



Veremes

 #FMEWT



WORLD TOUR
2018

1 an après : retour d'expérience sur le programme de BugBounty de Veremes

Armand Bahi

Qu'est-ce qu'un programme BugBounty ?



Améliorer la sécurité
d'une application



Hackers
professionnels



Récompenses



Première plateforme européenne de bug bounty reposant sur la législation et les règles en vigueur en Europe

The screenshot shows the 'Submitted Reports List' page on the Bounty Factory.io platform. The interface includes a sidebar with navigation options like 'Programs Directory', 'Submitted Reports', and 'Invitations'. The main content area displays a table of reports with columns for ID, description, tags, priority, status, hunter, and reward.

#	Bug Description	Tags	Priority	Status	Hunter	Reward
#PGM120-1	OWASP-2013-A5-Security Misconfiguration Technical information leak [Veremes] Managed by: a_bahi	Select value	Select value	INFORMATIVE	BZHash	-
#PGM120-2	OWASP-2013-A6-Sensitive Data Exposure Too verbose error message [Veremes] Managed by: a_bahi	Select value	Select value	INFORMATIVE	BZHash	-
#PGM120-3	None Applicable [https://bugbounty.veremes.net/vmap/] Dossier .svn... [Veremes] Managed by: a_bahi	Select value	Select value	INFORMATIVE	Rbcafe	-
#PGM120-4	OWASP-2013-A5-Security Misconfiguration Default apache 2 page accessible [Veremes] Managed by: a_bahi	Select value	Select value	INFORMATIVE	BZHash	-
#PGM120-5	OWASP-2013-A1-Injection SQL Injection dans le parametre filter de la page /rest/vitis/VitisSections [Veremes] Managed by: a_bahi,olivier	Select value	Select value	RESOLVED	BZHash	200€
#PGM120-6	OWASP-2013-A1-Injection SQL injection dans paramètre filter de la page	Select value	Select value	DUPLICATE	BZHash	-



HUNTER

📁 Programs Directory 11📄 Submitted Reports 0

☕ Invitations

PROGRAM MANAGER

🐛 Bugs >

⚙️ Programs >

🏠 Home / Submitted Reports List

Program Manager

📄 Export ▾

📄 Export PGM ▾

🔥 Bugs Open

Bugs Closed ☰

Filter: Show: [Column filter](#)

#	Bug Description	Tags	Priority	Status	Hunter	Reward
		Select value ▾	Select value ▾	Select value ▾	Select value ▾	
#PGM120 -1	OWASP-2013-A5-Security Misconfiguration Technical information leak [Veremes] Managed by: a_bahi			INFORMATIVE	BZHash	-
#PGM120 -2	OWASP-2013-A6-Sensitive Data Exposure Too verbose error message [Veremes] Managed by: a_bahi			INFORMATIVE	BZHash	-
#PGM120 -3	None Applicable [https://bugbounty.veremes.net/vmap/] Dossier .svn... [Veremes] Managed by: a_bahi			INFORMATIVE	Rbcafe	-
#PGM120 -4	OWASP-2013-A5-Security Misconfiguration Default apache 2 page accessible [Veremes] Managed by: a_bahi			INFORMATIVE	BZHash	-
#PGM120 -5	OWASP-2013-A1-Injection SQL Injection dans le parametre filter de la page /rest/vitis/VitisSections [Veremes] Managed by: a_bahi,olivier			RESOLVED	BZHash	200€
#PGM120 -6	OWASP-2013-A1-Injection SQL injection dans paramètre filter de la page /rest/vitis/VitisSections			DUPLICATE	BZHash	-

