

Responsible Vulnerability Disclosure



Howdy!

I'm Miglen Evlogiev / www.miglen.com

- Director of Infosec @ Payhawk
- Hacking is not a crime advocate
- Ex-Amazon Security Engineer
- Script kiddie before it was cool



Overview

- Little bit of terminology
- The security.txt standard
- Implementation guidance
- The good example GDI.Foundation
- Bulgaria's first steps - CERT & CSF
- Shkolo.bg case study
- Preventing cybercrime

What is a vulnerability?

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.



What does Responsible Disclosure mean?

Responsible disclosure is a process that allows security researchers to safely report found vulnerabilities to your team.

Basically saying it's ok to hack us on these terms and we will not press charges if you do it in an ethical way.

What about Bug Bounty?

Responsible Disclosure opens the door for ethical hackers to find and report vulnerabilities to you. Bug Bounty, on the other hand, means offering monetary compensation to the ethical hackers who find vulnerabilities. You can decide whether to pay out bounties as part of your program.

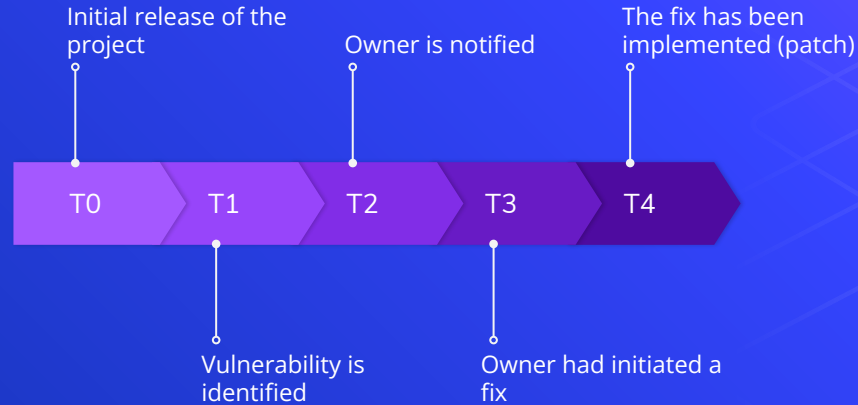
Why it matters?

- ⬡ Allows you to receive structured reports
- ⬡ Provides secure channel for communication
- ⬡ Answers repetitive questions
- ⬡ Defines scope for testing and exclusions

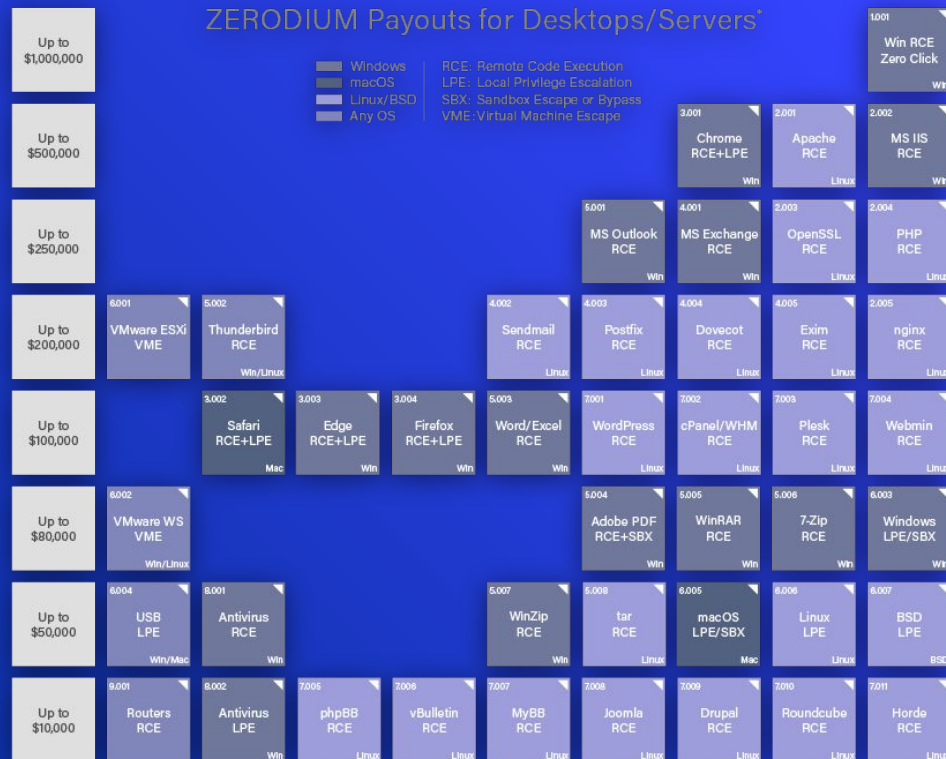
Other benefits?

