Vulnerability Assessment Report

www.e-commune.org

By

Akila MUTHULAKSHMANAN (Msc. CS)

UdhayaShankar PALANIVEL (M.E. SNS)

Recipients

Name	Title	Company
Adele	Professor	EPITA

Document History

Date	Prepared by	Status
23/05/2018	Akila	Draft Report
25/05/2018	UdhayaShankar	Final Report

Contents

EXECUTIVE SUMMARY

Synthesis

The website *www.e-commune.org* owned by government for small community that allows residential people or chef to access and request for their daily needs. Agent is the one who responsible for managing bills and creating tickets for chef to pay their penalty who miss to pay the bills on time and so on. Visiter can go through the page to know uptodate events going on in the town/city and they need no authentication. Finally admin who have all access to create a page, upload image on server, Database, provide limited access to vister, updating the events and so on.

Scope of the Audit

The assignment was carried out by EPITA master students between the 19th to the 25th of May 2017 with the following goals:

- Identifying security vulnerabilities.
- Providing risk mitigation recommendations for the discovered vulnerabilities.
- Mapping the discovered vulnerabilities to e-commune.com Information policy

The found vulnerability are categoried as mentioned below

Metric	***Skill Level***
Easy	Casual user
Medium	Computer-Savvy Individual
High	Determined Hacker

Vulnerability

Weak Passwords Accepted

Indicators of criticity

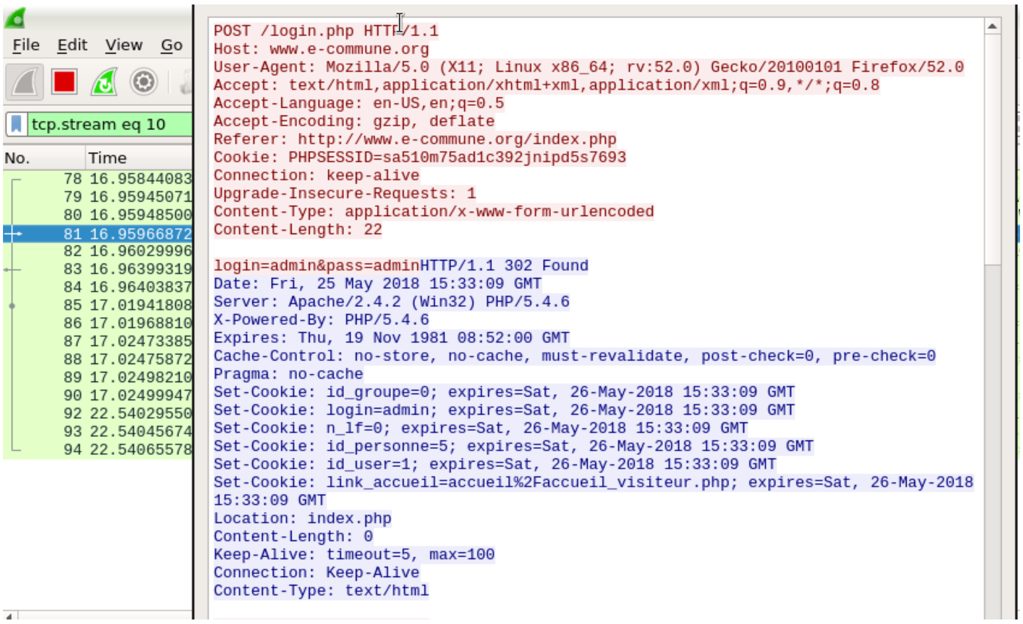
Business Risk	Critical
Exploitation	(Very) Easy
Correction	Easy

Description

Words with simple obfuscation: p@ssw0rd, l33th4x0r, g0ldf1sh, etc., can be tested automatically with little additional effort. For example, a domain administrator password compromised in the DigiNotar attack was reportedly Pr0d@dm1n. Common sequences from a keyboard row: qwerty, 12345, asdfgh, fred, etc.

Exploitation

Hacker, first try out password would be system default credentials. Next, typical passwords that are most likely used by many users. Next try, by running scripts with dictionary list which contains distinct set of usernames and passwords.



```
No.   Time
 78 16.95844083
 79 16.95945071
 80 16.95948500
 81 16.95966872
 82 16.96029996
 83 16.96399319
 84 16.96403837
 85 17.01941808
 86 17.01968810
 87 17.02473385
 88 17.02475872
 89 17.02498210
 90 17.02499947
 92 22.54029550
 93 22.54045674
 94 22.54065578
```

```
POST /login.php HTTP/1.1
Host: www.e-commune.org
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
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
Referer: http://www.e-commune.org/index.php
Cookie: PHPSESSID=sa510m75ad1c392jnipd5s7693
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 22

login=admin&pass=adminHTTP/1.1 302 Found
Date: Fri, 25 May 2018 15:33:09 GMT
Server: Apache/2.4.2 (Win32) PHP/5.4.6
X-Powered-By: PHP/5.4.6
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: id_groupe=0; expires=Sat, 26-May-2018 15:33:09 GMT
Set-Cookie: login=admin; expires=Sat, 26-May-2018 15:33:09 GMT
Set-Cookie: n_lf=0; expires=Sat, 26-May-2018 15:33:09 GMT
Set-Cookie: id_personne=5; expires=Sat, 26-May-2018 15:33:09 GMT
Set-Cookie: id_user=1; expires=Sat, 26-May-2018 15:33:09 GMT
Set-Cookie: link_accueil=accueil%2Faccueil_visiteur.php; expires=Sat, 26-May-2018
15:33:09 GMT
Location: index.php
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
```

It accepts username and password even if they are same and this leads for brute force attack and SQL injection is possible can crack passwords and so on ways to crack the week password.

