INTERNSHALA
internships that matter

Hacking Environment Web Application

Detailed Developer Report

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 pages 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 execute any commands to extract information from website and deface it(admin panel access)
- Hacker can easily view default and debug pages, can easily guess the default passwords and can exploit all the vulnerability related to the third party components used (Security misconfiguration)

Vulnerability statistics

Critical	Severe
11	8

High	Low
3	7

Vulnerabilities index

Serial number	Severity	Vulnerabilities	count
1	Critical	SQL injections	2
2	Critical	Remote file inclusion	1
3	Critical	Admin panel access	1
4	Critical	Insecure file uploads	1
5	Critical	Seller account access	1
6	Critical	Default admin password	1
7	Critical	Components with known vulnerability	3

Serial number	Severity	Vulnerabilities	count
8	Critical	Customer account access	1
9	Severe	Forced browsing	1
10	Severe	C.S.R.F	2
11	Severe	Coupon code brute force	1
12	Severe	Insecure direct object ref.	1
13	Severe	Open redirection	1
14	Severe	Cross site scripting	2
15	High	Client side filter bypass	1
16	High	Directory listing	1
17	High	PII Leakage	1
18	Low	Default debug pages	5
19	Low	Descriptive error messages	2

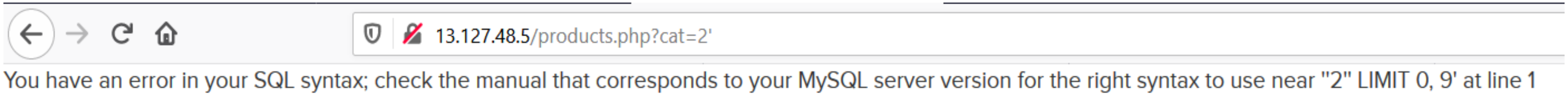
1. S.Q.L. Injections

SQL	The bellow mentioned url is vulnerable to sql injections • Affacted url https://13.127.48.5/products .php?cat=(here) https://13.127.48.5/search/search.php?q=(here) • Affacted parameters 1. cat 2. q • Payload cat=2’ q=adidas’

Observations

At home page click on any 1 category.

Notice the get category of cat and add ‘ and then observe the error.



13.127.48.5/products.php?cat=2'

```
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''2'' LIMIT 0, 9' at line 1
```

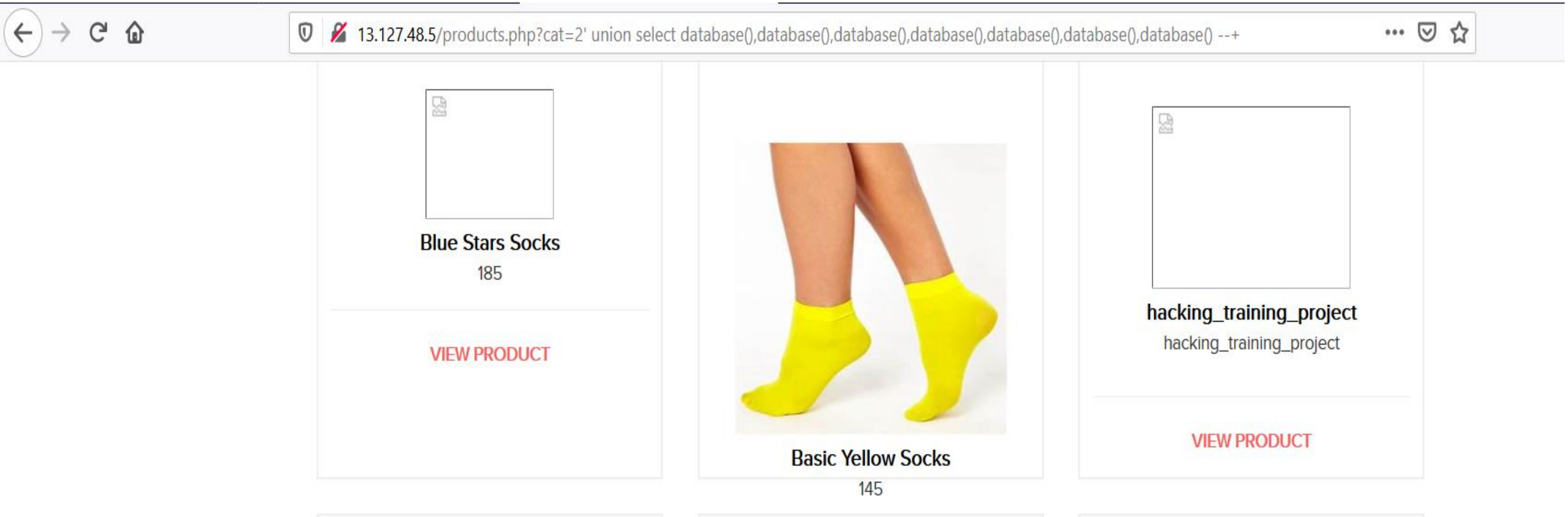
Observations

When we write https://13.127.48.5/products .php?cat=2’ --+ the error would be removed

That confirms the sql injection

Proof of concept

Attacker can execute the sql commands as shown below and access confidential data.



```
13.127.48.5/products.php?cat=2' union select database(),database(),database(),database(),database(),database(),database() --+
```

Blue Stars Socks

185

VIEW PRODUCT

Basic Yellow Socks

145

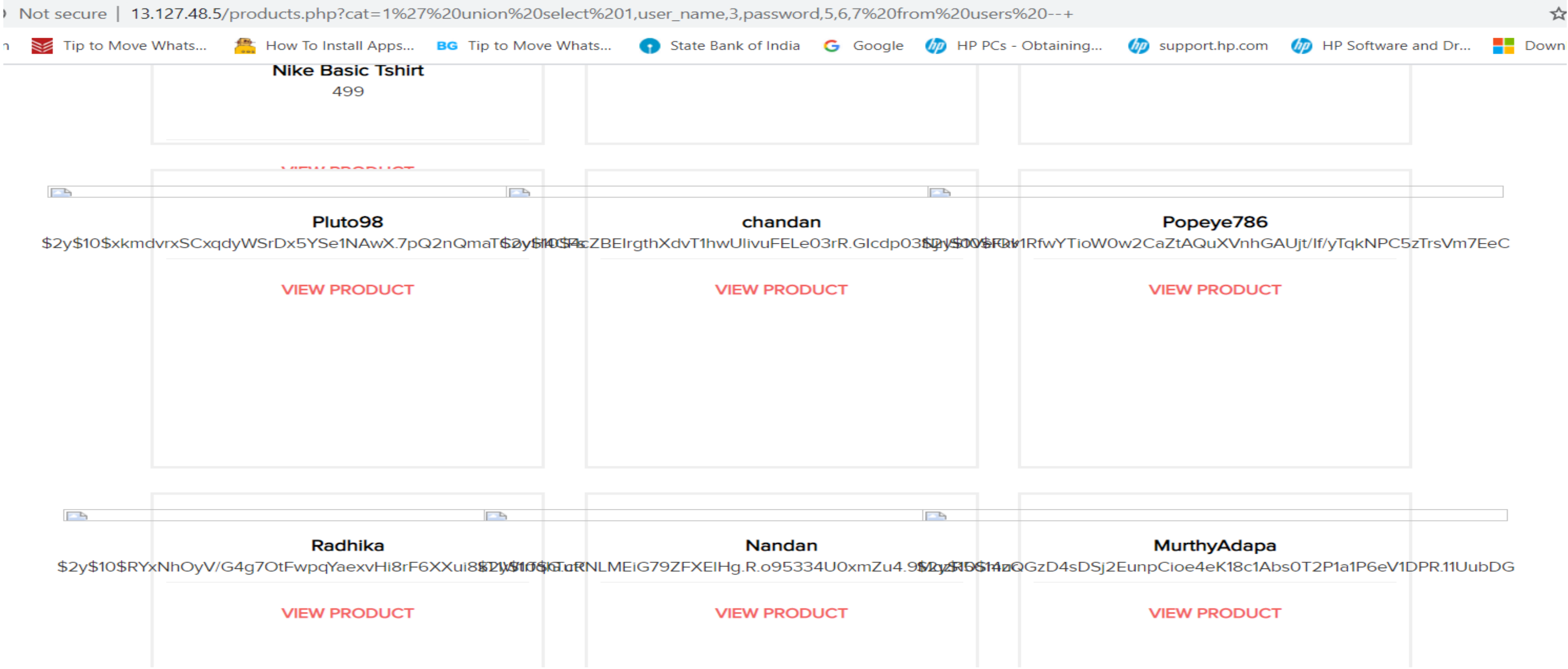
hacking_training_project

hacking_training_project

VIEW PRODUCT

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.



Not secure | 13.127.48.5/products.php?cat=1%27%20union%20select%201,user_name,3,password,5,6,7%20from%20users%20--+

Nike Basic Tshirt
499

Pluto98
$2y$10$xkmdvrxSCxqdyWSrDx5YSe1NAwX.7pQ2nQmaT$2y$10$FlcZBEIrgthXdvT1hwUlivuFELe03rR.Glcdp03$2y$10$FRw1RfwYTioW0w2CaZtAQuXVnhGAUjt/If/yTqkNPC5zTrsVm7EeC

chandan

Popeye786

Radhika
$2y$10$RYxNhOyV/G4g7OtFwpqYaexvHi8rF6XXui8$2y$10$lGTuRNLMEiG79ZFXEIHg.R.o95334U0xmZu4.9$2y$10$14zQGzD4sDSj2EunpCioe4eK18c1Abs0T2P1a1P6eV1DPR.11UubDG

Nandan

MurthyAdapa

Recommendations

Take the following precautions to avoid exploitation of SQL injections:

- 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 has 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://en.wikipedia.org/wiki/SQL_injection*

2.Remote File inclusion

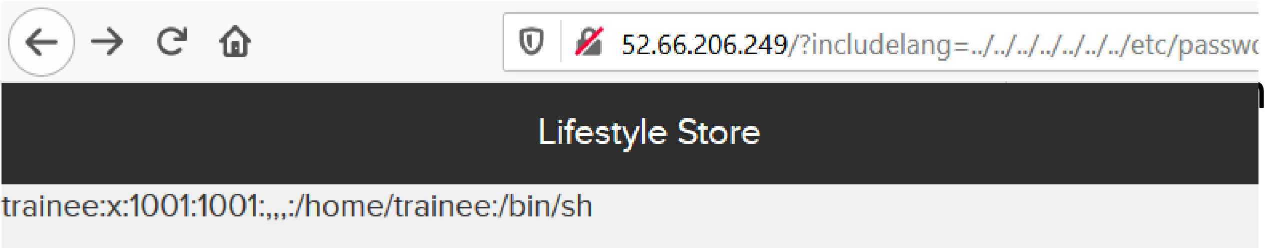
RFI	Below mentioned url is vulnerable to RFI • Affected url 52.66.206.249/?includelang=(here) • Payload ../../../../../../../etc/passwd https://google.co.in

Observations

When you click on change language you get a ‘get’ parameter of includelang which is vulnerable for file inclusion.

Her ich gives us

use



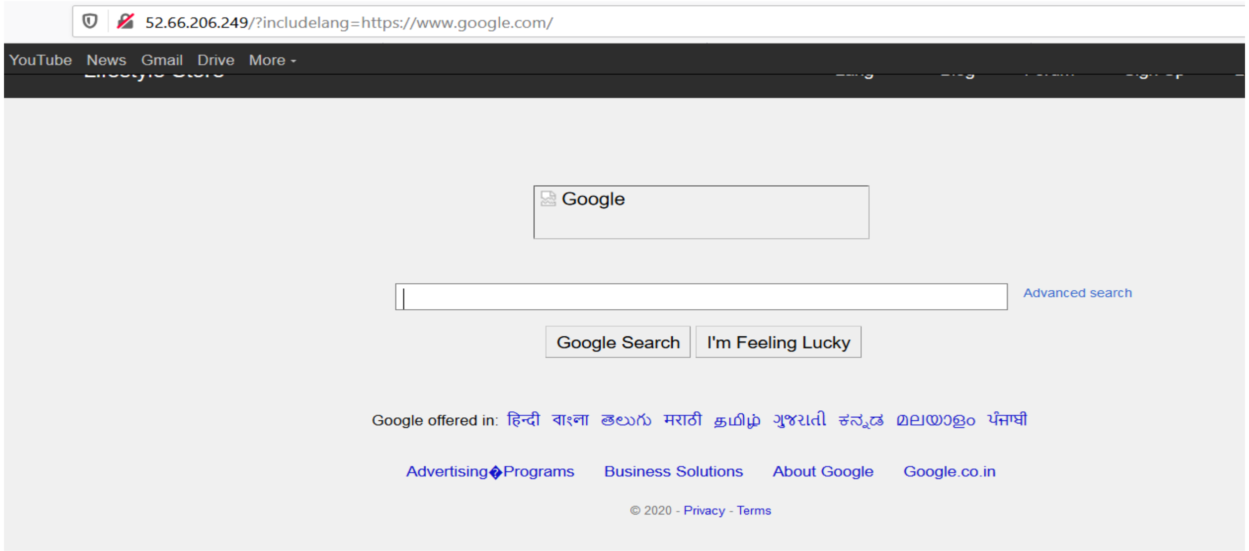
52.66.206.249/?includelang=../../../../../../../etc/passw

Lifestyle Store

```
trainee:x:1001:1001:,,,:/home/trainee:/bin/sh
```

POC-attacker can upload shells

- **Attacker can exploit** the referencing function in an application to upload malware (e.g., backdoor shells) from a remote URL located within a different domain.



52.66.206.249/?includelang=https://www.google.com/

Business impact- Extremely high

- Any attacker can have the root access of of your website
- He can execute commands
- Through the website he can have access of the server and can infect other websites hosted on that server
- He can even deface your websites

Recommendations

- To safely parse user-supplied filenames it’s much better to **maintain a whitelist of acceptable filenames** and use a corresponding identifier (not the actual name) to access the file. Any request containing an invalid identifier can then simply be rejected. This is the approach that OWASP recommends.