- ⬡ Helps build a healthy infosec community
- ⬡ Prevents full information disclosures
- ⬡ Reduces reports to authorities

The life of a vulnerability



Vulnerability markets



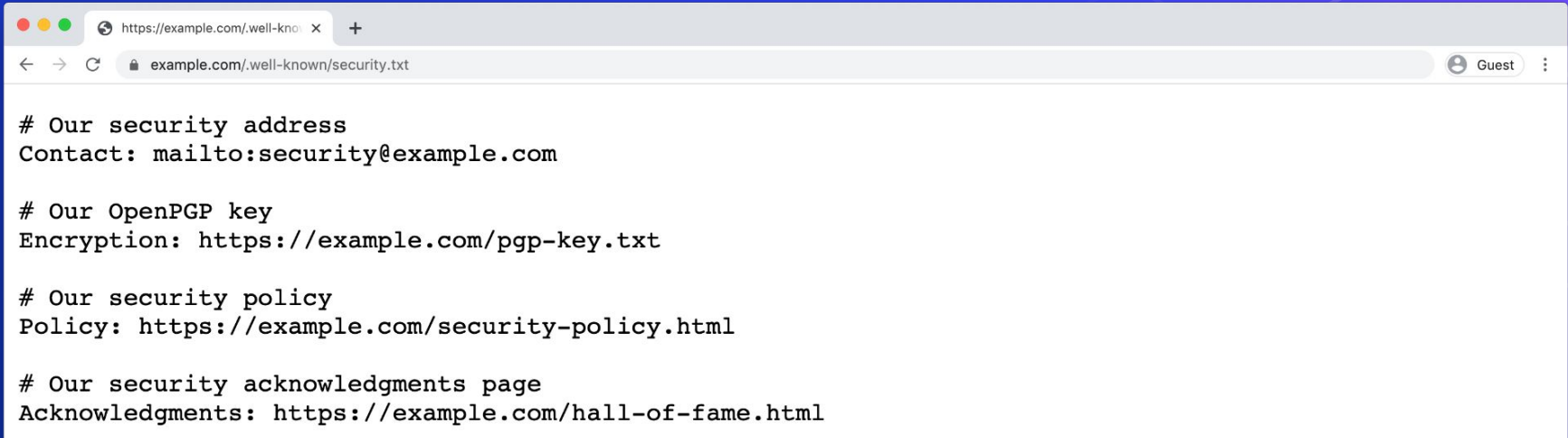
* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

