राजा महेन्द्र प्रताप सिंह विश्वविद्यालय, अलीगढ़

Email:- registrar.rmpu@gmail.com

पत्रांकःआर0एम0पी0यू0/1860/2024 दिनांकः 07, सितम्बर, 2024

सेवा में,

प्राचार्य/प्राचार्या
समस्त सम्बद्ध महाविद्यालय
राजा महेन्द्र प्रताप सिंह राज्य विश्वविद्यालय
अलीगढ़।

विषयः Compromised सरकारी वेबसाइट को सुरक्षित करने के लिए CERT-In के सम्बन्ध में।

महोदय/महोदया,

उपरोक्त विषयक शासन के पत्र संख्या–2161/सत्तर–3–2024 दिनांक 03 सितम्बर, 2024 (प्रति संलग्न) का संदर्भ ग्रहण करें। उक्त के क्रम में प्राप्त निर्देशों का अनुपालन सुनिश्चित करें।

संलग्नकः यथोक्त।

भवदीय

07/9/24

(अजय कृष्ण यादव)
कुलसचिव

प्रतिलिपिः सूचनार्थ एवं आवश्यक कार्यवाही हेतु प्रेषित।

1. उप सचिव, उ0प्र0 शासन, उच्च शिक्षा अनुभाग–3, लखनऊ।
2. निजी सचिव, मा0 कुलपति, मा0 कुलपति जी के अवलोकनार्थ।
3. प्रभारी वेबसाइट को वेबसाइट एवं समस्त महाविद्यालयों की लागइन आई0 पर पर अपलोड करने हेतु प्रेषित
4. गार्ड फाइल।

07.09.24

उप कुलसचिव

संख्या–2161 /सत्तर–3–2024

प्रेषक,

एस0पी0 मिश्र,
उप सचिव,
उ0प्र0 शासन।

सेवा में,

1. निदेशक, उच्च शिक्षा उ0प्र0, प्रयागराज।
2. कुलसचिव, समस्त राज्य विश्वविद्यालय, उ0प्र0।
3. उप निदेशक, राष्ट्रीय उच्चतर शिक्षा अभियान, लखनऊ।
4. अपर सचिव, उत्तर प्रदेश राज्य उच्च शिक्षा परिषद, लखनऊ।
5. समस्त क्षेत्रीय उच्च शिक्षा अधिकारी, उ0प्र0।

उच्च शिक्षा अनुभाग–3

लखनऊ : दिनांक 03 सितम्बर, 2024

विषय : Compromised सरकारी वेबसाइट को सुरक्षित करने के लिए CERT-In द्वारा दिये गये दिशा–निर्देशों के सम्बन्ध में।

महोदय,

उपर्युक्त विषयक प्रमुख सचिव, आई0टी0 एवं इलेक्ट्रानिक्स विभाग, उ0प्र0 शासन के पत्र संख्या–1099/78–1–2024–1099/29/2021, दिनांक 12.08.2024 की छायाप्रति संलग्नक सहित प्रेषित करते हुये मुझे यह कहने का निदेश हुआ है कि कृपया प्रश्नगत प्रकरण में की गयी अपेक्षानुसार आवश्यक कार्यवाही करते हुए कृत कार्यवाही से शासन को समयान्तर्गत अवगत कराने का कष्ट करें।

संलग्नक–यथोक्त।

भवदीय,

(एस0पी0 मिश्र)
उप सचिव।

संख्या एवं दिनांक तदैव।

प्रतिलिपि निम्नलिखित को सूचनार्थ एवं आवश्यक कार्यवाही हेतु प्रेषित :–

1– निजी सचिव, प्रमुख सचिव, उच्च शिक्षा विभाग, उ0प्र0 शासन।
2– निजी सचिव, समस्त विशेष सचिव, उच्च शिक्षा विभाग, उ0प्र0 शासन।
3– समस्त संयुक्त सचिव/उप सचिव/अनु सचिव, उच्च शिक्षा विभाग, उ0प्र0 शासन।
4– समस्त अनुभाग अधिकारी, उच्च शिक्षा विभाग, उ0प्र0 शासन।

आज्ञा से,

(एस0पी0 मिश्र)
उप सचिव।

संख्या 9560 /VIP PSHED/2024

संख्या 2161 /सत्तर-3-2024

शीर्ष प्राथमिकता/महत्वपूर्ण

संख्या :-1099/78-1-2024-1099/29/2021

प्रेषक,

अनिल कुमार सागर,
प्रमुख सचिव,
उ०प्र० शासन ।

सेवा में,

समस्त अपर मुख्य सचिव/ प्रमुख सचिव/सचिव,
उ०प्र० शासन।

आई.टी. एवं इलेक्ट्रानिक्स अनुभाग-1 लखनऊः दिनांक 12 अगस्त, 2024

विषयः Compromised सरकारी वेवसाइट्स को सुरक्षित करने के लिए CERT-In द्वारा दिये गये दिशा- निर्देशों के सम्बन्ध में।

