SAIVS

Spider Artificial Intelligence Vulnerability Scanner

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?

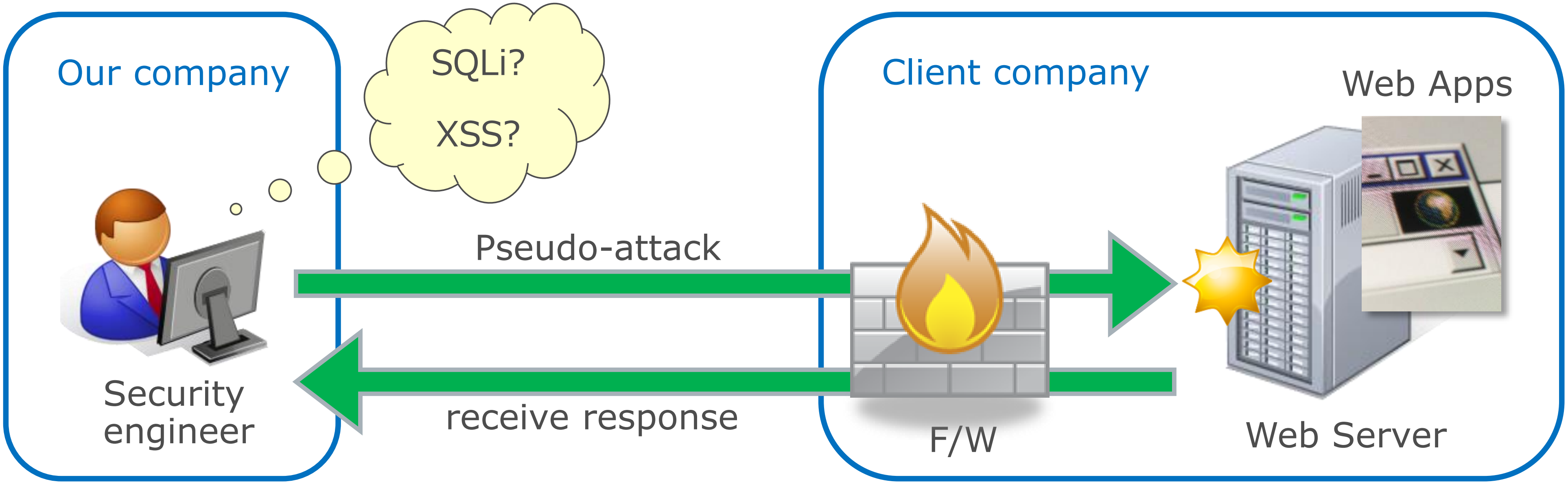
- ✓ SAIVS

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

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

What is vulnerability assessment?

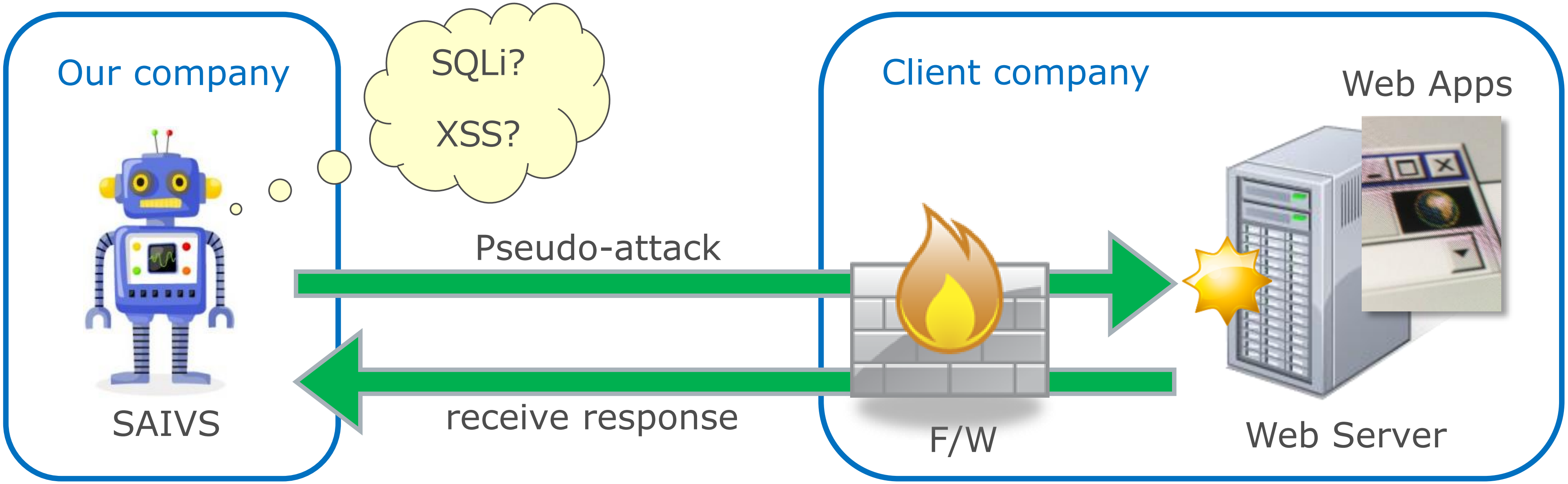
Web application vulnerability assessment by a security engineer



