

VAPT REPORT FOR E-COMMERCE WEBSITE. LIFESTYLE STORE : A WEB BASED APPLICATION

Report by: Arjun shetty



Introduction:

- This is the vulnerability assessment and penetration testing (VAPT) report for “Lifestyle Store”.
- I have reported all the vulnerabilities found on this store
- I have also provided business risks and expert recommendations to tackle those vulnerabilities.

Security Status: **EXTREMELY CRITICAL**

SQLi : Hackers can steal all records from the databases of the website.

Hackers can take complete control of the website including view, edit, add or delete files and folders via shell upload.

IDOR : Hackers can extract mobile numbers of all customers using user-id.

Hackers can change the source code and can upload any malicious code, **phishing** etc. in the website via shell upload.

XSS : Hackers can trick users to click on malicious pop up links and steal information via cross-site-scripting.

Vulnerability Statistics:

CRITICAL	SEVERE	MODERATE	LOW
12	7	3	3

Vulnerabilities Found:

<u>SEVERITY</u>	<u>VULNERABILITY</u>
MODERATE	CLIENT SIDE FILTER BYPASS
SEVERE	SERVER MISCONFIGURATION
CRITICAL	PII LEAKAGE
CRITICAL	OPEN REDIRECTION
SEVERE	CSRF
CRITICAL	SQL INJECTION
SEVERE	STORED AND REFLECTED XSS
CRITICAL	IDOR
SEVERE	RATE LIMITING FLAW
CRITICAL	INSECURE FILE UPLOAD

<u>COUNT</u>
2
2
4
2
2
2
2
3
4
2

SQL Injection

CRITICAL



Below mentioned URL is vulnerable to SQL injection attack.

Relevant URL :

`http://52.66.203.250/products.php?cat=1`

Affected Parameters :

category (GET)

Payload:

`cat=1'`

URL Vulnerable to SQLi:

URL #1 :

`http://52.66.203.250/products.php?cat=4'`

PAYLOAD:

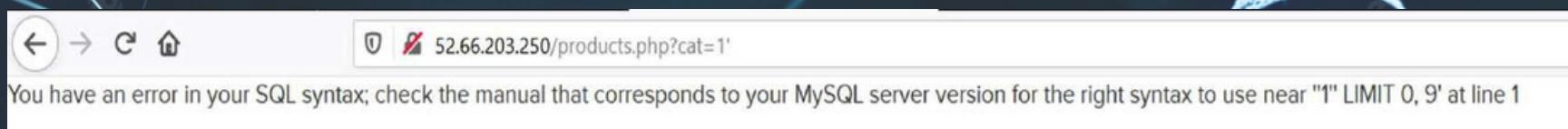
`cat=1'`

Observations :

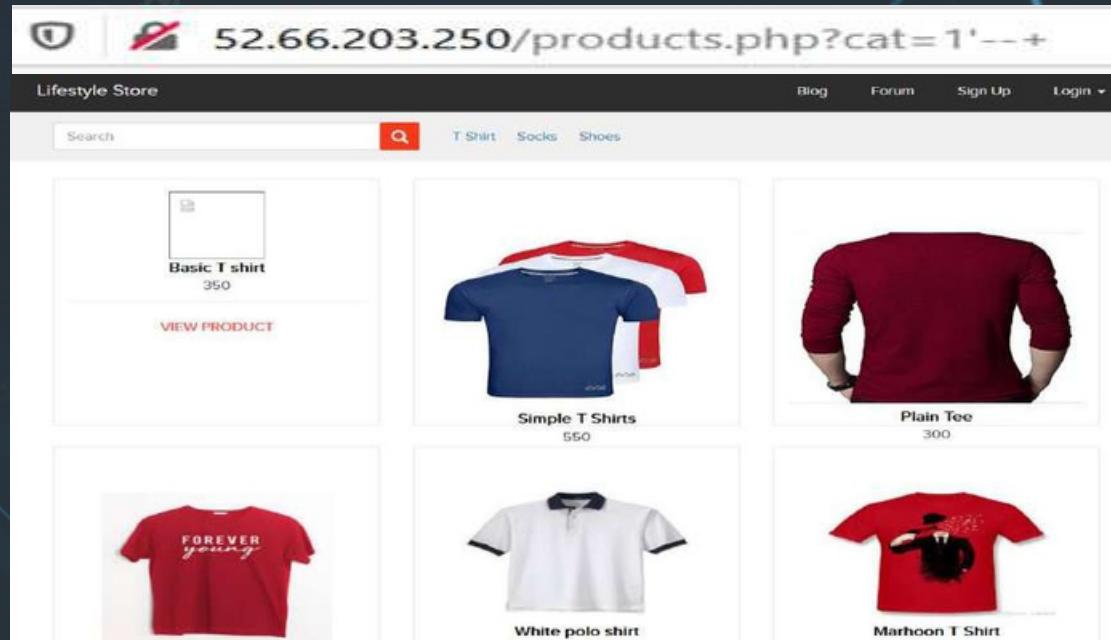
the following observation are being made related to
the vulnerabilities of the website

- Go to the categories option from the home page of the website and click on “T-Shirt”, “Socks” or “Shoes”, to get into the URL, you will see products as per the option you have chosen but notice the get parameter in the URL.

When you apply a single quote (') in the get parameter, you get a MySQL error.



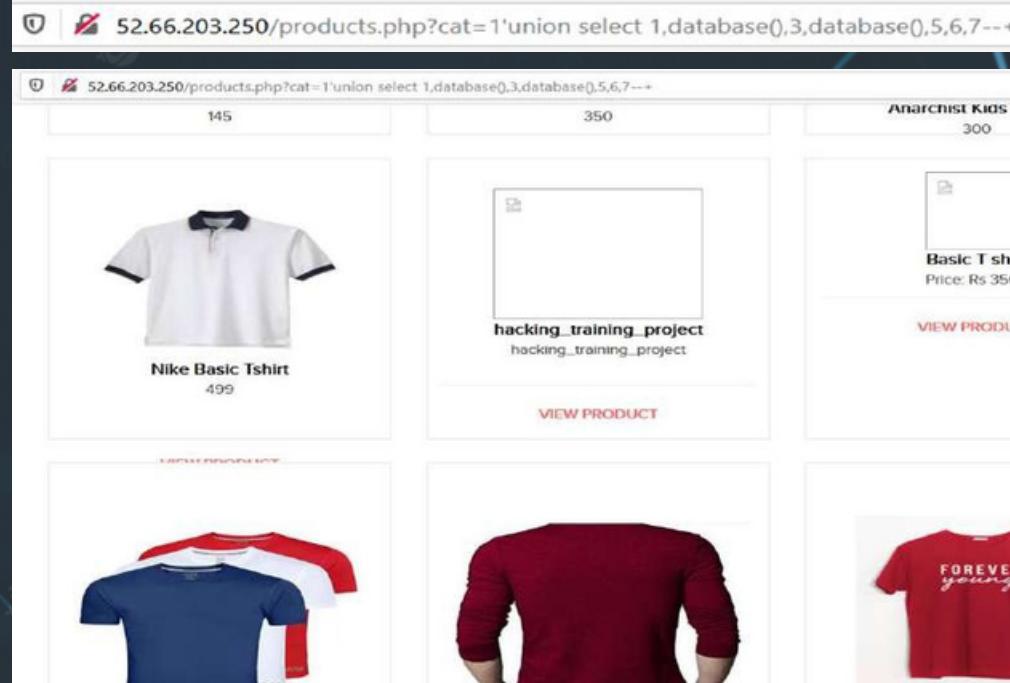
To confirm the MySQL error, you can put “--+” in the end of the parameter, and the page loads in its original format, this confirms the error.



