

Bug bounty Hunting Workshop

DEFCON

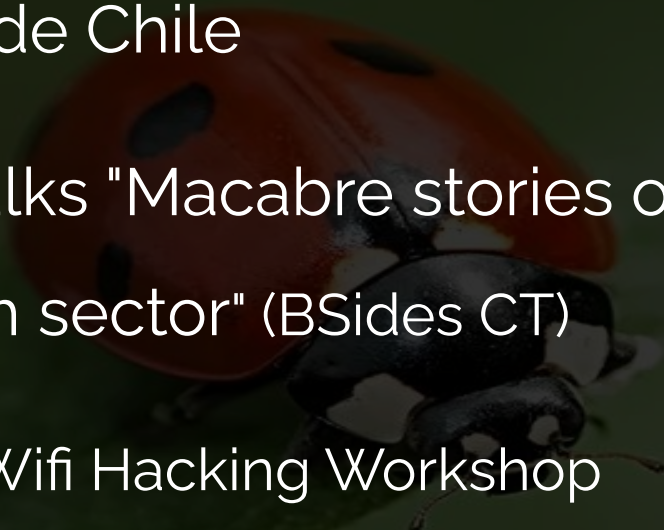
>Philippe Delteil  @philippedelteil

CS Universidad de Chile

Defcon 26 Skytalks "Macabre stories of a hacker in the public health sector" (BSides CT)

Defcon 27/China Wifi Hacking Workshop

Bug Bounty Hunter



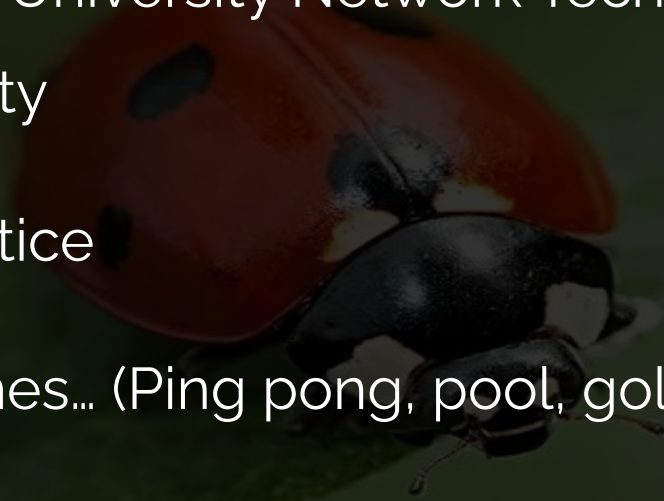
> David Patten

M.S. East Carolina University Network Technology &
Information Security

Locksmith Apprentice

Avid player of games... (Ping pong, pool, golf)

Proud Dad



> Question Where are you from?

Go here!

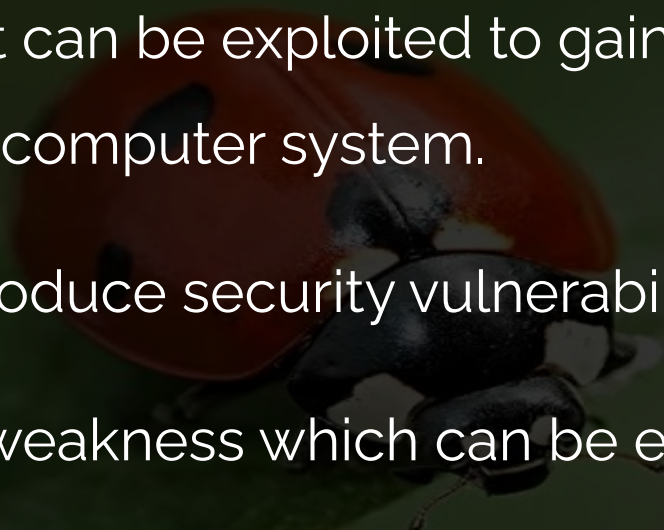


> What is a bug?

