



DR CBS CYBER SECURITY SERVICES LLP

LLP Id No. AAK-4058

CERT-In Empanelled Information Security Auditing Organization (2020-2023)

Registered with MSME No.: UDYAM-RJ-17-0052608 &

Government e-Marketplace GeM Seller Id : IZ80210002192567

Certificate of Recognition as #Startupindia No.: DIPP77174

Registered with iSTART Startup Rajasthan No. : 5F7054D

Member Data Security Council of India (DSCI): DSCI/AM/2018/03

Friday, 25th February 2022

Vulnerability Closure cum Final Report

To,

Shri Ashish Singhal

Sr. Business Analyst

B.R. Softech Pvt Ltd

Jaipur


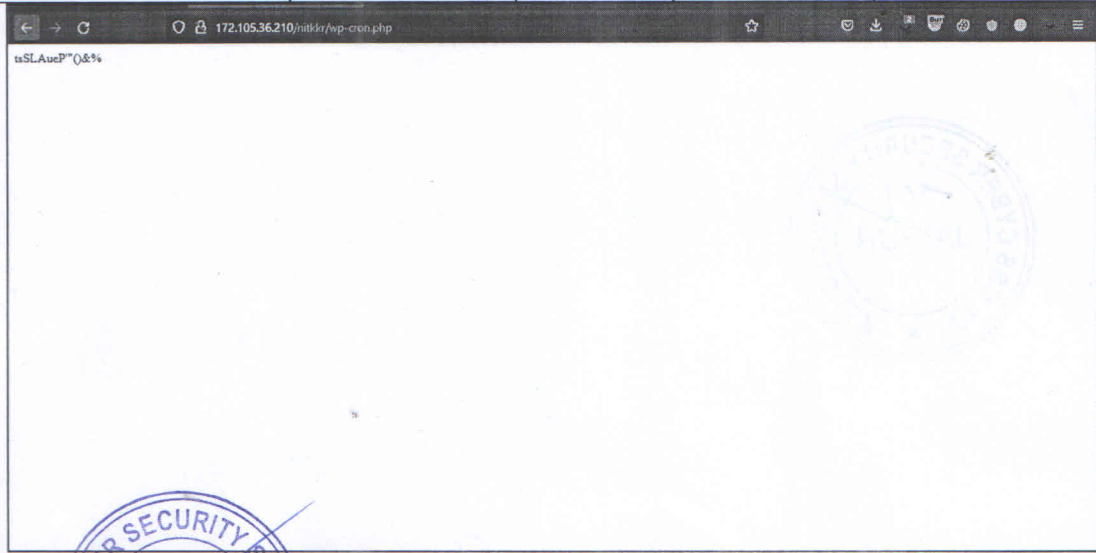
Sub: Final Detailed IT Security Audit / VAPT Report of website of National Institute of Technology Kurukshetra (NITKKR).

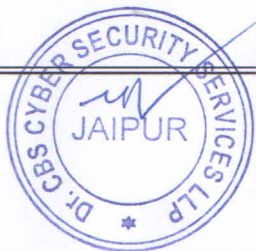
Ref: Work Order dated 09/02/2022 & Compliance Report Dated 25th February 2022

