PRESS REVIEW ARCHIVE

Digital Media Monitoring & Documentation Service

Source URL: https://www.exploit-db.com/exploits/7076

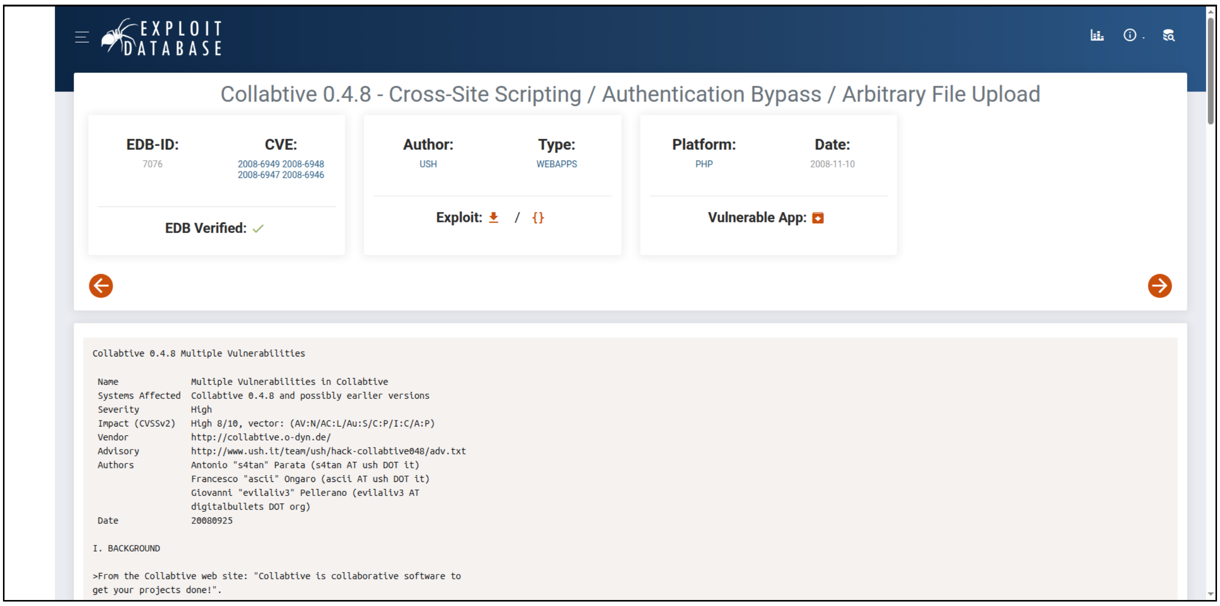
Archived Date: August 15, 2025 at 15:05

Published: November 10, 2008

Document Type: Web Page Archive

Wayback Machine: https://web.archive.org/web/*/https://www.exploit-db.com/exploits/7076

Page Screenshot



Collabtive 0.4.8 - Cross-Site Scripting / Authentication Bypass / Arbitrary File Upload

EDB-ID: 7076

CVE: 2008-6949 2008-6948 2008-6947 2008-6946

EDB Verified: ✓

Author: USH

Type: WEBAPPS

Exploit: ⭳ / {}

Platform: PHP

Date: 2008-11-10

Vulnerable App:

```
Collabtive 0.4.8 Multiple Vulnerabilities

 Name              Multiple Vulnerabilities in Collabtive
 Systems Affected  Collabtive 0.4.8 and possibly earlier versions
 Severity          High
 Impact (CVSSv2)   High 8/10, vector: (AV:N/AC:L/Au:S/C:P/I:C/A:P)
 Vendor            http://collabtive.o-dyn.de/
 Advisory          http://www.ush.it/team/ush/hack-collabtive048/adv.txt
 Authors           Antonio "s4tan" Parata (s4tan AT ush DOT it)
                   Francesco "ascii" Ongaro (ascii AT ush DOT it)
                   Giovanni "evilaliv3" Pellerano (evilaliv3 AT
                   digitalbullets DOT org)
 Date              20080925

I. BACKGROUND

>From the Collabtive web site: "Collabtive is collaborative software to
get your projects done!".
```

Collabtive 0.4.8 - Cross-Site Scripting / Authentication Bypass / Arbitrary File Upload