Proof Of Concept:

Following Slides Have The Proof and Risks Of The Proposed Vulnerability.

- Attacker can execute commands as shown below to get critical information, here we have used the payload to find the name of the database of MySQL.



Proof Of Concept :

No. Of Databases : 2

- Information_Schema
- Hacking_training_project

No. Of Tables in “Hacking_training_Project” : 9

- brands
- cart_items
- categories
- customers
- orders
- product_reviews
- products
- users
- order_items

Business Impact:

Using this vulnerability, the attacker can execute arbitrary SQL commands on Lifestyle Store's server and gain complete access to the internal database, which also makes all customer data inside it visible.

This is the screenshot of users table which shows user credentials being leaked.

name	password
admin	\$2y\$10\$xkmdvrxsCxqdywsrDx5YSe1NAwX.Zpq2nQmaTCovH4CFssxgyJTk1
Donald Duck	\$2y\$10\$PM.7nbSP5FMa1dxIM/S3s./p5xr6GtKvJry7ysJtxokBqoJURAHsO
Brutus	\$2y\$10\$xkmdvrxsCxqdywsrDx5YSe1NAwX./pQZnQmaTCovH4CFssxgyJTk1
Chandan	\$2y\$10\$cZBEIrghxvdvT1hwu1ivuFELe03rR.Gicdp03Njrls0VeiOKLVDa
Popeye the sailor man	\$2y\$10\$Fkv1RfwYTioow0w2caztAQuXVnhGAUjt/If/yTqkNPc5zTrsVm7EeC
Radhika	\$2y\$10\$RYxNhoYv/G4g70tFwpqYae xvHi8rF6Xxui8kT1wtrf qhTutCA8JC
Nandan	\$2y\$10\$G.cRNLME1G79ZFxE1Hg.R.o95334U0xmzu4.9MqzR5614ucwnk59K
Murthy Adapa	\$2y\$10\$mzQGzD4sdsj2Eu npcioe4ek18c1Abs0T2P1a1P6ev1DPR.11uubDG
john Albert	\$2y\$10\$Ghdb8h1x6xjPMY12Gz1vD07Y3en97u1/.oxTZLmYqB6F18FBgevg
Bob	\$2y\$10\$kiuikn3HPFbuyTtk757LNurxzqCOLX3emGy0/ux16j0og37dCGKLq
Jack	\$2y\$10\$z/nyN1kRJ76m9ItMz4N570eRx6Gkq19N/UBcJ45zeO7eM7N4pTHu
Bulla Boy	\$2y\$10\$HT5oiRMetqaz7xGZPE9s2.Mk1yF4PnYDjHCwbm2w/xuKpjEEI/zjG
hunter	\$2y\$10\$spB3U9iFkwBgsb12AkBp1EeIBdh1Yfwy9y.xv23q12gGbMCyn7N3g2
asd	\$2y\$10\$At5pFZnRwpjCD/yNnJwDL.L3Cc4cv0w8Q/weHmwzBFqvIkBQFpcF2
acdc	\$2y\$10\$J50B78.gpuculTwpHwbcPedycain.Yi.tsTLyQtK17FzdSpmiRRbi

Recommendations:

1. Prepared Statements : Use SQL prepared statements available in all web development languages and frameworks to avoid attacker being able to modify SQL query.
2. Do not run Database Service as admin/rootuser.
3. Disable/remove default accounts, passwords.
4. Character Encoding : Convert the simple codes to different characters like ‘~’/’^’. It is also suggested to follow HTML and other encodings.

Below mentioned page has a login form that allows login via OTP that can be brute forced.

Relevant URL :

- <http://52.66.203.250/login/admin.php>

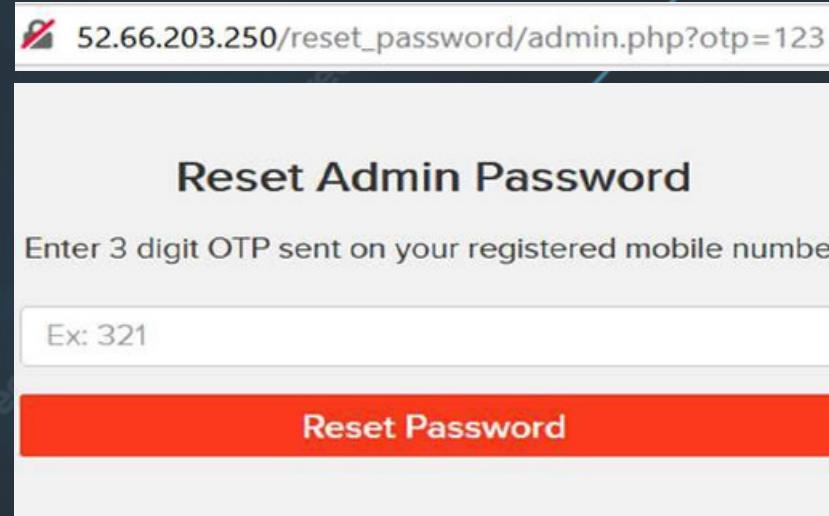
Affected Parameters :

- OTP (POST)

Observations :

the following observations are being made related to the vulnerabilities of the website

Navigate to <http://52.66.203.250/login/admin.php> you will see a “forgot password” hyperlink which asks for OTP which is sent to victim’s mobile number ,input any anonymous 3 digit OTP and intercept the request with burp suite.