- ✓ 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.

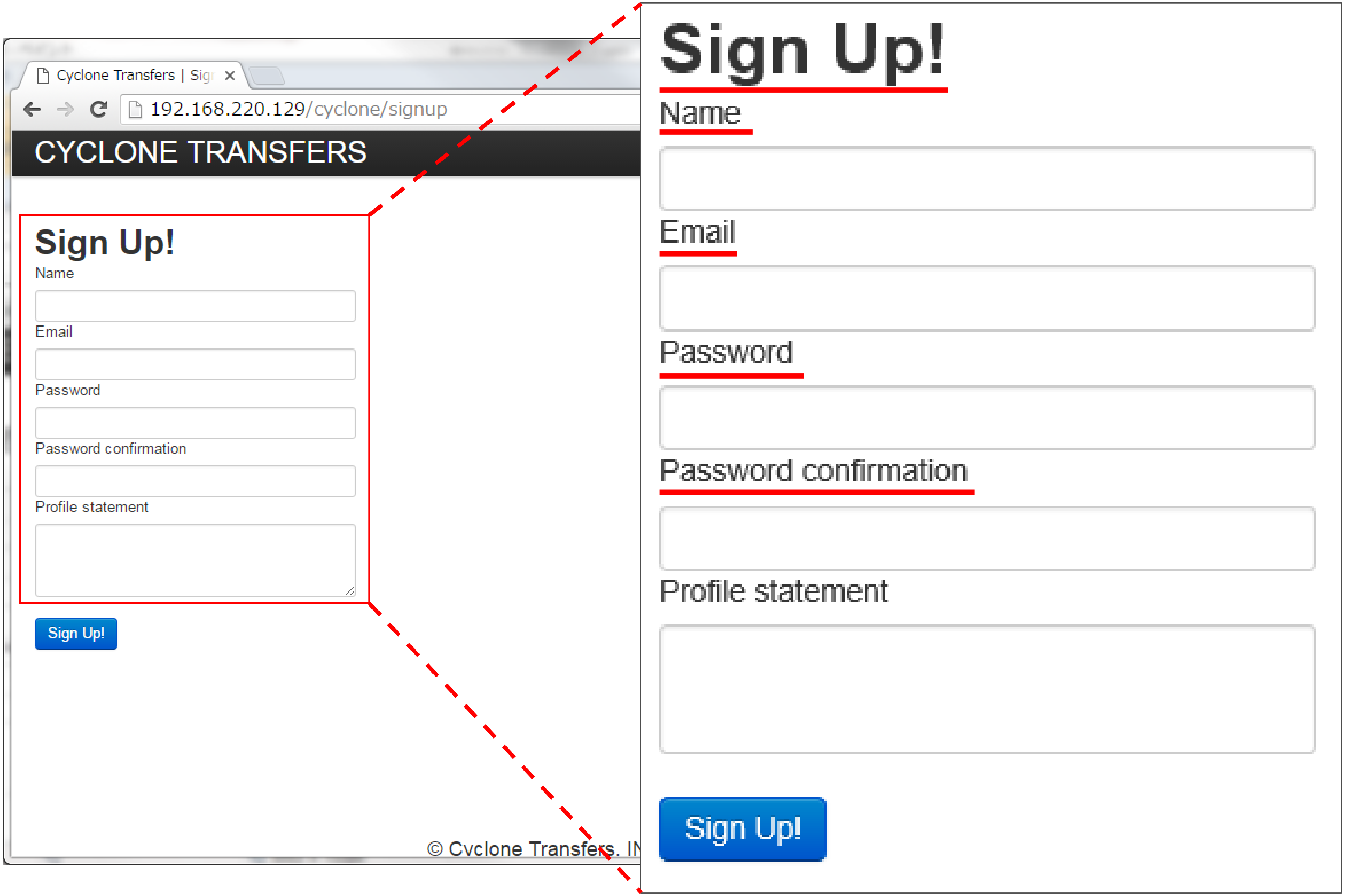
✓ Apply to actual security assessments and bug bounty programs.

