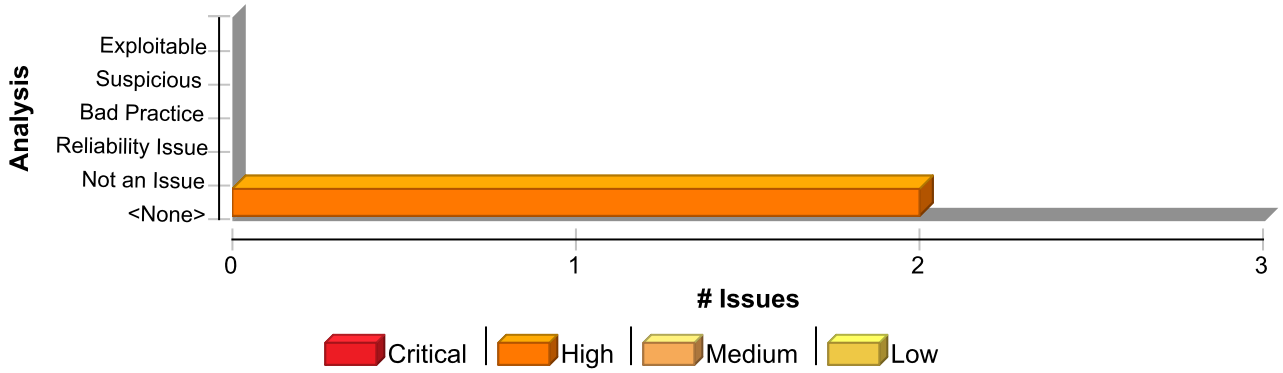
```
...
userOps = request.GET['operation']
result = eval(userOps)
...
```

當 `operation` 參數是良性的值時，例如「8 + 7 * 2」，程式會正常運作。在此案例中，會指定 `result` 變數的值為 22。不過，如果攻擊者指定同時為有效且惡意的作業，則會使用父系程序的完整權限來執行這些作業。當主要語言提供系統資源的存取權限或允許執行系統指令時，這類攻擊會更加危險。例如，如果攻擊者指定「os.system('shutdown -h now')」做為 `operation` 的值，則會在主機系統上執行系統關機指令。

Recommendation

不論何時，請儘可能避免進行 Dynamic code 解譯。如果程式的功能必須動態解譯程式碼，可透過下列方式使受攻擊的可能性減至最低：盡量限制您的程式將動態執行程式碼的數量，將此類程式碼應用在特定的應用程式和上下環境、基於程式語言的子集。 如果執行 Dynamic code 是必要的，則不應由應用程式直接執行和解譯未經驗證的使用者輸入。而是，使用間接方法：建立允許使用者指定的合法作業與資料物件的清單，並且只允許使用者從該清單中進行選擇。使用此方法，就不會直接執行使用者所提供的輸入。

Issue Summary



Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Dynamic Code Evaluation: Code Injection	2	0	0	2
Total	**2**	**0**	**0**	**2**

Dynamic Code Evaluation: Code Injection — High

Package: .venv.lib.python3.13.site-packages.pip._vendor.pygments.formatters

.venv/lib/python3.13/site-packages/pip/_vendor/pygments/formatters/__init__.py, line 103 (Dynamic Code Evaluation: Code Injection) — High

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: file.read()
From: .venv.lib.python3.13.site-packages.pip._vendor.pygments.formatters.load_formatter_from_file
File: .venv/lib/python3.13/site-packages/pip/_vendor/pygments/formatters/__init__.py:103

```
100  # This empty dict will contain the namespace for the exec'd file
101  custom_namespace = {}
102  with open(filename, 'rb') as f:
103  exec(f.read(), custom_namespace)
104  # Retrieve the class `formattername` from that namespace
105  if formattername not in custom_namespace:
106  raise ClassNotFound(f'no valid {formattername} class found in {filename}')
```

Sink Details

Sink: exec()
Enclosing Method: load_formatter_from_file()
File: .venv/lib/python3.13/site-packages/pip/_vendor/pygments/formatters/__init__.py:103
Taint Flags: FILE_SYSTEM

```
100  # This empty dict will contain the namespace for the exec'd file
101  custom_namespace = {}
102  with open(filename, 'rb') as f:
103  exec(f.read(), custom_namespace)
104  # Retrieve the class `formattername` from that namespace
105  if formattername not in custom_namespace:
106  raise ClassNotFound(f'no valid {formattername} class found in {filename}')
```

Package: .venv.lib.python3.13.site-packages.pip._vendor.pygments.lexers

.venv/lib/python3.13/site-packages/pip/_vendor/pygments/lexers/__init__.py, line 154 (Dynamic Code Evaluation: Code Injection) — High

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: file.read()

Dynamic Code Evaluation: Code Injection	High
Package: .venv.lib.python3.13.site-packages.pip._vendor.pygments.lexers	
.venv/lib/python3.13/site-packages/pip/_vendor/pygments/lexers/__init__.py, line 154 (Dynamic Code Evaluation: Code Injection)	High

From: .venv.lib.python3.13.site-packages.pip._vendor.pygments.lexers.load_lexer_from_file
File: .venv/lib/python3.13/site-packages/pip/_vendor/pygments/lexers/__init__.py:154

```
151  # This empty dict will contain the namespace for the exec'd file
152  custom_namespace = {}
153  with open(filename, 'rb') as f:
154  exec(f.read(), custom_namespace)
155  # Retrieve the class `lexername` from that namespace
156  if lexername not in custom_namespace:
157  raise ClassNotFound(f'no valid {lexername} class found in {filename}')
```

Sink Details

Sink: exec()
Enclosing Method: load_lexer_from_file()
File: .venv/lib/python3.13/site-packages/pip/_vendor/pygments/lexers/__init__.py:154
Taint Flags: FILE_SYSTEM

```
151  # This empty dict will contain the namespace for the exec'd file
152  custom_namespace = {}
153  with open(filename, 'rb') as f:
154  exec(f.read(), custom_namespace)
155  # Retrieve the class `lexername` from that namespace
156  if lexername not in custom_namespace:
157  raise ClassNotFound(f'no valid {lexername} class found in {filename}')
```

Hardcoded Domain in HTML (1 issue)

Abstract

包含其他網域的 script，這表示，這個網頁的安全性依賴另一個網域的安全性。

Explanation

包含另外一個網站中可執行的內容是有風險的。這樣會導致您網站的安全性與另一個網站息息相關。 **範例 1**：請考慮以下 `script` 標籤。

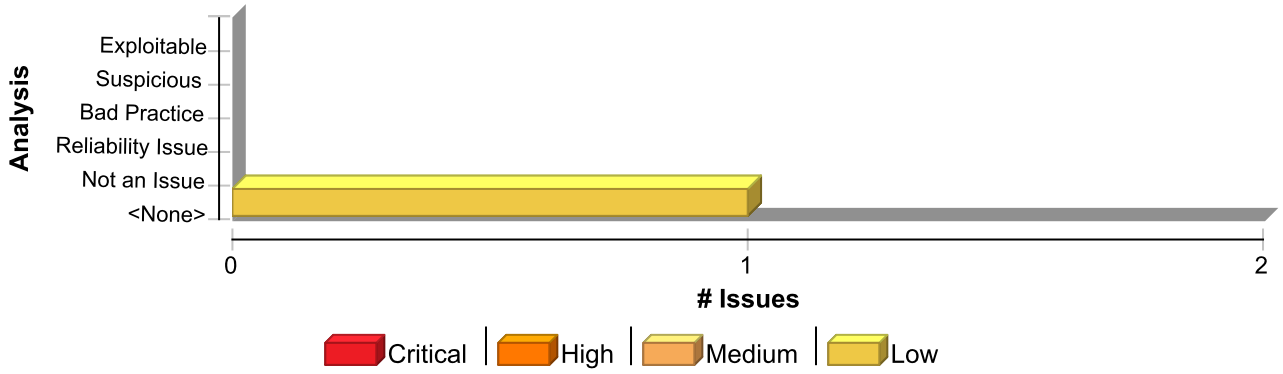
```
<script src="http://www.example.com/js/fancyWidget.js"></script>
```

如果這個標籤出現在 `www.example.com` 以外的網站上，則該網站依賴 `www.example.com` 提供正確且無惡意的程式碼。如果攻擊者能危害 `www.example.com`，他們就能修改 `fancyWidget.js` 的內容來破壞網站的安全性。例如，他們可以新增程式碼至 `fancyWidget.js` 來竊取使用者的機密資料。

Recommendation

請掌控您網頁呼叫的程式碼。請不要使用來自第三方網站的 script 或其他人工項目。

Issue Summary



Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Hardcoded Domain in HTML	1	0	0	1
Total	**1**	**0**	**0**	**1**

Hardcoded Domain in HTML	Low
Package: frontend.node_modules.sprintf-js.demo	
frontend/node_modules/sprintf-js/demo/angular.html, line 4 (Hardcoded Domain in HTML)	**Low**

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Content)

Sink Details

File: frontend/node_modules/sprintf-js/demo/angular.html:4
Taint Flags:

Hardcoded Domain in HTML	Low

Package: frontend.node_modules.sprintf-js.demo

frontend/node_modules/sprintf-js/demo/angular.html, line 4 (Hardcoded Domain in HTML)	Low

```
1 <!doctype html>
2 <html ng-app="app">
3 <head>
4   <script src="https://ajax.googleapis.com/ajax/libs/angularjs/1.3.0-rc.3/angular.min.js"></
script>
5   <script src="../src/sprintf.js"></script>
6   <script src="../src/angular-sprintf.js"></script>
7 </head>
```

Insecure Randomness (7 issues)

Abstract

標準的虛擬亂數產生器也無法抵擋加密攻擊。

Explanation

在安全性要求較高的環境中，將一個能夠產生可預測值的函數當作隨機來源使用時，會產生 Insecure Randomness 錯誤。 電腦是一種決定性的機器，因此不可能產生真正的隨機性。虛擬亂數產生器 (PRNG, Pseudorandom Number Generator) 近似於隨機演算，會從一個可以計算後續值的種子開始。 PRNG 包括兩種類型：統計式和加密式。統計式 PRNG 可提供有用的統計內容，但是它們的輸出很容易預測，導致複製數值串流很容易。因此，對於因安全性由產生數值決定而導致其不可預測的環境，其並不適用。加密式 PRNG 則會藉由產生更難以預測的輸出來解決這個問題。若要對數值進行加密保護，必須使攻擊者無法或難以區別產生的隨機數值和真實的隨機數值。一般來說，如果沒有指出某個 PRNG 演算法經過加密保護，那麼它很可能是統計式 PRNG，不應在安全性要求較高的環境中使用，否則會引發嚴重弱點，例如易猜的臨時密碼、容易預測的加密金鑰、Session Hijacking 以及 DNS 欺騙。 **範例 1：**以下程式碼使用統計式 PRNG，為購買後仍在有效期內的收據建立 URL。

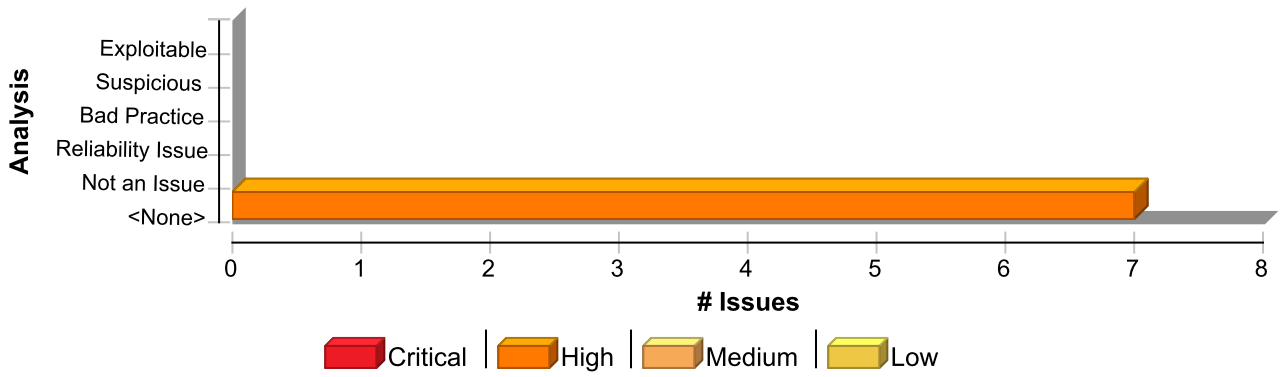
```
function genReceiptURL (baseURL){
  var randNum = Math.random();
  var receiptURL = baseURL + randNum + ".html";
  return receiptURL;
}
```

此程式碼使用 `Math.random()` 函數為其所產生的收據頁面產生「唯一」識別碼。由於 `Math.random()` 是統計式 PRNG，攻擊者很容易就能猜到其所產生的字串。雖然收據系統的基礎設計也存在錯誤，但是如果它使用一個不會產生可預測收據識別碼的亂數產生器 (例如加密式 PRNG)，那就會安全很多。

Recommendation

當不可預測性至關重要時 (例如大多數對安全性要求較高的環境都採用隨機性)，請使用加密型 PRNG。不管您選擇哪一種 PRNG，請務必使用擁有足夠複雜度 (entropy) 的值來進行演算。(像當前值的複雜度就很低，因此不宜使用。) 對於 Node.js 應用程式，請考慮使用 `crypto` 模組中的函數，以提供加密安全的隨機數。

Issue Summary



Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Insecure Randomness	7	0	0	7
Total	**7**	**0**	**0**	**7**

Insecure Randomness — High

Package: .src.app.features.cards.components

frontend/src/app/features/cards/components/live-preview.component.ts, line 161 (Insecure Randomness) — High

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: random
Enclosing Method: generateQRPattern()
File: frontend/src/app/features/cards/components/live-preview.component.ts:161
Taint Flags:

```
158  if (i < 7 && j < 7) pattern[i][j] = (i + j) % 2 === 0; // 左上角
159  else if (i < 7 && j >= size - 7) pattern[i][j] = (i + j) % 2 === 1; // 右上角
160  else if (i >= size - 7 && j < 7) pattern[i][j] = (i + j) % 2 === 0; // 左下角
161  else pattern[i][j] = Math.random() > 0.5; // 隨機填充
162  }
163  }
164
```

Package: .src.app.features.cards.services

frontend/src/app/features/cards/services/card-designer.service.ts, line 37 (Insecure Randomness) — High

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: random
Enclosing Method: createNewDesign()
File: frontend/src/app/features/cards/services/card-designer.service.ts:37
Taint Flags:

```
34  createNewDesign(name: string = '新圖卡'): CardDesign {
35  // 確保每次都創建全新的設計，避免重複使用舊資料
36  const timestamp = Date.now();
37  const randomId = Math.random().toString(36).substr(2, 9);
38
39  const newDesign = {
40  id: `new_${timestamp}_${randomId}`, // 更複雜的ID避免衝突
```

frontend/src/app/features/cards/services/card-designer.service.ts, line 339 (Insecure Randomness) — High

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Insecure Randomness — High

Package: .src.app.features.cards.services

frontend/src/app/features/cards/services/card-designer.service.ts, line 339 (Insecure Randomness) — High

Sink Details

Sink: FunctionPointerCall: random
Enclosing Method: generateId()
File: frontend/src/app/features/cards/services/card-designer.service.ts:339
Taint Flags:

```
336
337  // 工具方法
338  private generateId(): string {
339  return 'el_' + Math.random().toString(36).substr(2, 9);
340  }
341
342  private getNextZIndex(): number {
```

frontend/src/app/features/cards/services/collaboration.service.ts, line 29 (Insecure Randomness) — High

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: random
Enclosing Method: initializeCurrentUser()
File: frontend/src/app/features/cards/services/collaboration.service.ts:29
Taint Flags:

```
26  // 初始化當前用戶
27  private initializeCurrentUser(): void {
28  const colors = ['#ff6b6b', '#4ecdc4', '#45b7d1', '#f9ca24', '#f0932b', '#eb4d4b',
'#6c5ce7'];
29  const randomColor = colors[Math.floor(Math.random() * colors.length)];
30
31  const currentUser: CollaborationUser = {
32  id: this.generateUserId(),
```

frontend/src/app/features/cards/services/collaboration.service.ts, line 140 (Insecure Randomness) — High

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: random
Enclosing Method: generateUserId()

Insecure Randomness — High

Package: .src.app.features.cards.services

frontend/src/app/features/cards/services/collaboration.service.ts, line 140 (Insecure Randomness) — High

File: frontend/src/app/features/cards/services/collaboration.service.ts:140
Taint Flags:

```
137
138  // 工具方法
139  private generateUserId(): string {
140  return 'user_' + Math.random().toString(36).substr(2, 9);
141  }
142
143  // 獲取協作者顏色
```

Package: .src.app.features.deploy.components

frontend/src/app/features/deploy/components/deploy.component.ts, line 491 (Insecure Randomness) — High

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: random
Enclosing Method: lambda()
File: frontend/src/app/features/deploy/components/deploy.component.ts:491
Taint Flags:

```
488  let progress = 0;
489  let lastProgressUpdate = 0;
490  const progressInterval = setInterval(() => {
491  progress += Math.random() * 15 + 5; // 每次增加5-20%
492  if (progress > 90) progress = 90;
493
494  // 只在進度有明顯變化時才更新（至少5%差異）
```

Package: .src.app.shared.services

frontend/src/app/shared/services/notification.service.ts, line 32 (Insecure Randomness) — High

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: random
Enclosing Method: generateId()
File: frontend/src/app/shared/services/notification.service.ts:32

Insecure Randomness	High
Package: .src.app.shared.services	
frontend/src/app/shared/services/notification.service.ts, line 32 (Insecure Randomness)	**High**

Taint Flags:

```
29  }
30
31  private generateId(): string {
32  return Math.random().toString(36).substr(2, 9);
33  }
34
35  show(notification: Omit<NotificationMessage, 'id'>): string {
```

Insecure Transport (18 issues)

Abstract

呼叫使用不安全的通訊協定而非安全的通訊協定來與伺服器通訊。

Explanation

經由 HTTP、FTP 或 gopher 進行的所有通訊皆未經驗證且未加密。因此其安全性會降低，特別是在行動環境中，裝置經常使用 WiFi 連線連接到不安全且公開的無線網路。 **範例 1：** 以下範例會透過 HTTP 通訊協定來讀取資料 (而非使用 HTTPS)。

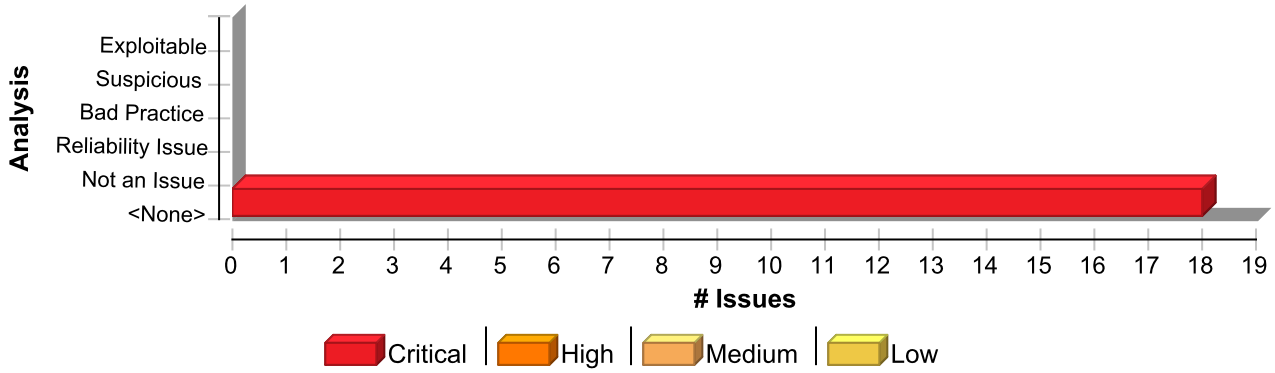
```
var http = require('http');
...
http.request(options, function(res){
  ...
});
...
```

傳入的 `http.IncomingMessage` 物件 `res` 安全性可能降低，因為它是透過未加密和未經驗證通道傳遞。

Recommendation

請儘可能使用安全的通訊協定 (例如 HTTPS) 與伺服器進行資料交換。

Issue Summary



Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Insecure Transport	18	0	0	18
Total	**18**	**0**	**0**	**18**

Insecure Transport	Critical
Package: .src.app.features.admin	
frontend/src/app/features/admin/database-schema.component.ts, line 306 (Insecure Transport)	**Critical**

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Insecure Transport — Critical

Package: .src.app.features.admin

frontend/src/app/features/admin/database-schema.component.ts, line 306 (Insecure Transport) — Critical

Sink Details

Sink: FunctionPointerCall: get
Enclosing Method: selectTable()
File: frontend/src/app/features/admin/database-schema.component.ts:306
Taint Flags:

```
303  this.columns = cols;
304  });
305  this.loadingRows = true;
306  this.http.get<any[]>(`/api/database/tables/${table}/rows`).subscribe(rows => {
307  this.rows = rows;
308  this.loadingRows = false;
309  }, _ => this.loadingRows = false);
```

frontend/src/app/features/admin/database-schema.component.ts, line 289 (Insecure Transport) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: get
Enclosing Method: ngOnInit()
File: frontend/src/app/features/admin/database-schema.component.ts:289
Taint Flags:

```
286  constructor(private http: HttpClient) {}
287
288  ngOnInit() {
289  this.http.get<string[]>('/api/database/tables').subscribe(tables => {
290  this.tables = tables;
291  if (tables.length > 0) {
292  this.selectTable(tables[0]);
```

frontend/src/app/features/admin/database-schema.component.ts, line 302 (Insecure Transport) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: get
Enclosing Method: selectTable()
File: frontend/src/app/features/admin/database-schema.component.ts:302

Insecure Transport — Critical

Package: .src.app.features.admin

frontend/src/app/features/admin/database-schema.component.ts, line 302 (Insecure Transport) — Critical

Taint Flags:

```
299  this.columns = [];
300  this.rows = [];
301  this.pageIndex = 0;
302  this.http.get<any[]>(`/api/database/tables/${table}/columns`).subscribe(cols => {
303  this.columns = cols;
304  });
305  this.loadingRows = true;
```

Package: .src.app.features.cards.services

frontend/src/app/features/cards/services/custom-color-api.service.ts, line 31 (Insecure Transport) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: get
Enclosing Method: getCustomColors()
File: frontend/src/app/features/cards/services/custom-color-api.service.ts:31
Taint Flags:

```
28  constructor(private http: HttpClient) {}
29
30  getCustomColors(): Observable<CustomColor[]> {
31  return this.http.get<CustomColor[]>(this.apiUrl);
32  }
33
34  getCustomColor(id: number): Observable<CustomColor> {
```

frontend/src/app/features/cards/services/card-api.service.ts, line 45 (Insecure Transport) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: get
Enclosing Method: getCard()
File: frontend/src/app/features/cards/services/card-api.service.ts:45
Taint Flags:

```
42
```

Insecure Transport — Critical

Package: .src.app.features.cards.services

frontend/src/app/features/cards/services/card-api.service.ts, line 45 (Insecure Transport) — Critical

```
43  // 根據 ID 獲取桌牌
44  getCard(id: number): Observable<Card> {
45  return this.http.get<Card>(`${this.baseUrl}/${id}`);
46  }
47
48  // 創建新桌牌
```

frontend/src/app/features/cards/services/template-api.service.ts, line 63 (Insecure Transport) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: get
Enclosing Method: getTemplates()
File: frontend/src/app/features/cards/services/template-api.service.ts:63
Taint Flags:

```
60  if (category) {
61  params.category = category;
62  }
63  return this.http.get<TemplateListItem[]>(this.baseUrl, { params });
64  }
65
66  // 根據 ID 獲取樣板
```

frontend/src/app/features/cards/services/custom-color-api.service.ts, line 35 (Insecure Transport) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: get
Enclosing Method: getCustomColor()
File: frontend/src/app/features/cards/services/custom-color-api.service.ts:35
Taint Flags:

```
32  }
33
34  getCustomColor(id: number): Observable<CustomColor> {
35  return this.http.get<CustomColor>(`${this.apiUrl}/${id}`);
36  }
```

Insecure Transport — Critical

Package: .src.app.features.cards.services

frontend/src/app/features/cards/services/custom-color-api.service.ts, line 35 (Insecure Transport) — Critical

```
37
38  createCustomColor(data: CreateCustomColorDto): Observable<CustomColor> {
```

frontend/src/app/features/cards/services/template-api.service.ts, line 68 (Insecure Transport) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: get
Enclosing Method: getTemplate()
File: frontend/src/app/features/cards/services/template-api.service.ts:68
Taint Flags:

```
65
66  // 根據 ID 獲取樣板
67  getTemplate(id: number): Observable<Template> {
68  return this.http.get<Template>(`${this.baseUrl}/${id}`);
69  }
70
71  // 創建新樣板
```

frontend/src/app/features/cards/services/element-image-api.service.ts, line 52 (Insecure Transport) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: get
Enclosing Method: getElementById()
File: frontend/src/app/features/cards/services/element-image-api.service.ts:52
Taint Flags:

```
49  }
50
51  getElementById(id: number): Observable<ElementImage> {
52  return this.http.get<ElementImage>(`${this.baseUrl}/${id}`);
53  }
54
55  createElement(elementImage: CreateElementImageDto): Observable<ElementImage> {
```

Insecure Transport — Critical

Package: .src.app.features.cards.services

frontend/src/app/features/cards/services/background-api.service.ts, line 47 (Insecure Transport) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: get
Enclosing Method: getBackgroundImage()
File: frontend/src/app/features/cards/services/background-api.service.ts:47
Taint Flags:

```
44
45  // 根據 ID 獲取背景圖片
46  getBackgroundImage(id: number): Observable<BackgroundImage> {
47  return this.http.get<BackgroundImage>(`${this.baseUrl}/${id}`);
48  }
49
50  // 創建新背景圖片
```

frontend/src/app/features/cards/services/background-api.service.ts, line 42 (Insecure Transport) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: get
Enclosing Method: getBackgroundImages()
File: frontend/src/app/features/cards/services/background-api.service.ts:42
Taint Flags:

```
39  if (category) {
40  params.category = category;
41  }
42  return this.http.get<BackgroundImage[]>(this.baseUrl, { params });
43  }
44
45  // 根據 ID 獲取背景圖片
```

frontend/src/app/features/cards/services/element-image-api.service.ts, line 48 (Insecure Transport) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Insecure Transport — Critical

Package: .src.app.features.cards.services

frontend/src/app/features/cards/services/element-image-api.service.ts, line 48 (Insecure Transport) — Critical

Sink Details

Sink: FunctionPointerCall: get
Enclosing Method: getElementImages()
File: frontend/src/app/features/cards/services/element-image-api.service.ts:48
Taint Flags:

```
45
46  getElementImages(category?: string): Observable<ElementImage[]> {
47  const url = category ? `${this.baseUrl}?category=${category}` : this.baseUrl;
48  return this.http.get<ElementImage[]>(url);
49  }
50
51  getElementById(id: number): Observable<ElementImage> {
```

frontend/src/app/features/cards/services/card-api.service.ts, line 40 (Insecure Transport) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: get
Enclosing Method: getCards()
File: frontend/src/app/features/cards/services/card-api.service.ts:40
Taint Flags:

```
37
38  // 獲取所有桌牌
39  getCards(): Observable<Card[]> {
40  return this.http.get<Card[]>(this.baseUrl);
41  }
42
43  // 根據 ID 獲取桌牌
```

Package: .src.app.features.deploy.services

frontend/src/app/features/deploy/services/deploy.service.ts, line 71 (Insecure Transport) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: get
Enclosing Method: getDevices()

Insecure Transport — Critical

Package: .src.app.features.deploy.services

frontend/src/app/features/deploy/services/deploy.service.ts, line 71 (Insecure Transport) — Critical

File: frontend/src/app/features/deploy/services/deploy.service.ts:71
Taint Flags:

```
68  }
69
70  getDevices(): Observable<Device[]> {
71  return this.http.get<Device[]>(`${this.apiUrl}/bluetooth/devices`);
72  }
73
74  updateDevice(id: number, device: UpdateDevice): Observable<void> {
```

frontend/src/app/features/deploy/services/deploy.service.ts, line 32 (Insecure Transport) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: get
Enclosing Method: getGroup()
File: frontend/src/app/features/deploy/services/deploy.service.ts:32
Taint Flags:

```
29  }
30
31  getGroup(id: number): Observable<GroupDetail> {
32  return this.http.get<GroupDetail>(`${this.apiUrl}/groups/${id}`);
33  }
34
35  createGroup(group: CreateGroup): Observable<Group> {
```

frontend/src/app/features/deploy/services/deploy.service.ts, line 58 (Insecure Transport) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: get
Enclosing Method: getCards()
File: frontend/src/app/features/deploy/services/deploy.service.ts:58
Taint Flags:

```
55
56  // Cards API
```