References

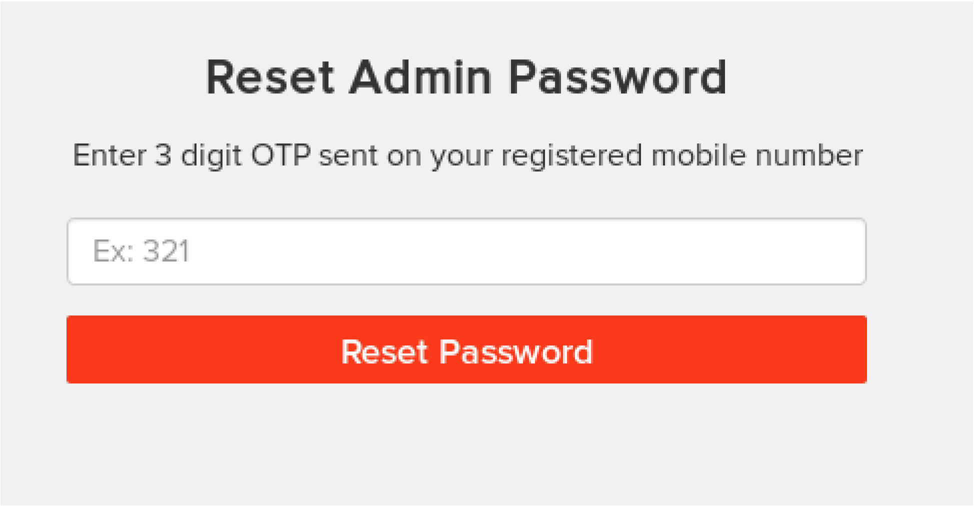
- https://www.pivotpointsecurity.com/blog/file-inclusion-vulnerabilities/
- https://www.netsparker.com/blog/web-security/local-file-inclusion-vulnerability/
- https://en.wikipedia.org/wiki/File_inclusion_vulnerability

3.Admin panel access

Admin panel access	Admin panel of this website can easily be taken over by brute forcing O.T.P. • Affected url http://13.126.208.41/reset_password/admin.php • Payload 001-999 digits

Observation

- In the admin login section there is a reset admin option which only needs a 3-digit otp

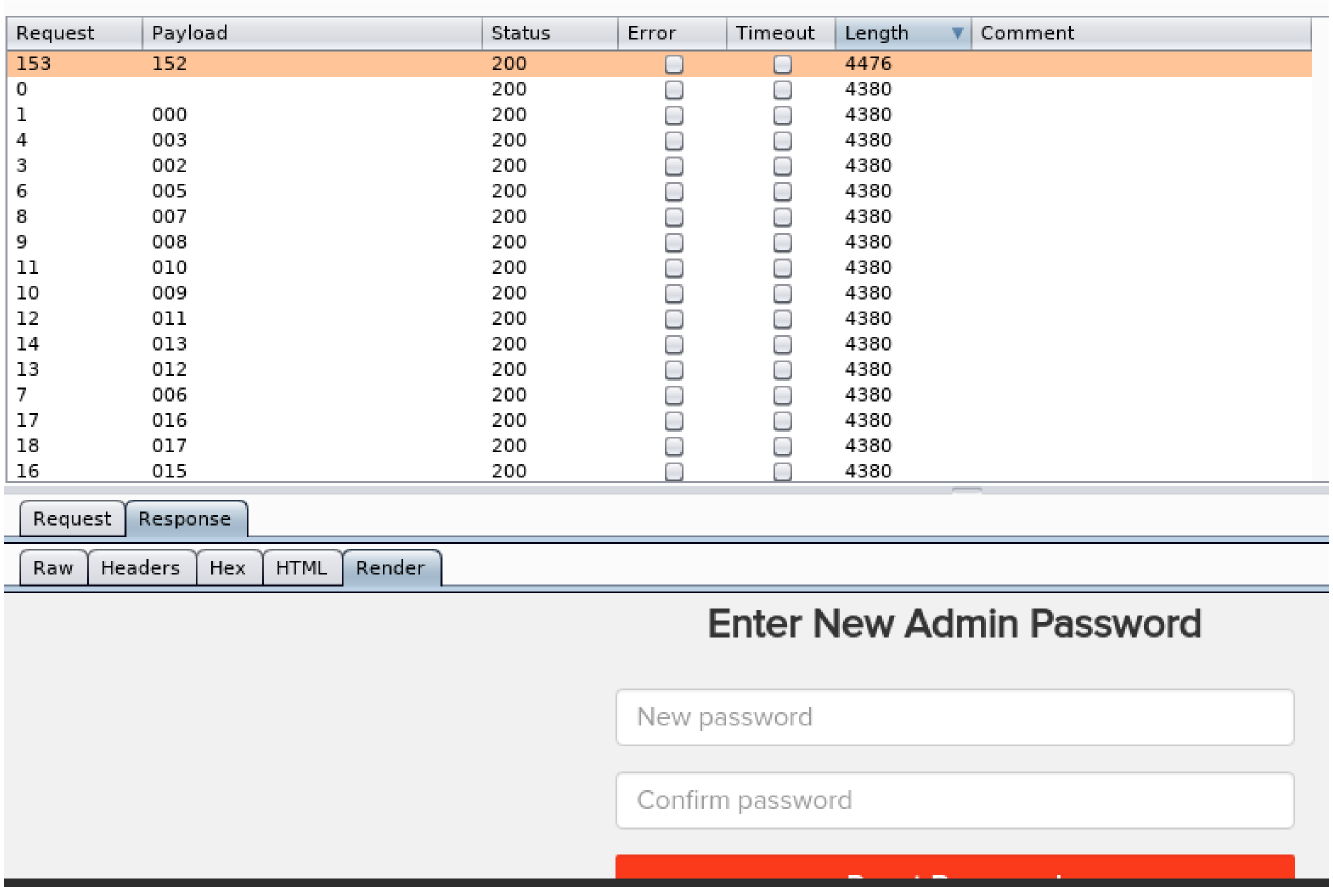


Reset Admin Password

Enter 3 digit OTP sent on your registered mobile number

POC-Easy access to admin panel

- By using burp suite we can easily bruteforce the otp



Request	Payload	Status	Error	Timeout	Length	Comment
153	152	200	☐	☐	4476	
0		200	☐	☐	4380	
1	000	200	☐	☐	4380	
4	003	200	☐	☐	4380	
3	002	200	☐	☐	4380	
6	005	200	☐	☐	4380	
8	007	200	☐	☐	4380	
9	008	200	☐	☐	4380	
11	010	200	☐	☐	4380	
10	009	200	☐	☐	4380	
12	011	200	☐	☐	4380	
14	013	200	☐	☐	4380	
13	012	200	☐	☐	4380	
7	006	200	☐	☐	4380	
17	016	200	☐	☐	4380	
18	017	200	☐	☐	4380	
16	015	200	☐	☐	4380	

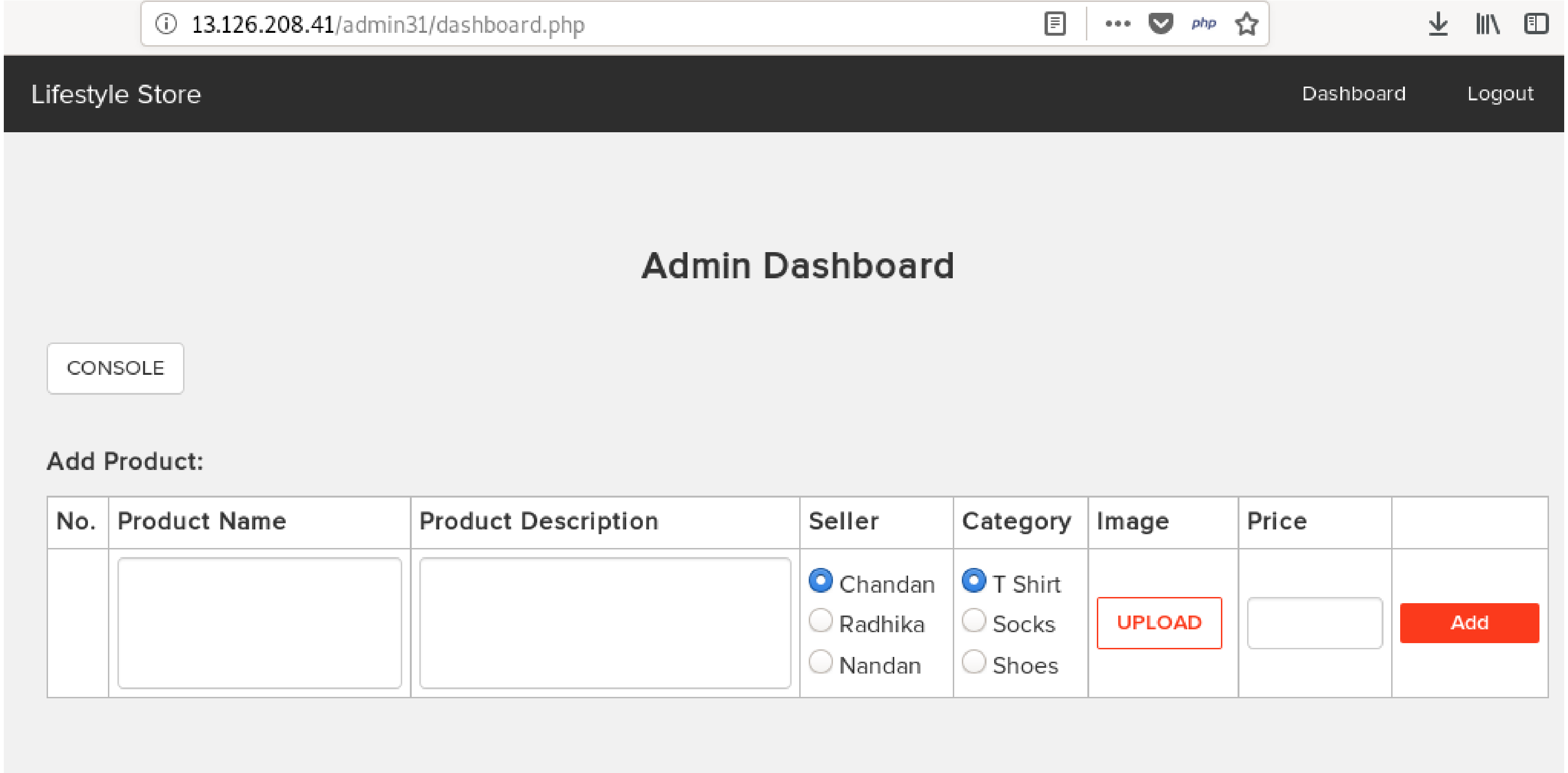
Enter New Admin Password

New password

Confirm password

POC

Here is the admin dashboard:-



Admin Dashboard

Add Product:

No.	Product Name	Product Description	Seller	Category	Image	Price	
			● Chandan ○ Radhika ○ Nandan	● T Shirt ○ Socks ○ Shoes	UPLOAD		Add

Business impact-extremely high

- He can change the rates of items selling on the web sites
- He can add and delete the items
- He can change the seller and catagories
- He can execute commands on the server through console options, which can be further used to harm your website

Recommendations

- The first is to implement an account lockout policy. For example, after three failed login attempts, the account is locked out until an administrator unlocks it.
- Tools such as the free reCAPTCHA can be used to require the user to enter a word or solve a simple math problem to ensure the user is, in fact, a person.
- Admin login page should be hidden very securely
- The otp should be alpha numeric and at least of 6-letters and digits.

Refernces

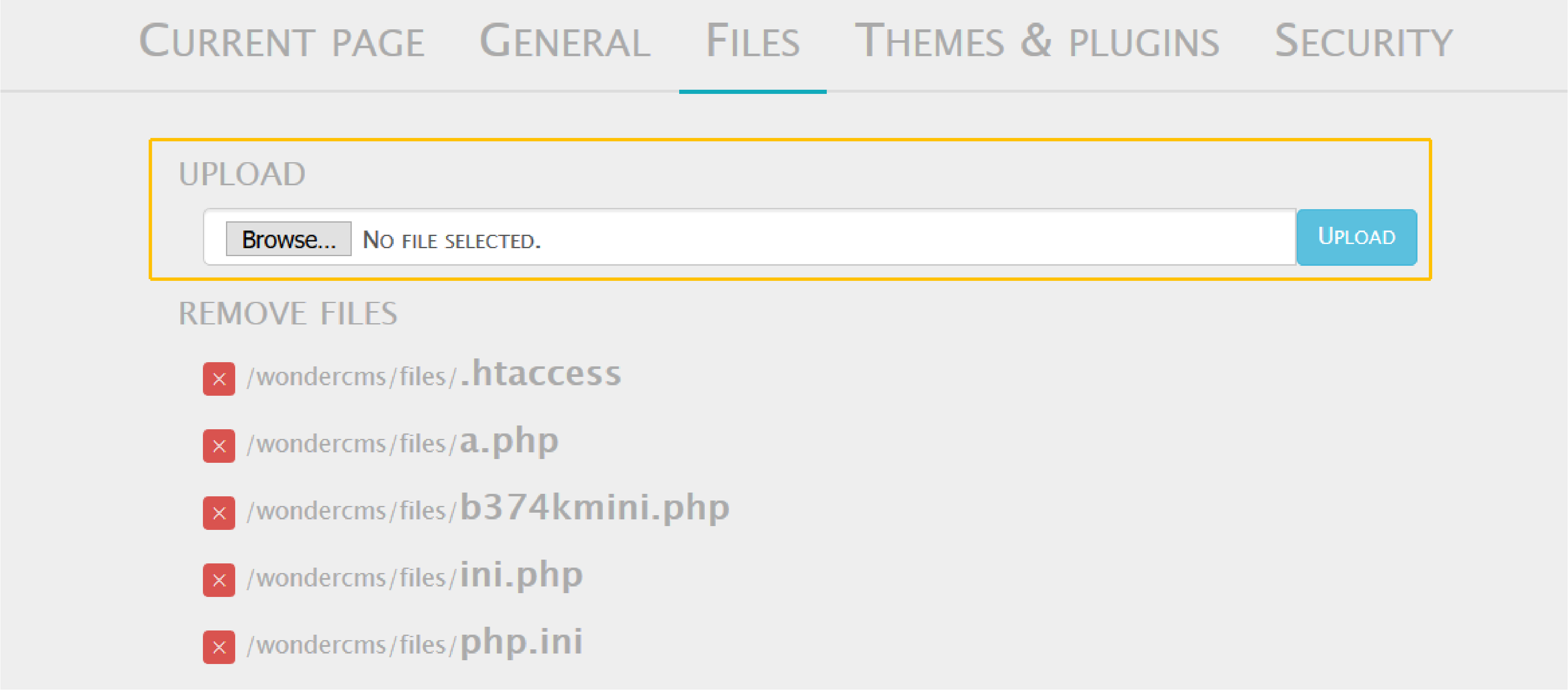
- https://www.computerweekly.com/answer/Techniques-for-preventing-a-brute-force-login-attack
- https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks

4.Insecure file uploads

Insecure file uploads	The url given below is vulnerable to insecure file uploads • Affected url http://13.233.83.32/wondercms/ • Uploaded file backdoor shell

Observations

- In the blog page of website there is a upload option in the settings



UPLOAD

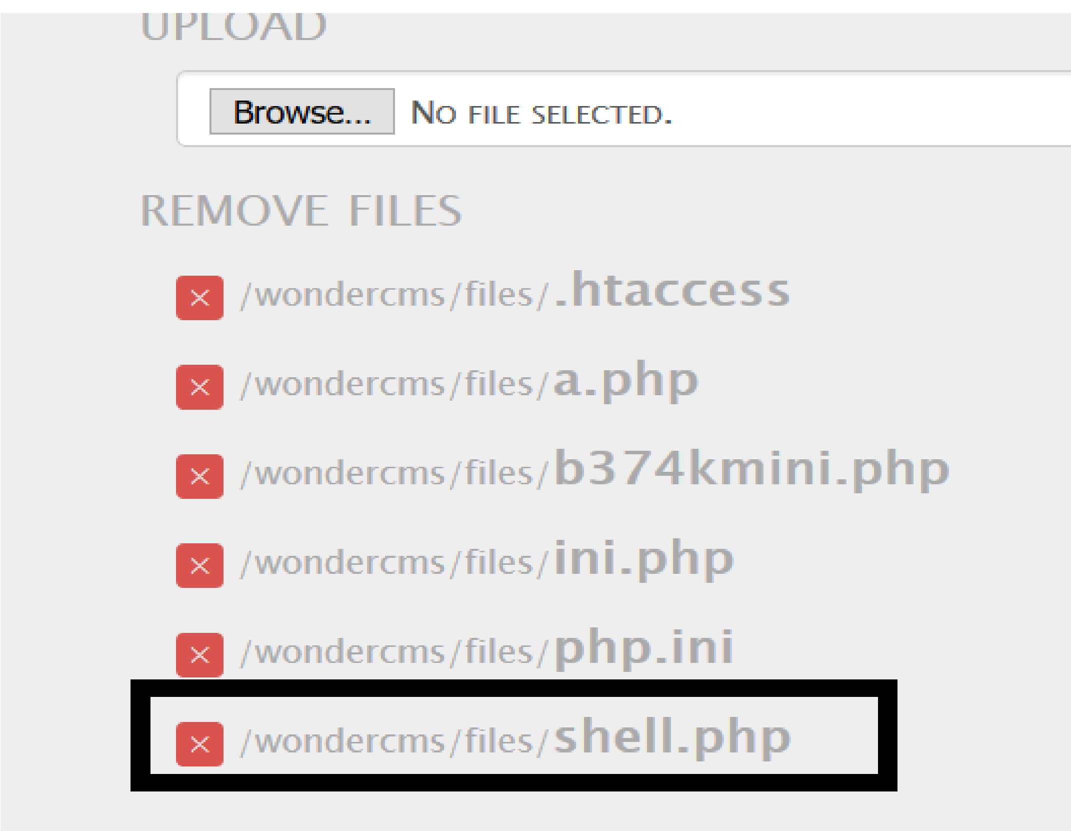
No file selected.

