What Hackers See That You Don’t:

A Real-World Look at Vulnerabilities

About Me

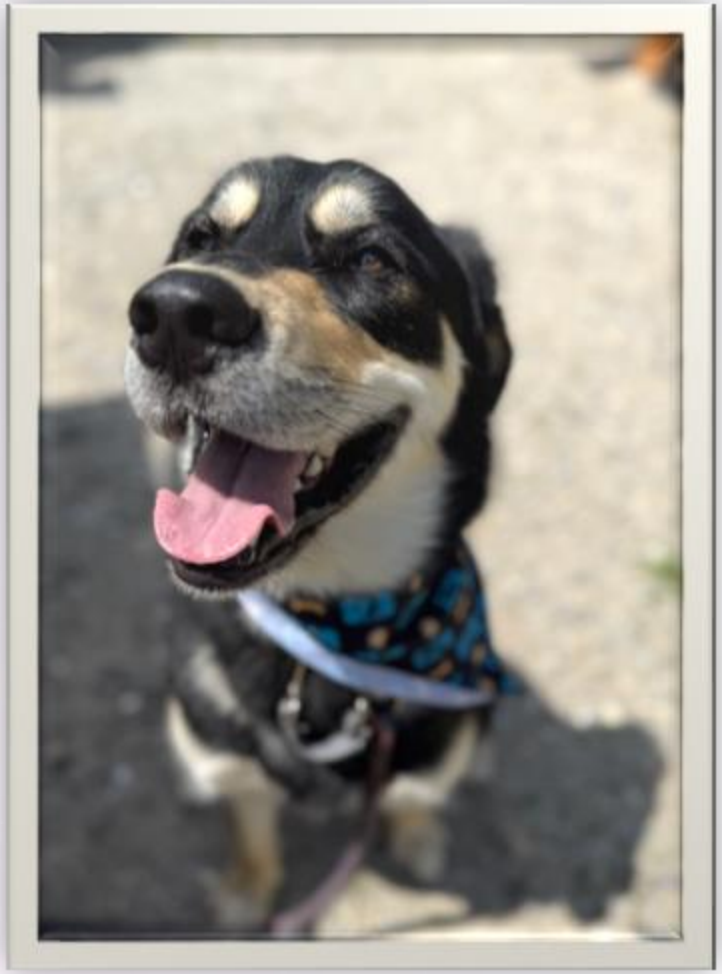
Alexandria Poulin

Director of Service Delivery

Cloud Security Partners

> Formerly at the University of Maine

> Passionate about sports, skiing, traveling, cooking, and reading



alexandria-poulin

CLOUD SECURITY PARTNERS

Agenda

What attackers exploit.

- Open Source Intelligence (OSINT)
- Misconfigurations
- Outdated dependencies
- Default and Weak Credentials
- Common vulnerabilities

How to prevent it.

- Principle of least privilege
- Logging and monitoring
- Easy Wins
- Testing

What attackers exploit.

Image by pngtree.com

OSINT

People

Companies

Technical Footprint

Location

OSINT – Company Data

Domain & Network Info

- DNS records
- Subdomains and IP ranges

People & Communication

- Employee names and email formats
- Job postings

Technology Stack

- Tech Used
- Web servers, frameworks, and cloud providers

Public Disclosures

- Press releases & investor filings
- Publicly listed partners and third-party vendors

The Lead Software Engineer Is involved in all stages of software development, including front-end development, back-end development, database integrations, network and hosting management, user interface, user experience, and back-end server management. Begins to influence department's strategy. Makes decisions on moderately complex to complex issues regarding technical approach for project components, and work is performed with minimal direction. Exercises considerable latitude in determining objectives and approaches to assignments

Required Qualifications

Minimum 3 years React JS Hands-on experience.

Minimum 5 years Java Spring Boot Hands-on experience.

Experience with Azure DevOps, CIT, CI/CD, TDD, and Automated Build Processes

Experience with Cloud Technologies (Azure, GCP, AWS, etc.)

Bachelor's degree in Computer Science or related field

8 or more years of progressive IT experience as a senior developer in large IT projects

2 or more years of project leadership experience

Must be passionate about contributing to an organization focused on continuously improving consumer experiences.

OSINT – Technical Footprint

Open Services & Ports	• **Shodan, Censys,**– Scan for exposed ports, services, and banners
Subdomain Discovery	• **crt.sh, DNSDumpster, Sublist3r** – Find subdomains via certs and DNS records
SSL/TLS Certificate Intelligence	• **crt.sh, Censys** – Analyze cert transparency logs and identify associated domains
Leaked Code & Configs	• **GitHub, GitLab, Pastebin** – Search for exposed credentials, keys, or configuration files
Vulnerability Disclosures	• **HackerOne, Bugcrowd, OpenBugBounty** – Review reported bugs for tech stack insights
Tech Stack	• **Wappalyzer, BuiltWith** – Identify web servers and frameworks

Security
April 21, 2025

Share

Hawk Eye: Open-source scanner uncovers secrets and PII across platforms

Hawk Eye is an open-source tool that helps find sensitive data before it leaks. It runs from the command line and checks many types of storage for PII and secrets: passwords, API keys, and personal information.

