HUNT: Data Driven Web Hacking & Manual Testing

$(whoami)

- JP Villanueva @swagnetow
- Current:
  - Trust & Security @ Bugcrowd
- Past:
  - Security Researcher @ Bugcrowd
  - Solutions Architect @ WhiteHat Security
  - Application Security Engineer @ WhiteHat Security

Shoutouts

- Motley crew @bugcrowd
  - SecEng and SecOps teams
- Bug Hunters and Pentesters
- Portswigger Burp Suite
- OWASP ZAP
- Github contributors

The Problems

- Increasingly large and complicated web applications that need manual testing
- Applications assessment training lacks “tribal knowledge” of vulnerability location
- No in-tool workflow for web hacking methodologies

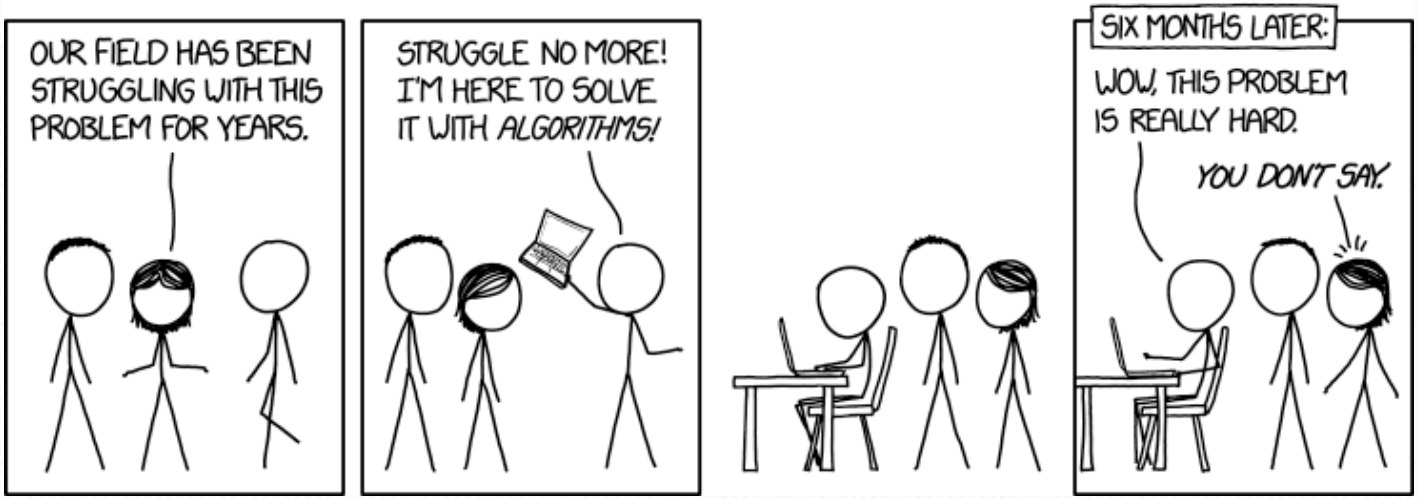
Current Solutions

- Hacker who can eyeball and effectively find security bugs
  - May or may not have a methodology
  - Definitely has accrued “tribal knowledge”
  - Bug hunts and/or does consultant work
- Dynamic Scanner
  - Limited test cases (fuzzing)
  - Cost prohibitive
  - Limited in detection cases (dynamic pages, errors, etc)
  - Complex sites are hard (auth)

Introducing HUNT

- Tribal knowledge passive alerts
- Methodology in Burp
- Manual testing references in Burp

HUNT Scanner



Source: xkcd

Bug Location (Tribal Knowledge)

- Data from over 600+ bug bounty programs
  - ~2 web targets per program on average
- www.bugcrowd.com, www2.bugcrowd.com
  - ~15 parameters per target on average