52.66.203.250/reset_password/admin.php?otp=123

Reset Admin Password

Enter 3 digit OTP sent on your registered mobile number

Ex: 321

Reset Password



The request below will be generated in burp suite using GET parameter.

```
GET /reset_password/admin.php?otp=123 HTTP/1.1
Host: 52.66.203.250
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0) Geck
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://52.66.203.250/reset_password/admin.php?otp=123
Cookie: key=99ED5631-C072-64B1-BF30-655746AE1719; PHPSESSID=mflois
Upgrade-Insecure-Requests: 1
```

We'll brute force by getting all combination of 3 digit OTP's and input the correct one to bypass.

Attack type: Sniper

```
1 GET /reset_password/admin.php?otp=$123$ HTTP/1.1
2 Host: 52.66.203.250
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0) Gecko/20100101 Firefox/77.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://52.66.203.250/reset_password/admin.php?otp=123
```

Business Impact:

A hacker can gain complete access to admin account just by brute-forcing due to rate limiting flaw as a hacker can attempt as many times as he wants as there is no bounds in number of trials.

- Attacker can log in can then carry out actions on behalf of the victim which could lead to serious financial loss to him/her.

Recommendations:

Take the following precautions :

1. Use rate limiting checks on the number of times the OTP request is generated.
2. OTP should be at least of 6 digits, a 3 digit OTP can be guessed or brute-forced easily.
3. OTP should expire in a particular time like 2 minutes or 5 minutes to make authorization process more secure.

The “My Orders” section shows an Insecure Direct Object Reference (IDOR).

This allows hackers to get access to any customer’s order details and more.

Relevant URL :

- <http://52.66.203.250/orders/orders.php?customer=2>
- http://52.66.203.250/products/details.php?p_id=7.

Affected Parameters

- Customer Data (GET)

Observations :

the following observation are being made related to
the vulnerabilities of the website

Login to your account and go to “My Orders” section, you’ll see a GET parameter as shown below, “customer=2”.

Change the customer number to any random number, and we get the details of the new customer ID.

The screenshot shows a web browser window with the URL 52.66.203.250/orders/orders.php?customer=2. The page is titled "My Orders".

Order Id: 7B1D17C63974

PRODUCTS:

- Adidas Socks
- White polo shirt

Total: INR 595

SHIPPING DETAILS:

Name - Donald Duck
Email - donald@lifestylestore.com
Phone - 9489625136
Address - B-34/ the duck lane, Disneyland

PAYMENT MODE: Cash on delivery

Order placed on : 2019-02-15 15:29:49 **Status:** DELIVERED

Business Impact:

This vulnerability can be exploited by hackers to carry out targeted phishing attacks on the users and the information can also be sold to the black-market.

As there is no rate limiting checks, attacker can brute-force the “user_id” for all possible values and get bill information of each and every user of the organization resulting in a massive information leakage.

Recommendations:

Take the following precautions :

- Make sure user only have the access to self data.
- Use proper rate limiting checks on the number of request comes from a single user in a small amount of time.
- Implement proper authentication and authorization checks to make sure that the user has permission to the data he/she is requesting

These parameters are vulnerable to XSS.

Relevant URL :

13.234.113.207/products/details.php?p_id=2

Affected Parameters :

Comment / Review Box

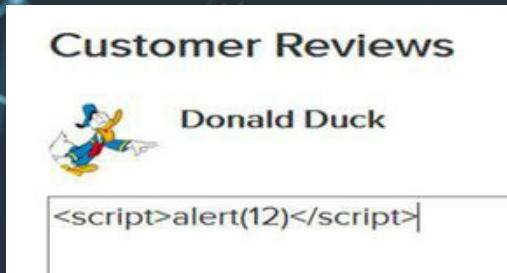
Payload :

<script>alert(1)</script>

Observations :

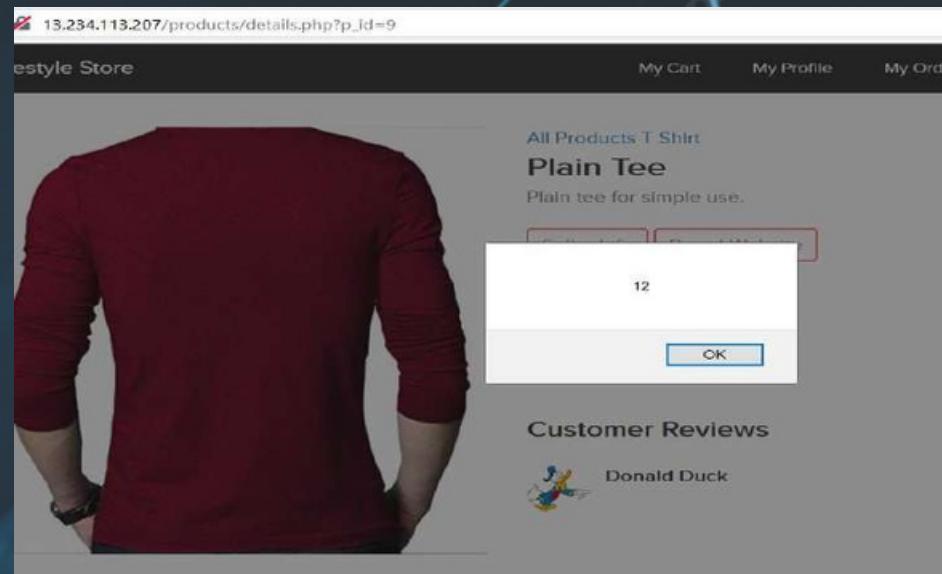
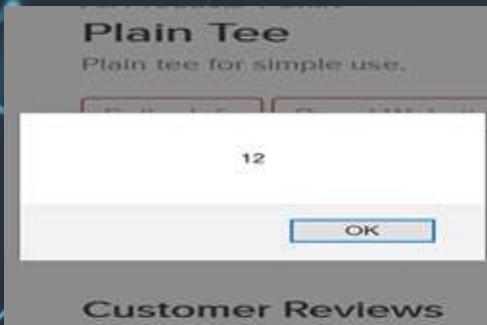
the following observation are being made related to
the vulnerabilities of the website

- We have an issue, in the review / comment section.
- Inject payload <script>alert(12)</script>



A screenshot of a product page for a "Plain Tee". The product image shows a person wearing a red long-sleeved t-shirt. To the right of the image, the product details are listed: "All Products T Shirt", "Plain Tee", "Plain tee for simple use.", "Seller Info", "Brand Website", and the price "INR 300/-". Below the product details is a "Add To cart" button. Further down, there is a "Customer Reviews" section. It shows a review by "Donald Duck" with the same injected payload: <script>alert(12)</script>. A "POST" button is visible at the bottom right of the review area.

