



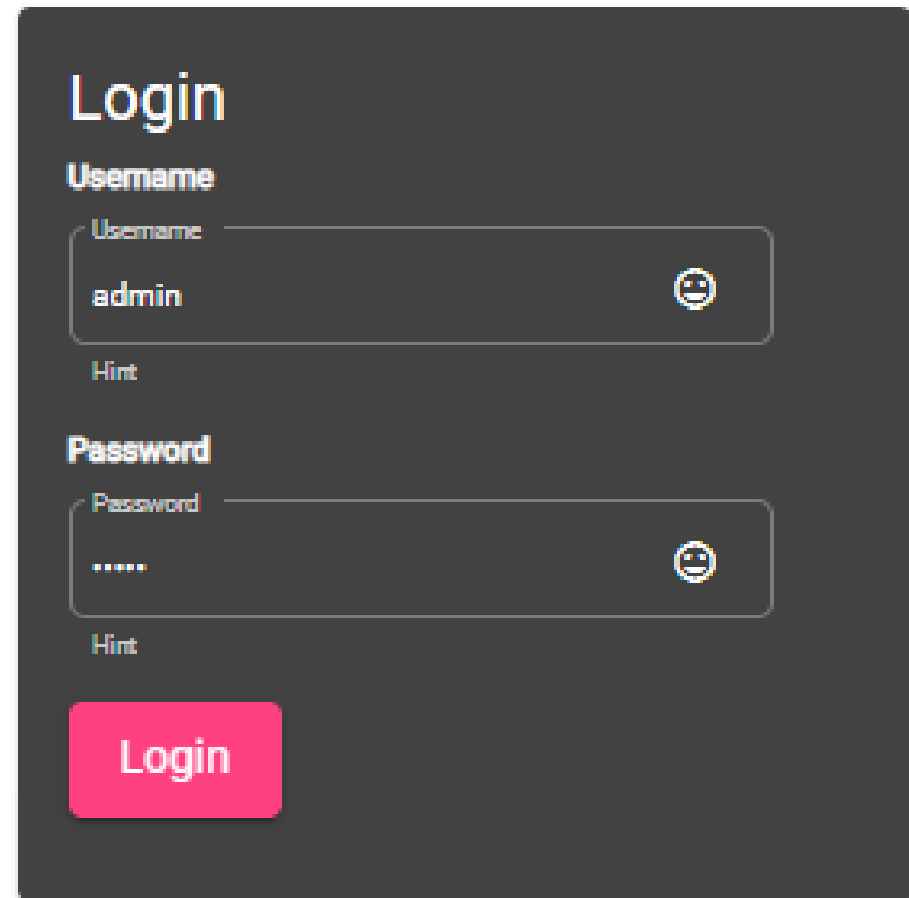
OWASP

RISK ASSESSMENT FRAMEWORK

HOW TO LOGIN

Use below credentials,

- Username : admin
- Password : admin-RAF

A login form interface with a dark gray background. At the top, the word "Login" is displayed in a large, white, sans-serif font. Below it, the label "Username" is shown in a smaller, white, sans-serif font. Under the label, there is a text input field with a light gray border. Inside the field, the word "admin" is entered in a white, sans-serif font. To the right of the input field is a small, white, circular icon containing a smiley face. Below the input field, the word "Hint" is displayed in a small, white, sans-serif font. Below "Hint", the label "Password" is shown in a smaller, white, sans-serif font. Under the label, there is a text input field with a light gray border. Inside the field, several dots represent a masked password. To the right of the input field is a small, white, circular icon containing a smiley face. Below the input field, the word "Hint" is displayed in a small, white, sans-serif font. At the bottom of the form, there is a large, red, rectangular button with rounded corners. The button contains the word "Login" in a white, sans-serif font.

