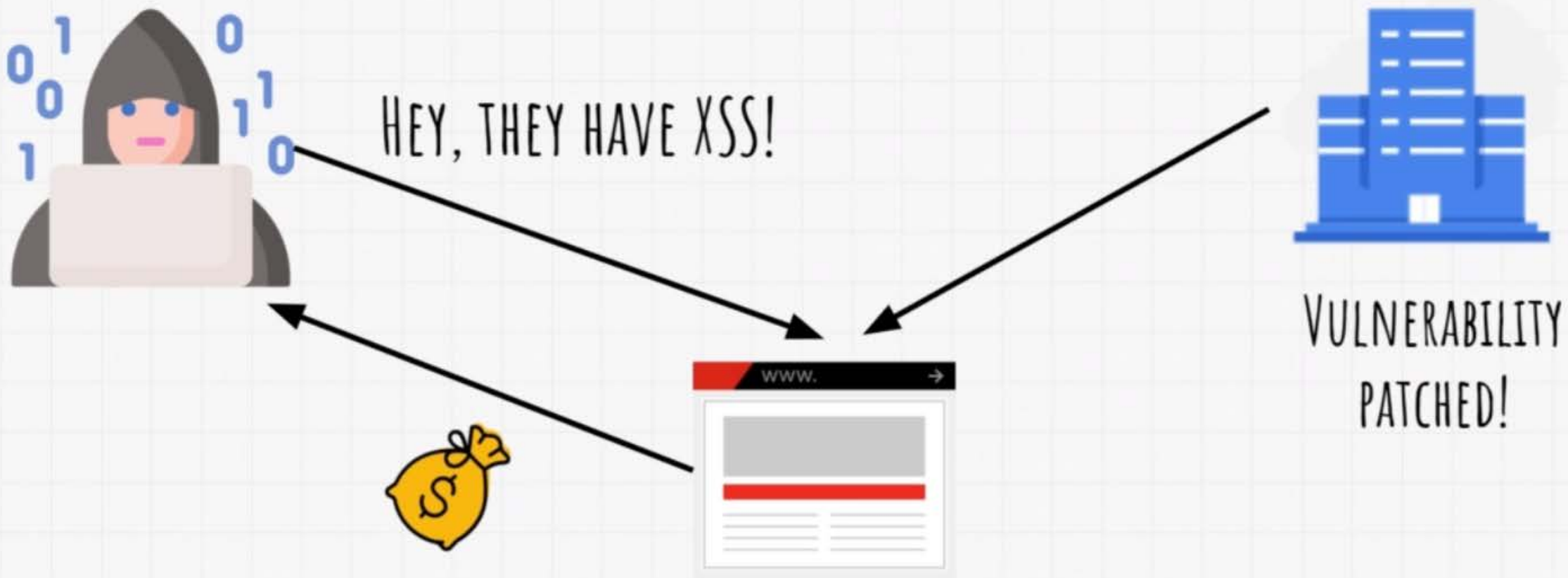
How To Earn Money With Bug Bounty ?

What are the next steps ?

PRACTICE


HEY, THEY HAVE XSS!
www.
VULNERABILITY PATCHED!

IMPORTANT STUFF ..

BUG BOUNTY PROGRAM RULES

HEY MY WEBSITE IS OFFLINE!

OPSS

HackerOne

BugCrowd

Intigriti

Synack

...