REMOVE FILES

- ☒ /wondercms/files/.htaccess
- ☒ /wondercms/files/a.php
- ☒ /wondercms/files/b374kmini.php
- ☒ /wondercms/files/ini.php
- ☒ /wondercms/files/php.ini

Observations

- I tried uploading a shell and I was successful



UPLOAD

No file selected.

REMOVE FILES

/wondercms/files/.htaccess

/wondercms/files/a.php

/wondercms/files/b374kmini.php

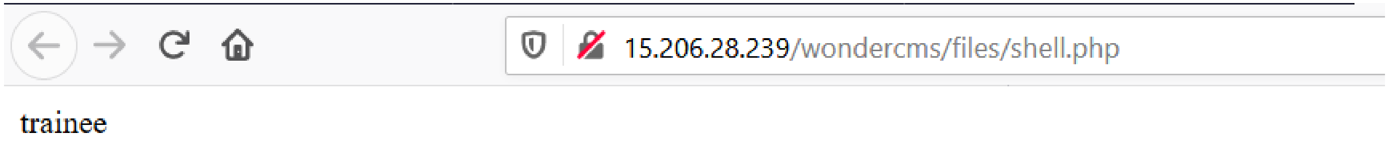
/wondercms/files/ini.php

/wondercms/files/php.ini

/wondercms/files/shell.php

POC-Any command can be executed

- The shell I uploaded was executed successfully



15.206.28.239/wondercms/files/shell.php

trainee

Business impact-Extremely high

The consequences of unrestricted file upload can vary:-

- including complete system takeover, an overloaded file system or database.
- forwarding attacks to back-end systems
- client-side attacks, or simple defacement.

It depends on what the application does with the uploaded file and especially where it is stored.

Recommendations

- The file types allowed to be uploaded should be restricted to only those that are necessary for business functionality.
- Never accept a filename and its extension directly without having a whitelist filter.
- All the control characters and Unicode andthe special characters should be discarded

References

- IIS 6.0 Security Best Practices[http://technet.microsoft.com/en-us/library/cc782762(WS.10).aspx]
- Securing Sites with Web Site Permissions[http://technet.microsoft.com/en-us/library/cc756133(WS.10).aspx]
- IIS 6.0 Operations Guide[http://technet.microsoft.com/en-us/library/cc785089(WS.10).aspx]
- https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload

Server misconfigurations

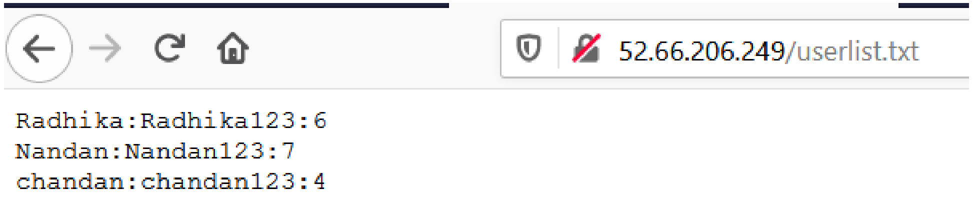
- Default debug files
- Weak/default passwords
- Components with known vulnerability

5.Seller account access

Seller account access	The default page given below shows the seller accounts and passwords • Affected url http://13.233.83.32/userlist.txt

Observations

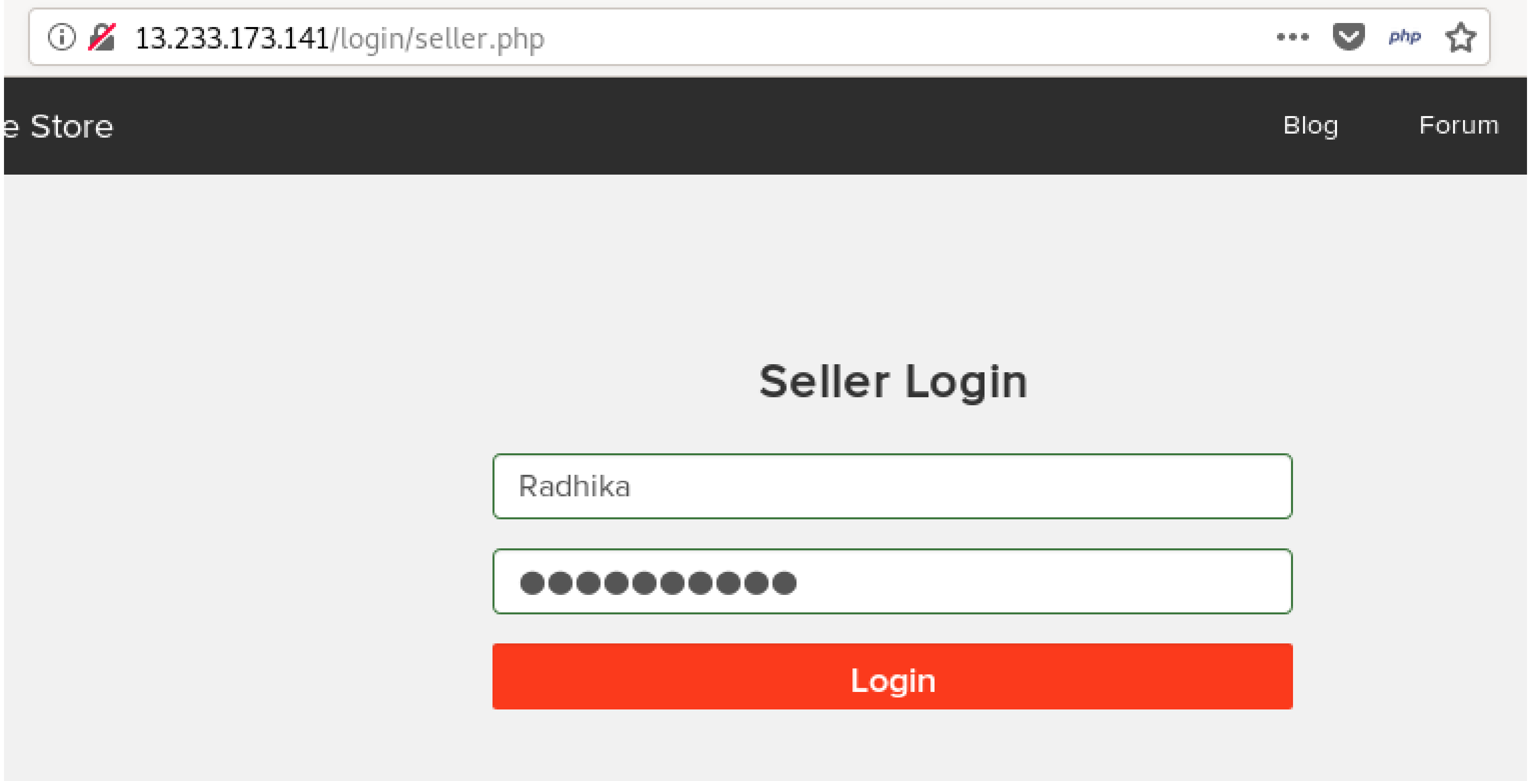
At the homepage after adding userlist.txt the following page is opened



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

POC-attacker has the seller dashboard acess

- On entering the credentials in the seller account login we have accessed the dashboard



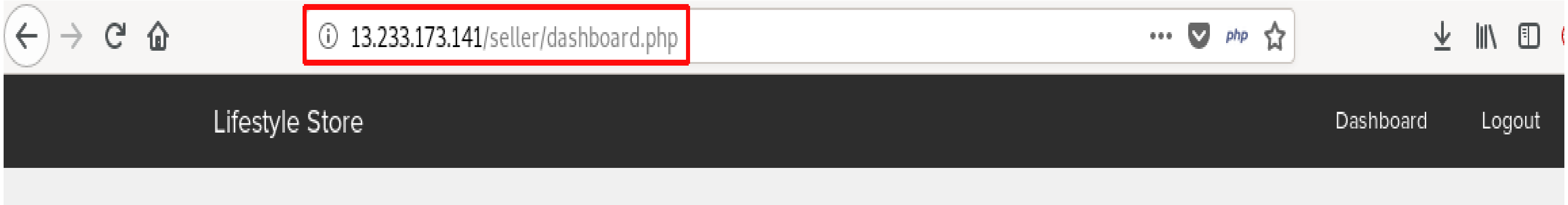
13.233.173.141/login/seller.php

Seller Login

Radhika

●●●●●●●●●●

POC



13.233.173.141/seller/dashboard.php

Bussiness impact-Extremely high

- Attacker can access the seller dashboard and then can edit the items he is selling

Recommendations

- The developer should disable these confidential default pages

References

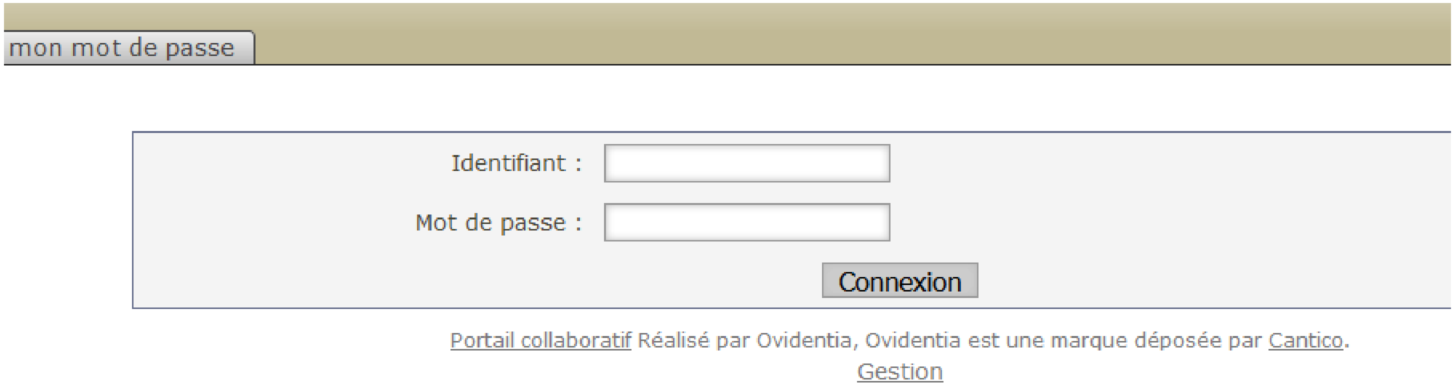
- https://www.indusface.com/blog/owasp-security-misconfiguration/
- https://hdivsecurity.com/owasp-security-misconfiguration

6.Default admin password

Default admin password	The url given below is using the default admin credentials • Affected url http://52.66.65.223/ovidentiaCMS/index.php?tg=login&cmd=authform&msg=Connexion&err=&restricted=1 • Component name ovidentia content management system

Observations

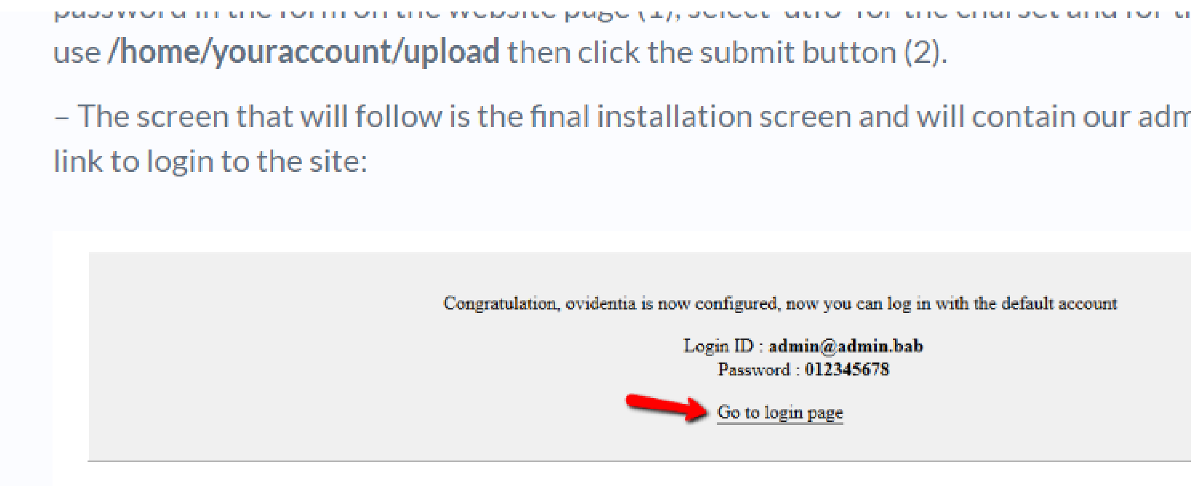
- In the ovidentia cms page there is option to login as admin
- On clicking it we saw this page



Portail collaboratif Réalisé par Ovidentia, Ovidentia est une marque déposée par Cantico.

POC-ovidentia admin access

- In searching for default ovidentia admin credentials we get



password in the form on the website page (1), select 'utf8' for the charset and for t

use **/home/youraccount/upload** then click the submit button (2).