Today’s point!!

SAIVS can **crawl** simple Web applications.

⇒using **machine learning** algorithms.

What is the type of this page?



Cyclone Transfers | Sig

192.168.220.129/cyclone/signup

CYCLONE TRANSFERS

Sign Up!

Name

Email

Password

Password confirmation

Profile statement

Sign Up!

© Cyclone Transfers, IN

Sign Up!

Name

Email

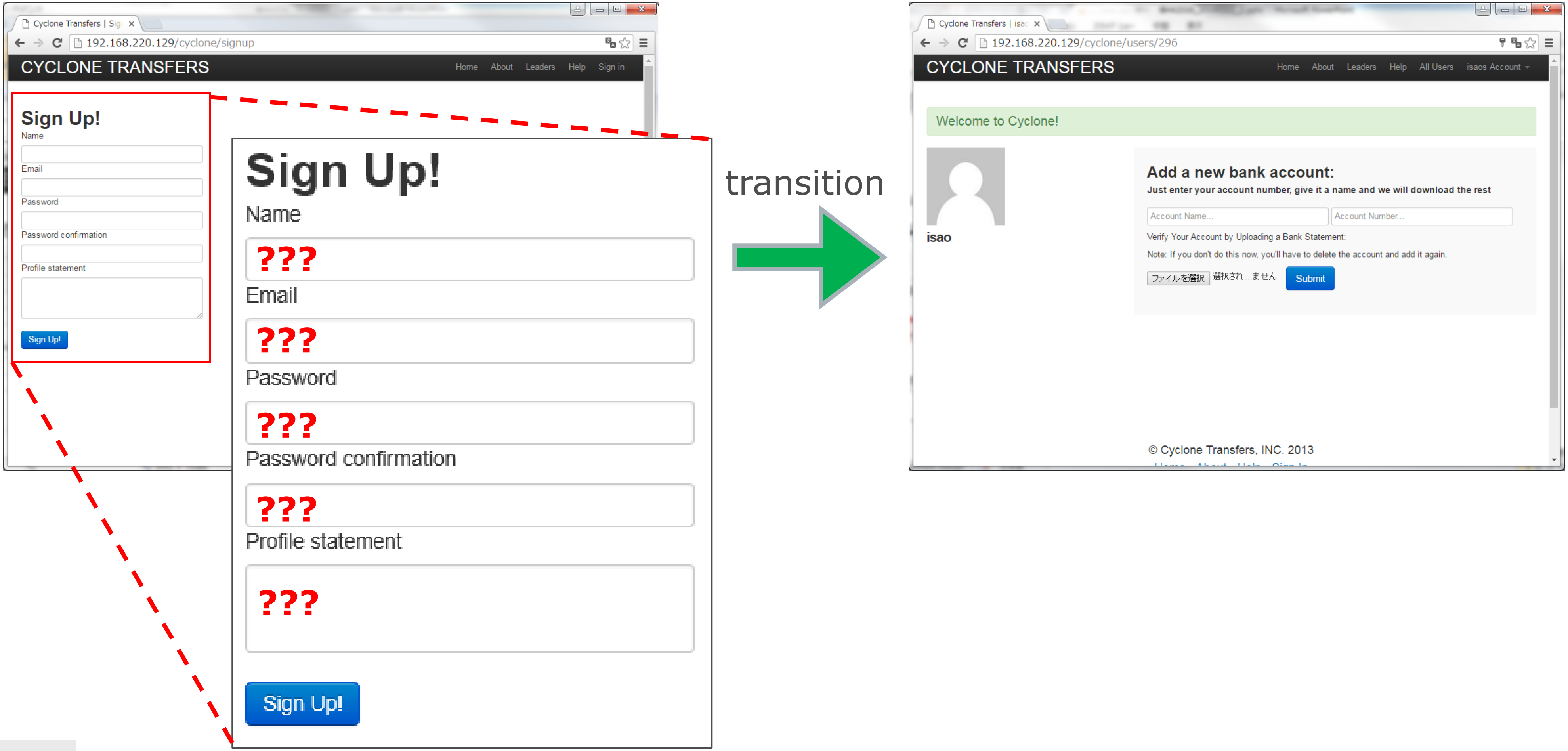
Password

Password confirmation

Profile statement

Sign Up!