LANDING PAGE/ HOME PAGE

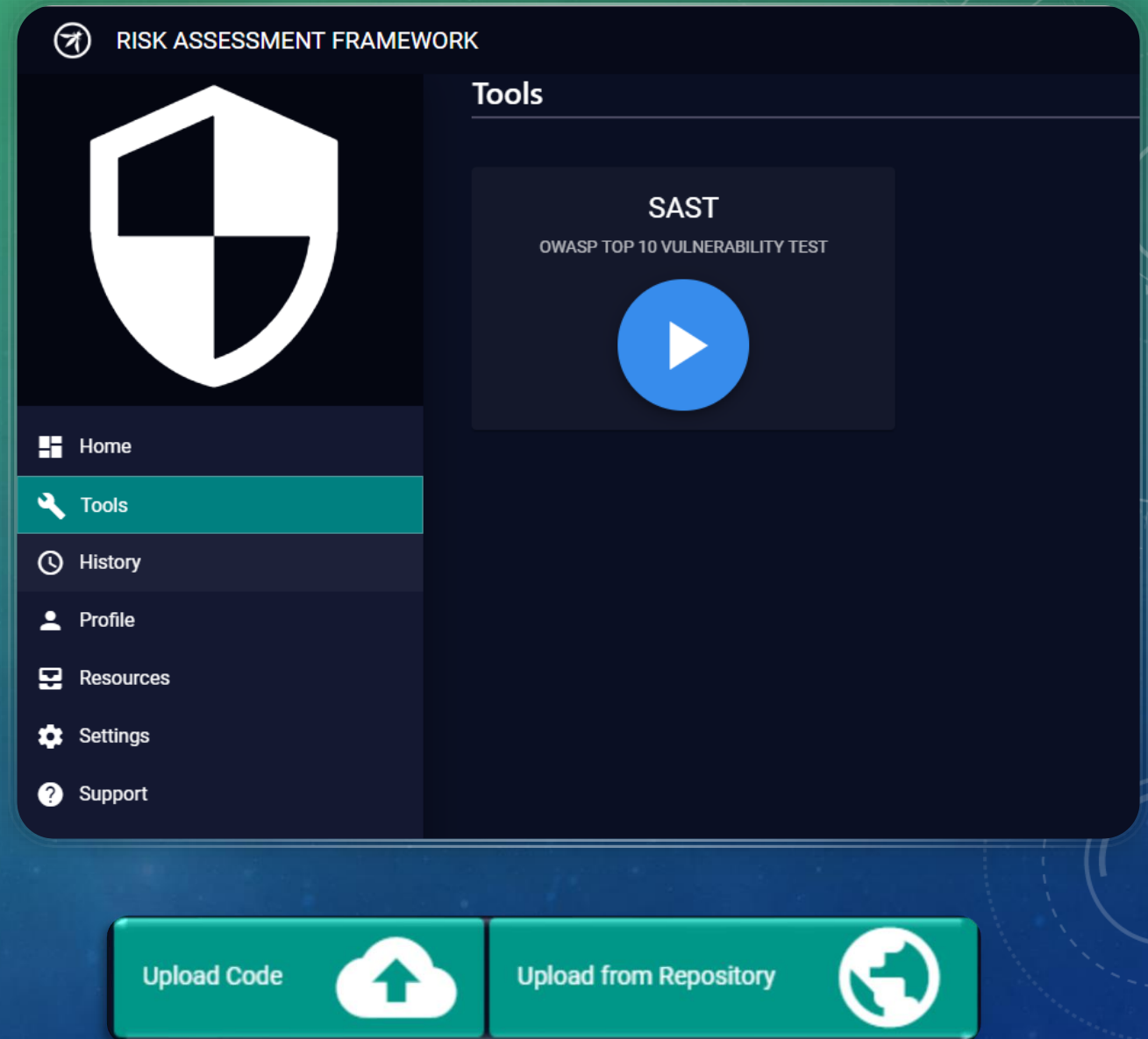
- Summarized results of your tests can be viewed from here
- Using the left sidebar you will be able to navigate to other pages.
- Mainly,
 - Total Scans
 - Vulnerabilities detected
 - Report count

