

# SAIVS

**S**pider **A**rtificial **I**ntelligence **V**ulnerability **S**canner

MBSD Professional Service Div.

Isao Takaesu



Isao Takaesu



## About the presenter

- Occupation: Web security engineer.
- Company: Mitsui Bussan Secure Directions.
- Hobbies: Bug hunting, Making scanners.

# Agenda

1. Introduction
2. Objectives of SAIVS
3. Future Prospects
4. Demonstration

# What is SAIVS?

---

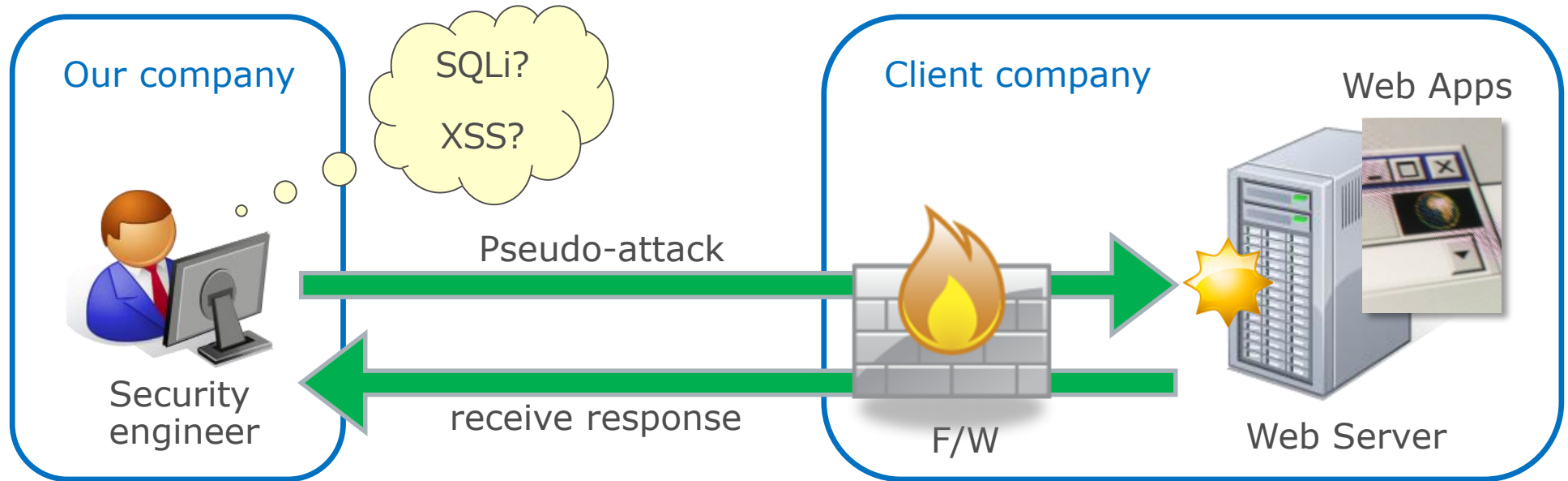
✓ SAIVS

= **S**pider **A**rtificial **I**ntelligence **V**ulnerability **S**canner.

✓ It performs **vulnerability assessment** in **Web apps**.

