SAIVS

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

MBSD Professional Service Div.
Isao Takaesu

Isao Takaesu

M|B|S|D

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?

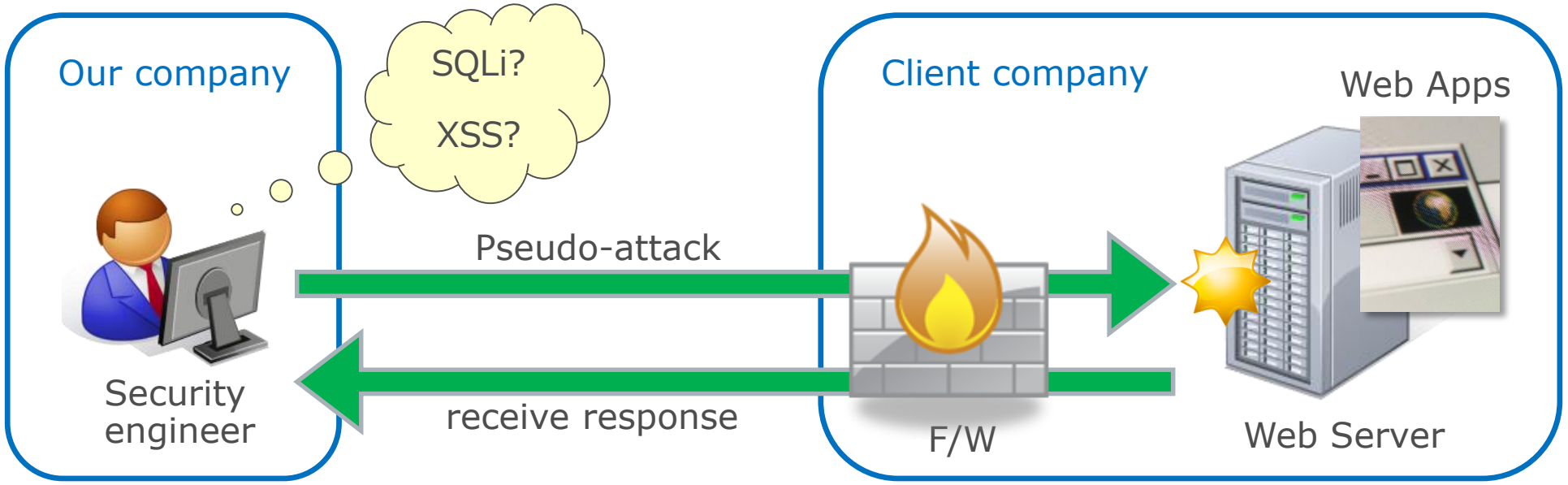
- ✓ SAIVS

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

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

What is vulnerability assessment?

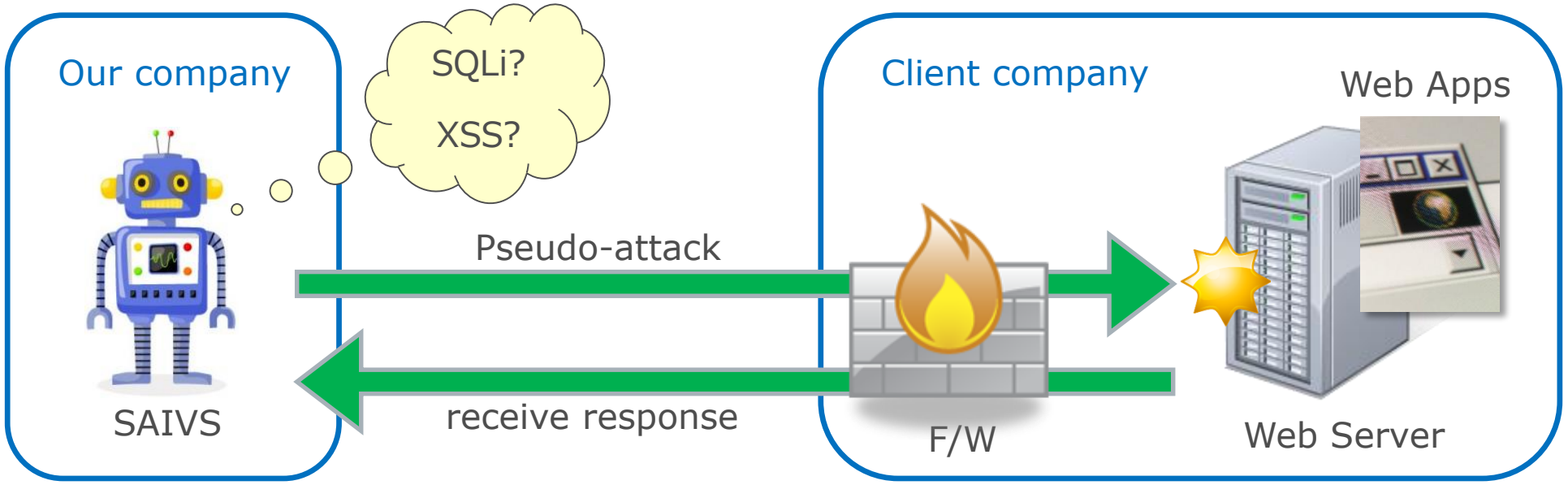
Web application vulnerability assessment by a security engineer



