Abstract

Add nice abstract statement

Final Report

SePr 2016

Radu Stoica, Armin Roushan, Jan-Niklas Schneider, Georgiana Manolache, Nena O’Driscoll, Raditya Pratama

Table of Contents

[1 Introduction 2](#_Toc461745928)

[2 Web Application Overview 2](#_Toc461745929)

[3 Architecture 2](#_Toc461745930)

[4 Threat analysis 2](#_Toc461745931)

[4.1 CIA Analysis 2](#_Toc461745932)

[4.2 Authorization requirements 2](#_Toc461745933)

[4.3 Risk analysis 2](#_Toc461745934)

[5 Secure design 2](#_Toc461745935)

[6 Implementation choices 2](#_Toc461745936)

[7 Code example? 2](#_Toc461745937)

[8 References 3](#_Toc461745938)

# Introduction

# Web Application Overview

# Architecture

# Threat analysis

## CIA Analysis

## Authorization requirements

## Risk analysis

|  |  |  |  |
| --- | --- | --- | --- |
| Threat | Risk | Impact | Needed Security level Risk impact |
| Password Database Theft | High | High | High |
| Man-in-the-Middle (MitM), Man-in-the-Browser (MitB) | High | High | High |
| Identity Theft | High | High | High |
|  |  |  |  |

Password Database Theft = hackers get possession of costumer data from other less protected websites assuming user uses similar user ID and password.

Identity Theft = usage of fake profiles, malicious document links, site masking, blogs linked or hosting malware

# Secure design

# Implementation choices

# Code example?References