Updated: 2023-10-27 / v1.0.1

All4sports security guidelines

Rules of engagement

Our promise to you

- We will do everything possible to solve any shortcomings as quickly as possible, and we will keep you posted.
- If we require additional information, we may choose to contact you, if possible.

Your promise to us

- Cease testing and submit a report immediately if you encounter any user data during testing, such as Personally Identifiable Information (PII), order history and information, payment data, or proprietary information.
- Provide detailed but to-the point reproduction steps
- Include a clear attack scenario. How will this affect us exactly?
- Remember: quality over quantity!
- Please do NOT publicly discuss or publish any vulnerability before it has been fixed and you have received explicit permission from us to do so. You can send us a video as proof of concept, but remember to change its privacy settings to private.
- Please do *not* use automatic scanners. Be creative and do it yourself! We cannot accept any submissions found by using automatic scanners. Scanners also won't improve your skills, and can cause a high server load.

Updated: 2023-10-27 / v1.0.1

Domains and scopes

Domains in scope:

- *.21run.com
- *.all4running.nl
- *.all4running.be

Shared code between sites

Please note that our websites share a high percentage of their source code. This means that if you submit a vulnerability on one domain, it will not be accepted as a separate vulnerability on a second domain.

Any products delivered to you that have gained during this program must be returned to All4sports.

Out of scope

Application

- No captcha on the customer login portal
- Self-XSS that cannot be used to exploit other users
- Verbose messages/files/directory listings without disclosing any sensitive information
- CORS misconfiguration on non-sensitive endpoints
- Missing cookie flags
- Missing security headers
- Cross-site Request Forgery with no or low impact
- Presence of autocomplete attribute on web forms
- Reverse tabnabbing
- Bypassing rate-limits or the non-existence of rate-limits.
- Best practices violations (password complexity, expiration, re-use, etc.)
- Clickjacking without proven impact/unrealistic user interaction
- CSV Injection
- Sessions not being invalidated (logout, enabling 2FA, etc.)
- Content injection without being able to modify the HTML
- Username/email enumeration

- Email bombing
- HTTP Request smuggling without any proven impact
- Homograph attacks
- XMLRPC enabled
- Banner grabbing/Version disclosure
- Not stripping metadata of files
- Same-site scripting
- Subdomain takeover without taking over the subdomain
- Arbitrary file upload without proof of the existence of the uploaded file
- Blind SSRF without proven business impact (pingbacks are not sufficient)
- Disclosed/misconfigured Google Maps API keys
- Host header injection without proven business impact

General

- In case that a reported vulnerability was already known to the company from their own tests, it will be flagged as a duplicate
- Theoretical security issues with no realistic exploit scenario(s) or attack surfaces, or issues that would require complex end user interactions to be exploited
- Spam, social engineering and physical intrusion
- DoS/DDoS attacks or brute force attacks
- Vulnerabilities that only work on software that no longer receive security updates
- Attacks requiring physical access to a victim's computer/device, man in the middle or compromised user accounts
- Recently discovered zero-day vulnerabilities found in in-scope assets within 14 days after the public release of a patch or mitigation may be reported, but are usually not eligible for a bounty
- Reports that state that software is out of date/vulnerable without a proof-of-concept

Updated: 2023-10-27 / v1.0.1

Bounties

Low - € 0

- A reflected XSS vulnerability that requires significant user interaction
- A CSRF vulnerability in a non-critical feature
- Open redirect

Medium - € 250

- A DOM XSS vulnerability
- Reflected XSS
- An IDOR leading to the disclosure of non-critical data
- A CSRF with a significant impact
- Lateral authentication bypass

High - € 500

- Access to random users' data (sensitive PII)
- A stored XSS vulnerability (excluding unexploitable self-XSS)
- Vertical authentication bypass

Critical - € 1,000

- A SQL injection vulnerability
- Access to all customer personal data or access to a targeted user
- A numeric IDOR that allows mass write/read actions on critical features
- Path traversal leading to the disclosure of local files

Exceptional - € 2,000

- A remote code execution vulnerability on the production server
- Full database access (incl. update/delete)