⇒ 600 * 2 * 15 ~= 18,000 parameters seen

Vulnerability Locations

- ⇒ 18,000 parameters
  - Anonymize the data
  - Reduce to params with vulns on them
  - Reduce to only Critical and High severity bugs/vulns
  - Sort by recurring instances
  - Include top 5-10 reoccurring instances per vuln/bug category
  - Review top 100 for possible permutations manually and/or with regex
  - Manually add ancillary data (pentest/fuzzdb/seclists/etc)

Alerts and Advisory

Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | Alerts | HUNT Scanner | HUNT Methodology

- HUNT Scanner
  - Debug & Logic Parameters (1)
  - File Inclusion & Path Traversal
  - Insecure Direct Object Reference (5)
  - OS Command Injection (1)
  - SQL Injection (12)
  - Server Side Request Forgery (7)
  - Server Side Template Injection (9)
    - activity
    - content
    - id (1)
    - name (6)
    - view (2)
    - redirect
    - template
    - view
  - Settings

Parameter	Host	Path	ID
ctl00$PlaceHolderMain$signInControl...	clientelesupport.trx.com	/_layouts/15/ClienteleCRM8.6.1/Pag...	409a9193
ctl00$PlaceHolderMain$signInControl...	clientelesupport.trx.com	/_layouts/15/ClienteleCRM8.6.1/Pag...	409a9193
j_username	correxemailportal.trx.com	/AdminPortal/j_spring_security_check	2b4450b4
j_agencyname	correxemailportal.trx.com	/AdminPortal/j_spring_security_check	2b4450b4
firstName	correximplementations-dev.trx.com	/correxui/welcome/userSignUp	508ef189
lastName	correximplementations-dev.trx.com	/correxui/welcome/userSignUp	508ef189

Advisory | Request | Response

Location: https://correxemailportal.trx.com/AdminPortal/j_spring_security_check

HUNT located the **j_username** parameter inside of your application traffic. The **j_username** parameter is most often susceptible to Server Side Template Injection. HUNT recommends further manual analysis of the parameter in question.

Source: Twitter

Bug Location by Bug/Vuln Class

Source: Shirtoid.com

SQL Injection

{regex + perm} id	{regex} select	{regex} report	{regex} role
{regex} update	{regex} query	{regex + perm} user	{regex + perm} name
{regex} sort	{regex} where	{regex + perm} search	{regex} params
{regex} process	{regex + perm} row	{regex + perm} view	{regex} table
{regex + perm} from	{regex + perm} sel	{regex} results	{regex} sleep
{regex} fetch	{regex + perm} order	{regex} keyword	{regex} count
{regex + perm} column	{regex} input	{regex + perm} key	
{regex + perm} code	{regex + perm} field	{regex} delete	{*type*} Custom headers
{regex} string	{regex} number	{regex + perm} filter	{*type*} JSON and XML services

File Includes/Directory Indexing

{regex + perm} file	{regex} location	{regex} locale	{regex + perm} path
{regex} display	{regex} load	{regex + perm} read	{regex} retrieve
{regex + perm} folder	{regex} style	{regex + perm} doc	{regex} document
{regex} root	{regex} pdf	{regex} pg	{regex} include
{regex} list	{regex} view	{regex} img	{regex} image

Server Side Request Forgery 🔥🔥🔥

{regex + perm} dest	{regex} redirect	{regex + perm} uri	{regex} path
{regex} continue	{regex + perm} url	{regex} window	{regex} next
{regex} data	{regex} reference	{regex + perm} site	{regex} html
{regex + perm} val	{regex} validate	{regex} domain	{regex} callback
{regex} return	{regex + perm} page	{regex} feed	{regex} host
{regex} port			

OS Command Injection

{regex} daemon	{regex + perm} upload	{regex + perm} dir
{regex} execute	{regex + perm} download	{regex + perm} log
{*type*} .cgi	{regex} ip	
{regex} cli		

Insecure Direct Object Reference

{regex + perm} id	{regex + perm} user	
{regex + perm} account	{regex + perm} number	
{regex + perm} order	{regex + perm} no	
{regex + perm} doc	{regex + perm} key	
{regex + perm} email	{regex + perm} group	
{regex + perm} profile	{regex + perm} edit	REST numeric paths

