Subject:- **Cyber Security Advisory – Vulnerable NHA website and Motorway Mobile Application (Advisory No. 93)**

1. It has been observed that National Highway Authority's (NHA) website **(nha.gov.pk)** and Motorway's M-Tag mobile application **onenetwork.pk** are vulnerable to cyberattacks. Critical vulnerabilities such as **SQL Injection, Directory Listing** and **broken authentication** etc have been identified in subject website and mobile application. Exploitation of these vulnerabilities may result in compromise of webserver, remote command & control and partial authentication of users. It is also recommended that M-Tag application be thoroughly screened by 3rd party from Cyber Security aspect before its official launching. Moreover, an advisory is attached at **Annexure A** for compliance.

2. Disseminate the same message in your organizations, all attached / affiliated departments and ensure Cyber Security aspect of web / mobile applications that contain **personally identifiable information (PII)** or **citizen's data.** The PII or citizens data must be protected by ensuring **secure software development practices, hosting services and security testing** of web / mobile applications **prior to their official launch**.

Annexure-A

Cyber Security Advisory – Vulnerable NHA website and Motorway Mobile Application (Advisory No. 92)

1. The identified vulnerabilities, their impact and recommended mitigation measures are as under :-

Ser	Vulnerability	Description	Mitigation
a.	SQL Injection (mis.nha.gov.pk) RAMD, LBMIS, PMIS (**Appendix I**)	An attacker may execute arbitrary statements on the vulnerable system. This may compromise integrity of Database and expose sensitive information	• Data received from external parties must be validated such that only the value that passes the validation can be processed. • By employing parameterized queries, user input is automatically quoted and the user / attacker supplied input will not cause change of the intent. This coding style helps prevent SQL injection attack. • Stored procedures can reduce direct access to fractions of database, making it essential in database security. • Always use character-escaping functions for user-supplied input provided by database management system (DBMS). This is done to make sure that DMBS never confuses it with SQL statement provided by developer.
b.	Weak Password RAMD, LBMIS (**Appendix II**)	An Attacker can access the content of web pages	Use strong passwords at all levels
c.	Directory Listing Enabled (**Appendix III**)	Directly listing is enabled on website that can results in increasing attack surface during exploitation and leakage of data.	Web servers should be configured to disable directory listing by default

d.	Cross Site Scripting (mis.nha.gov.pk)	Malicious users may inject JavaScript, VBScript, ActiveX, HTML or Flash into a vulnerable application to lure users to gather data from them. An attacker can steal the session cookie and take over account, impersonating the user. It is also possible to modify the content or the page presented to the user.	• Whenever possible prohibit HTML code in inputs • Validate Inputs. Validating the data to ensure it meets specific criteria. • Secure cookies. By setting rules for web applications defining how cookies are handled can prevent XSS and even block JavaScript from accessing cookies • Use a web application Firewall (WAF). Rules can be created on WAF to specifically address XSS by blocking abnormal server requests
e.	Insecure Communication **(http://mis.nha.gov.pk) (http://nha.gov.pk)**	Website communicates over insecure HTTP protocol	Incorporate secure certificate (https)
Motorway M-Tag Mobile Application (onenetwork.pk)			
f.	M-Tag Onenetwork Mobile Application; **Broken Authentication Flaw** (**Appendix IV**)	• An attacker can utilize Onenetwork server to send customized SMS instead of OTP to anyone with knowledge of victim's phone number. • Authentication tokens can be reused for any person and tokens are generated prior to complete user authentication.	Two factor authentication must be ensured by sending an OTP to registered phone number only to avoid illegitimate / unauthorized access to potentially sensitive data.

2. **Cyber Security Best Practices for Website and Mobile Application**

a. **Upgrade OS** and **Webserver** to latest version.

b. Website **admin panel** should only be accessible via **white-listed IPs.**

c. **Vulnerability Assessment and penetration testing** of application be carried out to identify potential threats **on routine basis.**

d. Complete website be **deployed on inland servers** including **database** and web infrastructure.

e. **HTTPS** protocol be used for communication between client and web server.

f. **Application and database** be installed on **different machines** with proper security **hardening**.

g. Sensitive data be stored in **encrypted** form with **no direct public access.**

h. Proper **security hardening of endpoints** and servers be performed and no **unnecessary ports** and applications be used.

i. Updated **Antivirus tools / Firewalls** be used on both endpoints and servers to safeguard from potential threats.

j. Enforce a strong **password usage policy.**

k. Remote management services like **RDP and SSH must be disabled** in production environment.

