ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

NCAIT-2017

JSS Academy of Technical Education, Bengaluru

Vol. 6, Special Issue 5, May 2017

ISRO Awards Secure Web Application

Neelavarsha DK[1], Nikhil R[2], Nishchita A[3]

Students, Dept. of ISE, SJB Institute of Technology, Bangalore[1,2,3]

Abstract: The necessity of cyber security is more today than ever. A proliferation of cyber-attacks is causing increasing attacks to companies, institutions and the government. The numbers of threats are increasing evidently and organizations need to counter these attacks by using appropriate security measures. Cybercrime has steadily risen to become a major threat. According to the Global Economic Survey conducted in 2016, only 37 percent of organizations have a dedicated cyber incident response plan and these need to be driven to a greater extent. Security is important for two main reasons. Firstly, due to the increase in cyber-attacks in recent years and secondly, due to the severity of these attacks which are able to compromise the security and integrity of applications. The necessity of countering cyber threats is more important in private organizations and government organizations due to high precision and confidentiality of data. As the organizations become increasingly interdependent, analysts must pay more attention to the security of their organizations. The best way to counter attacks is the use of certain security plans and procedures.

Keywords: Cyber security, Severity of attacks, precision, confidentiality.

1. INTRODUCTION

Indian Space Research Organization (ISRO) is an organization that requires utmost confidentiality, privacy and integrity of data. An organization this huge requires numerous applications to work interdependently on a network. One such web application is the Award Portal for ISRO. Every year, the esteemed scientists and research persons involved in important projects and breakthroughs are recognized and rewarded for their contribution towards various missions, projects, applications and research innovations. A portal is designed and developed to cater the requirements of ISRO awards activity starting from registration to award distribution, which involves gathering information which is sensitive in nature requires confidentiality to be maintained.

Various types of information are required by the different users like nominee, nominator and screening committee like, personal details, details about the project completed, directors approval for a certain award etc. Once the information is submitted by the different users, the screening committee screens information of all the users available to the committee. Therefore, the details of all users have to be maintained confidentially. On being selected for an award, the user is given a cash prize for his or her achievements which is directly credited to their bank account. Such data is confidential in natureand should not be exploited. If an attacker gains access to the awardee's nomination details, then the security of the awardees' information is at risk and such risks are very severe. In this paper we are proposing methodologies to counter such attacks, security measures and procedures on par with the OWASP Top-10 most critical web application security risks [1]. The following sections provide ways to counter the attacks. Section 2 provides plans and procedures by which security can be enforced. Section 3 shows the results of enforcing these security measures. Section 4 elaborates on conclusion and future enhancements.

2. SECURITY PLANS AND PROCEDURES

2.1. Encryption of User Credentials to prevent Broken Authentication

Every user that wants to be nominated or wants to nominate a candidate for the award needs to register with certain details like name, email Id, username and password. Once the user is registered, he or she may login using the registered credentials. On entering the username and password, the user can login and perform specific operations. To validate the user, the servlet is called which checks the credentials with those that are entered during registration. If a middle man attack is performed successfully at this stage, then the user becomes prone to exploitation of login details. To avoid such an occurrence, encryption of the user login details can be performed before being sent to the servlet. There are a number of encryption mechanisms that can be used. These include MD5 hashing, SHA etc. By using such an encryption mechanism, a successful middle man attack cannot perceive the information sent across in the network since the data is encrypted and the user cannot make any sense out of the perceived data. By such an encryption we can also avoid the attacker from deciphering debit card numbers and other bank details provided by the awardees.

2.2. Validation at Client and Server side to prevent SQL Injections

The award portal has a number of forms for entering data. Each of these forms specifies fields that need to be entered with certain data only. Any user including external users, internal users and administrators can be the source for entering data and this may lead to injection flaws. An injection flaw occurs when insecure data is sent to the interpreter. The interpreter cannot differentiate between the types of data andsimply interprets it to produce the results. Injection flaws are easy to detect when examining the code but is difficult toidentify during testing.Any user may enter invalid data to cause an injection flaw knowingly or unknowingly. A small snippet of JavaScript may be entered by an untrusted user that may send all user profile and data into a separate location. Therefore, validations need to be done both at the client side and server side. Consider a scenario where the client side validation performs only checks of length of the required field, then a loophole is created for the data to bypass by the server side. Therefore validations at the client and server side are mandatory for complete prevention of any injection flaw. The preferred option for preventing injections is the use of white list input validation routines. White list input validation is a set of correct inputs for the field. This can be enforced by use of patterns. So if a particular field can have data of a particular order only, then this can be specified by using patterns.