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



Cyclone Transfers | Sig

192.168.220.129/cyclone/signup

CYCLONE TRANSFERS

Home About Leaders Help Sign in

Sign Up!

Name

Email

Password

Password confirmation

Profile statement

Sign Up!

Sign Up!

Name

???

Email

???

Password

???

Password confirmation

???

Profile statement

???

Sign Up!

transition

Cyclone Transfers | isa

192.168.220.129/cyclone/users/296

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...

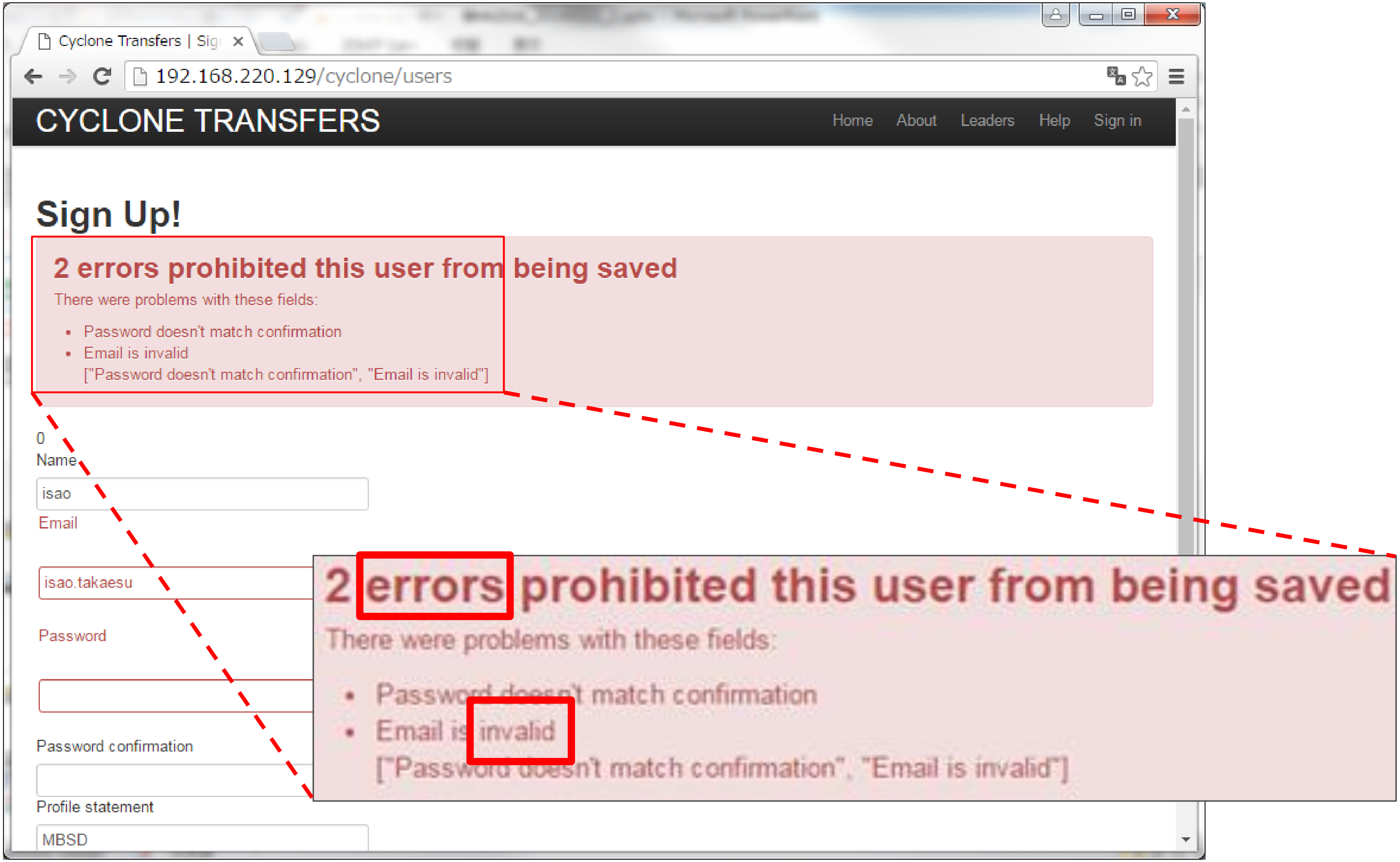
Verify Your Account by Uploading a Bank Statement:

Note: If you don't do this now, you'll have to delete the account and add it again.