2019/01 © zerodium.com

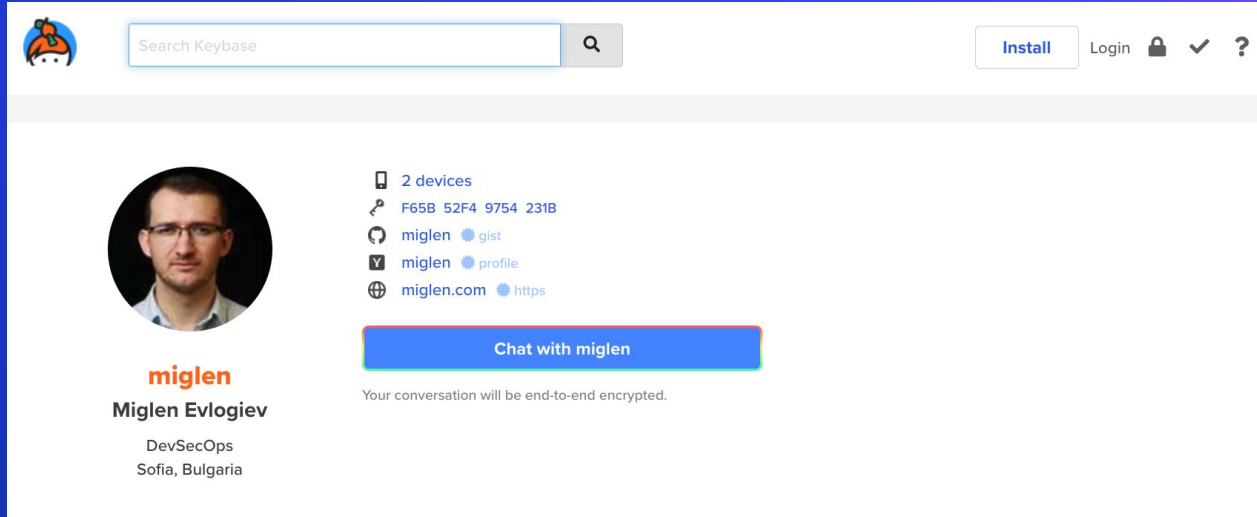


Security.txt standard

A proposed standard which allows websites to define security policies.

A screenshot of a web browser window showing a security.txt file. The browser's address bar displays the URL 'https://example.com/well-known/security.txt'. The page content is a plain text file with four sections, each starting with a comment line (prefixed with '#') and followed by a specific policy or contact information. The sections are: 'Our security address' with contact email 'mailto:security@example.com'; 'Our OpenPGP key' with encryption URL 'https://example.com/pgp-key.txt'; 'Our security policy' with policy URL 'https://example.com/security-policy.html'; and 'Our security acknowledgments page' with acknowledgments URL 'https://example.com/hall-of-fame.html'. The browser interface includes standard navigation buttons (back, forward, refresh) and a user profile indicator labeled 'Guest'.


Keybase for key sharing



The screenshot shows the Keybase profile page for a user named 'miglen'. At the top, there is a search bar labeled 'Search Keybase' and navigation links for 'Install', 'Login', and a help icon. The profile section includes a circular profile picture of a man with glasses, the username 'miglen' in orange, and the full name 'Miglen Evlogiev'. Below the name is the bio 'DevSecOps' and 'Sofia, Bulgaria'. To the right of the profile picture, there is a list of linked accounts and devices: '2 devices', 'F65B 52F4 9754 231B', 'miglen' (gist), 'miglen' (profile), and 'miglen.com' (https). A blue button labeled 'Chat with miglen' is prominently displayed, with a note below it stating 'Your conversation will be end-to-end encrypted.'

Search Keybase

Install Login



miglen
Miglen Evlogiev
DevSecOps
Sofia, Bulgaria

2 devices
F65B 52F4 9754 231B
miglen (gist)
miglen (profile)
miglen.com (https)

Chat with miglen

Your conversation will be end-to-end encrypted.

Best practices for your policy

- ⬡ Allows you to receive structured reports
- ⬡ Provides secure channel for communication
- ⬡ Answers repetitive questions
- ⬡ Defines scope for testing and exclusions

Exclusions

- ⬡ Volumetric / Denial of Services (DDoS)
- ⬡ Suboptimal / best practices reports
- ⬡ Self XSS / Dom-based XSS
- ⬡ Host-header injections
- ⬡ Network data enumerations (i.e. private server addresses)
- ⬡ Resource enumerations (i.e. public images with UUID)

Security Disclosure

Acknowledgements

Security Disclosure Policy

Working with the research community to improve our online security

Contents

Policy

[Scope](#)

[Bug Bounty](#)

[Reporting a vulnerability](#)

[What to expect](#)

[Guidance](#)

[Legalities](#)

[Feedback](#)

[Acknowledgements](#)

The BBC greatly appreciates investigative work into security vulnerabilities which is carried out by well-intentioned, ethical security researchers. We are committed to thoroughly investigating and resolving security issues in our platform and services in collaboration with the security community. This document aims to define a method by which the BBC can work with the security research community to improve our online security.

Scope

Vulnerabilities in BBC products and services are only within scope of the Bug Bounty Scheme when they meet the following conditions:

- They have not been previously reported or have not already been discovered by our own internal procedures;
- It can be demonstrated that there would be a real impact to the BBC, its users or its customers should the vulnerability reported be exploited by a malicious actor. The existence of a vulnerability does not necessarily demonstrate that such a potential impact exists: theoretical impacts will not be considered as within the scope of the scheme;
- It exists within a domain that has a security.txt file in its root. Subdomains are considered in scope provided their parent domain is in scope. (i.e. The existence of: `https://<bbc.com>/security.txt` means that `shop.bbc.com` and `www.bbc.com` are also in scope.)

