How to get the best out of your bug bounty program

A view from both sides

Edwin Foudil
EdOverflow

Bug Bounty Program
vs
Vulnerability Disclosure Program

Public
vs
Private

Scope

https://example.com/

https://example.com/*

*.example.com

In Scope

Note: Severity shown here only indicates the **maximum** severity possible for reports submitted to the Asset.

Domain	[redacted]	Critical	Eligible for bounty
Domain	[redacted]	Critical	Eligible for bounty
Domain	[redacted]	High	Eligible for bounty
Other	**other**	Critical	Eligible for bounty

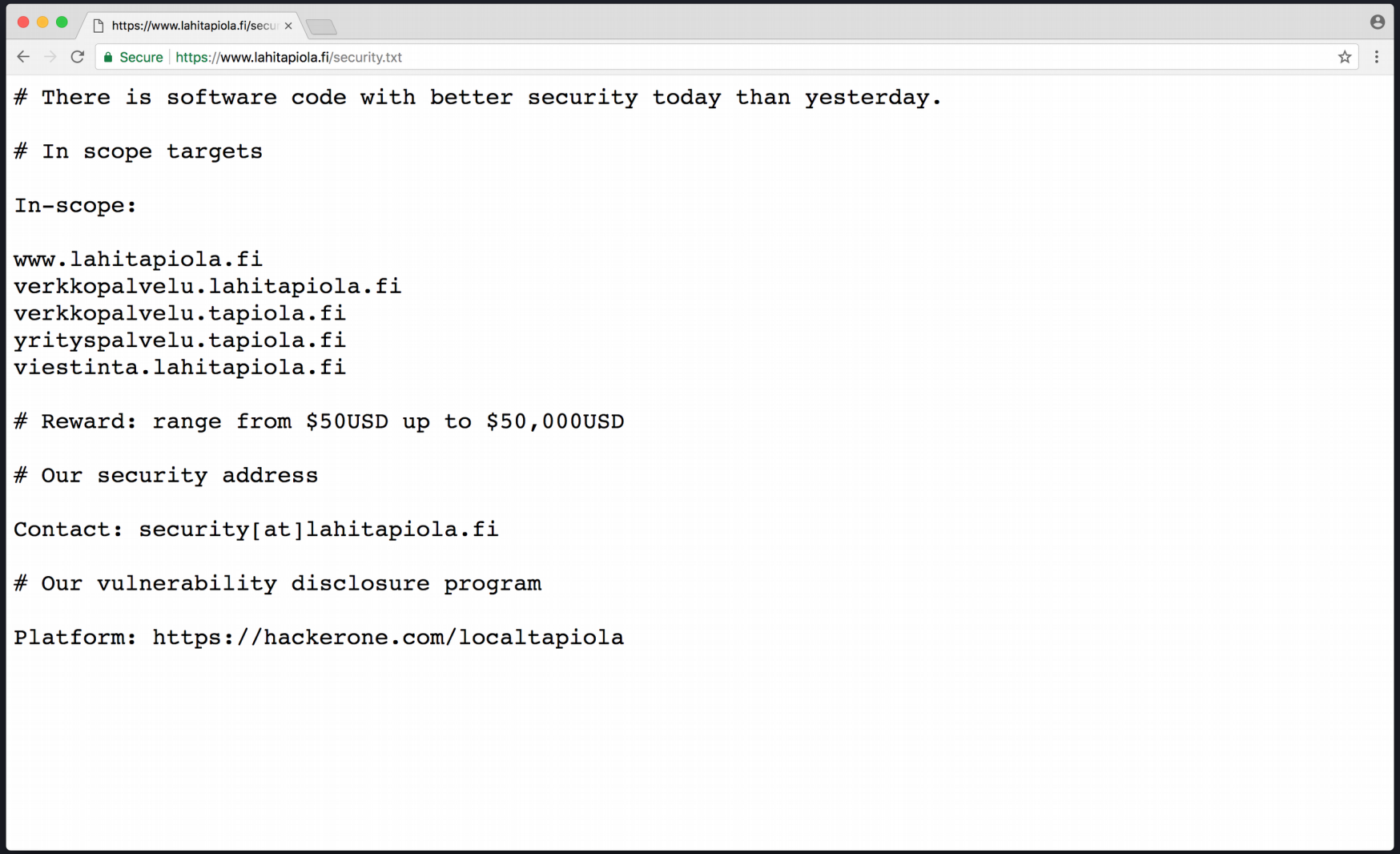
Last updated on November 30, 2017. View changes

