SECURITY INFORMATICS

Introduction

INSIDE THIS ISSUE

Security Informatics

A Quarterly Publication

July 2023- September 2023

Regional Centre of Excellence for Application Security, Lucknow

Under the immense leadership of

Shri RH Khan
Dy. Director General
&
SIO, NIC-UP

&

Shri V.T.V. Ramana
Dy. Director General
&
HOG, CoE-AppSec

Under the able direction of
Shailesh Kumar Srivastava
Senior Director (IT) & HoD, CoEAS-UP

Team Members

Ravikar Srivastava, *Deputy Director (IT)*
Aparna Khare, *Deputy Director (IT)*
Rohit Sharma, *Deputy Director (IT)*
Divyanshi Kushwaha, *Deputy Director (IT)*
Aviral Awasthi, *Assistant Director (IT)*

(There has never been any Hired Resource/Auditor since inception)

As the National Informatics Centre intensifies its efforts in developing and launching an array of web and mobile applications using state-of-the-art technologies, the call for rigorous application security audits and penetration testing has concurrently amplified. This surge in demand reflects the evolving landscape of cyber threats that lurk in the digital realm. Penetration testing activities have taken precedence, delving deep into systems to identify vulnerabilities that could be exploited by malicious entities. While adherence to SSL and TLS compliance remains important, the central emphasis is now on the comprehensive evaluation and testing of applications through Penetration Testing Activity to ensure they are impervious to external threats. The Regional Centre of Excellence for Application Security, Lucknow, shoulders the responsibility of upholding these testing standards for the seven states in its jurisdiction, fortifying the nation's digital infrastructure against potential threats.

The Regional Centre of Excellence for Application Security, Lucknow handles application security activities for seven states, namely, ***Uttar Pradesh, Uttarakhand, Himachal Pradesh, Punjab, Chandigarh and Jammu & Kashmir.***

Work Highlights

Centre Of Excellence for Application Security, Lucknow Work Highlights

ACTIVITIES UNDERTAKEN

Several activities were undertaken to enhance the safety and security of web applications, including infrastructure scans (300+), penetration testing (20+ new tickets, and 50+ follow ups), black box, white box and manual audits (40+), SSL compliance scans(100+ new scans) , and development of modules for CoEAS applications (ASTS and ASAMS). However, for this quarter, the primary emphasis is on Penetration Testing activity. The escalating cyber threats and the imperatives of ensuring robust application security have catapulted Penetration Testing to the forefront of our security measures. In response, the organization is channeling more resources and focus towards ensuring our web applications undergo comprehensive penetration testing. This activity is not just about identifying vulnerabilities, but also understanding how attackers might exploit them. By simulating cyberattacks in a controlled environment, we assess the strength of our systems against real-world threats. Undertaking Penetration Testing is pivotal in upholding the highest echelons of security for our organization's web applications and infrastructure. It empowers us to be proactive, staying not just abreast but ahead of potential security risks and threats.