GDI.Foundation & Victor Gevers



In the last 5 years, the GDI.foundation identified
39M security issues were accessible via the internet.
With the help of 38 volunteers, we were able to report
1.1M security issues and data leaks.



CERT & CSF



Как да хакнем shkolo

Мирослав Джоканов За ученици, Новини, Ръководство 19 коментара



4
ян. 19

Според информация на Google през 2018-а година търсачката им е получила стотици запитвания с ключов израз "Как да хакнем shkolo". Това ме мотивира да напиша следната публикация.

Търсения, сродни на как да се регистрирам в школо

shkolo.bg вход

електронен училищен дневник

shkolo.bg blog

как да хакнем школо

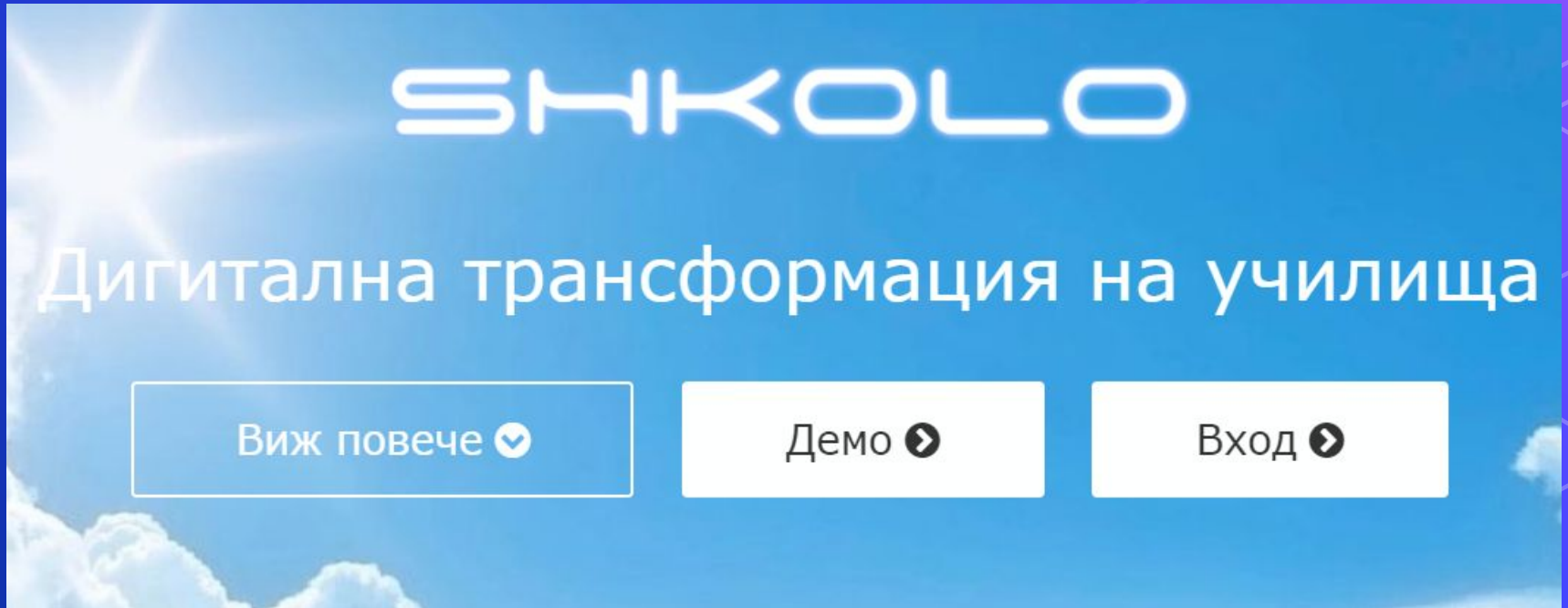
<https://www.shkolo.bg/blog/nov-roditel>

електронен дневник мон

регистрация на учител

shkolo.bg vhd

Shkolo.bg case study



How Responsible Disclosure will prevent Cybercrime?



Thank you!



References

