



NCIIPC Responsible Vulnerability Disclosure

1. Reporter's Details			
a) Full Name			
b) Email			
c) Organisation/Company			
2. Vulnerability Details (✓ Check mark)			
a) Vulnerability Name			
b) Vulnerability category	<input type="checkbox"/> XSS	<input type="checkbox"/> SQLI	<input type="checkbox"/> Stack Overflow
	<input type="checkbox"/> LFI	<input type="checkbox"/> Click Jacking	<input type="checkbox"/> User After Free
	<input type="checkbox"/> XSRF	<input type="checkbox"/> Information Leakage	<input type="checkbox"/> Heap Overflow
	<input type="checkbox"/> Insecure Direct Object Reference		<input type="checkbox"/> Broken Authentication
	<input type="checkbox"/> Memory Corruption		<input type="checkbox"/> Security Misconfiguration
c) Description	(Use Separate Sheet for additional information)		
3. Type of Vulnerability (✓ Check mark)	<input type="checkbox"/> Web Application	<input type="checkbox"/> Operating System(OS)	
	<input type="checkbox"/> SCADA	<input type="checkbox"/> Any Other	
If other please describe in brief			
4. Date when issue found	(dd/mm/yyyy)		
5. Steps to reproduce			
6. Whether POC screenshots/files/documents attached?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
7. Reported to Affected Organisation?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
8. Affected Organisation's name			
9. Affected Organisation's URL			
10. Affected Organisation's email			
11. Vulnerable Product type	<input type="checkbox"/> Web Application		<input type="checkbox"/> Client Software
	<input type="checkbox"/> Server Software		<input type="checkbox"/> Firmware
	<input type="checkbox"/> Operating System		<input type="checkbox"/> Hardware
12. Vulnerable Product name & Version			
13. If reported, Email ID to whom details sent			
14. If reported, date when reported			
15. Patch released?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
16. If patch released, date of patch release	(dd/mm/yyyy)		
17. Anonymity	(Yes/No)		