⚠ Use *security.txt* to define your scope

https://edoverflow.com/.well-k ×

Secure | https://edoverflow.com/.well-known/security.txt

```
# If you would like to report a security issue
# you may report it to me on HackerOne.
Contact: https://hackerone.com/ed
Encryption: https://keybase.pub/edoverflow/pgp_key.asc
Acknowledgements: https://hackerone.com/ed/thanks
```


https://www.lahitapiola.fi/secu
Secure | https://www.lahitapiola.fi/security.txt
There is software code with better security today than yesterday.
In scope targets
In-scope:
www.lahitapiola.fi
verkkopalvelu.lahitapiola.fi
verkkopalvelu.tapiola.fi
yrityspalvelu.tapiola.fi
viestinta.lahitapiola.fi
Reward: range from $50USD up to $50,000USD
Our security address
Contact: security[at]lahitapiola.fi
Our vulnerability disclosure program
Platform: https://hackerone.com/localtapiola

Dedicated staff

Ways to inform third parties

Service status: Security Issue

2018.01.09 Issue with TLS-SNI-01 and Shared Hosting Infrastructure

Incidents

josh ISRG Executive Director 1 5h

At approximately 5 p.m. Pacific time on January 9, 2018, we received a report from Frans Rosén of Detectify outlining a method of exploiting some shared hosting infrastructures to obtain certificates for domains he did not control, by making use of the ACME TLS-SNI-01 challenge type. We quickly confirmed the issue and mitigated it by entirely disabling TLS-SNI-01 validation in Let's Encrypt. We're grateful to Frans for finding this issue and reporting it to us.

We'd like to describe the issue and our plans for possibly re-enabling TLS-SNI-01 support.