- ✓ 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.

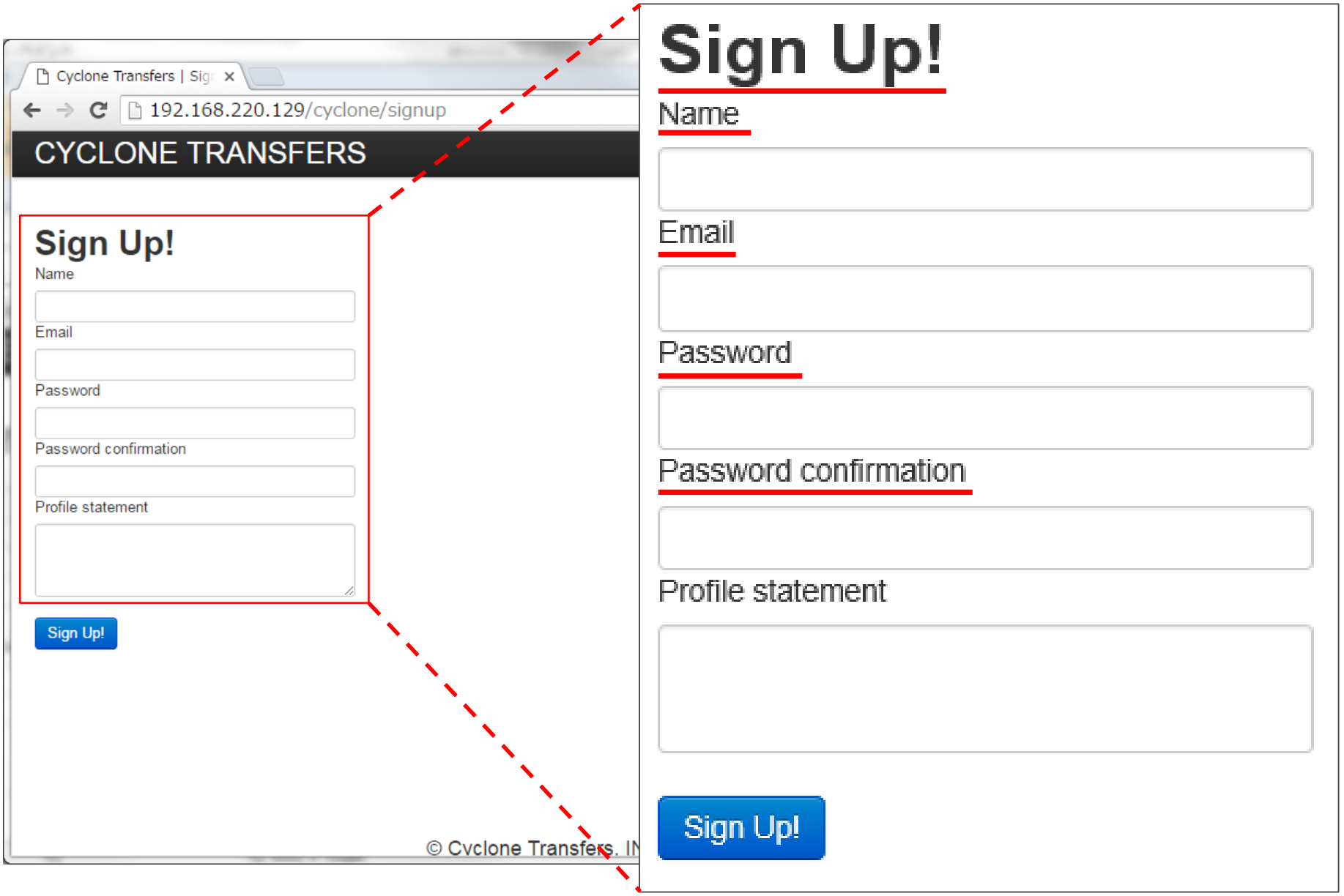
POWERPOINT DESIGN

Today’s point!!