Comment Veremes a lancé le programme



Lien vers l'application, GitHub et documentation



Vulnérabilités récompensées



Vulnérabilités non récompensées



Rémunération

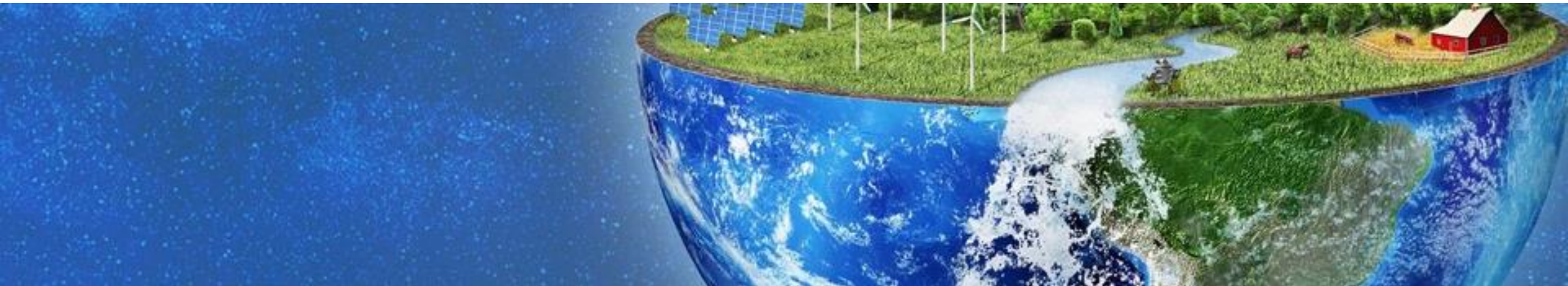
- Entre 100 et 800€ suivant la criticité du bug remonté
- Récompense maximale pour les informations confidentielles (cadastre propriétaire)

An aerial photograph of a beach. The top half of the image shows deep blue and turquoise ocean water with white waves crashing onto a sandy beach. The bottom half shows the sandy beach and some green foliage on the right side. A semi-transparent white banner is overlaid across the middle of the image.

Interlude technique

Grands types d'attaques

- Attaques par injection
 - **SQL injection**
 - **Cross-site Scripting (XSS)**
 - Code injection
 - OS Command injection
- **Détournement du domaine**
- Security Misconfiguration
- Man in the middle
- Déni de service



An aerial photograph of a coastline. The top half shows deep blue water transitioning to a vibrant turquoise near the shore. White waves are breaking onto a wide, sandy beach. The bottom right corner shows some green trees and a paved area.

Lancement du programme

Ce qui a été reporté



48 bugs reportés



14 bugs acceptés



16 bugs refusés



18 bugs dupliqués



Détournement du
domaine



Injection SQL



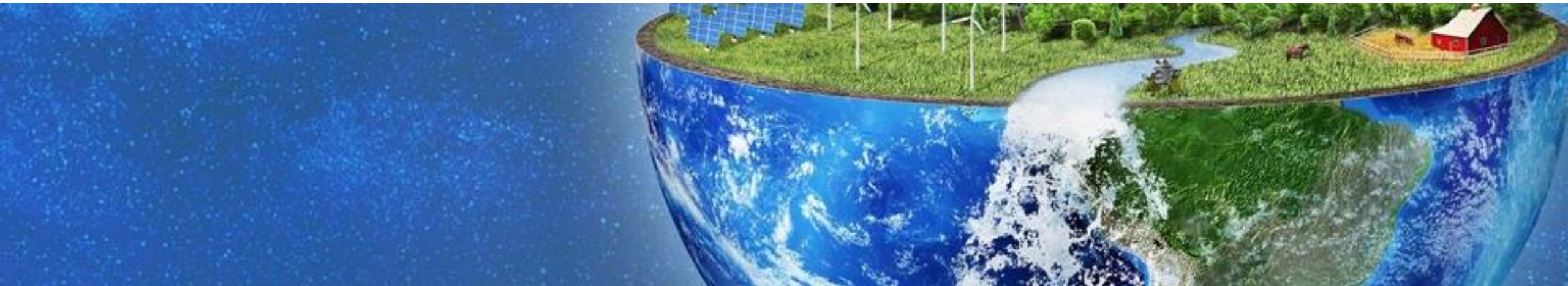
Cross-site Scripting (XSS)



Time Based Blind SQLi

Combien ça coûte ?

- Rewards : 3700€
- Ressources humaines : 80h de travail
 - Surévaluation des bugs remontés
 - Compréhension et vérification des bugs
 - Dialogue avec les hackers



Conclusion

- Outil de sécurisation
- Motive les équipes
- Contacts
- Savoir faire
- Lancement d'un programme pour GTF