Check out this free automated tool that hunts for exposed AWS secrets in public repos

You can find out if your GitHub codebase is leaking keys ... but so can miscreants

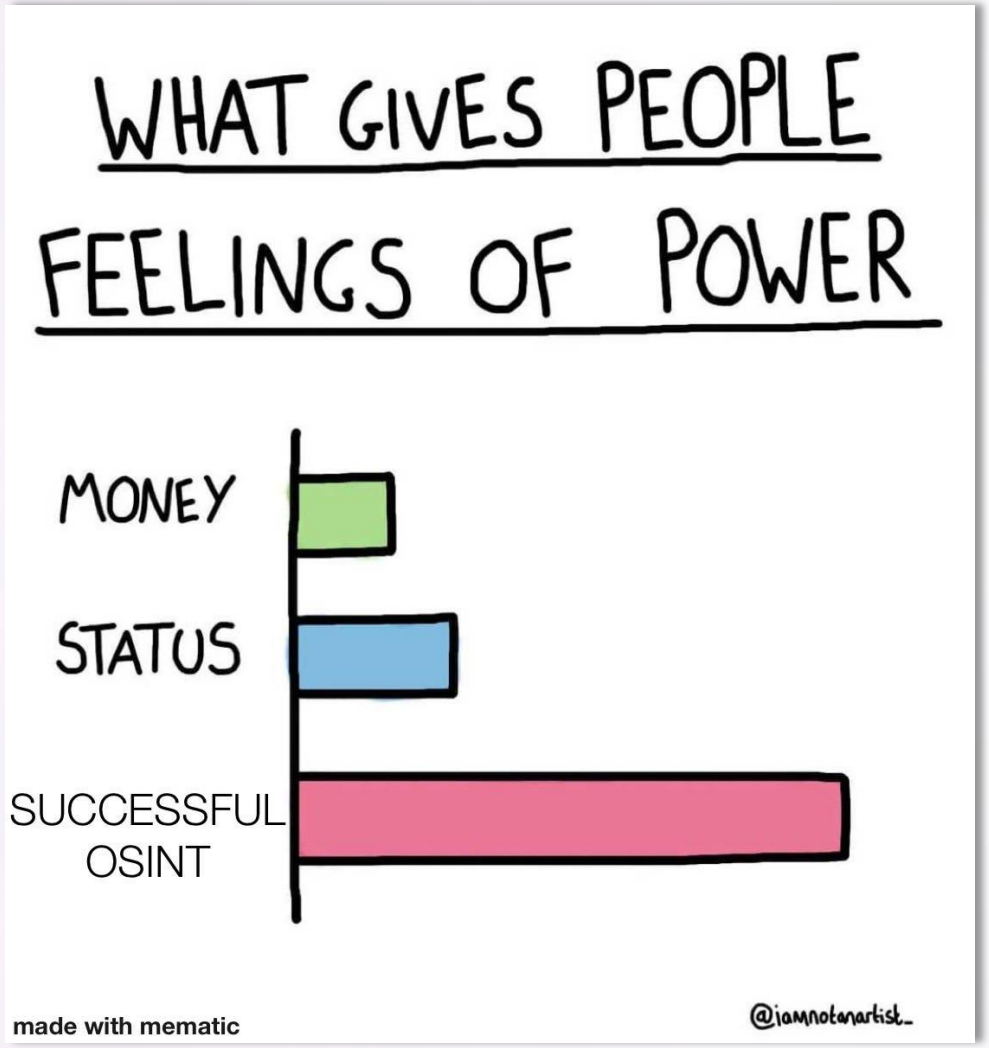
Jessica Lyons — Wed 19 Feb 2025 // 20:45 UTC

A free automated tool that lets anyone scan public GitHub repositories for exposed AWS credentials has been released.

Before you say anything, yes, we're pretty sure similar programs and services are out there – including GitHub's own built-in secrets scanner – but hey, where's the harm in highlighting today the fact that this sort of software is easily available?

OSINT – Tools

Google Dorking	Shodan	Censys
crt.sh	theHarvester	Hunter.io
HavelBeenPwned	Maltego	Spiderfoot
	Sublist3r	