SAIVS can **crawl** simple Web applications.

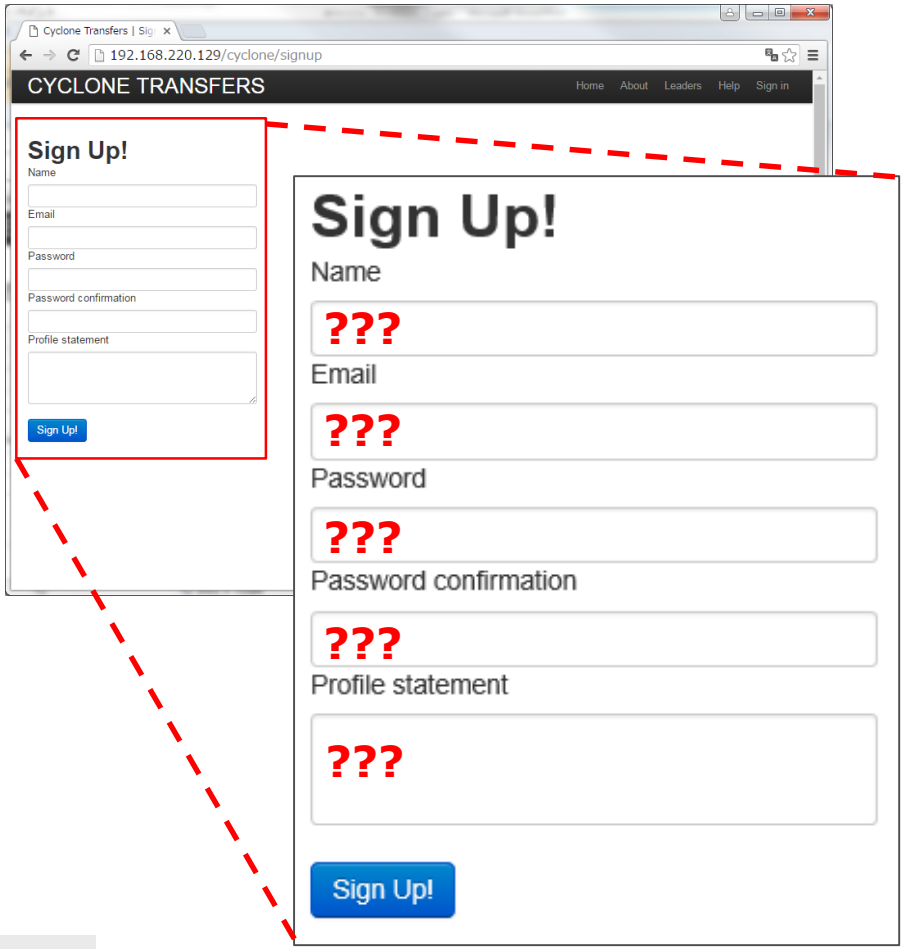
⇒using **machine learning** algorithms.

What is the type of this page?