महोदय,

उपर्युक्त विषय के संबंध में महानिदेशक, Indian Computer Emergency Response Team (CERT-In), इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय, भारत सरकार के अर्द्ध शासकीय पत्र सं0-10(24)/2023-CERT-In दिनांक 27 मई, 2024 (छायाप्रति संलग्नक-1) का कृपया सन्दर्भ ग्रहण करने का कष्ट करें।

2- इस संबंध में अवगत कराना है कि CERT-In इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय, भारत सरकार के अधीन एक संस्था है, जोकि सूचना प्रौद्योगिकी अधिनियम 2000 (धारा 70बी) के अन्तर्गत साइबर सिक्योरिटी इन्सीडेन्ट हेतु राष्ट्रीय नोडल एजेंसी है।

3- CERT-In को कई Compromised सरकारी वेवसाइटों (*.gov.in) के संबंध मे रिपोर्ट प्राप्त हुयी है, जिनका उपयोग सर्च इंजन ऑप्टिमाइजेशन (एस०ई०ओ०) पोइजनिंग / स्पैमिंग तथा कुछ अन्य प्रकरण में थर्ड पार्टी की वेवसाइटों पर पुनर्निर्देशन (Redirection) के लिए किया जा रहा है। हैकर्स द्वारा वल्नरेबल सरकारी वेवसाइटों (*.gov.in) में मलेशियस कोड इंजेक्ट करके तथा साईटमैप में संशोधन करके उसका शोषण किया जा रहा है। यदि कोई उपयोगकर्ता Google-search परिणामों में सूचीबद्ध संवंधित वेव लिंक पर जाता है, तो यह उपयोगकर्ताओं को सट्टेवाजी / गेमिंग / ई-कॉमर्स पोर्टल जैसी अनपेक्षित थर्ड पार्टी वेवसाइटों पर पुनर्निर्देशित कर देती है।

गूगल सर्च के लिए कुछ डॉर्क निम्नवत् हैः-

a. betting site: gov.in
b. casino site: gov.in
c. rummy site: gov.in

3- CERT-In द्वारा वेवसाईटों को सुरक्षित करने के लिए निम्नलिखित सुरक्षा उपाय सुझायें गये है, जिसका विभागों द्वारा अनुपालन किया जाना प्रस्तावित हैः-

(प्रेम कुमार पाण्डेय)
संयुक्त सचिव
उच्च शिक्षा विभाग
उ०प्र० शासन।

a. Search Web pages (html, asp, jsp, js etc) for obfuscated malicious content, JavaScript/VBScript/IFRAME code injected by attackers. These links are embedded in the source code of the Web page associated with an IFRAME/script tag. Remove these malicious contents (Javascripts/vbscripts/IFRAMES) that are injected by the attackers in all the above listed webpages.

b. Search for a hidden folder .sys and delete the same, if found.

c. Review the sitemaps for any unauthorized changes

d. Site administrators are advised to check htaccess, php_includes, and other configuration settings, as well as ensuring that directory permissions are set appropriately.

e. Users may consider using Browser addons such as "NoScript" which pre- emptively block malicious scripts and allows JavaScript, Java and other potentially dangerous content only from the user trusted sites.

f. Scan the system with Anti-virus/Anti-spyware.

g. Change FTP credentials (if any) for the administrators to upload content into your website and secure the same.

4- इस सम्बन्ध में मुझे यह कहने का निदेश हुआ है कि कृपया उपरोक्तानुसार आवश्यक कार्यवाही सुनिश्चित करने हेतु अपने विभाग में कार्यरत अधिकारियों/संस्थाओं को निर्देशित करने का कष्ट करें।

संलग्नकःयथोक्त।

भवदीय,

Signed by
Anil Kumar Sagar (अनिल कुमार सागर)
Date: 10-08-2024 12:45:37 प्रमुख सचिव।

पृ0संख्या-1099(1)/78-1-2024 तद्दिनांक

प्रतिलिपि निम्नलिखित को सूचनार्थ एवं आवश्यक कार्यवाही हेतु प्रेषितः-

1- निजी सचिव, मुख्य सचिव, उ०प्र० शासन।
2- निजी सचिव, अपर मुख्य सचिव, गृह एवं गोपन विभाग, उ०प्र० शासन।
3- निजी सचिव, पुलिस महानिदेशक, उ०प्र० ।
4- राज्य समन्वयक, सेन्टर फॉर ई-गवर्नेन्स, अपट्रान बिल्डिंग, गोमती नगर, लखनऊ।
5- प्रबन्ध निदेशक, यूपीडेस्को, लखनऊ।
6- राज्य सूचना विज्ञान अधिकारी, एन०आई०सी०, लखनऊ।
7- स्टेट, चीफ इन्फॉरमेशन सिक्योरिटी ऑफिसर (सी०आई०एस०ओ०), उ०प्र०।

