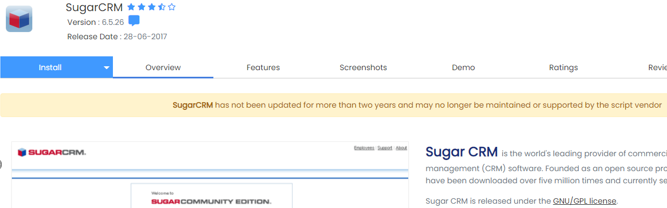
# Vulnerabilities Discussion

The potential vulnerabilities detected on RedHat Enterprise Linux 7, Exim smtpd 4.94.2, MySQL 5.5.5-10.3.23-MariaDB-cll-lve (Appendix Nmap) that provided by the hosting company are out of control. This discussion will focus on the target WebApp “SugarCRM”.

Since the “About” page of SugarCRM Community Edition is required to login to check. Based on the known CMS software, Softaculous, assumed that the target site used the latest version it provided 6.5.26 as below (Softaculous, N.D.).



According to the Vulmon Search, there are 5 expected vulnerabilities found in SugarCRM Community Edition 6.5.26 (Vulmon Search, N.D.):

* CVE-2018-6308
* CVE-2017-14508
* CVE-2017-14509
* CVE-2017-14510
* CVE-2018-17784

## SQL Injection

### CVE-2017-14508 to 10

Common Vulnerability Scoring System (CVSS) Score: 6.5 - 4.3

Vulnerability Type(s): SQL Injection

Description:

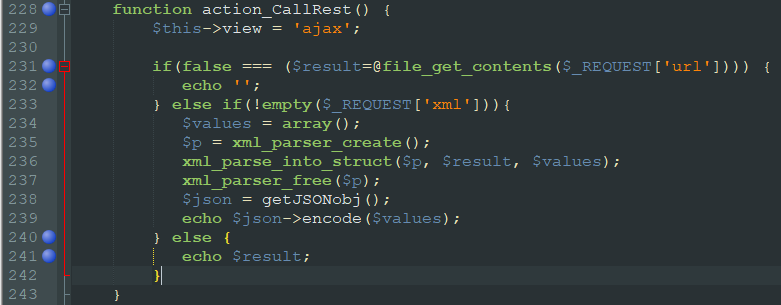
Identified a remote file inclusion in the Connectors module that allows authorized users to use module=CallRest&url= query string to access system files remotely. To address this problem, proper input validation was implemented. (Robin, 2017). On the other hand, several sections in SugarCRM's Documents and Emails module have been discovered as being vulnerable to SQL injection by an authorized user. A remote attacker might read, remove, and update data in the database and gain complete control over the affected application if this vulnerability is successfully exploited.

To avoid such attacks, proper SQL escaping has been added, other than that there is no official solution to address this vulnerability for version 6.5.26 or below. (SugarCRM, 2017)

Detection:

The vulnerable function call could be found in the source code of SugarCE as below.

Path: SugarCE-Full-6.5.26/modules/Connectors/controller.php



ZAP scan results were successfully manipulated 5 hits in the target site using the boolean conditions [Log In AND 1=1 -- ] and [Log In AND 1=2 -- ]. (Appendix ZAP)



### CVE-2018-6308

CVSS Score: 7.5

Vulnerability Type(s): SQL Injection

Description:

During the security audit analysis, DefenseCode ThunderScan application discovered multiple SQL injection vulnerabilities in SugarCRM Community Edition (DefenseCode, 2018). A remote attacker might read, remove, and update data in the database and gain complete control over the affected application if this vulnerability is successfully exploited.

Due to the software being End of Life (EoL), there is no official solution to address this vulnerability for version 6.5.26 or below. (Sugar Club, 2018)

Detection:

The vulnerable function call could be found in the open-source file of SugarCE as below (Matthew, 2018).

Path: SugarCE-Full-6.5.26\modules\Campaigns\Tracker.php



### Not detected explanations

For CVE-2017-14508 to 10, it required an authorized user for the successful exploitation.

For CVE-2018-6308, it required to call specific functions and steps for the successful exploitation which penetration testing tool could not scan by default.

## Cross Site Scripting (XSS)

### CVE-2018-17784

Risk Score: 4.3

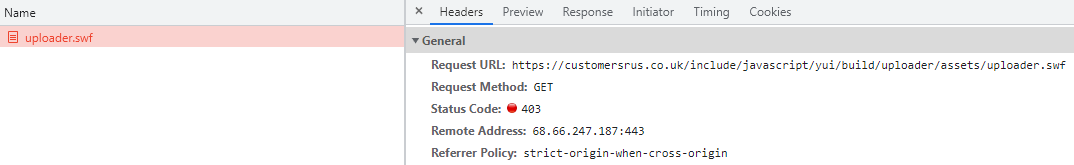
Vulnerability Type(s): SQL Injection

Description:

Multiple vulnerabilities in embedded YUI and FlashCanvas potentially allow an unauthenticated, remote attacker to launch an XSS attack on an affected machine (Exploit Database, 2018).