Software bug that can be exploited to gain unauthorized access or privileges on a computer system.

Security bugs introduce security vulnerabilities

Vulnerability is a weakness which can be exploited by a threat actor



> What is bug bounty hunting?

Finding bugs in

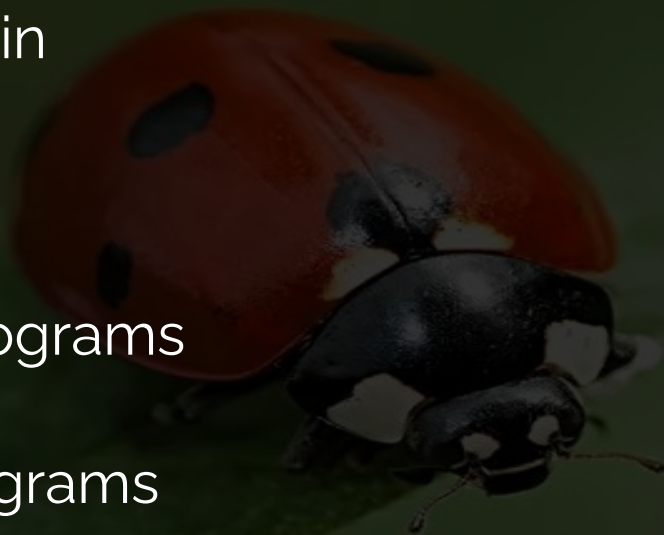
Internet

Private programs

Public programs

BBH sites

No programs



> How did I start?