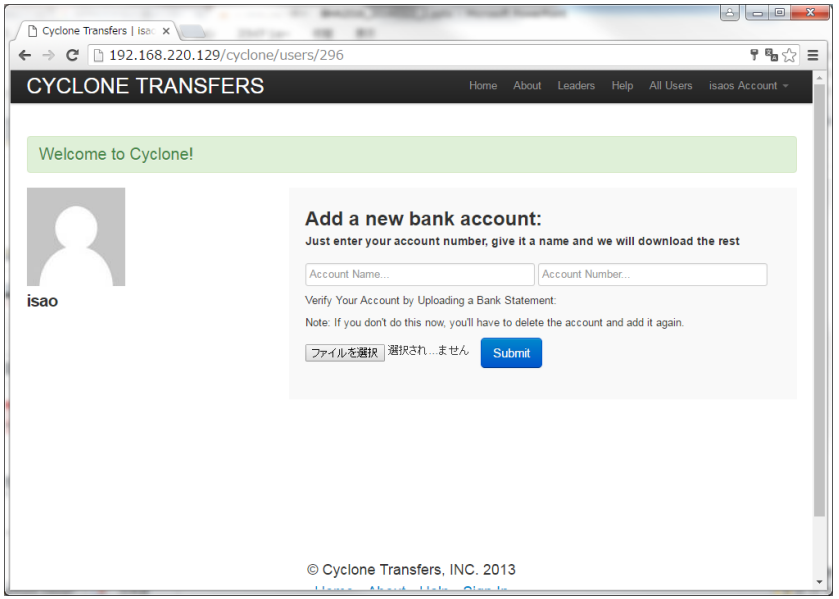


POWERPOINT DESIGN

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

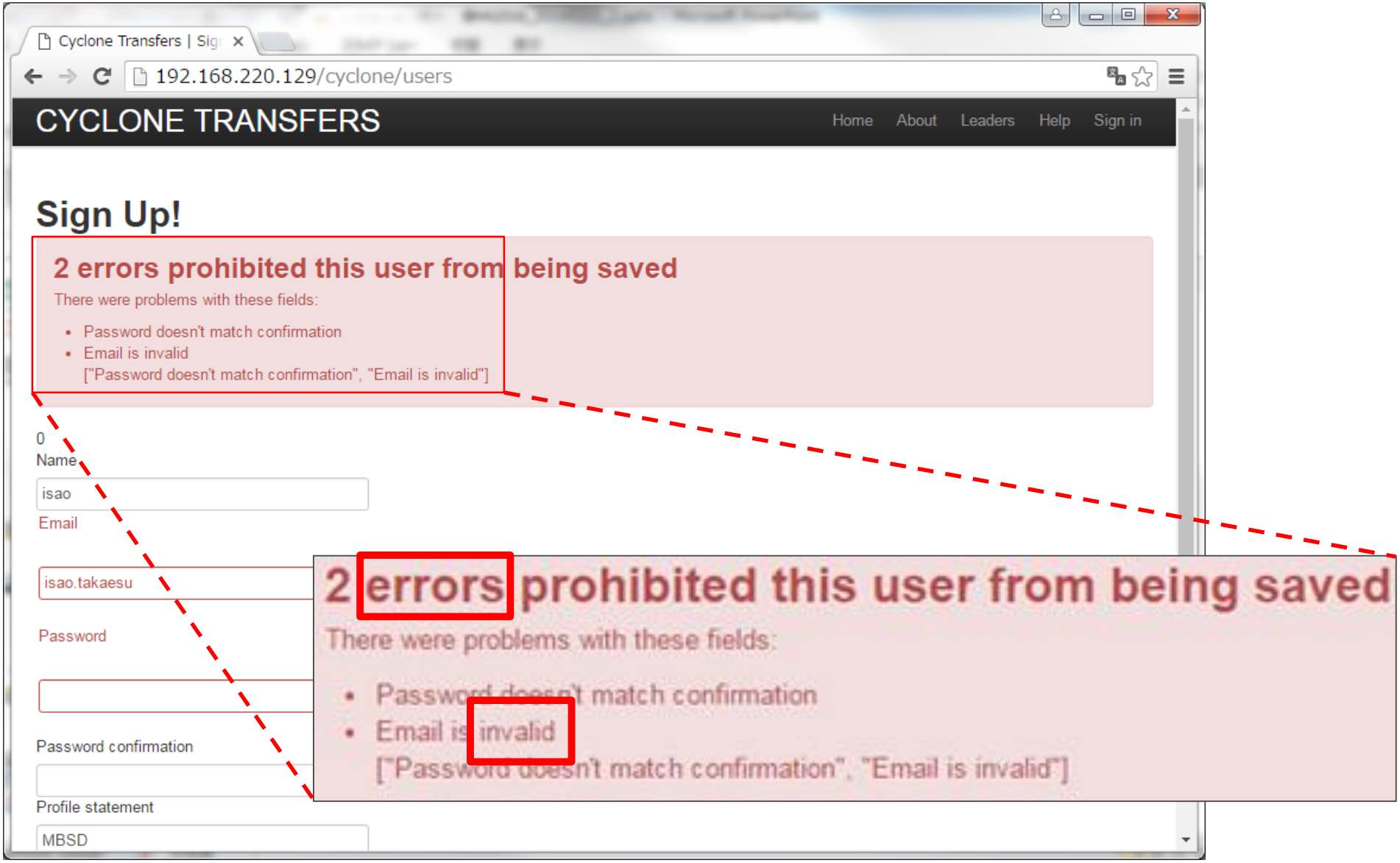


transition



POWERPOINT DESIGN

What has just happened?



SAIVS uses machine learning algorithms to “think”

Crawling requires the following **thinking patterns**:

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

What is **Naive Bayes**?

Naive Bayes is used for auto classification of texts

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

examples)

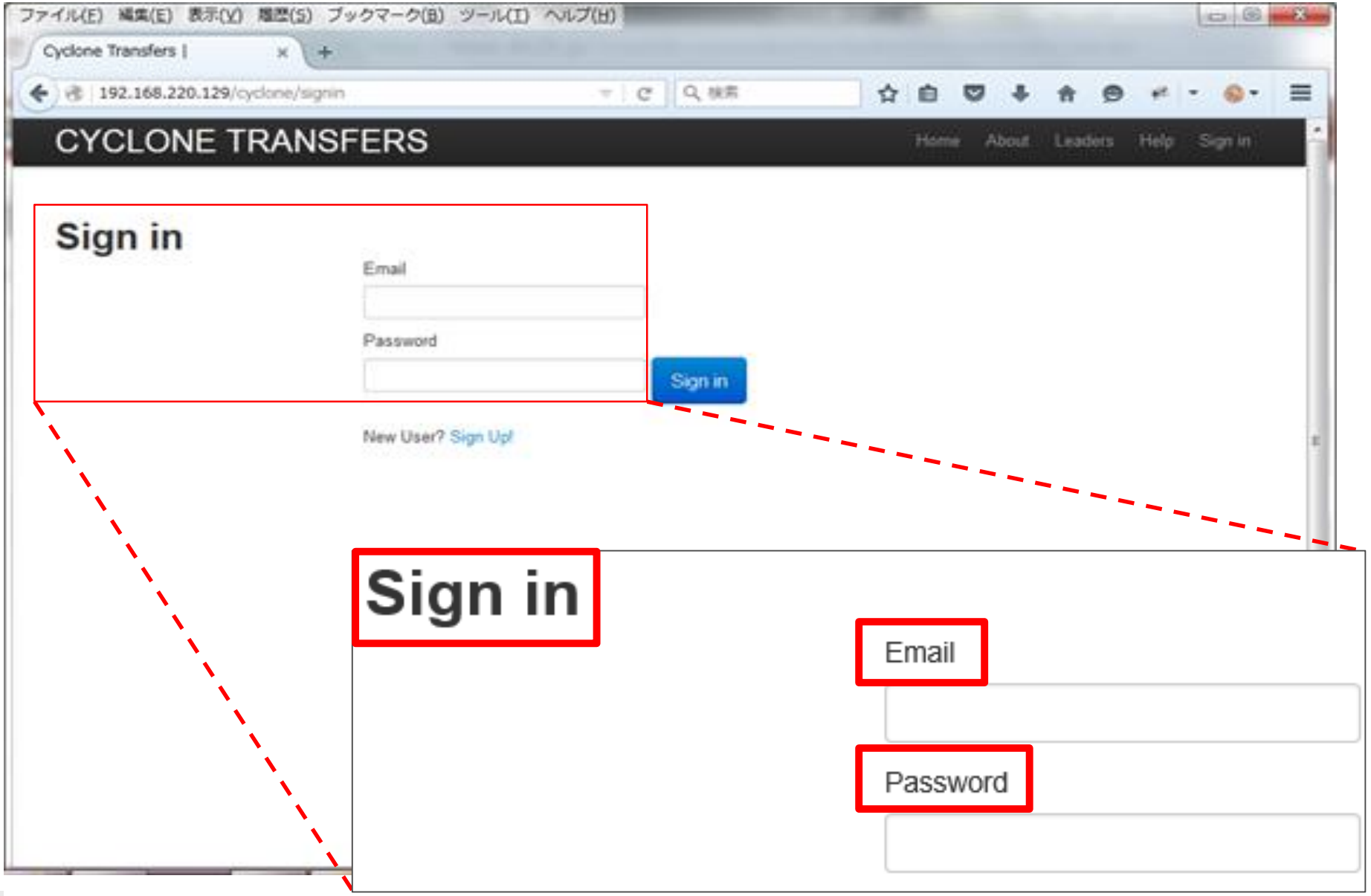
- ✓ Spam mail filter (Spam or Ham).
- ✓ Classify blog post genres (Sports or Politics or Music or Tech).