– The screen that will follow is the final installation screen and will contain our adm

link to login to the site:

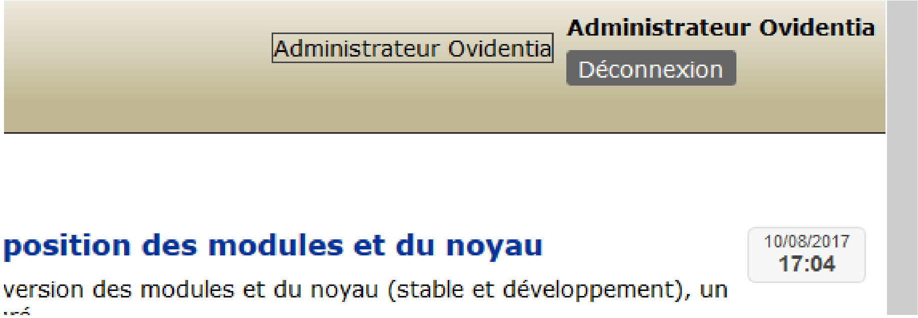
Congratulation, ovidentia is now configured, now you can log in with the default account

Login ID : **admin@admin.bab**
Password : **012345678**

Go to login page

POC

- We got the admin access



Administrateur Ovidentia

Administrateur Ovidentia

position des modules et du noyau

10/08/2017
17:04

version des modules et du noyau (stable et développement), un

Business impact- Extremely high

- Attacker will have all the admin privileges
- He can easily deface the ovidentia CMS

Recommendations

- Disable the default debug pages
- Hide the admin login page
- Disable the default passwords and use a strong username and password

References

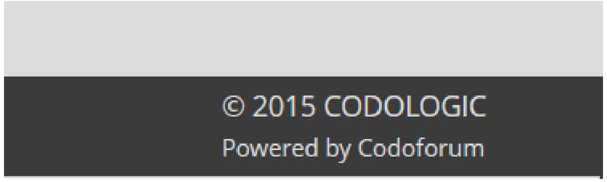
- https://www.indusface.com/blog/owasp-security-misconfiguration/
- https://hdivsecurity.com/owasp-security-misconfiguration

7.Components with known vulnerability

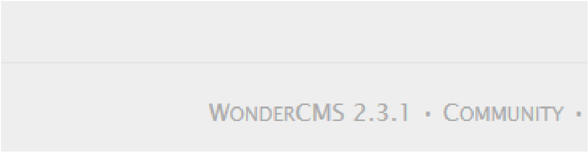
Components with known vulnerability	The urls given below are of the components with known vulnerability • Affected url http://52.66.65.223/wondercms/ http://52.66.65.223/forum/ And PHP

Observations

- I checked the versions of these components they were out dated



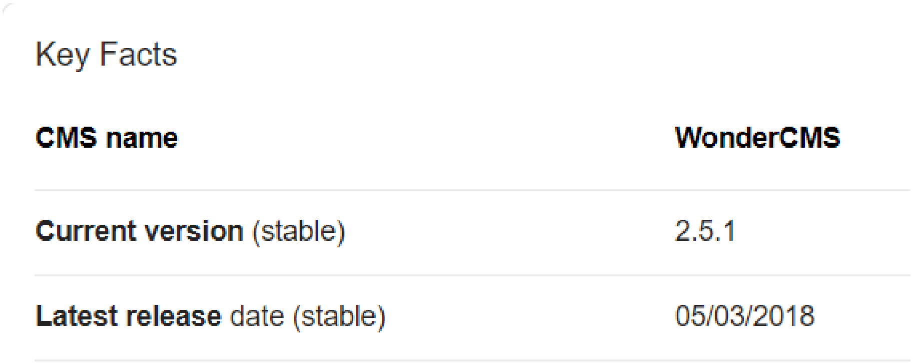
© 2015 CODOLOGIC
Powered by Codoforum



WONDERCMS 2.3.1 · COMMUNITY ·

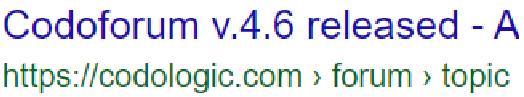
Observations

In 2015 version of codoforum was 3.0



Key Facts

CMS name	**WonderCMS**
Current version (stable)	2.5.1
Latest release date (stable)	05/03/2018

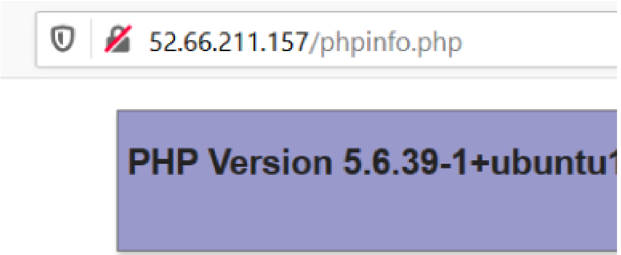


Codoforum v.4.6 released - A

https://codologic.com › forum › topic

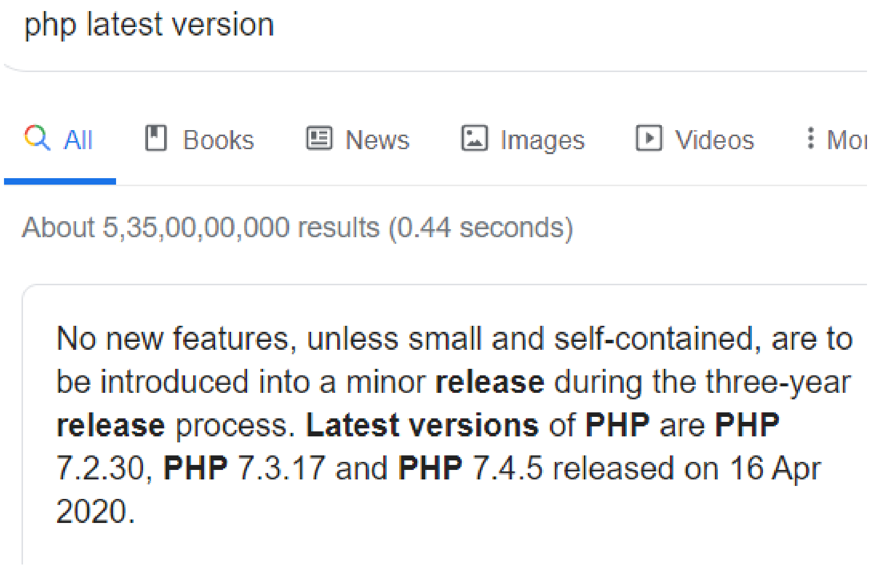
Observations

- The php version of this website is 5.6.39-1 which is out dated



52.66.211.157/phpinfo.php

PHP Version 5.6.39-1+ubuntu1



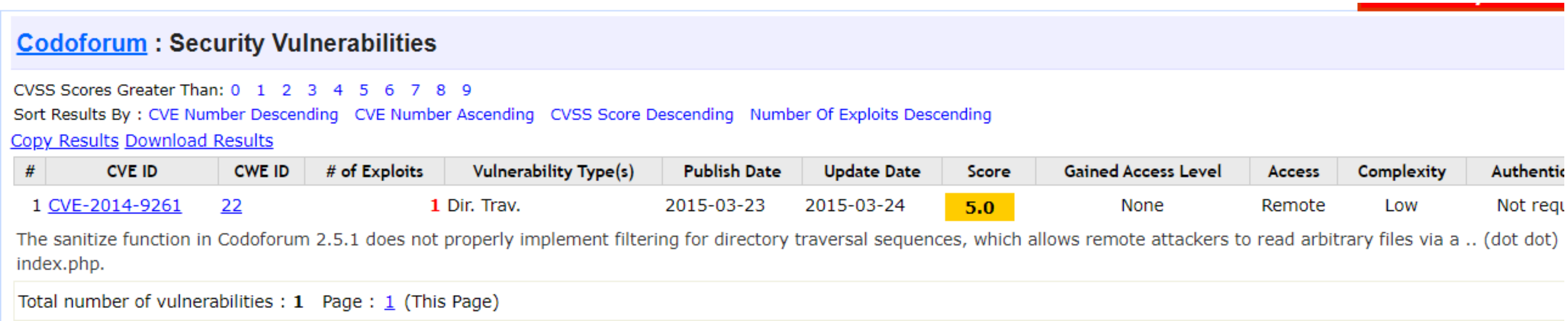
php latest version

About 5,35,00,00,000 results (0.44 seconds)

No new features, unless small and self-contained, are to be introduced into a minor **release** during the three-year **release** process. **Latest versions** of **PHP** are **PHP** 7.2.30, **PHP** 7.3.17 and **PHP** 7.4.5 released on 16 Apr 2020.

POC

- Both the components have known public exploits



Codoforum : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

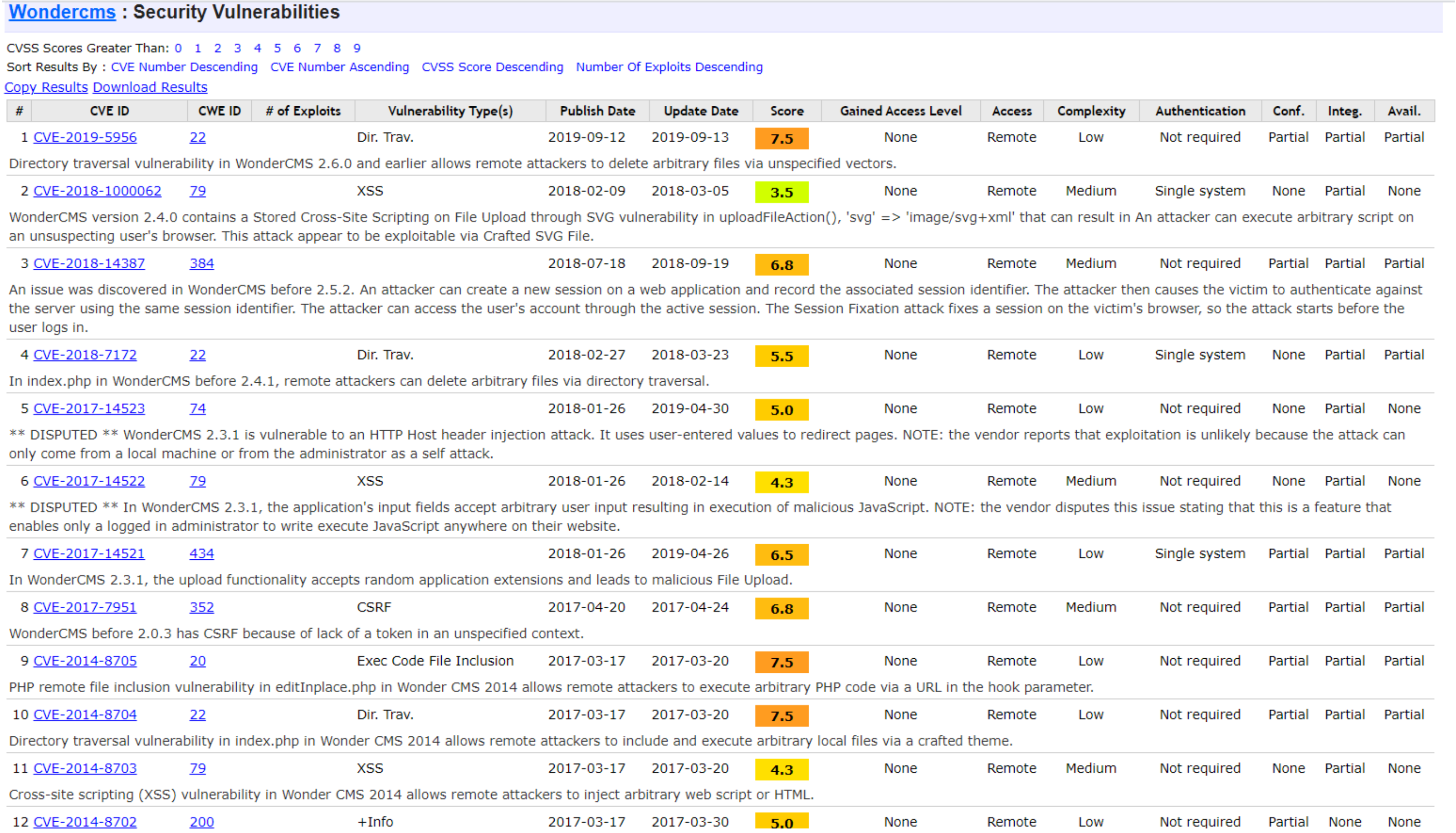
Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentic
1	CVE-2014-9261	22	1	Dir. Trav.	2015-03-23	2015-03-24	5.0	None	Remote	Low	Not requ

The sanitize function in Codoforum 2.5.1 does not properly implement filtering for directory traversal sequences, which allows remote attackers to read arbitrary files via a .. (dot dot) index.php.

Total number of vulnerabilities : **1** Page : 1 (This Page)