J. Haddix Recon Methodology ([Video](#))

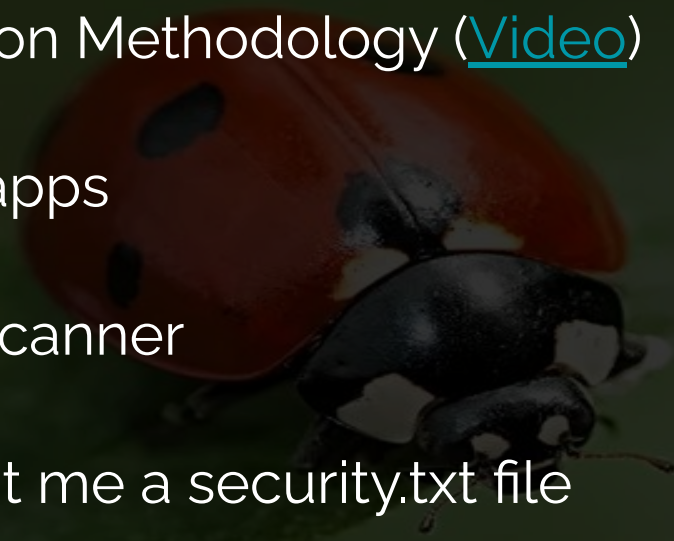
Tried tons of apps

Tried Nuclei scanner

Someone sent me a security.txt file

Tested 3 results from Nuclei

US\$5,550




> My first \$\$ bounties

By accident

Didn't know what I was doing

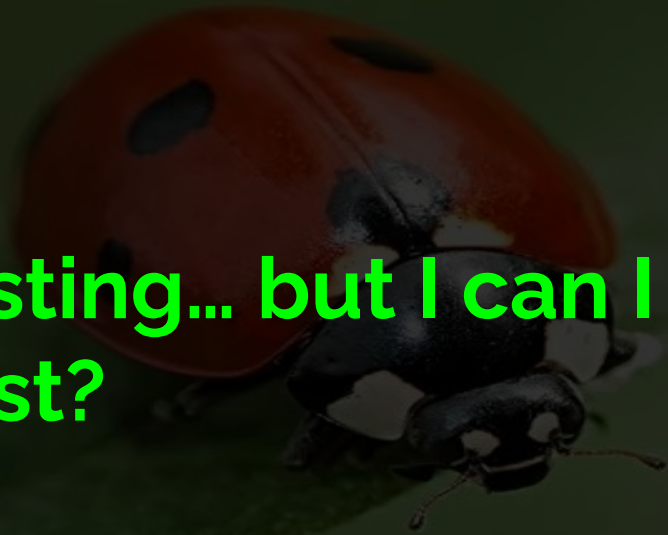
Take over of a Google Cloud bucket

All clients IDs and financial info

A close-up photograph of a ladybug on a green leaf. The ladybug is dark brown with several black spots on its back. It is positioned in the center-right of the frame, facing towards the right. The leaf is a vibrant green and shows some texture. The background is slightly blurred, showing more of the leaf and some dark green areas.

```
(2020-09-01) RS K - Session doesn't expire after log  
(2020-08-29) Deleite - Clickjacking vulnerability  
(2020-08-28) Deleite - Google bucket enumeration  
(2020-08-27) Deleite - Subdomain takeover  
(2020-08-17) Yehor Malin - Email enumeration on 10
```


> Very interesting... but I can I become a BBH
billionaire fast?



> Programs

Scope (*.domains.tld)

You can still report bugs out of scope

test.domain.com

staging.domain.com *.domain.com

Bounty (swag, points (p1 or p2), services, pay)

Safe Harbor + Exclusions

> Where to find programs?

Public

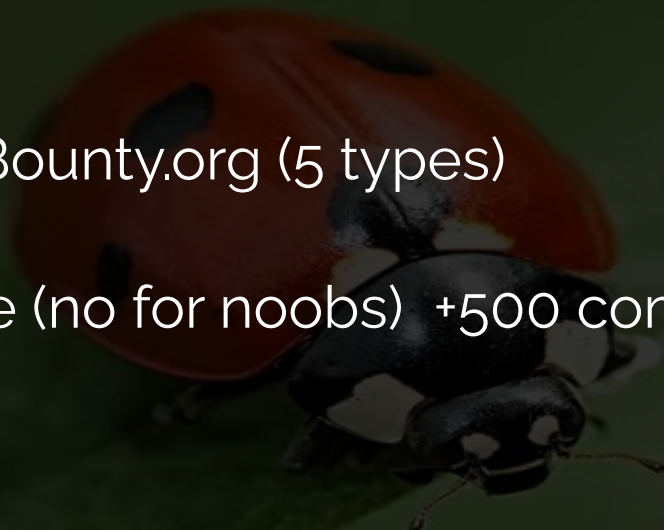
OpenBugBounty.org (5 types)

HackerOne (no for noobs) +500 companies

BugCrowd

Intigrity (OK) (duplicated clap you, points)

Others



> Where to find programs?

Private (invitation required, ask sending an email)

HackerOne

BugCrowd

Intigriti

Company A -> report@company.com -> Invitation h1



> Where to find programs?

Self Hosted

HackerOne

BugCrowd

Security files

Google dork

Not a program but OK, there's a bug



> Give me some tips, fast!

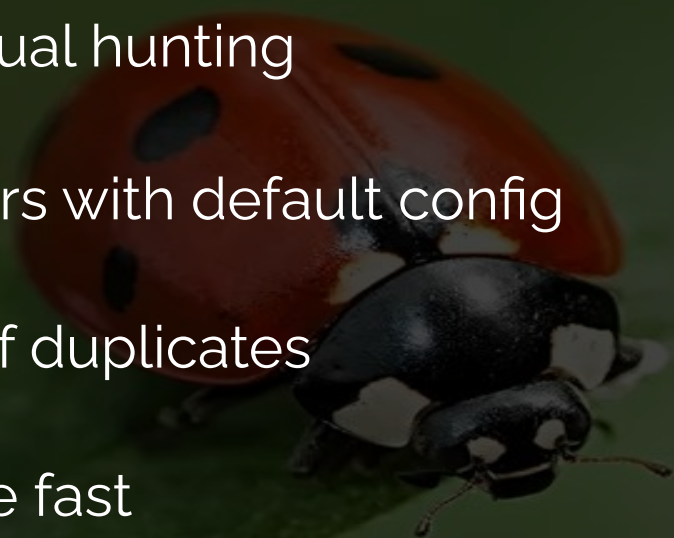
Automated vs Manual hunting

Automatic scanners with default config

High chance of duplicates

You need to be fast

Have automated steps (notification, report)