ファイルを選択 選択され...ません Submit

© Cyclone Transfers, INC. 2013

What has just happened?



Cyclone Transfers | Sig

192.168.220.129/cyclone/users

Sign Up!

2 errors prohibited this user from being saved

There were problems with these fields:

- Password doesn't match confirmation
- Email is invalid
  ["Password doesn't match confirmation", "Email is invalid"]

0

Name

isao

Email

isao.takaesu

Password

Password confirmation

Profile statement

MBSD

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)

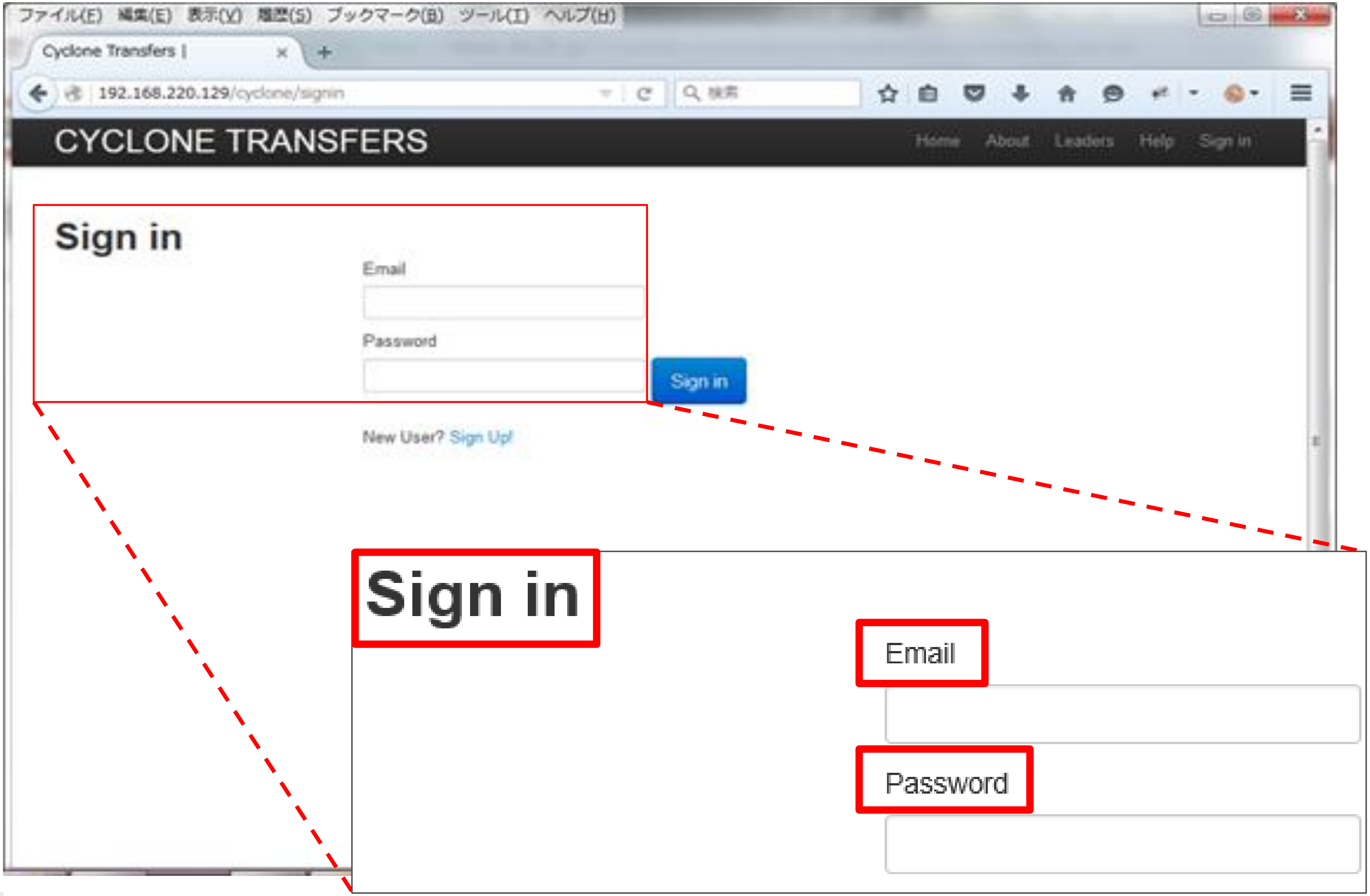
- ✓ Spam mail filter (Spam or Ham).
- ✓ Classify blog post genres (Sports or Politics or Music or Tech).