Insecure Transport — Critical

Package: .src.app.features.deploy.services

frontend/src/app/features/deploy/services/deploy.service.ts, line 58 (Insecure Transport) — Critical

```
57  getCards(): Observable<Card[]> {
58  return this.http.get<Card[]>(`${this.apiUrl}/cards`);
59  }
60
61  // Bluetooth API
```

frontend/src/app/features/deploy/services/deploy.service.ts, line 28 (Insecure Transport) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: get
Enclosing Method: getGroups()
File: frontend/src/app/features/deploy/services/deploy.service.ts:28
Taint Flags:

```
25
26  // Groups API
27  getGroups(): Observable<Group[]> {
28  return this.http.get<Group[]>(`${this.apiUrl}/groups`);
29  }
30
31  getGroup(id: number): Observable<GroupDetail> {
```

frontend/src/app/features/deploy/services/deploy.service.ts, line 63 (Insecure Transport) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: get
Enclosing Method: scanBluetoothDevices()
File: frontend/src/app/features/deploy/services/deploy.service.ts:63
Taint Flags:

```
60
61  // Bluetooth API
62  scanBluetoothDevices(): Observable<BluetoothDevice[]> {
63  return this.http.get<BluetoothDevice[]>(`${this.apiUrl}/bluetooth/scan`);
64  }
65
```

Insecure Transport	Critical
Package: .src.app.features.deploy.services	
frontend/src/app/features/deploy/services/deploy.service.ts, line 63 (Insecure Transport)	**Critical**

```
66  connectDevice(device: ConnectDevice): Observable<Device> {
```

Insecure Transport: External Link (3 issues)

Abstract

檔案透過未加密的通道連結到第三方網站。

Explanation

請確保網頁上的超連結僅連結到安全位置，以防止瀏覽網站時發生任何使用者洩漏資訊。即使連結從不安全的通訊協定 (例如 HTTP) 重新導向到安全的通訊協定 (例如 HTTPS)，透過未加密通道的初始連線也會讓攻擊者能夠執行 Man-in-the-Middle (MiTM) 攻擊。如此一來，攻擊者就能夠控制頁面，即產生的登陸頁面。 **範例 1：**請考慮以下超連結：

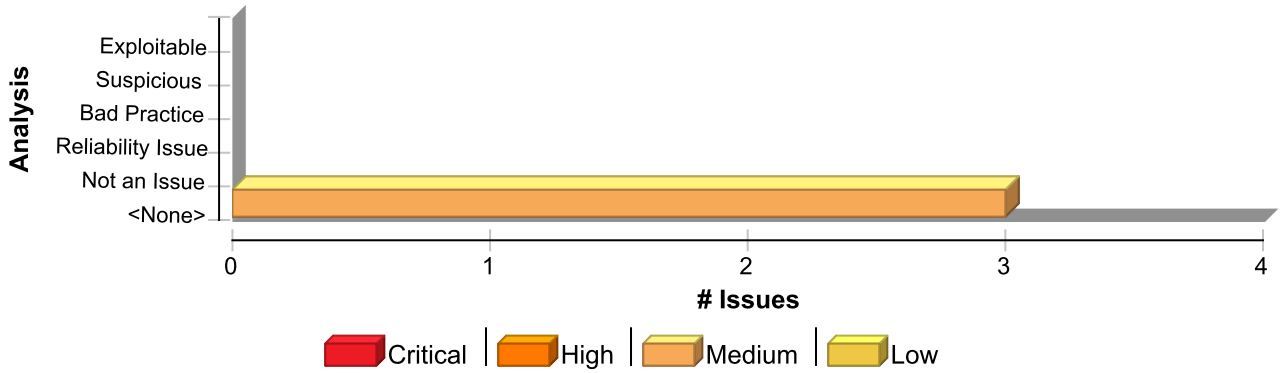
```
<a href="http://www.example.com/index.html"/>
```

如果攻擊者正在監聽使用者與伺服器之間的網路流量，就可以模擬或操縱 `www.example.com` 來載入自己的網頁。第三方網站的連結最初可能不被認為對安全很重要，但是對使用者來說，任何洩漏都可能顯示為來自您網頁上的連結，因此會降低使用者對使用您平台的信任度。

Recommendation

請控制您網站上連結的網頁，並儘可能確保始終透過安全的通訊協定載入連結。如果目標伺服器需要使用不安全的通訊協定，請提供警語，告知使用者按一下連結會有額外風險。請儘可能不要使用來自第三方網站的 script 或其他人工項目。

Issue Summary



Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Insecure Transport: External Link	3	0	0	3
Total	**3**	**0**	**0**	**3**

Insecure Transport: External Link	**Medium**
Package: node_modules.unique-filename.coverage	
node_modules/unique-filename/coverage/index.html, line 61 (Insecure Transport: External Link)	**Medium**

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Content)

Insecure Transport: External Link — Medium

Package: node_modules.unique-filename.coverage

node_modules/unique-filename/coverage/index.html, line 61 (Insecure Transport: External Link) — Medium

Sink Details

File: node_modules/unique-filename/coverage/index.html:61
Taint Flags:

```
58 </div>
59 </div>
60 <div class="footer">
61  <div class="meta">Generated by <a href="http://istanbul-js.org/" target="_blank">istanbul</a> at Thu Dec 03 2015 15:00:03 GMT-0800 (PST)</div>
62 </div>
63 <script src="prettify.js"></script>
64 <script>
```

Package: node_modules.unique-filename.coverage.__root__

node_modules/unique-filename/coverage/__root__/index.js.html, line 57 (Insecure Transport: External Link) — Medium

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Content)

Sink Details

File: node_modules/unique-filename/coverage/__root__/index.js.html:57
Taint Flags:

```
54
55 </div>
56 <div class="footer">
57  <div class="meta">Generated by <a href="http://istanbul-js.org/" target="_blank">istanbul</a> at Thu Dec 03 2015 15:00:03 GMT-0800 (PST)</div>
58 </div>
59 <script src="../prettify.js"></script>
60 <script>
```

node_modules/unique-filename/coverage/__root__/index.html, line 61 (Insecure Transport: External Link) — Medium

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Content)

Sink Details

File: node_modules/unique-filename/coverage/__root__/index.html:61
Taint Flags:

```
58 </div>
```

Insecure Transport: External Link	Medium
Package: node_modules.unique-filename.coverage.__root__	
node_modules/unique-filename/coverage/__root__/index.html, line 61 (Insecure Transport: External Link)	Medium

```
59 </div>
60 <div class="footer">
61  <div class="meta">Generated by <a href="http://istanbul-js.org/" target="_blank">istanbul</a> at Thu Dec 03 2015 15:00:03 GMT-0800 (PST)</div>
62 </div>
63 <script src="../prettify.js"></script>
64 <script>
```

Key Management: Hardcoded Encryption Key (7 issues)

Abstract

硬式編碼加密金鑰會導致無法輕易修正的安全性問題。

Explanation

切勿將加密金鑰硬式編碼，因為不僅所有專案開發人員都能看到加密金鑰，也會讓修正問題的工作變得相當困難。程式碼進入生產階段後，只有修補軟體才能變更加密金鑰。如果加密金鑰保護的帳戶遭到入侵，系統的所有者必須在安全性和系統可用性之間做出選擇。 **範例 1：**以下範例顯示 .pem 檔案內的加密金鑰：

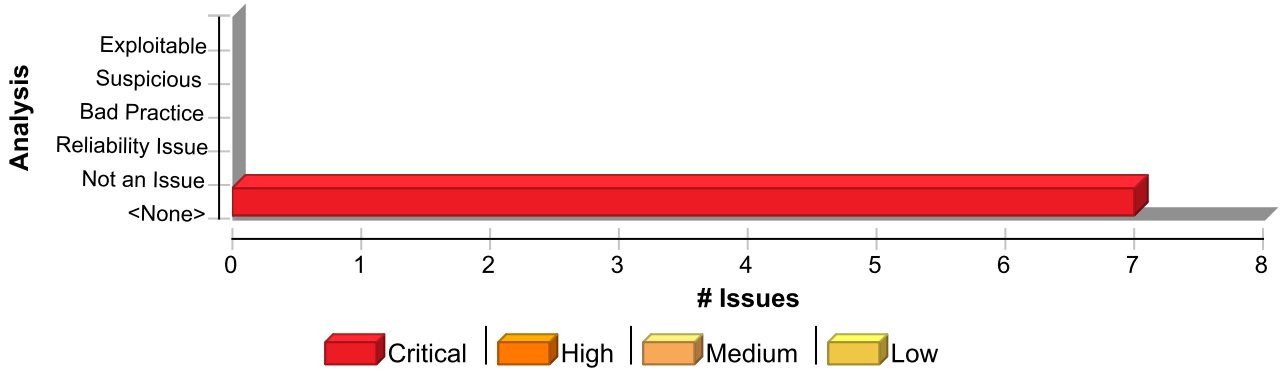
```
...
-----BEGIN RSA PRIVATE KEY-----
MIICXwIBAAKBgQCtVacMo+w+TFOm0p8MlBWvwXtVRpF28V+o0RNPx5x/1TJTlKEl
...
DiJPJY2LNBQ7jS685mb6650JdvH8uQl6oeJ/aUmq63o2zOw=
-----END RSA PRIVATE KEY-----
...
```

任何有程式碼存取權的人都能夠看到加密金鑰。發佈應用程式之後，除非修補此程式，否則無法變更加密金鑰。若員工有此資訊的存取權，可能會使用此資訊來進入並破壞系統。任何攻擊者只要取得權限存取應用程式可執行檔案，就可以擷取加密金鑰值。

Recommendation

切勿將加密金鑰簽入至您的來源控制系統，也不要對它們進行硬式編碼。務必模糊化及管理外部來源中的加密金鑰。將加密金鑰以純文字方式儲存於系統的任一處，會讓任何有足夠權限的人讀取加密金鑰，並可能誤用加密金鑰。

Issue Summary



Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Key Management: Hardcoded Encryption Key	7	0	0	7
Total	**7**	**0**	**0**	**7**

Key Management: Hardcoded Encryption Key	**Critical**
Package: frontend.node_modules.npm-registry-fetch	
frontend/node_modules/npm-registry-fetch/README.md, line 322 (Key Management: Hardcoded Encryption Key)	**Critical**
Issue Details	

Key Management: Hardcoded Encryption Key — Critical

Package: frontend.node_modules.npm-registry-fetch

frontend/node_modules/npm-registry-fetch/README.md, line 322 (Key Management: Hardcoded Encryption Key) — Critical

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Sink Details

File: frontend/node_modules/npm-registry-fetch/README.md:322
Taint Flags:

```
319
320 ```
321 {
322   key: '-----BEGIN PRIVATE KEY-----\nXXXX\nXXXX\n-----END PRIVATE KEY-----'
323 }
324 ```
325
```

Package: frontend.node_modules.selfsigned

frontend/node_modules/selfsigned/README.md, line 30 (Key Management: Hardcoded Encryption Key) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Sink Details

File: frontend/node_modules/selfsigned/README.md:30
Taint Flags:

```
27
28 ```js
29 {
30   private: '-----BEGIN RSA PRIVATE KEY-----\r\nMIICXAIBAAKBgQCBFMXMYS/
+RZz6+qzv+xeqXPdjw4YKZC4y3dPhSwgEwkecrCTX\r\nsR6boue+1MjIqPqWggXZnotIGldfEN0kn0Jbh2vMTrTx6YwqQ8t
lx6LhpIKAgY0m5WIuaKrW6mvLXQIDAQAB\r\nAoGAU6ODGxAqSecPdayyG/
ml9vSwNAuAMgGB0eHcpZG5i2PbhRAh+0TAIXaoFQXJ\r\naAPeA2ISqlTJyRmQXYAO2uj61FzeyDzYCf0z3+yZEVz3cO7jB5
jioc8F0EAzZ+lkC/
XuVJdwKHDmwt2qvJO+ECQQD+dvo1g3Sz9xGw\r\n21n+fDG5i4128+Qh+JPgh5AeLuXSofc1HMHaOXcC6Wu/
Cloh7QAD934b7W0A7VoD\r\ndLd/
JLyFAkEAgdwjryyvdhy69e516IrPB3b+m4rggtntBlZREMrk9tOzeIucVO3W\r\ntKI3FHm6JebN2gVcG+rZ+FaDPo+ifJkW
Bi53CEQqg7Gq5+F6H33qcHmBEN8LQTngN9rY+vZh0CQBg0\r\nqJImii5B/
LeK03+dICoMDDmCEYdSh9P+ku3GZBd+Lp3xqBpMmxDgi9PNPN2DwCs7\r\nhIfPpwGbXqtyqp7/
CkECQB4OdY+2FbCciI473eQkTu310RMf8jElU63iwnx4R/XN\r\n/mgqN589OfF4SS0U/MoRzYk9jF9IAJN1Mi/
571T+nw4=\r\n-----END RSA PRIVATE KEY-----\r\n',
31   public: '-----BEGIN PUBLIC KEY-----\r\nMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCBFMXMYS/
+RZz6+qzv+xeqXPdj\r\nw4YKZC4y3dPhSwgEwkecrCTXsR6boue+1MjIqPqWggXZnotIGldfEN0kn0Jbh2vM\r\nTrTx6Yw
lx6LhpIKA\r\ngY0m5WIuaKrW6mvLXQIDAQAB\r\n-----END PUBLIC KEY-----\r\n',
32   cert: '-----BEGIN CERTIFICATE-----
\r\nMIICjTCCAfagAwIBAgIBATANBgkqhkiG9w0BAQUFADBpMRQwEgYDVQQDEwtleGFt\r\ncGxlLm9yZzELMAkGA1UEBhMC
kWc+vqs7/
sXqlz3Y8OGCmQuMt3T4UsI\r\nBMJHnKwk17Eem6LnvtTIyKj6loIF2Z6LSBpXXxDdJJ9CW4drzE608emMKkPLXHgT\r\n6M
```

Key Management: Hardcoded Encryption Key — Critical

Package: frontend.node_modules.selfsigned

frontend/node_modules/selfsigned/README.md, line 30 (Key Management: Hardcoded Encryption Key) — Critical

```
zALBgNVHQ8EBAMCAvQwJgYDVR0RBB8w\r\nHYYbaHR0cDovL2V4YW1wbGUub3JnL3dlYmlkI211MA0GCSqGSIb3DQEBBQUAA
+kixblGaOkoDROPsWepUpL6kMDUtbAM\r\n4uXTyFkvlUQSaQkhNgOY5w/
BRIAkCIu6u4D4XcjlCdwFq6vcKMEuWTHMAlBWFla3\r\nXJZAPO10PHuDen7JeMOUf1Re7lRFtwfRGAvVYmrvYFKv\r\n---
END CERTIFICATE-----\r\n'
33 }
```

frontend/node_modules/selfsigned/README.md, line 68 (Key Management: Hardcoded Encryption Key) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Sink Details

File: frontend/node_modules/selfsigned/README.md:68
Taint Flags:

```
65 Will return the following like this:
66
67 ```js
68 { private: '-----BEGIN RSA PRIVATE KEY-----\r\nMIICXQIBAAKBgQDLg/
kS4dCPVu96sbK6MQuUPmhqnF8SeBXVHH18h+0BTj7HqnrA\r\nA75hNVIiSLTChvpzQ0qi2Ju7O2ESUOdx7cvGiftGuZLiI8
QSDyxAH/
uJzfr6gOJOD5nT\r\n5gZYblC+CCMDkgDUpro6oATNyeRNoU3GOQJBANdaW26DWZ1WqV9hCpcGAxdJrT30\r\nuVASq66w93
pjz2ugoD2wrk+sYXwoujj/
NH5mnAaOhAsw5AJ0pcLfpe\r\nw6QHtmD+68ouUaJbIFkCQQDeu0AXAp6Kbk6570i2DpGUSnkRdGCGS+3ekqqJUpE7\r\nfV
wVkrkjiR\r\n-----END RSA PRIVATE KEY-----\r\n',
69  public: '-----BEGIN PUBLIC KEY-----\r\nMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDLg/
kS4dCPVu96sbK6MQuUPmhq\r\nnF8SeBXVHH18h+0BTj7HqnrAA75hNVIiSLTChvpzQ0qi2Ju7O2ESUOdx7cvGiftG\r\nuZ
END PUBLIC KEY-----\r\n',
70  cert: '-----BEGIN CERTIFICATE-----
\r\nMIIClTCCAf6gAwIBAgIJdMZqoEeGMVYKMA0GCSqGSIb3DQEBBQUAMGkxFDASBgNV\r\nBAMTC2V4YW1wbGUub3JnMQsw
kS4dCPVu96sbK6MQuUPmhqnF8S\r\neBXVHH18h+0BTj7HqnrAA75hNVIiSLTChvpzQ0qi2Ju7O2ESUOdx7cvGiftGuZLi\r
MAsGA1UdDwQEAwIC9DAm\r\nBgNVHREEHzAdhhtodHRwOi8vZXhhbXBsZS5vcmcvd2ViaWQjbWUwDQYJKoZIhvcN\r\nAQEF
riWylW4CdOK1hOyJZ+VRBWeYLKfX\r\ni///V+tqRvLlYY5x5DnrjXbDjBy0CZuN/J772/
Srgp7Nl5cn92zynMJK1q4MEEs3\r\nAE/FO85R0HbGEp+IrwUwDOLR6omBFVdh1EUOTcQU2jLZNbWvLDiWbDo=\r\n-----
END CERTIFICATE-----\r\n',
71  clientprivate: '-----BEGIN RSA PRIVATE KEY-----
\r\nMIICWwIBAAKBgQDjR5FrrdZ1jirqkx3KMPnGjrcObj/
vmztWTEZ1kX6gTskQugJU\r\noxktzwDZza4jYODC6Ud2jouFLWeAi5BDSAeLwAQb951qVD9zVsmQ+63V/
mvSJUoj\r\nigwj7YjcxyReJ17F0YgjceqrkZaPM8YRo8h1fj1JdPc4ZOUgA5ASZ0h2ewIDAQAB\r\nAoGAfB5DbjibG8ut6
jE+hDPA+wnsMg+TgGARECQQDzlc+5WA9JsG9f\r\nwNRzhMGRxDP4QLmL0iLWupF4BMP/
k4OLMjDtzWl725WJ4FjCzML7mSmkWWe/
P8f5\r\nwrbR+e8lAkEA7t0CEsiIw8BE55YMuGIz5xI0QDnuwNWmCEmq6+ZziW3L+EuAr1S4\r\nDORqBYm5DuRvBWkWE9Sl
sA56hLoazrV90ORxC73lfKNfcb\r\nZF2bnoGPGEMuQ1lG3wJAPnHysm3DgbSHZQiXWMjF4YDRRV2AeOqX1fmlSeMErwdj\r
END RSA PRIVATE KEY-----\r\n',
```

frontend/node_modules/selfsigned/README.md, line 71 (Key Management: Hardcoded Encryption Key) — Critical

Issue Details

Key Management: Hardcoded Encryption Key — Critical

Package: frontend.node_modules.selfsigned

frontend/node_modules/selfsigned/README.md, line 71 (Key Management: Hardcoded Encryption Key) — Critical

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Sink Details

File: frontend/node_modules/selfsigned/README.md:71
Taint Flags:

```
68 { private: '-----BEGIN RSA PRIVATE KEY-----\r\nMIICXQIBAAKBgQDLg/
kS4dCPVu96sbK6MQuUPmhqnF8SeBXVHH18h+0BTj7HqnrA\r\nA75hNVIiSLTChvpzQ0qi2Ju7O2ESUOdx7cvGiftGuZLiI8
QSDyxAH/
uJzfr6gOJOD5nT\r\n5gZYblC+CCMDkgDUpro6oATNyeRNoU3GOQJBANdaW26DWZ1WqV9hCpcGAxdJrT30\r\nuVASq66w93
pjz2ugoD2wrk+sYXwoujj/
NH5mnAaOhAsw5AJ0pcLfpe\r\nw6QHtmD+68ouUaJbIFkCQQDeu0AXAp6Kbk6570i2DpGUSnkRdGCGS+3ekqqJUpE7\r\nfV
wVkrkjiR\r\n-----END RSA PRIVATE KEY-----\r\n',
69  public: '-----BEGIN PUBLIC KEY-----\r\nMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDLg/
kS4dCPVu96sbK6MQuUPmhq\r\nnF8SeBXVHH18h+0BTj7HqnrAA75hNVIiSLTChvpzQ0qi2Ju7O2ESUOdx7cvGiftG\r\nuZ
END PUBLIC KEY-----\r\n',
70  cert: '-----BEGIN CERTIFICATE-----
\r\nMIIClTCCAf6gAwIBAgIJdMZqoEeGMVYKMA0GCSqGSIb3DQEBBQUAMGkxFDASBgNV\r\nBAMTC2V4YW1wbGUub3JnMQsw
kS4dCPVu96sbK6MQuUPmhqnF8S\r\neBXVHH18h+0BTj7HqnrAA75hNVIiSLTChvpzQ0qi2Ju7O2ESUOdx7cvGiftGuZLi\r
MAsGA1UdDwQEAwIC9DAm\r\nBgNVHREEHzAdhhtodHRwOi8vZXhhbXBsZS5vcmcvd2ViaWQjbWUwDQYJKoZIhvcN\r\nAQEF
riWylW4CdOK1hOyJZ+VRBWeYLKfX\r\ni///V+tqRvLlYY5x5DnrjXbDjBy0CZuN/J772/
Srgp7Nl5cn92zynMJK1q4MEEs3\r\nAE/FO85R0HbGEp+IrwUwDOLR6omBFVdh1EUOTcQU2jLZNbWvLDiWbDo=\r\n-----
END CERTIFICATE-----\r\n',
71  clientprivate: '-----BEGIN RSA PRIVATE KEY-----
\r\nMIICWwIBAAKBgQDjR5FrrdZ1jirqkx3KMPnGjrcObj/
vmztWTEZ1kX6gTskQugJU\r\noxktzwDZza4jYODC6Ud2jouFLWeAi5BDSAeLwAQb951qVD9zVsmQ+63V/
mvSJUoj\r\nigwj7YjcxyReJ17F0YgjceqrkZaPM8YRo8h1fj1JdPc4ZOUgA5ASZ0h2ewIDAQAB\r\nAoGAfB5DbjibG8ut6
jE+hDPA+wnsMg+TgGARECQQDzlc+5WA9JsG9f\r\nwNRzhMGRxDP4QLmL0iLWupF4BMP/
k4OLMjDtzWl725WJ4FjCzML7mSmkWWe/
P8f5\r\nwrbR+e8lAkEA7t0CEsiIw8BE55YMuGIz5xI0QDnuwNWmCEmq6+ZziW3L+EuAr1S4\r\nDORqBYm5DuRvBWkWE9Sl
sA56hLoazrV90ORxC73lfKNfcb\r\nZF2bnoGPGEMuQ1lG3wJAPnHysm3DgbSHZQiXWMjF4YDRRV2AeOqX1fmlSeMErwdj\r
END RSA PRIVATE KEY-----\r\n',
72  clientpublic: '-----BEGIN PUBLIC KEY-----
\r\nMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDjR5FrrdZ1jirqkx3KMPnGjrcO\r\nbj/
vmztWTEZ1kX6gTskQugJUoxktzwDZza4jYODC6Ud2jouFLWeAi5BDSAeLwAQb\r\n951qVD9zVsmQ+63V/
mvSJUojigwj7YjcxyReJ17F0YgjceqrkZaPM8YRo8h1fj1J\r\ndPc4ZOUgA5ASZ0h2ewIDAQAB\r\n-----END PUBLIC
KEY-----\r\n',
73  clientcert: '-----BEGIN CERTIFICATE-----
\r\nMIICSzCCAbSgAwIBAgIBAjANBgkqhkiG9w0BAQUFADBpMRQwEgYDVQQDEwtleGFt\r\ncGxlLm9yZzELMAkGA1UEBhMC
vmztW\r\nTEZ1kX6gTskQugJUoxktzwDZza4jYODC6Ud2jouFLWeAi5BDSAeLwAQb951qVD9z\r\nVsmQ+63V/
mvSJUojigwj7YjcxyReJ17F0YgjceqrkZaPM8YRo8h1fj1JdPc4ZOUg\r\nA5ASZ0h2ewIDAQABMA0GCSqGSIb3DQEBBQUAA
ezePELKbyRggUvVgN\r\nB0XdIQkpR9X4mPdtFYkMiWKNVYKd79r0kolprgFPryhT3jsICIOnwE1Ur23Q+Fk2\r\nnnizRS0H
END CERTIFICATE-----\r\n' }
74 ```
```

frontend/node_modules/selfsigned/README.md, line 55 (Key Management: Hardcoded Encryption Key) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Key Management: Hardcoded Encryption Key — Critical

Package: frontend.node_modules.selfsigned

frontend/node_modules/selfsigned/README.md, line 55 (Key Management: Hardcoded Encryption Key) — Critical

Sink Details

File: frontend/node_modules/selfsigned/README.md:55
Taint Flags:

```
52 });
53 ```
54
55 > You can avoid key pair generation specifying your own keys (`{ keyPair: { publicKey:
'-----BEGIN PUBLIC KEY-----...', privateKey: '-----BEGIN RSA PRIVATE KEY-----...' }`)
56
57 ### Generate Client Certificates
58
```

Package: frontend.node_modules.spdy.test

frontend/node_modules/spdy/test/fixtures.js, line 9 (Key Management: Hardcoded Encryption Key) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Sink Details

File: frontend/node_modules/spdy/test/fixtures.js:9
Taint Flags:

```
6 exports.port = 23433
7
8 exports.keys = {
9  key: '-----BEGIN RSA PRIVATE KEY-----\n' +
10  'MIIEogIBAAKCAQEA1ARXSoyizYSnHDYickxX4x2UG/8uNWnQWKlWR97NAwRsspN6\n' +
11  'aFF1+LnyN9bvLNnhxIowcYy68+LpZ7pYAQgBZSyAhnF1S4qz2w/rxH4CNn96B/je\n' +
12  'vQGo3e8vIQ8ChhfuYvGAtTEYJzW8aRoxWSPcukZZdxPQ1Wgbhd9DSXhgkUnkEEET\n' +
```

Package: node_modules.node-gyp.test.fixtures

node_modules/node-gyp/test/fixtures/server.key, line 1 (Key Management: Hardcoded Encryption Key) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Sink Details

File: node_modules/node-gyp/test/fixtures/server.key:1
Taint Flags:

Key Management: Hardcoded Encryption Key	Critical

Package: node_modules.node-gyp.test.fixtures

node_modules/node-gyp/test/fixtures/server.key, line 1 (Key Management: Hardcoded Encryption Key)	Critical

```
1 -----BEGIN RSA PRIVATE KEY-----
2 MIIEowIBAAKCAQEA6S1E2WchgmbJYqCnpN7310ZgHjIOqeJe6MpSue2u6z6mTNd5
3 izgvQNaANmn3xLFCS5zsuZaTvdPYPkcmSQzb1YcZSUYnAxZifjYARc6kb5GSBl3q
4 +O70ELyFrimXfZ4JI+bdIG9KiHY17DlvZZZj/csGYVWWg0mkeH3O5LPX6/DXQVh/
5
6 undefined
7 undefined
```

Key Management: Null Encryption Key (1 issue)

Abstract

Null 加密金鑰會導致無法輕易修正的安全性問題。

Explanation

將 None 指定給加密金鑰變數是不當的做法，因為會讓敏感與加密資訊暴露給攻擊者。使用 null 加密金鑰不僅會明顯降低良好的加密演算法提供的保護，還會使修正問題變得極為困難。產生違反規則的程式碼以後，除非修補軟體，否則無法變更 null 加密金鑰。如果 null 加密金鑰保護的帳戶出現問題，系統的所有者將必須在安全性和可行性之間做出選擇。 **範例 1：**以下程式碼會將加密金鑰變數初始化為 null。

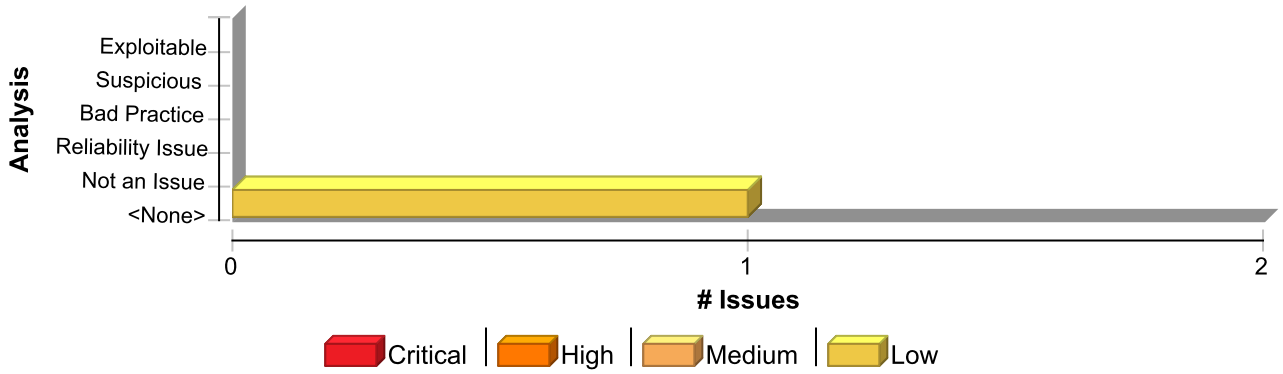
```
...
from Crypto.Ciphers import AES
cipher = AES.new(None, AES.MODE_CFB, iv)
msg = iv + cipher.encrypt(b'Attack at dawn')
...
```