Can be viewed



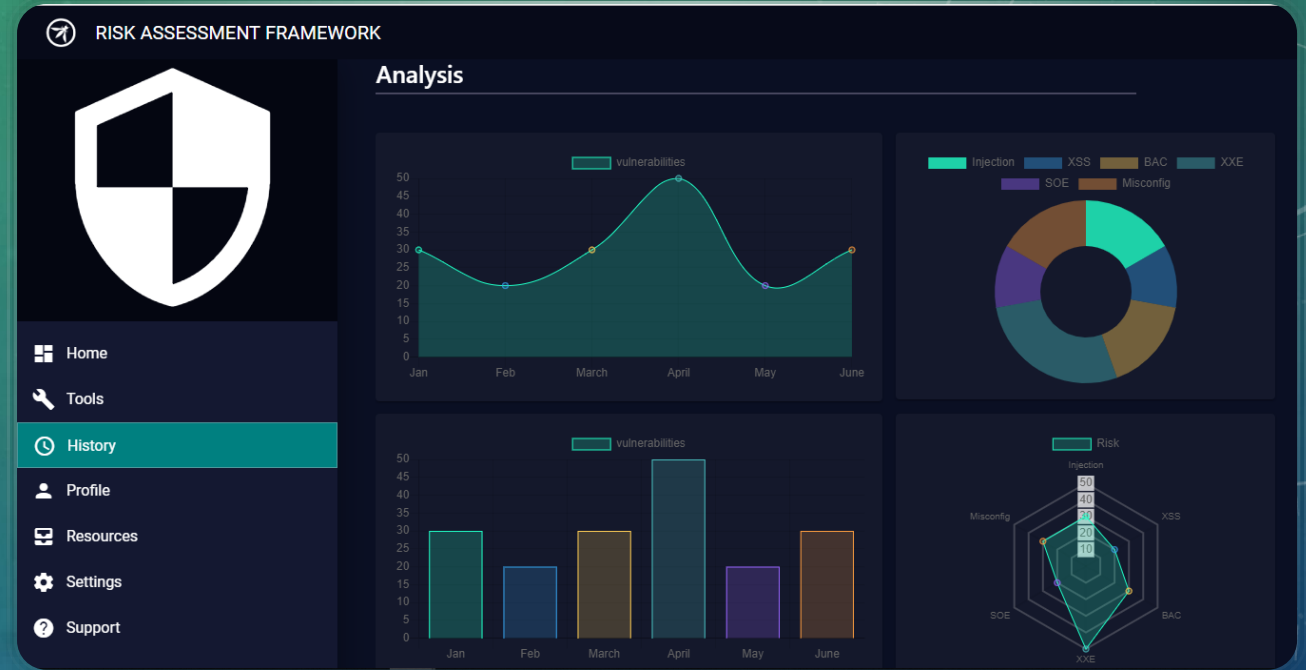
TOOLS PAGE

- Tools page let you access the tools provided by the Risk Assessment Framework
- Where you can upload your code to get the results.
- Types of code upload,
 - Upload from local disk
 - Upload from repository



HISTORY PAGE

- In Analysis section you will be able to view your results of the tests you conducted
 - By Time Line
 - By Vulnerability Type
- You can download your monthly reports from the report section.

