QCubed Cross Site Scripting (CVE-2020-24912)

2 March 2021

Identifier:	AIT-SA-20210215-03
Target:	QCubed Framework
Vendor:	QCubed
Version:	all versions including 3.1.1
CVE:	CVE-2020-24912
Accessibility:	Remote
Severity:	High
Author:	Wolfgang Hotwagner (AIT Austrian Institute of Technology)

Summary

QCubed is a PHP Model-View-Controller Rappid Application Development framework.

Vulnerability Description

A reflected cross-site scripting (XSS) vulnerability in qcubed (all versions including 3.1.1) in profile.php via the stQuery-parameter allows unauthenticated attackers to steal sessions of authenticated users.

Proof Of Concept

The XSS occurs because the SQL-output is not sanitized properly. Since we are able to tamper the output using a SQL-injection(CVE-2020-24913), we can easily output a common XSS string.

We use the following payload(unencoded):

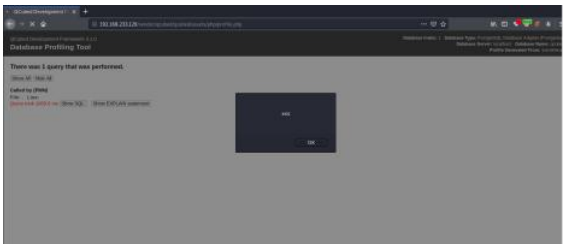
```
a:1:{i:0;a:3:{s:12:"objBacktrace";a:1:{s:4:"args";a:1:{
```

PHNjcmlwdD5hbGVydCgneHNzJyk8L3NjcmlwdD4K is unencoded:

```
"<script>alert('xss')</script>"
```

The following Burp-Screenshot illustrated a http-request using the payload from above:

The response indicates that the payload worked properly:



Vulnerable Versions

All versions including 3.1.1 are affected.

Tested Versions

QCubed 3.1.1

Impact

An unauthenticated attacker could steal sessions of authenticated users.

Mitigation

A patch was delivered by QCubed that allows to disable the profile-functionality.

Vendor Contact Timeline

2020-04-19 Contacting the vendor
2020-04-19 Vendor replied
2020-05-01 Vendor released a patch at Github
2021-02-15 Public disclosure

Advisory URL

https://www.ait.ac.at/ait-sa-20210215-03-xss-qcubed

[PHP Programming Web Security CVE]

My name is Wolfgang Hotwagner. I am a Linux and Information Security enthusiast. This blog is about my journey through Computer Science.

Tag Cloud

Downloads Perl Debian Linux Zsh One-Liner Nagios Fun Firewall git Ruby Certification Programming Suricata C Kernel Web External Security Hardware Network Toscom Docker openssl Crypto Blog HackADay logrotate Btrfs Database Mail Virtualization Proxy News Email Bash vim PHP Backup Open-Source Sysadmin Mathematics Tricks Anniversary Postgresql xmas Ansible Raspberry apache TerminalEmulator Shell Software-Raid LVM Puppet Desktop CLI Multimedia CVE

Recent Posts

- BSidesVienna 2022: Logrotten.
- SexyPolling SQL Injection
- Seventh Anniversary
- ForkCMS PHP Object Injection (CVE-2020-24036)
- QCubed Cross Site Scripting (CVE-2020-24912)
- QCubed SQL Injection (CVE-2020-24913)

- QCubed PHP Object Injection (CVE-2020-24914)
- Pimp my shell
- Refurbished Blog
- How to build a music-box for children