Server Side Template Injection 🔥

{regex + perm} template	content	id
preview	redirect	view
activity	name	

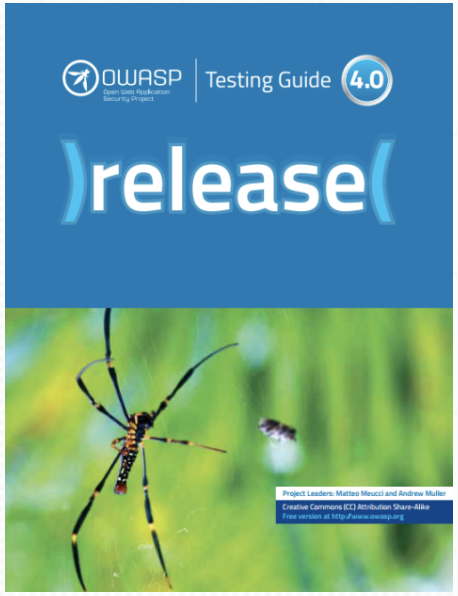
Debug & Logic Parameters

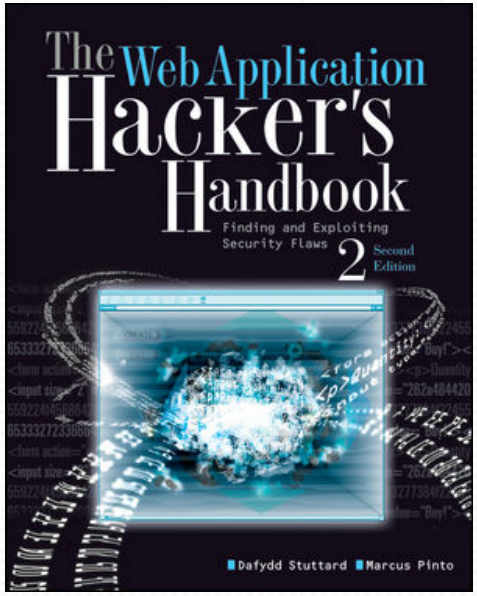
access	admin	dbg
debug	edit	grant
test	alter	clone
create	delete	disable
enable	exec	execute
load	make	modify
rename	reset	shell
toggle	adm	root
cfg	config	

HUNT Methodology

Source: Capcom

Methodologies





HIPAA

PCI

Right Click -> Send-To Methodology Section

Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | Alerts | HUNT Scanner | HUNT Methodology

Intercept | HTTP history | WebSockets history | Options

Filter: Hiding out of scope items; hiding CSS and image content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comme
313	https://www.concur.com	GET	/sites/default/files/js/js_gE5rgnx...			200	29592	script	js		
314	https://www.concur.com	GET	/sites/default/files/js/js_YDk2Yq...			200	6278	script	js		
315	http://www.trx.com	GET	/robots.txt			301	438	HTML	txt	301 Moved Permanently	
316	http://amexco.trx.com	GET	/robots.txt					text	txt		
317	http://atl104.trx.com	GET	/robots.txt					text	txt		
318	http://atl110.trx.com	GET	/robots.txt					text	txt		
319	https://www.concur.com	GET	/sites/all/modules/custom_conc	✓		200	2395	script	js		
320	https://www.concur.co						4710	script	js		
321	https://www.concur.co						913	XML	svg		
325	http://autodiscover.trx							text	txt		
326	http://cft.trx.com							text	txt		
327	http://correx.trx.com							text	txt		

