

**Graphical Passwords for avoiding shoulder surfing**

PROJECT DATE: 21-08-2020

BATCH NO: CSI-12

| TEAM MEMBERS | | | | |
| --- | --- | --- | --- | --- |
| S.No | NAME | ROLE | COLLEGE | CONTACT NO |
| 01 | Shanmuk Pandranki | Team Leader | Vignan’s institute of information technology | 9573294956,9490463466 |
| 02 | K.Akhliesh | Team Member | Vignan’s institute of information technology | 7382340034 |
| 03 | V.Jahnavi | Team Member | Vignan’s institute of information technology | 9381552400 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **PREPARED BY** | Shanmuk,Akhliesh,Jahnavi | **TITLE** | Graphical passwords for avoiding shoulder surfing | **DATE** | 3-8-2020 |
| **GUIDED BY** | Rajesh.D | **TITLE** | Graphical passwords for avoiding shoulder surfing | **DATE** | 21-8-2020 |

Table of Contents

[PROBLEM STATEMENT 3](#_Toc18578293)

[PROJECT SCOPE 3](#_Toc18578294)

[PRODUCT OR SYSTEM FEATURES AND REQUIREMENTS 4](#_Toc18578295)

[PROJECT SUCCESS CRITERIA 4](#_Toc18578296)

[PROJECT SUCCESS CRITERIA 5](#_Toc18578297)

[1. STATEMENT OF WORK 6](#_Toc18578298)

[1.1 SCOPE OF WORK 6](#_Toc18578299)

[1.2 LOCATION OF WORK 6](#_Toc18578300)

[1.3 PERIOD OF PERFORMANCE 6](#_Toc18578301)

[1.4 SCHEDULE 6](#_Toc18578302)

[1.5 STANDARDS FOLLOWED 6](#_Toc18578303)

[1.6 ACCEPTANCE CRITERIA FOR USERS 6](#_Toc18578304)

[1.7 ADDITIONAL REQUIREMENTS 6](#_Toc18578305)

# PROBLEM STATEMENT

Problems faced by the users while using the current system

|  |
| --- |
| Almost everyone of us faced an issue like we have been watched when we type our credentials. This is called Shoulder Surfing. Though it looks normal, it leads to serious issues like password theft and leads to hacked user accounts.So, ti prevent these type of Shoulder surfing attacks taking place we have to implement a new type of authenticating system like using graphical passwords instead of convetional passwords. |

# PROJECT SCOPE

Project Purpose and Justification

|  |
| --- |
| Shoulder surfing is a serious issue, and has legal implications as well. Despite the column appearing in CIO magazine, where the “I” stands for “Information” and not computers, it fails to understand that companies have to protect information in all of its forms, and not just the underlying technology of computers. A “hacker” doesn’t care if they get the information by compromising computer technology, stealing a laptop from a car, or looking over someone’s computer on an airplane. More important, there are more than just “real live hackers” today, i.e. criminals, competitors, malicious insiders, and even the “creepers”.  Graphical password schemes have been proposed as a possible alternative to text-based schemes, motivated partially by the fact that humans can remember pictures better than text; psychological studies support such an assumption. Pictures are generally easier to be remembered or recognized than text. In addition, if the number of possible pictures is sufficiently large, the possible password space of a graphical password scheme may exceed that of text-based schemes and thus presumably offer better resistance to attacks. Because of these advantages, there is a growing interest in graphical password. In addition to web log-in applications, graphical passwords have been applied to ATM machines and mobile services. |

# PRODUCT OR SYSTEM FEATURES AND REQUIREMENTS

|  |
| --- |
| Software Requirements  Python3.x to be installed.  The following modules are to be installed:  - Flask  - SQLAlchemy  - Flask\_login  - Werkzeug.Security |

# PROJECT SUCCESS CRITERIA

|  |
| --- |
| we used two different methods in our project to take graphical passwords  Method-1  The user is asked to select a certain number of images (four)  from a set of random pictures generated by a program in the registration process . Later, the user will be required to identify the pre selected images in  login form in order to be authenticated.  Method-2  The user is asked to select one image from row and another image from the column in the registration process. Later, a number of images will be displayed along with registration page images .The intersection image of the preselected image should be considered as a password.  The results showed that 90% of all participants succeeded in the authentication using this technique, while only 70% succeeded using text-based passwords and PINS |

# STATEMENT OF WORK

## SCOPE OF WORK

|  |
| --- |
| Much more research is needed for graphical password techniques to achieve higher levels of usefulness.  The results showed that 90% of all participants succeeded in the authentication using this graphical passwords, while only 70% succeeded using text-based passwords and PINS |

## LOCATION OF WORK

|  |
| --- |
| Online platform |

## PERIOD OF PERFORMANCE

|  |
| --- |
| 3-August-2020 to 21-August-2020 |

## SCHEDULE

|  |  |  |  |
| --- | --- | --- | --- |
| **CATEGORY/TASK** | **WORK DONE** | **START DATE** | **END DATE** |
| Phase 1 - Planning | Gathering information and downloading required software | 3-8-2020 | 6-8-2020 |
| Task A | Gathered information about frontend and backend of a website | 3-8-2020 | 4-8-2020 |
| Task B | Gathered information of database | 4-8-2020 | 6-8-2020 |
| Phase 2 - Execution | Designing frontend and worked on server authentication | 7-8-2020 | 13-8-2020 |
| Task A | Designed login and registration page and completed website work | 7-8-2020 | 10-8-2020 |
| Task B | Working on website authentication | 10-8-2020 | 13-8-2020 |
| Phase 3 - Monitoring | Working on different methods for taking graphical passwords | 14-8-2020 | 17-8-2020 |
| Task A | Working on method one to take four different images in login and registration process | 14-8-2020 | 15-8-2020 |
| Task B | Working on method two to take intersection element in login page | 16-8-2020 | 17-8-2020 |
| Phase 4 - Closing | Completed coding , authentication, document ,ppt. | 17-8-2020 | 21-8-2020 |
| Task A | Checked the coding part, website ,password authentication and output | 17-8-2020 | 19-8-2020 |
| Task B | Done with entire project successfully | 20-8-2020 | 21-8-2020 |

## STANDARDS FOLLOWED

|  |
| --- |
| Hyper Text Markup Language (HTML)  Cascading Style Sheets(CSS)  Javascript(Js)  Bootstrap  Python Flask  Flask SQLAlchemy (Database)  Sha-256 hasing for hasing passwords |

## ACCEPTANCE CRITERIA FOR USERS

|  |
| --- |
| Pictures are generally easier to remembered or recognized than text. The results showed that 90% of all participants succeeded in the authentication using this graphical passwords, while only 70% succeeded using text-based passwords and PINS |

## ADDITIONAL REQUIREMENTS

|  |
| --- |
|  |

CONCLUSION

Graphical passwords are an alternative to alphanumeric passwords

It satisfies both conflicting requirements i.e. easy to remember and hard to guess

By the problem of shoulder surfing problem, it becomes more secure and easier password scheme

REFERENCES

<https://www.geeksforgeeks.org/graphical-password-authentication/>

<https://stackoverflow.com/questions/17541614/use-images-instead-of-radio-buttons>

<https://flask.palletsprojects.com/en/1.1.x/patterns/flashing/>