An alert is registered in the pop-up
when submitting.



Business Impact:

- As the attacker can inject arbitrary HTML, CSS and JavaScript via the URL, he/she can put any content on the page like phishing pages, and can even host explicit content that could compromise the reputation of the organization.
- When the attacker sends the link with the payload to the victim, the victim sees a modified content on the website. As the user trusts the website, he/she will trust the content.

Recommendations:

Take the following precautions :

- Secure the user input by blocking all the input that isn't made by the developer.
- Encode the HTML / CSS special characters and codes in an encoded form before printing them on the website.

This URL is vulnerable.

Relevant URL :

- <http://35.154.158.143/robots.txt>

Observations :

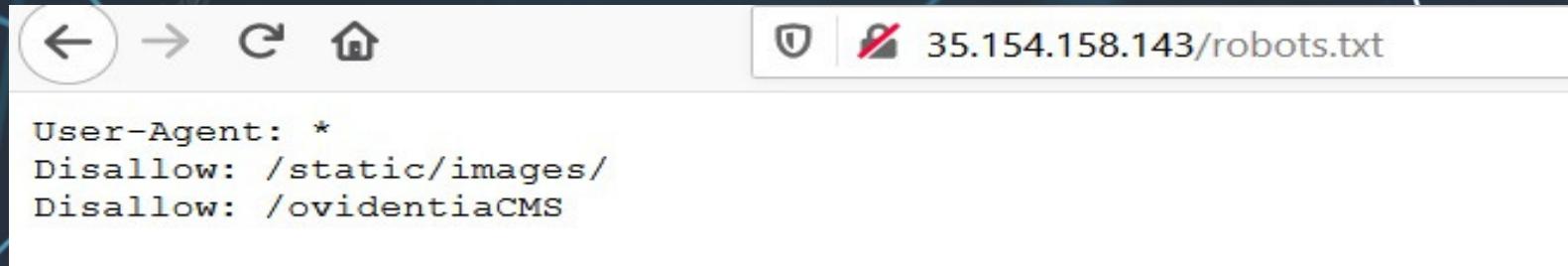
the following observation are being made related to
the vulnerabilities of the website

Go to <http://35.154.158.143/robots.txt>

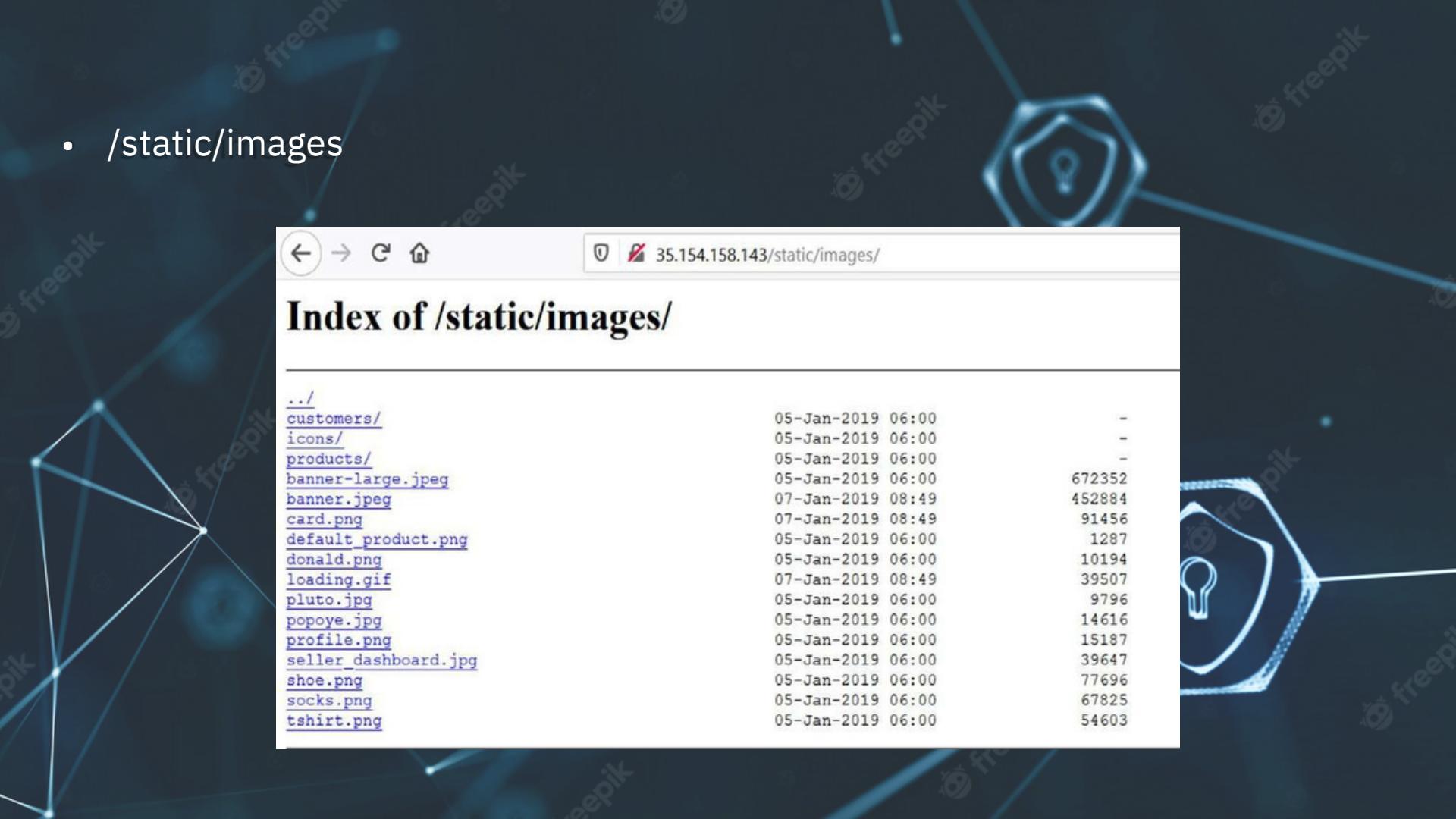
Here, we can see a complete list and directories of the customers, images of products and all the products-page info.

We can also see the administrator directory.

This has a weak password flaw in Ovidentia CMS, which lets an attacker access the administrator panel without much trials.