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



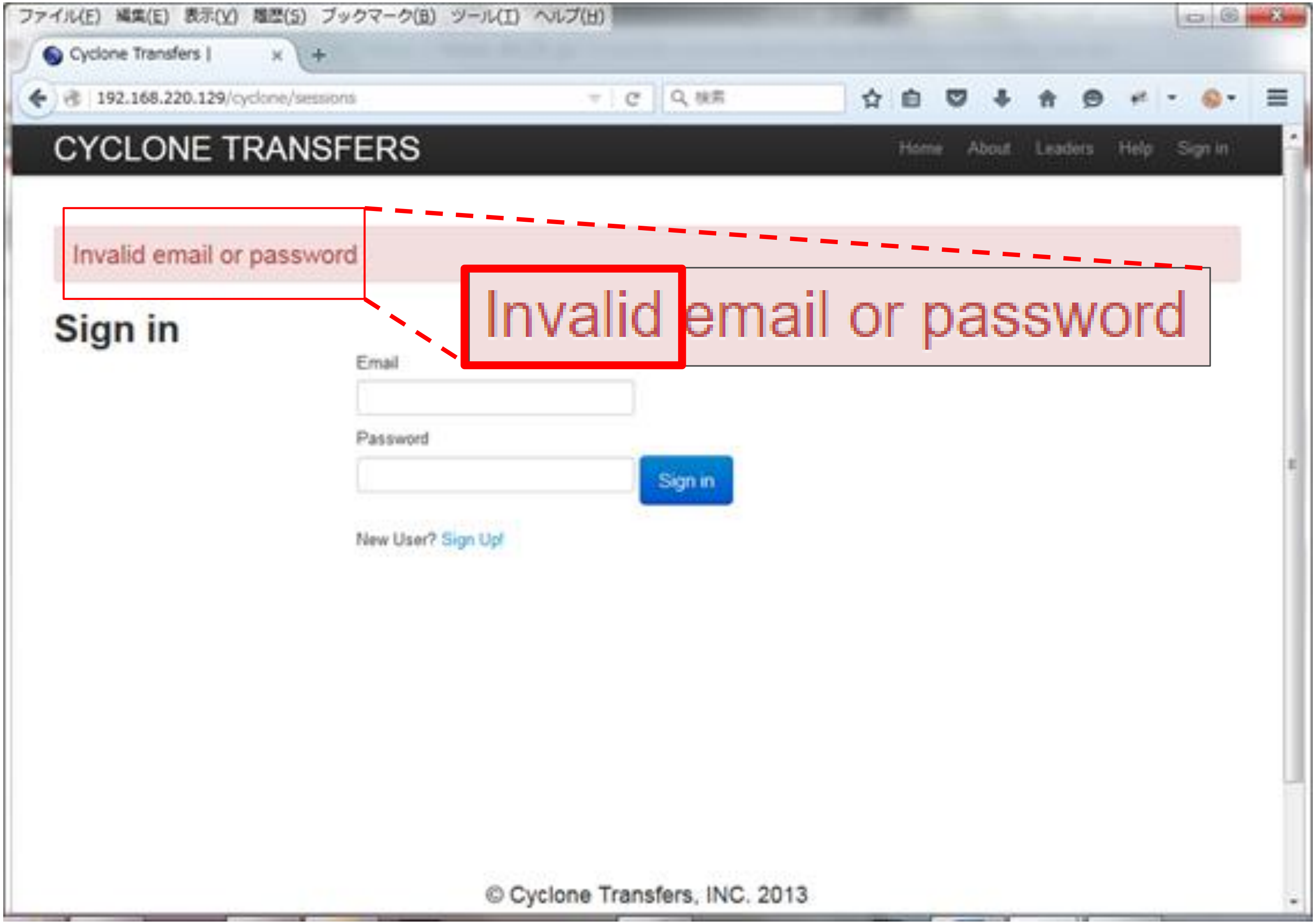
HTML source of “Sign in” page

```
<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



ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)
Cyclone Transfers |
192.168.220.129/cyclone/sessions
検索
CYCLONE TRANSFERS
Home
About
Leaders
Help
Sign in

Invalid email or password