Page categories and classified texts for Naive Bayes

Category table used for **page classification**

Category(page types)	keywords used for classification
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



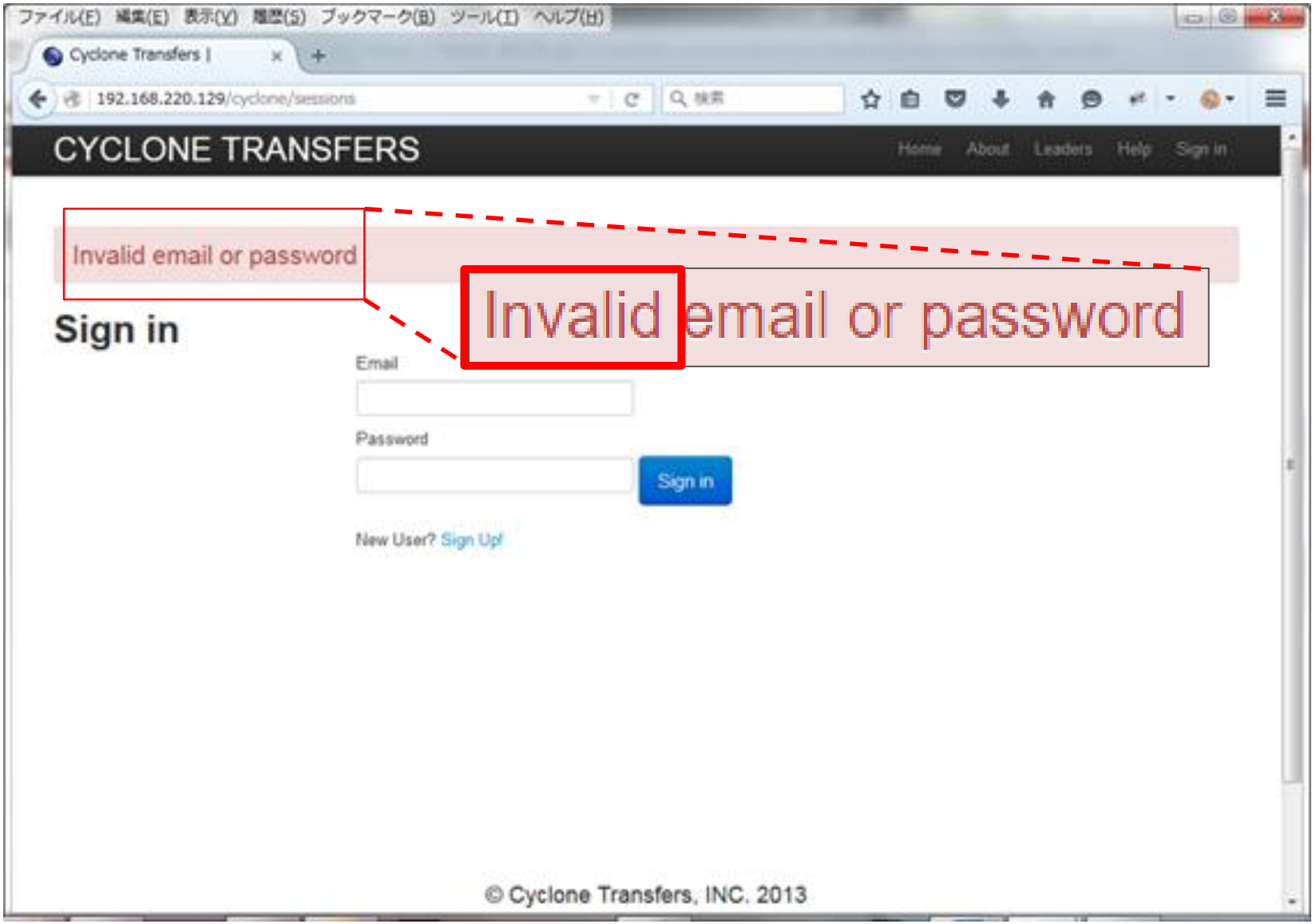
HTML source of “Sign in” page