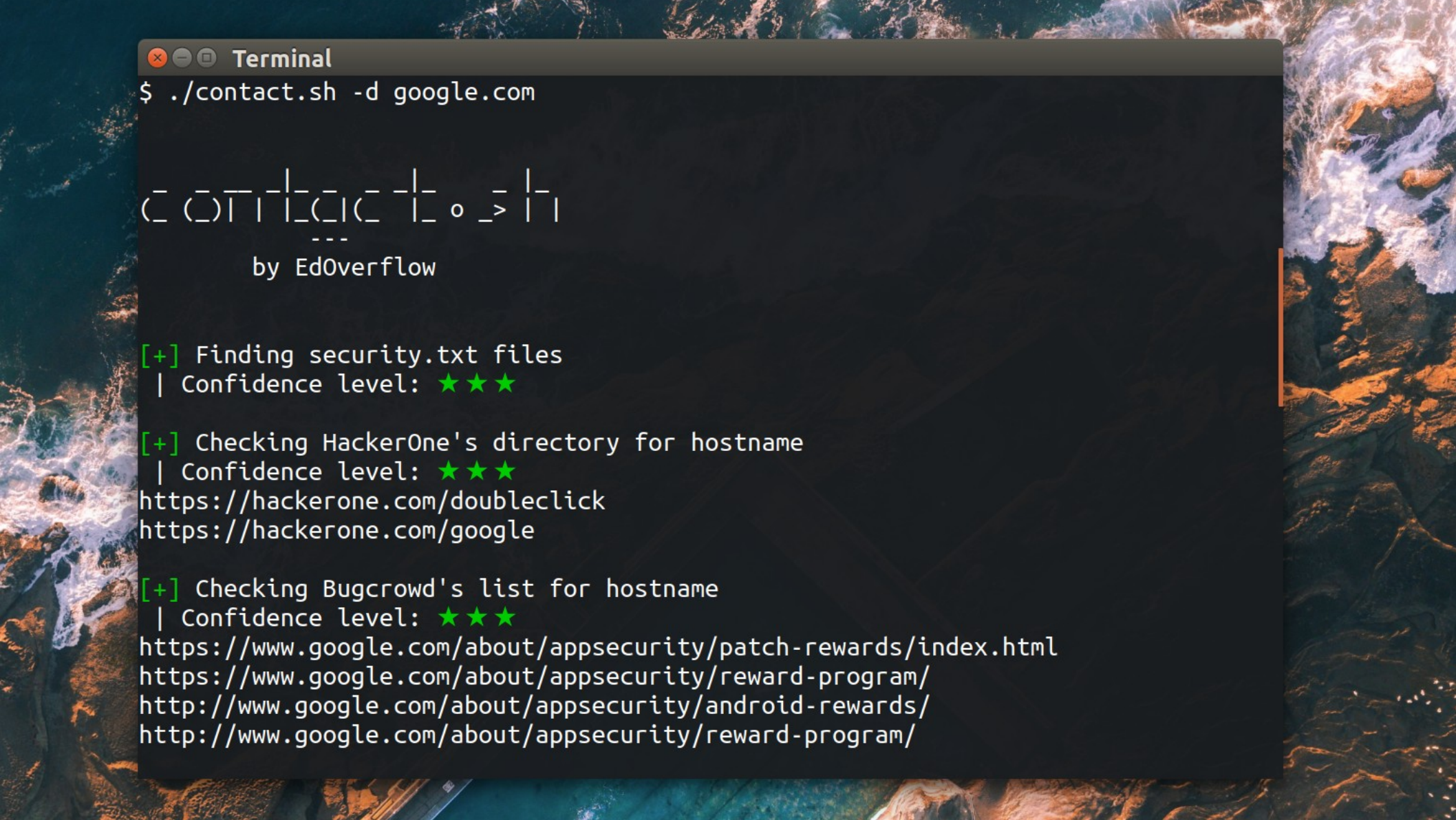
Problem Summary

In the ACME protocol's TLS-SNI-01 challenge, the ACME server (the CA) validates a domain name by generating a random token and communicating it to the ACME client. The ACME client uses that token to create a self-signed certificate with a specific, invalid hostname (for example, 773c7d.13445a.acme.invalid), and configures the web server on the domain name being validated to serve that certificate. The ACME server then looks up the domain name's IP address, initiates a TLS connection, and sends the specific .acme.invalid hostname in the SNI extension. If the response is a self-signed certificate containing that hostname, the ACME client is considered to be in control of the domain name, and will be allowed to issue certificates for it.

Jan 10

1 / 2
Jan 10

5h ago


Terminal
$ ./contact.sh -d google.com
by EdOverflow
[+] Finding security.txt files
| Confidence level: ★★★
[+] Checking HackerOne's directory for hostname
| Confidence level: ★★★
https://hackerone.com/doubleclick
https://hackerone.com/google
[+] Checking Bugcrowd's list for hostname
| Confidence level: ★★★
https://www.google.com/about/appsecurity/patch-rewards/index.html
https://www.google.com/about/appsecurity/reward-program/
http://www.google.com/about/appsecurity/android-rewards/
http://www.google.com/about/appsecurity/reward-program/