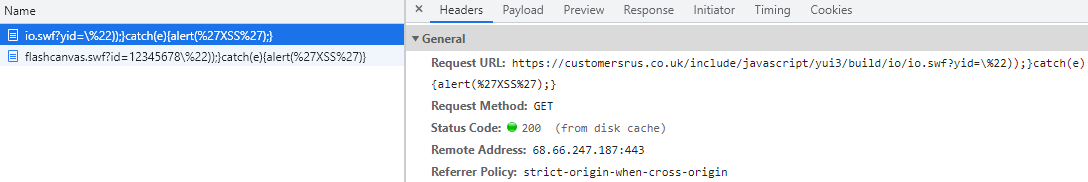
Detection:

Except for uploader.swf file, the vulnerable .swf file can be accessed in the target site as below.

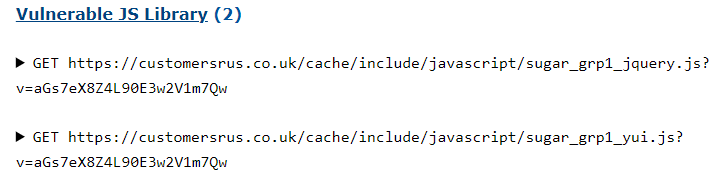
https://customersrus.co.uk/include/javascript/yui/build/uploader/assets/uploader.swf 

https://customersrus.co.uk/include/javascript/yui3/build/io/io.swf

https://customersrus.co.uk/include/SugarCharts/Jit/FlashCanvas/flashcanvas.swf



ZAP scan results identified library jquery, version 1.7.1 is vulnerable. Moreover, misconfigurations were found on Anti-CSRF tokens and HttpOnly Flag which might cause XSS exploits. (Appendix ZAP)







Burp Suite scan results provided similar findings as ZAP. (Appendix Burp Suite)


## Buffer Overflow

Description:

Buffer overflow errors are defined by the overwriting of process memory fragments that should never have been changed, either purposely or unexpectedly. (Common Weakness Enumeration, 2021).

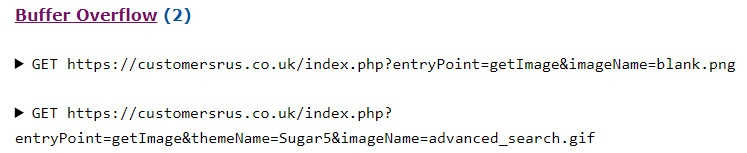
Detection:

The vulnerable files can be accessed in the target site with the below links.

<https://customersrus.co.uk/index.php?entryPoint=getImage&imageName=blank.png>

<https://customersrus.co.uk/index.php?entryPoint=getImage&themeName=Sugar5&imageName=advanced_search.gif>

ZAP scan results detected potential buffer overflow with overflow attack, the script closed the connection and threw a 500 Internal Server Error. (Appendix ZAP)

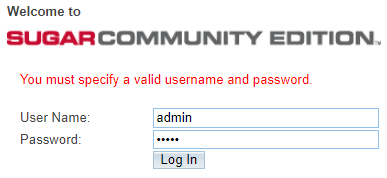


## Brute Force Attack

Description:

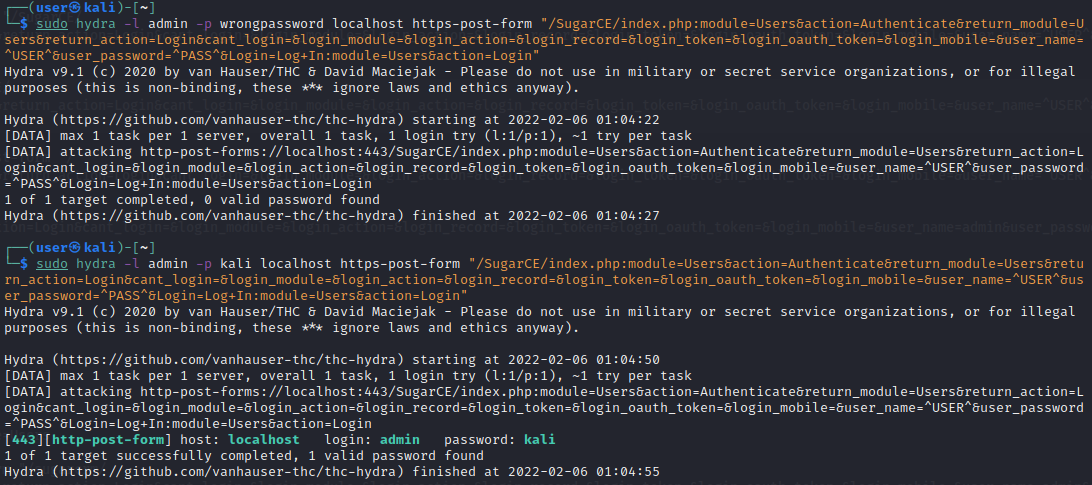
With trial-and-error, guessing login details, encryption keys, or discovering hidden web pages. Try all conceivable combinations in the hopes of the right guess.