# What is vulnerability assessment?

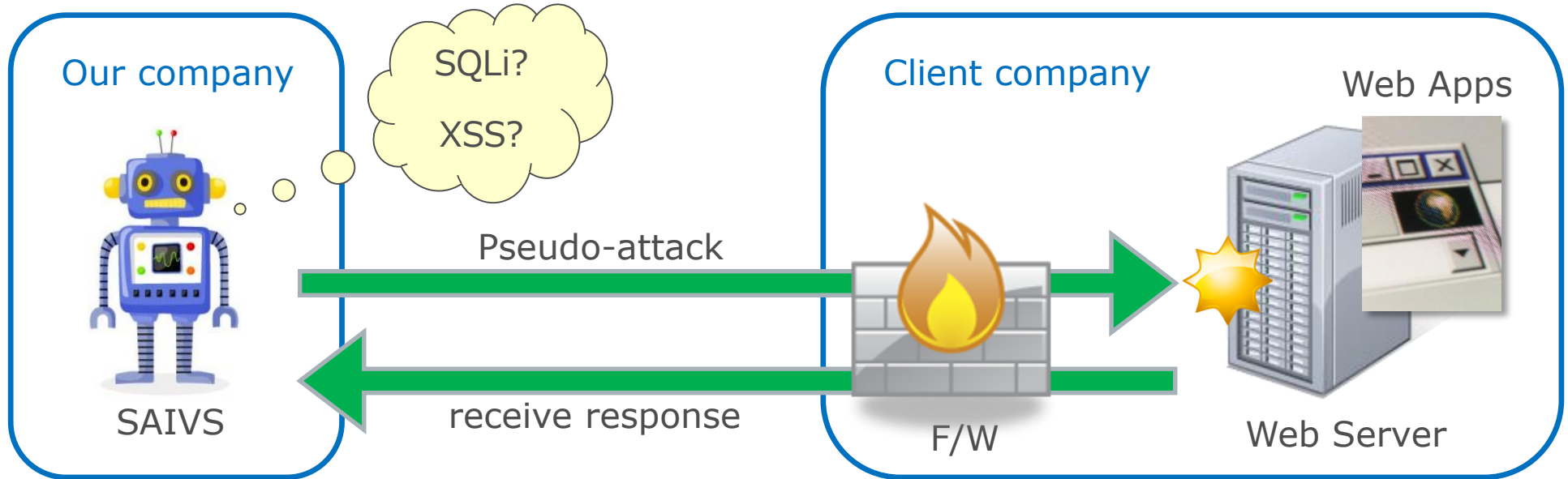
## Web application vulnerability assessment by a security engineer



- ✓ Performs pseudo-attacks while **crawling the pages** of Web Apps.
- ✓ Analyzes the response and finds vulnerabilities.

# Our "GOAL"

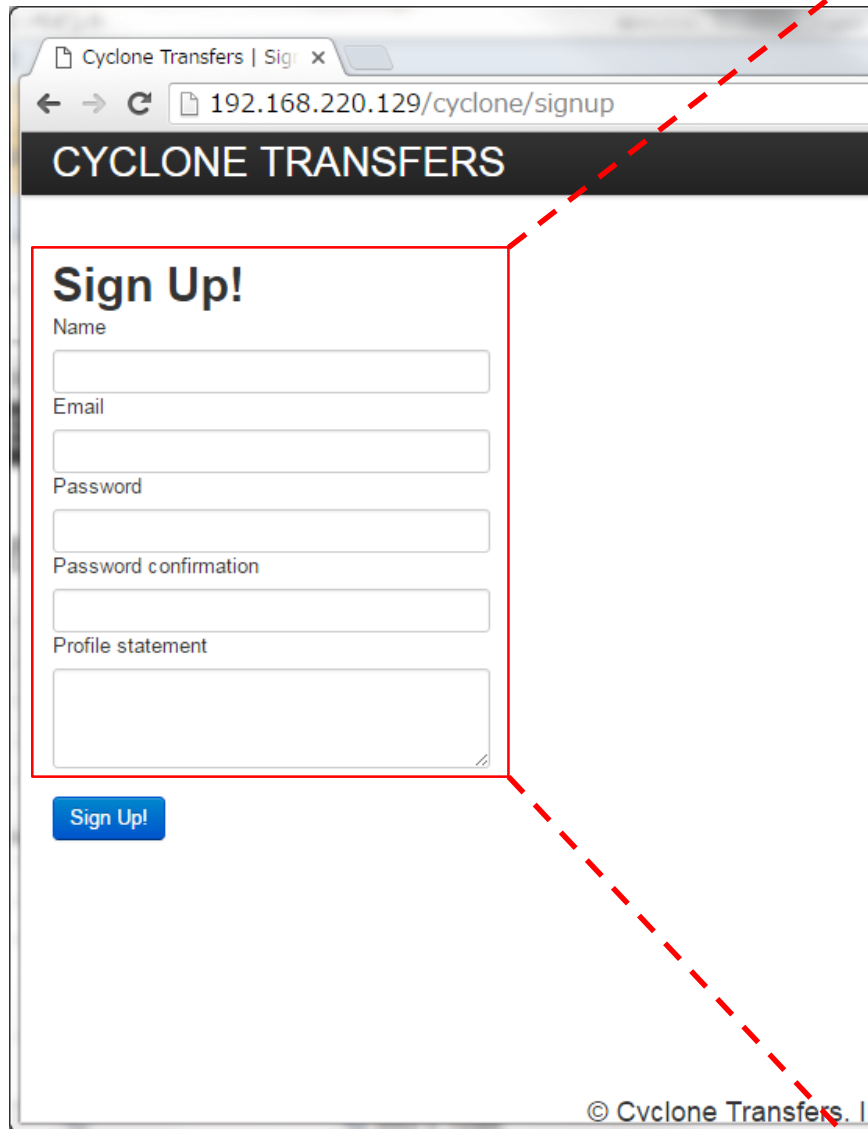
Realize "ALL MACHINE" Web application vulnerability assessment.