Incident response

Service-level agreement

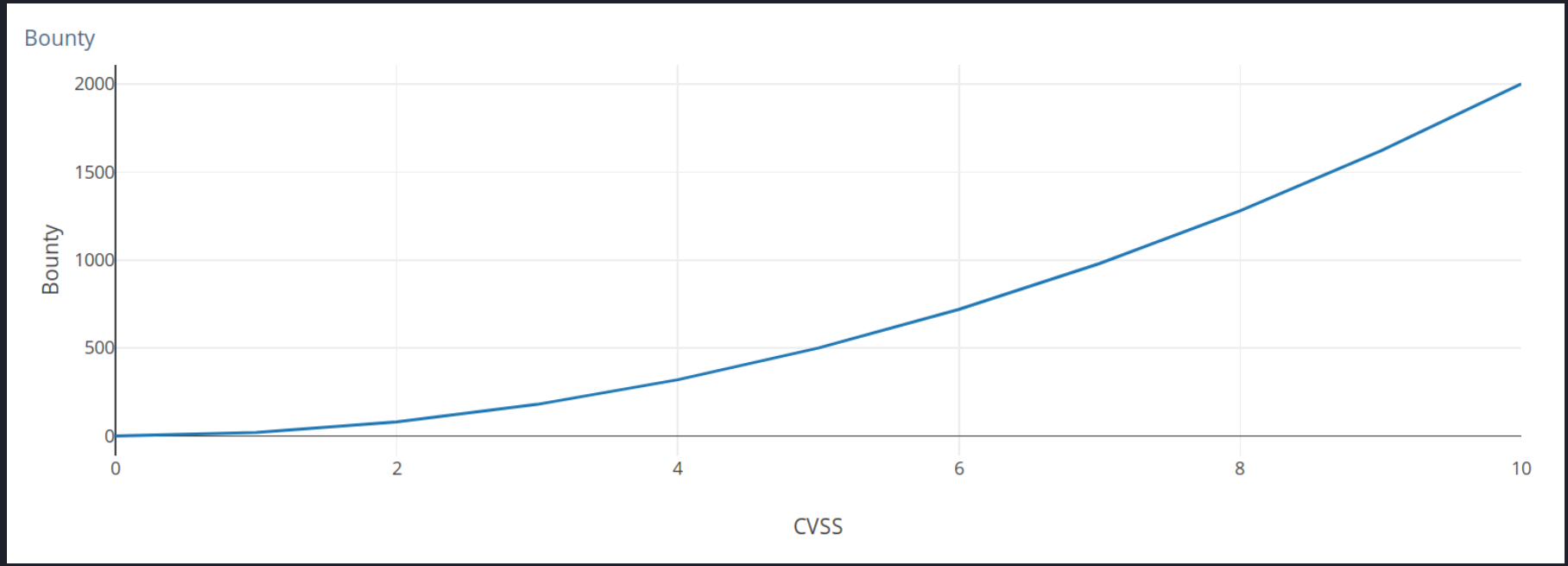
Bounties

$$\forall C(0 \leq C \leq 10)$$

$$\forall n(n \in \mathbb{R}^{+} \wedge 1.0 \leq n \leq 3.0)$$

$$N = \frac{b_{max}}{(C_{max})^{n}}$$

$$b = N \times (C^{n})$$


Bounty
2000
1500
1000
500
0
Bounty
0
2
4
6
8
10
CVSS

Julia Galef 
@juliagalef

Follow

Aquarium rewards dolphins w/a fish if they bring a piece of litter or dead gull (to help keep pool clean)