- /static/images



The screenshot shows a file listing for the directory `/static/images/`. The browser address bar indicates the URL is `35.154.158.143/static/images/`.

..		
customers/	05-Jan-2019 06:00	-
icons/	05-Jan-2019 06:00	-
products/	05-Jan-2019 06:00	-
banner-large.jpeg	05-Jan-2019 06:00	672352
banner.jpeg	07-Jan-2019 08:49	452884
card.png	07-Jan-2019 08:49	91456
default_product.png	05-Jan-2019 06:00	1287
donald.png	05-Jan-2019 06:00	10194
loading.gif	07-Jan-2019 08:49	39507
pluto.jpg	05-Jan-2019 06:00	9796
popoye.jpg	05-Jan-2019 06:00	14616
profile.png	05-Jan-2019 06:00	15187
seller_dashboard.jpg	05-Jan-2019 06:00	39647
shoe.png	05-Jan-2019 06:00	77696
socks.png	05-Jan-2019 06:00	67825
tshirt.png	05-Jan-2019 06:00	54603

- /ovidentiaCMS/

The screenshot shows a web browser window displaying the Ovidentia CMS homepage at the URL 35.154.158.143/ovidentiaCMS/. The page has a light blue header with the Ovidentia logo and navigation links for Accueil and Utilisateur.

Ovidentia

Ovidentia est un outil permettant de publier avec une grande aisance et très rapidement un portal intranet, extranet ou internet. En commençant par ses fonctions de système de gestion de contenus (CMS) telles que :

- publier des informations (éditeur WYSIWYG, arborescence d'articles, catégorisation),
- mise en place de circuits d'approbations (permettant de définir des schémas d'approbations, du plus simple au plus complexe),
- Un moteur de recherche,
- ...

— **OVIDENTIA** intègre aussi de puissants outils de travail collaboratif :

- Gestion des utilisateurs, agendas partagés, notifications, annuaires,
- Un gestionnaire de fichiers (avec gestion du versioning)
- Forums,
- FAQ,
- Gestionnaire de congés (avec circuit de validation)
- Possibilité de gérer des groupes avec administration déléguée (dans un certain périmètre et pour certaines fonctions uniquement)
- ...

Son architecture, complètement modulaire, permet d'y installer des modules développés par la communauté **OVIDENTIA**.

Pour plus d'informations : <http://www.ovidentia.org>

Les prochains événements

Ovidentia.org

Nouvel environnement de mise à disposition des modules et du noyau

Afin de faciliter la mise à disposition des dernières versions des modules et du noyau (stable et développement), un "store applicatif" dédié à Ovidentia vient d'être intégré.

10/03/2017 - 17:34

Modules

26/03 -

LibFileManagement (0.4.2)

13/03 -

orgchart (0.13.10)

28/02 -

Business Impact:

- The hacker can get all the information on the CMS and also get the privileges to tackle with the administrator login credentials.
- A malicious hacker can take important information from seller point of view and what products every seller is selling at price and also the information of users.

Recommendations:

Take the following precautions :

1. • Disable all the directory listings.
2. • Include a index.html in all folders with default messages.

Remove all the default passwords and add your own new strong passwords which must have a special character and at least 8 character long for maximum security

Below mentioned URL LEAKS Critical information via PII leakage.

Relevant URL :

<http://35.154.158.143/static/images/uploads/products/2socks.jpeg>

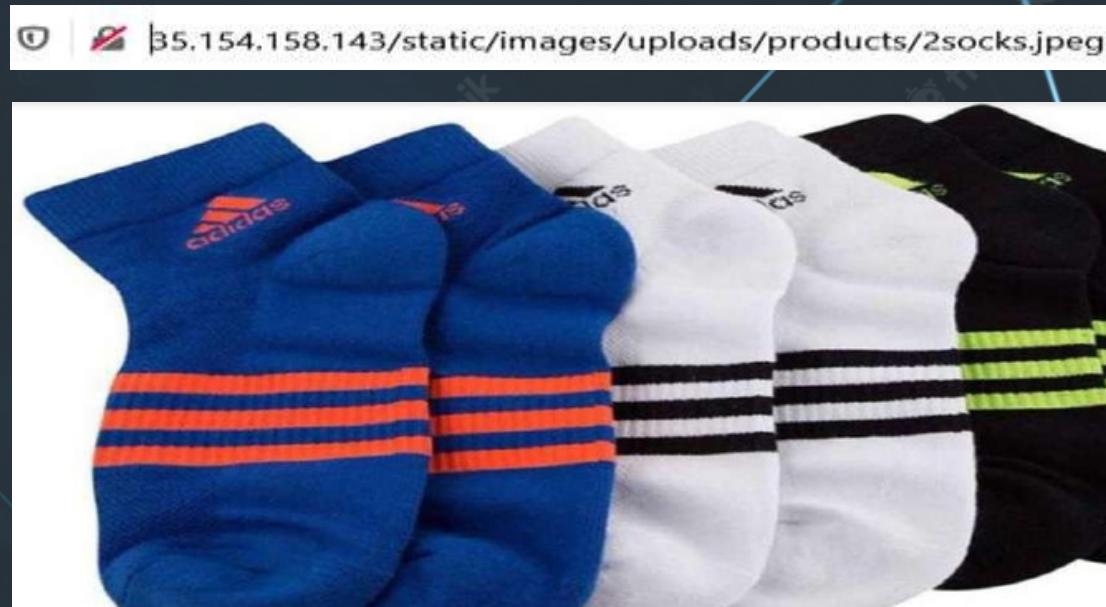
Affected Parameters :

IMAGE (every image after “products/”)

Observations :

the following observation are being made related to
the vulnerabilities of the website

Go to <http://35.154.158.143/products.php> and drag any drop product image in a new tab, the following page will look like the one shown below with the image of the product you chose.



Now, we remove the image name, i.e."2socks.jpeg" in our case and hit enter, the following page with details will be shown.