Request | Response

Raw | Params | Headers | H

```
GET /sites/all/modules
Host: www.concur.com
User-Agent: Mozilla/5.
Accept: */*
Accept-Language: en-US
Accept-Encoding: gzip,
Referer: https://www.c
Connection: close
```

epage.js?oyt71g HTTP/1.1

- https://www.concur.com/sites...pts/header_homepage.js?oyt71g
- Remove from scope
- Spider from here
- Do an active scan
- Do a passive scan
- Send to Intruder ⌘+^+I
- Send to Repeater ⌘+^+R
- Send to Sequencer
- Send to Comparer (request)
- Send to Comparer (response)
- Show response in browser
- Request in browser ▶
- Send to HUNT Methodology ▶
  - Account ▶
    - Insecure Direct Object Reference
    - Cross Site Request Forgery
    - Authentication Bypass - Vertical
    - Cross Site Scripting
    - SQL Injection
    - Authentication Bypass - Horizontal
  - Account Registration ▶
  - File Download/Upload ▶
  - Account Recovery ▶
  - Money Transactions ▶
  - Authentication ▶
  - Search ▶
  - Contact Us ▶
  - General ▶
  - API ▶
- Engagement tools ▶
- Show new history window
- Add comment
- Highlight ▶
- Delete item
- Clear history
- Copy URL
- Copy as curl command
- Copy links
- Save item
- Proxy history help

Description

Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | Alerts | HUNT Scanner | HUNT Methodology

- HUNT – Methodology
  - Functionality
    - API
    - Account
      - Authentication Bypass – Horizontal
      - Authentication Bypass – Vertical
      - Cross Site Request Forgery
      - Cross Site Scripting
      - Insecure Direct Object Reference
      - SQL Injection
    - Account Recovery
    - Account Registration
    - Authentication
    - Contact Us
    - File Download/Upload
    - General
    - Money Transactions
    - Search
  - Settings

Description | Bugs | Resources | Notes

Check to see if any kind of checks can be bypassed in any way to perform actions that require higher level permissions.

Multiple Request/Response

Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | Alerts | HUNT Scanner | HUNT Methodology

- HUNT - Methodology
  - Functionality
    - API
    - Account
      - Authentication Bypass - Horizontal
      - Authentication Bypass - Vertical
      - Cross Site Request Forgery
      - Cross Site Scripting
      - Insecure Direct Object Reference
      - SQL Injection
    - Account Recovery
    - Account Registration
    - Authentication
    - Contact Us
    - File Download/Upload
    - General
    - Money Transactions
    - Search
  - Settings

Description | Bugs | Resources | Notes

0 x | 1 x | 2 x | 3 x

Request | Response

```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 03 Nov 2017 16:41:29 GMT
Content-Type: text/html;charset=ISO-8859-1
Connection: close
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Vary: Accept-Encoding
Content-Length: 76365



<!--[if lt IE 7]> <html class="lt-ie9 lt-ie8 lt-ie7" lang="en"> <![endif]-->
<!--[if IE 7]> <html class="lt-ie9 lt-ie8" lang="en"> <![endif]-->
<!--[if IE 8]> <html class="lt-ie9" lang="en"> <![endif]-->
<!--[if IE 9]> <html class="lt-ie9" lang="en"> <![endif]-->
<html>
<head>
<title>TRX CORREX Mail Portal</title>
<style>
.errorblock {
        color: #ff0000;
        background-color: #ffEEEE;
        border: 3px solid #ff0000;
        padding: 8px;
        margin: 16px;
}

.login-help {
```