- ✓ Performs vulnerability assessment like a human security engineer.
- ✓ Apply to actual security assessments and bug bounty programs.

SAIVS can **crawl** simple Web applications.  
⇒ using **machine learning** algorithms.

What is the **type** of this page?



# Sign Up!

Name

Email

Password

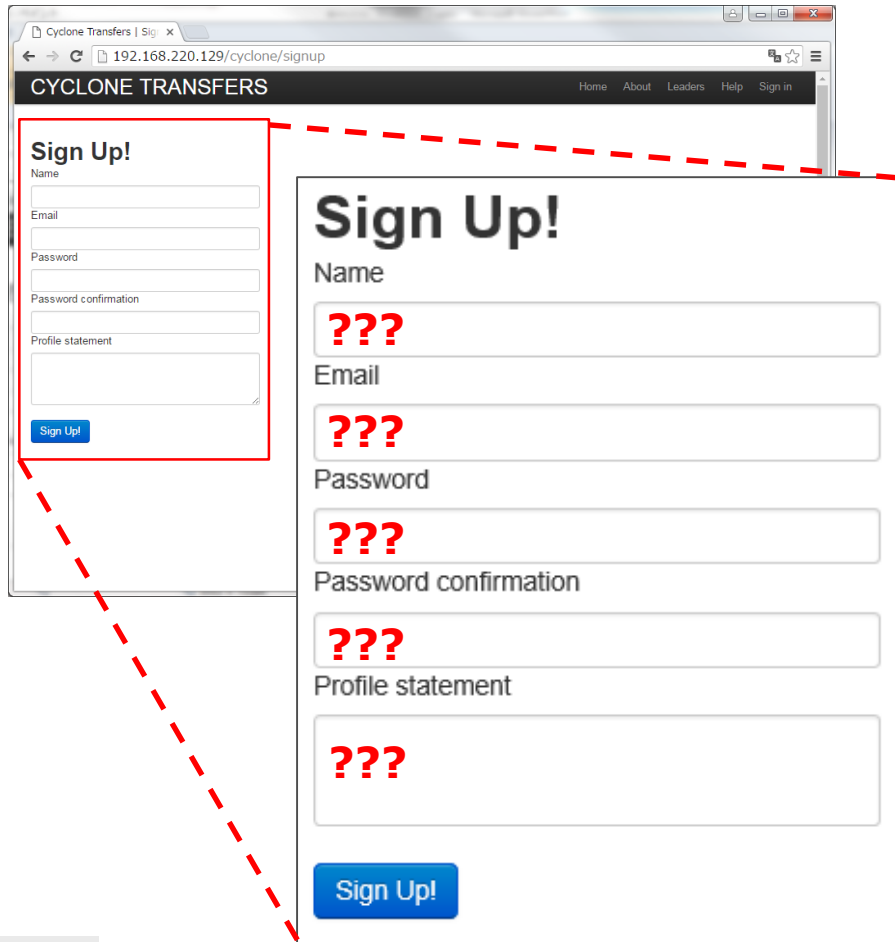
Password confirmation

Profile statement

**Sign Up!**



# What are your **input values** to transition to the next page?



**CYCLONE TRANSFERS** Home About Leaders Help Sign in

### Sign Up!

Name

Email

Password

Password confirmation

Profile statement

**Sign Up!**

Name

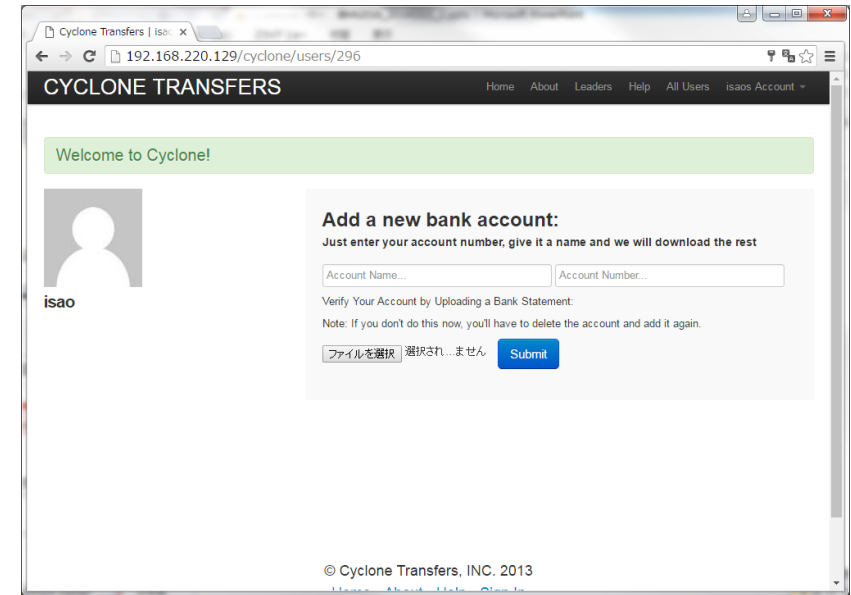
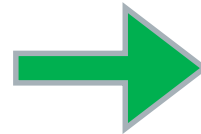
Email

Password

Password confirmation


Profile statement

transition



**CYCLONE TRANSFERS** Home About Leaders Help All Users isaos Account

Welcome to Cyclone!

  
isao

### Add a new bank account:

Just enter your account number, give it a name and we will download the rest

Account Name...  Account Number...

Verify Your Account by Uploading a Bank Statement:  
Note: If you don't do this now, you'll have to delete the account and add it again.

選択され...ません

© Cyclone Transfers, INC. 2013

# What has just happened?

The screenshot shows a web browser window with the URL `192.168.220.129/cyclone/users`. The page title is "CYCLONE TRANSFERS" and it has a navigation menu with "Home", "About", "Leaders", "Help", and "Sign in". The main heading is "Sign Up!".

Two error messages are displayed in light red boxes. The top one says "2 errors prohibited this user from being saved" and lists "Password doesn't match confirmation" and "Email is invalid". A red dashed line connects this message to a second, identical one below it. In the second message, the word "invalid" in the second bullet point is highlighted with a red box.

The sign-up form fields are as follows:

- Name:
- Email:
- Password:
- Password confirmation:
- Profile statement:

# SAIVS uses machine learning algorithms to “think”

Crawling requires the following **thinking patterns**:

Thinking pattern	Algorithm
Recognize the <b>page type</b>	<b>Naive Bayes</b>
Recognize the <b>success or failure</b> of a page transition	
Learn the <b>optimal parameter values</b>	<b>Multilayer Perceptron Q-Learning</b>

# What is **Naive Bayes**?

---

Naive Bayes is used for **auto classification of texts**

using **pre-defined categories** & **laws of probability**.

examples)