擁有程式碼存取權的任何人均可以判斷是否使用 null 加密金鑰，且採用甚至是基本破解技術的任何人都很有可能成功解密任何加密的資料。程式發佈後，除非修補軟體，否則無法變更 null 加密金鑰。若員工有此資訊的存取權，則可能會使用此資訊來進入並破壞系統。即使攻擊者僅有應用程式可執行檔的存取權，他們也可以擷取 null 加密金鑰的使用證據。

Recommendation

請勿使用 null 加密金鑰，且通常應將加密金鑰模糊化，並於外部來源中進行管理。將加密金鑰 (null 或其他) 以純文字方式儲存於系統的任一處，會讓任何有足夠權限的人讀取加密金鑰，並可能誤用加密金鑰。

Issue Summary



Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Key Management: Null Encryption Key	1	0	0	1
Total	**1**	**0**	**0**	**1**

Key Management: Null Encryption Key	Low
Package: .venv.lib.python3.13.site-packages.pip._vendor.urllib3.contrib.securetransport	
.venv/lib/python3.13/site-packages/pip/_vendor/urllib3/contrib/securetransport.py, line 798 (Key Management: Null Encryption Key)	Low
Issue Details	

Key Management: Null Encryption Key	Low
Package: .venv.lib.python3.13.site-packages.pip._vendor.urllib3.contrib.securetransport	
.venv/lib/python3.13/site-packages/pip/_vendor/urllib3/contrib/securetransport.py, line 798 (Key Management: Null Encryption Key)	Low

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FieldAccess: _client_key_passphrase
Enclosing Method: __init__()
File: .venv/lib/python3.13/site-packages/pip/_vendor/urllib3/contrib/securetransport.py:798
Taint Flags:

```
795  self._trust_bundle = None
796  self._client_cert = None
797  self._client_key = None
798  self._client_key_passphrase = None
799  self._alpn_protocols = None
800
801  @property
```

Password Management: Empty Password (3 issues)

Abstract

空白密碼可能會導致無法輕易修正的系統安全性問題。

Explanation

使用空白密碼絕對不是明智的想法。一旦產生程式碼，還將難以修復此問題。除非修補軟體，否則無法變更密碼。如果受空白密碼保護的帳戶出現問題，系統的所有者將必須在安全性和可行性之間做出選擇。 **範例 1：**以下程式碼使用空白密碼來連線至應用程式並擷取通訊錄項目：

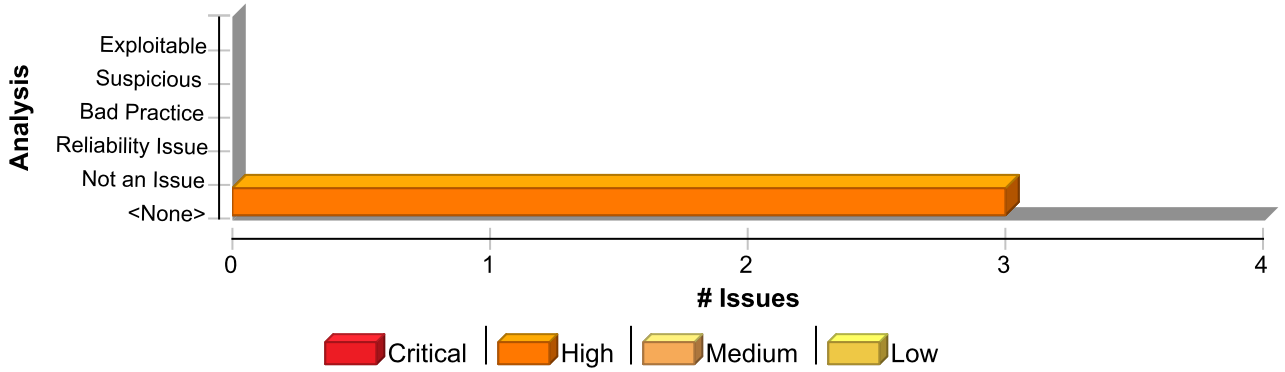
```
...
obj = new XMLHttpRequest();
obj.open('GET','/fetchusers.jsp?id='+form.id.value,'true','scott','');
...
```

此程式碼將成功執行，但任何知道使用者名稱的使用者都可以存取。

Recommendation

請勿使用空白密碼，且通常應該要將密碼模糊化，並於外部資源中進行管理。在網站中的任何純文字密碼會允許任何有充分許可權的人讀取並可能誤用密碼。至於在 JavaScript 呼叫必要密碼時，最好在連線時提示使用者密碼。

Issue Summary



Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Password Management: Empty Password	3	0	0	3
Total	**3**	**0**	**0**	**3**

Password Management: Empty Password	High
Package: .src.app.shared.components.login-modal	
frontend/src/app/shared/components/login-modal/login-modal.component.ts, line 37 (Password Management: Empty Password)	**High**

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Password Management: Empty Password — High

Package: .src.app.shared.components.login-modal

frontend/src/app/shared/components/login-modal/login-modal.component.ts, line 37 (Password Management: Empty Password) — High

Sink: FieldAccess: password
Enclosing Method: LoginModalComponent()
File: frontend/src/app/shared/components/login-modal/login-modal.component.ts:37
Taint Flags:

```
34
35  loginData: LoginRequest = {
36  username: '',
37  password: ''
38  };
39
40  isLoading: boolean = false;
```

frontend/src/app/shared/components/login-modal/login-modal.component.ts, line 110 (Password Management: Empty Password) — High

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FieldAccess: password
Enclosing Method: resetForm()
File: frontend/src/app/shared/components/login-modal/login-modal.component.ts:110
Taint Flags:

```
107  private resetForm(): void {
108  this.loginData = {
109  username: '',
110  password: ''
111  };
112  this.showPassword = false;
113  this.errorMessage = '';
```

Package: .src.app.shared.components.modals

frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts, line 248 (Password Management: Empty Password) — High

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FieldAccess: wifiPassword
Enclosing Method: QRCodeEditorModalComponent()
File: frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts:248

Password Management: Empty Password	High
Package: .src.app.shared.components.modals	
frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts, line 248 (Password Management: Empty Password)	High

Taint Flags:

```
245  phoneNumber = '';
246  emailAddress = '';
247  wifiSSID = '';
248  wifiPassword = '';
249  wifiSecurity = 'WPA';
250
251  // 譲模板能訪問Math
```

Password Management: Hardcoded Password (16 issues)

Abstract

Hardcoded Password 會導致難以修正系統的安全性問題。

Explanation

切勿使用 Hardcoded Password。這不僅會將密碼公開給所有的專案開發人員，也會使得修正問題的工作變得異常困難。程式碼進入生產階段後，程式修補可能是變更密碼的唯一方法。如果受密碼保護的帳戶出現問題，組織將必須在安全性和系統可用性之間做出選擇。 **範例 1：**下列 URL 使用 Hardcoded Password：

```
...
https://user:secretpassword@example.com
...
```

範例 2：下列 ODBC 連線字串使用硬式編碼密碼：

```
...
server=Server;database=Database;UID=UserName;PWD=Password;Encrypt=yes;
...
```

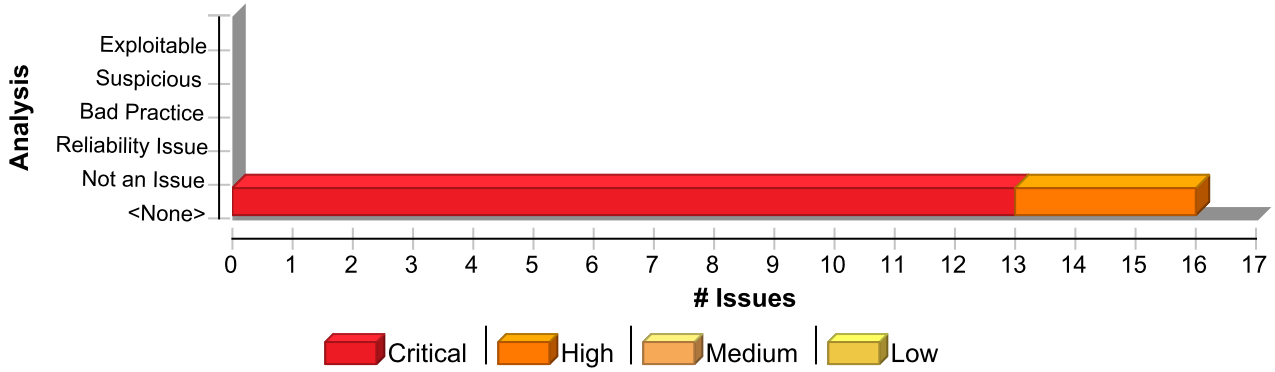
Recommendation

範例 3：以下 ODBC 連線字串透過實作整合式 Windows 驗證，解決了 範例 2 中的硬式編碼密碼問題：

```
...
server=Server;database=Database;Trusted_Connection=yes;Encrypt=yes;
...
```

切勿使用硬式編碼密碼。務必模糊化及管理外部來源中的密碼。將密碼以純文字方式儲存於系統的任一處，任何有足夠權限的人都能夠讀取密碼，並可能誤用密碼。

Issue Summary



Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Password Management: Hardcoded Password	16	0	0	16
Total	**16**	**0**	**0**	**16**

Password Management: Hardcoded Password — Critical

Package: backend

backend/appsettings.json, line 11 (Password Management: Hardcoded Password) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Sink Details

File: backend/appsettings.json:11
Taint Flags:

```
8  "AllowedHosts": "*",
9  "ConnectionStrings": {
10  "DefaultConnection":
"Host=localhost;Database=smart_nameplate;Username=postgres;Password=password",
11  "NeonConnection": "postgresql://neondb_owner:npg_uahZf7vMVn2c@ep-polished-bird-a8agssl9-
pooler.eastus2.azure.neon.tech/neondb?sslmode=require"
12  },
13  "Database": {
14  "Provider": "PostgreSQL",
```

Package: frontend.node_modules.@npmcli.redact

frontend/node_modules/@npmcli/redact/README.md, line 40 (Password Management: Hardcoded Password) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Sink Details

File: frontend/node_modules/@npmcli/redact/README.md:40
Taint Flags:

```
37 ])
38 // [
39 // 'Something --x=https://user:***@registry.npmjs.org/ foo bar',
40 // '--url=http://foo:***@registry.npmjs.org/',
41 // ]
42 ```
43
```

frontend/node_modules/@npmcli/redact/README.md, line 36 (Password Management: Hardcoded Password) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Sink Details

Password Management: Hardcoded Password — Critical

Package: frontend.node_modules.@npmcli.redact

frontend/node_modules/@npmcli/redact/README.md, line 36 (Password Management: Hardcoded Password) — Critical

File: frontend/node_modules/@npmcli/redact/README.md:36
Taint Flags:

```
33
34 redactLog([
35  'Something --x=https://user:pass@registry.npmjs.org/ foo bar',
36  '--url=http://foo:bar@registry.npmjs.org',
37 ])
38 // [
39 // 'Something --x=https://user:***@registry.npmjs.org/ foo bar',
```

frontend/node_modules/@npmcli/redact/README.md, line 19 (Password Management: Hardcoded Password) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Sink Details

File: frontend/node_modules/@npmcli/redact/README.md:19
Taint Flags:

```
16 const { redact } = require('@npmcli/redact')
17
18 redact('https://user:pass@registry.npmjs.org/')
19 // https://user:***@registry.npmjs.org/
20
21 redact(`https://registry.npmjs.org/path/npm_${'a'.repeat('36')}`)
22 // https://registry.npmjs.org/path/npm_***
```

frontend/node_modules/@npmcli/redact/README.md, line 39 (Password Management: Hardcoded Password) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Sink Details

File: frontend/node_modules/@npmcli/redact/README.md:39
Taint Flags:

```
36  '--url=http://foo:bar@registry.npmjs.org',
37 ])
38 // [
39 // 'Something --x=https://user:***@registry.npmjs.org/ foo bar',
40 // '--url=http://foo:***@registry.npmjs.org/',
```

Password Management: Hardcoded Password — Critical

Package: frontend.node_modules.@npmcli.redact

frontend/node_modules/@npmcli/redact/README.md, line 39 (Password Management: Hardcoded Password) — Critical

```
41 // ]
42 ```
```

Package: frontend.node_modules.needle.test

frontend/node_modules/needle/test/proxy_spec.js, line 161 (Password Management: Hardcoded Password) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Sink Details

File: frontend/node_modules/needle/test/proxy_spec.js:161
Taint Flags:

```
158
159  before(function() {
160  opts = {
161  proxy: 'http://mj:x@' + nonexisting_host + ':123/done'
162  }
163  })
164
```

frontend/node_modules/needle/test/proxy_spec.js, line 197 (Password Management: Hardcoded Password) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Sink Details

File: frontend/node_modules/needle/test/proxy_spec.js:197
Taint Flags:

```
194
195  it('url user:pass wins', function(done) {
196  var opts = {
197  proxy: 'http://xxx:yyy@' + nonexisting_host + ':123',
198  proxy_user: 'someone',
199  proxy_pass: 'else'
200  }
```

Password Management: Hardcoded Password — Critical

Package: frontend.node_modules.socks-proxy-agent

frontend/node_modules/socks-proxy-agent/README.md, line 20 (Password Management: Hardcoded Password) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Sink Details

File: frontend/node_modules/socks-proxy-agent/README.md:20
Taint Flags:

```
17 import { SocksProxyAgent } from 'socks-proxy-agent';
18
19 const agent = new SocksProxyAgent(
20  'socks://your-name%40gmail.com:abcdef12345124@br41.nordvpn.com'
21 );
22
23 https.get('https://ipinfo.io', { agent }, (res) => {
```

frontend/node_modules/socks-proxy-agent/README.md, line 36 (Password Management: Hardcoded Password) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Sink Details

File: frontend/node_modules/socks-proxy-agent/README.md:36
Taint Flags:

```
33 import { SocksProxyAgent } from 'socks-proxy-agent';
34
35 const agent = new SocksProxyAgent(
36  'socks://your-name%40gmail.com:abcdef12345124@br41.nordvpn.com'
37 );
38
39 var socket = new WebSocket('ws://echo.websocket.events', { agent });
```

Package: node_modules.pg-connection-string

node_modules/pg-connection-string/README.md, line 52 (Password Management: Hardcoded Password) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Sink Details

Password Management: Hardcoded Password — Critical

Package: node_modules.pg-connection-string

node_modules/pg-connection-string/README.md, line 52 (Password Management: Hardcoded Password) — Critical

File: node_modules/pg-connection-string/README.md:52
Taint Flags:

```
49 import { ClientConfig } from 'pg';
50 import { parse, toClientConfig } from 'pg-connection-string';
51
52 const config = parse('postgres://someuser:somepassword@somehost:381/somedatabase')
53 const clientConfig: ClientConfig = toClientConfig(config)
54 ```
55
```

node_modules/pg-connection-string/README.md, line 17 (Password Management: Hardcoded Password) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Sink Details

File: node_modules/pg-connection-string/README.md:17
Taint Flags:

```
14 ```js
15 const parse = require('pg-connection-string').parse;
16
17 const config = parse('postgres://someuser:somepassword@somehost:381/somedatabase')
18 ```
19
20 The resulting config contains a subset of the following properties:
```

node_modules/pg-connection-string/README.md, line 43 (Password Management: Hardcoded Password) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Sink Details

File: node_modules/pg-connection-string/README.md:43
Taint Flags:

```
40 import { ClientConfig } from 'pg';
41 import { parseIntoClientConfig } from 'pg-connection-string';
42
43 const config: ClientConfig = parseIntoClientConfig('postgres://
someuser:somepassword@somehost:381/somedatabase')
44 ```
```

Password Management: Hardcoded Password	Critical

Package: node_modules.pg-connection-string

node_modules/pg-connection-string/README.md, line 43 (Password Management: Hardcoded Password)	Critical

```
45
46 You can also use `toClientConfig` to convert an existing `ConnectionOptions` interface into
a `ClientConfig` interface:
```

Package: node_modules.pg-pool

node_modules/pg-pool/README.md, line 72 (Password Management: Hardcoded Password)	Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Sink Details

File: node_modules/pg-pool/README.md:72
Taint Flags:

```
69 const pool = new Pool(config);
70
71 /*
72  Transforms, 'postgres://DBuser:secret@DBHost:#####/myDB', into
73  config = {
74  user: 'DBuser',
75  password: 'secret',
```

Password Management: Hardcoded Password	High

Package: .src.app.shared.components.modals

frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts, line 307 (Password Management: Hardcoded Password)	High

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FieldAccess: wifiPassword
Enclosing Method: selectContentType()
File: frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts:307
Taint Flags:

```
304  break;
305  case 'wifi':
306  this.wifiSSID = 'MyWiFi';
307  this.wifiPassword = 'password123';
308  this.wifiSecurity = 'WPA';
309  this.onWifiChange();
```

Password Management: Hardcoded Password — High

Package: .src.app.shared.components.modals

frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts, line 307 (Password Management: Hardcoded Password) — High

```
310  break;
```

Package: <none>

extract_thumbnails.js, line 10 (Password Management: Hardcoded Password) — High

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FieldAccess: password
Enclosing Method: ~file_function()
File: extract_thumbnails.js:10
Taint Flags:

```
7  host: 'localhost',
8  database: 'smart_nameplate',
9  username: 'postgres',
10  password: 'password',
11  port: 5432,
12 });
13
```

fix_boundary_elements.js, line 8 (Password Management: Hardcoded Password) — High

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FieldAccess: password
Enclosing Method: ~file_function()
File: fix_boundary_elements.js:8
Taint Flags:

```
5  host: 'localhost',
6  database: 'smart_nameplate',
7  username: 'postgres',
8  password: 'password',
9  port: 5432,
10 });
11
```

Password Management: Null Password (7 issues)

Abstract

Null 密碼會危及安全性。

Explanation

指派 `null` 給密碼變數絕對不是個好方法，因為會讓攻擊者略過密碼驗證，或指出資源是由 Empty Password 所保護。 **範例 1：**以下程式碼將密碼變數初始化為 `null`，嘗試讀取已儲存的密碼值，並與使用者提供的值進行比較。

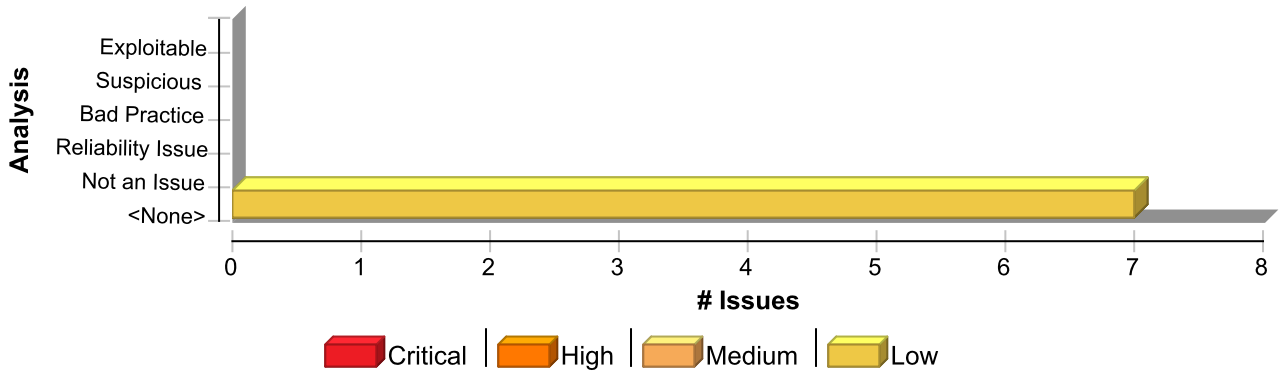
```
...
storedPassword = NULL;

temp = getPassword()
if (temp is not None) {
  storedPassword = temp;
}

if(storedPassword == userPassword) {
    // Access protected resources
    ...
}
...
```

如果 `getPassword()` 因為資料庫錯誤或其他問題而無法擷取儲存的密碼，攻擊者就可藉由提供 `null` 值給 `userPassword` 而輕易地略過密碼檢查。

Recommendation

務必從加密的外部資源讀取儲存的密碼值，並指派有意義的值給密碼變數。確保絕不要使用空白或 `null` 密碼來保護敏感資源。

Issue Summary



Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Password Management: Null Password	7	0	0	7
Total	**7**	**0**	**0**	**7**

Password Management: Null Password — Low

Package: .venv.lib.python3.13.site-packages.pip._vendor.distlib

.venv/lib/python3.13/site-packages/pip/_vendor/distlib/index.py, line 19 (Password Management: Null Password) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FieldAccess: HTTPPasswordMgr
File: .venv/lib/python3.13/site-packages/pip/_vendor/distlib/index.py:19
Taint Flags:

```
16  from dummy_threading import Thread
17
18 from . import DistlibException
19 from .compat import (HTTPBasicAuthHandler, Request, HTTPPasswordMgr,
20  urlparse, build_opener, string_types)
21 from .util import zip_dir, ServerProxy
22
```

Package: .venv.lib.python3.13.site-packages.pip._vendor.distlib.index

.venv/lib/python3.13/site-packages/pip/_vendor/distlib/index.py, line 49 (Password Management: Null Password) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FieldAccess: password_handler
Enclosing Method: __init__()
File: .venv/lib/python3.13/site-packages/pip/_vendor/distlib/index.py:49
Taint Flags:

```
46  scheme, netloc, path, params, query, frag = urlparse(self.url)
47  if params or query or frag or scheme not in ('http', 'https'):
48  raise DistlibException('invalid repository: %s' % self.url)
49  self.password_handler = None
50  self.ssl_verifier = None
51  self.gpg = None
52  self.gpg_home = None
```

Package: .venv.lib.python3.13.site-packages.pip._vendor.distlib.util

.venv/lib/python3.13/site-packages/pip/_vendor/distlib/util.py, line 816 (Password Management: Null Password) — Low

Issue Details

Kingdom: Security Features

Password Management: Null Password — Low

Package: .venv.lib.python3.13.site-packages.pip._vendor.distlib.util

.venv/lib/python3.13/site-packages/pip/_vendor/distlib/util.py, line 816 (Password Management: Null Password) — Low

Scan Engine: SCA (Structural)

Sink Details

Sink: VariableAccess: password
Enclosing Method: parse_credentials()
File: .venv/lib/python3.13/site-packages/pip/_vendor/distlib/util.py:816
Taint Flags:

```
813
814
815 def parse_credentials(netloc):
816  username = password = None
817  if '@' in netloc:
818  prefix, netloc = netloc.rsplit('@', 1)
819  if ':' not in prefix:
```

Package: .venv.lib.python3.13.site-packages.pip._vendor.urllib3.connectionpool

.venv/lib/python3.13/site-packages/pip/_vendor/urllib3/connectionpool.py, line 975 (Password Management: Null Password) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FieldAccess: key_password
Enclosing Method: __init__()
File: .venv/lib/python3.13/site-packages/pip/_vendor/urllib3/connectionpool.py:975
Taint Flags:

```
972  self.key_file = key_file
973  self.cert_file = cert_file
974  self.cert_reqs = cert_reqs
975  self.key_password = key_password
976  self.ca_certs = ca_certs
977  self.ca_cert_dir = ca_cert_dir
978  self.ssl_version = ssl_version
```

Package: node_modules.pg.lib

node_modules/pg/lib/defaults.js, line 14 (Password Management: Null Password) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Password Management: Null Password — Low

Package: node_modules.pg.lib

node_modules/pg/lib/defaults.js, line 14 (Password Management: Null Password) — Low

Sink Details

Sink: FieldAccess: password
Enclosing Method: ~file_function()
File: node_modules/pg/lib/defaults.js:14
Taint Flags:

```
11  database: undefined,
12
13  // database user's password
14  password: null,
15
16  // a Postgres connection string to be used instead of setting individual connection items
17  // NOTE: Setting this value will cause it to override any other value (such as database or
user) defined
```

node_modules/pg/lib/client.js, line 222 (Password Management: Null Password) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FieldAccess: password
Enclosing Method: lambda()
File: node_modules/pg/lib/client.js:222
Taint Flags:

```
219  }
220  this.connectionParameters.password = this.password = pass
221  } else {
222  this.connectionParameters.password = this.password = null
223  }
224  cb()
225  })
```

node_modules/pg/lib/client.js, line 222 (Password Management: Null Password) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FieldAccess: password
Enclosing Method: lambda()
File: node_modules/pg/lib/client.js:222
Taint Flags:

```
219  }
```

Password Management: Null Password	Low

Package: node_modules.pg.lib

node_modules/pg/lib/client.js, line 222 (Password Management: Null Password)	Low

```
220  this.connectionParameters.password = this.password = pass
221  } else {
222  this.connectionParameters.password = this.password = null
223  }
224  cb()
225  })
```

Password Management: Password in Comment (61 issues)

Abstract

若以純文字形式將密碼或密碼詳細資訊儲存在系統或系統程式碼的任意位置，可能會導致無法輕易修正的系統安全性問題。

Explanation

將密碼硬式編碼絕對不是明智的想法。將密碼詳細資訊儲存在註解中等同於對密碼執行硬式編碼。這不僅會將密碼公開給所有的專案開發人員，也會使得修正問題的工作變得異常困難。在程式碼進入生產階段後，會向外部環境洩漏密碼，除非修補軟體，否則無法保護或變更密碼。如果受密碼保護的帳戶出現問題，系統的所有者將必須在安全性和可行性之間做出選擇。 **範例 1：**以下註解指定要連接到資料庫的預設密碼：

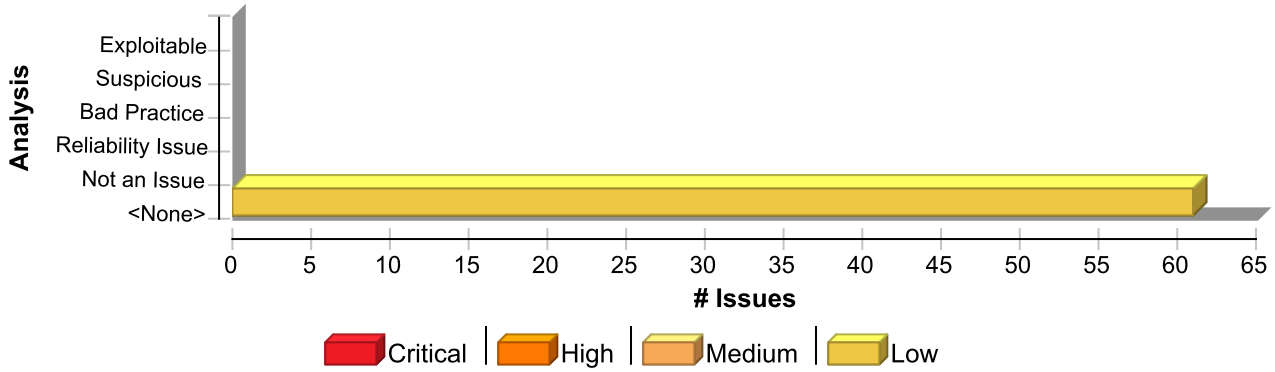
```
...
# Default username for database connection is "scott"
# Default password for database connection is "tiger"
...
```

此程式碼能夠成功執行，但有程式碼存取權的任何人都能夠存取密碼。若員工有此資訊的存取權，可能會使用此資訊來進入並破壞系統。

Recommendation

請勿將密碼硬式編碼，且通常應該要將密碼模糊化，並於外部資源中進行管理。將密碼以純文字方式儲存於系統的任一處，任何有足夠權限的人都可以讀取密碼，並可能誤用密碼。

Issue Summary



Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Password Management: Password in Comment	61	0	0	61
Total	**61**	**0**	**0**	**61**

Password Management: Password in Comment	Low
Package: .venv.lib.python3.13.site-packages.pip._internal.models	
.venv/lib/python3.13/site-packages/pip/_internal/models/link.py, line 417 (Password Management: Password in Comment)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Password Management: Password in Comment	Low

Package: .venv.lib.python3.13.site-packages.pip._internal.models

.venv/lib/python3.13/site-packages/pip/_internal/models/link.py, line 417 (Password Management: Password in Comment)	Low

Sink Details

Sink: Comment
File: .venv/lib/python3.13/site-packages/pip/_internal/models/link.py:417
Taint Flags:

Package: .venv.lib.python3.13.site-packages.pip._internal.network

.venv/lib/python3.13/site-packages/pip/_internal/network/auth.py, line 512 (Password Management: Password in Comment)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: .venv/lib/python3.13/site-packages/pip/_internal/network/auth.py:512
Taint Flags:

```
509  if username is not None and password is not None:
510  self.passwords[parsed.netloc] = (username, password)
511
512  # Prompt to save the password to keyring
513  if save and self._should_save_password_to_keyring():
514  self._credentials_to_save = Credentials(
515  url=parsed.netloc,
```

.venv/lib/python3.13/site-packages/pip/_internal/network/auth.py, line 424 (Password Management: Password in Comment)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: .venv/lib/python3.13/site-packages/pip/_internal/network/auth.py:424
Taint Flags:

```
421  # Convert the username and password if they're None, so that
422  # this netloc will show up as "cached" in the conditional above.
423  # Further, HTTPBasicAuth doesn't accept None, so it makes sense to
424  # cache the value that is going to be used.
425  username = username or ""
426  password = password or ""
427
```