Notes

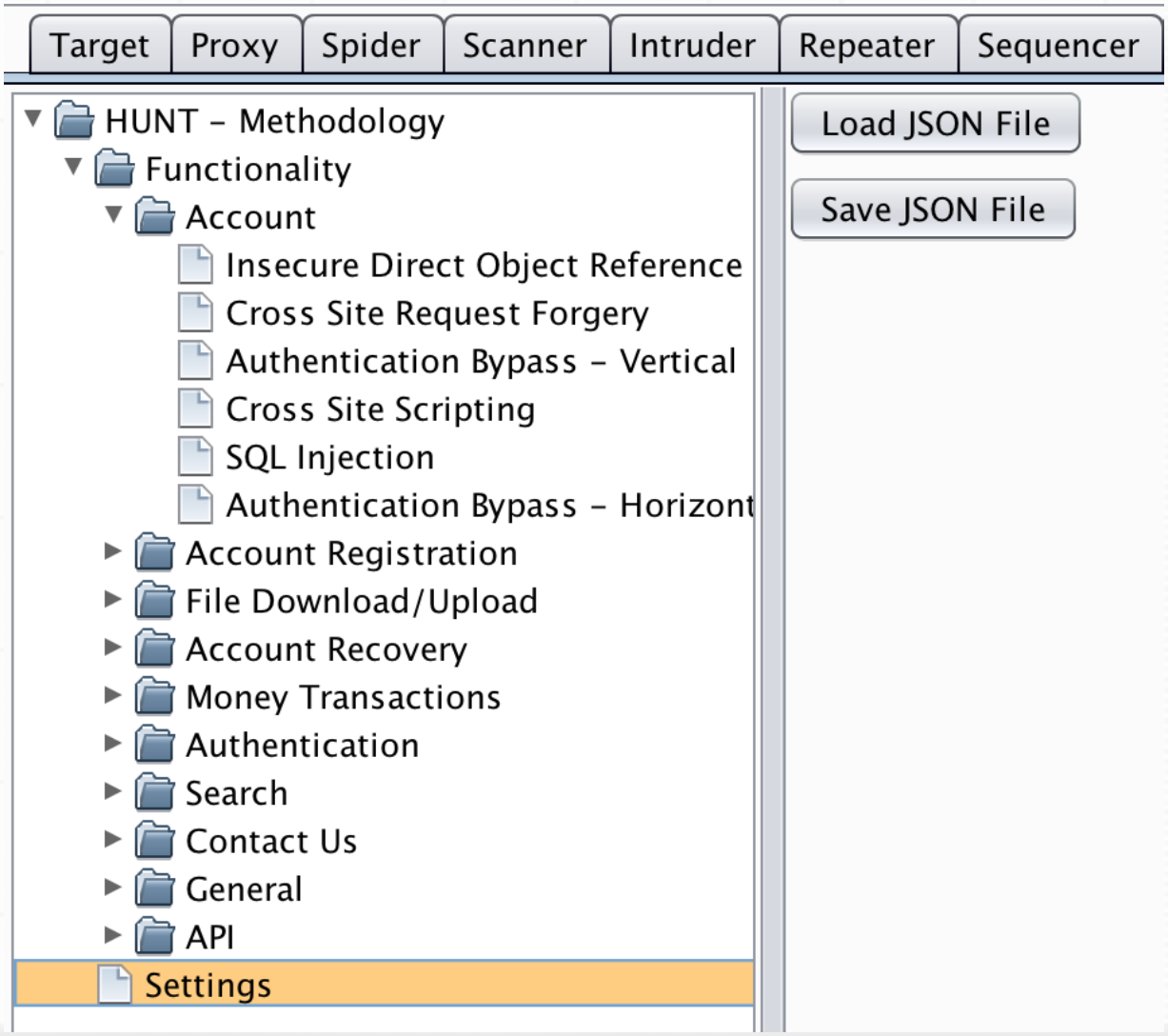
Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender

- HUNT – Methodology
  - Functionality
    - Account
      - Insecure Direct Object Reference
      - Cross Site Request Forgery
      - Authentication Bypass – Vertical
      - Cross Site Scripting
      - SQL Injection
      - Authentication Bypass – Horizont
    - Account Registration
    - File Download/Upload
    - Account Recovery
    - Money Transactions
    - Authentication
    - Search
    - Contact Us
    - General
    - API
  - Settings

Description | Bugs | Resources | Notes

- Try and pop the SQLi on your own, you n00b
- If all else fails, try SQLmap
- Get help from Jason because he's an uber l33t h4x0r

Save/Load JSON File



Resources

Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options

- HUNT - Methodology
  - Functionality
    - Account
      - Insecure Direct Object Reference
      - Cross Site Request Forgery
      - Authentication Bypass - Vertical
      - Cross Site Scripting
      - SQL Injection
      - Authentication Bypass - Horizont
    - Account Registration
    - File Download/Upload
    - Account Recovery
    - Money Transactions
    - Authentication
    - Search
    - Contact Us
    - General
    - API
  - Settings

Description | Bugs | Resources | Notes

http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
http://pentestmonkey.net/cheat-sheet/sql-injection/oracle-sql-injection-cheat-sheet

Plugin Installation

Source: github

Installation - Jython

Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender

Extensions | BApp Store | APIs | Options

Settings

This setting controls how Burp handles extensions on startup.