POC



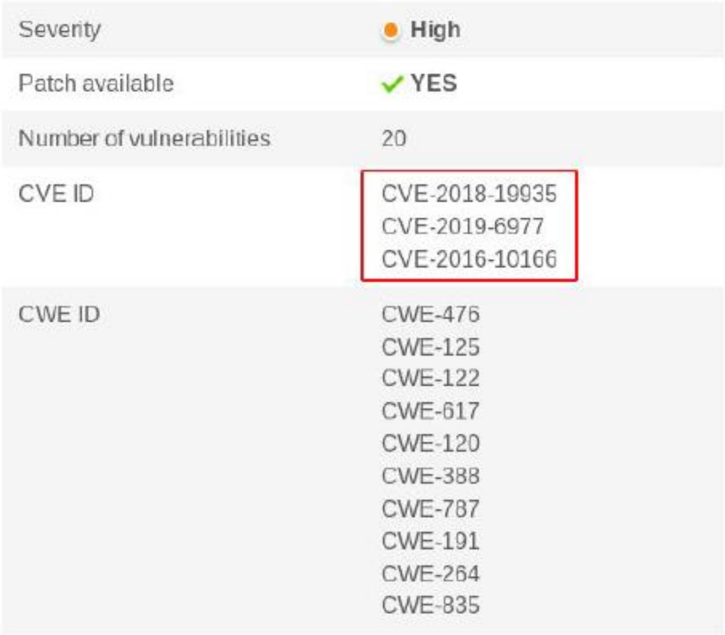
Wondercms : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending
Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2019-5956	22		Dir. Trav.	2019-09-12	2019-09-13	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Directory traversal vulnerability in WonderCMS 2.6.0 and earlier allows remote attackers to delete arbitrary files via unspecified vectors.														
2	CVE-2018-1000062	79		XSS	2018-02-09	2018-03-05	3.5	None	Remote	Medium	Single system	None	Partial	None
WonderCMS version 2.4.0 contains a Stored Cross-Site Scripting on File Upload through SVG vulnerability in uploadFileAction(), 'svg' => 'image/svg+xml' that can result in An attacker can execute arbitrary script on an unsuspecting user's browser. This attack appear to be exploitable via Crafted SVG File.														
3	CVE-2018-14387	384			2018-07-18	2018-09-19	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
An issue was discovered in WonderCMS before 2.5.2. An attacker can create a new session on a web application and record the associated session identifier. The attacker then causes the victim to authenticate against the server using the same session identifier. The attacker can access the user's account through the active session. The Session Fixation attack fixes a session on the victim's browser, so the attack starts before the user logs in.														
4	CVE-2018-7172	22		Dir. Trav.	2018-02-27	2018-03-23	5.5	None	Remote	Low	Single system	None	Partial	Partial
In index.php in WonderCMS before 2.4.1, remote attackers can delete arbitrary files via directory traversal.														
5	CVE-2017-14523	74			2018-01-26	2019-04-30	5.0	None	Remote	Low	Not required	None	Partial	None
** DISPUTED ** WonderCMS 2.3.1 is vulnerable to an HTTP Host header injection attack. It uses user-entered values to redirect pages. NOTE: the vendor reports that exploitation is unlikely because the attack can only come from a local machine or from the administrator as a self attack.														
6	CVE-2017-14522	79		XSS	2018-01-26	2018-02-14	4.3	None	Remote	Medium	Not required	None	Partial	None
** DISPUTED ** In WonderCMS 2.3.1, the application's input fields accept arbitrary user input resulting in execution of malicious JavaScript. NOTE: the vendor disputes this issue stating that this is a feature that enables only a logged in administrator to write execute JavaScript anywhere on their website.														
7	CVE-2017-14521	434			2018-01-26	2019-04-26	6.5	None	Remote	Low	Single system	Partial	Partial	Partial
In WonderCMS 2.3.1, the upload functionality accepts random application extensions and leads to malicious File Upload.														
8	CVE-2017-7951	352		CSRF	2017-04-20	2017-04-24	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
WonderCMS before 2.0.3 has CSRF because of lack of a token in an unspecified context.														
9	CVE-2014-8705	20		Exec Code File Inclusion	2017-03-17	2017-03-20	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
PHP remote file inclusion vulnerability in editInplace.php in Wonder CMS 2014 allows remote attackers to execute arbitrary PHP code via a URL in the hook parameter.														
10	CVE-2014-8704	22		Dir. Trav.	2017-03-17	2017-03-20	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Directory traversal vulnerability in index.php in Wonder CMS 2014 allows remote attackers to include and execute arbitrary local files via a crafted theme.														
11	CVE-2014-8703	79		XSS	2017-03-17	2017-03-20	4.3	None	Remote	Medium	Not required	None	Partial	None
Cross-site scripting (XSS) vulnerability in Wonder CMS 2014 allows remote attackers to inject arbitrary web script or HTML.														
12	CVE-2014-8702	200		+Info	2017-03-17	2017-03-30	5.0	None	Remote	Low	Not required	Partial	None	None

POC

- The running php version has multiple vulnerabilities



Severity	● **High**
Patch available	✓ **YES**
Number of vulnerabilities	20
CVE ID	CVE-2018-19935 CVE-2019-6977 CVE-2016-10166
CWE ID	CWE-476 CWE-125 CWE-122 CWE-617 CWE-120 CWE-388 CWE-787 CWE-191 CWE-264 CWE-835

Business impact- Extremely high

- Anyone can perform any attacks (available) as all the exploits are available publicly .
- It can cause severe damage to the website
- He may be able to upload backdoor shells
- He will easily deface your website

Recommendations

- Update all the components and the php version which is running on it
- Hide the current versions info from there pages

References

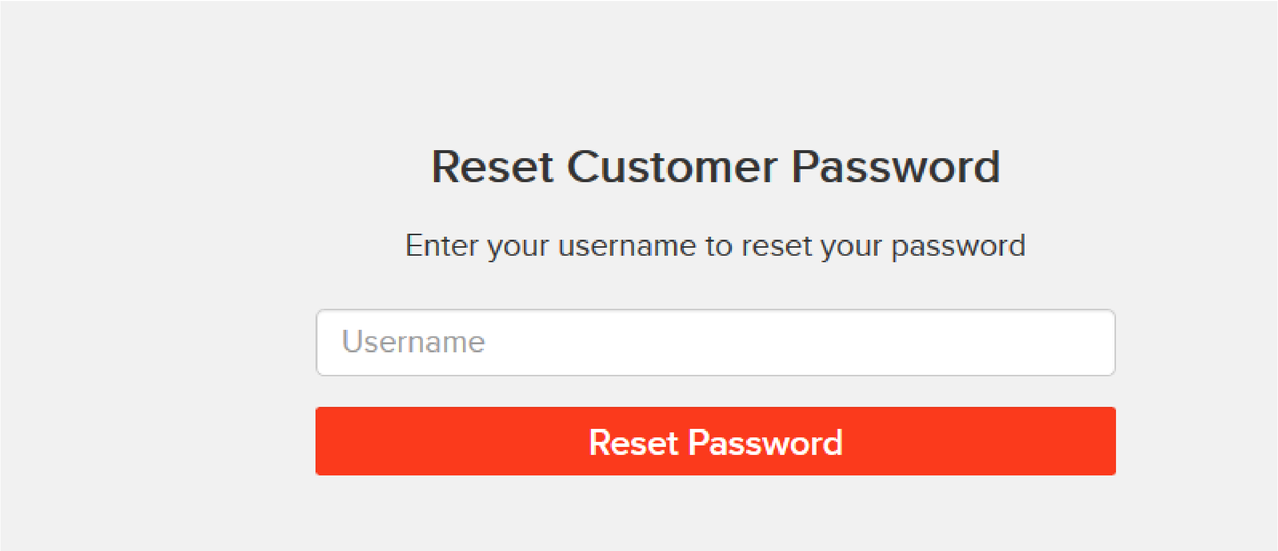
- https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A9-Using_Components_with_Known_Vulnerabilities

8.Customer account access

Customer account access	The url given bellow contains the is giving a descriptive error whith change password option - Affected url http://52.66.65.223/reset_password/customer.php?username=Donal234 - User names Donal234 Pluto98 Popeye786

Observations

- In the forgot password option only username is required to change password

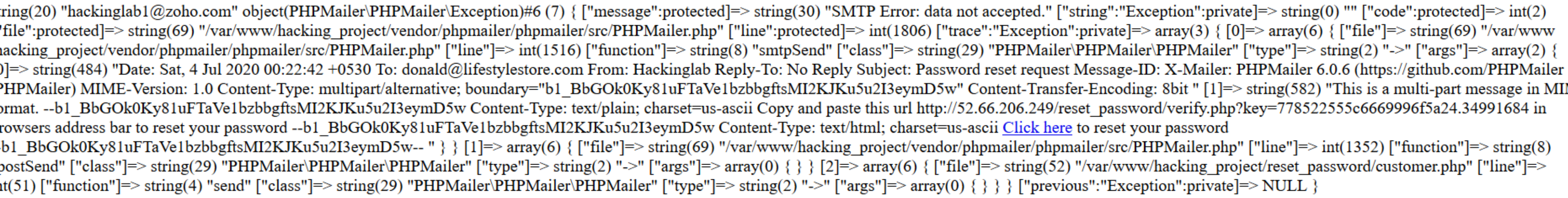


Reset Customer Password

Enter your username to reset your password

Observations

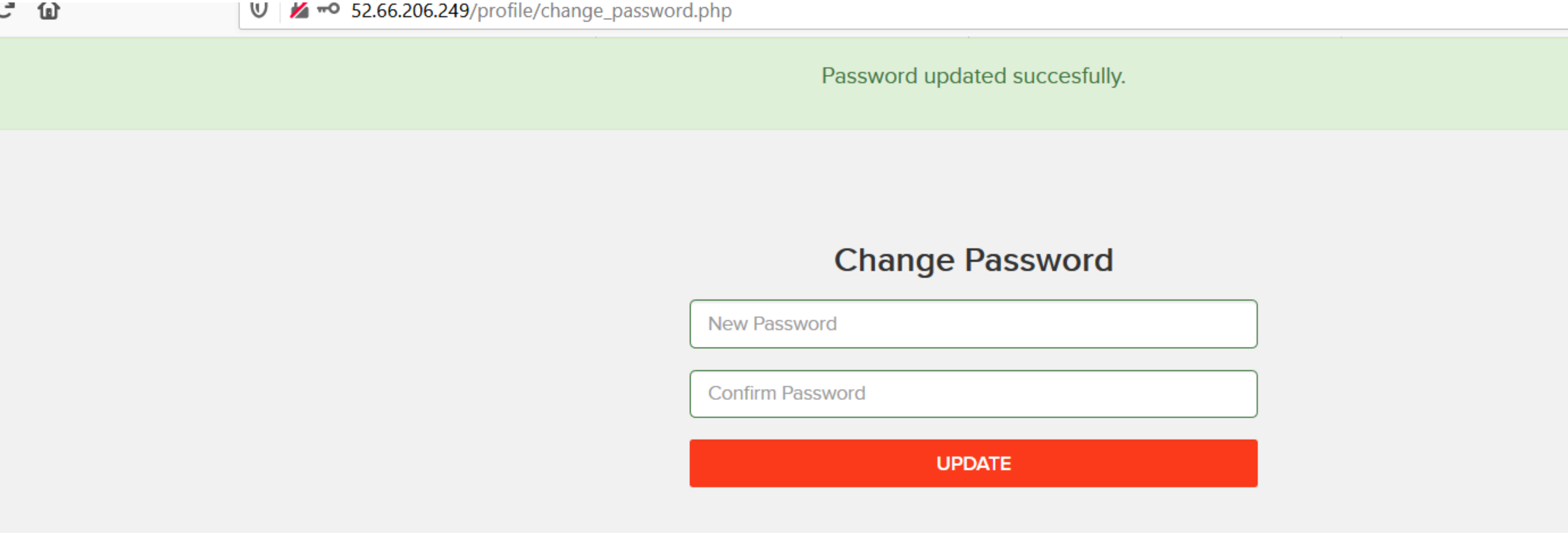
- On entering the username it gives the change password link on email which can be edited by burp suite



```
ring(20) "hackinglab1@zoho.com" object(PHPMailer\PHPMailer\Exception)#6 (7) { ["message":protected]=> string(30) "SMTP Error: data not accepted." ["string":"Exception":private]=> string(0) "" ["code":protected]=> int(2)
'file":protected]=> string(69) "/var/www/hacking_project/vendor/phpmailer/phpmailer/src/PHPMailer.php" ["line":protected]=> int(1806) ["trace":"Exception":private]=> array(3) { [0]=> array(6) { ["file"]=> string(69) "/var/www
acking_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) {
)]=> string(484) "Date: Sat, 4 Jul 2020 00:22:42 +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_BbGOk0Ky81uFTaVe1bzbbgftsMI2KJKu5u2I3eymD5w" Content-Transfer-Encoding: 8bit " [1]=> string(582) "This is a multi-part message in MI
ormat. --b1_BbGOk0Ky81uFTaVe1bzbbgftsMI2KJKu5u2I3eymD5w Content-Type: text/plain; charset=us-ascii Copy and paste this url http://52.66.206.249/reset_password/verify.php?key=778522555c6669996f5a24.34991684 in
rowsers address bar to reset your password --b1_BbGOk0Ky81uFTaVe1bzbbgftsMI2KJKu5u2I3eymD5w Content-Type: text/html; charset=us-ascii Click here to reset your password
-b1_BbGOk0Ky81uFTaVe1bzbbgftsMI2KJKu5u2I3eymD5w-- " } } [1]=> 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) { } } [2]=> array(6) { ["file"]=> string(52) "/var/www/hacking_project/reset_password/customer.php" ["line"]=>
nt(51) ["function"]=> string(4) "send" ["class"]=> string(29) "PHPMailer\PHPMailer\PHPMailer" ["type"]=> string(2) "->" ["args"]=> array(0) { } } } } ["previous":"Exception":private]=> NULL }
```

POC

- After entering another email address password can be changed easily



52.66.206.249/profile/change_password.php

Password updated succesfully.

Change Password

Business impact –extremely high

- Attacker can get the customer account access
- Then he can make changes on it like changing the personnel details , cancel the orders , etc
- This will reduce your organisations reputation

Recommendations

- You should include the otp option and make it compulsory
- Security checks on the server side should be done completely
- Captcha option should also be included

9.Forced browsing

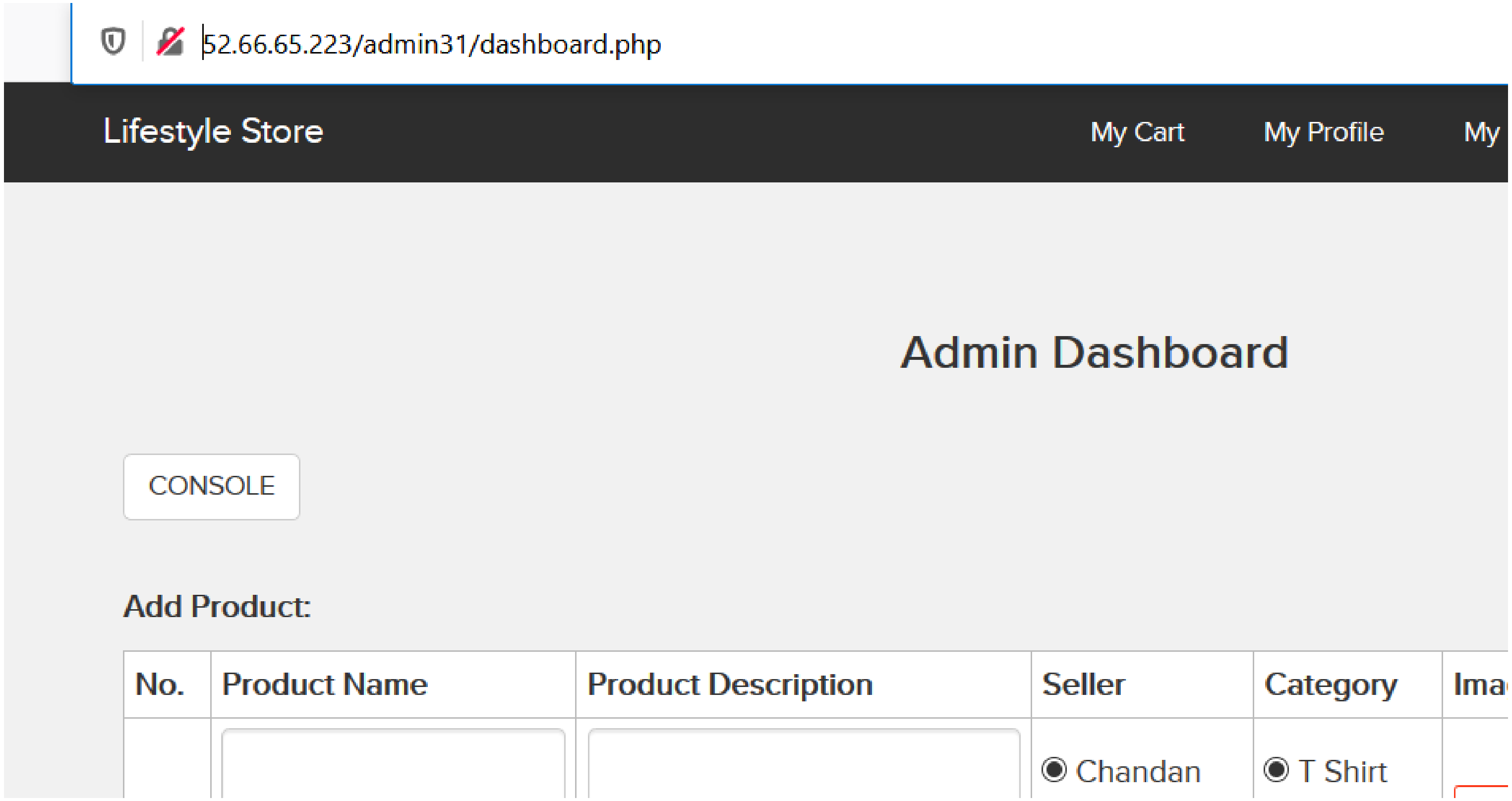
Forced browsing	The below mentioned url is vulnerable toforced browsing • Affected url http://52.66.65.223/ • Forced url http://52.66.65.223/admin31/dashboard.php

observations

When I tried to go in admin dashboard without logging in I was successful

POC-admin dashboard access

Here is the admin dashboard just by entering its complete url



52.66.65.223/admin31/dashboard.php

Admin Dashboard

Add Product:

No.	Product Name	Product Description	Seller	Category	Ima
			● Chandan	● T Shirt	

Business impact- severe

- Attacker can have all the admin privileges
- He can edit all the items
- He can execute any harmful command through console

Recommendations

- Server side security checks should be performed perfectly
- Make the admin page url complicated so that it couldn’t be guessed

References

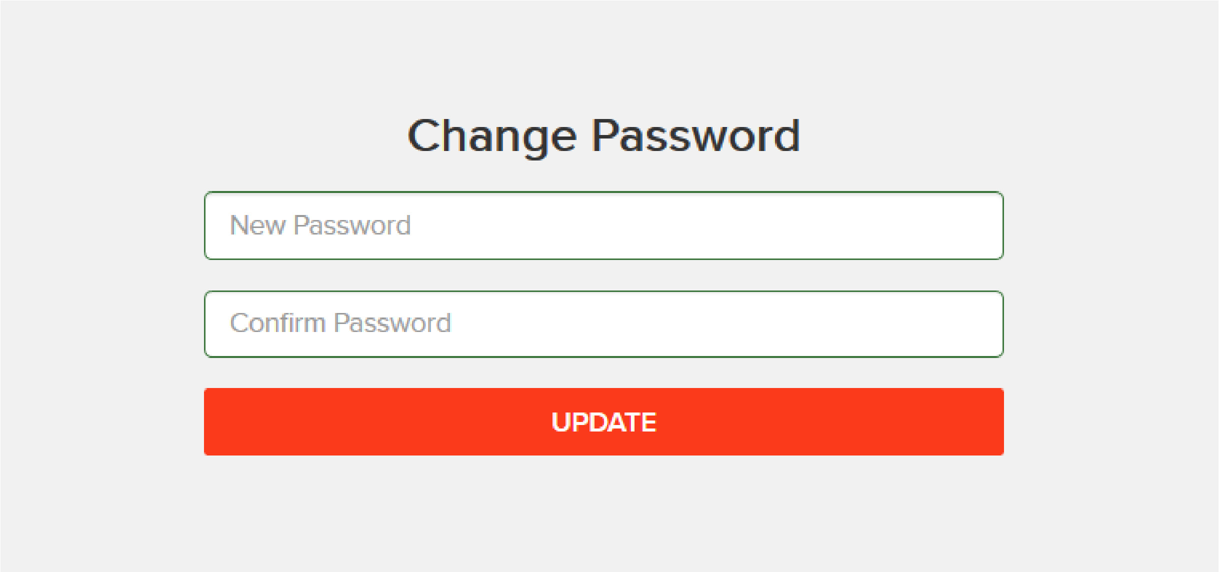
- https://owasp.org/www-community/attacks/Forced_browsing
- https://campus.barracuda.com/product/webapplicationfirewall/doc/42049348/forced-browsing-attack/

10.C.S.R.F.

CSRF	The url given below is vulnerable to CSRF • Affected url http://52.66.65.223/profile/change_password.php http://52.66.65.223/cart/cart.php

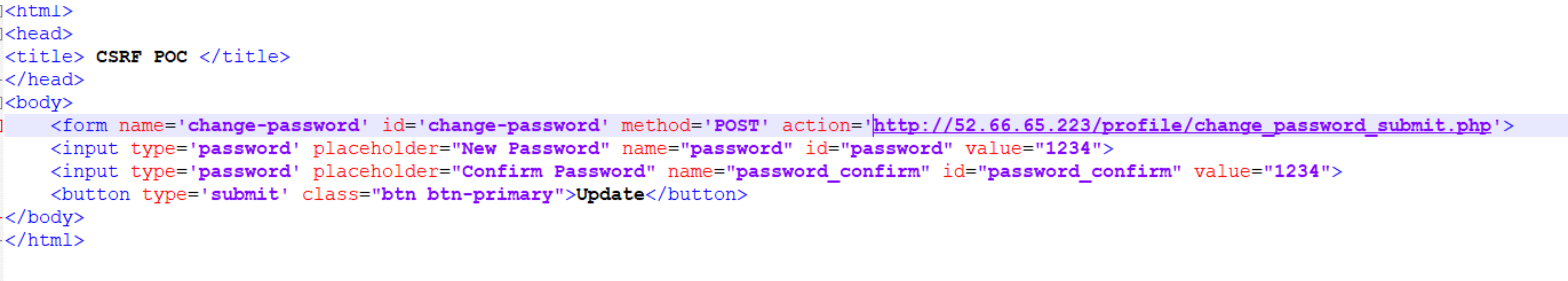
observations

- There is a change password option in profile page



POC

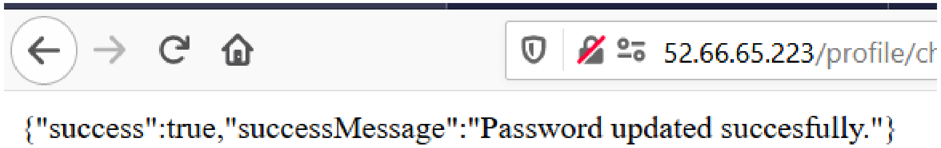
- Make a html page to change username and password



```
<html>
<head>
<title> CSRF POC </title>
</head>
<body>
    <form name='change-password' id='change-password' method='POST' action='http://52.66.65.223/profile/change_password_submit.php'>
    <input type='password' placeholder="New Password" name="password" id="password" value="1234">
    <input type='password' placeholder="Confirm Password" name="password_confirm" id="password_confirm" value="1234">
    <button type='submit' class="btn btn-primary">Update</button>
</body>
</html>
```

POC

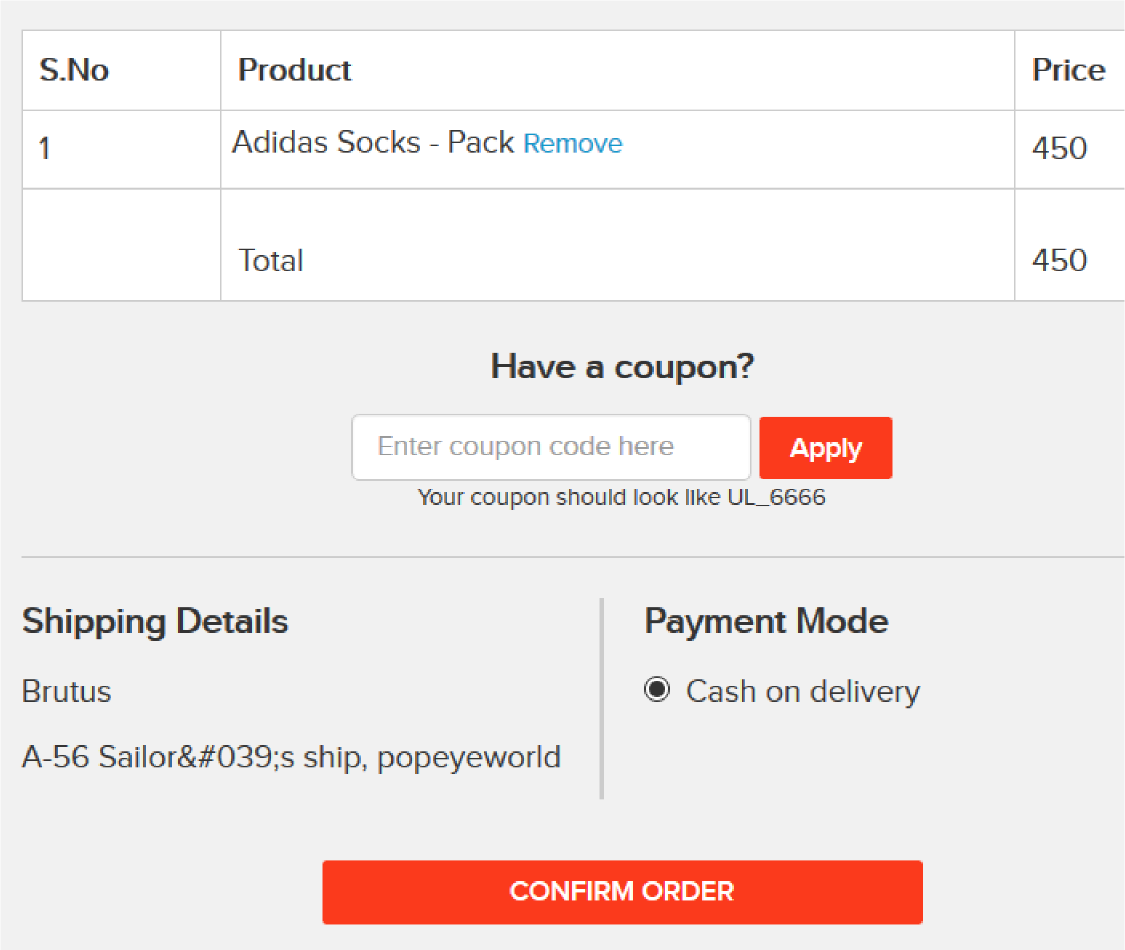
- On clicking the update button we get success



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

Observations

- There is a confirm button in my orders



S.No	Product	Price
1	Adidas Socks - Pack Remove	450
	Total	450

Have a coupon?

Your coupon should look like UL_6666

Shipping Details

Brutus

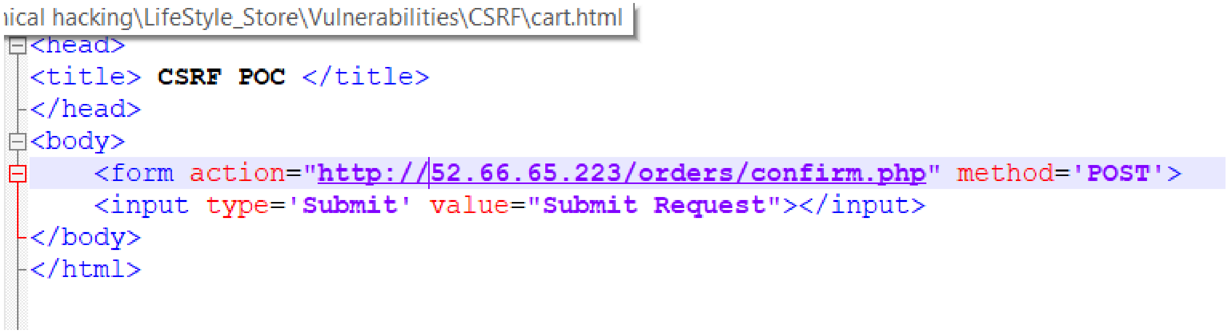
A-56 Sailor&#039;s ship, popeyeworld

Payment Mode

● Cash on delivery

POC

- Make a html page to confirm order

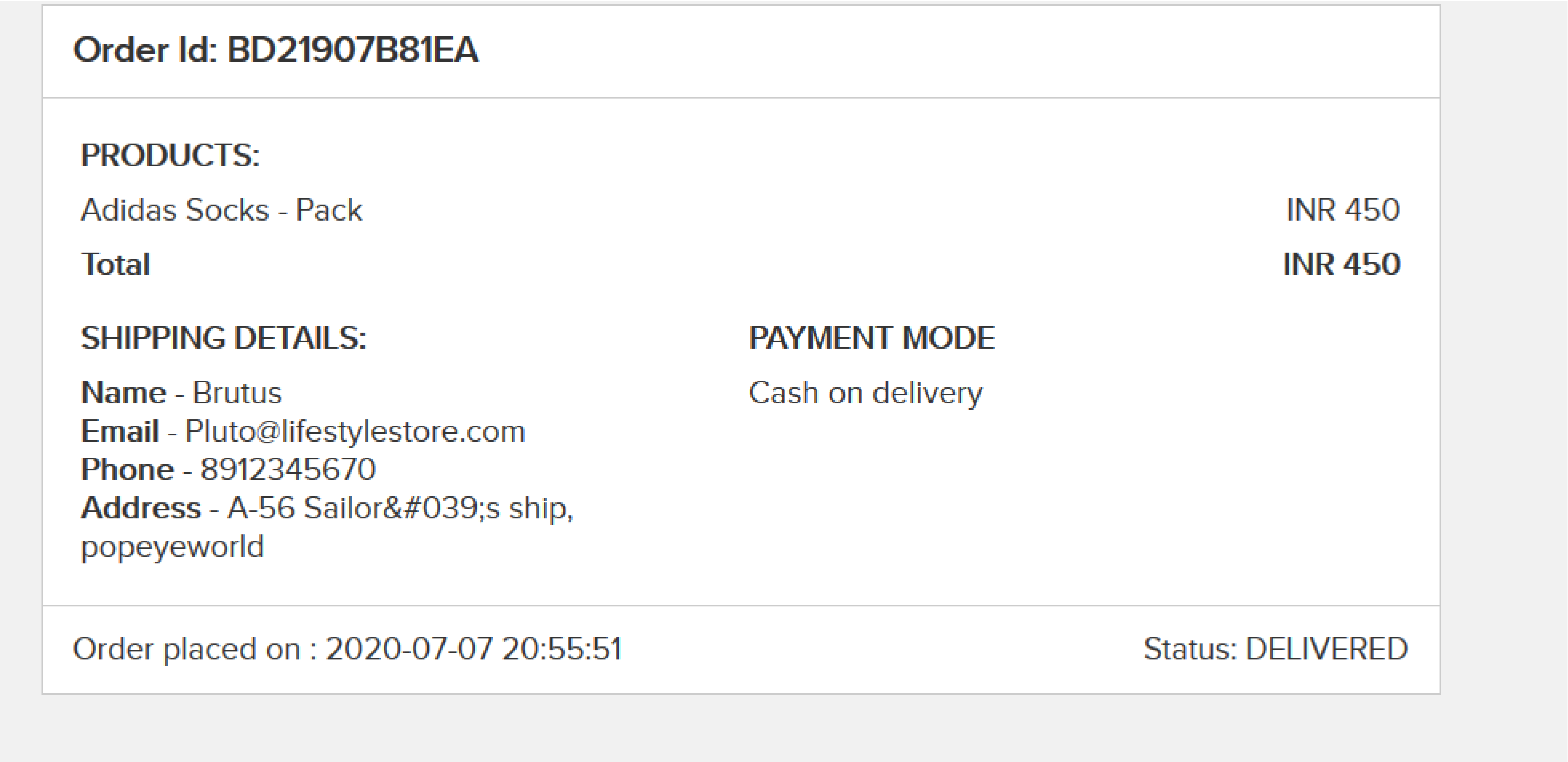


ical hacking\LifeStyle_Store\Vulnerabilities\CSRF\cart.html

```
<head>
<title> CSRF POC </title>
</head>
<body>
    <form action="http://52.66.65.223/orders/confirm.php" method='POST'>
    <input type='Submit' value="Submit Request"></input>
</body>
</html>
```