Dear Sir,

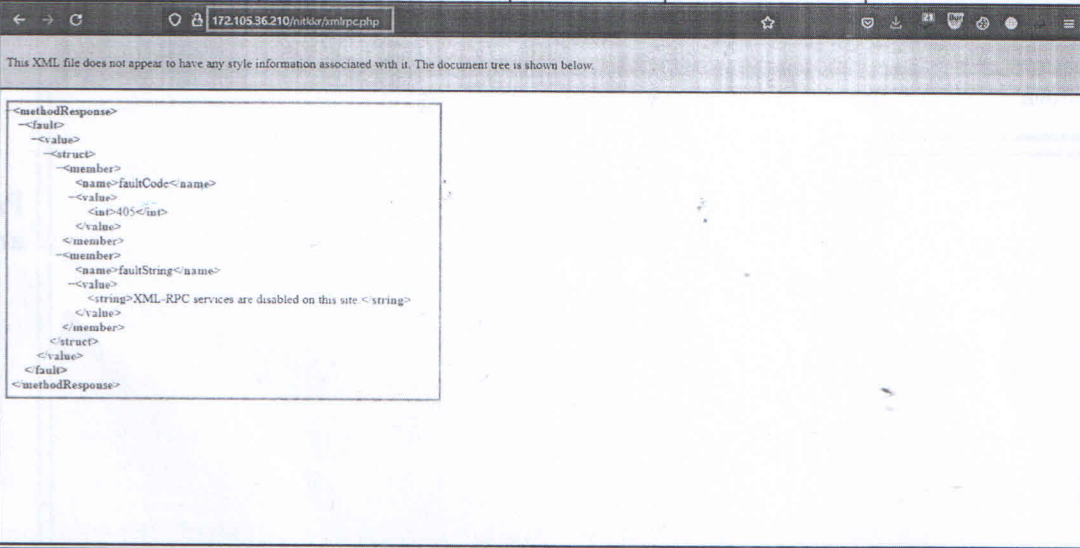
In continuation to the earlier audit report forwarded on 09th February 2022, After receiving the compliance report on 25th February 2022 of Web Application of NIT kurukshetra , the final audit report prepared by Audit team of our organization headed by Mr. Satyendra Singh is authenticated and attached for your perusal & needful action at your end.



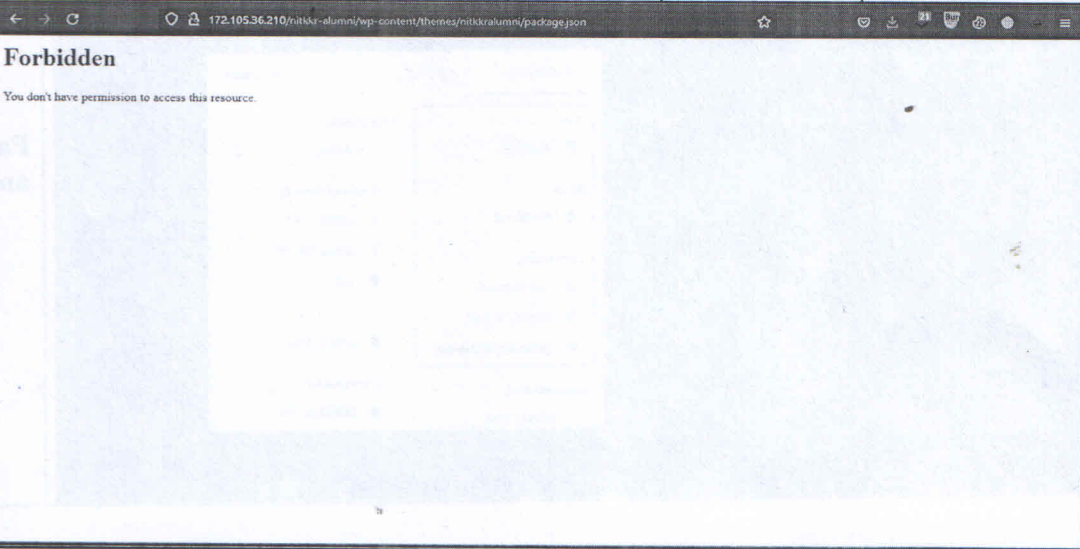
Final Security Audit / VAPT Report						
S No	Vulnerable Point / Location	Vulnerability	Manually / Tool Based	Comments / Review of flaw / Reference	Auditee Remark	Auditor Remark
1	2	3	4	5	6	7
1. DOM Based XSS (Cross-site scripting)						
1.1	http://172.105.36.210/nitkkr/	DOM Based XSS (Cross-site scripting)	Manual	CWE-79 CAPEC-588	The issue is resolved	Patched and Closed
						