☑ Automatically reload extensions on startup

Java Environment

These settings let you configure the environment for executing extensions that are written in Java. If

Folder for loading library JAR files (optional):

Select folder ...

Python Environment

These settings let you configure the environment for executing extensions that are written in Python Java.

Location of Jython standalone JAR file:

/Users/jpvillanueva/Downloads/jython-standalone-2.7.0.jar

Select file ...

Folder for loading modules (optional):

Select folder ...

Installation - Plugin

Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | Alerts | HUNT Scanner | HUNT Metho

Extensions | BApp Store | APIs | Options

Burp Extensions

Extensions let you customize Burp's behavior using your own or third-party code.

Add | Remove | Up | Down

Loaded	Type	Name
☑	Python	
☑	Python	

Details | Output | Errors

☑ Extension loaded

Name: HUNT Methodology

Item
Extension type
Filename
Method
Extension state listeners
Context menu providers
Suite tabs

Load Burp Extension

Please enter the details of the extension, and how you would like to handle standard output and error.

Extension Details

Extension type:

Extension file (.py

Standard Outp

Output to sy

Save to file:

Show in UI

Standard Erro

Output to sy

Save to file:

Show in UI

Look In: Burp

conf
hunt_methodology.py
hunt_scanner.py

File Name:

Files of Type: All Files

Open | Cancel

Cancel | Next

Setting Target Scope

Site map | Scope

Target Scope

Define the in-scope targets for your current work. This configuration affects the behavior of tools throughout the suite. The ea
in the site map to include or exclude URL paths.

☑ Use advanced scope control

Include in scope

Add
Edit
Remove
Paste URL
Load ...

Enabled	Protocol	Host / IP range	Port	File
☑	Any	contgo.com		
☑	Any	trx.com		
☑	Any	tripit.com		
☑	Any	concur		

Exclude from scope

Add
Edit
Remove
Paste URL
Load ...

Enabled	Protocol	Host / IP range	Port	File
☑	Any			logout
☑	Any			logoff
☑	Any			exit
☑	Any			signout

Setting Passive Scanner Scope

Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder

Issue activity | Scan queue | Live scanning | Issue definitions | Options

Live Active Scanning

Automatically scan the following targets as you browse. Active scan checks

- ○ Don't scan
- ◉ Use suite scope [defined in Target tab]
- ○ Use custom scope

Live Passive Scanning

Automatically scan the following targets as you browse. Passive scan checks

- ○ Don't scan
- ○ Scan everything
- ◉ Use suite scope [defined in Target tab]
- ○ Use custom scope

Run Passive Scanner

Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Co

Site map | Scope

Filter: Hiding out of scope and not found items; hiding CSS, image and general binary

- http://api.dev.tripit.com
- https://api.dev.tripit.com
- http://api.machupicchu.tripit.com
- http://api.mobile-dev.tripit.com
- http://api.staging.tripit.com
- https://api.staging.tripit.com
- http://api.stonehenge.tripit.com
- http://api.tripit.com
- https://api.tripit.com
- https://assets.concur.com
- http://assets.dev.tripit.com
- https://assets.dev.tripit.con
- https://assets.machupicchu
- http://assets.mobile-dev.tri
- http://assets.staging.tripit.
- https://assets.staging.tripit
- http://assets.tripit.com
- https://assets.tripit.com
- http://bcdportal.tripit.com
- https://bcdportal.tripit.com
- http://blog.tripit.com
- http://business.dev.tripit.co
- https://business.dev.tripit.c
- http://business.staging.trip
- https://business.staging.tri
- http://careers.tripit.com
- https://careers.tripit.com
- http://clientelesupport.trx.c
- https://clientelesupport.trx.
- https://concur.demdex.net