crt.sh Identity Search

Criteria	Type: Identity	Match: ILIKE	Search: 'su

Certificates

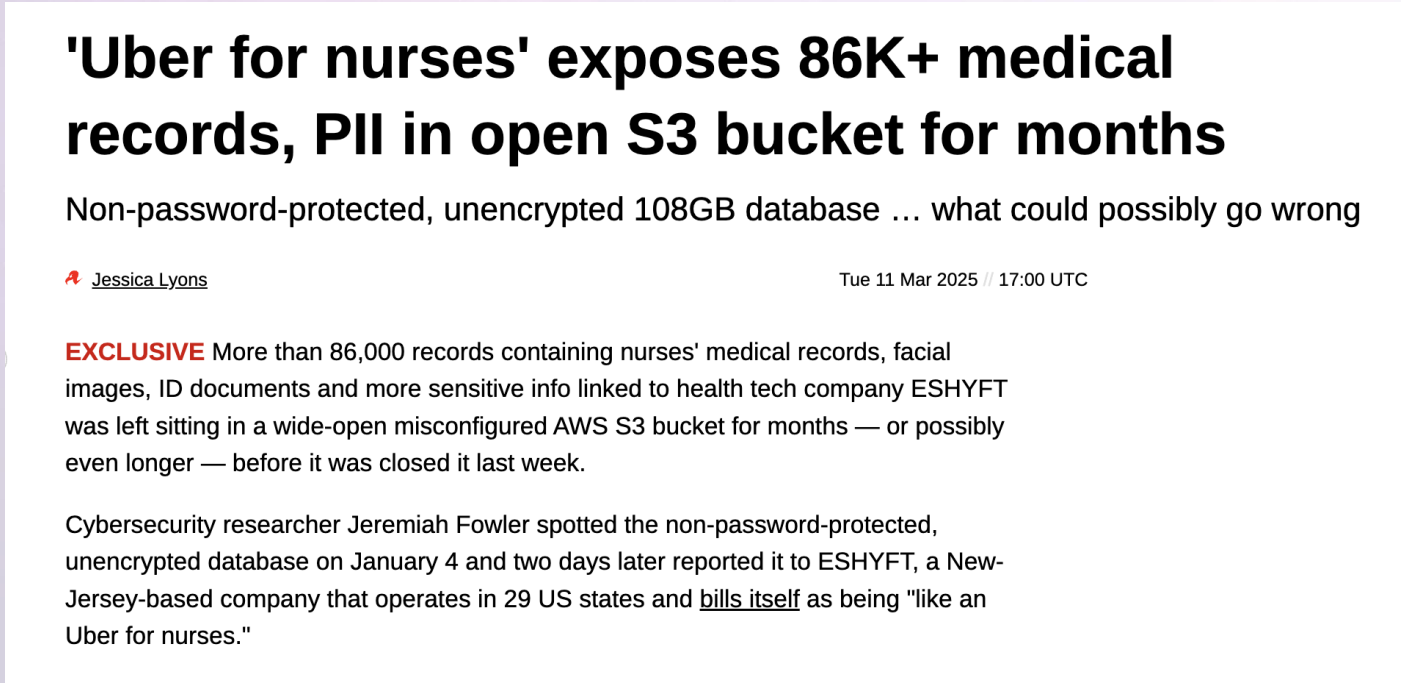
crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities
18918040417	2025-06-09	2025-06-09	2026-06-10	help.sundayriver.com	help.sundayriver.com
18832032621	2025-06-05	2025-06-05	2025-12-05	orderprocessor.sundayriver.com	orderprocessor.sundayriver.com
18747351976	2025-06-01	2025-06-01	2025-12-01	orderprocessor.sundayriver.com	orderprocessor.sundayriver.com
18731520003	2025-05-31	2025-05-31	2025-11-30	shopdev.sundayriver.com	shopdev.sundayriver.com
18714730468	2025-05-30	2025-05-30	2025-11-30	srunity.sundayriver.com	srunity.sundayriver.com
18713480208	2025-05-30	2025-05-30	2025-11-30	shop.sundayriver.com	shop.sundayriver.com
18706845626	2025-05-30	2025-05-30	2025-11-30	srunity-test.sundayriver.com	srunity-test.sundayriver.com
18701980023	2025-05-30	2025-05-30	2025-11-30	arrival.sundayriver.com	arrival.sundayriver.com
18642688977	2025-05-26	2025-05-26	2026-05-26	remoteaccess.boyne.com	remoteaccess.sundayriver.com
18642689136	2025-05-26	2025-05-26	2026-05-26	remoteaccess.boyne.com	remoteaccess.sundayriver.com
18610535334	2025-05-25	2025-05-25	2025-11-25	orderprocessor.sundayriver.com	orderprocessor.sundayriver.com
18610539144	2025-05-25	2025-05-25	2025-11-25	orderprocessor.sundayriver.com	orderprocessor.sundayriver.com
18513239760	2025-05-20	2025-05-16	2025-11-16	arrival-test.sundayriver.com	arrival-test.sundayriver.com
18497416308	2025-05-19	2025-05-16	2025-11-16	shop.sundayriver.com	shop.sundayriver.com
18496690725	2025-05-19	2025-05-16	2025-11-16	arrival.sundayriver.com	arrival.sundayriver.com
18476315557	2025-05-18	2025-05-16	2025-11-16	shopdev.sundayriver.com	shopdev.sundayriver.com
18448334057	2025-05-16	2025-05-16	2025-11-16	arrival-test.sundayriver.com	arrival-test.sundayriver.com
18441834618	2025-05-16	2024-12-29	2025-06-29	shop.sundayriver.com	shop.sundayriver.com
18441839492	2025-05-16	2025-05-16	2025-11-16	shop.sundayriver.com	shop.sundayriver.com
18441523238	2025-05-16	2024-12-29	2025-06-29	arrival.sundayriver.com	arrival.sundayriver.com
18441555243	2025-05-16	2025-05-16	2025-11-16	arrival.sundayriver.com	arrival.sundayriver.com
18433644131	2025-05-16	2025-05-16	2025-11-16	shopdev.sundayriver.com	shopdev.sundayriver.com
18402739301	2025-05-14	2024-12-29	2025-06-29	arrival-test.sundayriver.com	arrival-test.sundayriver.com
18402732766	2025-05-14	2025-05-14	2025-11-14	arrival-test.sundayriver.com	arrival-test.sundayriver.com
18098458789	2025-04-27	2024-12-10	2025-06-10	cms.sundayriver.com	cms.sundayriver.com