2. Reflected XSS (Cross-site scripting)						
2.1	http://172.105.36.210/nitkkr/wp-cron.php	Reflected XSS (Cross-site scripting)	Manual	CWE-79	The issue is resolved	Patched and Closed
						



3. WordPress XML-RPC authentication brute force

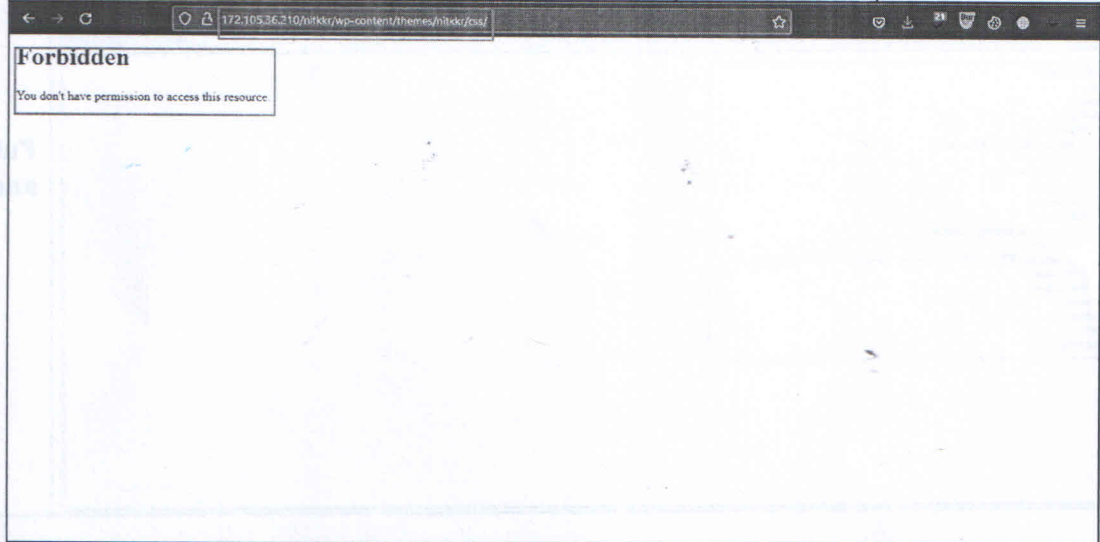
3.1	http://172.105.36.210/nitkkr/xmlrpc.php	WordPress XML-RPC authentication brute force	Manual	CWE-521	The issue is resolved	Patched and Closed
						

4. Exposure of Development configuration files

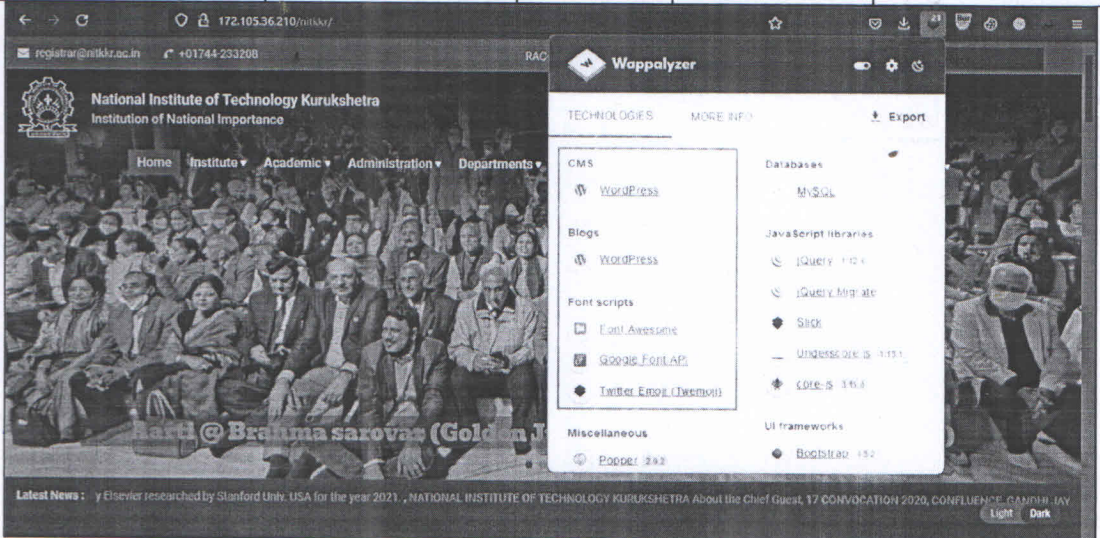
4.1	http://172.105.36.210/nitkkr/wp-content/themes/nitkkr/package.json	Exposure of Development configuration files	Manual	CWE-538	The issue is resolved	Patched and Closed
						