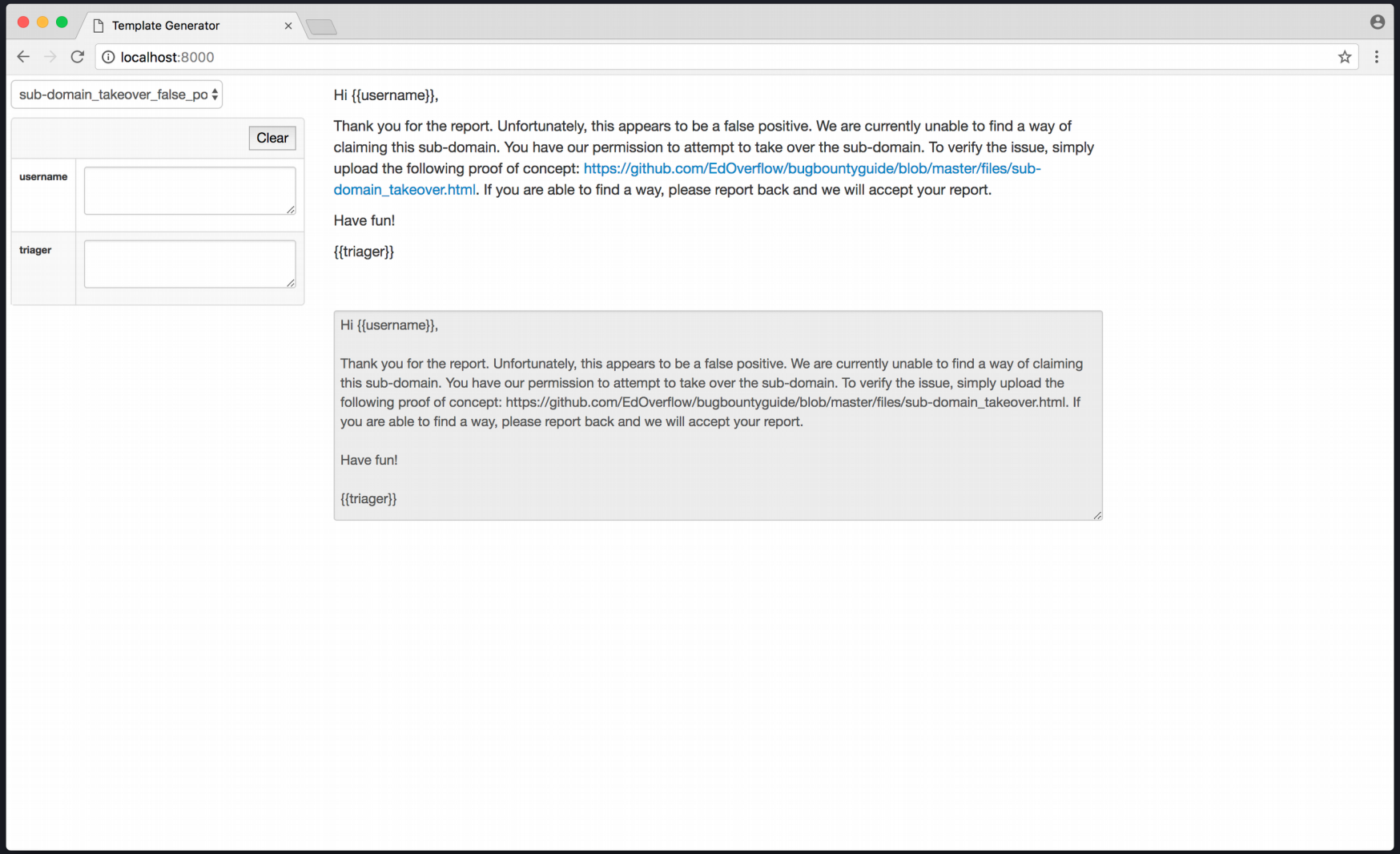
One dolphin starts (1) tearing pieces of litter into smaller pieces & trading each piece in for a reward & (2) stockpiling fish to lure & kill gulls

Why dolphins are deep thinkers

The more we study dolphins, the brighter they turn out to be, writes Anuschka de Rohan

theguardian.com

Make triaging easier


Template Generator
localhost:8000
sub-domain_takeover_false_po
Clear
username
triager
Hi {{username}},
Thank you for the report. Unfortunately, this appears to be a false positive. We are currently unable to find a way of claiming this sub-domain. You have our permission to attempt to take over the sub-domain. To verify the issue, simply upload the following proof of concept: https://github.com/EdOverflow/bugbountyguide/blob/master/files/sub-domain_takeover.html. If you are able to find a way, please report back and we will accept your report.
Have fun!
{{triager}}
Hi {{username}},
Thank you for the report. Unfortunately, this appears to be a false positive. We are currently unable to find a way of claiming this sub-domain. You have our permission to attempt to take over the sub-domain. To verify the issue, simply upload the following proof of concept: https://github.com/EdOverflow/bugbountyguide/blob/master/files/sub-domain_takeover.html. If you are able to find a way, please report back and we will accept your report.
Have fun!
{{triager}}

BOT: Gratipay posted a comment. Jun 17th (7 months ago)