The screenshot shows a web browser window with the URL `35.154.158.143/static/images/uploads/products/`. The page displays a list of files with their names and last modified dates. The file names include various extensions like jpg, jpeg, php, and png. The last modified dates range from February 2019 to March 2019. The file names are:

File Name	Last Modified	Size
115.jpg	15-Feb-2019 08:45	834
12.jpg	15-Feb-2019 08:16	8457
13.jpg	15-Feb-2019 08:17	9101
14.jpg	15-Feb-2019 08:19	50523
15.jpg	15-Feb-2019 08:18	894
2.jpg	15-Feb-2019 07:59	3946
200.jpg	15-Feb-2019 08:48	1152
202.jpg	15-Feb-2019 08:51	787
203.jpg	15-Feb-2019 08:52	12338
204.jpg	15-Feb-2019 08:53	610
2socks.jpeg	15-Feb-2019 07:44	4174
3.jpg	15-Feb-2019 08:04	872
4.jpg	15-Feb-2019 08:05	473
5.jpg	15-Feb-2019 08:06	934
51BYEKENSKL.. SX. UX. SY. UX_.jpg	15-Feb-2019 07:55	3467
SlrPlAnz8GL.jpg	15-Feb-2019 07:52	3599
6.jpg	15-Feb-2019 08:07	453
61W68b5cf+L. UX679 .jpg	15-Feb-2019 07:52	3272
8.jpg	15-Feb-2019 08:08	804
9.jpg	15-Feb-2019 08:08	867
Johnny-Walker-Facebook-Covers-1369.jpeg	14-Feb-2019 12:30	2533
a.html	08-Mar-2019 23:27	6
a.jpg	09-Mar-2019 12:59	5
ad.jpeg	18-Feb-2019 10:15	259
banner-large.jpeg	05-Jan-2019 06:00	67235
blue.jpeg	15-Feb-2019 08:30	367
c99.php	18-Feb-2019 06:35	66577
crews.jpeg	15-Feb-2019 08:19	210
default_product.png	05-Jan-2019 06:00	120
donald.png	05-Jan-2019 06:00	1019
free-adisks9099-adidas-original-imaf4c22sq5bnvz...>fs.jpeg	15-Feb-2019 07:40	6358
nike.jpeg	15-Feb-2019 08:01	297
og_image.png	15-Feb-2019 07:54	3953
popeye.jpg	05-Jan-2019 12:00	7509
pumasocks.jpeg	05-Jan-2019 06:00	1461
r57.php	15-Feb-2019 07:45	4194
rebook.jpeg	18-Feb-2019 06:25	61239
reebok.jpeg	15-Feb-2019 07:46	4110
s1.jpg	15-Feb-2019 07:53	4748
s2.jpg	15-Feb-2019 08:00	1034
seasocks.jpeg	15-Feb-2019 08:00	719
shell.php	15-Feb-2019 08:17	1014
	14-Feb-2019 12:38	771
	03-Mar-2019 08:48	3

Business Impact:

- A hacker can gain access to the shell application and various other html files which has been shown in the listings.
- It also has a weak-password flaw.
- A hacker can get access to the shell and upload his own malicious codes to make the trusted site a hackers room for phishing and tricking users. This will result in defamation of the website.

Recommendations:

Take the following precautions :

- Enable 2-factor authentication for sensitive data, and also use stronger passwords of at least 8 characters of different types.
- Find all PII stored, and encrypt them with various techniques and also disable all the listings.

Below mentioned URL has a major development flaw , as it redirects to password reset link without authentication.

Relevant URL :

http://35.154.158.143/reset_password/customer.php

Affected Parameters :

Password Reset

Observations :

the following observation are being made related to
the vulnerabilities of the website

- After adding any username , click “forgot your password” and then input the used username and click “reset password”. We’ll see the page like this, click send.

35.154.158.143/reset_password/customer.php?username=Donal234

Reset Customer Password

Your new password will be sent to your email address

Send

When you click send you are directed to a page like this due to development/authentication error, click "click here" button and'll be redirected to change the password of the customer.



The screenshot shows a browser window with the URL `35.154.158.143/reset_password/customer.php?username=Donal234`. The page displays a PHPMailer exception message:

```
string(20) "hackinglab2@zoho.com" object[PHPMailer\PHPMailer\Exception]#6 (7) { ["message":protected]=> string(35) "SMTP Error: Could not authenticate." ["string":"Exception":private]=> string(0) "" ["code":protected]=> int(0) ["file":protected]=> string(69) "/var/www/hacking_project/vendor/phpmailer/src/PHPMailer.php" ["line":protected]=> int(1960) ["trace":"Exception":private]=> array(4) { [0]=> array(6) { ["file"]=> string(69) "/var/www/hacking_project/vendor/phpmailer/phpmailer/src/PHPMailer.php" ["line"]=> int(1774) ["function"]=> string(11) "smtpConnect" ["class"]=> string(29) "PHPMailer\PHPMailer\PHPMailer" ["type"]=> string(2) ">" ["args"]=> array(1) { [0]=> array(0) {} } [1]=> array(6) { ["file"]=> string(69) "/var/www/hacking_project/vendor/phpmailer/phpmailer/src/PHPMailer.php" ["line"]=> int(1516) ["function"]=> string(8) "smtpSend" ["class"]=> string(29) "PHPMailer\PHPMailer\PHPMailer" ["type"]=> string(2) ">" ["args"]=> array(2) { [0]=> string(482) "Date: Fri, 3 Jul 2020 17:06:47 +0530 To: donald@lifestylestore.com From: Hackinglab Reply-To: No Reply Subject: Password reset request Message-ID: X-Mailer: PHPMailer 6.0.6 (https://github.com/PHPMailer/PHPMailer) MIME-Version: 1.0 Content-Type: multipart/alternative; boundary="b1_qVCgIPgGXOnG8nNnxkZXFrQ9qsUSE6IGhVmRBtlkQ" Content-Transfer-Encoding: 8bit" [1]=> string(581) "This is a multi-part message in MIME format. --b1_qVCgIPgGXOnG8nNnxkZXFrQ9qsUSE6IGhVmRBtlkQ Content-Type: text/plain; charset=us-ascii Copy and paste this url http://35.154.158.143/reset_password/verify.php?key=7852255566669996f52434991684 in browsers address bar to reset your password --b1_qVCgIPgGXOnG8nNnxkZXFrQ9qsUSE6IGhVmRBtlkQ Content-Type: text/html; charset=us-ascii Click here to reset your password --b1_qVCgIPgGXOnG8nNnxkZXFrQ9qsUSE6IGhVmRBtlkQ" } [2]=> array(6) { ["file"]=> string(69) "/var/www/hacking_project/vendor/phpmailer/phpmailer/src/PHPMailer.php" ["line"]=> int(1352) ["function"]=> string(8) "postSend" ["class"]=> string(29) "PHPMailer\PHPMailer\PHPMailer" ["type"]=> string(2) ">" ["args"]=> array(0) {} } [3]=> array(6) { ["file"]=> string(52) "/var/www/hacking_project/reset_password/customer.php" ["line"]=> int(51) ["function"]=> string(4) "send" ["class"]=> string(29) "PHPMailer\PHPMailer\PHPMailer" ["type"]=> string(2) ">" ["args"]=> array(0) {} } [4]=> array(1) { ["previous":"Exception":private]=> NULL }
```

#4

- You'll be redirected to change password of the customer id ,and you'll be automatically logged in to that customer's account even if you don't change the password, you can change the password for completely takeover the customer id.