5. Directory Browsing

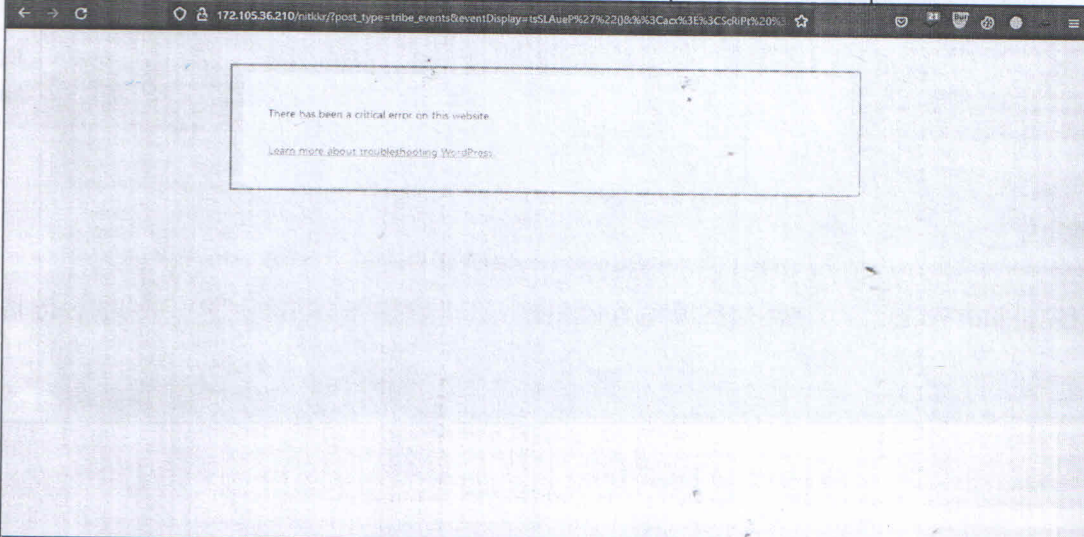
http://172.105.36.210/nitkkr/wp-content/themes/nitkkr/css/	Directory Browsing	Manual	CWE-548 CWE-552	The issue is resolved
5.1				Patched and Closed

6. Information Disclosure


http://172.105.36.210/nitkkr/	Information Disclosure	Manual	CWE-200 CWE-359	The issue is resolved
6.1				Patched and Closed



7. HTTP parameter pollution


	http://172.105.36.210/nitkkr/?post_type=tribe_events&eventDisplay=month&n908707=v937972	HTTP parameter pollution	Manual	CWE-88	The issue is resolved	
7.1						Patched and Closed