Sign in

Email

Password

New User? Sign Up!

© Cyclone Transfers, INC. 2013

Invalid email or password

HTML source of a failed page transition

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

SAIVS will recognize the transition success/failure

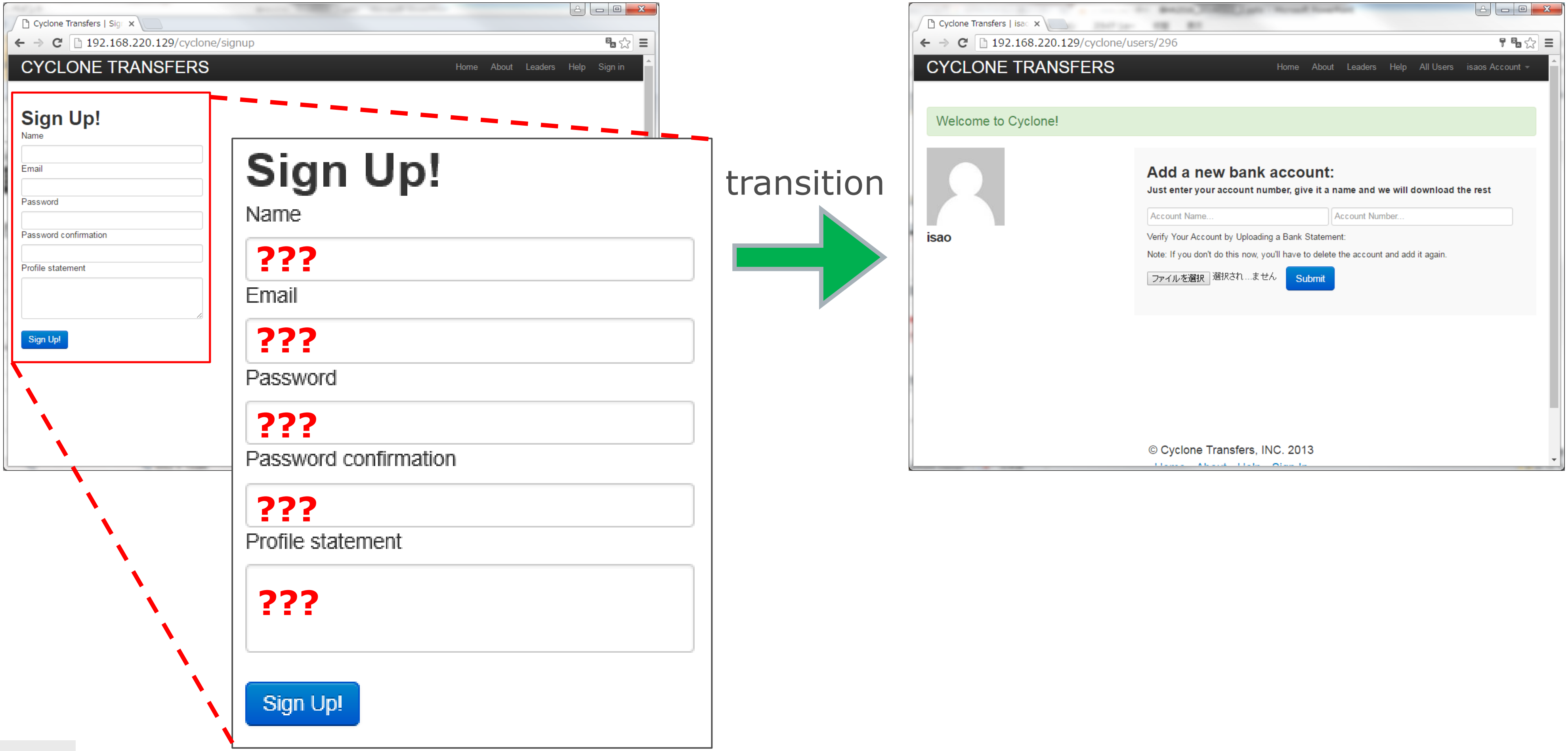
using the texts presented on the page.

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