Misconfigurations- Cloud

- Overly permissive IAM roles and policies
- Lack of multi-factor authentication (MFA)
- Insecure network configurations (open security groups)
- Missing encryption for data in transit

Misconfigurations- Exposed Cloud Storage

> Publicly accessible S3 buckets, Azure blobs, Google Cloud Storage
> Misconfigured bucket permissions allowing read/write access
> Sensitive data leaks (credentials, backups, PII)
> Lack of access controls and auditing on storage endpoints



'Uber for nurses' exposes 86K+ medical records, PII in open S3 bucket for months

Non-password-protected, unencrypted 108GB database … what could possibly go wrong

Jessica Lyons Tue 11 Mar 2025 // 17:00 UTC

EXCLUSIVE More than 86,000 records containing nurses' medical records, facial images, ID documents and more sensitive info linked to health tech company ESHYFT was left sitting in a wide-open misconfigured AWS S3 bucket for months — or possibly even longer — before it was closed it last week.

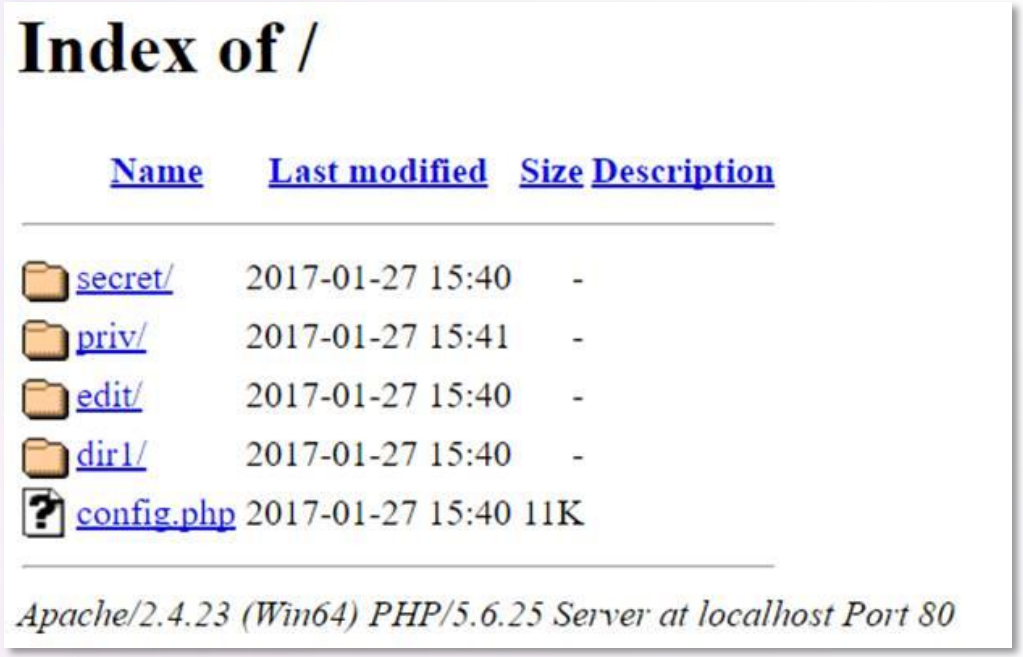
Cybersecurity researcher Jeremiah Fowler spotted the non-password-protected, unencrypted database on January 4 and two days later reported it to ESHYFT, a New-Jersey-based company that operates in 29 US states and bills itself as being "like an Uber for nurses."