Contents

Host	Met
https://assets.machu...	GET
http://images.tripit.c...	GET
http://reporting.trx.c...	GET
https://www.concur....	GET
https://www.dev.tripi...	GET
machup...	GET
mobile-...	GET
taging....	GET
tonehe...	GET
ripit.com	GET
.machu...	GET

sponse

s | Headers

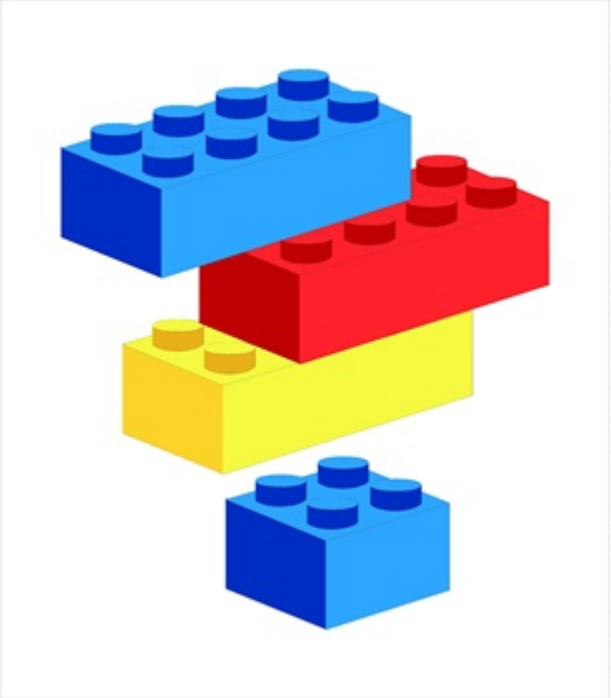
1.1
s.machupic
Mozilla/5
:56.0) Gec

application
.8
guage: en-L
ding: gzip

149 items selected

- Add to scope
- Remove from scope
- Spider selected items
- Actively scan selected items
- Passively scan selected items
- Send to HUNT Methodology ▶
- Engagement tools ▶
- Compare site maps
- Expand branch
- Collapse branch
- Delete selected items
- Copy selected URLs
- Copy links in selected items
- Save selected items
- Issues ▶
- View ▶
- Show new site map window
- Site map help

Extensibility



Source: logic-canvas.com

Scanner Extensibility

Creating new issue checks are as simple as adding to the JSON file.

```
{
  "issues": {
    "OS Command Injection": {
      "check_location": {
        "request": true,
        "response": false
      },
      "detail": "HUNT located the <b>$param$</b> parameter
inside of your application traffic. The <b>$param$</b>
parameter is most often susceptible to OS Command Injection.
HUNT recommends further manual analysis of the parameter in
question.<br><br>For OS Command Injection HUNT recommends the
following resources to aid in manual testing:",
      "level": "Information",
      "name": "Possible OS Command Injection",
      "params": [
        "daemon",
        "upload",
        "dir",
        "execute",
        "download",
        “vulnerable_parameter”
      ]
    }
}
```

Methodology Extensibility

Creating new methodologies are as simple as adding to the JSON file.

```
{
  "checklist": {
    "Settings": "",
    "Functionality": {
      "NEW METHODOLOGY SECTION": {
        "description": "",
        "tests": {
          "Authentication Bypass - Vertical": {
            "description": "Check to see if the login sequence
can be bypassed in any way to get higher level permissions.",
            "resources": [],
            "bugs": [],
            "notes": ""
          }
        }
      }
    }
  }
}
```

The Future

- More built-in methodologies
  - OWASP, PCI, HIPAA, CREST, PTES
- ~~Port to ZAP?~~
- More scanner checks/vulnerability classes
- More resources
- Dynamic JSON structure support
- Perfect GUI (lol, yeah right)
- REST Support
- ~~Full Burp helpers (right click, search, highlight, etc)~~
- Resource/File name analysis (Instead of params)
- Alerts on content types (XML, JSON, Multipart-form)
- Response analysis alerts (errors)
- Submit from Burp/ZAP to Bugcrowd program
- Get on BApp Store

Questions?

https://www.github.com/bugcrowd/hunt
@swagnetow