Staff

Searching for and identifying employees on social media platforms can also reveal a lot about the teams' infrastructure and makeup. This, in turn, can lead to us identifying which technologies, programming languages, and even software applications are being used. To a large extent, we will also be able to assess each person's focus based on their skills. The posts and material shared with others are also a great indicator of what the person is currently engaged in and what that person currently feels is important to share with others.

Employees can be identified on various business networks such as LinkedIn or Xing. Job postings from companies can also tell us a lot about their infrastructure and give us clues about what we should be looking for.

LinkedIn - Job Post

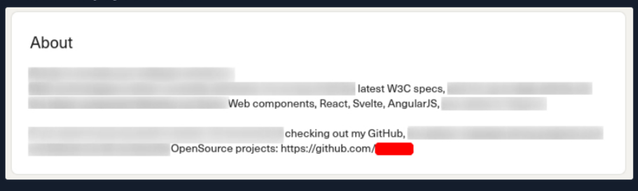
Code: txt

```
Required Skills/Knowledge/Experience:

* 3-10+ years of experience on professional software development projects.

« An active US Government TS/SCI Security Clearance (current SSBI) or eligibility to obtain TS/SCI within
« Bachelor's degree in computer science/computer engineering with an engineering/math focus or another ec
« Experience with one or more object-oriented languages (e.g., Java, C#, C++).
« Experience with one or more scripting languages (e.g., Python, Ruby, PHP, Perl).
« Experience using SQL databases (e.g., PostgreSQL, MySQL, SQL Server, Oracle).
« Experience using ORM frameworks (e.g., SQLAIchemy, Hibernate, Entity Framework).
« Experience using Web frameworks (e.g., Flask, Django, Spring, ASP.NET MVC).
« Proficient with unit testing and test frameworks (e.g., pytest, JUnit, NUnit, xUnit).
« Service-Oriented Architecture (SOA)/microservices & RESTful API design/implementation.
« Familiar and comfortable with Agile Development Processes.
« Familiar and comfortable with Continuous Integration environments.
« Experience with version control systems (e.g., Git, SVN, Mercurial, Perforce).

Desired Skills/Knowledge/ Experience:

« CompTIA Security+ certification (or equivalent).
« Experience with Atlassian suite (Confluence, Jira, Bitbucket).
« Algorithm Development (e.g., Image Processing algorithms).
« Software security.
« Containerization and container orchestration (Docker, Kubernetes, etc.)
« Redis.
« NumPy.
```

From a job post like this, we can see, for example, which programming languages are preferred: `Java, C#, C++, Python, Ruby, PHP, Perl`. It also required that the applicant be familiar with different databases, such as: `PostgreSQL, Mysql, and Oracle`. In addition, we know that different frameworks are used for web application development, such as: `Flask, Django, ASP.NET, Spring`.

Furthermore, we use `REST APIs, Github, SVN, and Perforce`. The job offer also results that the company works with Atlassian Suite, and therefore there may be resources that we could potentially access. We can see some skills and projects from the career history that give us a reasonable estimate of the employee's knowledge.

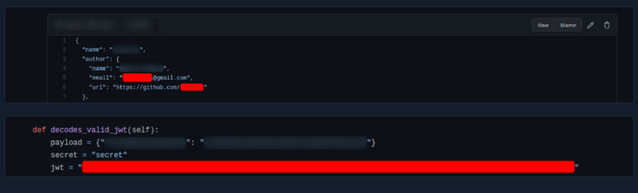
LinkedIn - Employee #1 About



We try to make business contacts on social media sites and prove to visitors what skills we bring to the table inevitably lead to us sharing with the public what we know and what we have learned so far. Companies always hire employees whose skills they can use and apply to the business. For example, we know that Flask and Django are web frameworks for the Python programming language.

If we do a little search for Django security misconfigurations, we will eventually come across the following Github repository that describes OWASP Top10 for Django. We can use this to understand the inner structure of Django and how it works. The best practices also often tell us what to look for. Because many blindly trust them and even name many of the files as shown in the instructions.

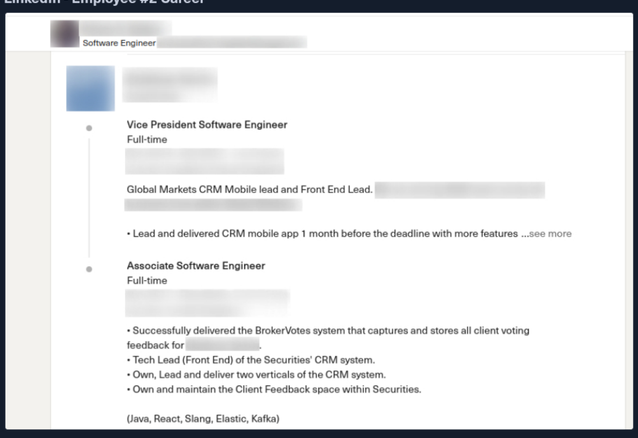
Github




```
def decodes_valid_jwt(self):
    payload = {"                ": "                    "}
    secret = "secret"
    jwt = "
```

Showing our projects can, of course, be of great advantage to make new business contacts and possibly even get a new job, but on the other hand, it can lead to mistakes that will be very difficult to fix. For example, in one of the files, we can discover the employee's personal email address, and upon deeper investigation, the web application has a hardcoded JWT token.

LinkedIn - Employee #2 Career



LinkedIn offers a comprehensive search for employed, sorted by connections, locations, companies, school, industry, profile language, services, names, titles, and more. Understandably, the more detailed information we provide there, the fewer results we get. Therefore, we should think carefully about the purpose of performing the search.

Suppose we are trying to find the infrastructure and technology the company is most likely to use. We should look for technical employees who work both in development and security. Because based on the security area and the employees who work in that area, we will also be able to determine what security measures the company has put in place to secure itself.

Previous Next

Mark Complete & Next

Cheat Sheet
Resources

Table of Contents

Introduction
Enumeration Principles
Enumeration Methodology

Infrastructure Based Enumeration
Domain Information
Cloud Resources
Staff

Host Based Enumeration
FTP
SMB
NFS
DNS
SMTP
IMAP / POP3
SNMP
MySQL
MSSQL
IPMI

Remote Management Protocols
Linux Remote Management Protocols
Windows Remote Management Protocols

Skills Assessment
Footprinting Lab - Easy
Footprinting Lab - Medium
Footprinting Lab - Hard

My Workstation
OFFLINE
Start Instance
∞ / 1 spawns left

Powered by HACKTHEBOX