Hi,

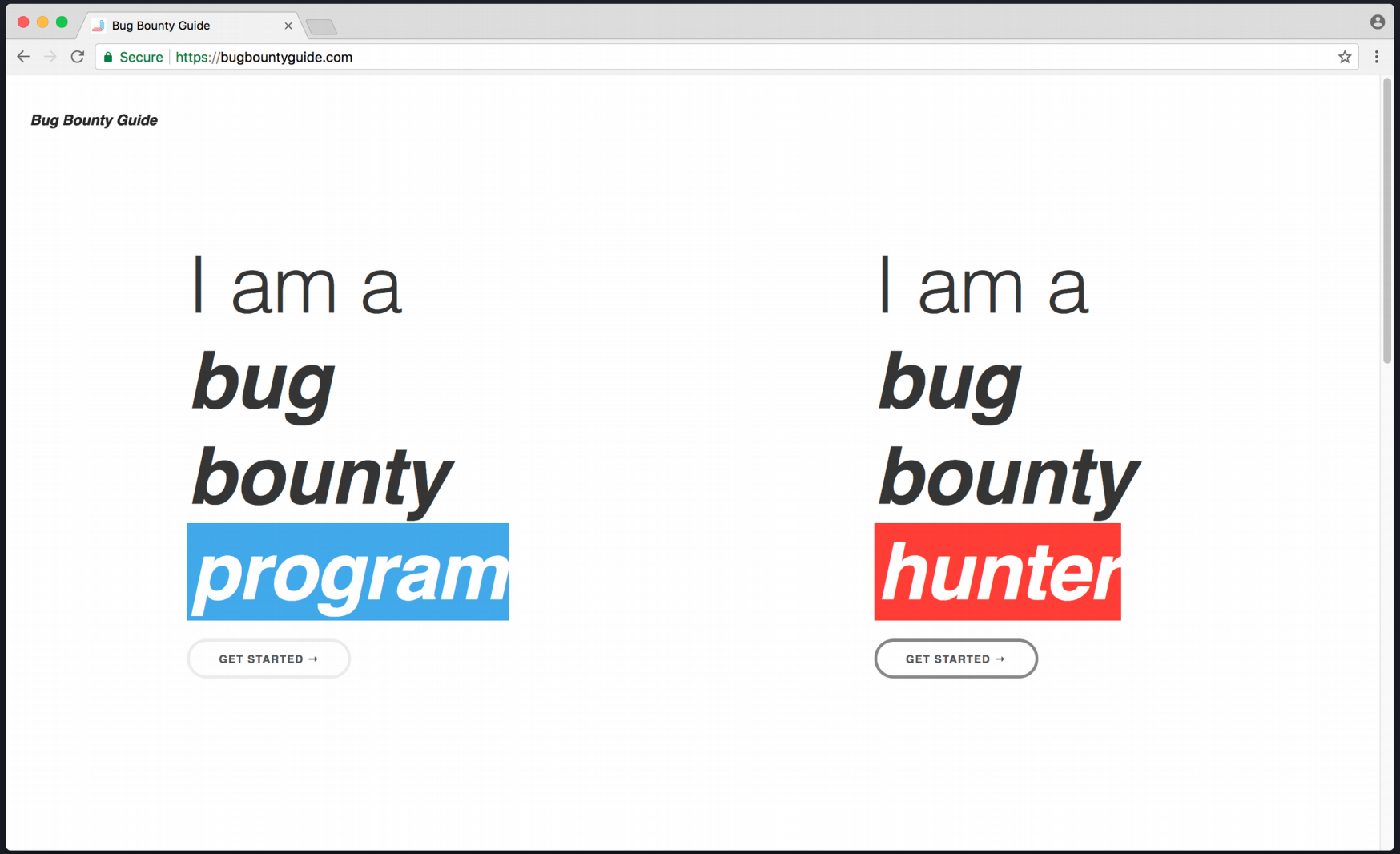
Thanks for the report. Unfortunately, this has already been reported to us. We look forward to more reports from you in the future.

Best regards,
The Gratipay Security Team

Consider the hunter's reputation

Familiarise yourself with the community

Hire bug bounty hunters


Bug Bounty Guide
Secure https://bugbountyguide.com
Bug Bounty Guide
I am a
bug
bounty
program
GET STARTED →
I am a
bug
bounty
hunter
GET STARTED →