???

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...

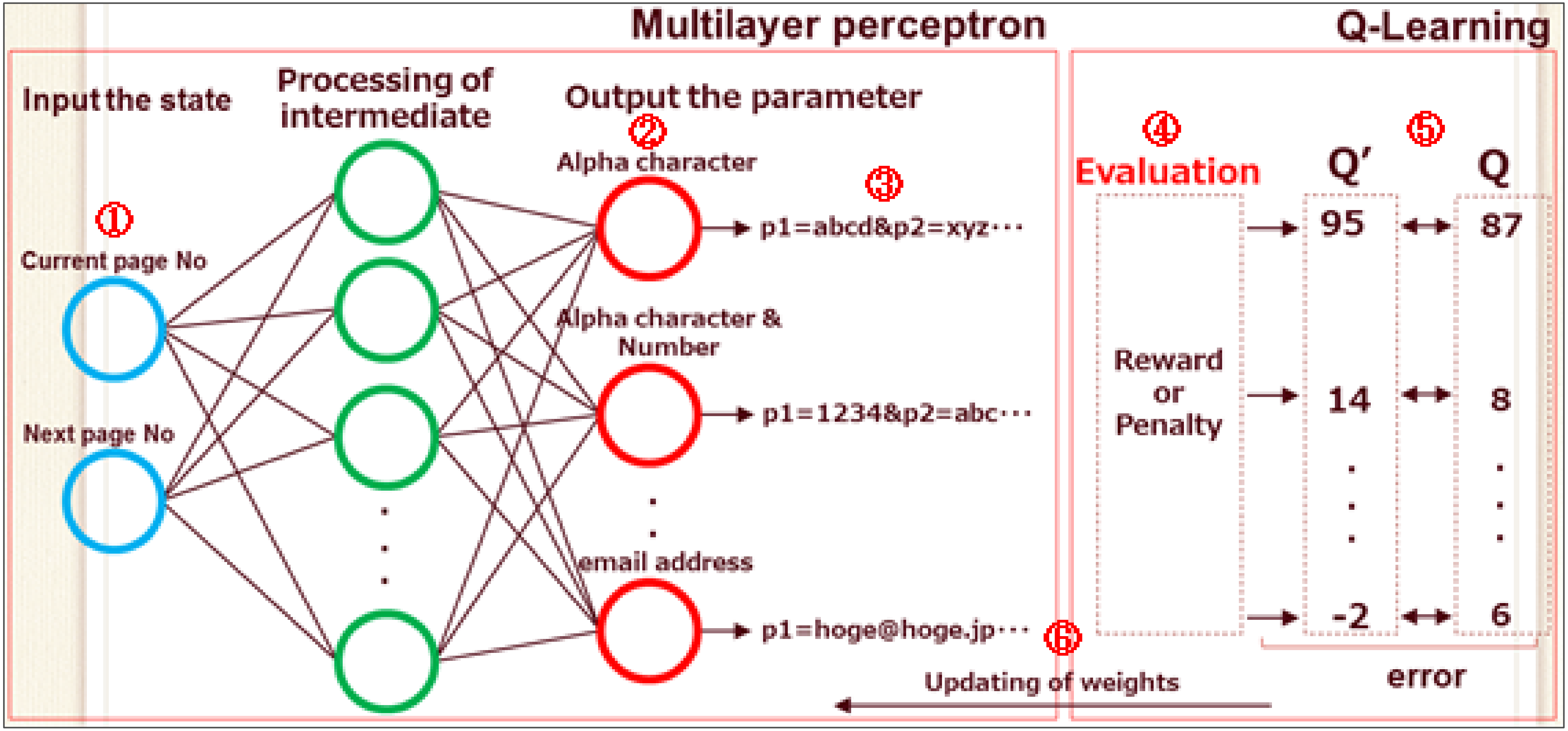
Verify Your Account by Uploading a Bank Statement:

Note: If you don't do this now, you'll have to delete the account and add it again.

ファイルを選択 選択され…ません

© Cyclone Transfers, INC. 2013

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