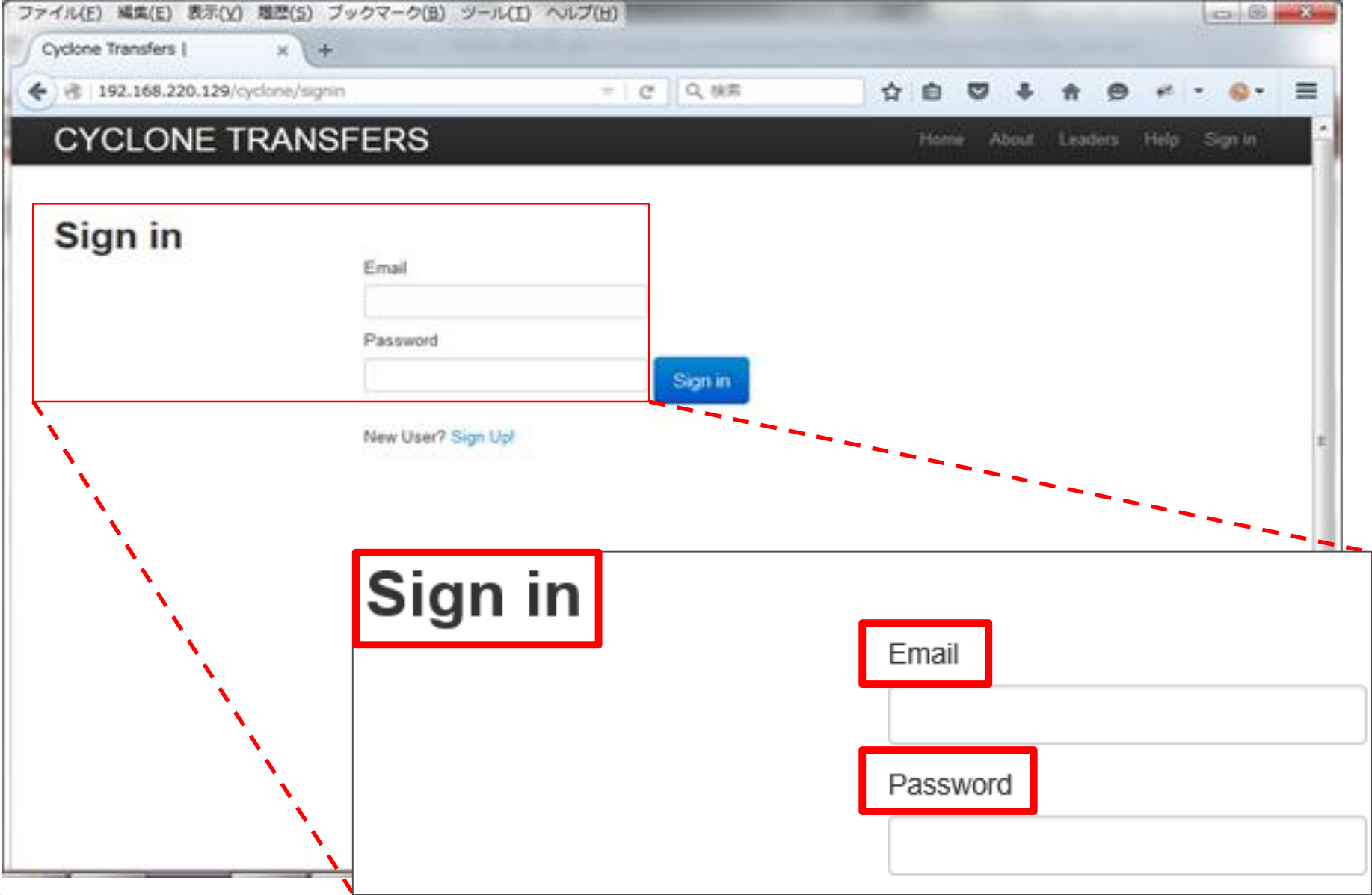
- ✓ Spam mail filter (Spam or Ham).
- ✓ Classify blog post genres (Sports or Politics or Music or Tech).

# Page categories and classified texts for Naive Bayes

Category table used for **page classification**

<b>Category(page types)</b>	<b>keywords used for classification</b>
Login	Email, User ID, Password, Sign in ...
Registration	Email, Password, Confirm, Sign up ...
Search	Word, Text, String, Sort, Search ...