The screenshot shows a web browser window with the URL `35.154.158.143/profile/change_password.php`. The page title is "Lifestyle Store" and the main heading is "Change Password". There are two input fields: "New Password" and "Confirm Password", both currently empty. Below these fields is a large red button labeled "UPDATE".

Lifestyle Store

Change Password

New Password

Confirm Password

UPDATE

Business Impact:

- The impact on the business is high, as a hacker can get access to every user in the website and can login and perform tasks for his benefits as can also make the site vulnerable for security of customers.
- This will result in the defamation of the website as the users trust it.

Recommendations:

Take the following precautions :

- Better authentication should be provided and re-direction site must be re-checked before action.
- There must be a proper authorization access.



Multiple vulnerabilities found in blog site

(PII leakage , temporary XSS and more)

(CRITICAL)

Below are the affected parameters.

URL of the Blog Site : <http://15.206.75.142/wondercms/>

Relevant URL :

- <http://15.206.75.142/wondercms/files/b374kmini.php>

Affected Parameters :

- File Upload (POST)

Relevant URL :

- <http://15.206.75.142/wondercms/home>

Affected Parameters :

- Files (GET)

Relevant URL :

- <http://13.235.0.176/wondercms/files/minisell.php>

Affected Parameters :

- Shell Upload

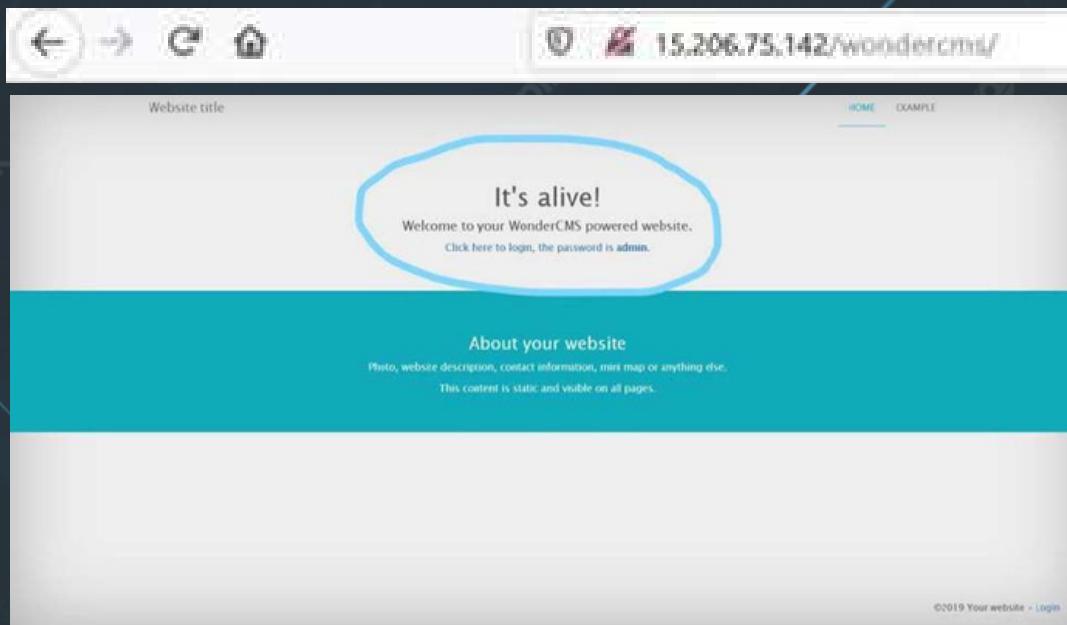
Go to <http://35.154.158.143/login/customer.php> and you will see names of top customers ,as shown below, take note of any username. ,



Observations :

the following observations are being made related to
the vulnerabilities of the website

At the front page of the blog site we can directly find the login option, that says “click here to login, the password is admin” by clicking on it, it will redirect us to the login page where just by entering ‘admin’ as password one can get access to the admin account of this site.



When we log-in as the admin ,at the first page of the site we can see some text written as “It’s alive !” if we click on it , the html codes just starts running.

A hacker can easily make changes and can use the page as his/her phishing portal . This is a classic example of temporary XSS.

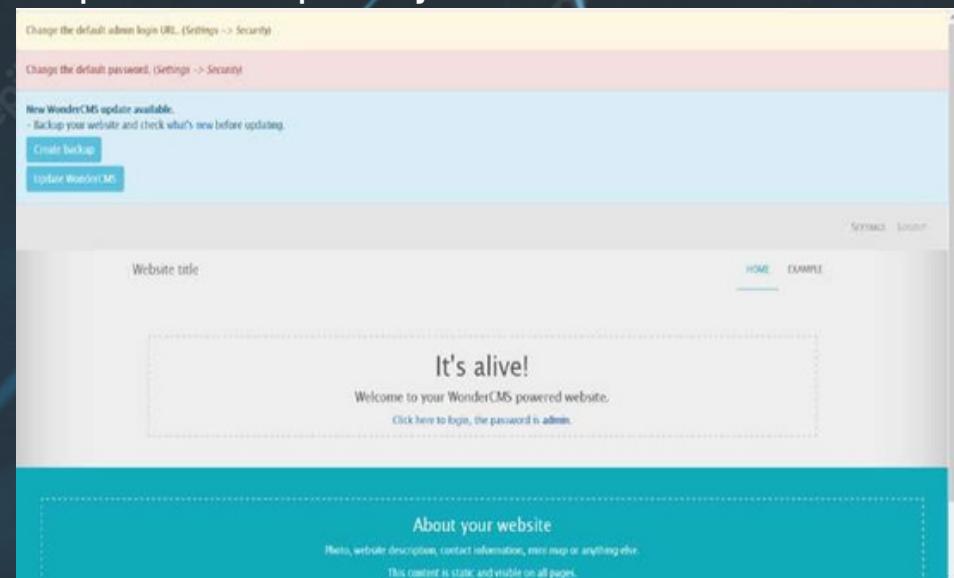
Change the default admin login URL. (*Settings -> Security*)

Change the default password. (*Settings -> Security*)

New WonderCMS update available.
- Backup your website and check what's new before updating.

