Multiple Vulnerabilities in TCExam

Critical

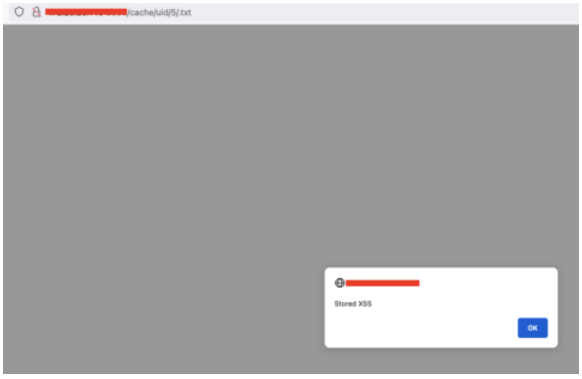
← View More Research Advisories

Synopsis

A researcher at Tenable discovered multiple vulnerabilities in TCExam 14.8.1.

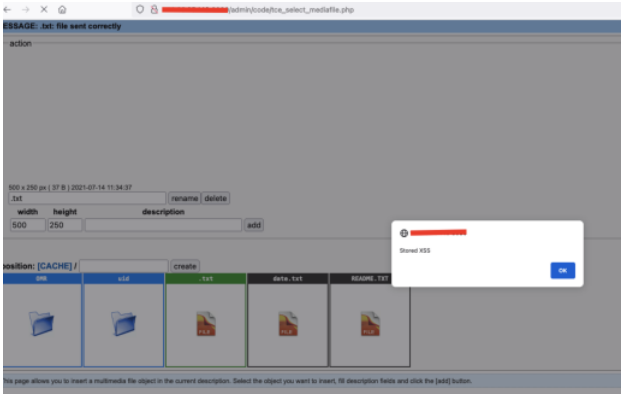
CVE-2021-20111 - Stored Cross Site Scripting Vulnerability in tce_filemanager.php

CVSSv3 Base Score: 4.6
CVSSv3 Vector: AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N
CWE: 79
A stored cross-site scripting vulnerability exists in TCExam <= 14.8.1. Valid files uploaded via tce_filemanager.php with a filename beggining with a period will be rendered as text/html. An attacker with access to tce_filemanager.php could upload a malicious javascript payload which would be triggered when another user views the file (either via tce_filemanager.php, other pages which allow the viewing of files, or via direct link).



CVE-2021-20112 - Stored Cross Site Scripting Vulnerability in tce_select_mediafile.php

CVSSv3 Base Score: 4.6
CVSSv3 Vector: AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N
CWE: 79
A stored cross-site scripting vulnerability exists in TCExam <= 14.8.1. Valid files uploaded via tce_select_mediafile.php with a filename beggining with a period will be rendered as text/html. An attacker with access to tce_select_mediafile.php could upload a malicious javascript payload which would be triggered when another user views the file (either via tce_select_mediafile.php, other pages which allow the viewing of files, or via direct link).



CVE-2021-20113 - Unauthenticated User Enumeration

CVSSv3 Base Score: 5.3
CVSSv3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CWE-203
An exposure of sensitive information vulnerability exists in TCExam <= 14.8.1. If a password reset request was made for an email address that was not registered with a user then we would be presented with an 'unknown email' error. If an email is given that is registered with a user then this error will not appear. A malicious actor could abuse this to enumerate the email addresses of registered users.

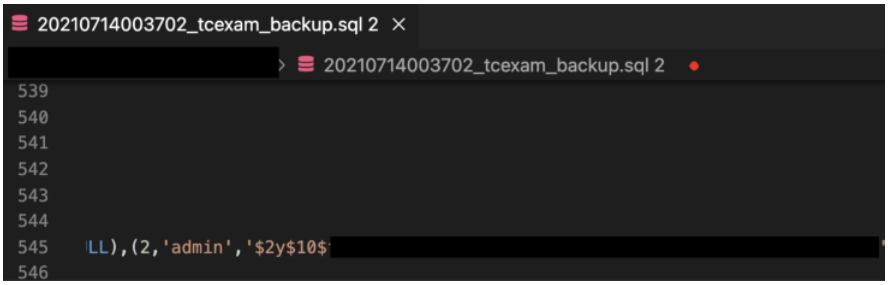
CVE-2021-20114 - Unauthenticated Access to Sensitive Objects via /cache/backup/

CVSSv3 Base Score: 9.1
CVSSv3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
CWE: 200
When installed following the default/recommended settings, TCExam <= 14.8.1 allowed unauthenticated users to access the /cache/backup/ directory, which included sensitive database backup files.

tenable

Name	Last modified	Size	Description
Parent Directory		-	
20210713155748_tcexam_backup.sql.gz	2021-07-13 13:57	22K	
20210713155832_tcexam_backup.sql.gz	2021-07-13 13:58	22K	
20210714003457_tcexam_backup.sql.gz	2021-07-13 22:34	3.3K	
20210714003702_tcexam_backup.sql.gz	2021-07-13 22:37	3.5K	
empty	2021-07-13 11:56	0	