# Recognizing the page type from the texts on the page



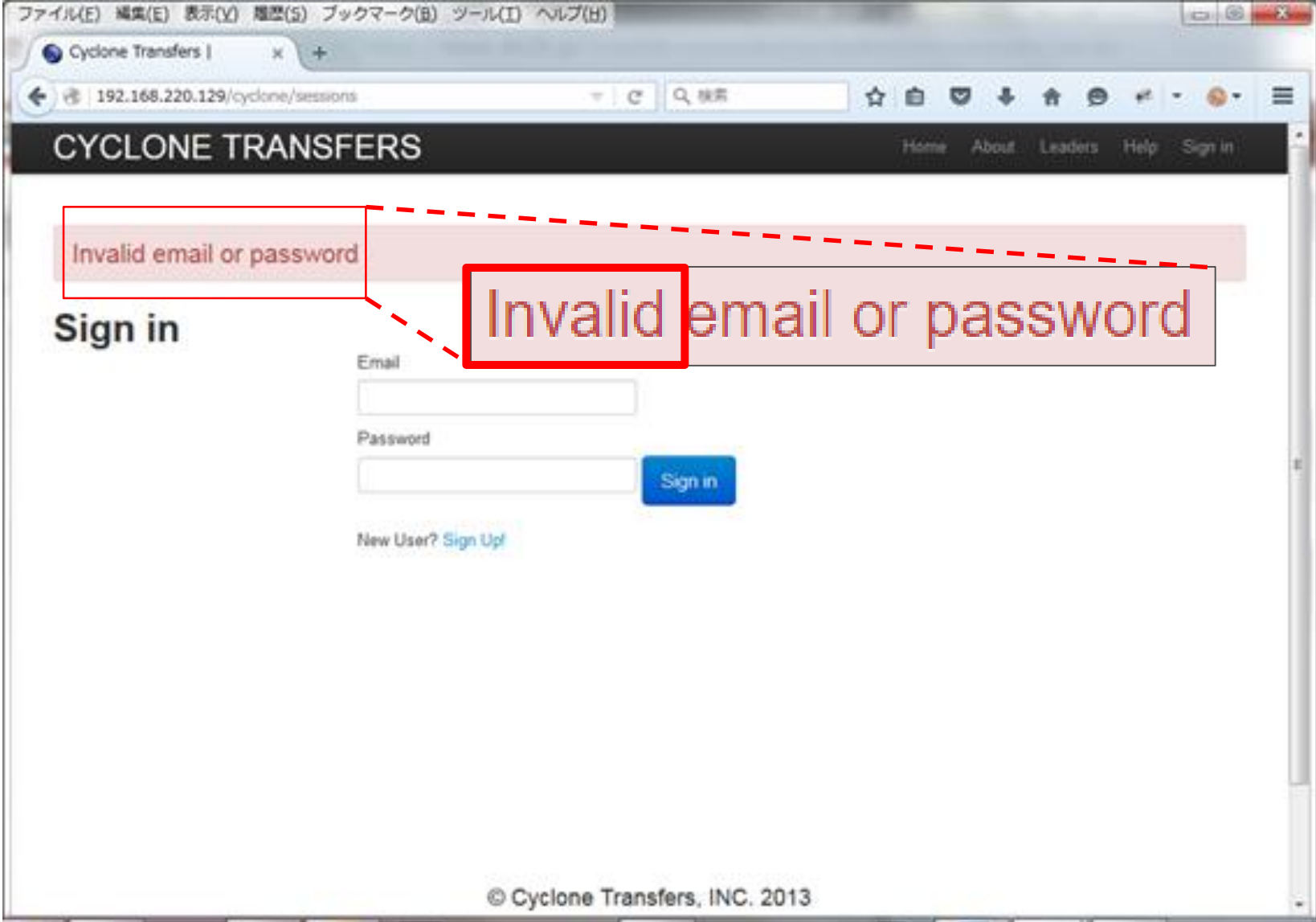
# HTML source of "Sign in" page

```
<h1>Sign in</h1>  
<form action="/cyclone/sessions" method="post">  
<label for="email">Email</label>  
<input id="email" name="email" type="text" />  
<label for="password">Password</label>  
<input id="password" name="password" type="password" />  
</form>
```

SAIVS will recognize the page type using:

- the texts presented on the page (keywords)
- probabilities of the keywords appearing in the categories (page types)