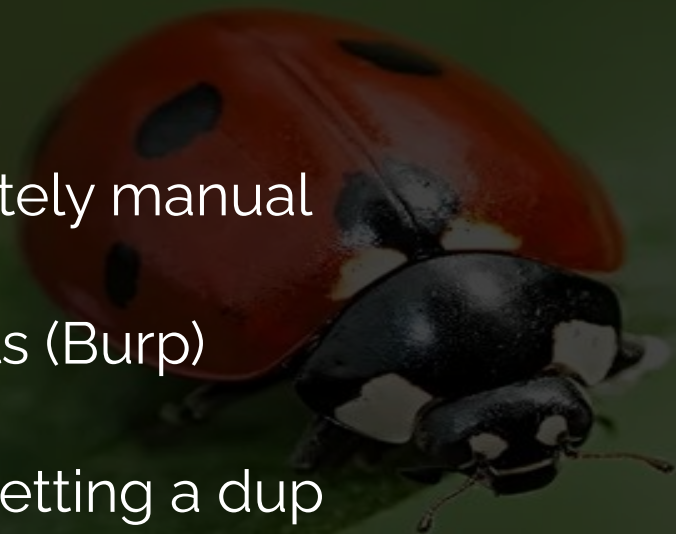
> Give me some tips, fast

Manual hunting

Not really completely manual

Supported by tools (Burp)

Less chances of getting a dup



> Give me some tips, fast

Steps?

1. Recon
 - a. Find (sub)domains
 - b. Find urls
 - c. Find IPs
2. Automated tools (many)
3. Manual hunting
 - a. Browser + Burp



> My favorite tools?

Subdomain finder



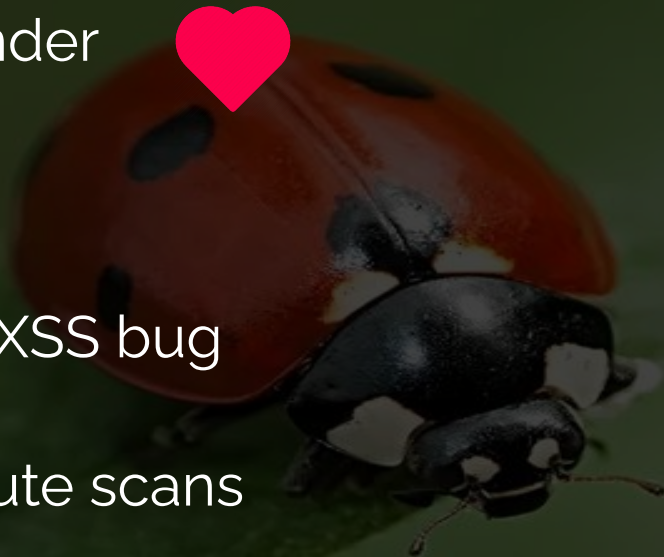
Nuclei

Dalfox finds XSS bug

Axiom distribute scans

BBRF Storing programs, urls, domains, ip , services

Burp Suite (Pro)



> Skill set?