EDB-ID: 7076	**CVE:** 2008-6949 2008-6948 2008-6947 2008-6946

EDB Verified: ✓

Author: USH	**Type:** WEBAPPS

Exploit: ⭳ / {}

Platform: PHP	**Date:** 2008-11-10

Vulnerable App: ⭳

← →

```
Collabtive 0.4.8 Multiple Vulnerabilities

 Name              Multiple Vulnerabilities in Collabtive
 Systems Affected  Collabtive 0.4.8 and possibly earlier versions
 Severity          High
 Impact (CVSSv2)   High 8/10, vector: (AV:N/AC:L/Au:S/C:P/I:C/A:P)
 Vendor            http://collabtive.o-dyn.de/
 Advisory          http://www.ush.it/team/ush/hack-collabtive048/adv.txt
 Authors           Antonio "s4tan" Parata (s4tan AT ush DOT it)
                   Francesco "ascii" Ongaro (ascii AT ush DOT it)
                   Giovanni "evilaliv3" Pellerano (evilaliv3 AT
                   digitalbullets DOT org)
 Date              20080925

I. BACKGROUND

>From the Collabtive web site: "Collabtive is collaborative software to
get your projects done!".

II. DESCRIPTION

Multiple vulnerabilities exist in Collabtive software.

III. ANALYSIS

Summary:

 A) Stored Cross Site Scripting
 B) Forceful browsing authentication bypass
 C) Arbitrary file upload

A) Stored Cross Site Scripting

A stored XSS vulnerability exists in the "/admin.php?action=projects"
section.

Once the attacker specifies an XSS attack vector, like
"<script>alert(0);</script>", as the "Name" property of a project then
an XSS vulnerability occurs because the projects "Name" fields are
stored and printed without any filtering.

While the cited section poses limits on the "Name" field when
reflecting the XSS payload, clicking on the edit link
"/manageproject.php?action=editform&id=<projectId>" results in a page
without limitations on the characters showed thus allowing complete
exploitation.

This vulnerability requires administrator authentication.

CSRF+XSS and timing (JS) can be used to successfully exploit this
vulnerability in an automated manner.

B) Forceful browsing authentication bypass

An authentication bypass vulnerability exists in
"/admin.php?action=users&mode=added". Directly pointing to that URL
shows an error, however at the bottom of the page there is a web
form that permits to create new users with full privileges.

With this vulnerability an attacker without any valid credentials can
create a new valid administrator.

Since this vulnerability has been discovered the exploitation
prerequisites changed as detailed below:

- A bug fix in the latest version 0.4.8 now requires "globals on" in
order to exploit this vulnerability.

- In version 0.4.6 instead the vulnerability is exploitable regardless
the "globals" settings.

C) Arbitrary file upload

It's possible to upload arbitrary files with arbitrary extensions.
An attacker that has not already gained Administration privileges using
the previously exposed vulnerabilities must be assigned to at least one
project.

To upload a file go to "/managefile.php?action=showproject&id=<projectId>"
and add a new file.

If a file with .php extension is uploaded then the mimetype will be
"php/plain" and the program will change the extension to .txt in order
to prevent exploitation.

This security control can be bypassed changing the mimetype to
text/plain, in this way the application will believe that a normal .txt
file was uploaded and the extension will not be changed.

The uploaded file resides in "/files/<projectId>/<filename>_$seed.php".

An authenticated attacker will simply see the seed (and the complete
filename) using the web interface and can directly execute it.

In case of unauthenticated attackers the filename must be guessed.
Luckily the make_seed() routine leaks real random proprieties and is
only based on the time. $seed can be easily bruteforced using values
that are likely to match the return derived by the microtime() of the
upload.

private function make_seed()
{
    list($usec, $sec) = explode(' ', microtime());
    $value = (float) $sec + ((float) $usec * 100000);
    return $value;
}

As easily understandable $seed can be guessed in really few tries. The
same vulnerability exists when attaching a file in the "Messages"
section.

This vulnerability can also be exploited via CSRF.

IV. DETECTION

Collabtive 0.4.8 and possibly earlier versions are vulnerable.

V. WORKAROUND

Proper input validation will fix the vulnerabilities.

VI. VENDOR RESPONSE

No fix available.

VII. CVE INFORMATION

No CVE at this time.
```

```
VIII. DISCLOSURE TIMELINE

20080926 Initial vendor contact (No Response)
20081003 Second vendor contact (No Response)
20081010 Third vendor contact
20081010 Vendor response (Fix promised for the end of October)
20081010 Vendor contact to sync disclosure time (No response)
20081110 Advisory released (Fix not available)

IX. CREDIT

Antonio "s4tan" Parata, Francesco "ascii" Ongaro and
Giovanni "evilaliv3" Pellerano are credited with the discovery of this
vulnerability.

Antonio "s4tan" Parata
web site: http://www.ictsc.it/
mail: s4tan AT ictsc DOT it, s4tan AT ush DOT it

Francesco "ascii" Ongaro
web site: http://www.ush.it/
mail: ascii AT ush DOT it

Giovanni "evilaliv3" Pellerano
mail: evilaliv3 AT digitalbullets DOT org

X. LEGAL NOTICES

Copyright (c) 2008 Francesco "ascii" Ongaro

Permission is granted for the redistribution of this alert
electronically. It may not be edited in any way without mine express
written consent. If you wish to reprint the whole or any
part of this alert in any other medium other than electronically,
please email me for permission.

Disclaimer: The information in the advisory is believed to be accurate
at the time of publishing based on currently available information. Use
of the information constitutes acceptance for use in an AS IS condition.
There are no warranties with regard to this information. Neither the
author nor the publisher accepts any liability for any direct, indirect,
or consequential loss or damage arising from use of, or reliance on,
this information.

# milw0rm.com [2008-11-10]
```

Tags:

Advisory/Source: Link