# Recognize the success or failure of page transitions





# HTML source of a failed page transition

```
<div>Invalid email or password </div>
```

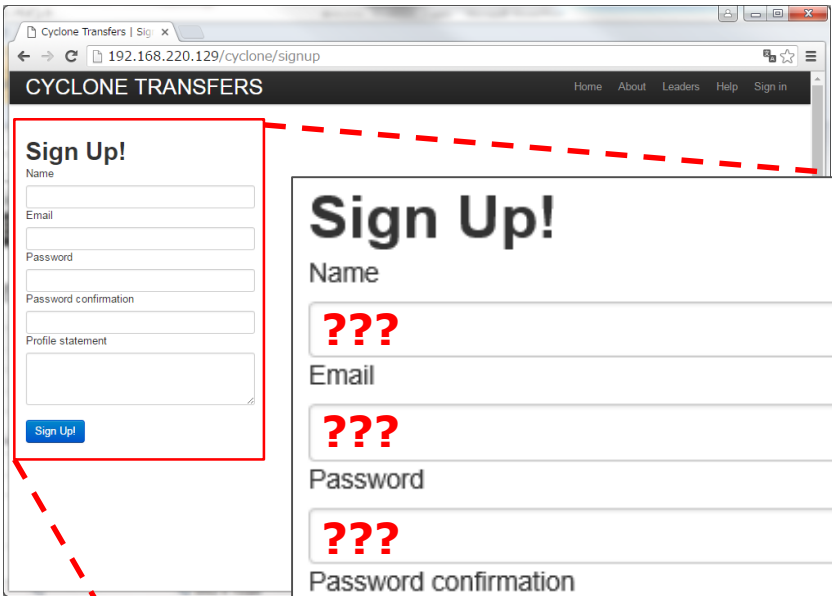
SAIVS will recognize the transition success/failure  
using the texts presented on the page.

Category(good or not)	Keywords used for classification
Success	Good, Valid, Success, Normal, Fine ...
Failure	Bad, Invalid, Failure, Error, Unmatch ...

Category table for "success/failure" texts

# Learning optimal values

What are your **input values** to transition to the next page?



**Sign Up!**

Name  
???

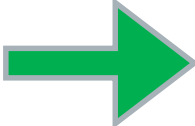
Email  
???

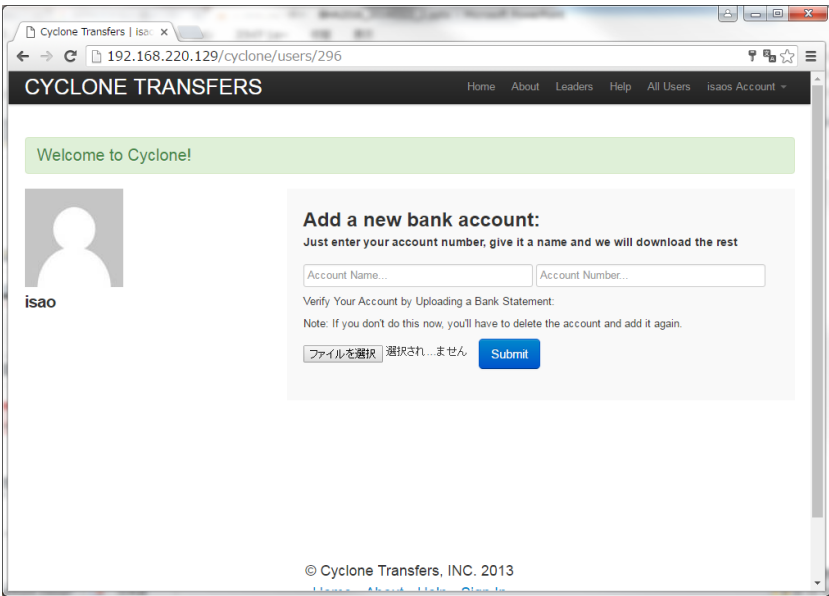
Password  
???

Password confirmation  
???