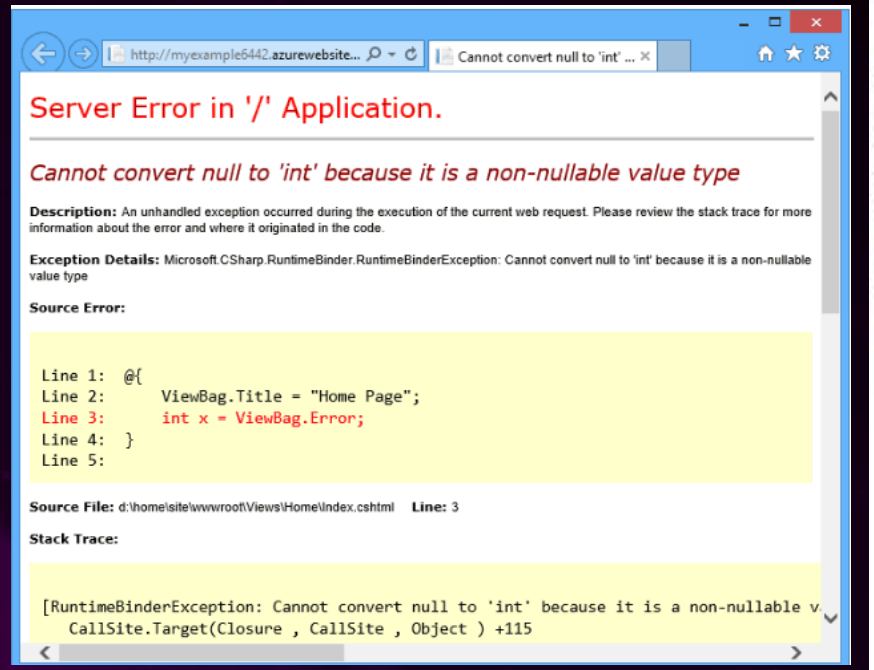
alexandria-poulin

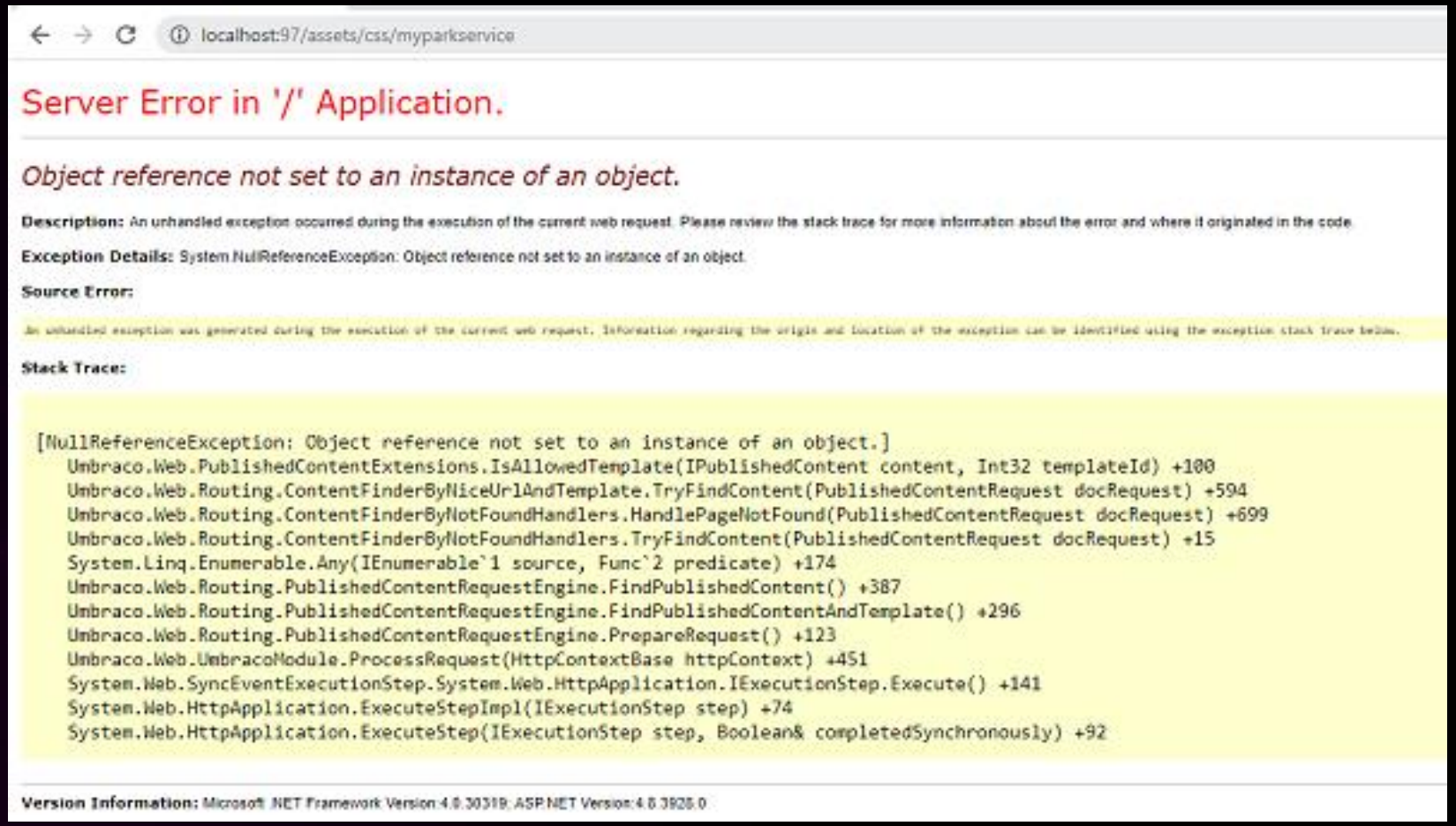
CLOUD SECURITY PARTNERS

Misconfigurations- Directory Listing, Sensitive Files & Error Exposure

- Directory listing enabled
- Exposure of config files, backups, logs
- Verbose error messages leaking system info







Outdated Dependencies

- Known vulnerabilities in old libraries or frameworks
- Exploits targeting unpatched software components
- Compatibility issues causing security gaps
- Increased attack surface due to unsupported versions

HOME › NEWS › SECURITY

Homeland Security Warns Log4j's 'Endemic' Threats for Years to Come

"Log4j is an 'endemic vulnerability' and vulnerable instances of Log4j will remain in systems for many years to come," the Cyber Safety Review Board noted.