2.3 Session Management using HttpSession Interface to prevent Broken Session

Since ISRO maintains a lot of confidential data, session management needs to be effectively enforced to prevent any unauthenticated users from gaining access to the web application. Consider a scenario where a registered user logs into the application and leaves it pen for a long period of time. If a different user opens the page after some time, then the user is given the page that was opened by the first user after successful login. Such misuse can be avoided by enforcing a proper session management package using the java HttpSession Interface. The HttpSession object is used to store an entire session with a specific client. Any servlet ccan have access to HttpSession object through the getSession() method.Sometimes web applications are exposed to flaws by printing the session ID in the URL itself. If an external user gains this session ID, then the attacker can modify and exploit the data available. To prevent this, session IDs are added to the timestamp and this is then encrypted. When an attacker tries to acquire the session ID, the encrypted session ID is retrieved and any attempts to gain access is stopped [2].

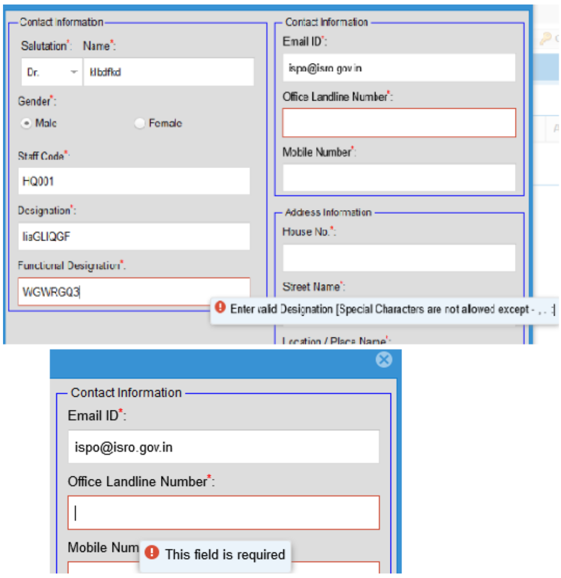
2.4 HTTPS channel

The complete web application is hosted on a HTTPS channel instead of a HTTP channel. HTTPS stands for Hyper Text Transfer Protocol Secure which is the secure version of HTTP. It means all communications between the browser and the website are encrypted. HTTPS is used to protect bank details stored in the awardees details and also to protect the communication between the browser and the website. Web browsersalso display a padlock icon in the address bar to visually indicate that a HTTPS connection is in effect.All communications sent over HTTP are in plain text and can be read by any hacker that manages to break into the connection between the browser and the website. By using a HTTPS connection, all communications are encrypted and attacks can be prevented [3].

3. RESULTS AND DISCUSSION

3.1 Future Use for Web Application

The above mentioned methodologiesprovide security to the web application in a number of ways. The Figure.1(a&b) show the validation of data on different forms. Every field of data received by a registered user is first validated on the client side and if this is bypassed then the server side validation is done to provide added protection of the web application.



Contact Information
Salutation*: Dr.
Name*: klbdfkd
Gender*: ● Male ○ Female
Staff Code*: HQ001
Designation*: liaGLIQGF
Functional Designation*: WGWRGQ3
Enter valid Designation [Special Characters are not allowed except - , . :]

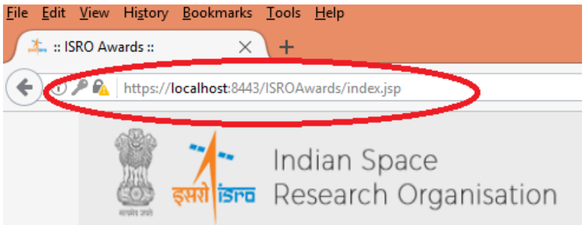
Contact Information
Email ID*: ispo@isro.gov.in
Office Landline Number*:
Mobile Number*:

Address Information
House No.*:
Street Name*:
Location / Place Name*:

Contact Information
Email ID*: ispo@isro.gov.in
Office Landline Number*:
Mobile Num
This field is required

Figure.1. (a & b) Validation of data at client side

The use of HTTPS channel provides a secure communication channel for communication between the browser and the website. This is achieved through encryption of all requests and responses between the communicating entities. The Figure 2.shows the use of https channel indicated by the padlock icon. An audit report can be obtained of the testing performed to study the vulnerabilities and perform corrections on it.



https://localhost:8443/ISROAwards/index.jsp

Figure.2. Establishment of HTTPS channel.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

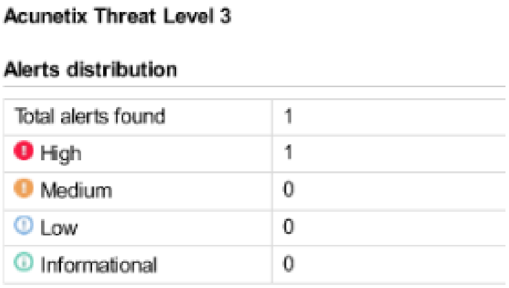
International Journal of Advanced Research in Computer and Communication Engineering

NCAIT-2017

JSS Academy of Technical Education, Bengaluru

Vol. 6, Special Issue 5, May 2017

Figure 3(a&b) shows the report before and after the resolution of vulnerability.

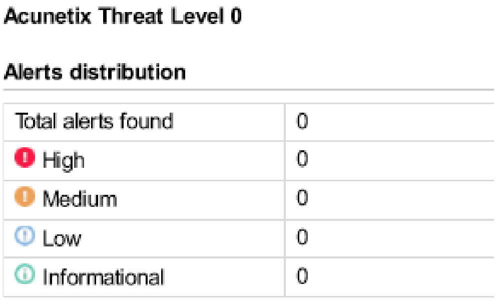


Acunetix Threat Level 3

Alerts distribution

Total alerts found	1
High	1
Medium	0
Low	0
Informational	0

Figure.3a. Reports of testing before vulnerability resolution.



Acunetix Threat Level 0

Alerts distribution

Total alerts found	0
High	0
Medium	0
Low	0
Informational	0

Figure.3b.Reportof testing after vulnerability resolution

CONCLUSIONS

Security in organizations has become a very important aspect in web applications today due to the increased number of attacks and severity of these attacks. In all cases, the highest vulnerabilities were identified with SQL Injections. The foremost reason being the presence of direct referencing and the absence of PreparedStatements during database extraction. Secondly, the enforcement of session management is evident in any secure web application due to the risk involved in its absence. Any random user may gain the access if it is not timed out properly. The sessions also have to be encrypted to prevent stealing of session IDs from URLs. Thirdly, the user credentials have to be encrypted and then sent over to the website, such that there is no loophole for any broken authentication.Testing has to be done mandatorily and a report can be obtained to study the level of threats.

ACKNOWLEDGMENTS

Heartfelt thanks to ISRO for providing the opportunity to work with esteemed analysts and scientists in the department of Information Systems Program Organization (ISPO) and the Director of ISPO department Dr. Rajiv RatanChetwani for giving us continuous support and encouragement in completion of the project. We would also like to thank Mr.Hariprasad CN for his guidance.A special thanks to the teaching staff at SJB Institute of Technology and our internal guide Prof. Kameswari K.

REFERENCES

1. http://investigatingnews.com/daily
2. Y. TAKAMATSU,Y. KOSUGA ANDK. KONO.Automated Detection of Session ManagementVulnerabilities in Web Applications. In Proc. Of Int'l Conf. on Privacy, Security and Trust (2012).
3. KONSTANTIN G. KOGOS, ELENA I. SELIVERSTOVA AND ANNA V. EPISHKINA.Review of Covert Channels over HTTP: Communication and Countermeasures. In Proc. Of IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (2017).