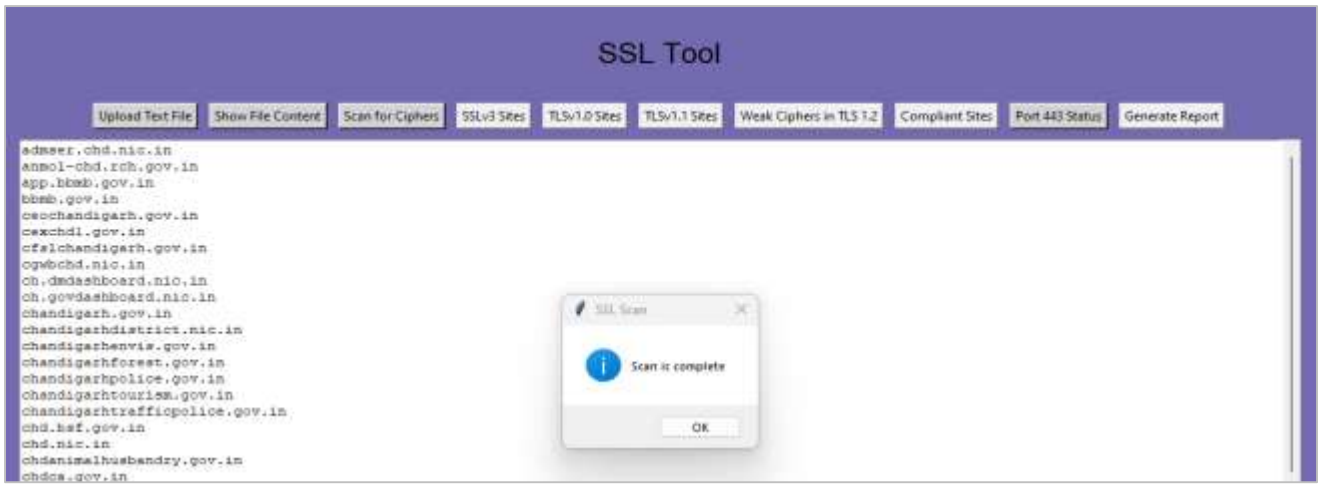
PENETRATION TESTING ACTIVITY

In the ever-evolving landscape of cyber threats, penetration testing stands as an indispensable tool to fortify an organization's digital defenses. In our recent penetration testing activity, the results were particularly enlightening. We successfully closed more than 50 outstanding tickets, indicating that previously identified vulnerabilities were addressed and rectified. Additionally, the activity spurred more than 50 follow-ups, underscoring the diligent and ongoing efforts to ensure that all potential threats are thoroughly investigated. However, it's worth noting that the process also led to the discovery of new vulnerabilities, resulting in around 10 fresh tickets being raised. Such findings reiterate the importance of regular penetration testing.

INNOVATIVE WORK DONE : SCANNING SUITE TOOL (VERSION 1.0)

A graphical user interface (GUI) application is designed to analyze the security of SSL/TLS configurations on web servers. Developed using Python this tool offers various functionalities including scanning for ports, Scanning for SSLv3, TLS 1.0 or TLS 1.1 vulnerable sites. Apart from this the tools can give the list of compliant sites which are not running on any weak ciphers.

This tool aims to help security professionals and system administrators evaluate and improve the SSL/TLS configurations of their web servers by providing an easy-to-use interface for conducting scans and generating reports.



Recent Incidents

Rising Ransomware Onslaught: Deciphering Trends and Fortifying Defenses

Image Source: https://pixabay.com/photos/ransomware-cybersecurity-cyber-3998798/

Ransomware attacks have seen a significant surge in India, with 73% of surveyed organizations admitting to being targeted, a sharp increase from the previous year's 57%. Surprisingly, while 77% of these attacks resulted in data encryption, only 44% opted to pay the ransom, a significant decrease from the prior year's 78%. Notably, the education sector emerged as the primary target, with both higher and lower education institutions bearing the brunt almost equally. The study revealed that paying ransoms often doubled recovery costs, and the recovery times were generally longer than using backups. Furthermore, the overall financial impact extended beyond just the ransom amount, as organizations grappled with potential reputational damage and lost operational hours. Interestingly, exploited vulnerabilities and compromised credentials were identified as leading causes for successful attacks, accounting for 35% and 33% respectively. As cyber threats continue to evolve, organizations are urged to bolster their defense mechanisms and maintain updated backups. The survey, conducted by a leading cybersecurity firm for its annual ransomware report, encompassed 3,000 cybersecurity and IT professionals from 14 countries between January and March 2023.

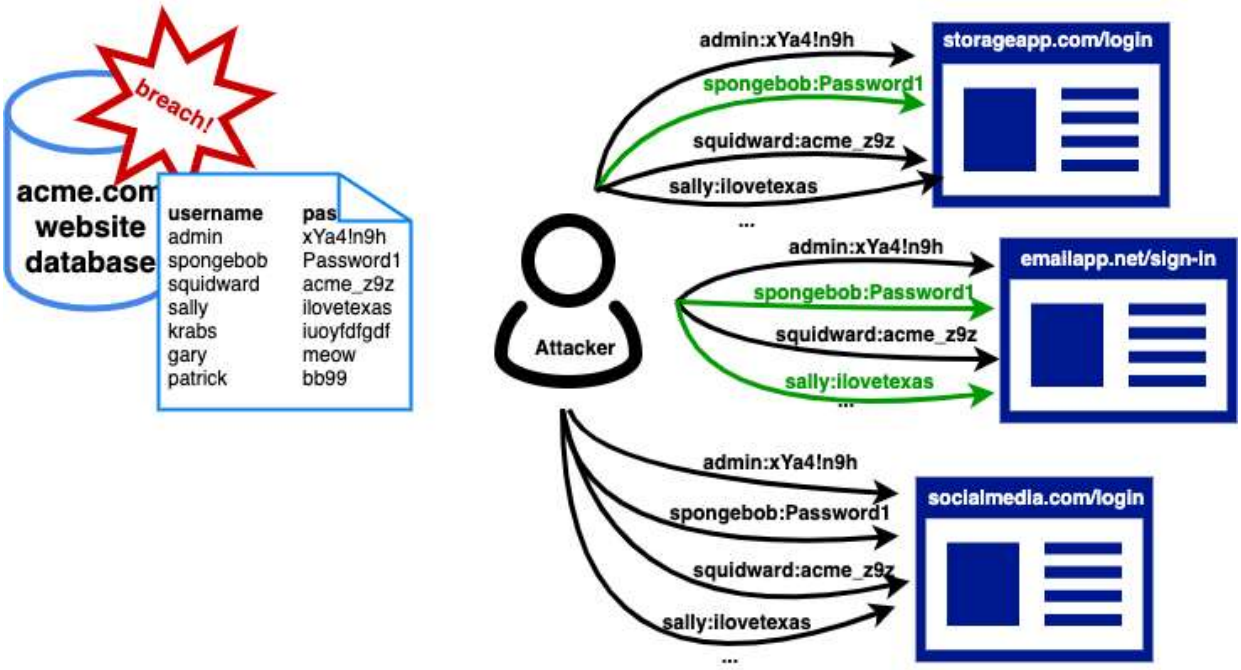
Resources for Further Reading:

https://www.thehindu.com/sci-tech/technology/education-sector-worst-hit-ransomware-attacks-rise-india/article66891972.ece