Password Management: Password in Comment — Low

Package: .venv.lib.python3.13.site-packages.pip._internal.network

.venv/lib/python3.13/site-packages/pip/_internal/network/auth.py, line 412 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: .venv/lib/python3.13/site-packages/pip/_internal/network/auth.py:412
Taint Flags:

```
409  # If credentials not found, use any stored credentials for this netloc.
410  # Do this if either the username or the password is missing.
411  # This accounts for the situation in which the user has specified
412  # the username in the index url, but the password comes from keyring.
413  if (username is None or password is None) and netloc in self.passwords:
414  un, pw = self.passwords[netloc]
415  # It is possible that the cached credentials are for a different username,
```

.venv/lib/python3.13/site-packages/pip/_internal/network/auth.py, line 502 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: .venv/lib/python3.13/site-packages/pip/_internal/network/auth.py:502
Taint Flags:

```
499
500  parsed = urllib.parse.urlparse(resp.url)
501
502  # Prompt the user for a new username and password
503  save = False
504  if not username and not password:
505  username, password, save = self._prompt_for_password(parsed.netloc)
```

.venv/lib/python3.13/site-packages/pip/_internal/network/auth.py, line 527 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Password Management: Password in Comment — Low

Package: .venv.lib.python3.13.site-packages.pip._internal.network

.venv/lib/python3.13/site-packages/pip/_internal/network/auth.py, line 527 (Password Management: Password in Comment) — Low

Sink: Comment
File: .venv/lib/python3.13/site-packages/pip/_internal/network/auth.py:527
Taint Flags:

```
524  _ = resp.content
525  resp.raw.release_conn()
526
527  # Add our new username and password to the request
528  req = HTTPBasicAuth(username or "", password or "")(resp.request)
529  req.register_hook("response", self.warn_on_401)
530
```

.venv/lib/python3.13/site-packages/pip/_internal/network/auth.py, line 507 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: .venv/lib/python3.13/site-packages/pip/_internal/network/auth.py:507
Taint Flags:

```
504  if not username and not password:
505  username, password, save = self._prompt_for_password(parsed.netloc)
506
507  # Store the new username and password to use for future requests
508  self._credentials_to_save = None
509  if username is not None and password is not None:
510  self.passwords[parsed.netloc] = (username, password)
```

.venv/lib/python3.13/site-packages/pip/_internal/network/auth.py, line 377 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: .venv/lib/python3.13/site-packages/pip/_internal/network/auth.py:377
Taint Flags:

```
374  logger.debug("Found credentials in netrc for %s", netloc)
375  return netrc_auth
376
```

Password Management: Password in Comment — Low

Package: .venv.lib.python3.13.site-packages.pip._internal.network

.venv/lib/python3.13/site-packages/pip/_internal/network/auth.py, line 377 (Password Management: Password in Comment) — Low

```
377  # If we don't have a password and keyring is available, use it.
378  if allow_keyring:
379  # The index url is more specific than the netloc, so try it first
380  # fmt: off
```

Package: .venv.lib.python3.13.site-packages.pip._internal.utils

.venv/lib/python3.13/site-packages/pip/_internal/utils/wheel.py, line 72 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: .venv/lib/python3.13/site-packages/pip/_internal/utils/wheel.py:72
Taint Flags:

.venv/lib/python3.13/site-packages/pip/_internal/utils/misc.py, line 444 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: .venv/lib/python3.13/site-packages/pip/_internal/utils/misc.py:444
Taint Flags:

```
441
442  # Split from the right because that's how urllib.parse.urlsplit()
443  # behaves if more than one @ is present (which can be checked using
444  # the password attribute of urlsplit()'s return value).
445  auth, netloc = netloc.rsplit("@", 1)
446  pw: Optional[str] = None
447  if ":" in auth:
```

.venv/lib/python3.13/site-packages/pip/_internal/utils/misc.py, line 450 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Password Management: Password in Comment — Low

Package: .venv.lib.python3.13.site-packages.pip._internal.utils

.venv/lib/python3.13/site-packages/pip/_internal/utils/misc.py, line 450 (Password Management: Password in Comment) — Low

Sink: Comment
File: .venv/lib/python3.13/site-packages/pip/_internal/utils/misc.py:450
Taint Flags:

```
447  if ":" in auth:
448  # Split from the left because that's how urllib.parse.urlsplit()
449  # behaves if more than one : is present (which again can be checked
450  # using the password attribute of the return value)
451  user, pw = auth.split(":", 1)
452  else:
453  user, pw = auth, None
```

Package: .venv.lib.python3.13.site-packages.pip._internal.vcs

.venv/lib/python3.13/site-packages/pip/_internal/vcs/subversion.py, line 162 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: .venv/lib/python3.13/site-packages/pip/_internal/vcs/subversion.py:162
Taint Flags:

.venv/lib/python3.13/site-packages/pip/_internal/vcs/subversion.py, line 274 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: .venv/lib/python3.13/site-packages/pip/_internal/vcs/subversion.py:274
Taint Flags:

.venv/lib/python3.13/site-packages/pip/_internal/vcs/subversion.py, line 83 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment

Password Management: Password in Comment	Low

Package: .venv.lib.python3.13.site-packages.pip._internal.vcs

.venv/lib/python3.13/site-packages/pip/_internal/vcs/subversion.py, line 83 (Password Management: Password in Comment)	Low

File: .venv/lib/python3.13/site-packages/pip/_internal/vcs/subversion.py:83
Taint Flags:

Package: .venv.lib.python3.13.site-packages.pip._vendor.distlib

.venv/lib/python3.13/site-packages/pip/_vendor/distlib/index.py, line 55 (Password Management: Password in Comment)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: .venv/lib/python3.13/site-packages/pip/_vendor/distlib/index.py:55
Taint Flags:

```
52  self.gpg_home = None
53  with open(os.devnull, 'w') as sink:
54  # Use gpg by default rather than gpg2, as gpg2 insists on
55  # prompting for passwords
56  for s in ('gpg', 'gpg2'):
57  try:
58  rc = subprocess.check_call([s, '--version'], stdout=sink,
```

.venv/lib/python3.13/site-packages/pip/_vendor/distlib/compat.py, line 61 (Password Management: Password in Comment)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: .venv/lib/python3.13/site-packages/pip/_vendor/distlib/compat.py:61
Taint Flags:

```
58
59  # match = _userprog.match(host)
60  # if match: return match.group(1, 2)
61  # return None, host
62
63 else: # pragma: no cover
64  from io import StringIO
```

Password Management: Password in Comment — Low

Package: .venv.lib.python3.13.site-packages.pip._vendor.requests

.venv/lib/python3.13/site-packages/pip/_vendor/requests/utils.py, line 247 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: .venv/lib/python3.13/site-packages/pip/_vendor/requests/utils.py:247
Taint Flags:

```
244  try:
245  _netrc = netrc(netrc_path).authenticators(host)
246  if _netrc:
247  # Return with login / password
248  login_i = 0 if _netrc[0] else 1
249  return (_netrc[login_i], _netrc[2])
250  except (NetrcParseError, OSError):
```

Package: .venv.lib.python3.13.site-packages.pip._vendor.urllib3.contrib._securetransport

.venv/lib/python3.13/site-packages/pip/_vendor/urllib3/contrib/_securetransport/low_level.py, line 272 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: .venv/lib/python3.13/site-packages/pip/_vendor/urllib3/contrib/_securetransport/low_level.py:272
Taint Flags:

```
269  None, # What the type of the file is, we don't care
270  None, # what's in the file, we don't care
271  0, # import flags
272  None, # key params, can include passphrase in the future
273  keychain, # The keychain to insert into
274  ctypes.byref(result_array), # Results
275  )
```

.venv/lib/python3.13/site-packages/pip/_vendor/urllib3/contrib/_securetransport/low_level.py, line 228 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Password Management: Password in Comment — Low

Package: .venv.lib.python3.13.site-packages.pip._vendor.urllib3.contrib._securetransport

.venv/lib/python3.13/site-packages/pip/_vendor/urllib3/contrib/_securetransport/low_level.py, line 228 (Password Management: Password in Comment) — Low

Sink Details

Sink: Comment
File: .venv/lib/python3.13/site-packages/pip/_vendor/urllib3/contrib/_securetransport/low_level.py:228
Taint Flags:

```
225  # we're going to create a temporary directory and a filename to use there.
226  # This filename will be 8 random bytes expanded into base64. We also need
227  # some random bytes to password-protect the keychain we're creating, so we
228  # ask for 40 random bytes.
229  random_bytes = os.urandom(40)
230  filename = base64.b16encode(random_bytes[:8]).decode("utf-8")
231  password = base64.b16encode(random_bytes[8:]) # Must be valid UTF-8
```

Package: .venv.lib.python3.13.site-packages.pip._vendor.urllib3.util

.venv/lib/python3.13/site-packages/pip/_vendor/urllib3/util/ssl_.py, line 421 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: .venv/lib/python3.13/site-packages/pip/_vendor/urllib3/util/ssl_.py:421
Taint Flags:

```
418
419  # Attempt to detect if we get the goofy behavior of the
420  # keyfile being encrypted and OpenSSL asking for the
421  # passphrase via the terminal and instead error out.
422  if keyfile and key_password is None and _is_key_file_encrypted(keyfile):
423  raise SSLError("Client private key is encrypted, password is required")
424
```

Package: .venv.lib.python3.13.site-packages.requests

.venv/lib/python3.13/site-packages/requests/utils.py, line 247 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: .venv/lib/python3.13/site-packages/requests/utils.py:247

Password Management: Password in Comment — Low

Package: .venv.lib.python3.13.site-packages.requests

.venv/lib/python3.13/site-packages/requests/utils.py, line 247 (Password Management: Password in Comment) — Low

Taint Flags:

```
244  try:
245  _netrc = netrc(netrc_path).authenticators(host)
246  if _netrc:
247  # Return with login / password
248  login_i = 0 if _netrc[0] else 1
249  return (_netrc[login_i], _netrc[2])
250  except (NetrcParseError, OSError):
```

Package: .venv.lib.python3.13.site-packages.urllib3.util

.venv/lib/python3.13/site-packages/urllib3/util/ssl_.py, line 468 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: .venv/lib/python3.13/site-packages/urllib3/util/ssl_.py:468
Taint Flags:

```
465
466  # Attempt to detect if we get the goofy behavior of the
467  # keyfile being encrypted and OpenSSL asking for the
468  # passphrase via the terminal and instead error out.
469  if keyfile and key_password is None and _is_key_file_encrypted(keyfile):
470  raise SSLError("Client private key is encrypted, password is required")
471
```

Package: frontend.node_modules.@jridgewell.source-map.dist

frontend/node_modules/@jridgewell/source-map/dist/source-map.umd.js, line 171 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: frontend/node_modules/@jridgewell/source-map/dist/source-map.umd.js:171
Taint Flags:

```
168
```

Password Management: Password in Comment — Low

Package: frontend.node_modules.@jridgewell.source-map.dist

frontend/node_modules/@jridgewell/source-map/dist/source-map.umd.js, line 171 (Password Management: Password in Comment) — **Low**

```
169  // Matches the scheme of a URL, eg "http://"
170  const schemeRegex = /^[\w+.-]+:\/\//;
171  /**
172  * Matches the parts of a URL:
173  * 1. Scheme, including ":", guaranteed.
174  * 2. User/password, including "@", optional.
```

Package: frontend.node_modules.body-parser.node_modules.debug.src

frontend/node_modules/body-parser/node_modules/debug/src/node.js, line 203 (Password Management: Password in Comment) — **Low**

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: frontend/node_modules/body-parser/node_modules/debug/src/node.js:203
Taint Flags:

```
200  // FIXME Should probably have an option in net.Socket to create a
201  // stream from an existing fd which is writable only. But for now
202  // we'll just add this hack and set the `readable` member to false.
203  // Test: ./node test/fixtures/echo.js < /etc/passwd
204  stream.readable = false;
205  stream.read = null;
206  stream._type = 'pipe';
```

Package: frontend.node_modules.compression.node_modules.debug.src

frontend/node_modules/compression/node_modules/debug/src/node.js, line 203 (Password Management: Password in Comment) — **Low**

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: frontend/node_modules/compression/node_modules/debug/src/node.js:203
Taint Flags:

```
200  // FIXME Should probably have an option in net.Socket to create a
201  // stream from an existing fd which is writable only. But for now
202  // we'll just add this hack and set the `readable` member to false.
203  // Test: ./node test/fixtures/echo.js < /etc/passwd
```

Password Management: Password in Comment — Low

Package: frontend.node_modules.compression.node_modules.debug.src

frontend/node_modules/compression/node_modules/debug/src/node.js, line 203 (Password Management: Password in Comment) — **Low**

```
204  stream.readable = false;
205  stream.read = null;
206  stream._type = 'pipe';
```

Package: frontend.node_modules.connect.node_modules.debug.src

frontend/node_modules/connect/node_modules/debug/src/node.js, line 203 (Password Management: Password in Comment) — **Low**

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: frontend/node_modules/connect/node_modules/debug/src/node.js:203
Taint Flags:

```
200  // FIXME Should probably have an option in net.Socket to create a
201  // stream from an existing fd which is writable only. But for now
202  // we'll just add this hack and set the `readable` member to false.
203  // Test: ./node test/fixtures/echo.js < /etc/passwd
204  stream.readable = false;
205  stream.read = null;
206  stream._type = 'pipe';
```

Package: frontend.node_modules.express.node_modules.debug.src

frontend/node_modules/express/node_modules/debug/src/node.js, line 203 (Password Management: Password in Comment) — **Low**

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: frontend/node_modules/express/node_modules/debug/src/node.js:203
Taint Flags:

```
200  // FIXME Should probably have an option in net.Socket to create a
201  // stream from an existing fd which is writable only. But for now
202  // we'll just add this hack and set the `readable` member to false.
203  // Test: ./node test/fixtures/echo.js < /etc/passwd
204  stream.readable = false;
205  stream.read = null;
206  stream._type = 'pipe';
```

Password Management: Password in Comment	Low
Package: frontend.node_modules.express.node_modules.debug.src	
frontend/node_modules/express/node_modules/debug/src/node.js, line 203 (Password Management: Password in Comment)	**Low**

Package: frontend.node_modules.finalhandler.node_modules.debug.src

frontend/node_modules/finalhandler/node_modules/debug/src/node.js, line 203 (Password Management: Password in Comment)	**Low**

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: frontend/node_modules/finalhandler/node_modules/debug/src/node.js:203
Taint Flags:

```
200  // FIXME Should probably have an option in net.Socket to create a
201  // stream from an existing fd which is writable only. But for now
202  // we'll just add this hack and set the `readable` member to false.
203  // Test: ./node test/fixtures/echo.js < /etc/passwd
204  stream.readable = false;
205  stream.read = null;
206  stream._type = 'pipe';
```

Package: frontend.node_modules.hosted-git-info.lib

frontend/node_modules/hosted-git-info/lib/parse-url.js, line 59 (Password Management: Password in Comment)	**Low**

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: frontend/node_modules/hosted-git-info/lib/parse-url.js:59
Taint Flags:

```
56  // username:password@hostname.com:user/repo
57  // proto://username@hostname.com:user/repo
58  // proto://:password@hostname.com:user/repo
59  // proto://username:password@hostname.com:user/repo
60  // then we replace the last : with a / to create a valid path
61  giturl = giturl.slice(0, lastColonBeforeHash) + '/' + giturl.slice(lastColonBeforeHash + 1)
62  }
```

Password Management: Password in Comment — Low

Package: frontend.node_modules.hosted-git-info.lib

frontend/node_modules/hosted-git-info/lib/parse-url.js, line 55 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: frontend/node_modules/hosted-git-info/lib/parse-url.js:55
Taint Flags:

```
52  // like it would in:
53  // proto://hostname.com:user/repo
54  // username@hostname.com:user/repo
55  // :password@hostname.com:user/repo
56  // username:password@hostname.com:user/repo
57  // proto://username@hostname.com:user/repo
58  // proto://:password@hostname.com:user/repo
```

frontend/node_modules/hosted-git-info/lib/parse-url.js, line 56 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: frontend/node_modules/hosted-git-info/lib/parse-url.js:56
Taint Flags:

```
53  // proto://hostname.com:user/repo
54  // username@hostname.com:user/repo
55  // :password@hostname.com:user/repo
56  // username:password@hostname.com:user/repo
57  // proto://username@hostname.com:user/repo
58  // proto://:password@hostname.com:user/repo
59  // proto://username:password@hostname.com:user/repo
```

frontend/node_modules/hosted-git-info/lib/parse-url.js, line 58 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Password Management: Password in Comment — Low

Package: frontend.node_modules.hosted-git-info.lib

frontend/node_modules/hosted-git-info/lib/parse-url.js, line 58 (Password Management: Password in Comment) — Low

Sink: Comment
File: frontend/node_modules/hosted-git-info/lib/parse-url.js:58
Taint Flags:

```
55  // :password@hostname.com:user/repo
56  // username:password@hostname.com:user/repo
57  // proto://username@hostname.com:user/repo
58  // proto://:password@hostname.com:user/repo
59  // proto://username:password@hostname.com:user/repo
60  // then we replace the last : with a / to create a valid path
61  giturl = giturl.slice(0, lastColonBeforeHash) + '/' + giturl.slice(lastColonBeforeHash + 1)
```

Package: frontend.node_modules.inquirer.lib.prompts

frontend/node_modules/inquirer/lib/prompts/base.js, line 142 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: frontend/node_modules/inquirer/lib/prompts/base.js:142
Taint Flags:

```
139  this.screen.renderWithSpinner(content, bottomContent);
140  }
141
142  /**
143  * Allow override, e.g. for password prompts
144  * See: https://github.com/SBoudrias/Inquirer.js/issues/1022
145  *
```

frontend/node_modules/inquirer/lib/prompts/base.js, line 169 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: frontend/node_modules/inquirer/lib/prompts/base.js:169
Taint Flags:

```
166  this.status !== 'touched' &&
```

Password Management: Password in Comment — Low

Package: frontend.node_modules.inquirer.lib.prompts

frontend/node_modules/inquirer/lib/prompts/base.js, line 169 (Password Management: Password in Comment) — Low

```
167   this.status !== 'answered'
168   ) {
169   // If default password is supplied, hide it
170   if (this.opt.type === 'password') {
171   message += chalk.italic.dim('[hidden] ');
172   } else {
```

Package: frontend.node_modules.node-forge.lib

frontend/node_modules/node-forge/lib/ssh.js, line 64 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: frontend/node_modules/node-forge/lib/ssh.js:64
Taint Flags:

```
61   // use the unencrypted buffer
62   priv = forge.util.encode64(privbuffer.bytes(), 64);
63   } else {
64   // encrypt RSA key using passphrase
65   var encLen = privbuffer.length() + 16 - 1;
66   encLen -= encLen % 16;
67
```

frontend/node_modules/node-forge/lib/ssh.js, line 20 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: frontend/node_modules/node-forge/lib/ssh.js:20
Taint Flags:

```
17
18 var ssh = module.exports = forge.ssh = forge.ssh || {};
19
20 /**
21   * Encodes (and optionally encrypts) a private RSA key as a Putty PPK file.
22   *
```

Password Management: Password in Comment — Low

Package: frontend.node_modules.node-forge.lib

frontend/node_modules/node-forge/lib/ssh.js, line 20 (Password Management: Password in Comment) — Low

```
23   * @param privateKey the key.
```

frontend/node_modules/node-forge/lib/ssh.js, line 139 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: frontend/node_modules/node-forge/lib/ssh.js:139
Taint Flags:

```
136   return type + ' ' + forge.util.encode64(buffer.bytes()) + ' ' + comment;
137 };
138
139 /**
140   * Encodes a private RSA key as an OpenSSH file.
141   *
142   * @param key the key.
```

Package: frontend.node_modules.send.node_modules.debug.src

frontend/node_modules/send/node_modules/debug/src/node.js, line 203 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: frontend/node_modules/send/node_modules/debug/src/node.js:203
Taint Flags:

```
200   // FIXME Should probably have an option in net.Socket to create a
201   // stream from an existing fd which is writable only. But for now
202   // we'll just add this hack and set the `readable` member to false.
203   // Test: ./node test/fixtures/echo.js < /etc/passwd
204   stream.readable = false;
205   stream.read = null;
206   stream._type = 'pipe';
```

Password Management: Password in Comment — Low

Package: frontend.node_modules.serve-index.node_modules.debug.src

frontend/node_modules/serve-index/node_modules/debug/src/node.js, line 203 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: frontend/node_modules/serve-index/node_modules/debug/src/node.js:203
Taint Flags:

```
200  // FIXME Should probably have an option in net.Socket to create a
201  // stream from an existing fd which is writable only. But for now
202  // we'll just add this hack and set the `readable` member to false.
203  // Test: ./node test/fixtures/echo.js < /etc/passwd
204  stream.readable = false;
205  stream.read = null;
206  stream._type = 'pipe';
```

Package: frontend.node_modules.vite.dist.node.chunks

frontend/node_modules/vite/dist/node/chunks/dep-C6uTJdX2.js, line 34822 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: frontend/node_modules/vite/dist/node/chunks/dep-C6uTJdX2.js:34822
Taint Flags:

```
34819  if (processEnv[key] === parsed[key]) {
34820  return processEnv[key]
34821  } else {
34822  // scenario: PASSWORD_EXPAND_NESTED=${PASSWORD_EXPAND}
34823  return interpolate(processEnv[key], processEnv, parsed)
34824  }
34825  }
```

frontend/node_modules/vite/dist/node/chunks/dep-C6uTJdX2.js, line 39868 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Password Management: Password in Comment — Low

Package: frontend.node_modules.vite.dist.node.chunks

frontend/node_modules/vite/dist/node/chunks/dep-C6uTJdX2.js, line 39868 (Password Management: Password in Comment) — Low

Sink Details

Sink: Comment
File: frontend/node_modules/vite/dist/node/chunks/dep-C6uTJdX2.js:39868
Taint Flags:

```
39865  // FIXME Should probably have an option in net.Socket to create a
39866  // stream from an existing fd which is writable only. But for now
39867  // we'll just add this hack and set the `readable` member to false.
39868  // Test: ./node test/fixtures/echo.js < /etc/passwd
39869  stream.readable = false;
39870  stream.read = null;
39871  stream._type = 'pipe';
```

frontend/node_modules/vite/dist/node/chunks/dep-C6uTJdX2.js, line 61668 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: frontend/node_modules/vite/dist/node/chunks/dep-C6uTJdX2.js:61668
Taint Flags:

```
61665
61666
61667 function createProxyServer(options) {
61668  /*
61669  * `options` is needed and it must have the following layout:
61670  *
61671  * {
```

Package: frontend.node_modules.webpack-dev-server.client.modules.sockjs-client

frontend/node_modules/webpack-dev-server/client/modules/sockjs-client/index.js, line 4771 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: frontend/node_modules/webpack-dev-server/client/modules/sockjs-client/index.js:4771
Taint Flags:

Password Management: Password in Comment — Low

Package: frontend.node_modules.webpack-dev-server.client.modules.sockjs-client

frontend/node_modules/webpack-dev-server/client/modules/sockjs-client/index.js, line 4771 (Password Management: Password in Comment) — Low

```
4768  }
4769
4770  //
4771  // Parse down the `auth` for the username and password.
4772  //
4773  url.username = url.password = '';
4774  if (url.auth) {
```

Package: frontend.node_modules.webpack-dev-server.client.utils

frontend/node_modules/webpack-dev-server/client/utils/createSocketURL.js, line 84 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: frontend/node_modules/webpack-dev-server/client/utils/createSocketURL.js:84
Taint Flags:

```
81  socketURLAuth = parsedURL.username;
82
83  // Since HTTP basic authentication does not allow empty username,
84  // we only include password if the username is not empty.
85  if (parsedURL.password) {
86  // Result: <username>:<password>
87  socketURLAuth = socketURLAuth.concat(":", parsedURL.password);
```

frontend/node_modules/webpack-dev-server/client/utils/createSocketURL.js, line 86 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: frontend/node_modules/webpack-dev-server/client/utils/createSocketURL.js:86
Taint Flags:

```
83  // Since HTTP basic authentication does not allow empty username,
84  // we only include password if the username is not empty.
85  if (parsedURL.password) {
86  // Result: <username>:<password>
87  socketURLAuth = socketURLAuth.concat(":", parsedURL.password);
```

Password Management: Password in Comment	Low

Package: frontend.node_modules.webpack-dev-server.client.utils

frontend/node_modules/webpack-dev-server/client/utils/createSocketURL.js, line 86 (Password Management: Password in Comment)	Low

```
88  }
89  }
```

Package: frontend.node_modules.webpack-dev-server.lib

frontend/node_modules/webpack-dev-server/lib/Server.js, line 147 (Password Management: Password in Comment)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: frontend/node_modules/webpack-dev-server/lib/Server.js:147
Taint Flags:

```
144  * @property {import("open").Options} options
145  */
146
147 /**
148  * @typedef {Object} WebSocketURL
149  * @property {string} [hostname]
150  * @property {string} [password]
```

Package: node_modules.pg-pool

node_modules/pg-pool/index.js, line 72 (Password Management: Password in Comment)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: node_modules/pg-pool/index.js:72
Taint Flags:

```
69  this.options = Object.assign({}, options)
70
71  if (options != null && 'password' in options) {
72  // "hiding" the password so it doesn't show up in stack traces
73  // or if the client is console.logged
74  Object.defineProperty(this.options, 'password', {
75  configurable: true,
```

Password Management: Password in Comment — Low

Package: node_modules.pg.lib

node_modules/pg/lib/client.js, line 186 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: node_modules/pg/lib/client.js:186
Taint Flags:

```
183  con.on('authenticationCleartextPassword', this._handleAuthCleartextPassword.bind(this))
184  // password request handling
185  con.on('authenticationMD5Password', this._handleAuthMD5Password.bind(this))
186  // password request handling (SASL)
187  con.on('authenticationSASL', this._handleAuthSASL.bind(this))
188  con.on('authenticationSASLContinue', this._handleAuthSASLContinue.bind(this))
189  con.on('authenticationSASLFinal', this._handleAuthSASLFinal.bind(this))
```

node_modules/pg/lib/defaults.js, line 13 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: node_modules/pg/lib/defaults.js:13
Taint Flags:

```
10  // name of database to connect
11  database: undefined,
12
13  // database user's password
14  password: null,
15
16  // a Postgres connection string to be used instead of setting individual connection items
```

node_modules/pg/lib/client.js, line 61 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Password Management: Password in Comment — Low

Package: node_modules.pg.lib

node_modules/pg/lib/client.js, line 61 (Password Management: Password in Comment) — Low

Sink: Comment
File: node_modules/pg/lib/client.js:61
Taint Flags:

```
58  this.processID = null
59  this.secretKey = null
60  this.ssl = this.connectionParameters.ssl || false
61  // As with Password, make SSL->Key (the private key) non-enumerable.
62  // It won't show up in stack traces
63  // or if the client is console.logged
64  if (this.ssl && this.ssl.key) {
```

node_modules/pg/lib/client.js, line 206 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: node_modules/pg/lib/client.js:206
Taint Flags:

```
203  con.on('notification', this._handleNotification.bind(this))
204  }
205
206  // TODO(bmc): deprecate pgpass "built in" integration since this.password can be a
function
207  // it can be supplied by the user if required - this is a breaking change!
208  _checkPgPass(cb) {
209  const con = this.connection
```

node_modules/pg/lib/client.js, line 182 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: node_modules/pg/lib/client.js:182
Taint Flags:

```
179  }
180
```

Password Management: Password in Comment — Low

Package: node_modules.pg.lib

node_modules/pg/lib/client.js, line 182 (Password Management: Password in Comment) — Low

```
181  _attachListeners(con) {
182  // password request handling
183  con.on('authenticationCleartextPassword', this._handleAuthCleartextPassword.bind(this))
184  // password request handling
185  con.on('authenticationMD5Password', this._handleAuthMD5Password.bind(this))
```

node_modules/pg/lib/client.js, line 184 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: node_modules/pg/lib/client.js:184
Taint Flags:

```
181  _attachListeners(con) {
182  // password request handling
183  con.on('authenticationCleartextPassword', this._handleAuthCleartextPassword.bind(this))
184  // password request handling
185  con.on('authenticationMD5Password', this._handleAuthMD5Password.bind(this))
186  // password request handling (SASL)
187  con.on('authenticationSASL', this._handleAuthSASL.bind(this))
```

node_modules/pg/lib/client.js, line 24 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: node_modules/pg/lib/client.js:24
Taint Flags:

```
21  this.port = this.connectionParameters.port
22  this.host = this.connectionParameters.host
23
24  // "hiding" the password so it doesn't show up in stack traces
25  // or if the client is console.logged
26  Object.defineProperty(this, 'password', {
27  configurable: true,
```

Password Management: Password in Comment — Low

Package: node_modules.pg.lib

node_modules/pg/lib/connection-parameters.js, line 69 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: node_modules/pg/lib/connection-parameters.js:69
Taint Flags:

```
66  this.port = parseInt(val('port', config), 10)
67  this.host = val('host', config)
68
69  // "hiding" the password so it doesn't show up in stack traces
70  // or if the client is console.logged
71  Object.defineProperty(this, 'password', {
72  configurable: true,
```