POC

- On executing the page order is confirmed



Order Id: BD21907B81EA

PRODUCTS:

Adidas Socks - Pack	INR 450
Total	**INR 450**

SHIPPING DETAILS:

Name - Brutus
Email - Pluto@lifestylestore.com
Phone - 8912345670
Address - A-56 Sailor&#039;s ship,
popeyeworld

PAYMENT MODE

Cash on delivery

Order placed on : 2020-07-07 20:55:51

Status: DELIVERED

Business impact- severe

- Attacker can change the password by uploading phishing pages
- Attacker can confirm the order without consent of user

Recommendations

- Use of tokens and session cookies
- Referrer header should be checked at server side

References

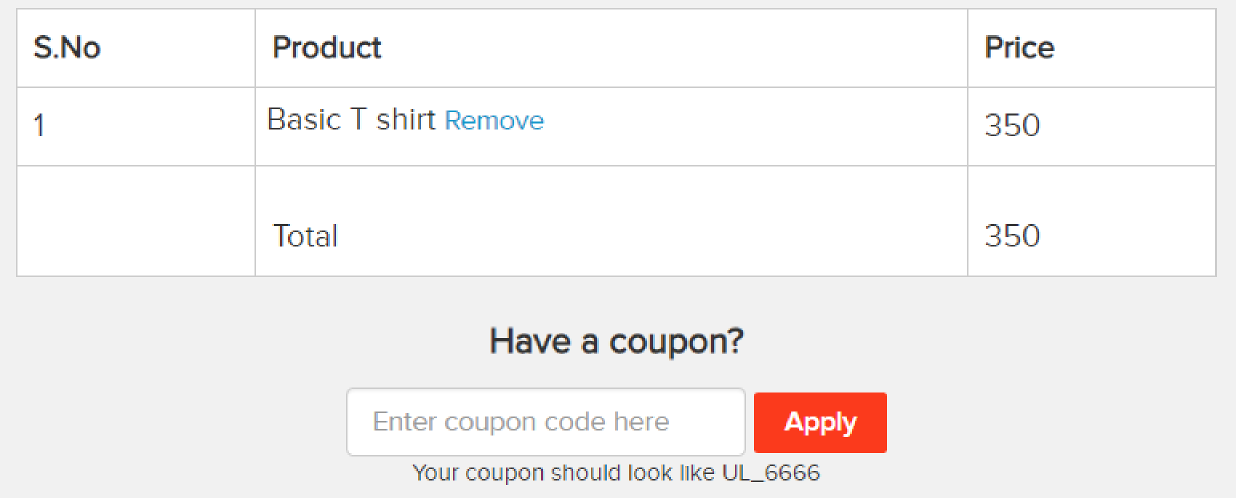
- https://owasp.org/www-community/attacks/csrf
- https://www.netsparker.com/blog/web-security/csrf-cross-site-request-forgery/

11.Coupon code brute forcing

Coupon code brute forcing	In the below url brute forcing can be performed for discounts • Affected url http://13.127.179.208/cart/apply_coupon.php

Observations

- When we go to the cart we see the apply coupon and coupon example



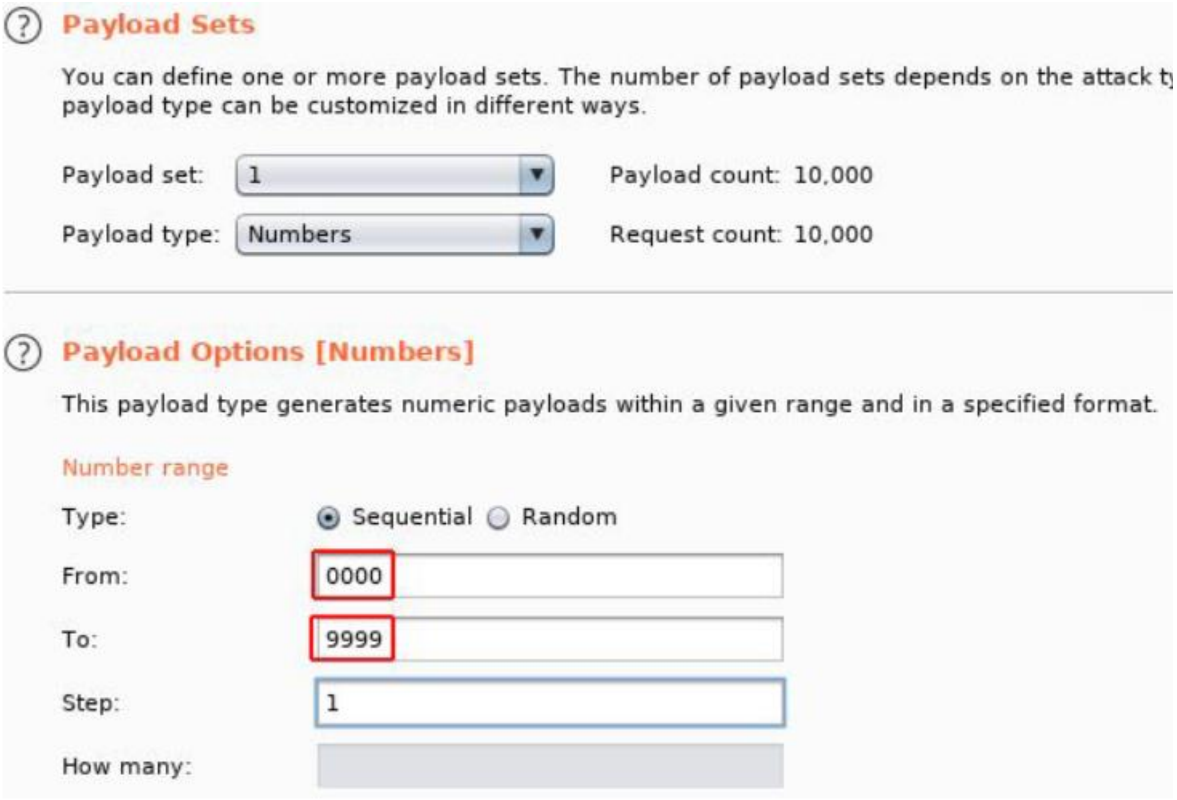
S.No	Product	Price
1	Basic T shirt Remove	350
	Total	350

Have a coupon?

Your coupon should look like UL_6666

Observations

Brute forcing the coupon code



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack ty
payload type can be customized in different ways.

Payload set: 1 Payload count: 10,000

Payload type: Numbers Request count: 10,000

Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: ● Sequential ○ Random

From: 0000

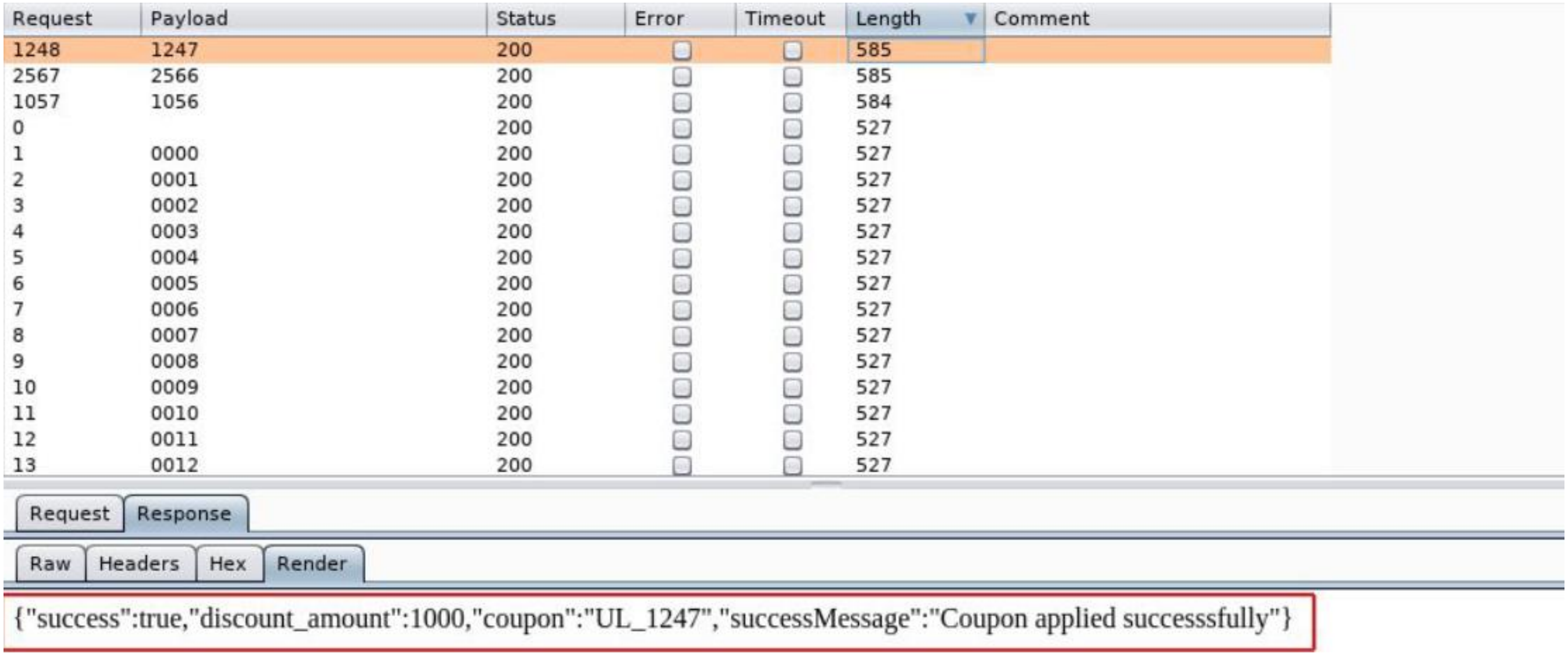
To: 9999

Step: 1

How many:

POC

- We were sucessful



Request	Payload	Status	Error	Timeout	Length	Comment
1248	1247	200	☐	☐	585	
2567	2566	200	☐	☐	585	
1057	1056	200	☐	☐	584	
0		200	☐	☐	527	
1	0000	200	☐	☐	527	
2	0001	200	☐	☐	527	
3	0002	200	☐	☐	527	
4	0003	200	☐	☐	527	
5	0004	200	☐	☐	527	
6	0005	200	☐	☐	527	
7	0006	200	☐	☐	527	
8	0007	200	☐	☐	527	
9	0008	200	☐	☐	527	
10	0009	200	☐	☐	527	
11	0010	200	☐	☐	527	
12	0011	200	☐	☐	527	
13	0012	200	☐	☐	527	

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

Business impact - severe

- Attacker can easily order the items on extreme discounts which will be harmful for the company

Recommendation

- Coupon codes should have limited no of use and regenerated after sometime
- Coupon code should be random alpha-numeric characters

References

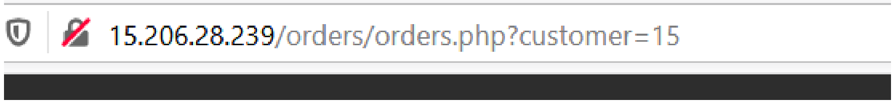
- https://www.digitalcommerce360.com/2017/03/17/prevent-fraud-brute-force-online-coupon-gift-card-attacks/
- https://www.couponxoo.com/brute-force-attack-coupon-code

12.Insecure direct object references

Insecure direct object references	The bellow mentioned url is vulnerable to IDOR • Affected url http://15.206.28.239/orders/orders.php?customer=(here) Payload 0-50

Observations

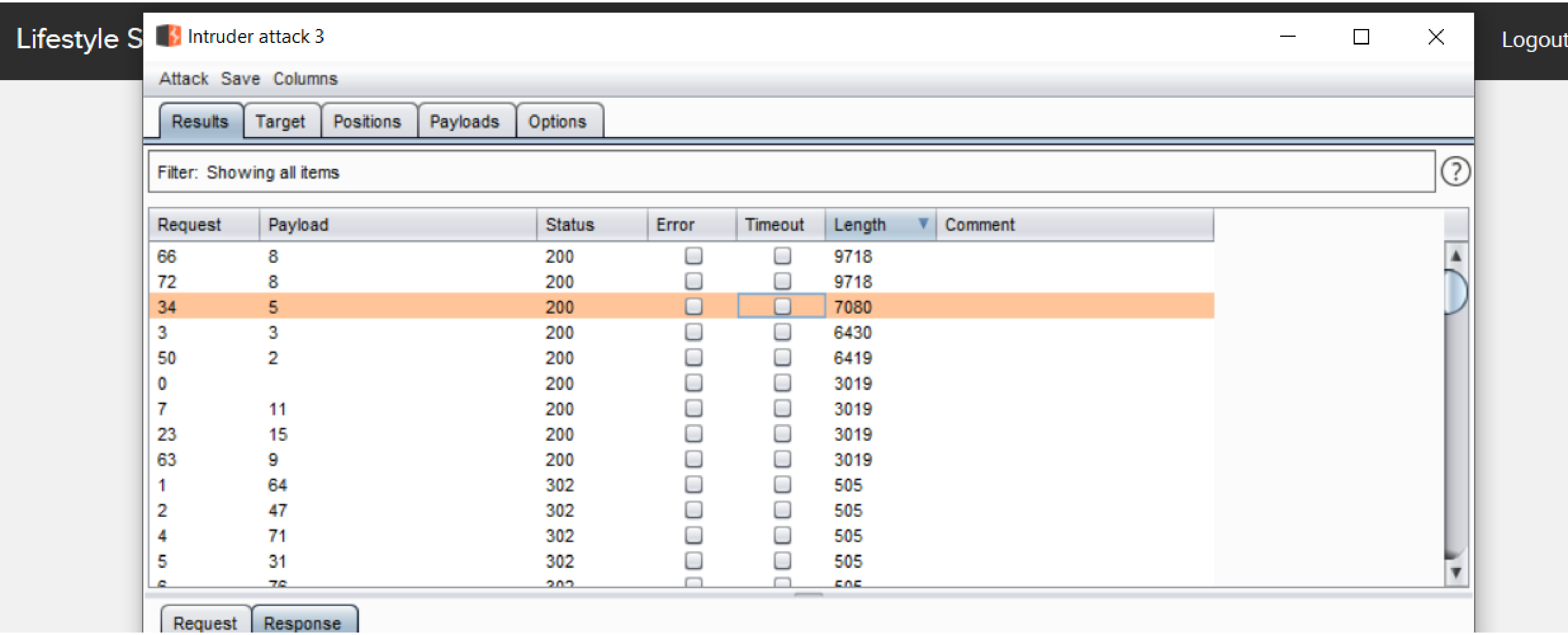
- In the my orders page I saw customer no in url