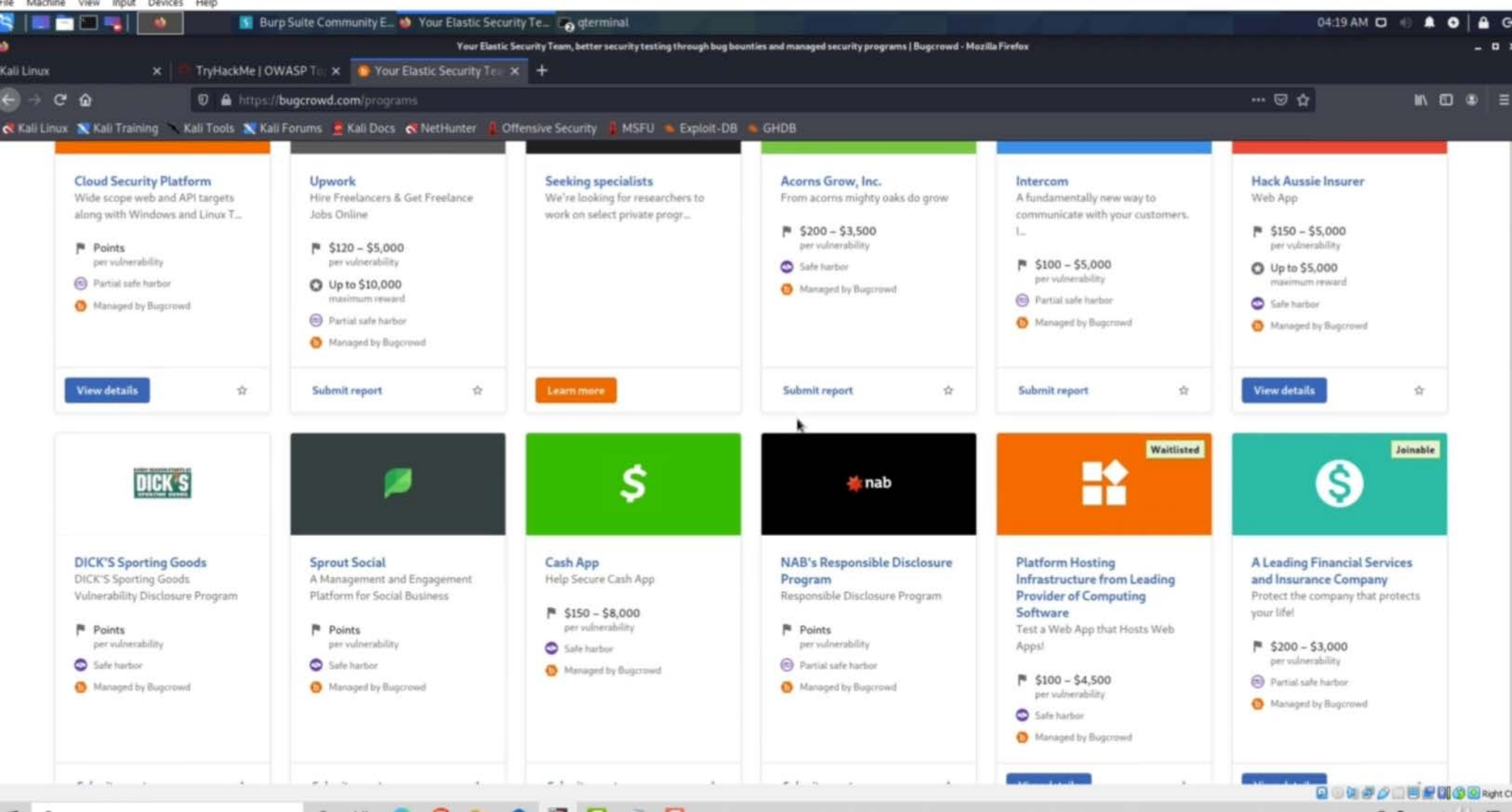
"Cybersecurity isn't a technology problem — it's a human one — and to compete against an army of adversaries we need an army of allies."

