ICT DIVISION
FUTURE IS HERE

BANGLADESH COMPUTER COUNCIL
COMPUTER FOR EVERYTHING

BGD e-GOV CIRT

Advisory on Web Application and Database Security

Cyber Threat Advisory

Advisory on Web Application and Database Security

TLP: CLEAR
Distribution: Public
Date: 25 July 2024

Overview

In recent days, the Cyber Threat Intelligence Unit of BGD e-GOV CIRT has observed an alarming rise in cyber-attacks targeting web applications and database servers of different organizations in Bangladesh.

Hackers and hacktivists are continuously attempting to deface government websites, exfiltrate critical business information, and carry out DDoS attacks to disrupt online services and promote their propaganda. This advisory is issued to urge concerned organizations to take necessary precautions to safeguard their presence in cyberspace.

Top Threats and Attack Trends:

1. DoS/DDoS attacks
2. Exploitation of database software vulnerabilities
3. SQL/NoSQL injection attacks
4. Insecure Direct Object Reference (IDOR) vulnerability exploitations
5. Breaches of compromised organizational databases from web and mobile applications

Root Causes:

Web and Mobile Applications:

1. Applications are not developed by following secure coding practices.
2. Default parameters are used for configuring applications and web services.
3. Lack of proper authorization and authentication in API development, handling, and management of web applications.
4. Absence of proper error handling capabilities in web and mobile applications.
5. Lack of strict session management controls for accessing and surfing web applications.
6. Failure to ensure secure communication protocols like SSL/TLS to encrypt data in transit between client and server.
7. Applications and databases are configured and running with default ports, protocols, and credentials.
8. Negligence in configuration hardening and continuous patch updates and upgrades for software, OS, and databases.
9. Insufficient or non-existent logging and monitoring practices.
10. Inadequate control to protect administrative or privileged access roles.

11. Lack of security measures to protect websites.

Databases:

1. Exploitation of database software vulnerabilities.
2. Remote login to application and database servers is configured and enabled for continuous maintenance by vendors, designers, and developers, which attackers exploit to gain remote access.
3. Use of leaked or exposed administrative credentials by threat actors.
4. Absence of proper authorization, authentication, and user verification, including multifactor authentication (MFA) for administrative access roles.
5. Lack of attack surface monitoring and continuous remediation strategies to reduce attack surface.

Organizations are strongly advised to address these vulnerabilities and implement robust security measures to protect their digital assets from these escalating threats.

Remediation Strategies:

Database and Application Security

- Use parameterized queries and ORM frameworks.
- Regularly validate and sanitize user inputs.
- Encode user inputs before displaying them.
- Implement Content Security Policy (CSP).

Database Access Management (DAM)

- Restrict database access to authorized users.
- Continuously monitor database activities.

Software Maintenance

- Patch all software and plugins frequently.

Log Monitoring (SIEM)

- Monitor logs for real-time threat detection.
- Detect anomalies and unusual activities.

Web Application Security

- Use WAF to safe guard against web threats.
- Deploy anti-DDoS solutions.

Incident Response

- Have predefined incident response plans.
- Minimize breach impact with quick containment and appropriate strategies.

Availability and Redundancy

- Implement redundancy mechanisms.
- Support plans to minimize downtime.

Web Security Practices

- Use security plugins.
- Disable remote file inclusions.
- Use the real path function.
- Implement CSRF tokens in forms.
- Use Same Site cookies.
- Check referrer and origin headers.
- Limit server file access.
- Configure web servers to deny access.
- Conduct regular VAPT.

Best Practices

- Harden applications according to OWASP standards.

  https://owasp.org/www-project-web-security-testing-guide/stable/

Previous Advisory/Alert

- https://www.cirt.gov.bd/surge-on-web-defacement-web-vulnerabilities-bd/

- https://www.cirt.gov.bd/traditional-vapt-vs-effective-security-testing-assessment-program-for-enterprises/