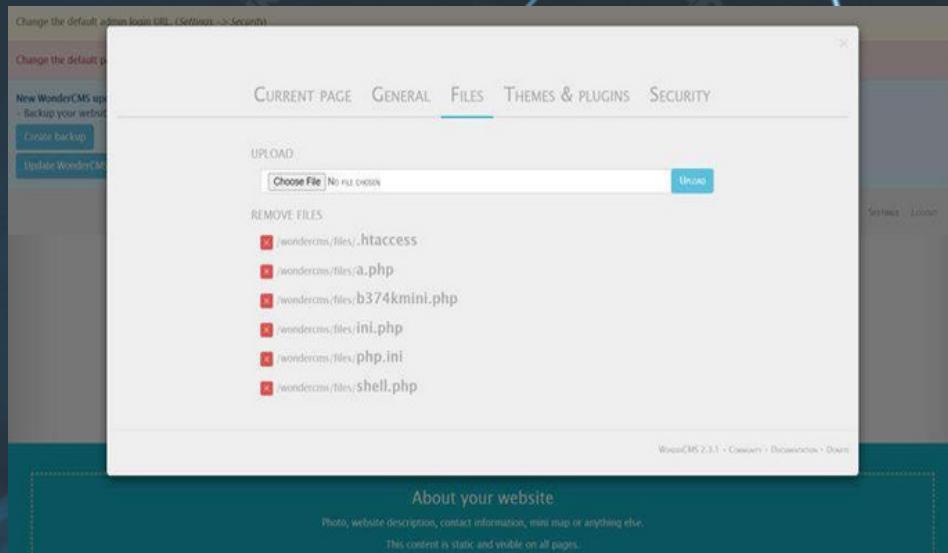
[Create backup](#)

[Update WonderCMS](#)



Here, if we select the '/wondercms/files/b374kmini.php' option it will redirect us to a page which will give us many crucial information like server IP address, Linux IP address , the server type, the database, shell, the php info, uploads.

As we are inside the admin account if we select the settings option and go to 'files' menu we can see some files with extension '.php' which can give information about the site and also very much capable of taking over the site.



The page is found using the b374K mini shell from which an attacker can know all system (backend) details like versions, and more.

The screenshot shows a terminal window with the following content:

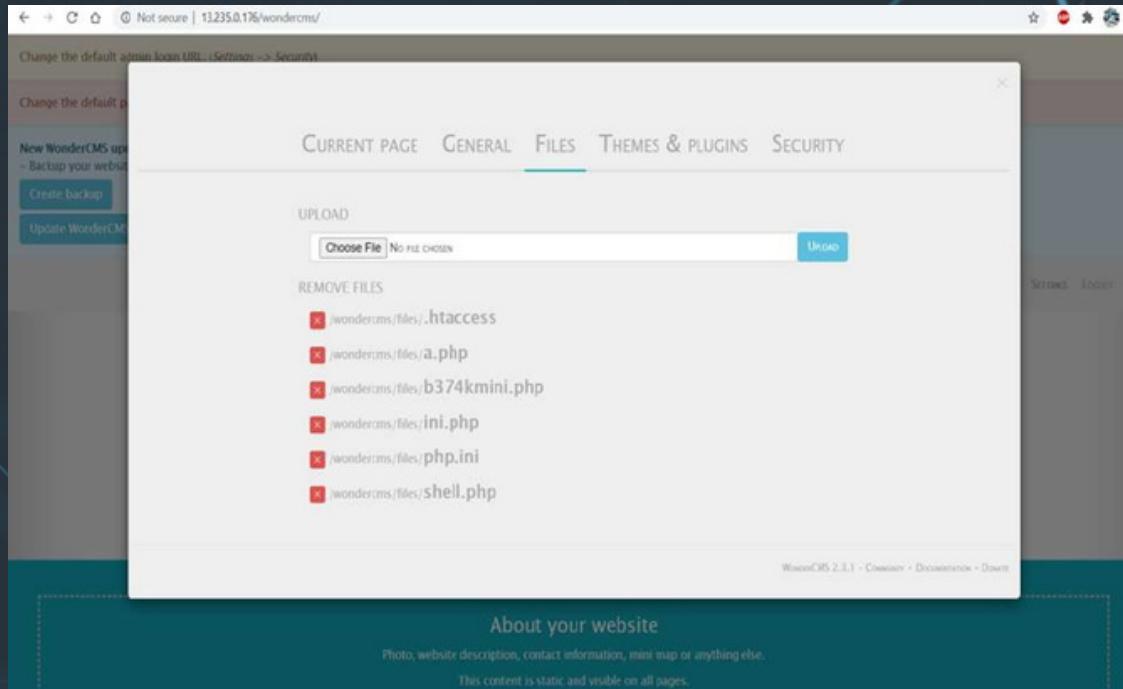
```
Not secure | 15.206.75.142/wondercms/files/b374kmini.php?y=/home/trainee/wondercms/files/&x=mysql  
b374k  
nginx/1.14.0  
Linux ip-172-26-2-38 4.15.0-1040-aws #45-Ubuntu SMP Mon Jun 24 14:07:03 UTC 2019 x86_64  
server ip : 15.206.75.142 your ip : 103.216.162.84  
saferemode OFF  
> /home/trainee/wondercms/files/  
explore shelf eval mysql phpinfo netsploit upload mail
```

A modal dialog box titled "Connect to MySQL server" is displayed, containing the following fields:

Host	localhost
Username	root
Password	password
Port	3306

At the bottom right of the modal is a blue "GO!" button.

- On the same page under settings, click on files, here we have a file upload option, which has no limitations on the type of file which can be uploaded.
- We can upload files of any extension.
Here when we upload a shell into the site, it will give access to take over the whole website.



Business Impact:

- As the blog site has multiple vulnerabilities such as temporary XSS, server side errors and development flaws the site is extremely vulnerable .
- As a hacker can indulge in the site and can use all the vulnerable components to do phishing and other attacks on user and perform malicious activities.
- This will result In defamation of the name of the company, money loss and customers never trusting the website again.

Recommendations:

Take the following precautions :

- The website should have proper two factor authentication.
- Try to develop the back end more stronger and secure.
- Remove all directory listings and add proper sanitization

THANK YOU

My name is **Arjun Shetty!!**

my linkedIn profile:

[https://www.linkedin.com/in/arjun-shetty-
255049229](https://www.linkedin.com/in/arjun-shetty-255049229)

you can contact me on :

91+ 9686630424

my GitHub account :

<https://github.com/shettyarjun>