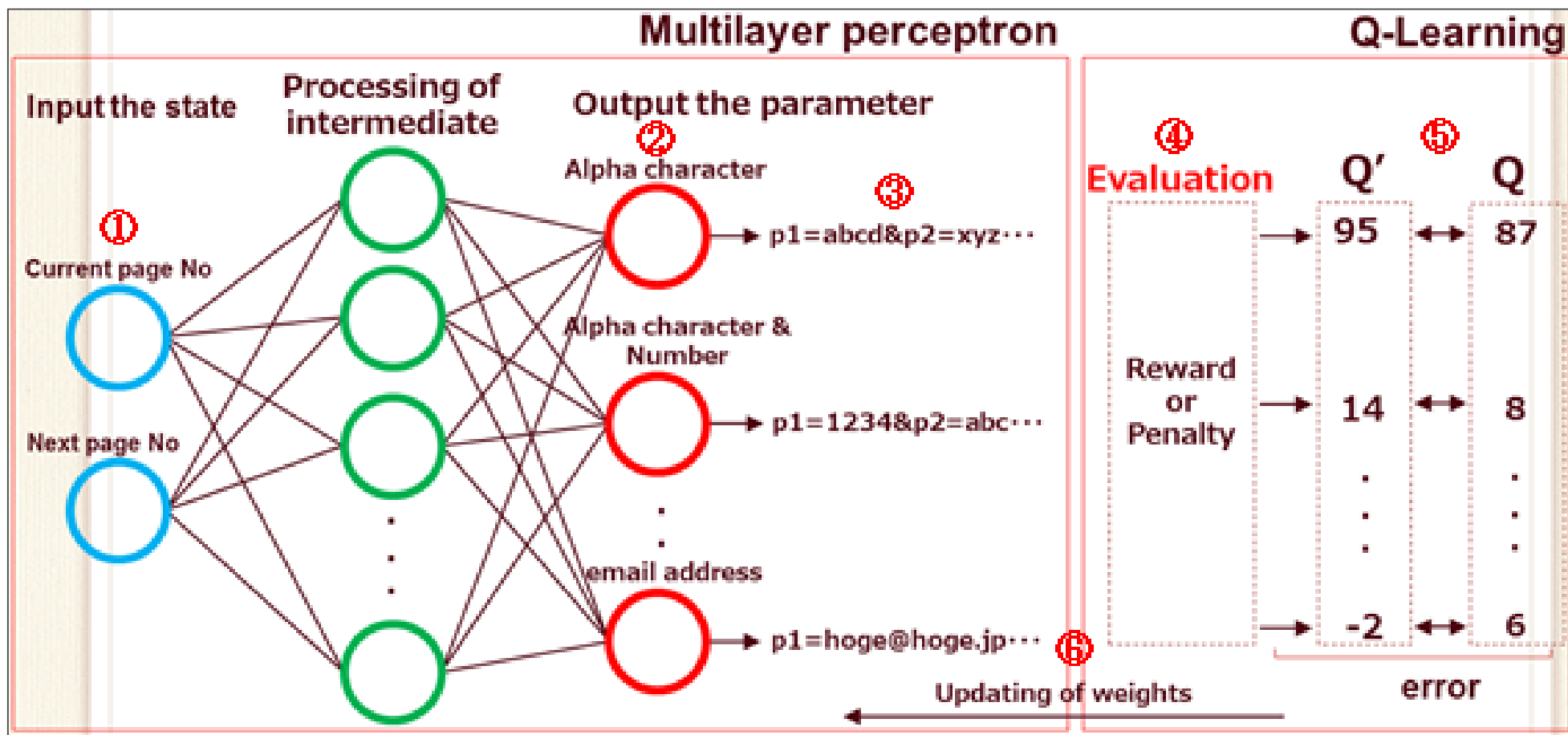
Profile statement  
???

**Sign Up!**

transition 



# Calculating optimal value for page transition



This model can determine the optimal parameter value for a page transition.

# Future prospects

---

We will enhance **scanning** and **page transition** abilities.

- ✓ Strengthening the **page transitioning** capability.
- ✓ Strengthening the **scanning** capability.
- ✓ Applying the technology to business.

Next step for SAIVS... adding NLP to improve the AI!?

[https://www.mbsd.jp/blog/20160113\\_2.html](https://www.mbsd.jp/blog/20160113_2.html)

Company:	MBSD - Mitsui Bussan Secure Directions, Inc.
Established:	2001
Head office:	Tokyo, Japan
Paid in capital:	JPY 400 Mil (100% subsidiary of Mitsui & Co., Ltd)
Employees:	180
Industry affiliations:	Leading companies in Japan, such as telecoms, banks, retailers, internet business, and the governments.
Businesses:	Professional security services to protect business from cyber attacks
Services:	Vulnerability Assessment/Pentesting (Web/Mobile/Game/IoT...) Managed Security Services (SOC 1.0/2.0) Incident Response & Handling, Digital forensics Secure Programming Training GRC Consulting Research & Development

# THANK YOU!

- **Download “.PDF” version of this document:**
  - **<https://www.blackhat.com/asia-16/arsenal.html>**