l. Deploy **web application firewalls** for protection against web attacks.

m. Employ **secure coding practices** such as parameterized queries, proper input sanitization and validation to remove malicious scripts.

n. Keep **system and network devices** up-to-date.

o. For attacker's reconnaissance, **Log retention policy** must be devised for at least 3x months on separate device.

p. In case of mobile applications, two factor authentication must be ensured by sending an OTP to registered phone number only to avoid illegitimate / unauthorized access to potentially sensitive data.

q. The mobile application must communicate with secure services over https to avoid MITM attacks. Android SSL pinning must be implemented as an additional security measure at application level.

r. Enable Android ProGuard for optimization and obfuscation of Android to thwart reverse engineering attempt.

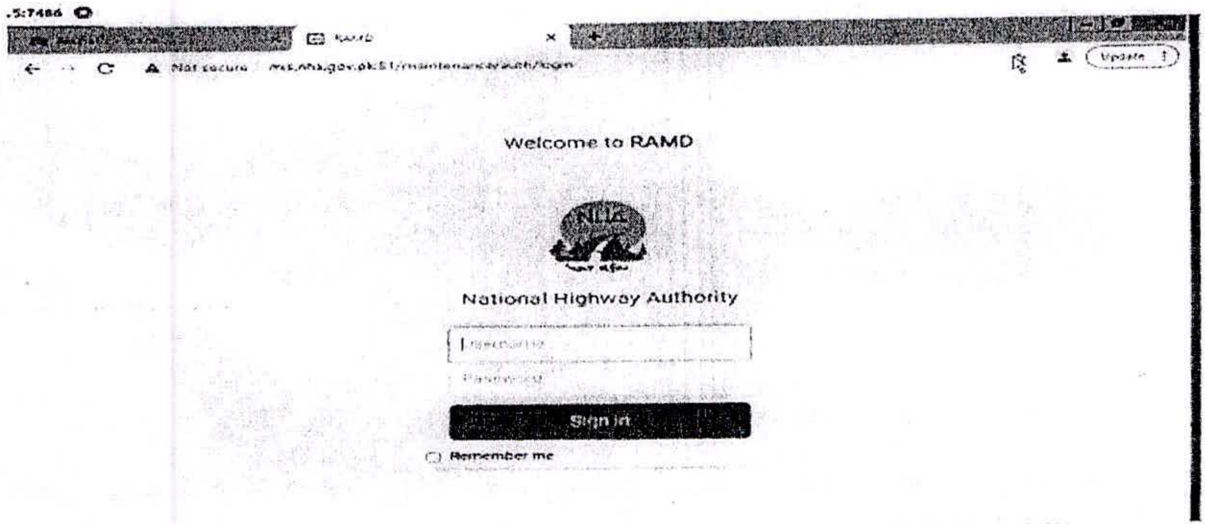
s. Vulnerability of mobile application must be carried out before public launch.

t. Adhere to Mobile Application Security Best Practices available at the link https://developer.android.com/topic/security/best-practices.

3. **Reporting of Cyber Security Issues / Queries.** For reporting malware or any other query or issues regarding Cyber Security, details may please be forwarded to the following email address: -

