

Secure Coding Phase 4

Team 6

Shady Botros
Subburam Rajaram
Vasudhara Venkatesh

Team 7's App

Major Vulnerabilities

Vulnerability	Likelihood	Impact	Old?
Reflected XSS	medium	high	yes
CSRF	medium	high	yes

Testing Methodology & Tools

OWASP Checklist

Configuration and Deploy Management Testing

Identity Management Testing

Authentication Testing

Authorization Testing

Session Management Testing

Data Validation Testing

Error Handling

Cryptography

Business Logic Testing

Client Side Testing

Tools Used

ZAP

Vega

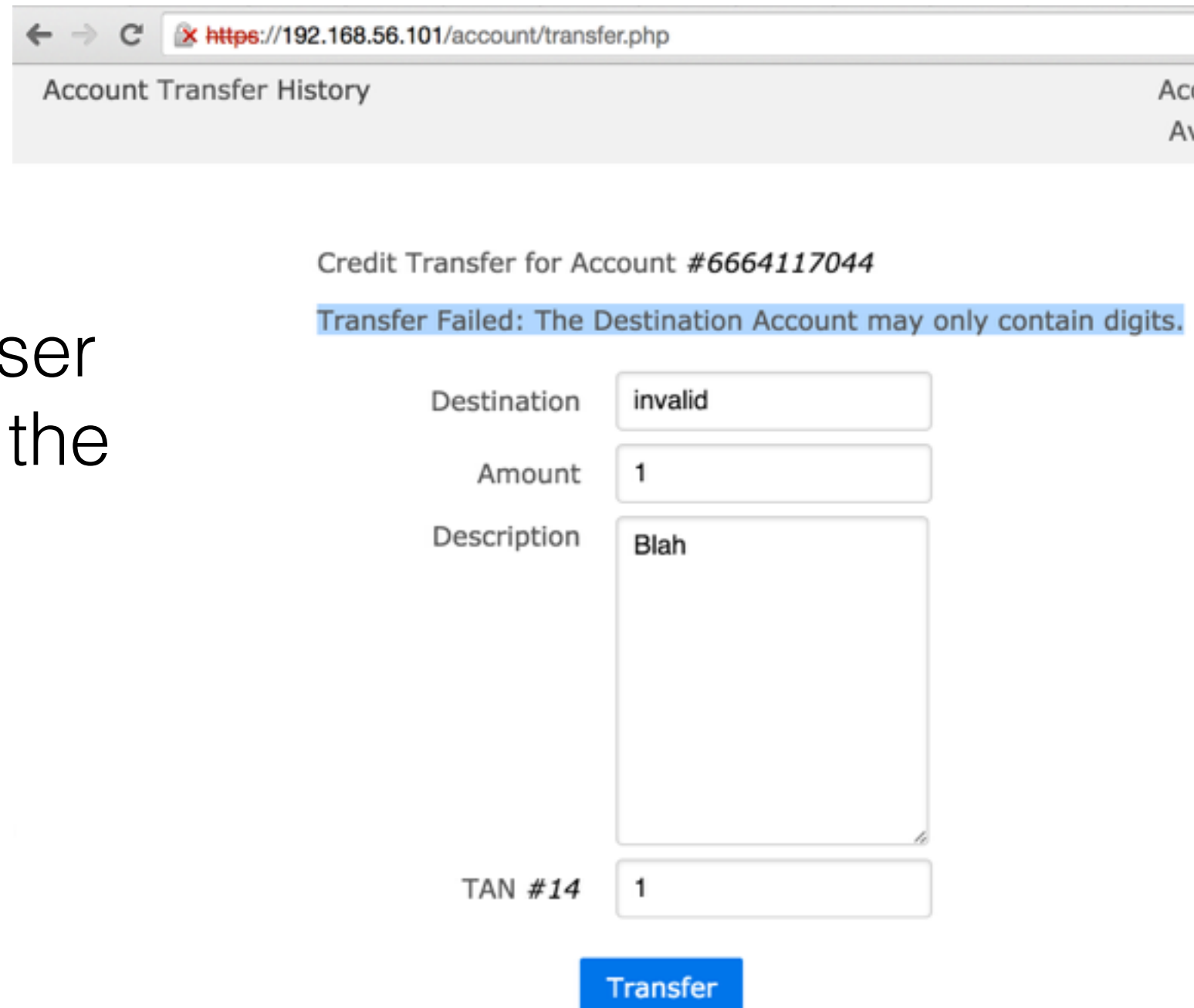
W3af

RIPS

Firefox Developer Tools

Reflected XSS

On transfer failure, user input is sent back to the browser unchecked.



The screenshot shows a web browser window with the address bar displaying `https://192.168.56.101/account/transfer.php`. The page title is "Account Transfer History". Below the title, there is a section for "Credit Transfer for Account #6664117044". A blue error message states: "Transfer Failed: The Destination Account may only contain digits." Below the error message, there is a form with the following fields:

- Destination:** A text input field containing the word "invalid".
- Amount:** A text input field containing the number "1".
- Description:** A large text area containing the word "Blah".
- TAN #14:** A text input field containing the number "1".

At the bottom of the form, there is a blue button labeled "Transfer".

```
<input id="destination" name="destination" type="text" placeholder="Account Number"
value="<?php if (isset($_POST['destination'])) echo $_POST['destination']; ?>" required>
```

CSRF

Anti-CSRF tokens remain the same before and after log-in

Before log-in

01/login.php

Account yet? *Click here* to register with us.

Email

Password

[Sign In](#)

Password?

After log-in

/192.168.56.101/account/index.php

History

Welcome, *tattioff42+user1@gmail.com*. Below is a list of your accounts.

You can *click* on any of your accounts to *select* it. The *active* account is **marked in the top right corner**.

You can also *create a new account* by clicking on the [Create new Account](#) button.

ark Sources Timeline Profiles Resources Audits Console

```

t">
block header">_</div>
">
countList">
:"post" action>
="hidden" name="CSRFToken" value="eb6b9051e8473e1cdb1961ff66155cf223a07ca5bcf064ef3d66fe0795ff8aff">
="hidden" name="accountNumber" value="6664117044">
="submit" name="selectAccount" class="pure-button pure-button-active" value="6664117044" style="width:

```

Timeline Profiles Resources Audits Console

```

>_</div>
class="pure-form pure-form-aligned">
e="CSRFToken" value="eb6b9051e8473e1cdb1961ff66155cf223a07ca5bcf064ef3d66fe0795ff8aff">
l-group">
il</label>

```

Demo

- Combine reflected XSS and CSRF to access sensitive information (e.g. account balance):
 1. Forged request makes an invalid transfer with an injected script in the “destination” field
 2. Transfer fails and injected script is reflected to victim’s browser
 3. Script runs and sends the account balance as a get-parameter to the attacker’s server
- Video

Thank you!