July 15, 2022 By: Nancy Liu Comment

The U.S. Department of Homeland Security (DHS) released a report this week to warn of the continued risk posed by the Log4 vulnerability discovered in late 2021 and called it an "endemic vulnerability."

The study was conducted by the Cyber Safety Review Board, which was established in February following President Biden's Executive Order on improving the nation's cybersecurity. DHS Under Secretary for Policy, Strategy, and Plans Rob Silvers leads the board, and Google's Senior Director for Security Engineering Heather Adkins serves as the deputy chairwoman.

For its first report, the board worked with nearly 80 organizations and individuals to gather insights into the Log4j vulnerabilities and develop 19 actionable recommendations. Google's VP of Security Royal Hansen noted the company was one of the participants and shared its own experiences in responding to this and other incidents.

MSSP, MSP, Distributed Workforce, Ransomware

DragonForce Ransomware Group Exploits MSP's RMM Software in Attacks

May 29, 2025

Share

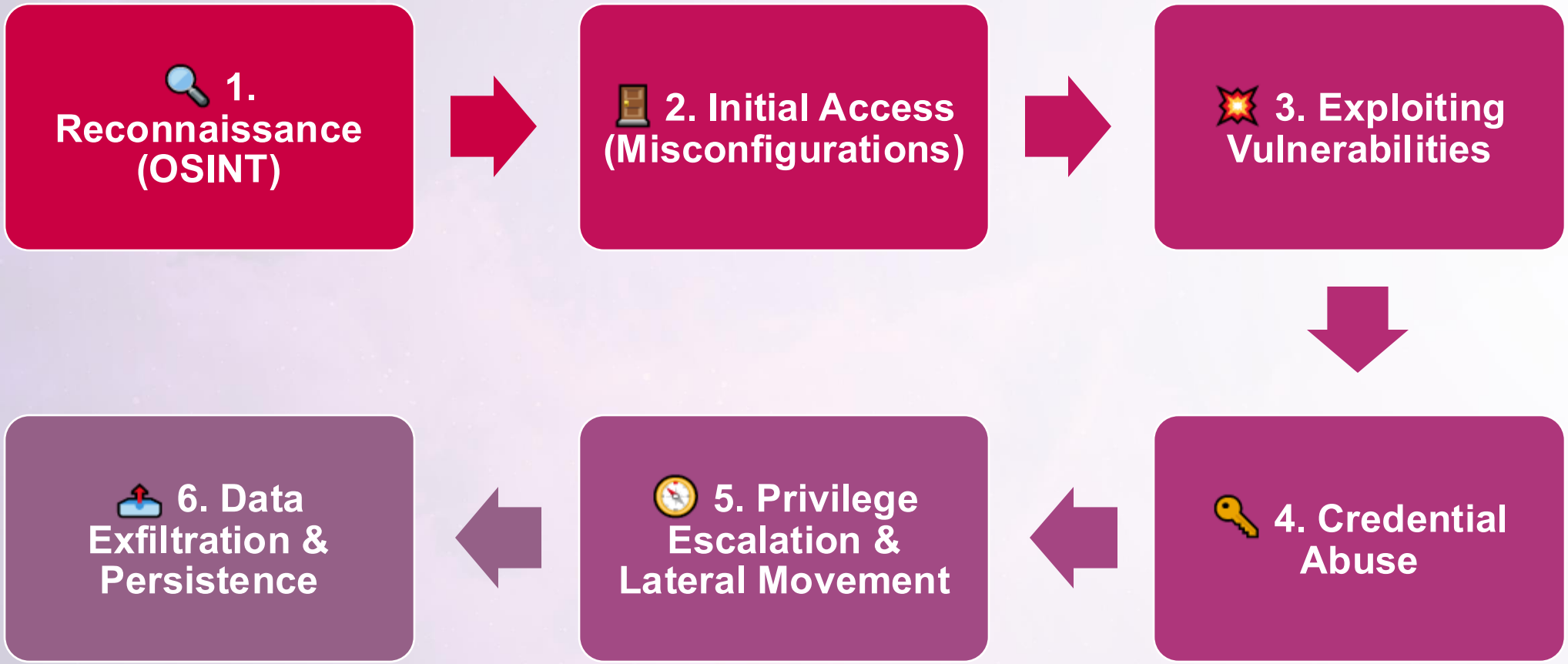
Default/Weak Credentials

> Default usernames and passwords often left unchanged
> Easily guessable or common passwords (e.g., "password123")
> Reused passwords across multiple accounts increase breach impact
> Credential stuffing and brute-force attacks exploiting reused creds
> Unauthorized access leading to data breaches and lateral movement

Other Common Vulnerabilities

SQL Injection (SQLi)	• Attackers inject malicious SQL queries to access or modify data
Broken Authentication	• Weak session management, credential leaks
Broken Authorization	• Users accessing resources or actions beyond their permissions
Cross-Site Scripting (XSS)	• Injecting malicious scripts into web pages viewed by others

Potential Attack Path



Ways to prevent it.

