Victor Ansart
Comp 116

Assignment 4

Type	Risk ID	Technical Risk Indicators	Impact Rating	Impact	Mitigation	Validation Steps
Code Injection	1	The user can execute arbitrary php code on the machine	Evidence of programs or code on computer that was not run by admin	High	Prevent untrusted user input from being run as code and validate all user input to ensure it conforms to desired format	The user cannot run arbitrary code
SQL Injection	2	The user can dynamically create SQL queries in order to access, modify, or delete data.	Deleted or modified database data, strange queries in access logs,	High	Validate user input to ensure that it conforms to the desired format. Use parametrized prepared statements for SQL queries rather than dynamic queries.	The user can no longer access the database or modify it
Credentials Management	3	Passwords are hard-coded into the application allowing access if an attacker knows the password	Evidence of access to the system (in access logs) using the default password	Medium	Store the username and password database separetely from the webserver code	The user can no longer gain access with the hardcoded passwords
Cross Site Scripting	4	User can send malicious scripts to another end user. These scripts can be used to create popups, modify content, exploit cookies, or compromise sensitive information	Popups when visiting website, modified content, evidence of un-authorized access using cookies, evidence of redirection when visiting website	Medium	Validate user input to ensure that it conforms to the desired format and does not contain undesired scripts. Also filter the output caused by user input to ensure XSS scripts cannot run.	The user can no longer execute arbitrary scripts that classify as XSS

Information Leakage	5	User can receive information about the application through unfiltered error messages which can give an attacker useful data about the system	Admin can try to see error messages that will give him potentially useful information about the system	Low	Filter error messages so that only a generic message is sent to the user which does not reveal system information	When the user causes a system error, a generic error message is displayed
Steganography	6	Data is hidden within an image on the main page of the website	Anyone who is curious can analyze the image and find the hidden data	Low	Encrypt the data that is hidden in the image so that it cannot be read even if it is found	Data hidden within the image is encrypted and can only be accessed with correct key
Cookie Tampering	7	User can gain access to system by modifying the login cookie	Evidence of aunauthorized access to the system through cookies or admin can try accessing system using cookies	High	Do not use cookies for authentication purposes, or cookies are used, they should be encrypted so that they cannot be modified	User cannot access the system by modifying cookies
Buffer Overflow	8	User can overflow a buffer in a program which can cause the program to crash or even allow arbitrary code to run	Evidence of runme program crashing in logs or unexpected running code on the machine	Medium	Use safe string operations such as strncpy, snprintf, etc to ensure that buffers are of sufficient size	User cannot cause the buffer to overflow in the runme app
Weak passwords	9	User can access the system through brute force easily because weak user passwords are used	Evidence of incorrect logins in access logs	High	Lockout access to account after 5 login attempts and utilize secure passwords	User account disabled after five login attempts