8. Vulnerable JS Library

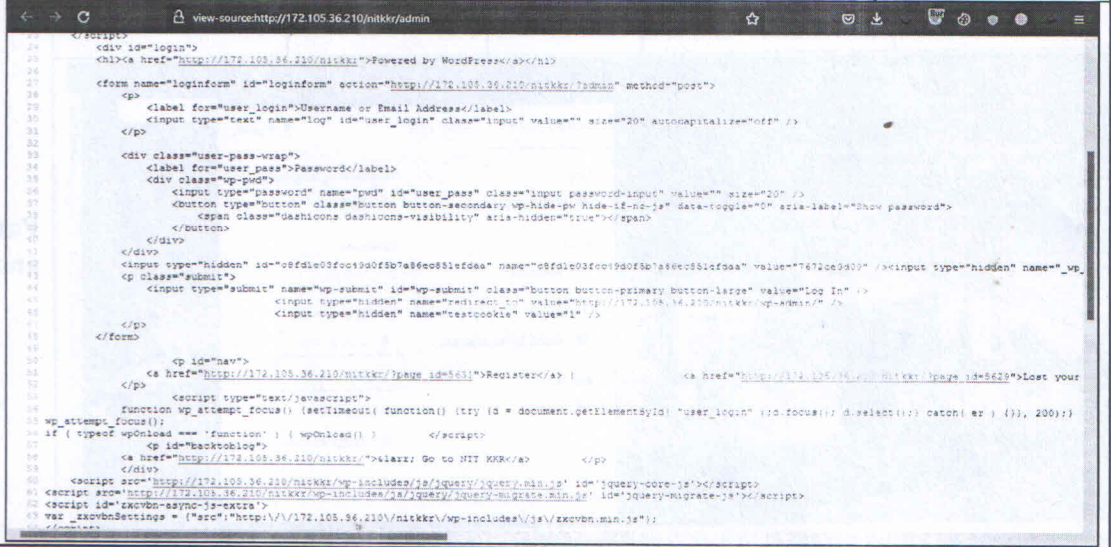
	http://172.105.36.210/nitkkr/	Vulnerable JS Library	Manual	CWE-829	The issue is resolved	
8.1						Patched and Closed



9. X-Frame Header not set

http://172.105.36.210/nitkkr/	X-Frame Header not set	Manual	CWE-1021	The issue is resolved	
9.1					Patched and Closed

10. Absence of Anti-CSRF Tokens

http://172.105.36.210/nitkkr/	Absence of Anti-CSRF Tokens	Manual	CWE-352 CWE-330	The issue is resolved	
10.1					Patched and Closed



13. Cookie without SameSite Attribute

http://172.105.36.210/nitkkr/	Cookie without SameSite Attribute	Manual	CWE-1275	The issue is resolved	Patched and Closed

13.1

14. Cookie Without Secure Flag

http://172.105.36.210/nitkkr/	Cookie Without Secure Flag	Manual	CWE-614	The issue is resolved	Patched and Closed

14.1



15. X-Content-Type-Options Header Missing

http://172.105.36.210/nitkkr/	X-Content-Type-Options Header Missing	Manual	CWE-200	The issue is resolved	
---	--	---------------	----------------	------------------------------	--

15.1

Patched and Closed

16. HTTP Strict Transport Security (HSTS) no implemented

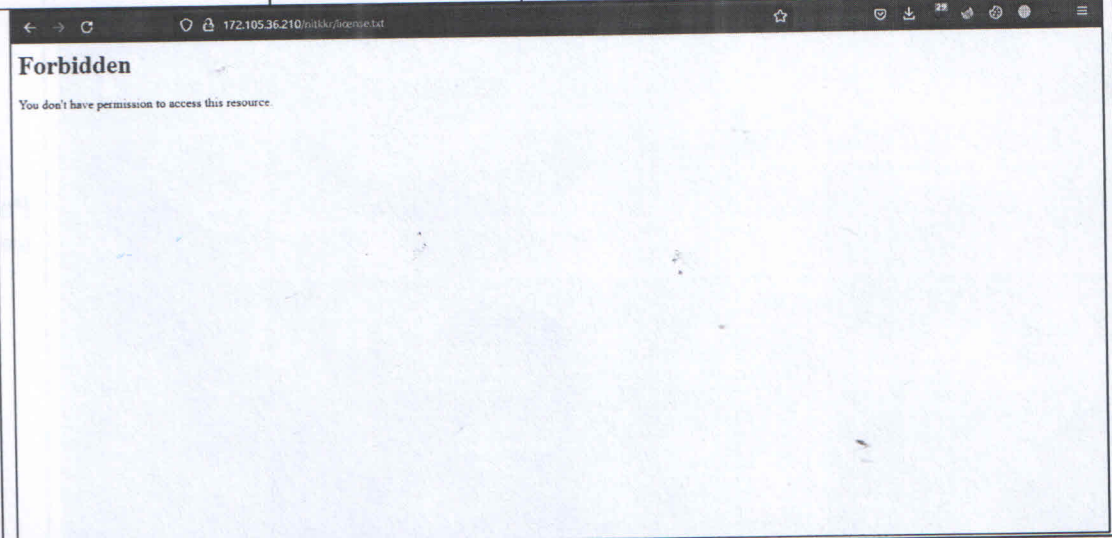
http://172.105.36.210/nitkkr/	HTTP Strict Transport Security (HSTS) no implemented	Manual	CWE-523	The issue is resolved	
---	---	---------------	----------------	------------------------------	--