Linux ^ Linux

Bash, Python and Go

Patience

Persistence

Passion

[Time]



> BBRF

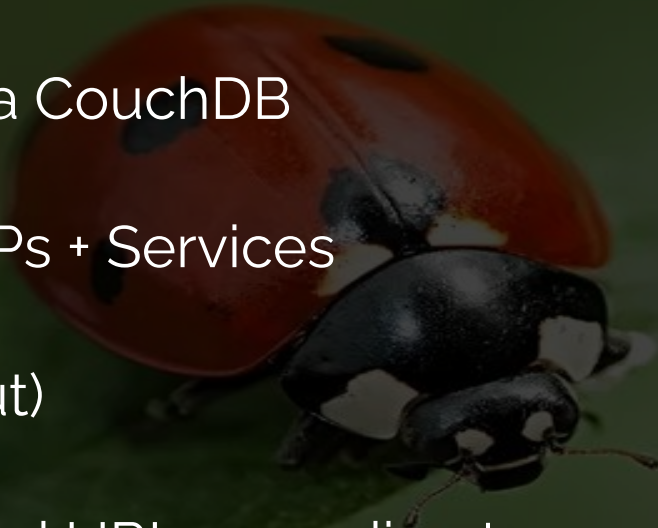
Store BBH data on a CouchDB

Domains + URLs + IPs + Services

Define scope (in/out)

Add subdomains and URL according to scopes

Pipe them everywhere



> BBRF

Commands

Live

<https://bugcrowd.com/dell>



> Exercise 1 (15 minutes)

Adding a program into BBRF

Program URL [Intergamma](#)

Instructions

1. Add the program using the tags 'url', 'site', 'reward'
2. Add inscope
3. Add outscope
4. List the inscope
5. List the outscope

Show how to use the addProgram function from repo.

Proposed exercise

Tag every url if it's tier 1, tier 2 or 'No bounty'. That way, when you find a bug you'll know beforehand if it has a bounty or not.

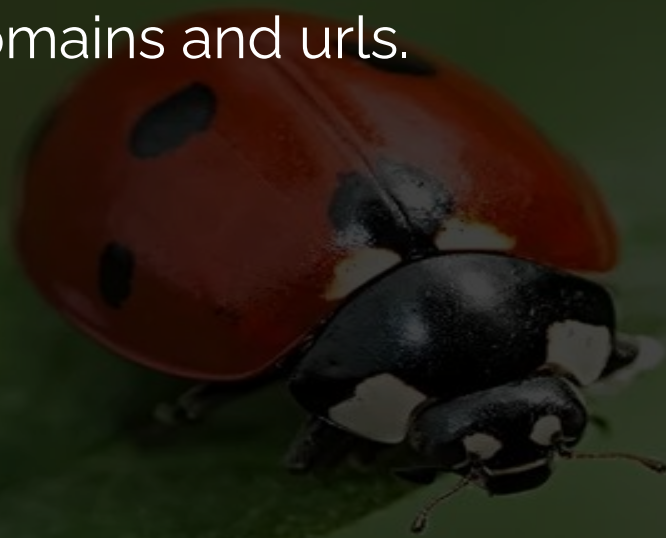


> Recon

Find all the domains and urls.

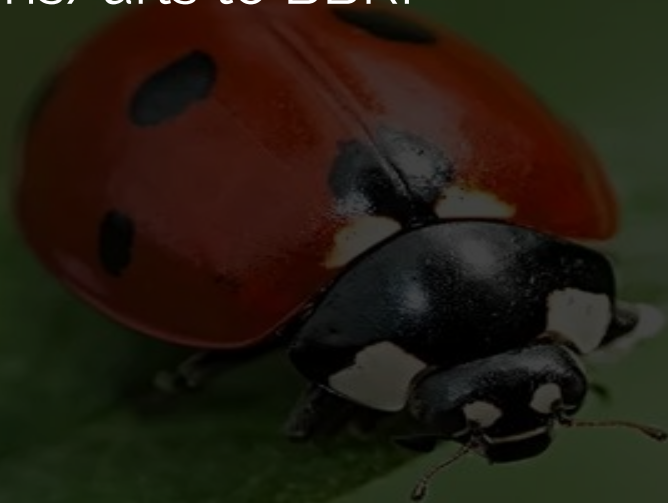
Subfinder

Asset finder



> Exercise 2 (20 minutes)