8- समस्त विभागीय, चीफ इन्फॉरमेशन सिक्योरिटी ऑफिसर (सी०आई०एस०ओ०), उ०प्र० द्वारा सीईजी।
9- हेड, एस.ई.एम.टी., लखनऊ।
10- गार्ड फाइल ।

आज्ञा से,

(नेहा जैन)
विशेष सचिव।

Dr. Sanjay Bahl
Director General

भारत सरकार
Government of India
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय
Ministry of Electronics & Information Technology
भारतीय कम्प्यूटर आपात प्रतिक्रिया दल (सर्ट-इन)
Indian Computer Emergency Response Team (CERT-In)
इलेक्ट्रॉनिक्स निकेतन 6, सी जी ओ कॉम्प्लेक्स, नई दिल्ली-110003
Electronics Niketan 6, C G O Complex, New Delhi-110003
Tel: 24368544, Fax: 24366806, E-mail : sanjay.bahl@gov.in

27 May 2024

10(24)/2023-CERT-In

Sub: Compromised Government Websites (*.gov.in)
Ref: CERTIn-20169224

The Indian Computer Emergency Response Team (CERT-In), is an organization under the Ministry of Electronics & Information Technology, Government of India. CERT-In is the national nodal agency for responding to cyber security incidents as per the Information Technology Act 2000 (Section 70B).

2. CERT-In has received several reports regarding compromise of multiple government (*.gov.in) websites, which are being used for Search Engine Optimization (SEO) poisoning/spamming and further redirection to third party websites in some cases. Threat actors are exploiting vulnerable gov.In websites for injecting malicious files (html, jsp, js, asp etc.), modification of sitemaps. When a user visits the associated web links listed in Google search results, it may redirect the users to unintended third-party websites such as betting/gaming/e-commerce portals.

Some of the dorks (specific search queries) for Google search:

a. betting site:gov.in
b. casino site:gov.in
c. rummy site:gov.in

There can be several other keywords, threat actor might be using for SEO poisoning purpose. Snapshots of such sample cases are placed in the annexure. Compromised state government web sites can be listed by replacing "gov.in" with "<State/UT_government_sub_domain>.gov.in" in the Google dork.(Example: betting site:goa.gov.in)

3. CERT-In is regularly notifying the concerned authorities as and when such compromises are noticed/reported.

4. The following security measures are recommended for securing those compromised websites:

a. Search Web pages (html, asp, jsp, js etc) for obfuscated malicious content, JavaScript/VBScript/IFRAME code injected by attackers. These links are embedded in the source code of the Web page associated with an IFRAME/script tag. Remove these malicious contents (Javascripts /vbscripts/IFRAMES) that are injected by the attackers in all the above listed webpages.
b. Search for a hidden folder .sys and delete the same, if found.
c. Review the sitemaps for any unauthorised changes
d. Site administrators are advised to check htaccess, php_includes, and other configuration settings, as well as ensuring that directory permissions are set appropriately.
e. Users may consider using Browser addons such as "NoScript" which pre-emptively block malicious scripts and allows JavaScript, Java and other potentially dangerous content only from the user trusted sites.
f. Scan the system with Anti-virus/Anti-spyware.
g. Change FTP credentials (if any) for the administrators to upload content into your website and secure the same.

आज़ादी का अमृत महोत्सव

G20 भारत 2023 INDIA

Digital India Power To Empower

h. Review the security of Web Server and website for application and Operating System vulnerabilities and apply appropriate patches/updates.
i. Implement information security best practices such as "Use Signed Scripting".
j. It is recommended to avoid internet browsing and remove all file shares on the Web Server.
k. Refer to the given below link for Google webmaster's help for the hacked site:
   URL: https://www.google.com/webmasters/hacked
l. Ensure security audits (VAPT) for the "*gov.in" websites on regular basis for identification and remediation of the vulnerabilities

5. In this regard, you are requested to take necessary action for identifying and securing all such vulnerable/compromised *.gov.in websites under your control. The action taken in this matter shall be intimated at the earliest.

(Dr. Sanjay Bahl)

Encl: As above

To,
Shri. Anil Kumar Sagar, IAS
Principal Secretary- IT & Electronics
Government of Uttar Pradesh
107, 1st Floor, Block-C,
Lokbhawan, Lucknow 226001
Email: ps.ite@up.gov.in