16.1

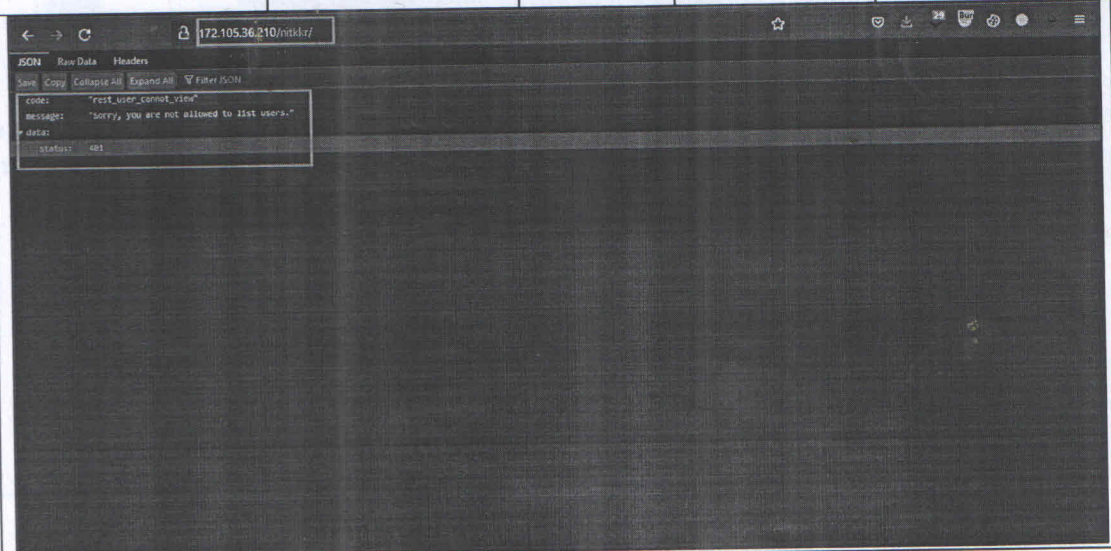
Patched and Closed

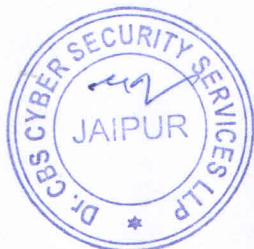


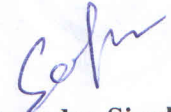
17. Disclosure of Documentation files

http://172.105.36.210/nitkkr/license.txt	Disclosure of Documentation files	Manual	CWE-538	The issue is resolved	Patched and Closed
17.1					

18. WordPress REST API User Enumeration

http://172.105.36.210/nitkkr/	WordPress REST API User Enumeration	Manual	CWE-200	The issue is resolved	Patched and Closed
18.1					




Satyendra Singh
Cyber Security Analyst

Forwarded in original

Safe to host certificate is forwarded separately.
Thanks & Regards





Dr. C. B. Sharma IPS R.
Founder & CEO

Dr. CB SHARMA IPS (R)
Certified Lead Auditor ISMS (ISO/IEC 27001: 2013),
Founder & CEO