Package: node_modules.pg.lib.crypto

node_modules/pg/lib/crypto/utils-legacy.js, line 11 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: node_modules/pg/lib/crypto/utils-legacy.js:11
Taint Flags:

```
8  return nodeCrypto.createHash('md5').update(string, 'utf-8').digest('hex')
9 }
10
11 // See AuthenticationMD5Password at https://www.postgresql.org/docs/current/static/protocol-flow.html
12 function postgresMd5PasswordHash(user, password, salt) {
13  const inner = md5(password + user)
14  const outer = md5(Buffer.concat([Buffer.from(inner), salt]))
```

node_modules/pg/lib/crypto/utils-webcrypto.js, line 50 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Password Management: Password in Comment — Low

Package: node_modules.pg.lib.crypto

node_modules/pg/lib/crypto/utils-webcrypto.js, line 50 (Password Management: Password in Comment) — Low

Sink Details

Sink: Comment
File: node_modules/pg/lib/crypto/utils-webcrypto.js:50
Taint Flags:

```
47  }
48 }
49
50 // See AuthenticationMD5Password at https://www.postgresql.org/docs/current/static/protocol-flow.html
51 async function postgresMd5PasswordHash(user, password, salt) {
52  const inner = await md5(password + user)
53  const outer = await md5(Buffer.concat([Buffer.from(inner), salt]))
```

node_modules/pg/lib/crypto/utils-webcrypto.js, line 79 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: node_modules/pg/lib/crypto/utils-webcrypto.js:79
Taint Flags:

```
76  return await subtleCrypto.sign('HMAC', key, textEncoder.encode(msg))
77 }
78
79 /**
80  * Derive a key from the password and salt
81  * @param {string} password
82  * @param {Uint8Array} salt
```

Package: node_modules.pg.lib.native

node_modules/pg/lib/native/client.js, line 42 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: node_modules/pg/lib/native/client.js:42
Taint Flags:

Password Management: Password in Comment — Low

Package: node_modules.pg.lib.native

node_modules/pg/lib/native/client.js, line 42 (Password Management: Password in Comment) — Low

```
39  if (config.nativeConnectionString) cp.nativeConnectionString =
config.nativeConnectionString
40  this.user = cp.user
41
42  // "hiding" the password so it doesn't show up in stack traces
43  // or if the client is console.logged
44  Object.defineProperty(this, 'password', {
45  configurable: true,
```

Package: node_modules.pgpass.lib

node_modules/pgpass/lib/helper.js, line 83 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: node_modules/pgpass/lib/helper.js:83
Taint Flags:

```
80  }
81
82  if (stats.mode & (S_IRWXG | S_IRWXO)) {
83  /* If password file is insecure, alert the user and ignore it. */
84  warn('WARNING: password file "%s" has group or world access; permissions should be u=rw
(0600) or less', fname);
85  return false;
86  }
```

node_modules/pgpass/lib/helper.js, line 215 (Password Management: Password in Comment) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: node_modules/pgpass/lib/helper.js:215
Taint Flags:

```
212  3 : function(x){
213  return x.length > 0;
214  } ,
```

Password Management: Password in Comment	Low
Package: node_modules.pgpass.lib	
node_modules/pgpass/lib/helper.js, line 215 (Password Management: Password in Comment)	Low

```
215  // password
216  4 : function(x){
217  return x.length > 0;
218  }
```

Path Manipulation (2 issues)

Abstract

允許使用者輸入來控制檔案系統操作中使用的路徑，可讓攻擊者存取或修改原本受保護的系統資源。

Explanation

當發生以下兩種情況的時候，會產生 path manipulation 錯誤： 1.攻擊者可以指定在檔案系統操作中所使用的路徑。 2. 攻擊者可藉由指定資源來取得一般情況下不被允許的權限。 例如，程式可能會讓攻擊者能夠覆寫指定的檔案，或是能夠在攻擊者控制的組態下執行。 **範例 1：**以下的程式碼使用 HTTP 要求的輸入建立一個檔案名稱。程式設計師沒有考慮到攻擊者能夠提供檔案名稱類似「`../../tomcat/conf/server.xml`」的可能性，這會導致應用程式刪除本身其中一個組態設定檔案。

```
rName = req.field('reportName')
rFile = os.open("/usr/local/apfr/reports/" + rName)
...
os.unlink(rFile);
```

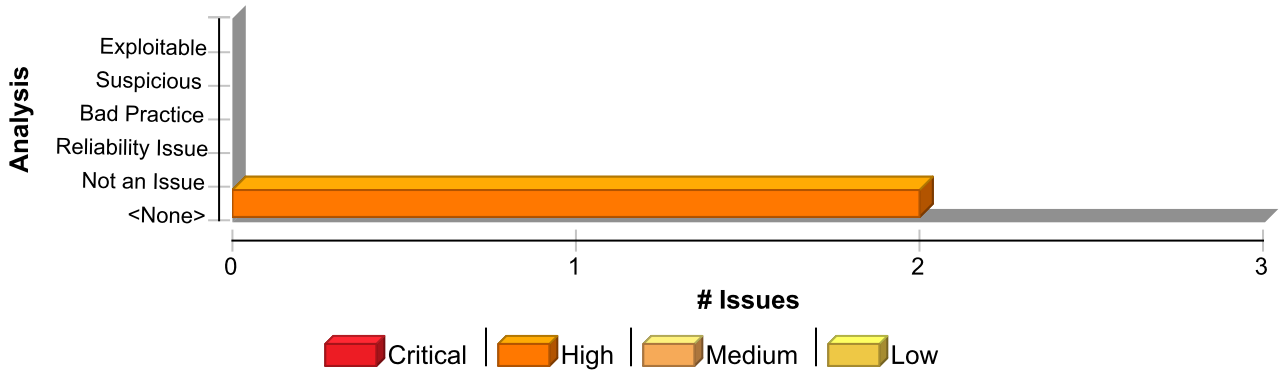
範例 2：以下程式碼使用來自配置檔案的輸入，來決定要開啟哪個檔案並返回給使用者。如果程式需要適當權限才能執行，且惡意使用者可以變更配置檔案，則他們可以使用程式來讀取系統中結尾副檔名為 `.txt` 的任意檔案。

```
...
filename = CONFIG_TXT['sub'] + ".txt";
handle = os.open(filename)
print handle
...
```

Recommendation

避免 Path Manipulation 的最佳方法是使用間接方法：建立合法值的清單，而使用者只能從清單中選取。使用此方法，使用者所提供的輸入就不會直接用來指定資源名稱。 但在某些情況下，這種方法是不切實際的，因為這樣一份合法資源名稱太過於龐大或是太難以維護。在這些情況下，程式設計師通常會實作拒絕清單。在使用輸入資料前，拒絕清單會選擇性的拒絕或避開可能有危險的字元。不過，任何此類不安全字元清單可能都不完整，並且幾乎肯定會過期。一個更好的方法是建立字元清單。此清單會列出允許出現於資源名稱中的字元，並僅接受由核准集中的字元組成的輸入。

Issue Summary



Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Path Manipulation	2	0	0	2
Total	**2**	**0**	**0**	**2**

Path Manipulation — High

Package: node_modules.node-gyp.gyp.tools.pretty_gyp

node_modules/node-gyp/gyp/tools/pretty_gyp.py, line 144 (Path Manipulation) — High

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: Read ~PythonGlobalsVar.sys.argv
From: node_modules.node-gyp.gyp.tools.pretty_gyp.main
File: node_modules/node-gyp/gyp/tools/pretty_gyp.py:144

```
141
142 def main():
143  if len(sys.argv) > 1:
144  data = open(sys.argv[1]).read().splitlines()
145  else:
146  data = sys.stdin.read().splitlines()
147  # Split up the double braces.
```

Sink Details

Sink: open()
Enclosing Method: main()
File: node_modules/node-gyp/gyp/tools/pretty_gyp.py:144
Taint Flags: ARGS

```
141
142 def main():
143  if len(sys.argv) > 1:
144  data = open(sys.argv[1]).read().splitlines()
145  else:
146  data = sys.stdin.read().splitlines()
147  # Split up the double braces.
```

Package: node_modules.node-gyp.gyp.tools.pretty_sln

node_modules/node-gyp/gyp/tools/pretty_sln.py, line 58 (Path Manipulation) — High

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: Read ~PythonGlobalsVar.sys.argv
From: node_modules.node-gyp.gyp.tools.pretty_sln.main
File: node_modules/node-gyp/gyp/tools/pretty_sln.py:171

```
168  print('Usage: %s "c:\\path\\to\\project.sln"' % sys.argv[0])
169  return 1
```

Path Manipulation — High

Package: node_modules.node-gyp.gyp.tools.pretty_sln

node_modules/node-gyp/gyp/tools/pretty_sln.py, line 58 (Path Manipulation) — High

```
170
171  (projects, deps) = ParseSolution(sys.argv[1])
172  PrintDependencies(projects, deps)
173  PrintBuildOrder(projects, deps)
174
```

Sink Details

Sink: open()
Enclosing Method: ParseSolution()
File: node_modules/node-gyp/gyp/tools/pretty_sln.py:58
Taint Flags: ARGS

```
55  dep_line = re.compile(" *({.*}) = ({.*})$")
56
57  in_deps = False
58  solution = open(solution_file)
59  for line in solution:
60  results = begin_project.search(line)
61  if results:
```

Poor Error Handling: Empty Catch Block (96 issues)

Abstract

忽略異常可能會導致程式忽略無法預期的狀態與情況。

Explanation

幾乎每一個對軟體系統嚴重的攻擊都是從破解程式設計師的假設開始的。在攻擊後，程式設計師所建立的假設似乎是脆弱且拙劣的，但在攻擊之前，許多程式設計師會在午休結束之前為他們的假設進行辯護。 在程式碼中很容易發現的兩個可疑假設為：「此方法呼叫永遠都不會失敗」以及「即使此呼叫失敗也沒有關係」。 因此當程式設計師忽略異常時，已暗示他們是以其中一個假設來執行操作。 **範例 1：**以下所引用的程式碼忽略了由 `open()` 拋出的罕見異常。

```
try:
    f = open('myfile.txt')
    s = f.readline()
    i = int(s.strip())
except:
   # This will never happen
   pass
```

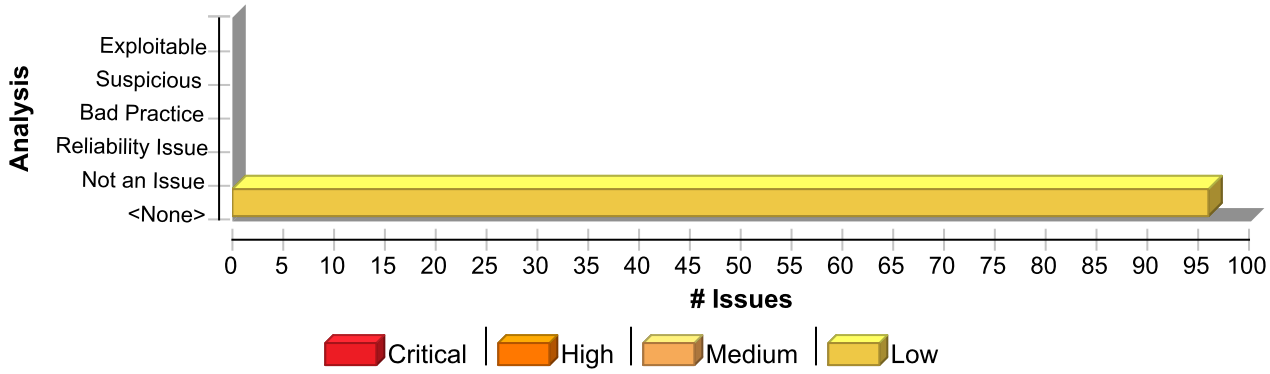
如果拋出了 `RareException`，程式會繼續執行，就像什麼都沒有發生過一樣。程式不會記錄有關此特殊情況，這將使得事後嘗試尋找程式此異常的運作方式變得很困難。

Recommendation

至少，應記錄所拋出的異常情況，可幫助事後回來檢查及得知對程式的運作方式造成的影響。然而，最好是中止目前的操作。如果因為呼叫者無法正確地處理而忽略某個異常，而程式環境使得呼叫者難以或者不可能聲明將會拋出異常，那麼可以考慮拋出 `RuntimeException` 異常或 `Error`，這兩者都是未經檢查的異常。 **範例 2：**`Example 1` 中的程式碼可以使用以下方式重寫：

```
try:
    f = open('myfile.txt')
    s = f.readline()
    i = int(s.strip())
except IOError as e:
    logging.error("I/O error({0}): {1}".format(e.errno, e.strerror))
except ValueError:
    logging.error("Could not convert data to an integer.")
except:
    logging.error("Unexpected error:", sys.exc_info()[0])
    raise
```

Issue Summary



Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Poor Error Handling: Empty Catch Block	96	0	0	96
Total	**96**	**0**	**0**	**96**

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.AppKit

.venv/lib/python3.13/site-packages/AppKit/__init__.py, line 213 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: _setup()
File: .venv/lib/python3.13/site-packages/AppKit/__init__.py:213
Taint Flags:

```
210  ]:
211  try:
212  globals_dict[nm] = chr(__getattr__(nm)) # noqa: F821
213  except AttributeError:
214  pass
215
216 undefined
```

Package: .venv.lib.python3.13.site-packages.PyObjCTools.KeyValueCoding

.venv/lib/python3.13/site-packages/PyObjCTools/KeyValueCoding.py, line 188 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.PyObjCTools.KeyValueCoding

.venv/lib/python3.13/site-packages/PyObjCTools/KeyValueCoding.py, line 188 (Poor Error Handling: Empty Catch Block) — Low

Sink: CatchBlock
Enclosing Method: getKey()
File: .venv/lib/python3.13/site-packages/PyObjCTools/KeyValueCoding.py:188
Taint Flags:

```
185  if getitem is not None:
186  try:
187  return getitem(key)
188  except (KeyError, IndexError, TypeError):
189  pass
190
191  # check for array-like objects
```

.venv/lib/python3.13/site-packages/PyObjCTools/KeyValueCoding.py, line 206 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: getKey()
File: .venv/lib/python3.13/site-packages/PyObjCTools/KeyValueCoding.py:206
Taint Flags:

```
203
204  try:
205  m = getattr(obj, "get" + keyCaps(key))
206  except AttributeError:
207  pass
208  else:
209  return m()
```

.venv/lib/python3.13/site-packages/PyObjCTools/KeyValueCoding.py, line 213 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: getKey()
File: .venv/lib/python3.13/site-packages/PyObjCTools/KeyValueCoding.py:213
Taint Flags:

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.PyObjCTools.KeyValueCoding

.venv/lib/python3.13/site-packages/PyObjCTools/KeyValueCoding.py, line 213 (Poor Error Handling: Empty Catch Block) — Low

```
210
211  try:
212  m = getattr(obj, "get_" + key)
213  except AttributeError:
214  pass
215  else:
216  return m()
```

.venv/lib/python3.13/site-packages/PyObjCTools/KeyValueCoding.py, line 276 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: setKey()
File: .venv/lib/python3.13/site-packages/PyObjCTools/KeyValueCoding.py:276
Taint Flags:

```
273  try:
274  m(value)
275  return
276  except TypeError:
277  pass
278
279  try:
```

.venv/lib/python3.13/site-packages/PyObjCTools/KeyValueCoding.py, line 281 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: setKey()
File: .venv/lib/python3.13/site-packages/PyObjCTools/KeyValueCoding.py:281
Taint Flags:

```
278
279  try:
280  m = getattr(obj, key)
281  except AttributeError:
```

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.PyObjCTools.KeyValueCoding

.venv/lib/python3.13/site-packages/PyObjCTools/KeyValueCoding.py, line 281 (Poor Error Handling: Empty Catch Block) — Low

```
282  pass
283
284  else:
```

.venv/lib/python3.13/site-packages/PyObjCTools/KeyValueCoding.py, line 298 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: setKey()
File: .venv/lib/python3.13/site-packages/PyObjCTools/KeyValueCoding.py:298
Taint Flags:

```
295
296  try:
297  getattr(obj, "_" + key)
298  except AttributeError:
299  pass
300  else:
301  setattr(obj, "_" + key, value)
```

Package: .venv.lib.python3.13.site-packages.bleak.backends.bluezdbus

.venv/lib/python3.13/site-packages/bleak/backends/bluezdbus/scanner.py, line 282 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
File: .venv/lib/python3.13/site-packages/bleak/backends/bluezdbus/scanner.py:282
Taint Flags:

```
279  try:
280  bdaddr = bdaddr_from_device_path(device_path)
281  del self.seen_devices[bdaddr]
282  except KeyError:
283  # The device will not have been added to self.seen_devices if no
284  # advertising data was received, so this is expected to happen
285  # occasionally.
```

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.objc

.venv/lib/python3.13/site-packages/objc/_context.py, line 45 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
File: .venv/lib/python3.13/site-packages/objc/_context.py:45
Taint Flags:

```
42  def unregister(self, value: Any):
43  try:
44  del self._registry[id(value)]
45  except KeyError:
46  pass
47
48  def get(self, uniq) -> Any:
```

Package: .venv.lib.python3.13.site-packages.objc._lazyimport

.venv/lib/python3.13/site-packages/objc/_lazyimport.py, line 409 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: load_cftypes()
File: .venv/lib/python3.13/site-packages/objc/_lazyimport.py:409
Taint Flags:

```
406  for nm in tollfree.split(","): # pragma: no branch
407  try:
408  objc.lookUpClass(nm)
409  except objc.error:
410  pass
411  else:
412  tollfree = nm
```

.venv/lib/python3.13/site-packages/objc/_lazyimport.py, line 418 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.objc._lazyimport

.venv/lib/python3.13/site-packages/objc/_lazyimport.py, line 418 (Poor Error Handling: Empty Catch Block) — Low

Sink Details

Sink: CatchBlock
Enclosing Method: load_cftypes()
File: .venv/lib/python3.13/site-packages/objc/_lazyimport.py:418
Taint Flags:

```
415  v = objc.registerCFSignature(name, typestr, None, tollfree)
416  globals_dict[name] = v
417  continue
418  except objc.nosuchclass_error:
419  pass
420
421  if gettypeid_func is None:
```

.venv/lib/python3.13/site-packages/objc/_lazyimport.py, line 378 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: get_constant()
File: .venv/lib/python3.13/site-packages/objc/_lazyimport.py:378
Taint Flags:

```
375  result = eval(info, {}, expressions_mapping)
376  expressions.pop(name)
377  return result
378  except: # noqa: E722, B001. Ignore all errors in evaluation the expression.
379  pass
380
381  if aliases:
```

.venv/lib/python3.13/site-packages/objc/_lazyimport.py, line 182 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: __getattr__()
File: .venv/lib/python3.13/site-packages/objc/_lazyimport.py:182

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.objc._lazyimport

.venv/lib/python3.13/site-packages/objc/_lazyimport.py, line 182 (Poor Error Handling: Empty Catch Block) — Low

Taint Flags:

```
179  value = getattr(p, name)
180  globals_dict[name] = value
181  return value
182  except AttributeError:
183  pass
184
185  if not _name_re.match(name):
```

.venv/lib/python3.13/site-packages/objc/_lazyimport.py, line 194 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: __getattr__()
File: .venv/lib/python3.13/site-packages/objc/_lazyimport.py:194
Taint Flags:

```
191  # the metadata files
192  try:
193  value = get_constant(name)
194  except AttributeError:
195  pass
196
197  else:
```

.venv/lib/python3.13/site-packages/objc/_lazyimport.py, line 204 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: __getattr__()
File: .venv/lib/python3.13/site-packages/objc/_lazyimport.py:204
Taint Flags:

```
201  # Then check if the name is class
202  try:
203  value = lookUpClass(name)
```

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.objc._lazyimport

.venv/lib/python3.13/site-packages/objc/_lazyimport.py, line 204 (Poor Error Handling: Empty Catch Block) — Low

```
204  except nosuchclass_error:
205  pass
206
207  else:
```

.venv/lib/python3.13/site-packages/objc/_lazyimport.py, line 225 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: calc_all()
File: .venv/lib/python3.13/site-packages/objc/_lazyimport.py:225
Taint Flags:

```
222  for nm in list(varmap_dct):
223  try:
224  expressions_mapping[nm]
225  except KeyError:
226  pass
227
228  varmap_dct.clear()
```

.venv/lib/python3.13/site-packages/objc/_lazyimport.py, line 248 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: calc_all()
File: .venv/lib/python3.13/site-packages/objc/_lazyimport.py:248
Taint Flags:

```
245  for nm, _val in re.findall(r"\$([A-Z0-9a-z_]*)@([^$]*)(?=\$)", enummap):
246  try:
247  expressions_mapping[nm]
248  except KeyError:
249  pass
250
251  enummap = ""
```

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.objc._lazyimport

.venv/lib/python3.13/site-packages/objc/_lazyimport.py, line 257 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: calc_all()
File: .venv/lib/python3.13/site-packages/objc/_lazyimport.py:257
Taint Flags:

```
254  for nm in list(funcmap):
255  try:
256  expressions_mapping[nm]
257  except KeyError:
258  pass
259
260  funcmap.clear()
```

.venv/lib/python3.13/site-packages/objc/_lazyimport.py, line 268 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: calc_all()
File: .venv/lib/python3.13/site-packages/objc/_lazyimport.py:268
Taint Flags:

```
265  for nm in list(expressions):
266  try:
267  expressions_mapping[nm]
268  except KeyError:
269  pass
270  expressions = []
271
```

.venv/lib/python3.13/site-packages/objc/_lazyimport.py, line 276 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.objc._lazyimport

.venv/lib/python3.13/site-packages/objc/_lazyimport.py, line 276 (Poor Error Handling: Empty Catch Block) — Low

Sink Details

Sink: CatchBlock
Enclosing Method: calc_all()
File: .venv/lib/python3.13/site-packages/objc/_lazyimport.py:276
Taint Flags:

```
273  for nm in list(aliases):
274  try:
275  expressions_mapping[nm]
276  except KeyError:
277  pass
278  aliases = []
279
```

Package: .venv.lib.python3.13.site-packages.objc._protocols

.venv/lib/python3.13/site-packages/objc/_protocols.py, line 21 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: protocolNamed()
File: .venv/lib/python3.13/site-packages/objc/_protocols.py:21
Taint Flags:

```
18  """
19  try:
20  return PROTOCOL_CACHE[name]
21  except KeyError:
22  pass
23  for p in _objc.protocolsForProcess():
24  pname = p.__name__
```

Package: .venv.lib.python3.13.site-packages.objc._pycoder

.venv/lib/python3.13/site-packages/objc/_pycoder.py, line 53 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.objc._pycoder

.venv/lib/python3.13/site-packages/objc/_pycoder.py, line 53 (Poor Error Handling: Empty Catch Block) — Low

Sink: CatchBlock
Enclosing Method: whichmodule()
File: .venv/lib/python3.13/site-packages/objc/_pycoder.py:53
Taint Flags:

```
50  if _getattribute(module, name) is obj:
51  return module_name
52
53  except AttributeError:
54  pass
55
56  return "__main__"
```

Package: .venv.lib.python3.13.site-packages.pip._vendor

.venv/lib/python3.13/site-packages/pip/_vendor/__init__.py, line 34 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: vendored()
File: .venv/lib/python3.13/site-packages/pip/_vendor/__init__.py:34
Taint Flags:

```
31
32  try:
33  __import__(modulename, globals(), locals(), level=0)
34  except ImportError:
35  # We can just silently allow import failures to pass here. If we
36  # got to this point it means that ``import pip._vendor.whatever``
37  # failed and so did ``import whatever``. Since we're importing this
```

Package: .venv.lib.python3.13.site-packages.pip._vendor.cachecontrol.filewrapper

.venv/lib/python3.13/site-packages/pip/_vendor/cachecontrol/filewrapper.py, line 56 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.pip._vendor.cachecontrol.filewrapper

.venv/lib/python3.13/site-packages/pip/_vendor/cachecontrol/filewrapper.py, line 56 (Poor Error Handling: Empty Catch Block) — Low

Enclosing Method: __is_fp_closed()
File: .venv/lib/python3.13/site-packages/pip/_vendor/cachecontrol/filewrapper.py:56
Taint Flags:

```
53  try:
54  return self.__fp.fp is None
55
56  except AttributeError:
57  pass
58
59  try:
```

.venv/lib/python3.13/site-packages/pip/_vendor/cachecontrol/filewrapper.py, line 63 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: __is_fp_closed()
File: .venv/lib/python3.13/site-packages/pip/_vendor/cachecontrol/filewrapper.py:63
Taint Flags:

```
60  closed: bool = self.__fp.closed
61  return closed
62
63  except AttributeError:
64  pass
65
66  # We just don't cache it then.
```

Package: .venv.lib.python3.13.site-packages.pip._vendor.distlib

.venv/lib/python3.13/site-packages/pip/_vendor/distlib/resources.py, line 302 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
File: .venv/lib/python3.13/site-packages/pip/_vendor/distlib/resources.py:302
Taint Flags:

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.pip._vendor.distlib

.venv/lib/python3.13/site-packages/pip/_vendor/distlib/resources.py, line 302 (Poor Error Handling: Empty Catch Block) — Low

```
299  # See issue #146
300  _finder_registry[_fi.SourcelessFileLoader] = ResourceFinder
301  del _fi
302 except (ImportError, AttributeError):
303  pass
304
305 undefined
```

.venv/lib/python3.13/site-packages/pip/_vendor/distlib/compat.py, line 656 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
File: .venv/lib/python3.13/site-packages/pip/_vendor/distlib/compat.py:656
Taint Flags:

```
653
654  try:
655  from _abcoll import KeysView, ValuesView, ItemsView
656  except ImportError:
657  pass
658
659  class OrderedDict(dict):
```

Package: .venv.lib.python3.13.site-packages.pip._vendor.distlib.compat

.venv/lib/python3.13/site-packages/pip/_vendor/distlib/compat.py, line 732 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: clear()
File: .venv/lib/python3.13/site-packages/pip/_vendor/distlib/compat.py:732
Taint Flags:

```
729  root = self.__root
730  root[:] = [root, root, None]
731  self.__map.clear()
732  except AttributeError:
```

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.pip._vendor.distlib.compat

.venv/lib/python3.13/site-packages/pip/_vendor/distlib/compat.py, line 732 (Poor Error Handling: Empty Catch Block) — Low

```
733  pass
734  dict.clear(self)
735
```

.venv/lib/python3.13/site-packages/pip/_vendor/distlib/compat.py, line 552 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: __getitem__()
File: .venv/lib/python3.13/site-packages/pip/_vendor/distlib/compat.py:552
Taint Flags:

```
549  try:
550  return mapping[
551  key] # can't use 'key in mapping' with defaultdict
552  except KeyError:
553  pass
554  return self.__missing__(
555  key) # support subclasses that define __missing__
```

Package: .venv.lib.python3.13.site-packages.pip._vendor.distlib.database

.venv/lib/python3.13/site-packages/pip/_vendor/distlib/database.py, line 433 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: matches_requirement()
File: .venv/lib/python3.13/site-packages/pip/_vendor/distlib/database.py:433
Taint Flags:

```
430  try:
431  result = matcher.match(p_ver)
432  break
433  except UnsupportedVersionError:
434  pass
435  return result
436
```

Poor Error Handling: Empty Catch Block	Low
Package: .venv.lib.python3.13.site-packages.pip._vendor.distlib.database	
.venv/lib/python3.13/site-packages/pip/_vendor/distlib/database.py, line 433 (Poor Error Handling: Empty Catch Block)	**Low**

Package: .venv.lib.python3.13.site-packages.pip._vendor.distlib.database.EggInfoDistribution

.venv/lib/python3.13/site-packages/pip/_vendor/distlib/database.py, line 919 (Poor Error Handling: Empty Catch Block) **Low**

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: parse_requires_path()
File: .venv/lib/python3.13/site-packages/pip/_vendor/distlib/database.py:919
Taint Flags:

```
916  try:
917  with codecs.open(req_path, 'r', 'utf-8') as fp:
918  reqs = parse_requires_data(fp.read())
919  except IOError:
920  pass
921  return reqs
922
```

Package: .venv.lib.python3.13.site-packages.pip._vendor.distlib.index

.venv/lib/python3.13/site-packages/pip/_vendor/distlib/index.py, line 63 (Poor Error Handling: Empty Catch Block) **Low**

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: __init__()
File: .venv/lib/python3.13/site-packages/pip/_vendor/distlib/index.py:63
Taint Flags:

```
60  if rc == 0:
61  self.gpg = s
62  break
63  except OSError:
64  pass
65
66  def _get_pypirc_command(self):
```

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.pip._vendor.distlib.locators

.venv/lib/python3.13/site-packages/pip/_vendor/distlib/locators.py, line 1050 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: get_distribution_names()
File: .venv/lib/python3.13/site-packages/pip/_vendor/distlib/locators.py:1050
Taint Flags:

```
1047  for locator in self.locators:
1048  try:
1049  result |= locator.get_distribution_names()
1050  except NotImplementedError:
1051  pass
1052  return result
1053
```