Add domains/urls to BBRF



> Nuclei

<https://github.com/projectdiscovery/nuclei>

<https://github.com/projectdiscovery/nuclei-templates>

Running example



> Nuclei How to use it

Install it

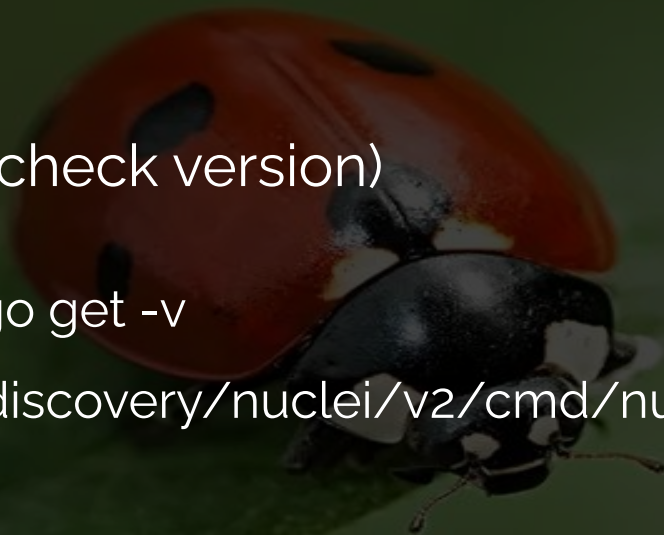
Install Go (check version)

GO111MODULE=on go get -v

github.com/projectdiscovery/nuclei/v2/cmd/nuclei

If issues ([here](#))

Test it



> Exercise 3 (20 minutes)

Running Nuclei



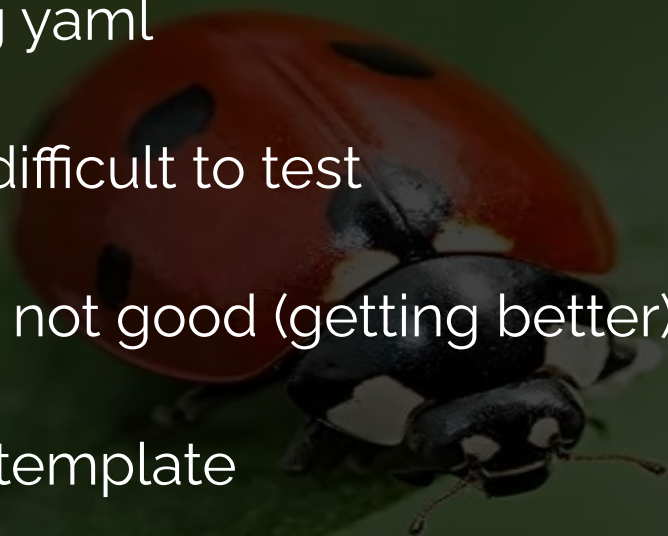
> Nuclei What are templates?

Define rules using yaml

Easy to develop, difficult to test

Documentation is not good (getting better)

- Requests per template
- Templates are running
- RPS server performance (100-150 RPS)
- # instances (10 to 20 instances)



