

GOVERNMENT OF PAKISTAN  
CABINET SECRETARIAT, CABINET DIVISION  
NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD  
(NTISB-II)

No. 1-5/2003 (NTISB-II)

Islamabad 15 August, 2018

Subject: Advisory - Prevention Against Hacking Attempts on National Day

(Advisory No 151)

17 AUG 2018

M(A)

M(I.T)

A.S (Rev 2 Div)

1. Context. Since the dawn of computing in Pakistan, there has always been a looming threat of cyber-attacks, espionage and sabotage. In this regard, various hostile elements launch offensive operations to cripple cyber infrastructure of Pakistan. Recently, websites of multiple departments of the government of Pakistan, including the Establishment division, the Law Ministry, ministry of Inter Provincial Cooperation, Ministry of Defense etc were hacked.

2. Implications of Cyber-attacks on National Day. Hackers performing malicious cyber activities on national days have serious consequences. Detail as under:-

- a. Loss of critical and sensitive national data.
- b. Display of anti-state content on national websites (web defacement).
- c. Unavailability of online services due to Denial of Service attack.

3. Hacker Strategy. Hackers are using multiple techniques to deface websites and gain illegitimate access to Pakistani servers through following technical means:-

- a. SQL Injection attack.
- b. Input Validation attack.
- c. Buffer overflows attack.
- d. Cross request forgery attack.
- e. XML External Entity XXE attack.

4. Remedial Measures. Following best practices are recommended to safeguard digital space:-

- a. Input sanitization on website.
- b. Keep Web server (Apache/HS/Tomcat) updated with the latest releases and patches.
- c. Implementation of secure login session.
- d. Do not use default configuration.
- e. Stores configuration files securely.
- f. Scan the applications running on the web server for all vulner

FBR eDOX No. 99489-R  
Received in Member (I)  
Dated 20/8/18

CC17  
Rep  
fig

9 2489  
FBR eDOX Dy. No.  
Received in Ch. Sect

ilities.

- g. Use secure protocols.h. **Disable** default account, follow **strict access control** policy.  
Install **anti-virus** and update it **regularly**.
- j. All **OS** and **software** used should be **latest** and **updated**.
- k. Enable **Fraud** warning in **safari browser**.
- l. **Turn off** unnecessary **services/ modules**.
- m. Ensure that **Apache Server-info** is **disabled**.
- n. Ensure that server **signature** is **disabled**.
- o. **DistribUte ownership** and don't run Web server as '**root**'.
- p. Install **WVAP (Web application Firewall)** and **DDOS** protection.
- q. Always keep **CMS (Wordpress, Joomla)** and **plUgins Updated**:
- r. **Admin panel** of Web,Site be only accessible via **White-listed IP**:
- s. Disable **Anonymous:IFTP** account.
- t. **Disable Root user** and **remote access** of Database server.
- u. **Store password** in **Fl6sh** form and do not save important **configuration** in Public folder.

5. **Recommendations**

- a. Strictly follow all **mitigation measures** mentioned at **Para 3** for **safety of digital infrastructure**.
  - b. Perform **vulnerability assessment** and **penetration testing** of website/ databases and share report with **iCERT**.
  - c. Employment of **dedicated** and **trained source** for managing **information security** of all **static** and **live data**.
6. Forwarded for perusal and dissemination of information to all concerned, please.

  
Major  
(Ch Usman Firdous)  
Assistant Secretary-II (NTISB)  
Ph# 051-9204560

✓ **All Secretaries of Ministries / Divisions of Federal Government and Chief Secretaries of Provincial Governments**

Copy to :-

SPS to Cabinet Secretary, Cabinet Division , Islamabad

PS to AS-III, Cabinet Division, Islamabad

APS Secretary, NTISB

APS Deputy Secretary, NTISB