Image by pngtree.com

OSINT - Prevention

Limit Public Tech Details

- Avoid revealing tech stack specifics in job posts or public docs
- Minimize detailed infrastructure info on websites

Control Domain & DNS Info

- Use privacy protection on WHOIS records
- Monitor and restrict unnecessary subdomains

Secure Cloud & Infrastructure

- Audit and lock down public cloud storage and services
- Close unused ports and disable unnecessary services

Protect Employee Info

- Educate staff on oversharing company data on LinkedIn/socials
- Avoid publishing detailed org charts or contact lists publicly

Monitor & Respond

- Use tools like Shodan and crt.sh to monitor exposed assets
- Set alerts for certificates, domains, and cloud exposures

Principle of Least Privilege (PoLP)

Why its Important

- Reduces attack surface
- Limits damage from compromised accounts
- Prevents unauthorized access to sensitive systems and data
- Essential for compliance and secure architecture

Where to Apply it

- User accounts
- Admin and service accounts
- Cloud IAM roles
- Applications and APIs
- Third-party integrations

Principle of Least Privilege (PoLP)

- **OSINT**
  - Limits public exposure if accounts have minimal access and no over-permissioned services are discoverable
- **Misconfigurations**
  - Reduces blast radius of exposed systems and misconfigured resources
- **Outdated Dependencies**
  - If access is limited, even vulnerable components are harder to exploit meaningfully
- **Weak/Default Credentials**
  - Minimizes impact when compromised accounts can't access sensitive data
- **Common Vulnerabilities**
  - Prevents privilege escalation and unauthorized actions via app or API flaws

Logging and Monitoring

Tracking and analyzing system and user activity across your environment to detect suspicious behavior, troubleshoot issues, and meet compliance needs.

Why It's Important

- **Early Detection of Attacks**
- **Incident Response & Forensics**
- **Compliance & Audit Requirements**
- **Operational Visibility**

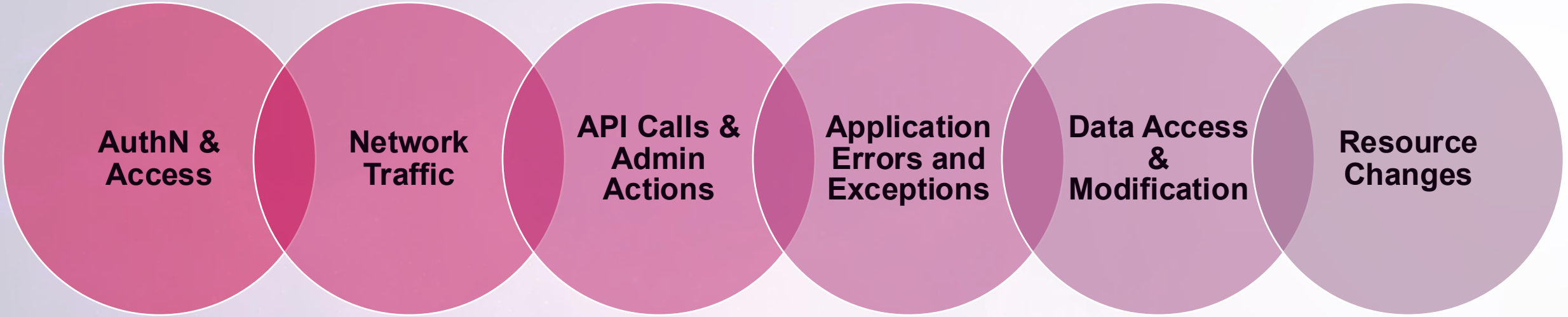
Logging and Monitoring

Centralize Logs	Log What Matters	Enable Retention & Archiving	Use Alerts & Thresholds
• Use a single platform to collect and correlate logs across systems and cloud providers.	• Focus on authentication events, privilege use, network traffic, API calls, and data access.	• Store logs securely and retain them per policy or compliance (e.g., 90 days, 1 year).	• Set up alerts for suspicious activity—multiple failed logins, unexpected admin actions, etc.

Logging and Monitoring

Limit Access to Logs	Regularly Review Logs	Integrate with SIEM
• Treat logs as sensitive data; only grant access to authorized personnel.	• Perform manual or automated reviews to spot patterns and identify threats.	• Use a Security Information and Event Management (SIEM) tool to automate correlation and alerting.