asntisb2@cabinet.gov.pk

Appendix I

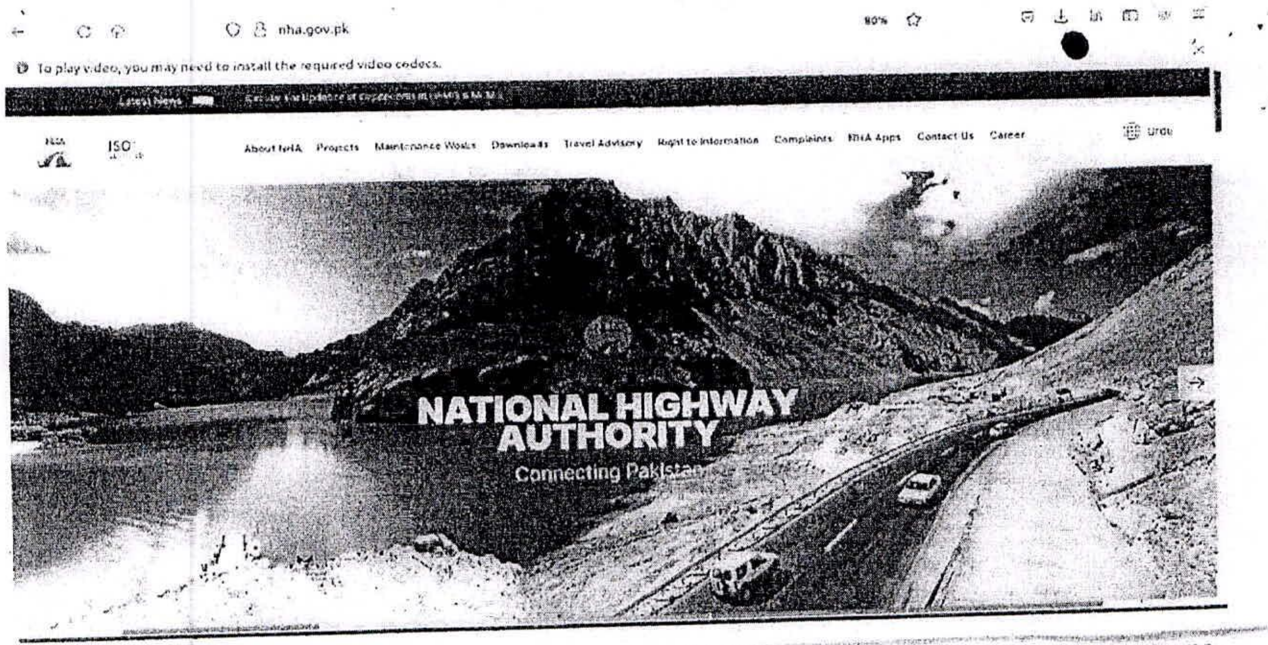


●	SQL injection	http://mis.nha.gov.pk:81/pmis/auth/login
●	SQL injection	http://mis.nha.gov.pk:81/lbmis/auth/login
●	SQL injection	http://mis.nha.gov.pk:81/maintenance/auth/login

Appendix II

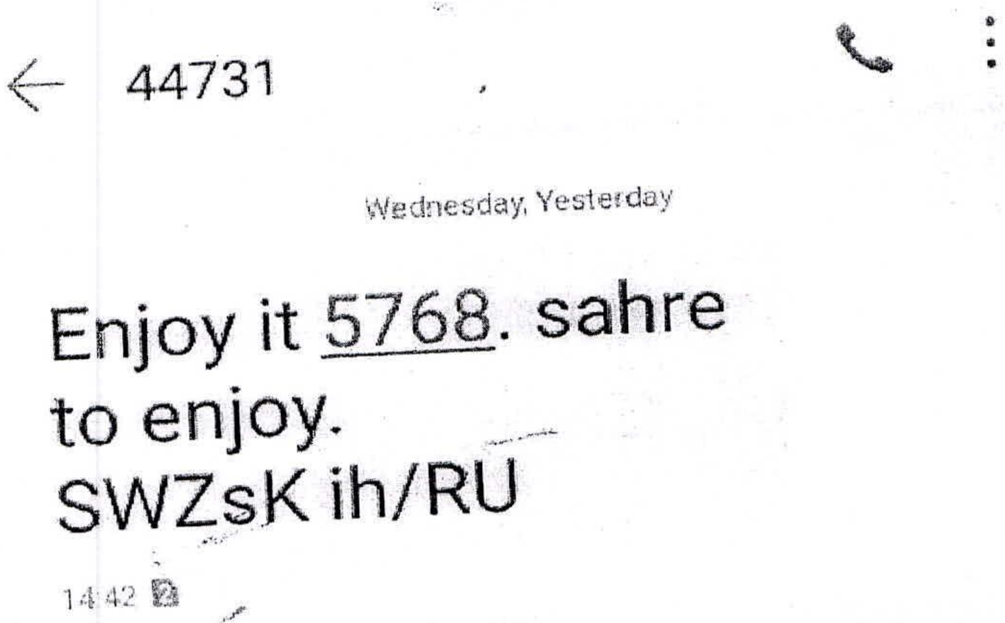
```
POST /lbmis/auth/login HTTP/1.1
Content-Length: 80
Content-Type: application/x-www-form-urlencoded
Referer: http://mis.nha.gov.pk:81/
Host: mis.nha.gov.pk:81
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21
Accept: */*

password=00000000&username=admin&_token=tUkbHrCCQiZmEh31QrDyj2OFCJUr410KQ9SFNOfj
```

Appendix III



To play video, you may need to install the required video codecs.

Appendix IV



Enjoy it 5768. sahre to enjoy.
SWZsK ih/RU

14:42