.venv/lib/python3.13/site-packages/pip/_vendor/distlib/locators.py, line 745 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: _fetch()
File: .venv/lib/python3.13/site-packages/pip/_vendor/distlib/locators.py:745
Taint Flags:

```
742  if (not self._process_download(link) and self._should_queue(link, url, rel)):
743  logger.debug('Queueing %s from %s', link, url)
744  self._to_fetch.put(link)
745  except MetadataInvalidError: # e.g. invalid versions
746  pass
747  except Exception as e: # pragma: no cover
748  self.errors.put(text_type(e))
```

Package: .venv.lib.python3.13.site-packages.pip._vendor.distlib.scripts

.venv/lib/python3.13/site-packages/pip/_vendor/distlib/scripts.py, line 301 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.pip._vendor.distlib.scripts

.venv/lib/python3.13/site-packages/pip/_vendor/distlib/scripts.py, line 301 (Poor Error Handling: Empty Catch Block) — Low

Sink Details

Sink: CatchBlock
Enclosing Method: _write_script()
File: .venv/lib/python3.13/site-packages/pip/_vendor/distlib/scripts.py:301
Taint Flags:

```
298   '.deleteme logic')
299   try:
300   os.remove(dfname)
301   except Exception:
302   pass # still in use - ignore error
303   else:
304   if self._is_nt and not outname.endswith('.' + ext): # pragma: no cover
```

Package: .venv.lib.python3.13.site-packages.pip._vendor.distlib.version

.venv/lib/python3.13/site-packages/pip/_vendor/distlib/version.py, line 481 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: _suggest_normalized_version()
File: .venv/lib/python3.13/site-packages/pip/_vendor/distlib/version.py:481
Taint Flags:

```
478   try:
479   _normalized_key(s)
480   return s # already rational
481   except UnsupportedVersionError:
482   pass
483
484   rs = s.lower()
```

Package: .venv.lib.python3.13.site-packages.pip._vendor.distlib.wheel

.venv/lib/python3.13/site-packages/pip/_vendor/distlib/wheel.py, line 772 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.pip._vendor.distlib.wheel

.venv/lib/python3.13/site-packages/pip/_vendor/distlib/wheel.py, line 772 (Poor Error Handling: Empty Catch Block) — Low

Sink: CatchBlock
Enclosing Method: _get_extensions()
File: .venv/lib/python3.13/site-packages/pip/_vendor/distlib/wheel.py:772
Taint Flags:

```
769  if extract:
770  zf.extract(relpath, cache_base)
771  result.append((name, dest))
772  except KeyError:
773  pass
774  return result
775
```

.venv/lib/python3.13/site-packages/pip/_vendor/distlib/wheel.py, line 275 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: metadata()
File: .venv/lib/python3.13/site-packages/pip/_vendor/distlib/wheel.py:275
Taint Flags:

```
272  result = Metadata(fileobj=wf)
273  if result:
274  break
275  except KeyError:
276  pass
277  if not result:
278  raise ValueError('Invalid wheel, because metadata is '
```

Package: .venv.lib.python3.13.site-packages.pip._vendor.platformdirs.windows

.venv/lib/python3.13/site-packages/pip/_vendor/platformdirs/windows.py, line 255 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: _pick_get_win_folder()
File: .venv/lib/python3.13/site-packages/pip/_vendor/platformdirs/windows.py:255

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.pip._vendor.platformdirs.windows

.venv/lib/python3.13/site-packages/pip/_vendor/platformdirs/windows.py, line 255 (Poor Error Handling: Empty Catch Block) — Low

Taint Flags:

```
252 def _pick_get_win_folder() -> Callable[[str], str]:
253  try:
254  import ctypes # noqa: PLC0415
255  except ImportError:
256  pass
257  else:
258  if hasattr(ctypes, "windll"):
```

Package: .venv.lib.python3.13.site-packages.pip._vendor.pygments.lexer

.venv/lib/python3.13/site-packages/pip/_vendor/pygments/lexer.py, line 646 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: get_tokendefs()
File: .venv/lib/python3.13/site-packages/pip/_vendor/pygments/lexer.py:646
Taint Flags:

```
643  # N.b. this is the index in items (that is, the superclass
644  # copy), so offset required when storing below.
645  new_inh_ndx = items.index(inherit)
646  except ValueError:
647  pass
648  else:
649  inheritable[state] = inherit_ndx + new_inh_ndx
```

Package: .venv.lib.python3.13.site-packages.pip._vendor.pygments.lexers

.venv/lib/python3.13/site-packages/pip/_vendor/pygments/lexers/__init__.py, line 328 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: guess_lexer()
File: .venv/lib/python3.13/site-packages/pip/_vendor/pygments/lexers/__init__.py:328
Taint Flags:

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.pip._vendor.pygments.lexers

.venv/lib/python3.13/site-packages/pip/_vendor/pygments/lexers/__init__.py, line 328 (Poor Error Handling: Empty Catch Block) — Low

```
325  if ft is not None:
326  try:
327  return get_lexer_by_name(ft, **options)
328  except ClassNotFound:
329  pass
330
331  best_lexer = [0.0, None]
```

Package: .venv.lib.python3.13.site-packages.pip._vendor.pygments.util

.venv/lib/python3.13/site-packages/pip/_vendor/pygments/util.py, line 306 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: guess_decode_from_terminal()
File: .venv/lib/python3.13/site-packages/pip/_vendor/pygments/util.py:306
Taint Flags:

```
303  if getattr(term, 'encoding', None):
304  try:
305  text = text.decode(term.encoding)
306  except UnicodeDecodeError:
307  pass
308  else:
309  return text, term.encoding
```

Package: .venv.lib.python3.13.site-packages.pip._vendor.requests

.venv/lib/python3.13/site-packages/pip/_vendor/requests/__init__.py, line 134 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
File: .venv/lib/python3.13/site-packages/pip/_vendor/requests/__init__.py:134
Taint Flags:

```
131  from cryptography import __version__ as cryptography_version
132
```

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.pip._vendor.requests

.venv/lib/python3.13/site-packages/pip/_vendor/requests/__init__.py, line 134 (Poor Error Handling: Empty Catch Block) — Low

```
133  _check_cryptography(cryptography_version)
134 except ImportError:
135  pass
136
137 # urllib3's DependencyWarnings should be silenced.
```

Package: .venv.lib.python3.13.site-packages.pip._vendor.urllib3

.venv/lib/python3.13/site-packages/pip/_vendor/urllib3/__init__.py, line 28 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
File: .venv/lib/python3.13/site-packages/pip/_vendor/urllib3/__init__.py:28
Taint Flags:

```
25 # See: https://github.com/urllib3/urllib3/issues/2680
26 try:
27  import urllib3_secure_extra # type: ignore # noqa: F401
28 except ImportError:
29  pass
30 else:
31  warnings.warn(
```

Package: .venv.lib.python3.13.site-packages.pip._vendor.urllib3._collections

.venv/lib/python3.13/site-packages/pip/_vendor/urllib3/_collections.py, line 212 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: discard()
File: .venv/lib/python3.13/site-packages/pip/_vendor/urllib3/_collections.py:212
Taint Flags:

```
209  def discard(self, key):
210  try:
211  del self[key]
212  except KeyError:
```

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.pip._vendor.urllib3._collections

.venv/lib/python3.13/site-packages/pip/_vendor/urllib3/_collections.py, line 212 (Poor Error Handling: Empty Catch Block) — Low

```
213  pass
214
215  def add(self, key, val):
```

Package: .venv.lib.python3.13.site-packages.pip._vendor.urllib3.connectionpool

.venv/lib/python3.13/site-packages/pip/_vendor/urllib3/connectionpool.py, line 1139 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: _close_pool_connections()
File: .venv/lib/python3.13/site-packages/pip/_vendor/urllib3/connectionpool.py:1139
Taint Flags:

```
1136  conn = pool.get(block=False)
1137  if conn:
1138  conn.close()
1139  except queue.Empty:
1140  pass # Done.
1141
1142 undefined
```

.venv/lib/python3.13/site-packages/pip/_vendor/urllib3/connectionpool.py, line 421 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: _make_request()
File: .venv/lib/python3.13/site-packages/pip/_vendor/urllib3/connectionpool.py:421
Taint Flags:

```
418  # We are swallowing BrokenPipeError (errno.EPIPE) since the server is
419  # legitimately able to close the connection after sending a valid response.
420  # With this behaviour, the received response is still readable.
421  except BrokenPipeError:
422  # Python 3
423  pass
424  except IOError as e:
```

Poor Error Handling: Empty Catch Block	Low
Package: .venv.lib.python3.13.site-packages.pip._vendor.urllib3.connectionpool	
.venv/lib/python3.13/site-packages/pip/_vendor/urllib3/connectionpool.py, line 421 (Poor Error Handling: Empty Catch Block)	**Low**

.venv/lib/python3.13/site-packages/pip/_vendor/urllib3/connectionpool.py, line 318 (Poor Error Handling: Empty Catch Block) **Low**

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: _put_conn()
File: .venv/lib/python3.13/site-packages/pip/_vendor/urllib3/connectionpool.py:318
Taint Flags:

```
315  try:
316  self.pool.put(conn, block=False)
317  return # Everything is dandy, done.
318  except AttributeError:
319  # self.pool is None.
320  pass
321  except queue.Full:
```

Package: .venv.lib.python3.13.site-packages.pip._vendor.urllib3.contrib._securetransport

.venv/lib/python3.13/site-packages/pip/_vendor/urllib3/contrib/_securetransport/bindings.py, line 301 (Poor Error Handling: Empty Catch Block) **Low**

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
File: .venv/lib/python3.13/site-packages/pip/_vendor/urllib3/contrib/_securetransport/bindings.py:301
Taint Flags:

```
298  try:
299  Security.SSLSetALPNProtocols.argtypes = [SSLContextRef, CFArrayRef]
300  Security.SSLSetALPNProtocols.restype = OSStatus
301  except AttributeError:
302  # Supported only in 10.12+
303  pass
304
```

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.pip._vendor.urllib3.fields

.venv/lib/python3.13/site-packages/pip/_vendor/urllib3/fields.py, line 47 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: format_header_param_rfc2231()
File: .venv/lib/python3.13/site-packages/pip/_vendor/urllib3/fields.py:47
Taint Flags:

```
44  result = u'%s="%s"' % (name, value)
45  try:
46  result.encode("ascii")
47  except (UnicodeEncodeError, UnicodeDecodeError):
48  pass
49  else:
50  return result
```

Package: .venv.lib.python3.13.site-packages.pip._vendor.urllib3.packages.six

.venv/lib/python3.13/site-packages/pip/_vendor/urllib3/packages/six.py, line 205 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: load_module()
File: .venv/lib/python3.13/site-packages/pip/_vendor/urllib3/packages/six.py:205
Taint Flags:

```
202  try:
203  # in case of a reload
204  return sys.modules[fullname]
205  except KeyError:
206  pass
207  mod = self.__get_module(fullname)
208  if isinstance(mod, MovedModule):
```

.venv/lib/python3.13/site-packages/pip/_vendor/urllib3/packages/six.py, line 102 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.pip._vendor.urllib3.packages.six

.venv/lib/python3.13/site-packages/pip/_vendor/urllib3/packages/six.py, line 102 (Poor Error Handling: Empty Catch Block) — **Low**

Sink Details

Sink: CatchBlock
Enclosing Method: __get__()
File: .venv/lib/python3.13/site-packages/pip/_vendor/urllib3/packages/six.py:102
Taint Flags:

```
99  # This is a bit ugly, but it avoids running this again by
100  # removing this descriptor.
101  delattr(obj.__class__, self.name)
102  except AttributeError:
103  pass
104  return result
105
```

Package: .venv.lib.python3.13.site-packages.pip._vendor.urllib3.poolmanager

.venv/lib/python3.13/site-packages/pip/_vendor/urllib3/poolmanager.py, line 317 (Poor Error Handling: Empty Catch Block) — **Low**

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: _merge_pool_kwargs()
File: .venv/lib/python3.13/site-packages/pip/_vendor/urllib3/poolmanager.py:317
Taint Flags:

```
314  if value is None:
315  try:
316  del base_pool_kwargs[key]
317  except KeyError:
318  pass
319  else:
320  base_pool_kwargs[key] = value
```

Package: .venv.lib.python3.13.site-packages.pip._vendor.urllib3.response

.venv/lib/python3.13/site-packages/pip/_vendor/urllib3/response.py, line 290 (Poor Error Handling: Empty Catch Block) — **Low**

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.pip._vendor.urllib3.response

.venv/lib/python3.13/site-packages/pip/_vendor/urllib3/response.py, line 290 (Poor Error Handling: Empty Catch Block) — Low

Sink: CatchBlock
Enclosing Method: drain_conn()
File: .venv/lib/python3.13/site-packages/pip/_vendor/urllib3/response.py:290
Taint Flags:

```
287  """
288  try:
289  self.read()
290  except (HTTPError, SocketError, BaseSSLError, HTTPException):
291  pass
292
293  @property
```

Package: .venv.lib.python3.13.site-packages.pip._vendor.urllib3.util

.venv/lib/python3.13/site-packages/pip/_vendor/urllib3/util/wait.py, line 8 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
File: .venv/lib/python3.13/site-packages/pip/_vendor/urllib3/util/wait.py:8
Taint Flags:

```
5
6 try:
7  from time import monotonic
8 except ImportError:
9  from time import time as monotonic
10
11 __all__ = ["NoWayToWaitForSocketError", "wait_for_read", "wait_for_write"]
```

.venv/lib/python3.13/site-packages/pip/_vendor/urllib3/util/ssl_.py, line 51 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
File: .venv/lib/python3.13/site-packages/pip/_vendor/urllib3/util/ssl_.py:51
Taint Flags:

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.pip._vendor.urllib3.util

.venv/lib/python3.13/site-packages/pip/_vendor/urllib3/util/ssl_.py, line 51 (Poor Error Handling: Empty Catch Block) — Low

```
48 try: # Test for SSL features
49  import ssl
50  from ssl import CERT_REQUIRED, wrap_socket
51 except ImportError:
52  pass
53
54 try:
```

.venv/lib/python3.13/site-packages/pip/_vendor/urllib3/util/ssl_.py, line 56 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
File: .venv/lib/python3.13/site-packages/pip/_vendor/urllib3/util/ssl_.py:56
Taint Flags:

```
53
54 try:
55  from ssl import HAS_SNI # Has SNI?
56 except ImportError:
57  pass
58
59 try:
```

.venv/lib/python3.13/site-packages/pip/_vendor/urllib3/util/ssl_.py, line 61 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
File: .venv/lib/python3.13/site-packages/pip/_vendor/urllib3/util/ssl_.py:61
Taint Flags:

```
58
59 try:
60  from .ssltransport import SSLTransport
61 except ImportError:
62  pass
63
```

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.pip._vendor.urllib3.util

.venv/lib/python3.13/site-packages/pip/_vendor/urllib3/util/ssl_.py, line 61 (Poor Error Handling: Empty Catch Block) — Low

```
64
```

Package: .venv.lib.python3.13.site-packages.pip._vendor.urllib3.util.connection

.venv/lib/python3.13/site-packages/pip/_vendor/urllib3/util/connection.py, line 141 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: _has_ipv6()
File: .venv/lib/python3.13/site-packages/pip/_vendor/urllib3/util/connection.py:141
Taint Flags:

```
138  sock = socket.socket(socket.AF_INET6)
139  sock.bind((host, 0))
140  has_ipv6 = True
141  except Exception:
142  pass
143
144  if sock:
```

Package: .venv.lib.python3.13.site-packages.pip._vendor.urllib3.util.response

.venv/lib/python3.13/site-packages/pip/_vendor/urllib3/util/response.py, line 21 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: is_fp_closed()
File: .venv/lib/python3.13/site-packages/pip/_vendor/urllib3/util/response.py:21
Taint Flags:

```
18  # Check `isclosed()` first, in case Python3 doesn't set `closed`.
19  # GH Issue #928
20  return obj.isclosed()
21  except AttributeError:
22  pass
23
24  try:
```

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.pip._vendor.urllib3.util.response

.venv/lib/python3.13/site-packages/pip/_vendor/urllib3/util/response.py, line 27 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: is_fp_closed()
File: .venv/lib/python3.13/site-packages/pip/_vendor/urllib3/util/response.py:27
Taint Flags:

```
24  try:
25  # Check via the official file-like-object way.
26  return obj.closed
27  except AttributeError:
28  pass
29
30  try:
```

.venv/lib/python3.13/site-packages/pip/_vendor/urllib3/util/response.py, line 34 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: is_fp_closed()
File: .venv/lib/python3.13/site-packages/pip/_vendor/urllib3/util/response.py:34
Taint Flags:

```
31  # Check if the object is a container for another file-like object that
32  # gets released on exhaustion (e.g. HTTPResponse).
33  return obj.fp is None
34  except AttributeError:
35  pass
36
37  raise ValueError("Unable to determine whether fp is closed.")
```

Package: .venv.lib.python3.13.site-packages.pip._vendor.urllib3.util.ssl_

.venv/lib/python3.13/site-packages/pip/_vendor/urllib3/util/ssl_.py, line 434 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.pip._vendor.urllib3.util.ssl_

.venv/lib/python3.13/site-packages/pip/_vendor/urllib3/util/ssl_.py, line 434 (Poor Error Handling: Empty Catch Block) — Low

Sink Details

Sink: CatchBlock
Enclosing Method: ssl_wrap_socket()
File: .venv/lib/python3.13/site-packages/pip/_vendor/urllib3/util/ssl_.py:434
Taint Flags:

```
431  try:
432  if hasattr(context, "set_alpn_protocols"):
433  context.set_alpn_protocols(ALPN_PROTOCOLS)
434  except NotImplementedError: # Defensive: in CI, we always have set_alpn_protocols
435  pass
436
437  # If we detect server_hostname is an IP address then the SNI
```

Package: .venv.lib.python3.13.site-packages.psutil._psosx

.venv/lib/python3.13/site-packages/psutil/_psosx.py, line 320 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: pids()
File: .venv/lib/python3.13/site-packages/psutil/_psosx.py:320
Taint Flags:

```
317  try:
318  Process(0).create_time()
319  ls.insert(0, 0)
320  except NoSuchProcess:
321  pass
322  except AccessDenied:
323  ls.insert(0, 0)
```

Package: .venv.lib.python3.13.site-packages.psutil._psposix

.venv/lib/python3.13/site-packages/psutil/_psposix.py, line 205 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.psutil._psposix

.venv/lib/python3.13/site-packages/psutil/_psposix.py, line 205 (Poor Error Handling: Empty Catch Block) — Low

Sink: CatchBlock
Enclosing Method: get_terminal_map()
File: .venv/lib/python3.13/site-packages/psutil/_psposix.py:205
Taint Flags:

```
202  assert name not in ret, name
203  try:
204  ret[os.stat(name).st_rdev] = name
205  except FileNotFoundError:
206  pass
207  return ret
208
```

Package: .venv.lib.python3.13.site-packages.psutil.tests.test_bsd

.venv/lib/python3.13/site-packages/psutil/tests/test_bsd.py, line 148 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: test_net_if_stats()
File: .venv/lib/python3.13/site-packages/psutil/tests/test_bsd.py:148
Taint Flags:

```
145  for name, stats in psutil.net_if_stats().items():
146  try:
147  out = sh(f"ifconfig {name}")
148  except RuntimeError:
149  pass
150  else:
151  assert stats.isup == ('RUNNING' in out)
```

Package: .venv.lib.python3.13.site-packages.psutil.tests.test_memleaks

.venv/lib/python3.13/site-packages/psutil/tests/test_memleaks.py, line 290 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.psutil.tests.test_memleaks

.venv/lib/python3.13/site-packages/psutil/tests/test_memleaks.py, line 290 (Poor Error Handling: Empty Catch Block) — Low

Enclosing Method: call()
File: .venv/lib/python3.13/site-packages/psutil/tests/test_memleaks.py:290
Taint Flags:

```
287  def call(self, fun):
288  try:
289  fun()
290  except psutil.NoSuchProcess:
291  pass
292
293  if WINDOWS:
```

Package: .venv.lib.python3.13.site-packages.psutil.tests.test_memleaks.TestTerminatedProcessLeaks

.venv/lib/python3.13/site-packages/psutil/tests/test_memleaks.py, line 315 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: call()
File: .venv/lib/python3.13/site-packages/psutil/tests/test_memleaks.py:315
Taint Flags:

```
312  def call():
313  try:
314  return cext.proc_info(self.proc.pid)
315  except ProcessLookupError:
316  pass
317
318  self.execute(call)
```

Package: .venv.lib.python3.13.site-packages.psutil.tests.test_misc

.venv/lib/python3.13/site-packages/psutil/tests/test_misc.py, line 260 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.psutil.tests.test_misc

.venv/lib/python3.13/site-packages/psutil/tests/test_misc.py, line 260 (Poor Error Handling: Empty Catch Block) — Low

Enclosing Method: test_serialization()
File: .venv/lib/python3.13/site-packages/psutil/tests/test_misc.py:260
Taint Flags:

```
257  with self.subTest(proc=proc, name=name):
258  try:
259  ret = fun()
260  except psutil.Error:
261  pass
262  else:
263  check(ret)
```

.venv/lib/python3.13/site-packages/psutil/tests/test_misc.py, line 274 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: test_serialization()
File: .venv/lib/python3.13/site-packages/psutil/tests/test_misc.py:274
Taint Flags:

```
271  with self.subTest(name=name):
272  try:
273  ret = fun()
274  except psutil.AccessDenied:
275  pass
276  else:
277  check(ret)
```

Package: .venv.lib.python3.13.site-packages.psutil.tests.test_osx

.venv/lib/python3.13/site-packages/psutil/tests/test_osx.py, line 181 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: test_net_if_stats()
File: .venv/lib/python3.13/site-packages/psutil/tests/test_osx.py:181
Taint Flags:

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.psutil.tests.test_osx

.venv/lib/python3.13/site-packages/psutil/tests/test_osx.py, line 181 (Poor Error Handling: Empty Catch Block) — Low

```
178  for name, stats in psutil.net_if_stats().items():
179  try:
180  out = sh(f"ifconfig {name}")
181  except RuntimeError:
182  pass
183  else:
184  assert stats.isup == ('RUNNING' in out), out
```

Package: .venv.lib.python3.13.site-packages.psutil.tests.test_process_all

.venv/lib/python3.13/site-packages/psutil/tests/test_process_all.py, line 346 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: open_files()
File: .venv/lib/python3.13/site-packages/psutil/tests/test_process_all.py:346
Taint Flags:

```
343  assert os.path.isabs(f.path), f
344  try:
345  st = os.stat(f.path)
346  except FileNotFoundError:
347  pass
348  else:
349  assert stat.S_ISREG(st.st_mode), f
```

Package: .venv.lib.python3.13.site-packages.psutil.tests.test_testutils

.venv/lib/python3.13/site-packages/psutil/tests/test_testutils.py, line 541 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: test_warns()
File: .venv/lib/python3.13/site-packages/psutil/tests/test_testutils.py:541
Taint Flags:

```
538  try:
```

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.psutil.tests.test_testutils

.venv/lib/python3.13/site-packages/psutil/tests/test_testutils.py, line 541 (Poor Error Handling: Empty Catch Block) — Low

```
539  with fake_pytest.warns(UserWarning):
540  warnings.warn("foo", DeprecationWarning, stacklevel=1)
541  except AssertionError:
542  pass
543  else:
544  raise self.fail("exception not raised")
```

.venv/lib/python3.13/site-packages/psutil/tests/test_testutils.py, line 554 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: test_warns()
File: .venv/lib/python3.13/site-packages/psutil/tests/test_testutils.py:554
Taint Flags:

```
551  try:
552  with fake_pytest.warns(UserWarning, match="foo"):
553  warnings.warn("bar", UserWarning, stacklevel=1)
554  except AssertionError:
555  pass
556  else:
557  raise self.fail("exception not raised")
```

Package: .venv.lib.python3.13.site-packages.qrcode.compat

.venv/lib/python3.13/site-packages/qrcode/compat/png.py, line 6 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
File: .venv/lib/python3.13/site-packages/qrcode/compat/png.py:6
Taint Flags:

```
3
4 try:
5  from png import Writer as PngWriter # type: ignore # noqa: F401
6 except ImportError: # pragma: no cover
7  pass
```

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.qrcode.compat

.venv/lib/python3.13/site-packages/qrcode/compat/png.py, line 6 (Poor Error Handling: Empty Catch Block) — Low

```
8
9 undefined
```

Package: .venv.lib.python3.13.site-packages.qrcode.image.pil

.venv/lib/python3.13/site-packages/qrcode/image/pil.py, line 21 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: new_image()
File: .venv/lib/python3.13/site-packages/qrcode/image/pil.py:21
Taint Flags:

```
18
19  try:
20  fill_color = fill_color.lower()
21  except AttributeError:
22  pass
23
24  try:
```

.venv/lib/python3.13/site-packages/qrcode/image/pil.py, line 26 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: new_image()
File: .venv/lib/python3.13/site-packages/qrcode/image/pil.py:26
Taint Flags:

```
23
24  try:
25  back_color = back_color.lower()
26  except AttributeError:
27  pass
28
29  # L mode (1 mode) color = (r*299 + g*587 + b*114)//1000
```

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.qrcode.image.styles.moduledrawers

.venv/lib/python3.13/site-packages/qrcode/image/styles/moduledrawers/__init__.py, line 9 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
File: .venv/lib/python3.13/site-packages/qrcode/image/styles/moduledrawers/__init__.py:9
Taint Flags:

```
6  from .pil import RoundedModuleDrawer # noqa: F401
7  from .pil import SquareModuleDrawer # noqa: F401
8  from .pil import VerticalBarsDrawer # noqa: F401
9 except ImportError:
10  pass
11
12 undefined
```

Package: .venv.lib.python3.13.site-packages.qrcode.image.svg

.venv/lib/python3.13/site-packages/qrcode/image/svg.py, line 47 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: units()
File: .venv/lib/python3.13/site-packages/qrcode/image/svg.py:47
Taint Flags:

```
44  try:
45  for d in (Decimal("0.01"), Decimal("0.1"), Decimal("0")):
46  units = units.quantize(d, context=context)
47  except decimal.Inexact:
48  pass
49  return f"{units}mm"
50
```

Package: .venv.lib.python3.13.site-packages.requests

.venv/lib/python3.13/site-packages/requests/__init__.py, line 139 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.requests

.venv/lib/python3.13/site-packages/requests/__init__.py, line 139 (Poor Error Handling: Empty Catch Block) — Low

Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
File: .venv/lib/python3.13/site-packages/requests/__init__.py:139
Taint Flags:

```
136  from cryptography import __version__ as cryptography_version
137
138  _check_cryptography(cryptography_version)
139 except ImportError:
140  pass
141
142 # urllib3's DependencyWarnings should be silenced.
```

Package: .venv.lib.python3.13.site-packages.requests.compat

.venv/lib/python3.13/site-packages/requests/compat.py, line 25 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: _resolve_char_detection()
File: .venv/lib/python3.13/site-packages/requests/compat.py:25
Taint Flags:

```
22  if chardet is None:
23  try:
24  chardet = importlib.import_module(lib)
25  except ImportError:
26  pass
27  return chardet
28
```

Package: .venv.lib.python3.13.site-packages.urllib3.util

.venv/lib/python3.13/site-packages/urllib3/util/response.py, line 21 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.urllib3.util

.venv/lib/python3.13/site-packages/urllib3/util/response.py, line 21 (Poor Error Handling: Empty Catch Block) — Low

Sink Details

Sink: CatchBlock
File: .venv/lib/python3.13/site-packages/urllib3/util/response.py:21
Taint Flags:

```
18  # Check `isclosed()` first, in case Python3 doesn't set `closed`.
19  # GH Issue #928
20  return obj.isclosed() # type: ignore[no-any-return, attr-defined]
21  except AttributeError:
22  pass
23
24  try:
```

.venv/lib/python3.13/site-packages/urllib3/util/response.py, line 27 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
File: .venv/lib/python3.13/site-packages/urllib3/util/response.py:27
Taint Flags:

```
24  try:
25  # Check via the official file-like-object way.
26  return obj.closed # type: ignore[no-any-return, attr-defined]
27  except AttributeError:
28  pass
29
30  try:
```

.venv/lib/python3.13/site-packages/urllib3/util/response.py, line 34 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
File: .venv/lib/python3.13/site-packages/urllib3/util/response.py:34
Taint Flags:

```
31  # Check if the object is a container for another file-like object that
32  # gets released on exhaustion (e.g. HTTPResponse).
```

Poor Error Handling: Empty Catch Block — Low

Package: .venv.lib.python3.13.site-packages.urllib3.util

.venv/lib/python3.13/site-packages/urllib3/util/response.py, line 34 (Poor Error Handling: Empty Catch Block) — Low

```
33  return obj.fp is None # type: ignore[attr-defined]
34  except AttributeError:
35  pass
36
37  raise ValueError("Unable to determine whether fp is closed.")
```