Recommandation

Obligate to use hard password which should contain (atlease one) upper-case, lower-case, (atleast one) number and (atleast one) special character and also minimum length of the password should be 8 character. Avoid using the same password to all websites.

Technical Information Leakage

Indicators of criticity

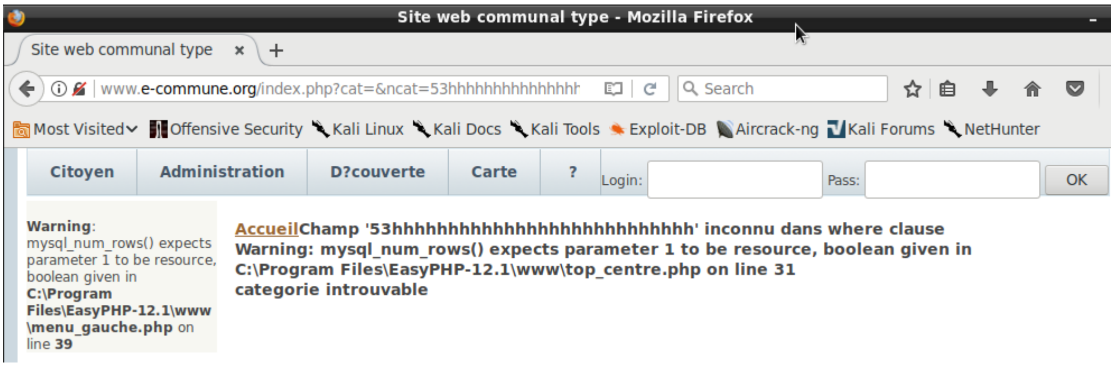
Business Risk	Medium
Exploitation	Easy
Correction	Medium

Description

If we pass any invalid parameter in url, error message gave few details such as where the website actually running either in server or remote machine (C:\Program Files\...), these technical information should not leak to users, only to developers.

Exploitation

Parameter passed in url should be validate from server side, if not, it would easy to exploit by passing random varibles.



www.e-commune.org/index.php?cat=&ncat=53hhhhhhhhhhhhhhh

Warning: mysql_num_rows() expects parameter 1 to be resource, boolean given in C:\Program Files\EasyPHP-12.1\www\menu_gauche.php on line 39

AccueilChamp '53hhhhhhhhhhhhhhhhhhhhhhhhhh' inconnu dans where clause
Warning: mysql_num_rows() expects parameter 1 to be resource, boolean given in C:\Program Files\EasyPHP-12.1\www\top_centre.php on line 31
categorie introuvable

For example, usually id are integers in database, if we didn’t valide variable ‘id’ from backend then passing any undefined value may produce errors which gives information or otherwords leaking data.

Recommandation

Validate all passing parameters through GET or POST requests.

Cross-Site Scripting (XSS)

Indicators of criticity

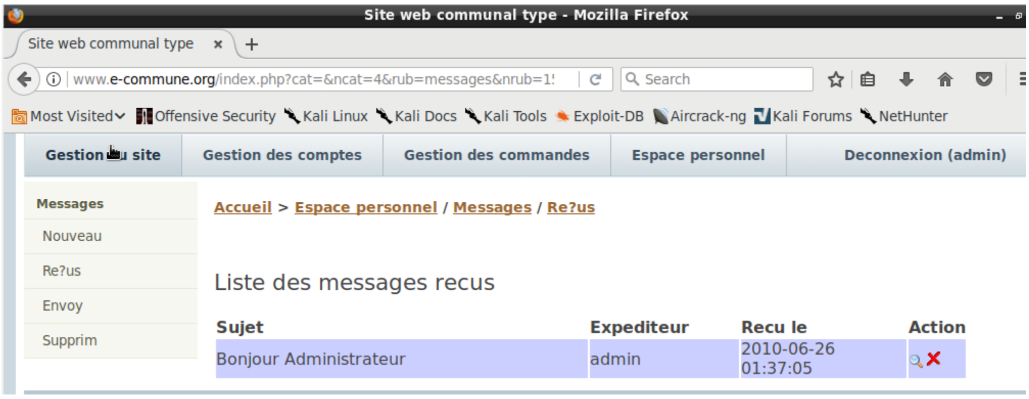
Business Risk	Medium
Exploitation	Medium
Correction	Hard

Description

Sending mail to admin which looks normal, when admin click anywhere that redirect to someother webpage that imitate the actual page and collect all data without user knowledge. This is termed as phishing .

Exploitation

The same phishing is the way to exploit this kinda of vulnerability.



Liste des messages recus

Sujet	Expediteur	Recu le	Action
Bonjour Administrateur	admin	2010-06-26 01:37:05	🔍 ✗

<!--redirect the victim to arbirary website-->
<script>document.location=http://www.e-commune-phishing.org</script>
<!--pop a window saying "here is xss"-->
<script>alert('here is xss')</script>

Recommandation

Using php functions *htmlspecialchars() and htmlentities()* that filter the script which prevent the user from redirecting.