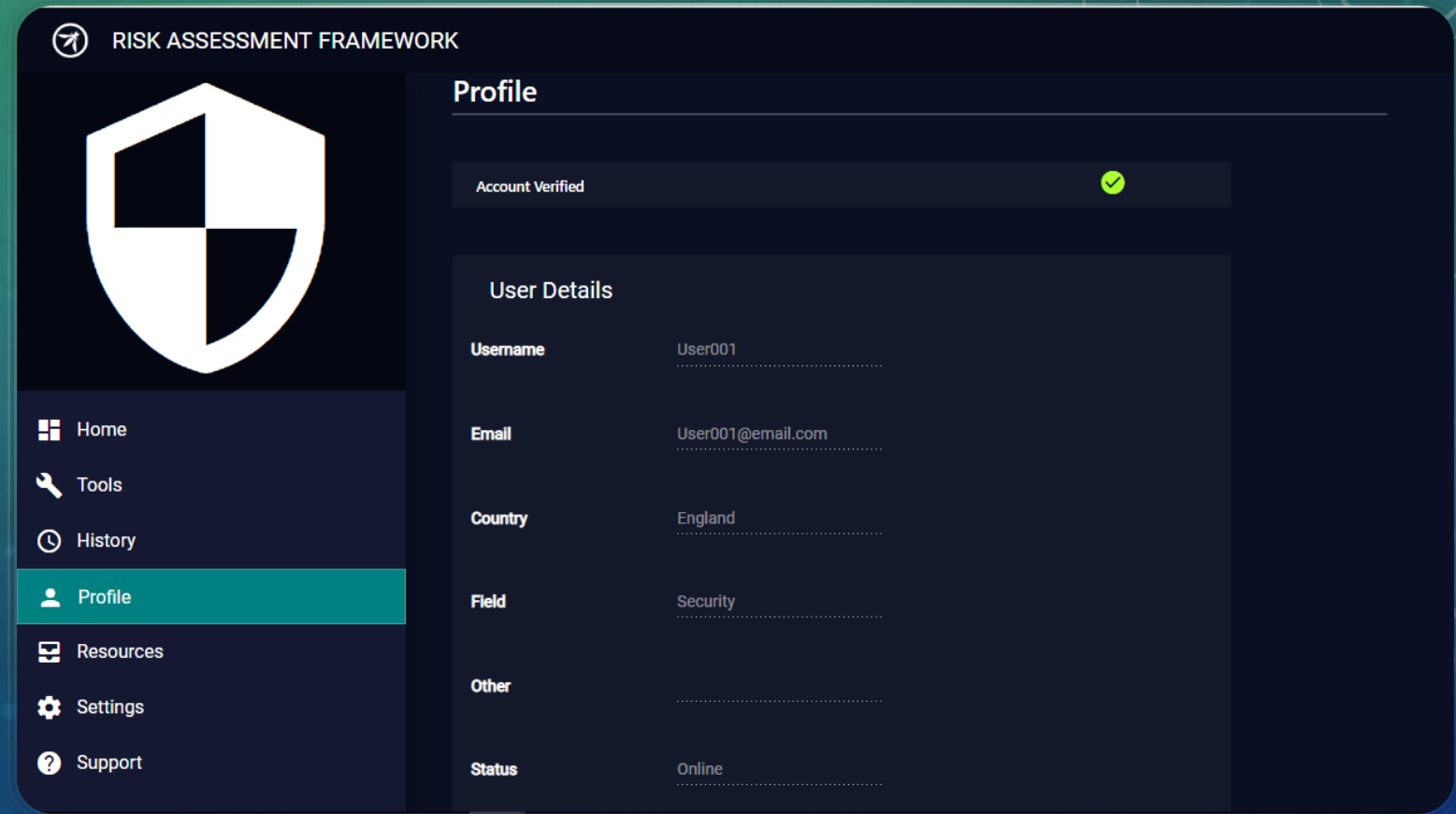


Reports

ID	Month	Issues	
1	Jan	1	Download
2	Feb	4	Download
3	March	6	Download
4	April	9	Download
5	May	10	Download
6	June	12	Download
7	July	14	Download
8	Aug	15	Download
9	Sep	18	Download