Knowledge Hub

The Menace of Credential Stuffing and the Path to Defense

As the digital world becomes more entwined with our daily lives, the protection of online accounts and data stands as a pivotal concern. A rising threat in this digital era is 'Credential Stuffing,' an attack method that exploits individuals who reuse passwords across multiple sites. Let's delve into what it is, how it operates, and the measures to guard against it.



Credential Stuffing

Image Source https://owasp.org/www-community/attacks/Credential_stuffing

WHAT IS CREDENTIAL STUFFING?

Credential stuffing is a type of cyber-attack where attackers use automated scripts to try large numbers of username and password combinations (often obtained from previous data breaches) across various websites, hoping that individuals have reused credentials.

HOW CREDENTIAL STUFFING IS EXECUTED:

1) **Obtaining Credentials**: Attackers first acquire sets of usernames and passwords, usually from dark web marketplaces or other illicit sources. These credentials typically come from previous data breaches.

2) **Automating Attacks**: Using automated tools or bots, attackers then try these credentials on various online services, such as email providers, e-commerce sites, and banking sites.
3) **Gaining Unauthorized Access**: With many individuals reusing passwords across multiple platforms, attackers inevitably gain access to several accounts.
4) **Exploitation**: Once inside, attackers can steal personal and financial data, make fraudulent purchases, or even use the compromised account as a launchpad for further attacks.

HOW THE ATTACK IS POSSIBLE:

1) **Reuse of Credentials**: The primary enabler of these attacks is the widespread reuse of passwords. Many individuals use the same password across multiple services, making them vulnerable.
2) **Proliferation of Data Breaches**: Frequent data breaches, big and small, mean that a large number of usernames and passwords are floating around in the darker corners of the internet.
3) **Sophisticated Bots**: Modern bots can mimic human behavior, bypassing CAPTCHAs and other security mechanisms to launch large-scale attacks without detection.

STEPS TO PREVENT CREDENTIAL STUFFING:

1) **Unique Passwords**: Always use a unique password for each service or website. It ensures that if one account is compromised, others remain safe.
2) **Password Managers:** Utilize password managers like LastPass or 1Password. They can generate and store complex passwords for each site you use, eliminating the need to remember each one.
3) **Two-Factor Authentication (2FA):** Enable 2FA wherever possible. Even if attackers have the correct password, they'd need a second verification method to access the account.
4) **Monitor for Breaches**: Services like "*Have I Been Pwned?*" can notify you if your email appears in a data breach.
5) **Educate and Train**: Ensure that everyone in an organization understands the risks and adheres to best practices, reducing the chances of successful attacks.
6) **Implement CAPTCHAs and Security Questions:** While not foolproof, they can deter automated attacks.
7) **Rate Limiting: Implement rate-limiting on login attempts**. After a certain number of failed tries, block further attempts for a set period.
8) **Monitor Account Activities:** Regularly monitor account activities for any suspicious actions and set up alerts for unfamiliar logins.

Resources for Further Reading:

https://owasp.org/www-community/attacks/Credential_stuffing

Advisories

List of Advisories

- **Regularly Update and Patch**: Always keep your server operating systems, software, databases, and all web platforms (like WordPress, Joomla) up to date. Many attacks exploit known vulnerabilities in outdated software.
- **Use HTTPS:** Implement SSL/TLS to encrypt data between the client and server. This prevents man-in-the-middle attacks and ensures data integrity.
- **Input Validation**: Always validate and sanitize inputs to prevent SQL injection, script injection, and other injection attacks. Inputs include form data, URLs, and any data from external sources.
- **Implement Content Security Policy (CSP):** This helps prevent cross-site scripting (XSS) by controlling which resources can be loaded.
- **Secure Password Policies**: Enforce strong password policies for users. Implement multi-factor authentication wherever possible.
- **Session Management**: Use secure methods for session management. Ensure session IDs are randomly generated, use HTTPS for transmitting session cookies, and set the "HttpOnly" and "Secure" flags for cookies.
- **Limit Rate of Requests**: Implement rate limiting to prevent brute force attacks on login and other transactional operations.
- **Least Privilege Principle**: Ensure that software components run with the least privilege necessary. If a component only needs read access to a database, do not give it write access.

Feel free to contact in case of any queries/feedback:

Shailesh Kumar Srivastava
HoD, CoEAS-Lucknow
Email - **shailesh.srivastava@nic.in**
IP Phone- **47055**