

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

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

Islamabad 29 August, 2018

Subject: Advisory - Prevention Against Hacking Attempts (Advisory No 156)

1. Context. During cyber monitoring of critical information infrastructure websites, **balochistanculture.gov.pk** was found compromised by Indian hacker. Hackers defaced the main page of website and displayed Indian flag alongwith Indian National anthem.

Remedial Measures. Above in view, following remedial measure may be followed to safeguard website in future:-

- a. The webserver account be **recreated** to prevent **unauthorized access to webserver.**
- b. Website be scanned using an **updated antivirus** before uploading.
- c. Restore website from **offline backup.**
- d. Input from client be **sanitized** to prevent any malicious script injection.
- e. Web server (**Apache/ IIS/ Tomcat**) be updated with the latest **releases** and **patches.**
- f. **Secure login session be implemented** (if necessary).
- g. **Configuration** files be stored securely.
- h. Enable **Https protocols.** **Disable** default account and follow **strict access** control policy.
- j. **Turn off unnecessary services/ modules.**
- k. Ensure that **Apache server-info** is **disabled.**
- l. Ensure that server **signature** is **disabled.**
- m. **Distribute ownership** and don't run Web server as '**root**'.
- n. Install **WAP (Web application Firewall)** and **DDOS** protection.
- o. **Admin panel** of Website be only accessible via **White-listed IP.**
- p. **Disable Anonymous FTP** account.
- a. **Disable Root user** and **remote access** of Database server.
- r. **Store password** in **Hash** form and do not save important **configuration** in Public folder.
- s. **Logs retention** be enabled on quarterly basis.

3. Recommendations.

- a. Strictly follow all **mitigation measures** mentioned at **Pate 2** for **safety of 1digital infrastructure**

03 SEP 2018
M(A)
M(I.T)
A.S(Rev. Secy)

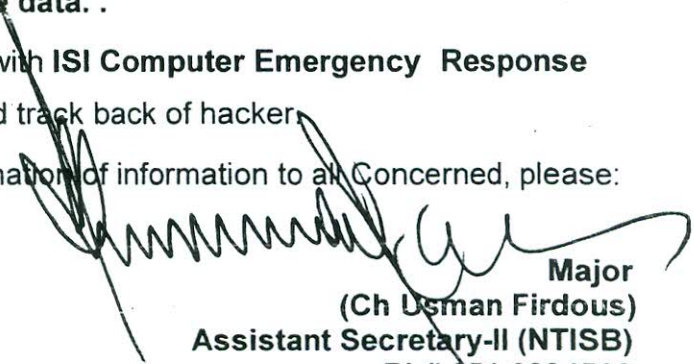
C(17)
40
7/19

FBR eDOX No. 103684-R
Received in Member (IT)
Dated 24/9/18
FBR eDOX Dy. No. 103684-R
Received in Ch. Secy.
on 03 SEP 2018

4-9-2018

Please send to PAGE for uploading on website
SS - IT
Assistant IT

- b. Perform **vulnerability assessment** and **penetration testing** of Website/ databases and share report with **ICERT**.
 - c. Employ **dedicated and trained resource** for managing **information security** of all **Static** and **live data** .
 - d. **Webserver logs** be shared with **ISI Computer Emergency Response Team** for further analysis and track back of hacker.
- 4 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 to Secretary, NTISB
- APS to Deputy Secretary, NTISB