Package: VisualStudioConfiguration

frontend/node_modules/node-gyp/lib/Find-VisualStudio.cs, line 212 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: PrintJson()
File: frontend/node_modules/node-gyp/lib/Find-VisualStudio.cs:212
Taint Flags:

```
209  {
210  instances.Add(InstanceJson(rgelt[0]));
211  }
212  catch (COMException)
213  {
214  // Ignore instances that can't be queried.
215  }
```

node_modules/node-gyp/lib/Find-VisualStudio.cs, line 212 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: PrintJson()
File: node_modules/node-gyp/lib/Find-VisualStudio.cs:212
Taint Flags:

```
209  {
210  instances.Add(InstanceJson(rgelt[0]));
211  }
212  catch (COMException)
213  {
```

Poor Error Handling: Empty Catch Block — Low

Package: VisualStudioConfiguration

node_modules/node-gyp/lib/Find-VisualStudio.cs, line 212 (Poor Error Handling: Empty Catch Block) — Low

```
214  // Ignore instances that can't be queried.
215  }
```

Package: frontend.node_modules.node-gyp.gyp.pylib.gyp.MSVSVersion

frontend/node_modules/node-gyp/gyp/pylib/gyp/MSVSVersion.py, line 248 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: _RegistryGetValue()
File: frontend/node_modules/node-gyp/gyp/pylib/gyp/MSVSVersion.py:248
Taint Flags:

```
245  """
246  try:
247  return _RegistryGetValueUsingWinReg(key, value)
248  except ImportError:
249  pass
250
251  # Fallback to reg.exe if we fail to import _winreg.
```

Package: frontend.node_modules.node-gyp.gyp.pylib.gyp.common

frontend/node_modules/node-gyp/gyp/pylib/gyp/common.py, line 423 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: EnsureDirExists()
File: frontend/node_modules/node-gyp/gyp/pylib/gyp/common.py:423
Taint Flags:

```
420  """Make sure the directory for |path| exists."""
421  try:
422  os.makedirs(os.path.dirname(path))
423  except OSError:
424  pass
425
```

Poor Error Handling: Empty Catch Block — Low

Package: frontend.node_modules.node-gyp.gyp.pylib.gyp.common

frontend/node_modules/node-gyp/gyp/pylib/gyp/common.py, line 423 (Poor Error Handling: Empty Catch Block) — Low

```
426 def GetCrossCompilerPredefines(): # -> dict
```

Package: frontend.node_modules.node-gyp.gyp.pylib.gyp.generator.compile_commands_json

frontend/node_modules/node-gyp/gyp/pylib/gyp/generator/compile_commands_json.py, line 116 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: GenerateOutput()
File: frontend/node_modules/node-gyp/gyp/pylib/gyp/generator/compile_commands_json.py:116
Taint Flags:

```
113  # generator_output can be `None` on Windows machines, or even not
114  # defined in other cases
115  output_dir = params.get("options").generator_output
116  except AttributeError:
117  pass
118  output_dir = output_dir or params["generator_flags"].get("output_dir", "out")
119  for configuration_name, commands in per_config_commands.items():
```

Package: frontend.node_modules.node-gyp.gyp.pylib.gyp.xcode_ninja

frontend/node_modules/node-gyp/gyp/pylib/gyp/xcode_ninja.py, line 50 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: _WriteWorkspace()
File: frontend/node_modules/node-gyp/gyp/pylib/gyp/xcode_ninja.py:50
Taint Flags:

```
47  input_string = input_file.read()
48  if input_string == output_string:
49  return
50  except OSError:
51  # Ignore errors if the file doesn't exist.
52  pass
53
```

Poor Error Handling: Empty Catch Block — Low

Package: node_modules.node-gyp.gyp.pylib.gyp

node_modules/node-gyp/gyp/pylib/gyp/__init__.py, line 34 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: DebugOutput()
File: node_modules/node-gyp/gyp/pylib/gyp/__init__.py:34
Taint Flags:

```
31  f = traceback.extract_stack(limit=2)
32  if f:
33  ctx = f[0][:3]
34  except Exception:
35  pass
36  if args:
37  message %= args
```

Package: node_modules.node-gyp.gyp.pylib.gyp.MSVSVersion

node_modules/node-gyp/gyp/pylib/gyp/MSVSVersion.py, line 248 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: _RegistryGetValue()
File: node_modules/node-gyp/gyp/pylib/gyp/MSVSVersion.py:248
Taint Flags:

```
245  """
246  try:
247  return _RegistryGetValueUsingWinReg(key, value)
248  except ImportError:
249  pass
250
251  # Fallback to reg.exe if we fail to import _winreg.
```

Package: node_modules.node-gyp.gyp.pylib.gyp.common

node_modules/node-gyp/gyp/pylib/gyp/common.py, line 429 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Poor Error Handling: Empty Catch Block — Low

Package: node_modules.node-gyp.gyp.pylib.gyp.common

node_modules/node-gyp/gyp/pylib/gyp/common.py, line 429 (Poor Error Handling: Empty Catch Block) — Low

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: EnsureDirExists()
File: node_modules/node-gyp/gyp/pylib/gyp/common.py:429
Taint Flags:

```
426  """Make sure the directory for |path| exists."""
427  try:
428  os.makedirs(os.path.dirname(path))
429  except OSError:
430  pass
431
432 undefined
```

Package: node_modules.node-gyp.gyp.pylib.gyp.xcode_ninja

node_modules/node-gyp/gyp/pylib/gyp/xcode_ninja.py, line 50 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: _WriteWorkspace()
File: node_modules/node-gyp/gyp/pylib/gyp/xcode_ninja.py:50
Taint Flags:

```
47  input_string = input_file.read()
48  if input_string == output_string:
49  return
50  except OSError:
51  # Ignore errors if the file doesn't exist.
52  pass
53
```

Package: node_modules.node-gyp.test.fixtures

node_modules/node-gyp/test/fixtures/test-charmap.py, line 6 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors

Poor Error Handling: Empty Catch Block — Low

Package: node_modules.node-gyp.test.fixtures

node_modules/node-gyp/test/fixtures/test-charmap.py, line 6 (Poor Error Handling: Empty Catch Block) — Low

Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
File: node_modules/node-gyp/test/fixtures/test-charmap.py:6
Taint Flags:

```
3
4 try:
5  reload(sys)
6 except NameError: # Python 3
7  pass
8
9
```

Package: node_modules.node-gyp.test.fixtures.test-charmap

node_modules/node-gyp/test/fixtures/test-charmap.py, line 17 (Poor Error Handling: Empty Catch Block) — Low

Issue Details

Kingdom: Errors
Scan Engine: SCA (Structural)

Sink Details

Sink: CatchBlock
Enclosing Method: main()
File: node_modules/node-gyp/test/fixtures/test-charmap.py:17
Taint Flags:

```
14
15  try:
16  sys.setdefaultencoding(encoding)
17  except AttributeError: # Python 3
18  pass
19
20  textmap = {
```

Poor Logging Practice: Use of a System Output Stream (10 issues)

Abstract

使用標準輸出或標準錯誤而不使用專用的記錄工具，會使得監控程式的運作方式變得非常困難。

Explanation

範例 1：開發者學習撰寫的第一個 Python 程式通常如下所示：

```
sys.stdout.write("hello world")
```

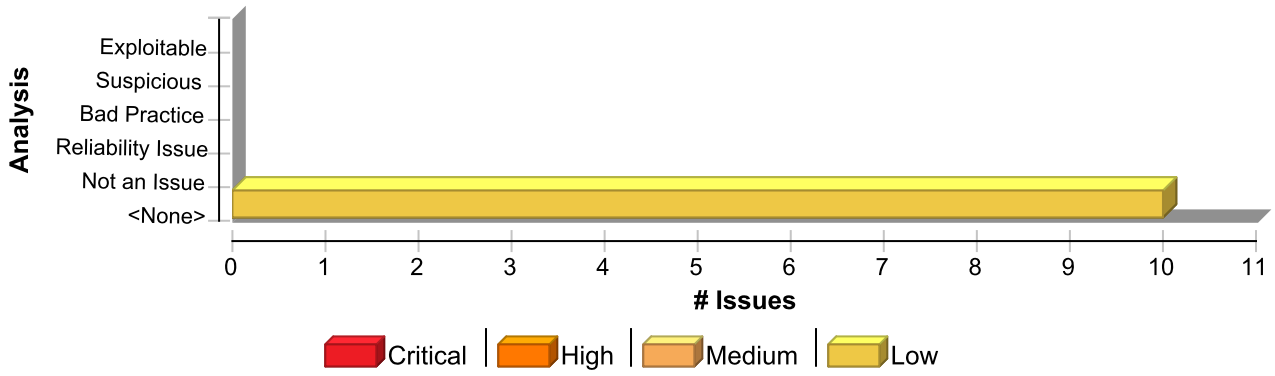
當大多數的程式設計師繼續學習許多關於 Python 的細微之處時，有一部分人仍僅依賴這些基本知識，撰寫訊息以執行標準輸出。 問題是，直接在標準輸出或標準錯誤中寫入資訊，通常是用來當做沒有結構的記錄格式。結構化的記錄工具提供了各種功能，如記錄層級、統一的格式化、記錄識別碼、時間戳記，另外可能是最重要的，將記錄訊息引導至正確位置的功能。當系統輸出串流的使用與正確使用記錄功能的程式碼混合在一起，得出的結果通常是一個保存良好但缺少重要資訊的記錄檔。 開發人員廣泛地認同對結構化記錄的需求，但很多人仍然繼續在程式開發前使用系統輸出串流功能。如果您正在檢閱的程式碼已過了程式開發的初始階段，使用 `sys.stdout` 或 `sys.stderr` 可能會在轉向結構化記錄系統時產生一個錯誤。

Recommendation

使用 Python 記錄功能，而不使用 `sys.stdout` 或 `sys.stderr`。 **範例 2：**例如，`Example 1` 中的「hello world」程式可以使用 `logging` 模組重寫，如下所示：

```
import logging
logging.debug("hello world")
```

Issue Summary



Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Poor Logging Practice: Use of a System Output Stream	10	0	0	10
Total	**10**	**0**	**0**	**10**

Poor Logging Practice: Use of a System Output Stream	**Low**
Package: .venv.lib.python3.13.site-packages.pip._internal.commands.completion	
.venv/lib/python3.13/site-packages/pip/_internal/commands/completion.py, line 133 (Poor Logging Practice: Use of a System Output Stream)	**Low**
Issue Details	

Poor Logging Practice: Use of a System Output Stream — Low

Package: .venv.lib.python3.13.site-packages.pip._internal.commands.completion

.venv/lib/python3.13/site-packages/pip/_internal/commands/completion.py, line 133 (Poor Logging Practice: Use of a System Output Stream) — Low

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionCall: write
Enclosing Method: ~ClassInit()
File: .venv/lib/python3.13/site-packages/pip/_internal/commands/completion.py:133
Taint Flags:

```
130  print(BASE_COMPLETION.format(script=script, shell=options.shell))
131  return SUCCESS
132  else:
133  sys.stderr.write(
134  "ERROR: You must pass {}\n".format(" or ".join(shell_options))
135  )
136  return SUCCESS
```

Package: .venv.lib.python3.13.site-packages.pip._internal.commands.freeze

.venv/lib/python3.13/site-packages/pip/_internal/commands/freeze.py, line 107 (Poor Logging Practice: Use of a System Output Stream) — Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionCall: write
Enclosing Method: ~ClassInit()
File: .venv/lib/python3.13/site-packages/pip/_internal/commands/freeze.py:107
Taint Flags:

```
104  skip=skip,
105  exclude_editable=options.exclude_editable,
106  ):
107  sys.stdout.write(line + "\n")
108  return SUCCESS
109
110 undefined
```

Package: .venv.lib.python3.13.site-packages.pip._internal.commands.lock

.venv/lib/python3.13/site-packages/pip/_internal/commands/lock.py, line 167 (Poor Logging Practice: Use of a System Output Stream) — Low

Issue Details

Kingdom: Encapsulation

Poor Logging Practice: Use of a System Output Stream — Low

Package: .venv.lib.python3.13.site-packages.pip._internal.commands.lock

.venv/lib/python3.13/site-packages/pip/_internal/commands/lock.py, line 167 (Poor Logging Practice: Use of a System Output Stream) — Low

Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionCall: write
Enclosing Method: ~ClassInit()
File: .venv/lib/python3.13/site-packages/pip/_internal/commands/lock.py:167
Taint Flags:

```
164  requirement_set.requirements.values(), base_dir=base_dir
165  ).as_toml()
166  if options.output_file == "-":
167  sys.stdout.write(pylock_toml)
168  else:
169  output_file_path.write_text(pylock_toml, encoding="utf-8")
170
```

Package: .venv.lib.python3.13.site-packages.pip._internal.utils

.venv/lib/python3.13/site-packages/pip/_internal/utils/entrypoints.py, line 35 (Poor Logging Practice: Use of a System Output Stream) — Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionCall: write
File: .venv/lib/python3.13/site-packages/pip/_internal/utils/entrypoints.py:35
Taint Flags:

```
32  directing them to an appropriate place for help, we now define all of
33  our old entrypoints as wrappers for the current one.
34  """
35  sys.stderr.write(
36  "WARNING: pip is being invoked by an old script wrapper. This will "
37  "fail in a future version of pip.\n"
38  "Please see https://github.com/pypa/pip/issues/5599 for advice on "
```

Package: .venv.lib.python3.13.site-packages.pip._vendor.distlib.util

.venv/lib/python3.13/site-packages/pip/_vendor/distlib/util.py, line 1757 (Poor Logging Practice: Use of a System Output Stream) — Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Poor Logging Practice: Use of a System Output Stream — Low

Package: .venv.lib.python3.13.site-packages.pip._vendor.distlib.util

.venv/lib/python3.13/site-packages/pip/_vendor/distlib/util.py, line 1757 (Poor Logging Practice: Use of a System Output Stream) — Low

Sink Details

Sink: FunctionCall: write
Enclosing Method: reader()
File: .venv/lib/python3.13/site-packages/pip/_vendor/distlib/util.py:1757
Taint Flags:

```
1754  if not verbose:
1755  sys.stderr.write('.')
1756  else:
1757  sys.stderr.write(s.decode('utf-8'))
1758  sys.stderr.flush()
1759  stream.close()
1760
```

.venv/lib/python3.13/site-packages/pip/_vendor/distlib/util.py, line 1773 (Poor Logging Practice: Use of a System Output Stream) — Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionCall: write
Enclosing Method: run_command()
File: .venv/lib/python3.13/site-packages/pip/_vendor/distlib/util.py:1773
Taint Flags:

```
1770  if self.progress is not None:
1771  self.progress('done.', 'main')
1772  elif self.verbose:
1773  sys.stderr.write('done.\n')
1774  return p
1775
1776 undefined
```

.venv/lib/python3.13/site-packages/pip/_vendor/distlib/util.py, line 1755 (Poor Logging Practice: Use of a System Output Stream) — Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionCall: write
Enclosing Method: reader()
File: .venv/lib/python3.13/site-packages/pip/_vendor/distlib/util.py:1755

Poor Logging Practice: Use of a System Output Stream — Low

Package: .venv.lib.python3.13.site-packages.pip._vendor.distlib.util

.venv/lib/python3.13/site-packages/pip/_vendor/distlib/util.py, line 1755 (Poor Logging Practice: Use of a System Output Stream) — Low

Taint Flags:

```
1752  progress(s, context)
1753  else:
1754  if not verbose:
1755  sys.stderr.write('.')
1756  else:
1757  sys.stderr.write(s.decode('utf-8'))
1758  sys.stderr.flush()
```

Package: frontend.node_modules.node-gyp.gyp.pylib.gyp.win_tool

frontend/node_modules/node-gyp/gyp/pylib/gyp/win_tool.py, line 239 (Poor Logging Practice: Use of a System Output Stream) — Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionCall: write
Enclosing Method: ExecLinkWithManifests()
File: frontend/node_modules/node-gyp/gyp/pylib/gyp/win_tool.py:239
Taint Flags:

```
236  dump(intermediate_manifest)
237  dump(our_manifest)
238  dump(assert_manifest)
239  sys.stderr.write(
240  'Linker generated manifest "%s" added to final manifest "%s" '
241  '(result in "%s"). '
242  "Were /MANIFEST switches used in #pragma statements? "
```

Package: node_modules.node-gyp.gyp.pylib.gyp

node_modules/node-gyp/gyp/pylib/gyp/__init__.py, line 656 (Poor Logging Practice: Use of a System Output Stream) — Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionCall: write
Enclosing Method: main()
File: node_modules/node-gyp/gyp/pylib/gyp/__init__.py:656
Taint Flags:

Poor Logging Practice: Use of a System Output Stream — Low

Package: node_modules.node-gyp.gyp.pylib.gyp

node_modules/node-gyp/gyp/pylib/gyp/__init__.py, line 656 (Poor Logging Practice: Use of a System Output Stream) — Low

```
653  try:
654  return gyp_main(args)
655  except GypError as e:
656  sys.stderr.write("gyp: %s\n" % e)
657  return 1
658
659 undefined
```

Package: node_modules.node-gyp.gyp.pylib.gyp.win_tool

node_modules/node-gyp/gyp/pylib/gyp/win_tool.py, line 240 (Poor Logging Practice: Use of a System Output Stream) — Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionCall: write
Enclosing Method: ExecLinkWithManifests()
File: node_modules/node-gyp/gyp/pylib/gyp/win_tool.py:240
Taint Flags:

```
237  dump(intermediate_manifest)
238  dump(our_manifest)
239  dump(assert_manifest)
240  sys.stderr.write(
241  'Linker generated manifest "%s" added to final manifest "%s" '
242  '(result in "%s"). '
243  "Were /MANIFEST switches used in #pragma statements? "
```

Privacy Violation (4 issues)

Abstract

隱私資訊 (比如客戶密碼或社會安全號碼) 處理不當會導致使用者隱私資訊洩漏，且是不合法的行為。

Explanation

在以下情況會發生 Privacy Violation： 1. 私人使用者資訊進入程式。 2. 資料寫入到外部位置，例如主控台、File System 或網路。 **範例 1：**下列程式碼會將使用者的純文字密碼儲存於本機。

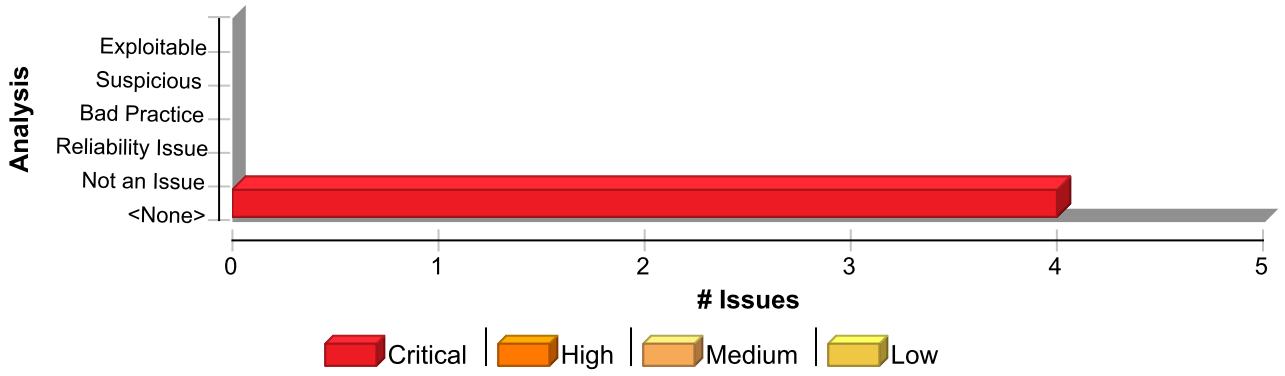
```
localStorage.setItem('password', password);
```

雖然許多的開發人員相信本機為儲存資料的安全位置，但不應對其絕對信賴，特別是關係到隱私問題時。 私人資料可以透過多種方式進入到程式中： — 直接來自於使用者的密碼或個人資訊 — 從應用程式存取資料庫或其他資料儲存 — 間接地來自於合作者或者第三方 有些資料未標示為私人資料，但仍有可能根據狀況有隱私含意。例如，學生的學號通常不被認為是隱私資訊，因為學號中沒有明確和公開的資訊以對應於個別學生的個人資訊。不過，如果學校以學生的身份證字號來產生學號，則此學號應視為隱私資訊。 安全和隱私似乎時常互相矛盾。從安全的觀點來看，您應該要記錄所有重要的操作，以便於日後辨別所有的異常活動。不過，當其中包含了私人資料時，此種作法將會造成風險。 雖然有多種情況會發生隱私資料處理不安全，但常見的風險多是來自盲目的信賴。程式設計師通常會信賴程式執行的作業環境，所以相信將隱私資訊儲存在檔案系統、登錄或是其他局部控制的資源中是可以接受的。但即使限制特定資源的存取權，也並不保證可以信任有存取權的個人。例如，在 2004 年時一位無恥的 AOL 員工將大約 9 千 2 百萬名客戶的私人電子郵件地址賣給了一個透過發送垃圾郵件進行行銷的賭博網站 [1]。 由於此類受矚目的資料攻擊事件，隱私資料的收集和管理方面的規範日益增加。要求各組織根據其位置、所管理的業務類型，以及其所處理的隱私資訊性質，遵守以下一個或多個聯邦和州的規定： - Safe Harbor Privacy Framework [3] - Gramm-Leach Bliley Act (GLBA) [4] - Health Insurance Portability and Accountability Act (HIPAA) [5] - California SB-1386 [6] 雖已制定規範，但 Privacy Violation 的情況仍持續發生。

Recommendation

當安全性和隱私要求發生矛盾時，通常隱私應該放在較重要的位置。為要滿足此要求，並仍維持所需的安全資訊，應在退出程式前清除所有的隱私資料。 為加強隱私管理，應改進發展並嚴格遵守內部的隱私規定。此規定應當具體描述應用程式如何處理隱私資訊。如果您的組織受到聯邦或者州法律的規範，請確定您的隱私規定可符合法律的要求。即使您的組織沒有受到規範，您必須要保護客戶的隱私資訊，以免失去客戶信賴。保護隱私資訊最好的方法就是減少隱私資料的暴露。不應允許應用程式、程序處理以及員工存取任何隱私資料，除非是他們執行工作時所需。遵守最低授權權限原則，不應授予使用者超出其所需的權限，存取資料的權限應該儘可能在最小範圍內。

Issue Summary



Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Privacy Violation	4	0	0	4
Total	**4**	**0**	**0**	**4**

Privacy Violation — Critical

Package: .src.app.shared.components.login-modal

frontend/src/app/shared/components/login-modal/login-modal.component.html, line 35 (Privacy Violation) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Data Flow)

Source Details

Source: Read password
From: ~file_function
File: frontend/src/app/shared/components/login-modal/login-modal.component.html:35

```
32  id="password"
33  [type]="showPassword ? 'text' : 'password'"
34  class="login-form__input"
35  [(ngModel)]="loginData.password"
36  name="password"
37  required
38  autocomplete="current-password"
```

Sink Details

Sink: Assignment to input_13.value
Enclosing Method: ~file_function()
File: frontend/src/app/shared/components/login-modal/login-modal.component.html:35
Taint Flags: PRIVATE

```
32  id="password"
33  [type]="showPassword ? 'text' : 'password'"
34  class="login-form__input"
35  [(ngModel)]="loginData.password"
36  name="password"
37  required
38  autocomplete="current-password"
```

Package: .src.app.shared.components.modals

frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts, line 206 (Privacy Violation) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Data Flow)

Privacy Violation — Critical

Package: .src.app.shared.components.modals

frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts, line 206 (Privacy Violation) — Critical

Source Details

Source: Read this.wifiPassword
From: frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts~QRCodeEditorModalComponent1.onWifiChange
File: frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts:327

```
324   }
325
326   onWifiChange(): void {
327   this.settings.data = `WIFI:T:${this.wifiSecurity};S:${this.wifiSSID};P:${this.wifiPassword};;`;
328   }
329
330   parseWifiData(data: string): void {
```

Sink Details

Sink: Assignment to p_72.innerHTML
Enclosing Method: ~file_function()
File: frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts:206
Taint Flags: CONCATENATED, PRIVATE

```
203   </div>
204
205   <div class="preview-info">
206   <p><strong>內容：</strong> {{ getPreviewText() }}</p>
207   <p><strong>大小：</strong> {{ settings.size }}x{{ settings.size }}px</p>
208   <p><strong>錯誤修正：</strong> {{ getErrorCorrectionText() }}</p>
209   <p><strong>邊距：</strong> {{ settings.margin }}px</p>
```

frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts, line 206 (Privacy Violation) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Data Flow)

Source Details

Source: Read component.wifiPassword
From: ~file_function
File: frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts:112

```
109   </mat-form-field>
110   <mat-form-field appearance="outline">
111   <mat-label>密碼</mat-label>
```

Privacy Violation — Critical

Package: .src.app.shared.components.modals

frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts, line 206 (Privacy Violation) — Critical

```
112  <input matInput [(ngModel)]="wifiPassword"
type="password" (input)="onWifiChange()">
113  </mat-form-field>
114  <mat-form-field appearance="outline">
115  <mat-label>加密方式</mat-label>
```

Sink Details

Sink: Assignment to p_72.innerHTML
Enclosing Method: ~file_function()
File: frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts:206
Taint Flags: CONCATENATED, PRIVATE

```
203  </div>
204
205  <div class="preview-info">
206  <p><strong>內容：</strong> {{ getPreviewText() }}</p>
207  <p><strong>大小：</strong> {{ settings.size }}x{{ settings.size }}px</p>
208  <p><strong>錯誤修正：</strong> {{ getErrorCorrectionText() }}</p>
209  <p><strong>邊距：</strong> {{ settings.margin }}px</p>
```

frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts, line 206 (Privacy Violation) — Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Data Flow)

Source Details

Source: Read HTMLInputElement_Password.prototype
From: ~file_function
File: frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts:112

```
109  </mat-form-field>
110  <mat-form-field appearance="outline">
111  <mat-label>密碼</mat-label>
112  <input matInput [(ngModel)]="wifiPassword"
type="password" (input)="onWifiChange()">
113  </mat-form-field>
114  <mat-form-field appearance="outline">
115  <mat-label>加密方式</mat-label>
```

Sink Details

Sink: Assignment to p_72.innerHTML

Privacy Violation	Critical
Package: .src.app.shared.components.modals	
frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts, line 206 (Privacy Violation)	Critical

Enclosing Method: ~file_function()
File: frontend/src/app/shared/components/modals/qrcode-editor-modal.component.ts:206
Taint Flags: CONCATENATED, PRIVATE

```
203   </div>
204
205   <div class="preview-info">
206   <p><strong>内容：</strong> {{ getPreviewText() }}</p>
207   <p><strong>大小：</strong> {{ settings.size }}x{{ settings.size }}px</p>
208   <p><strong>錯誤修正：</strong> {{ getErrorCorrectionText() }}</p>
209   <p><strong>邊距：</strong> {{ settings.margin }}px</p>
```

Privacy Violation: Shoulder Surfing (1 issue)

Abstract

密碼若被看見，將會危及系統安全性。

Explanation

密碼擁有者不需要查看密碼，而且絕對不可由他人查看。如果以純文字方式顯示密碼，則附近的任何人都可以看到密碼並用以危害系統。在電腦安全領域中，肩窺 (shoulder surfing) 意指直接越過某人肩膀偷窺並取得資訊的惡意觀察行為。肩窺行為最容易在擁擠的公共場所中得逞。尤其是在各種私人或公共場合皆可使用的行動裝置，更自然而然的成為此威脅的目標。

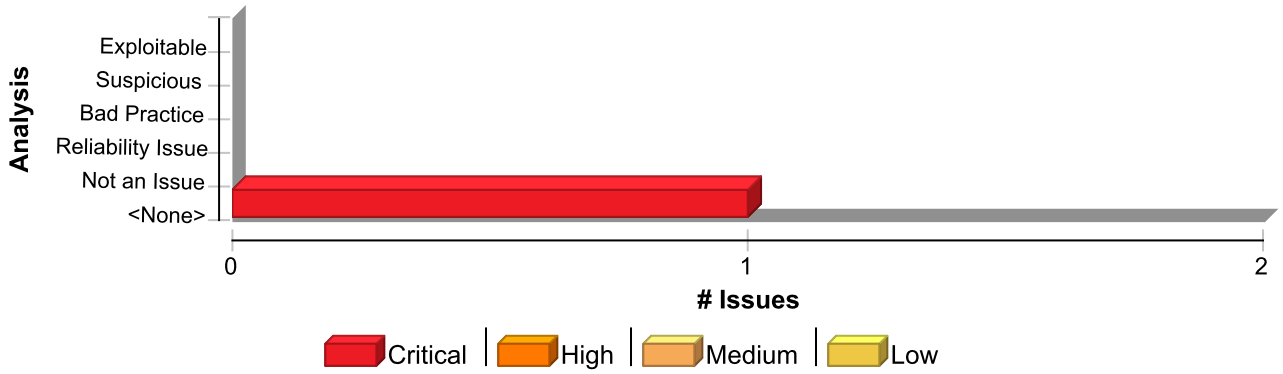
Recommendation

絕不以純文字顯示密碼。使用點或星號模糊欄位中的字元，取代可輕易閱讀的字元。 **範例 1：**在 HTML 表單中，將敏感輸入內容的 `type` 屬性設定為 `password`。

```
  <input name="password" type="password" />
```