The login module does not built-in with account locked out for unsuccessful login attempts in 6.5, it could install a third party’s module for IP address blocking (Lion Solution, N.D.) or upgrade to newer SugarCRM version (SugarCRM, 2020).

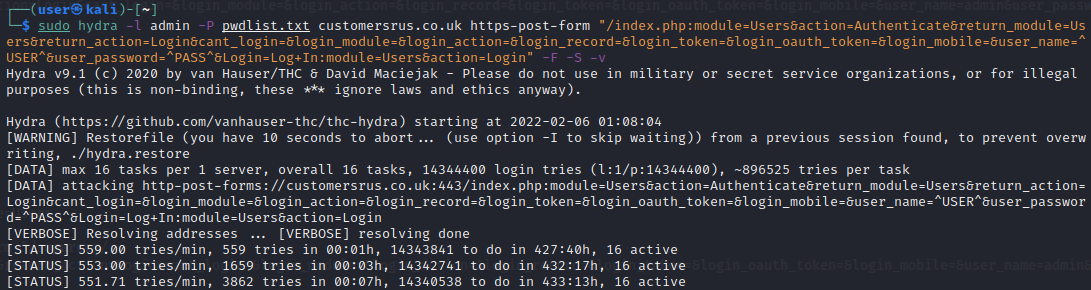


Detection:

Used Hydra performs brute force attack on the testing server to proof of concept (POC), verify command able to validate the correct password.



Perform brute force attack on target site with 3862 tries without blocked.



# References:

Softaculous. (N.D.) SugarCRM. *ERP App*. Available from: https://www.softaculous.com/apps/erp/SugarCRM [Accessed 9 February 2022].

Vulmon Search. (N.D.) Sugarcrm 6.5.26 vulnerabilities and exploits. *Vulmon Search*. Available from: https://vulmon.com/searchpage?q=sugarcrm+6.5.26&sortby=byrelevance [Accessed 9 February 2022].

Matthew, P. (May 6, 2018) SugarCRM-Community-Edition. *Github*. Available from: https://github.com/matthewpoer/SugarCRM-Community-Edition/tree/master/OldFiles [Accessed 9 February 2022].

DefenseCode. (January 23, 2018) SugarCRM Community Edition Multiple SQL Injection Vulnerabilities. *DefenseCode ThunderScan SAST Advisory.* Available from: https://www.defensecode.com/advisories/DC-2018-01-011\_SugarCRM\_Community\_Edition\_Advisory.pdf [Accessed 9 February 2022].

SugarCRM. (August 29, 2017) sugarcrm-sa-2017-006. *Security*. Available from: https://support.sugarcrm.com/Resources/Security/sugarcrm-sa-2017-006/ [Accessed 9 February 2022].

Robin, P. (September 14, 2017) SugarCRM's Security Diet - Multiple Vulnerabilities. *Security*. Available from: https://blog.sonarsource.com/sugarcrm-security-diet-multiple-vulnerabilities/?redirect=rips [Accessed 9 February 2022].

Sugar Club. (Apr 6, 2018) Sugar Community Edition open source project ends. *Sugar News*. Available from: https://sugarclub.sugarcrm.com/engage/b/sugar-news/posts/sugar-community-edition-open-source-project-ends [Accessed 9 February 2022].

Exploit Database. (October 12, 2018) SugarCRM 6.5.26 - Cross-Site Scripting. *Exploits*. Available from: https://www.exploit-db.com/exploits/45594 [Accessed 9 February 2022].

Common Weakness Enumeration. (July 20, 2021) CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'). *CWE List*. Available from: https://cwe.mitre.org/data/definitions/120.html [Accessed 9 February 2022].

Lion Solution. (N.D.) CRM Defender. *Sugar Outfitters*. Available from: https://www.sugaroutfitters.com/addons/crm\_defender [Accessed 9 February 2022].

SugarCRM. (October 8, 2020) Modifying the Unsuccessful Login Lockout Period*. User Login Management.* Available from: https://support.sugarcrm.com/Knowledge\_Base/Password\_Management/Modifying\_the\_Unsuccessful\_Login\_Lockout\_Period/ [Accessed 9 February 2022].