# ANNA UNIVERSITY: CHENNAI 600025

## BONAFIDE CERTIFICATE

Certified that this project report "**BCX MODEL FOR CROSS-SITE REQUEST FORGERY**" is the bonafide work of **"R.HARINI (312415104033) and C. M. KANIMOZHI (312415104042)",** who carried out the project work under my supervision.

**SIGNATURE**

**Dr. J. DAFNI ROSE M.E, Ph.D.,**
**Professor,**
**Head of the Department,**
**Computer Science and Engineering,**
St. Joseph's Institute of Technology,
Old Mamallapuram road,
Chennai - 600 119.

**SIGNATURE**

**Mr. K. S. ARIKUMAR M.E, (Ph.D.),**
**Assistant Professor,**
**Computer Science and Engineering,**
St. Joseph's Institute of Technology,
Old Mamallapuram road,
Chennai - 600 119.

## ACKNOWLEDGEMENT

We take this opportunity to thank our honourable Chairman **Dr. B. Babu Manoharan, M.A., M.B.A., Ph.D.** for the guidance he offered during our tenure in this institution.

We extend our heart felt gratitude to our honourable Managing Director **Mrs. B. Jessie Priya, M.Com.** and Director **Mr. B. Sashisekar, M.Sc. (INTL Business)** for providing us with the required resources to carry out this project.

We are indebted to our Principal **Dr. P. Ravichandran, M.Tech., Ph.D.** for granting us permission to undertake this project.

We would like to express our earnest gratitude to our Head of the Department **Dr. J. Dafni Rose, M.E., Ph.D.** for her commendable support and encouragement for the completion of the project with perfection.

We also take this opportunity to express our profound gratitude to our guide **Mr. K. S. Arikumar, M.E., (Ph.D.),** Assistant professor for his guidance, constant encouragement, immense help and valuable advice for the completion of this project.

We wish to convey our sincere thanks to all the teaching and non-teaching staff of the department of **Computer Science and Engineering, St. Joseph's Institute of Technology** without whose co-operation this venture would not have been a success.

## CERTIFICATE OF EVALUATION

College Name : St. JOSEPH'S INSTITUTE OF TECHNOLOGY

Branch : COMPUTER SCIENCE AND ENGINEERING

Semester : VIII

| Sl.No | Name of the Students | Title of the project | Name of the Supervisor with designation |
|---|---|---|---|
| 1<br><br>2 | R. Harini (312415104033)<br>C. M. Kanimozhi (312415104042) | BCX Model for Cross-Site Request Forgery. | Mr. K. S. Arikumar M.E, (Ph.D.)<br>Assistant Professor,<br>CSE Department,<br>St. Joseph's Institute of Technology. |

The report of the project work submitted by the above students in partial fulfilment for the award of Bachelor of Engineering Degree in **Computer Science and Engineering** of Anna University were evaluated and confirmed to be report of the work done by above students.

Submitted for project review and viva voce exam held on _____

**(INTERNAL EXAMINER)** **(EXTERNAL EXAMINER)**

## ABSTRACT

Cross-Site Request Forgery is a widely exploited Website vulnerability. The CSRF is a major security threat to the Online Transaction, in which the user is forced to enter into some malicious websites and reveal their login credentials, or the attacker enter into the user's authenticated session, without the user's knowledge. The existing approaches to prevent CSRF such as OTP, Tokens and removal of the Same-site cookies from the web application doesn't yield the expected security to the applications. Hence, this proposal uses the Mathematical Binary Conversion, Combination and X-OR (BCX) Model to remove CSRF attacks. In order to confirm that the user who makes the login and the Money transaction is one and the same and to prove that there is no Attacker intervention into the logged on session, the MAC address off the system is taken and subjected to the BCX Algorithm and the hash value of the MAC is saved on login and verified on making a transaction. Moreover, the Anti-Forgery Token(AFT) is produced from the combination of the IP Address and the password of the user and it is also subjected to the BCX Algorithm. The AFT is generated and saved during Login and verified on making a transaction. Thus, by using the BCX model, the security threats to the end user of the various applications is reduced and the Cross Site Request Forgery attacks on the web pages during the transaction is avoided.

## TABLE OF CONTENTS

## LIST OF FIGURES

# LIST OF TABLES

## LIST OF ABBREVATIONS

| | |
|---|---|
| CSRF | Cross-Site Request Forgery |
| BCX | Binary conversion-Combination-eXclusive OR |
| HTTP | Hyper Text Transfer Protocol |
| HTTPS | Hyper Text Transfer Protocol Secure |
| MAC | Medium Access Control |
| IP | Internet Protocol |
| AFT | Anti-Forgery Token |
| ASCII | American Standard Code for Information Interchange |
| SHA | Secured Hash Algorithm |
| URL | Uniform Resource Locator |
| XSS | Cross-Site Scripting |
| DOM | Document Object Model |
| MD | Message Digest |
| AES | Advanced Encryption Standard |
| DES | Data Encrytion Standard |
| RSA | Rivest Shamir Adleman |
| CPU | Central Processing Unit |
| PHP | Hypertext Preprocessor |
| HMAC | Hash Message Authentication Code |
| UML | Unified Modelling Language |
| CSS | Cascading Style Sheet |
| IMEI | International Mobile Equipment Identity |