請注意，`type` 屬性的預設值為 `text`，而非 `password`。因此，請勿在處理敏感輸入內容時略過該屬性。

Issue Summary



Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Privacy Violation: Shoulder Surfing	1	0	0	1
Total	**1**	**0**	**0**	**1**

Privacy Violation: Shoulder Surfing	Critical
Package: .src.app.shared.components.login-modal	
frontend/src/app/shared/components/login-modal/login-modal.component.html, line 31 (Privacy Violation: Shoulder Surfing)	Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Content)

Sink Details

File: frontend/src/app/shared/components/login-modal/login-modal.component.html:31
Taint Flags:

Privacy Violation: Shoulder Surfing	Critical

Package: .src.app.shared.components.login-modal

frontend/src/app/shared/components/login-modal/login-modal.component.html, line 31 (Privacy Violation: Shoulder Surfing)	Critical

```
28  <div class="login-form__group">
29  <label for="password" class="login-form__label">撤 Ⅳ</label>
30  <div class="login-form__password-wrapper">
31  <input
32  id="password"
33  [type]="showPassword ? 'text' : 'password'"
34  class="login-form__input"
```

Race Condition (1 issue)

Abstract

設定的回撥可能造成競爭情形。

Explanation

Node.js 可讓開發人員將回撥指派給 IO 封鎖的事件。這能夠帶來更好的效能，因為回撥會異步執行，以便主應用程式不會遭到 IO 的封鎖。但是，當回撥以外的內容仰賴回撥內的程式碼才能首先執行時，這可能會反過來造成競爭情形。 **範例 1：**以下程式碼會對照用於驗證的資料庫來檢查使用者。

```
...
var authenticated = true;
...
database_connect.query('SELECT * FROM users WHERE name == ? AND password = ?
LIMIT 1', userNameFromUser, passwordFromUser, function(err, results){
  if (!err && results.length > 0){
    authenticated = true;
  }else{
    authenticated = false;
  }
});

if (authenticated){
  //do something privileged stuff
  authenticatedActions();
}else{
  sendUnathenticatedMessage();
}
```

在此範例中，我們將會呼叫後端資料庫來確認使用者的登入憑證，且如果確認，我們會將變數設為 `true`，否則會設為 `false`。很遺憾，由於回撥遭到 IO 封鎖，因此將會異步執行, 並可能在對 `if (authenticated)` 進行檢查後執行，而由於預設值為 true，因此無論使用者是否確實得到驗證，回撥都將進入 if 陳述式。

Recommendation

建立 Node.js 應用程式時，您必須留意 IO 封鎖事件，以及相關的回撥所執行的功能。可能有一系列回撥需要按特定順序進行呼叫，或者只有在執行特定回撥時才能使用程式碼。 **範例 2：**以下程式碼將修正 `Example 1` 中的競爭情形。

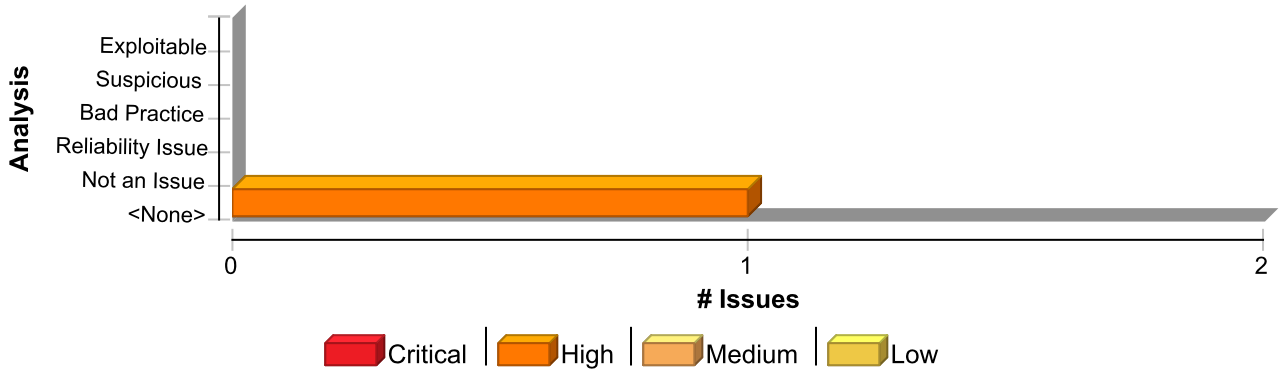
```
...
database_connect.query('SELECT * FROM users WHERE name == ? AND password = ?
LIMIT 1', userNameFromUser, passwordFromUser, function(err, results){
  if (!err && results.length > 0){
    // do privileged stuff
    authenticatedActions();
  }else{
    sendUnauthenticatedMessage();
  }
});
...
```

這是一個簡單的範例，實際情況可能更為複雜，並且可能需要對程式碼基底進行更大規模的重構，才能修正這些問題。嘗試和避免這些問題的其中一種簡單方式就是使用採用 `promises` 的 API，因為其代表了異步作業的最終成果，並讓您能夠指定代表成功和失敗的回撥。如果要經常使用這段程式碼，最好是建立可傳回 `promise` 以供驗證的 API，以便開發人員需要編寫的程式碼可以簡化為：

```
promiseAuthentication()
.then(authenticatedActions, sendUnauthenticatedMessage);
```

這反過來會更易於遵循程式碼並防止競爭情形，因為程式碼將始終按照清晰定義的順序來執行。

Issue Summary



Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Race Condition	1	0	0	1
Total	**1**	**0**	**0**	**1**

Race Condition — High

Package: node_modules.pg.lib.native

node_modules/pg/lib/native/client.js, line 105 (Race Condition) — High

Issue Details

Kingdom: Time and State
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: on
Enclosing Method: lambda()
File: node_modules/pg/lib/native/client.js:105
Taint Flags:

```
102  self._connected = true
103
104  // handle connection errors from the native layer
105  self.native.on('error', function (err) {
106  self._queryable = false
107  self._errorAllQueries(err)
108  self.emit('error', err)
```

System Information Leak: External (1 issue)

Abstract

顯示系統資料或除錯資訊可讓攻擊者使用系統資訊制訂攻擊計畫。

Explanation

在系統資料或除錯資訊離開程式，然後透過通訊端或網路連線前往遠端機器時，會發生外部資訊洩漏。外部洩漏可能會向攻擊者洩漏有關作業系統、完整路徑名稱、存在的使用者名稱或組態設定檔位置的特定資料，較內部資訊洩漏更嚴重，因為攻擊者存取這些資料的難度更大。 **範例 1：**以下程式碼會在網頁的文字區域中洩漏異常資訊：

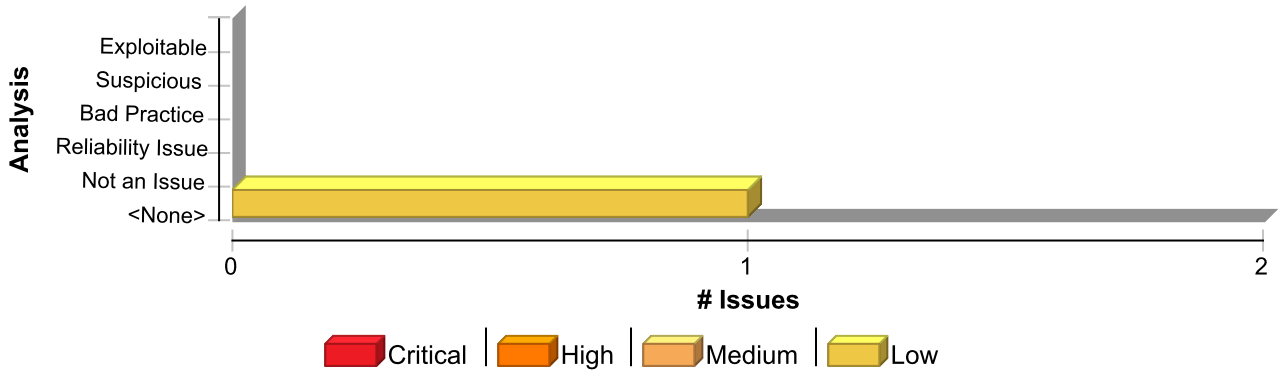
```
...
dirReader.readEntries(function(results){
  ...
}, function(error){
  $("#myTextArea").val('There was a problem: ' + error);
});
...
```

此資訊可能會暴露給遠端使用者。在某些情況下，錯誤訊息會為攻擊者提供系統容易受到哪些確切的攻擊類型影響。例如，資料庫錯誤訊息即可揭露應用程式容易受到 SQL injection 攻擊。其他錯誤訊息還可揭露更多關於系統的間接線索。在 `Example 1` 中，洩漏的資訊可能會暗示有關作業系統類型、系統上安裝的應用程式，以及管理員在配置程式時所花費的努力等資訊。

Recommendation

編寫錯誤訊息時，請將安全性問題考慮進去。在生產環境中，請儘量使用簡短的錯誤訊息，而不要使用詳細的錯誤資訊。限制產生與儲存詳細的輸出內容，將有助於管理員和程式設計師診斷問題。除錯追蹤有時可能會出現在不明顯的地方 (例如，內嵌在錯誤頁面的 HTML 註解中)。 即使是不會揭露堆疊追蹤或資料庫傾印的簡短錯誤訊息，都可能會助攻擊者一臂之力。例如，「拒絕存取」訊息可能表示系統中存在檔案或使用者。因此，切勿將資訊直接傳送至程式外部的資源。

Issue Summary



Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
System Information Leak: External	1	0	0	1
Total	**1**	**0**	**0**	**1**

System Information Leak: External — Low

Package: node_modules.pgpass.lib

node_modules/pgpass/lib/helper.js, line 35 (System Information Leak: External) — Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: onErr(0)
From: onErr
File: node_modules/pgpass/lib/helper.js:125

```
122  cb(pass);
123  };
124
125  var onErr = function(err) {
126  stream.destroy();
127  warn('WARNING: error on reading file: %s', err);
128  cb(undefined);
```

Sink Details

Sink: ~JS_Generic.write()
Enclosing Method: warn()
File: node_modules/pgpass/lib/helper.js:35
Taint Flags: CONCATENATED, EXCEPTIONINFO, SYSTEMINFO

```
32
33  if (isWritable) {
34  var args = Array.prototype.slice.call(arguments).concat("\n");
35  warnStream.write( util.format.apply(util, args) );
36  }
37 }
38
```

System Information Leak: Internal (5 issues)

Abstract

顯示系統資料或除錯資訊可讓攻擊者使用系統資訊制訂攻擊計畫。

Explanation

在透過列印或記錄將系統資料或除錯資訊傳送至本機檔案、主控台或螢幕時，會發生內部資訊洩漏。 **範例 1**：以下程式碼會將異常寫入標準輸出串流：

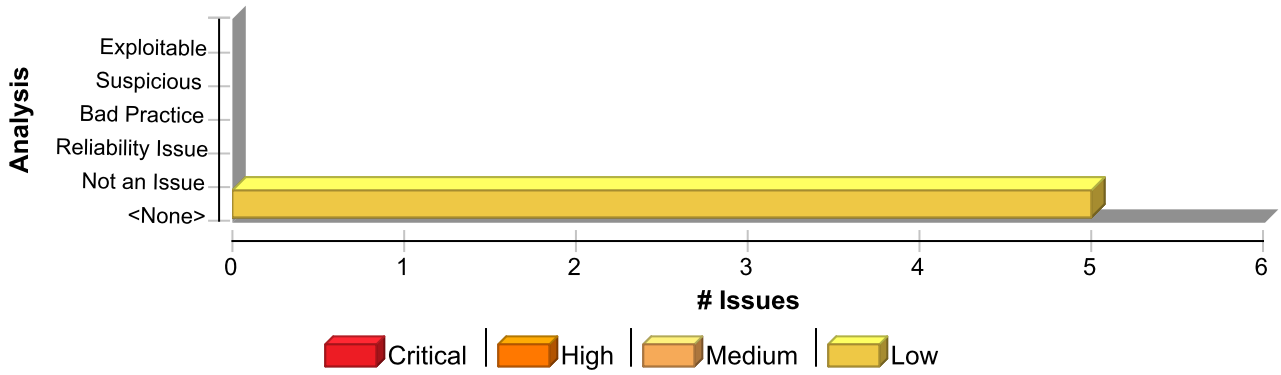
```
try:
    ...
except:
    print(sys.exc_info()[2])
```

此資訊會傾印至主控台。在某些情況下，錯誤訊息會為攻擊者提供系統容易受到哪些確切的攻擊類型影響。例如，資料庫錯誤訊息即可揭露應用程式容易受到 SQL injection 攻擊。其他錯誤訊息還可揭露更多關於系統的間接線索。在 `Example 1` 中，洩漏的資訊可能會暗示有關作業系統類型、系統上安裝的應用程式，以及管理員在配置程式時所花費的努力等資訊。

Recommendation

編寫錯誤訊息時，請將安全性問題考慮進去。在生產環境中，請儘量使用簡短的錯誤訊息，而不要使用詳細的錯誤資訊。限制產生與儲存詳細的輸出內容，將有助於管理員和程式設計師診斷問題。除錯追蹤有時可能會出現在不明顯的地方 (例如，內嵌在錯誤頁面的 HTML 註解中)。 即使是不會揭露堆疊追蹤或資料庫傾印的簡短錯誤訊息，都可能會助攻擊者一臂之力。例如，「拒絕存取」訊息可能表示系統中存在著檔案或使用者。

Issue Summary



Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
System Information Leak: Internal	5	0	0	5
Total	**5**	**0**	**0**	**5**

System Information Leak: Internal	**Low**
Package: .src.app.shared.services	
frontend/src/app/shared/services/thumbnail-generator.service.ts, line 264 (System Information Leak: Internal)	**Low**
Issue Details	

System Information Leak: Internal — Low

Package: .src.app.shared.services

frontend/src/app/shared/services/thumbnail-generator.service.ts, line 264 (System Information Leak: Internal) — Low

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: frontend/src/app/shared/services/thumbnail-generator.service.ts:263

```
260   // 生成 base64 圖片
261   const dataURL = canvas.toDataURL('image/jpeg', 0.8);
262   resolve(dataURL);
263   }).catch(error => {
264   console.error('繪製元素時發生錯誤:', error);
265   // 即使部分元素繪製失敗，也返回目前的結果
266   const dataURL = canvas.toDataURL('image/jpeg', 0.8);
```

Sink Details

Sink: ~JS_Generic.error()
Enclosing Method: lambda()
File: frontend/src/app/shared/services/thumbnail-generator.service.ts:264
Taint Flags: SYSTEMINFO

```
261   const dataURL = canvas.toDataURL('image/jpeg', 0.8);
262   resolve(dataURL);
263   }).catch(error => {
264   console.error('繪製元素時發生錯誤:', error);
265   // 即使部分元素繪製失敗，也返回目前的結果
266   const dataURL = canvas.toDataURL('image/jpeg', 0.8);
267   resolve(dataURL);
```

Package: frontend.node_modules.node-gyp.gyp.pylib.gyp.generator.analyzer

frontend/node_modules/node-gyp/gyp/pylib/gyp/generator/analyzer.py, line 589 (System Information Leak: Internal) — Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: __python_get_last_exception()
From: frontend.node_modules.node-gyp.gyp.pylib.gyp.generator.analyzer._WriteOutput
File: frontend/node_modules/node-gyp/gyp/pylib/gyp/generator/analyzer.py:588

```
585   f = open(output_path, "w")
```

System Information Leak: Internal — Low

Package: frontend.node_modules.node-gyp.gyp.pylib.gyp.generator.analyzer

frontend/node_modules/node-gyp/gyp/pylib/gyp/generator/analyzer.py, line 589 (System Information Leak: Internal) — Low

```
586   f.write(json.dumps(values) + "\n")
587   f.close()
588   except OSError as e:
589   print("Error writing to output file", output_path, str(e))
590
591
```

Sink Details

Sink: print()
Enclosing Method: _WriteOutput()
File: frontend/node_modules/node-gyp/gyp/pylib/gyp/generator/analyzer.py:589
Taint Flags: EXCEPTIONINFO, SYSTEMINFO

```
586   f.write(json.dumps(values) + "\n")
587   f.close()
588   except OSError as e:
589   print("Error writing to output file", output_path, str(e))
590
591
592 def _WasGypIncludeFileModified(params, files):
```

Package: frontend.src

frontend/src/main.ts, line 18 (System Information Leak: Internal) — Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: frontend/src/main.ts:18

```
15  provideHttpClient(),
16  // 其他 providers
17  ]
18 }).catch(err => console.error(err));
19
20 undefined
21 undefined
```

Sink Details

System Information Leak: Internal — Low

Package: frontend.src

frontend/src/main.ts, line 18 (System Information Leak: Internal) — Low

Sink: ~JS_Generic.error()
Enclosing Method: lambda()
File: frontend/src/main.ts:18
Taint Flags: SYSTEMINFO

```
15  provideHttpClient(),
16  // 其他 providers
17  ]
18 }).catch(err => console.error(err));
19
20 undefined
21 undefined
```

Package: node_modules.node-gyp.gyp.pylib.gyp.generator.analyzer

node_modules/node-gyp/gyp/pylib/gyp/generator/analyzer.py, line 589 (System Information Leak: Internal) — Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: __python_get_last_exception()
From: node_modules.node-gyp.gyp.pylib.gyp.generator.analyzer._WriteOutput
File: node_modules/node-gyp/gyp/pylib/gyp/generator/analyzer.py:588

```
585   f = open(output_path, "w")
586   f.write(json.dumps(values) + "\n")
587   f.close()
588   except OSError as e:
589   print("Error writing to output file", output_path, str(e))
590
591
```

Sink Details

Sink: print()
Enclosing Method: _WriteOutput()
File: node_modules/node-gyp/gyp/pylib/gyp/generator/analyzer.py:589
Taint Flags: EXCEPTIONINFO, SYSTEMINFO

```
586   f.write(json.dumps(values) + "\n")
587   f.close()
588   except OSError as e:
589   print("Error writing to output file", output_path, str(e))
590
591
```

System Information Leak: Internal	Low

Package: node_modules.node-gyp.gyp.pylib.gyp.generator.analyzer

node_modules/node-gyp/gyp/pylib/gyp/generator/analyzer.py, line 589 (System Information Leak: Internal)	Low

```
592 def _WasGypIncludeFileModified(params, files):
```

Package: node_modules.pgpass.lib

node_modules/pgpass/lib/helper.js, line 127 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: onErr(0)
From: onErr
File: node_modules/pgpass/lib/helper.js:125

```
122   cb(pass);
123   };
124
125   var onErr = function(err) {
126   stream.destroy();
127   warn('WARNING: error on reading file: %s', err);
128   cb(undefined);
```

Sink Details

Sink: environment~object.warn()
Enclosing Method: onErr()
File: node_modules/pgpass/lib/helper.js:127
Taint Flags: EXCEPTIONINFO, SYSTEMINFO

```
124
125   var onErr = function(err) {
126   stream.destroy();
127   warn('WARNING: error on reading file: %s', err);
128   cb(undefined);
129   };
130
```

Weak Cryptographic Hash (11 issues)

Abstract

低等的加密式 hash 無法保證資料完整性，不應在安全關鍵內容中使用。

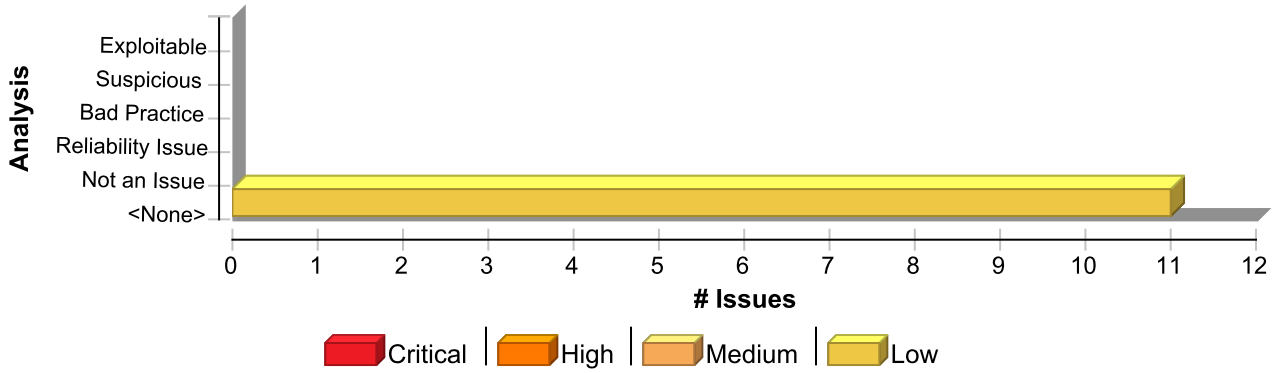
Explanation

MD2、MD4、MD5、RIPEMD-160 和 SHA-1 是最受廣泛使用的加密式雜湊演算法，通常用來驗證訊息及其他資料的完整性。不過，最近的加密分析研究指出這些演算法存在基本性弱點，不應再於安全關鍵內容中使用。 有效破解 MD5 和 RIPEMD 雜湊的技術隨處可得，因此不應依賴這些演算法做為安全性的保障。就 SHA-1 而言，目前的技術仍需要相當大量的運算能力，而且執行起來更加不容易。不過，攻擊者已找到演算法的致命弱點，且透過破解的技術，可能將發現更快速的攻擊方法。

Recommendation

請停止使用 MD2、MD4、MD5、RIPEMD-160 和 SHA-1 來進行安全關鍵內容中的資料驗證。目前，SHA-224、SHA-256、SHA-384、SHA-512 和 SHA-3 是很好的替代選擇。不過，這些安全雜湊演算法的不同版本尚未經過如 SHA-1 般嚴密的檢查，所以須留意未來可能會對這些演算法安全造成影響的研究。

Issue Summary



Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Weak Cryptographic Hash	11	0	0	11
Total	**11**	**0**	**0**	**11**

Weak Cryptographic Hash	**Low**
Package: node_modules.pg.lib	
node_modules/pg/lib/client.js, line 255 (Weak Cryptographic Hash)	**Low**

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: postgresMd5PasswordHash
Enclosing Method: lambda()
File: node_modules/pg/lib/client.js:255

Weak Cryptographic Hash — Low

Package: node_modules.pg.lib

node_modules/pg/lib/client.js, line 255 (Weak Cryptographic Hash) — Low

Taint Flags:

```
252  _handleAuthMD5Password(msg) {
253  this._checkPgPass(async () => {
254  try {
255  const hashedPassword = await crypto.postgresMd5PasswordHash(this.user, this.password, msg.salt)
256  this.connection.password(hashedPassword)
257  } catch (e) {
258  this.emit('error', e)
```

Package: node_modules.pg.lib.crypto

node_modules/pg/lib/crypto/utils-legacy.js, line 12 (Weak Cryptographic Hash) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionCall: postgresMd5PasswordHash
Enclosing Method: init^()
File: node_modules/pg/lib/crypto/utils-legacy.js:12
Taint Flags:

```
9 }
10
11 // See AuthenticationMD5Password at https://www.postgresql.org/docs/current/static/protocol-flow.html
12 function postgresMd5PasswordHash(user, password, salt) {
13  const inner = md5(password + user)
14  const outer = md5(Buffer.concat([Buffer.from(inner), salt]))
15  return 'md5' + outer
```

node_modules/pg/lib/crypto/utils-webcrypto.js, line 51 (Weak Cryptographic Hash) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionCall: postgresMd5PasswordHash
Enclosing Method: init^()
File: node_modules/pg/lib/crypto/utils-webcrypto.js:51
Taint Flags:

```
48 }
49
```

Weak Cryptographic Hash — Low

Package: node_modules.pg.lib.crypto

node_modules/pg/lib/crypto/utils-webcrypto.js, line 51 (Weak Cryptographic Hash) — Low

```
50 // See AuthenticationMD5Password at https://www.postgresql.org/docs/current/static/protocol-flow.html
51 async function postgresMd5PasswordHash(user, password, salt) {
52   const inner = await md5(password + user)
53   const outer = await md5(Buffer.concat([Buffer.from(inner), salt]))
54   return 'md5' + outer
```

node_modules/pg/lib/crypto/utils-legacy.js, line 7 (Weak Cryptographic Hash) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionCall: md5
Enclosing Method: init^()
File: node_modules/pg/lib/crypto/utils-legacy.js:7
Taint Flags:

```
4
5 const nodeCrypto = require('crypto')
6
7 function md5(string) {
8   return nodeCrypto.createHash('md5').update(string, 'utf-8').digest('hex')
9 }
10
```

node_modules/pg/lib/crypto/utils-webcrypto.js, line 35 (Weak Cryptographic Hash) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionCall: md5
Enclosing Method: init^()
File: node_modules/pg/lib/crypto/utils-webcrypto.js:35
Taint Flags:

```
32   return webCrypto.getRandomValues(Buffer.alloc(length))
33 }
34
35 async function md5(string) {
36   try {
37   return nodeCrypto.createHash('md5').update(string, 'utf-8').digest('hex')
```

Weak Cryptographic Hash — Low

Package: node_modules.pg.lib.crypto

node_modules/pg/lib/crypto/utils-webcrypto.js, line 35 (Weak Cryptographic Hash) — Low

```
38  } catch (e) {
```

node_modules/pg/lib/crypto/utils-legacy.js, line 13 (Weak Cryptographic Hash) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: md5
Enclosing Method: postgresMd5PasswordHash()
File: node_modules/pg/lib/crypto/utils-legacy.js:13
Taint Flags:

```
10
11 // See AuthenticationMD5Password at https://www.postgresql.org/docs/current/static/protocol-flow.html
12 function postgresMd5PasswordHash(user, password, salt) {
13   const inner = md5(password + user)
14   const outer = md5(Buffer.concat([Buffer.from(inner), salt]))
15   return 'md5' + outer
16 }
```

node_modules/pg/lib/crypto/utils-webcrypto.js, line 52 (Weak Cryptographic Hash) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: md5
Enclosing Method: postgresMd5PasswordHash()
File: node_modules/pg/lib/crypto/utils-webcrypto.js:52
Taint Flags:

```
49
50 // See AuthenticationMD5Password at https://www.postgresql.org/docs/current/static/protocol-flow.html
51 async function postgresMd5PasswordHash(user, password, salt) {
52   const inner = await md5(password + user)
53   const outer = await md5(Buffer.concat([Buffer.from(inner), salt]))
54   return 'md5' + outer
55 }
```

Weak Cryptographic Hash — Low

Package: node_modules.pg.lib.crypto

node_modules/pg/lib/crypto/utils-legacy.js, line 14 (Weak Cryptographic Hash) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: md5
Enclosing Method: postgresMd5PasswordHash()
File: node_modules/pg/lib/crypto/utils-legacy.js:14
Taint Flags:

```
11 // See AuthenticationMD5Password at https://www.postgresql.org/docs/current/static/protocol-flow.html
12 function postgresMd5PasswordHash(user, password, salt) {
13  const inner = md5(password + user)
14  const outer = md5(Buffer.concat([Buffer.from(inner), salt]))
15  return 'md5' + outer
16 }
17
```

node_modules/pg/lib/crypto/utils-webcrypto.js, line 53 (Weak Cryptographic Hash) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: md5
Enclosing Method: postgresMd5PasswordHash()
File: node_modules/pg/lib/crypto/utils-webcrypto.js:53
Taint Flags:

```
50 // See AuthenticationMD5Password at https://www.postgresql.org/docs/current/static/protocol-flow.html
51 async function postgresMd5PasswordHash(user, password, salt) {
52  const inner = await md5(password + user)
53  const outer = await md5(Buffer.concat([Buffer.from(inner), salt]))
54  return 'md5' + outer
55 }
56
```

node_modules/pg/lib/crypto/utils-legacy.js, line 8 (Weak Cryptographic Hash) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Weak Cryptographic Hash — Low

Package: node_modules.pg.lib.crypto

node_modules/pg/lib/crypto/utils-legacy.js, line 8 (Weak Cryptographic Hash) — Low

Sink: FunctionPointerCall: createHash
Enclosing Method: md5()
File: node_modules/pg/lib/crypto/utils-legacy.js:8
Taint Flags:

```
5 const nodeCrypto = require('crypto')
6
7 function md5(string) {
8   return nodeCrypto.createHash('md5').update(string, 'utf-8').digest('hex')
9 }
10
11 // See AuthenticationMD5Password at https://www.postgresql.org/docs/current/static/protocol-flow.html
```

node_modules/pg/lib/crypto/utils-webcrypto.js, line 37 (Weak Cryptographic Hash) — Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: createHash
Enclosing Method: md5()
File: node_modules/pg/lib/crypto/utils-webcrypto.js:37
Taint Flags:

```
34
35 async function md5(string) {
36   try {
37   return nodeCrypto.createHash('md5').update(string, 'utf-8').digest('hex')
38   } catch (e) {
39   // `createHash()` failed so we are probably not in Node.js, use the WebCrypto API instead.
40   // Note that the MD5 algorithm on WebCrypto is not available in Node.js.
```

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.

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.