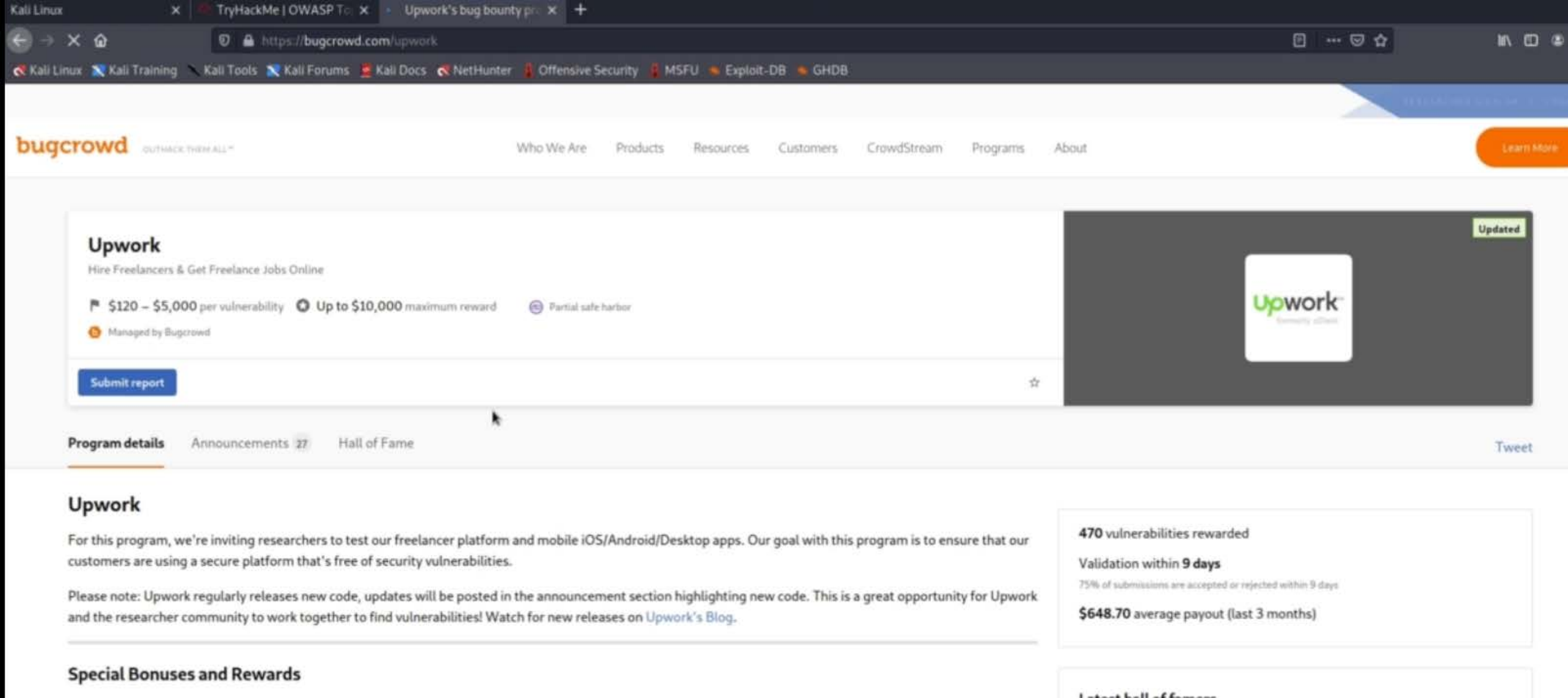
CASEY ELLIS, Founder, Bugcrowd

4 out of 5 cyber-attacks are driven by organized crime rings, in which data, tools & expertise are widely shared.

Why Crowdsourced Security?

Crowdsourced Security is a powerful tool – used by leading edge firms such as Google, Apple and Facebook – to decrease risk. However crowdsourced security is not yet well understood across the enterprise security community. This brief will define crowdsourced security and describe why it's a key element of any viable security architecture.


Burp Suite Community E...
Your Elastic Security Te...
qterminal
04:19 AM
Your Elastic Security Team, better security testing through bug bounties and managed security programs | Bugcrowd - Mozilla Firefox
Kali Linux
TryHackMe | OWASP T
Your Elastic Security Te
https://bugcrowd.com/programs
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
Cloud Security Platform
Wide scope web and API targets along with Windows and Linux T...
Points
per vulnerability
Partial safe harbor
Managed by Bugcrowd
View details
Upwork
Hire Freelancers & Get Freelance Jobs Online
$120 – $5,000
per vulnerability
Up to $10,000
maximum reward
Partial safe harbor
Managed by Bugcrowd
Submit report
Seeking specialists
We're looking for researchers to work on select private progr...
Learn more
Acorns Grow, Inc.
From acorns mighty oaks do grow
$200 – $3,500
per vulnerability
Safe harbor
Managed by Bugcrowd
Submit report
Intercom
A fundamentally new way to communicate with your customers. I...
$100 – $5,000
per vulnerability
Partial safe harbor
Managed by Bugcrowd
Submit report
Hack Aussie Insurer
Web App
$150 – $5,000
per vulnerability
Up to $5,000
maximum reward
Safe harbor
Managed by Bugcrowd
View details
DICK'S Sporting Goods
DICK'S Sporting Goods Vulnerability Disclosure Program
Points
per vulnerability
Safe harbor
Managed by Bugcrowd
Sprout Social
A Management and Engagement Platform for Social Business
Points
per vulnerability
Safe harbor
Managed by Bugcrowd
Cash App
Help Secure Cash App
$150 – $8,000
per vulnerability
Safe harbor
Managed by Bugcrowd
nab
NAB's Responsible Disclosure Program
Responsible Disclosure Program
Points
per vulnerability
Partial safe harbor
Managed by Bugcrowd
Waitlisted
Platform Hosting Infrastructure from Leading Provider of Computing Software
Test a Web App that Hosts Web Apps!
$100 – $4,500
per vulnerability
Safe harbor
Managed by Bugcrowd
Joinable
A Leading Financial Services and Insurance Company
Protect the company that protects your life!
$200 – $3,000
per vulnerability
Partial safe harbor
Managed by Bugcrowd


