RISK ID	TECHNICAL RISK	TECHNICAL RISK INDICATOR	IMPACT RATING	IMPACT	MITIGATION	VALIDATION STEPS
1	Pass arbitary code to eval function().	arbitrary PHP code could be executed on the server.	H	Code Injection, attacker can take take control of the sever and can do what ever they want such as editing,	Validate all the user suplied input. Include form fields, query strings, client side cookies, etc.	Submit a query as input then examine the inputand execute on the webserver.
2	System not validating users input, Invalid data can be loaded on the system.	Harmful data being uploaded.	M	Cross site scripting, Attackers can execute scripts in victim's browser to hijack user session, insert hostile content, redirect user's,	Sanitize the user input. Manipulate the input data to make sure it is safe by removing any unwanted bits from the data and normalizing it to the	Try to upload hamful data eg:<script>alert</script> and check whether in databse the stored input is sanitized or not.
3	System takes SQL statement as input	Query uploaded as user input.	H	Sql injection, can take complete control of data base, denial of service attacks	Use parameterized queries. This means defining the Sql code that is to be executed with place holders for parameter values, programically adding the parameter value, then executing the query.	Load sql code as user input, Ex: 'or 1=1-- for username or password and validate whether the system accepts SQL statement
4	Information leakage through error	System showed error message including database	L	This will reveal sensitive information which may be used for later attack.	Provide only the required information to the user about an error.	Create a error message by giving invalid input and verify it only required error
5	Hardcoded password used to connect to	Used the login and database information to dump the sql.	H	Attacker can crack the password and take control of database.	Put the login information in a separate configuration file outside	Try to use the previous hardcoded password and check whether DB is still

6	Sever login and password can be determind by cracking the	Logged in to sever with cracked password and use files inside the server.	H	Brite Force Attack, attackers can login to the server and take advantage of the files	Randomize (adding salt) to each hash to make it hard to crack.	Perform the cracking again and verify if the attack still exists.