Where to Log & Monitor



Password Policy & Hygiene

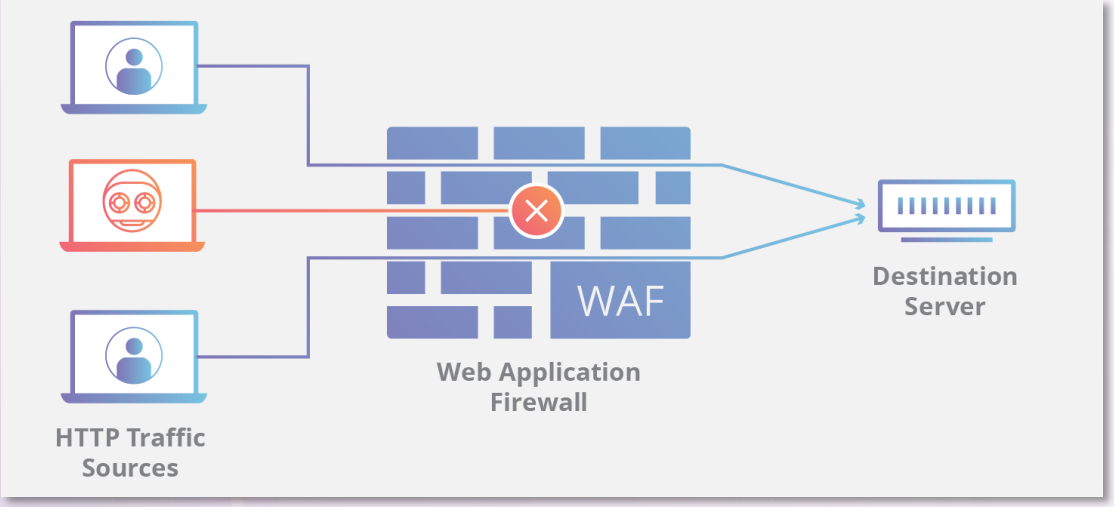
- Enforce strong password rules (length, complexity, no reuse)
  - Minimum 14 characters using (Upper, lower, number, and symbol)
- Require password changes every 90–180 days***
- Ban commonly used and breached passwords
- Use a password manager across the organization
- Implement and Enforce MFA

Easy IT Security Wins

- Enforce MFA across all systems
- Disable unused or stale accounts
- Change all default credentials immediately
- Restrict public access to cloud and network resources
- Patch outdated software and dependencies
- Limit admin access using least privilege principles
- Deploy a Web Application Firewall (WAF)

Web Application Firewall (WAF)

What it does:	Filters and blocks malicious traffic (e.g., SQL injection, XSS, bot attacks)
Why it matters:	Protects web apps from common threats



Web Application Firewall (WAF)

Easy Deployment Options:

- AWS WAF with CloudFront or ALB
- Azure WAF with Application Gateway
- Cloudflare, Fastly, or Imperva for SaaS WAF solutions

Best Practices:

- Start in monitor mode before blocking
- Customize rules for your app (e.g., rate limiting, geo-blocking)
- Regularly review logs and false positives

Configuration Review – What to Check

- Review cloud security groups/firewall rules for open ports
- Audit IAM roles for over-permissioned access
- Check storage settings for public access
- Validate logging and alerting configurations
  - Regularly review user access lists and admin privileges
- Compare current configs with secure baselines
  - CIS Benchmarks, AWS Well-Architected, Microsoft Secure Score

Scanning Tools IT Teams Can Use

External Exposure:

- Shodan / Censys
- Nmap
- Nessus

Web Apps:

- OWASP ZAP
- BURP Suite Pro

Cloud Environments:

- ScoutSuite
- Prowler
- Microsoft Defender for Cloud

Scanning Tools IT Teams Can Use

Why Third-Party Security Testing Matters

Independent, Objective Review

- Internal teams may miss issues due to familiarity or bias
- External experts bring fresh perspective and broader threat experience

Identify What You Overlook

- Catch misconfigurations, insecure defaults, and unknown exposures
- Validate controls and test your “assumed” security posture

Simulate Real-World Attacks

- Ethical hackers mimic adversaries to expose weaknesses
- Go beyond checklists—test how systems behave under real-world scenarios

Build Stakeholder Confidence

- Demonstrates due diligence to leadership, clients, and regulators
- Supports compliance (SOC 2, ISO 27001, HIPAA, etc.)

Third-Party Testing

When & How to Use Third-Party Testing

When to Engage

- Before product or app launches
- After major infrastructure changes (cloud migration, new integrations)
- Annually or quarterly as part of risk management cycles
- After incidents or in response to threat trends

Partner with the Right Firm

- Look for firms with experience in your industry and tech stack
- Ensure reports include clear remediation guidance
- Consider firms that align with your internal processes and maturity

Conclusion

- Public data and misconfigurations are low-effort, high-reward targets
- Easy IT wins can drastically reduce your attack surface
- Logging, patching, and privilege control = core defenses
- Third-party testing helps you see what attackers see
- Security isn’t a one-time task—it’s a continuous process

CLOUD SECURITY
PARTNERS

Thank you