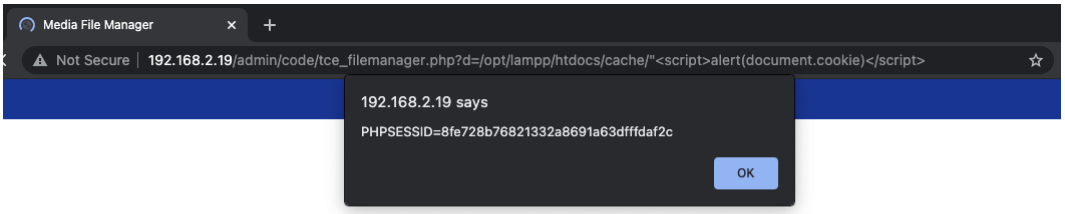
Among other things, these backup files contain usernames, password hashes and other user information that was supplied on signup.



CVE-2021-20115 - Stored Cross Site Scripting Vulnerability in tce_filemanager.php

CVSSv3 Base Score: 5.4
CVSSv3 Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N
CWE: 79

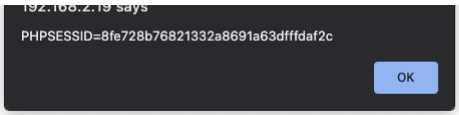
A reflected cross-site scripting vulnerability exists in TCExam <= 14.8.3. The paths provided in the f, d, and dir parameters in tce_filemanager.php were not properly validated and could cause reflected XSS via the unsanitized output of the path supplied. An attacker could craft a malicious link which, if triggered by an administrator, could result in the attacker hijacking the victim's session or performing actions on their behalf.



CVE-2021-20116 - Stored Cross Site Scripting Vulnerability in tce_select_mediafile.php

CVSSv3 Base Score: 5.4
CVSSv3 Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N
CWE: 79

A reflected cross-site scripting vulnerability exists in TCExam <= 14.8.4. The paths provided in the **f**, **d**, and **dir** parameters in tce_select_mediafile.php were not properly validated and could cause reflected XSS via the unsanitized output of the path supplied. An attacker could craft a malicious link which, if triggered by an administrator, could result in the attacker hijacking the victim's session or performing actions on their behalf.



Solution

All issues have been fixed as of TCExam 14.8.5

Additional References

https://github.com/tecnickcom/tcexam/commit/99ee2e02849c6285c5b9f18f31a1b5938d97191b
https://github.com/tecnickcom/tcexam/commit/9dce209ebb74857a50df70b31338a7002588d400
https://github.com/tecnickcom/tcexam/commit/c51f9e8a8bf0759da1534978b15a56910c9ae942
https://github.com/tecnickcom/tcexam/commit/e96ea335d73bcf60968cd003332a039fed0b7515
https://github.com/tecnickcom/tcexam/commit/c481b2890fb0f3ed2d9ec387b7954dd40af9246e

Disclosure Timeline

15 July 2021 - Vulnerabilities Discovered
19 July 2021 - Tecnick notified
20 July 2021 - Fixes pushed
21 July 2021 - Advisory published
22 July 2021 - Tenable asks if fixes are being prepare for the reflected XSS vulnerabilities
3 Aug 2021 - Tecnick having trouble reproducing, asks for clarification
4 Aug 2021 - Tenable provides clarification
4 Aug 2021 - Tecnick partially fixes issues in TCExam 14.8.4
4 Aug 2021 - Tenable informs Tecnick that the fixes need to be implemented in an additional file
5 Aug 2021 - Tecnick releases fix in 14.8.5. All vulnerabilities addressed

Risk Information

CVE ID: CVE-2021-20111
CVE-2021-20112
CVE-2021-20113
CVE-2021-20114
CVE-2021-20115
CVE-2021-20116
Tenable Advisory ID: TRA-2021-32
Credit: Derrie Sutton

CVSSv3 Base / Temporal Score: 9.1
CVSSv3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
Affected Products: TCExam <= 14.8.4
Risk Factor: Critical

Advisory Timeline

21 July 2021 - Advisory published
05 August 2021 - Advisory updated with additional vulnerabilities

Tenable.ad Active Directory

Tenable.ot Operational Technology

Tenable.sc Security Center

Tenable Lumin

Nessus

→ View all Products

FEATURED SOLUTIONS

Application Security

Building Management Systems

Cloud Security Posture Management

Compliance

Exposure Management

Finance

Healthcare

IT/OT

Ransomware

State / Local / Education

US Federal

Vulnerability Management

Zero Trust

→ View all Solutions

CUSTOMER RESOURCES

Resource Library

Community & Support

Customer Education

Tenable Research

Documentation

Trust and Assurance

Nessus Resource Center

Cyber Exposure Fundamentals

System Status

CONNECTIONS

Blog

Contact Us

Careers

Investors

Events

Media