```
<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

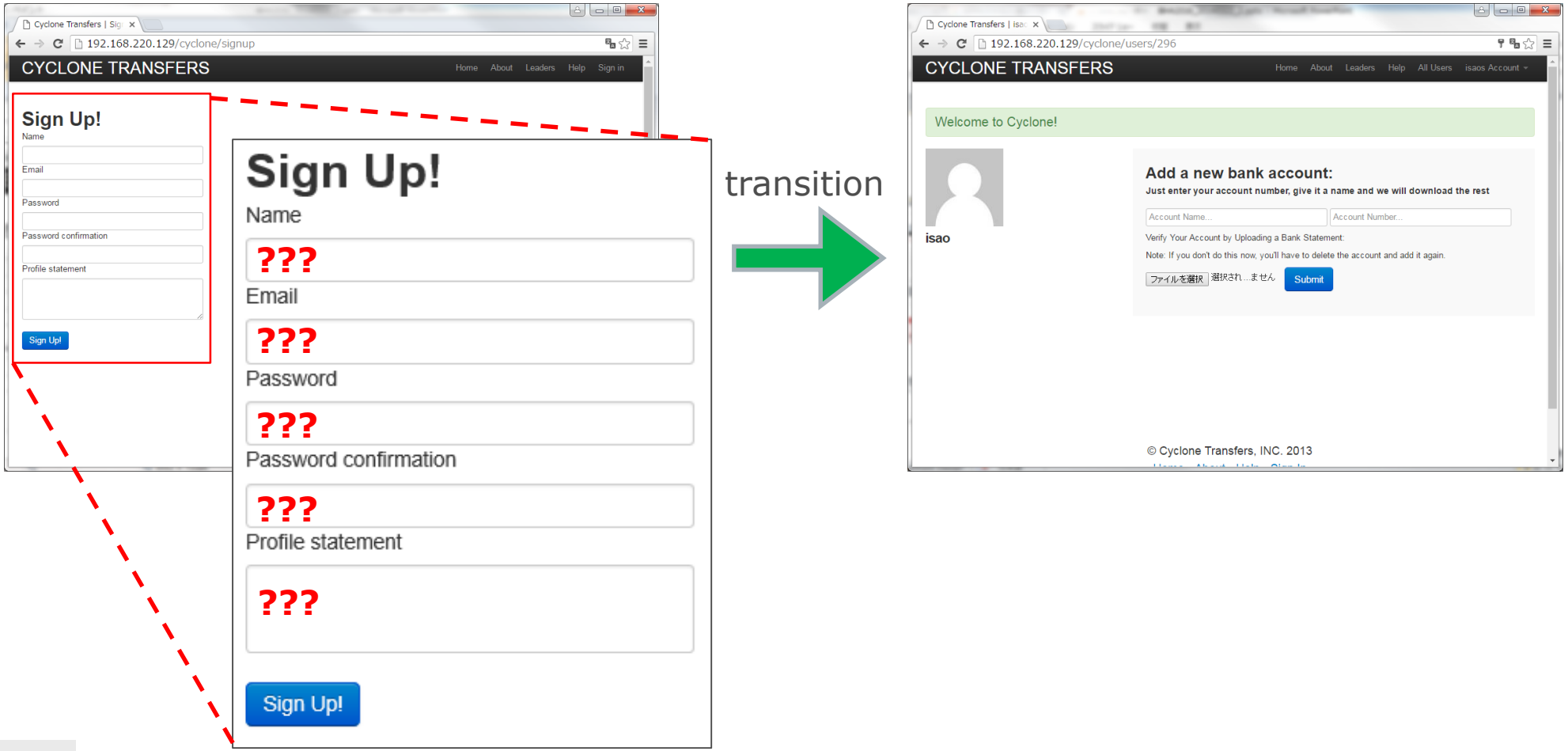
using the texts presented on the page.

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

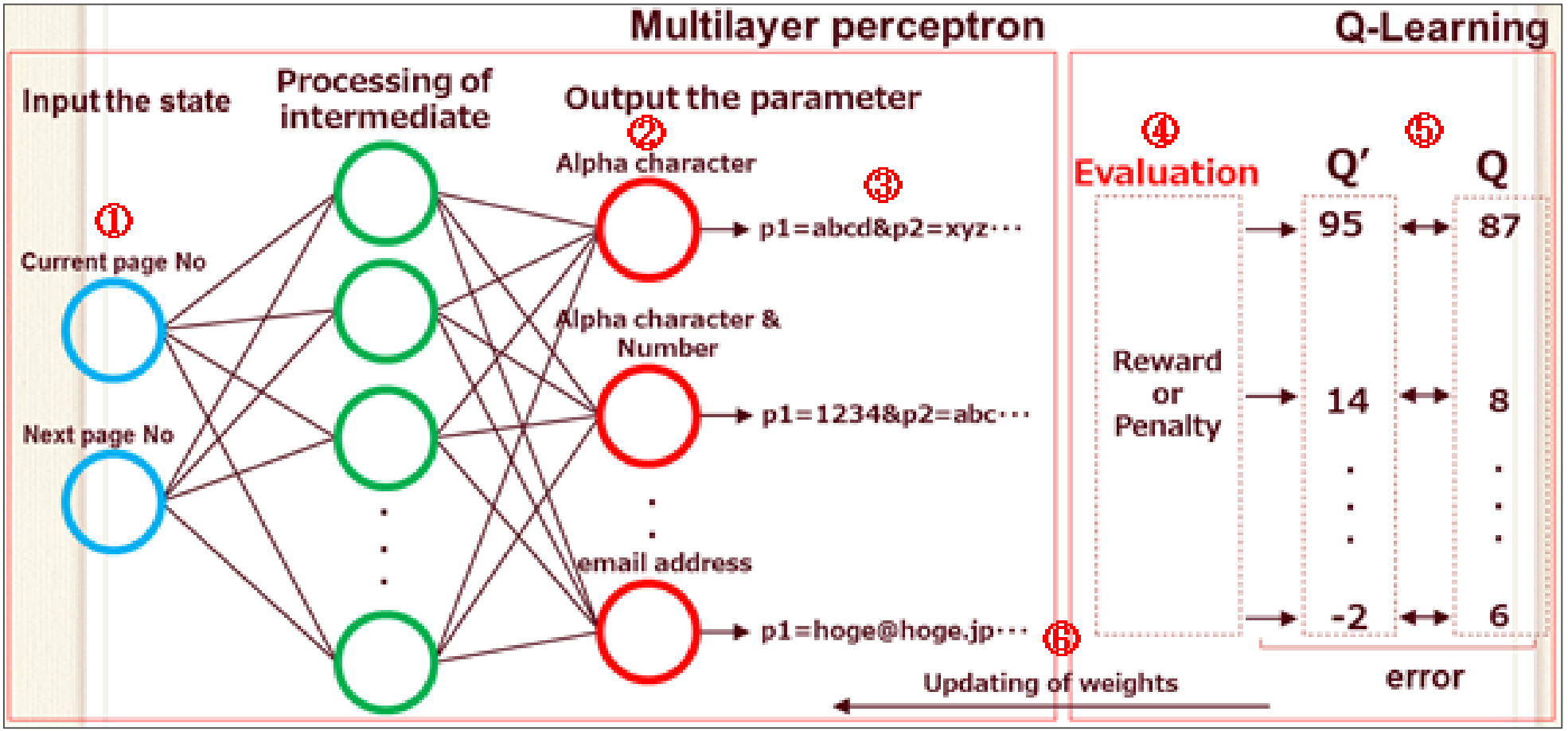
Category table for “success/failure” texts

Learning optimal values

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



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!?

Demonstration

https://www.mbsd.jp/blog/20160113_2.html

Who we are

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