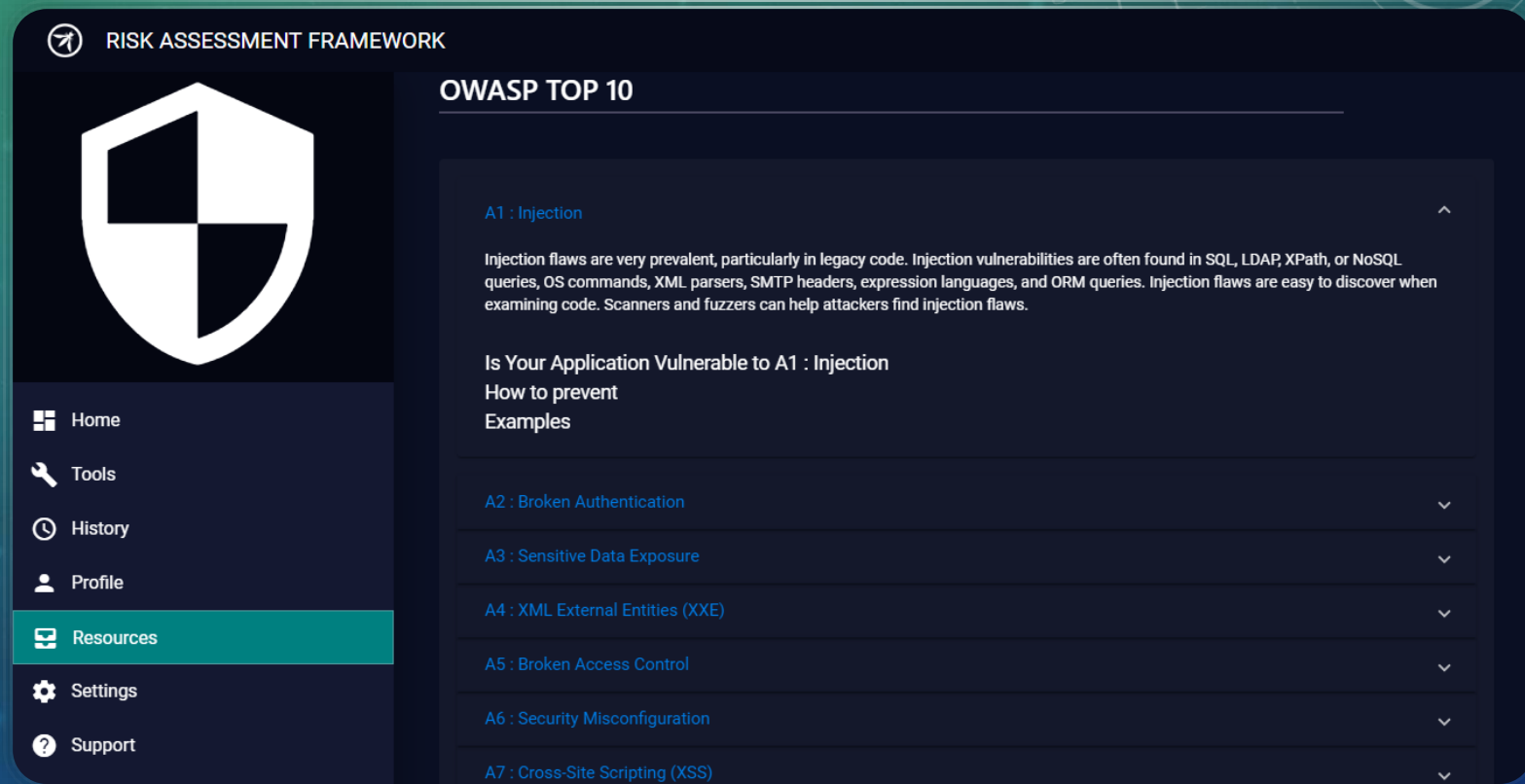
PROFILE PAGE

- You can view your profile details in this page
- You can check whether your account is verified




RESOURCE PAGE

- You can find resources relevant to securing your code from this section,
 - OWASP TOP 10
 - Video Tutorials
- “Is your application vulnerable” you will be able check if your code has issues related to the topic
- “How to prevent” will give you resources to prevent from that issue
- “Examples” will give you example vulnerable code examples.



SETTINGS PAGE

- You will be able to change the settings related to the dashboard using this page



Home

Tools

History

Profile

Resources

Settings

Support

RISK ASSESSMENT FRAMEWORK

Settings

USER SETTINGS

THEMES

DASHBOARD

TOOLS

ACCOUNT


Email :


Username :


Password :


SUPPORT PAGE


- This page will help you to with the Frequently Asked Questions about securing the code





 Home


 Tools

 History

 Profile

 Resources

 Settings

 Support

F.A.Q

How do we prevent SQL Injection in our applications?

It is quite simple to prevent SQL injection while developing the application. You need to check all input coming from the client before building a SQL query. The best method is to remove all unwanted input and accept only expected input. While server side input validation is the most effective method of preventing SQL Injection, the other method of prevention is not using dynamic SQL queries. This can be achieved by using stored procedures or bind variables in databases that support these features. For applications written in Java, CallableStatements and PreparedStatement can be used. For ASP applications, ADO Command Objects can be used. You can check the following article for more on SQL Injection in Oracle: [IntegrigyIntrotoSQLInjectionAttacks.pdf](#)

Is there some way to prevent these proxy tools from editing the data?

How can I prevent XSS?

How can I prevent XSS?

What are these W3C logs?