OISINT SUMMARY

# **OSINT Harvesting: University of Manchester Exposure**

*theHarvester Results (DuckDuckGo/Baidu/Yahoo)*

**1. Email Exposure (29 Found)**

* **Generic Addresses**:  
  president@manchester.ac.uk, international@manchester.ac.uk, ssc@manchester.ac.uk
* **Departmental Contacts**:  
  soe.programmes@manchester.ac.uk (School of Engineering)  
  sbs.wellbeing@manchester.ac.uk (Student Support)
* **Personal Emails**:  
  john.mcauliffe@manchester.ac.uk, serge.sagna@manchester.ac.uk

**2. Subdomain Exposure (29 Hosts)**

* **Critical Infrastructure**:  
  my.manchester.ac.uk (student portal)  
  research.manchester.ac.uk  
  iam.manchester.ac.uk (identity management)
* **Vulnerable Targets**:  
  documents.manchester.ac.uk (potential file leaks)  
  remoteit.itservices.manchester.ac.uk (remote access)

**3. Security Observations**

* **Pattern Risks**:  
  Generic email formats (firstname.lastname@...) enable phishing campaigns.
* **Outdated Data**:  
  Some subdomains (e.g., micklefieldlab.chemistry.manchester.ac.uk) may belong to deprecated services.

**Source**: theHarvester -d manchester.ac.uk -b duckduckgo,baidu,yahoo -l 100  
**Limitations**: 29/100 result limit reached | Search engine blocks may truncate data

# SSL Certificate Analysis: University of Manchester (manchester.ac.uk)

*Key Cybersecurity Insights from crt.sh Data*

**1. Domain Exposure**

* **150+ subdomains** discovered (e.g., login.manchester.ac.uk, blackboard.manchester.ac.uk, sharepoint.manchester.ac.uk)
* Critical systems exposed:
  + Student portals (my.manchester.ac.uk)
  + Payment systems (epayments.manchester.ac.uk)
  + Research platforms (research.manchester.ac.uk)

**2. Certificate Patterns**

* **Primary Issuers**:
  + TERENA SSL CA (70% of certificates)
  + Comodo, GeoTrust, Thawte (legacy systems)
* **Wildcard Certificates**:
  + \*.manchester.ac.uk (broad attack surface)
  + \*.cs.manchester.ac.uk (department-specific)

**3. Security Risks**

* **Expired Certificates**: 20+ lapsed certificates (e.g., esdsw2.mc.manchester.ac.uk expired in 2011)
* **Long Validity Periods**: Some certs valid for **5+ years** (e.g., utopia.cs.manchester.ac.uk until 2017)
* **Third-Party Issuers**: Reliance on external CAs (e.g., Comodo, GeoTrust) increases supply-chain risks.

**Source**: crt.sh (2013 dataset) | **Tool**: TheHarvester (OSINT)

# GitHub Exposure Analysis: University of Manchester

*Open-Source Intelligence (OSINT) Findings*

**1. Public Repository Exposure**

* **50+ repositories** linked to manchester.ac.uk
* Key groups:
  + **Research IT** (UoMResearchIT) – Skills visualization tools
  + **University Library** (UoMLibrary) – 23 public repos
  + **Cloud Physics Research** – Sensitive climate modeling code

**2. Data Leak Risks**

* **Email Addresses** exposed in commits/configs:
  + ITS-research@manchester.ac.uk
  + paul.connolly@manchester.ac.uk (cloud physics team)
  + william.finnigan@manchester.ac.uk (kinetics research)
* **Internal Systems** referenced:
  + Blackboard (online.manchester.ac.uk)
  + Research portals (rseskillsgraph.itservices.manchester.ac.uk)

**3. Security Concerns**

* **Hardcoded Credentials**:
  + Example: Blackboard API links in blackboard-scraper repo
* **Outdated Projects**:
  + Some repos inactive since 2021 (e.g., PACMAN citation file)
* **Third-Party Risks**:
  + Student projects with @manchester.ac.uk emails in public commits

**Source**: GitHub search (site:github.com "manchester.ac.uk") | **Tool**: Google dorking

# Shodan Exposure Analysis: University of Manchester

*Internet-Facing Infrastructure Risks*

**1. System Exposure (42 Hosts)**

* **Critical Services**:
  + Student portals (student.ambs.manchester.ac.uk)
  + Library systems (lapcat.library.manchester.ac.uk)
  + Research platforms (hesc.manchester.ac.uk)
* **Vulnerable Targets**:
  + Pre-production environments (preprod.\*.ambs.manchester.ac.uk)
  + Legacy systems (mhn.mc.man.ac.uk)

**2. Security Observations**

* **SSL/TLS Configurations**:
  + Mixed certificate authorities (Sectigo, GEANT)
  + TLS 1.2/1.3 support (no obsolete protocols detected)
* **Server Headers**:
  + Apache (34 instances) dominates infrastructure
  + Security headers present but inconsistent (X-Frame-Options, CSP)

**3. High-Risk Findings**

* **Pre-Prod Leakage**:  
  Development/staging systems (preprod.\*) publicly accessible
* **Orphaned Systems**:  
  tomcat4.prospects.ac.uk (outdated Tomcat server)
* **Redirect Vulnerabilities**:  
  apply.ambs.manchester.ac.uk uses HTTP 302 redirects

**Source**: Shodan (manchester.ac.uk filter) | **Scan Date**: July 2025