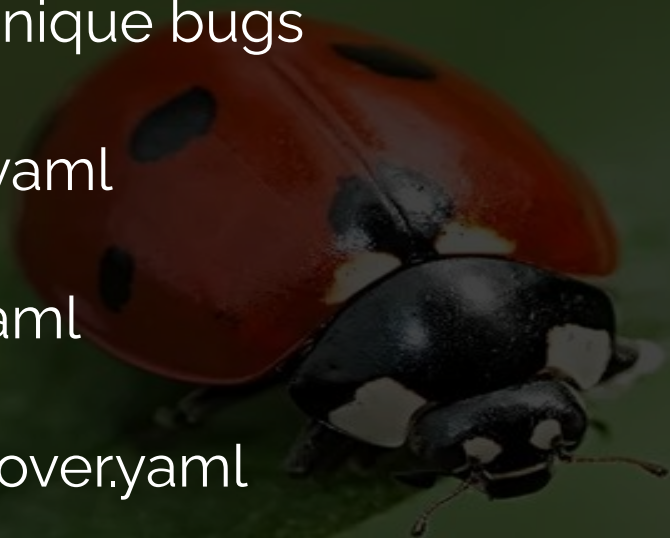
> Nuclei Creating your own template?

Best way to find unique bugs

CVE-2020-9490.yaml

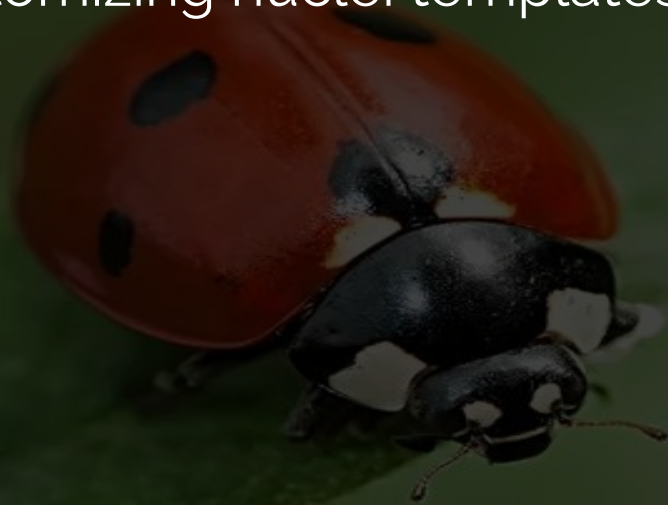
apache-detect.yaml

freshservice-takeover.yaml



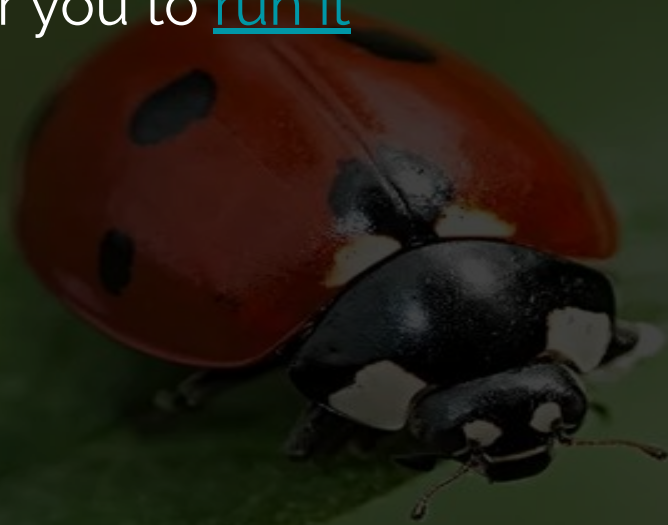
> Exercise 4 (25 minutes)

Building and Customizing nuclei templates.



> Axiom [Distributed Bug Bounty Hunting]

Let's try for you to [run it](#)



> How do you report? Word, Latex, Txt?

StackEdit

Uses Markdown

Syncs with Google Drive

Exports files PDF/HTML

<https://stackedit.io/app#>



> Exercise 5 (10 minutes)

StackEdit

Uses Markdown

Syncs with Google Drive

Exports files PDF/HTML

<https://stackedit.io/app#>



> Exercise 6 (15 minutes)

StackEdit

Uses Markdown

Syncs with Google Drive

Exports files PDF/HTML

<https://stackedit.io/app#>



Thank you!

We want your feedback

<https://feedback.info-sec.cl>