Kali Linux
TryHackMe | OWASP T
Upwork's bug bounty pr
https://bugcrowd.com/upwork
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
bugcrowd
Who We Are
Products
Resources
Customers
CrowdStream
Programs
About
Upwork
Hire Freelancers & Get Freelance Jobs Online
$120 – $5,000 per vulnerability
Up to $10,000 maximum reward
Partial safe harbor
Managed by Bugcrowd
Submit report
Updated
Upwork
Program details
Announcements 27
Hall of Fame
Tweet
Upwork
For this program, we're inviting researchers to test our freelancer platform and mobile iOS/Android/Desktop apps. Our goal with this program is to ensure that our customers are using a secure platform that's free of security vulnerabilities.
Please note: Upwork regularly releases new code, updates will be posted in the announcement section highlighting new code. This is a great opportunity for Upwork and the researcher community to work together to find vulnerabilities! Watch for new releases on Upwork's Blog.
Special Bonuses and Rewards
470 vulnerabilities rewarded
Validation within 9 days
75% of submissions are accepted or rejected within 9 days
$648.70 average payout (last 3 months)

Scope and rewards

In scope targets

In scope

P4 $120 – $300	P3 $480 – $720	P2 $1200 – $2000	P1 $2000 – $5000	$10000

Direct Contracts	Website Testing	
https://www.upwork.com/api	API Testing	HTTP
Upwork Dash Messenger Desktop Version (www.upwork.com/downloads)	Desktop Applica...	
Upwork - iOS Application	Mobile Applicati...	iOS SwiftUI +2
www.upwork.com	Vue.js jQuery	Angular +7
Upwork - Android Application	Mobile Applicati...	Android Java +1
api.upwork.com/graphql	API Testing	

Out of scope targets

Out of scope

Social media hijacking	
Any subdomain/domain/property not listed in the 'in scope' section, is out of scope.	
Any Third-party Services	Website Testing
support.upwork.com	Website Testing
community.stage.upwork.com	Website Testing
community.upwork.com	Website Testing
stage.upwork.com	Website Testing
e.upwork.com	Website Testing
status.upwork.com	Website Testing
signature.upwork.com	

security vulnerability on a target that is not in-scope, but that demonstrably belongs to Upwork, it may be reported to this program, and is appreciated - but will ultimately be marked as 'not applicable' and will not be eligible for monetary or points-based compensation.

Ratings/Rewards

For the initial prioritization/rating of findings (with a few exceptions), this program will use the Bugcrowd Vulnerability Rating Taxonomy.

However, it is essential to note that in some cases, a vulnerability priority will be modified due to its likelihood or impact. In any instance where an issue is downgraded, a full, detailed explanation will be provided to the researcher - along with the opportunity to appeal and make a case for a higher priority.

Please see Target Information for exclusions specific to this program.

Requirements

The following requirements are needed to test - ***not abiding by these rules may result in you not being ineligible from receiving the full reward amount or may lead to being suspended from testing and/or removal from the program.***

- **User-Agent** - To participate in the Upwork Bug Bounty, please configure your scanner to include `bugcrowd` in the user-agent string. Failure to do so may result in your IP being temporarily blocked from participation in the program.
- **Access / Upwork Account** - You can self-register for an Upwork account and Upwork API using your `@bugcrowdninja.com` email address. Testing using any other account is out of scope. Failure to use your `@bugcrowdninja.com` address may result in your account being temporarily locked or being suspended from participating in the program.

Target information

Search table

Technical severity ▼	VRT category	Specific vulnerability name	Variant / Affected function
P1	Server Security Misconfiguration	Using Default Credentials	
P1	Server-Side Injection	File Inclusion	Local
P1	Server-Side Injection	Remote Code Execution (RCE)	
P1	Server-Side Injection	SQL Injection	
P1	Server-Side Injection	XML External Entity Injection (XXE)	
P1	Broken Authentication and Session Management	Authentication Bypass	
P1	Sensitive Data Exposure	Disclosure of Secrets	For Publicly Accessible Asset
P1	Insecure OS/Firmware	Command Injection	
P1	Insecure OS/Firmware	Hardcoded Password	Privileged User
P1	Broken Cryptography	Cryptographic Flaw	Incorrect Usage
P1	Automotive Security Misconfiguration	Infotainment, Radio Head Unit	PII Leakage
P1	Automotive Security Misconfiguration	RF Hub	Key Fob Cloning
P2	Server Security Misconfiguration	Misconfigured DNS	High Impact Subdomain Takeover