15.206.28.239/orders/orders.php?customer=15

Observations

- I brute forced it

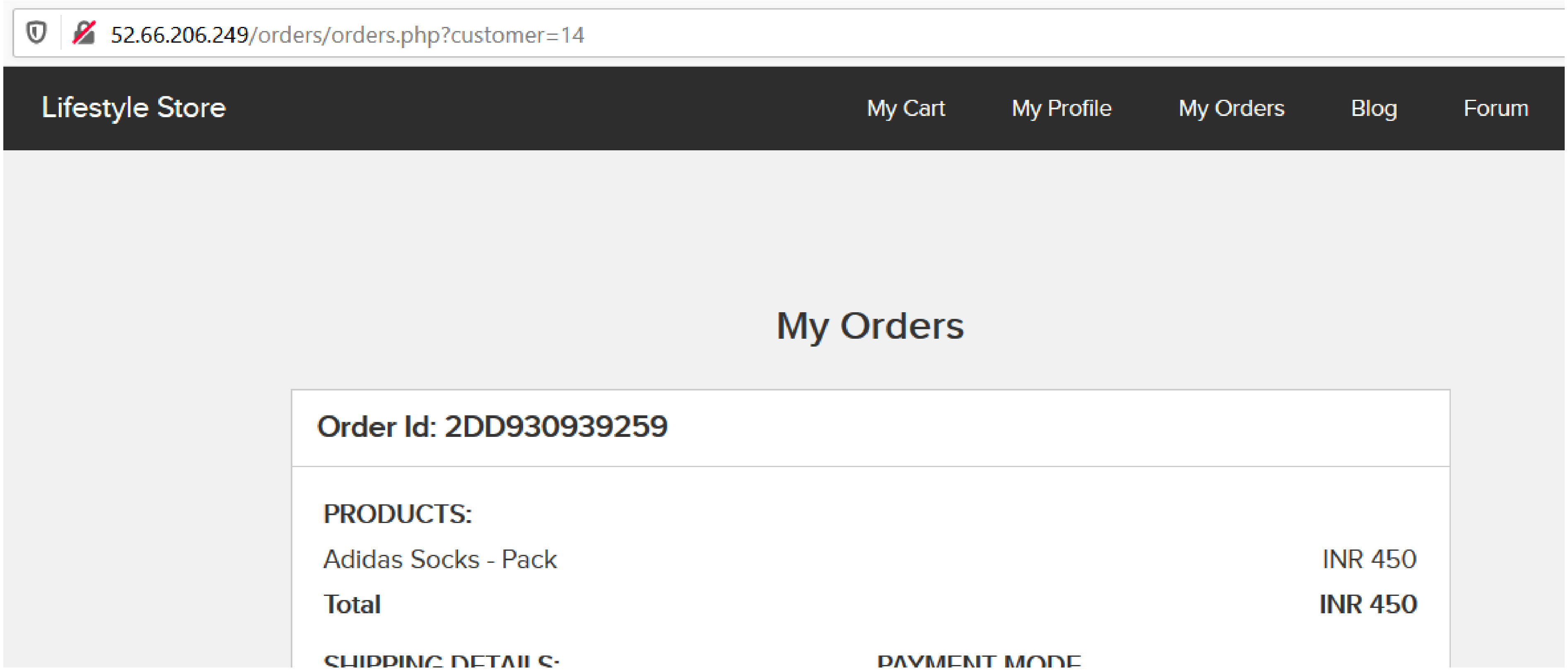


Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
66	8	200	□	□	9718	
72	8	200	□	□	9718	
34	5	200	□	□	7080	
3	3	200	□	□	6430	
50	2	200	□	□	6419	
0		200	□	□	3019	
7	11	200	□	□	3019	
23	15	200	□	□	3019	
63	9	200	□	□	3019	
1	64	302	□	□	505	
2	47	302	□	□	505	
4	71	302	□	□	505	
5	31	302	□	□	505	
6	76	302	□	□	505	

POC

- I got other customers and their order details



52.66.206.249/orders/orders.php?customer=14

My Orders

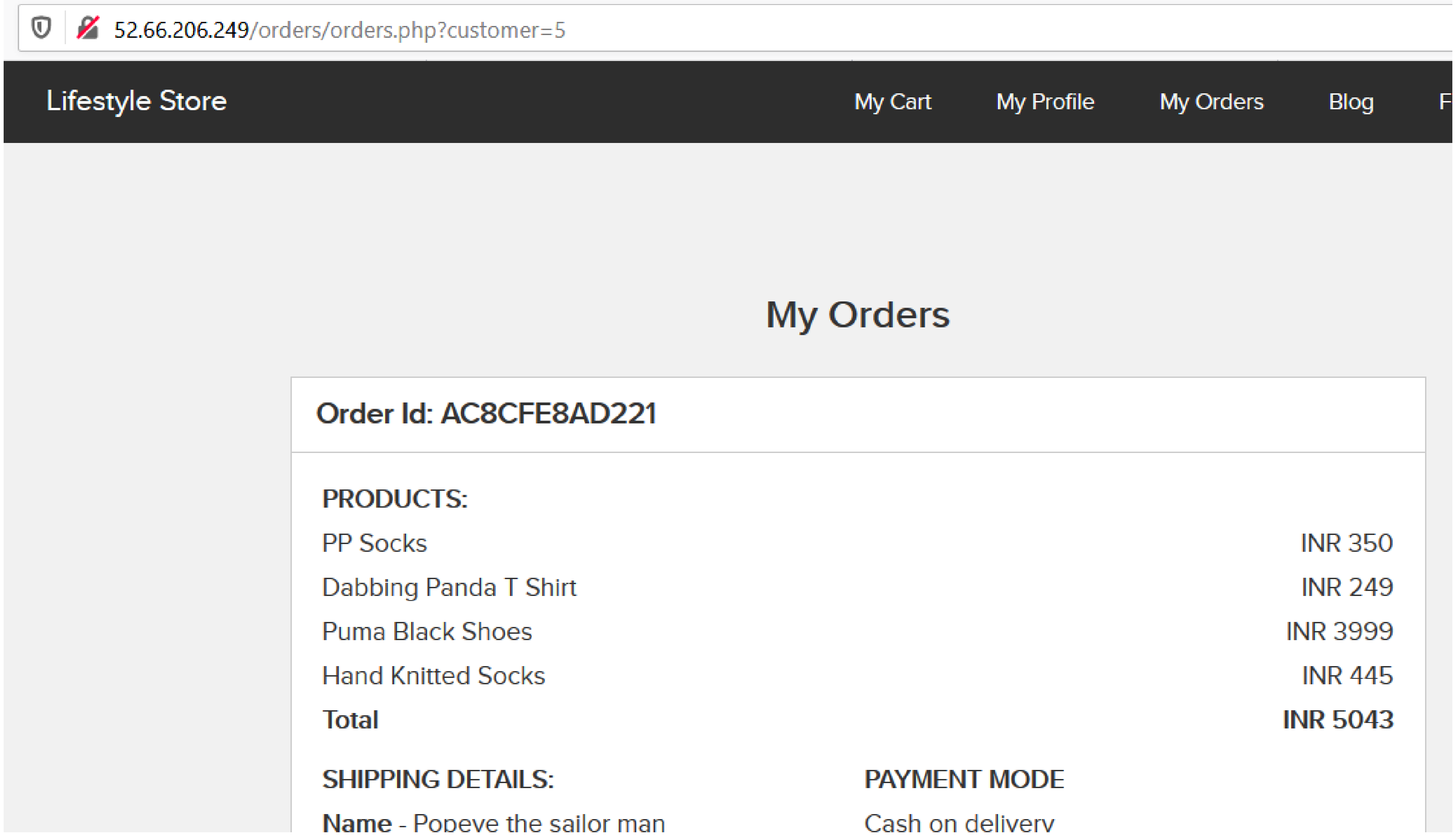
Order Id: 2DD930939259

PRODUCTS:

Adidas Socks - Pack	INR 450
Total	**INR 450**

SHIPPING DETAILS: **PAYMENT MODE**

POC



52.66.206.249/orders/orders.php?customer=5

My Orders

Order Id: AC8CFE8AD221

PRODUCTS:

PP Socks	INR 350
Dabbing Panda T Shirt	INR 249
Puma Black Shoes	INR 3999
Hand Knitted Socks	INR 445
Total	**INR 5043**

SHIPPING DETAILS:

Name - Popeye the sailor man

PAYMENT MODE

Cash on delivery

Recomendations

- Instead of requiring the references in the URL, use the information already present in the user's session on the server to locate the resources to serve.
- If it is not possible to avoid exposing the references to objects in the URL, as explained earlier, the *indirect reference map* technique is helpful. The idea behind it is to substitute the sensitive direct internal reference in URL parameters or form fields with a random value that is difficult to predict (such as a GUID) or specific only to the logged-in user

References

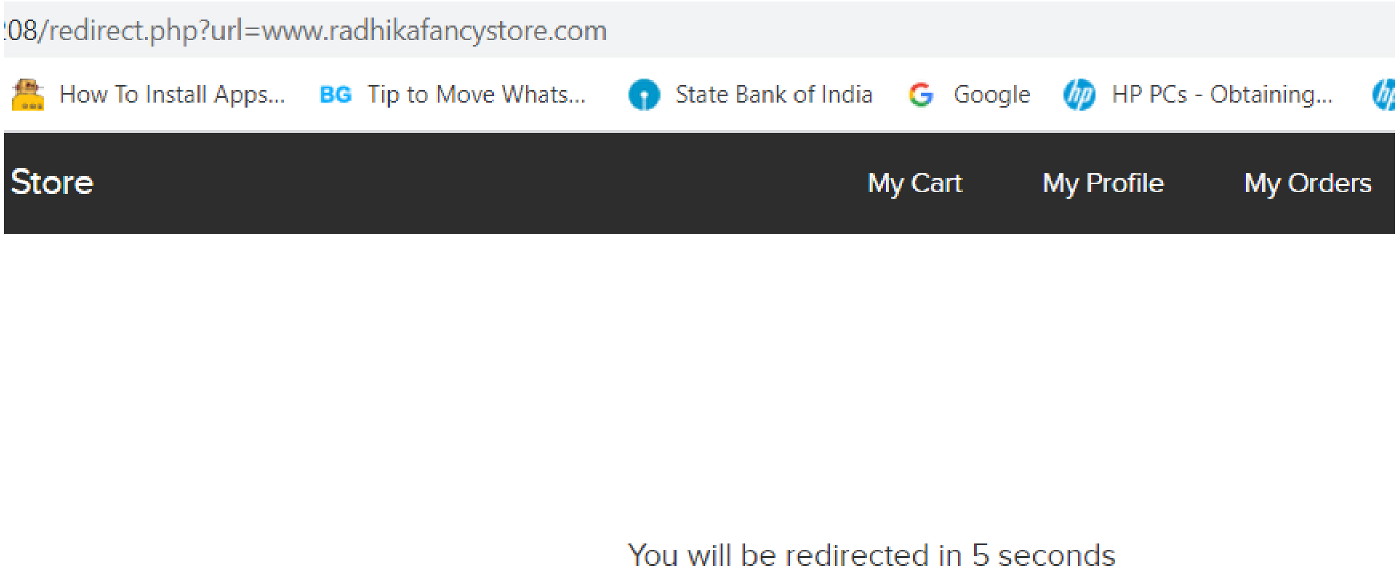
- https://www.oreilly.com/library/view/securing-node-applications/9781491982426/ch04.html
- https://cheatsheetseries.owasp.org/cheatsheets/Insecure_Direct_Object_Reference_Prevention_Cheat_Sheet.html

13.Open redirection

Open redirection	The url given below Is vulnerable to open redirection • Affected url http://13.127.179.208/redirect.php?url=(www.radhikafancystore.com) in the parentheses

Observations

- On clicking the brand website redirection occurs

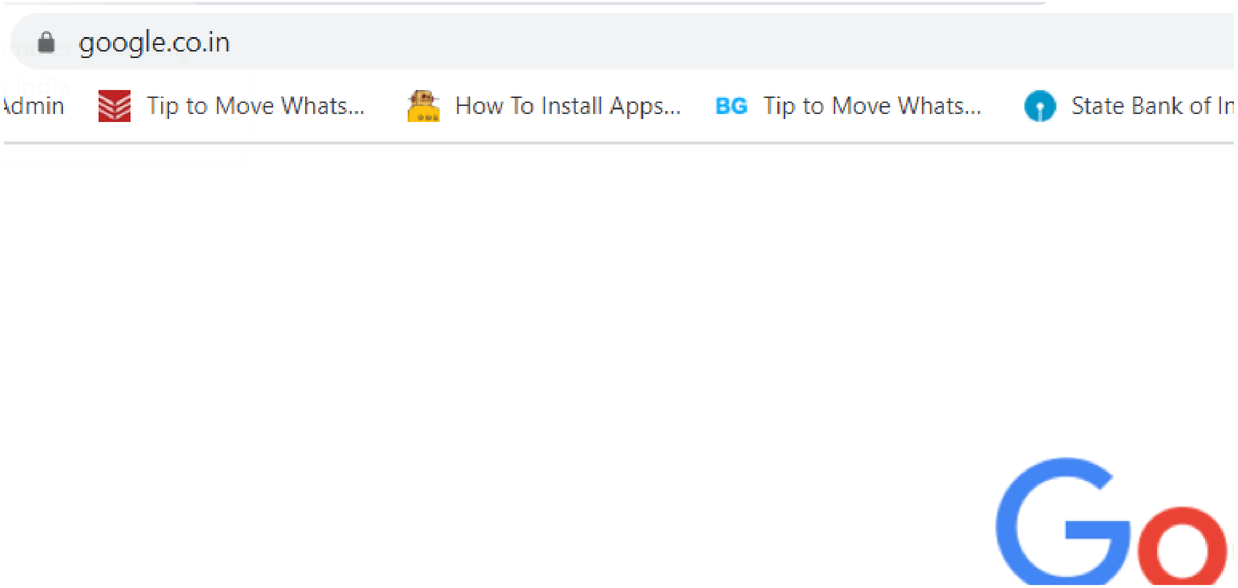


:08/redirect.php?url=www.radhikafancystore.com

You will be redirected in 5 seconds

POC

- On changing the link to google.co.in we were redirected to it



google.co.in

Admin · Tip to Move Whats... · How To Install Apps... · BG Tip to Move Whats... · State Bank of In

Business impact- severe

- He can access the users personnel credentials which would be very harmful
- They can redirect your page to a malware site
- They can redirect you to phishing pages

Recommendations

- Design your app to avoid URL redirects or forwards as a best practice. If unavoidable, encrypt the target URL such that the URL:token mapping is validated on the server.
- Verify URL patterns using regular expressions to check if they belong to valid URLs. However, malicious URLs can pass that check.
- Check your Referrers

References

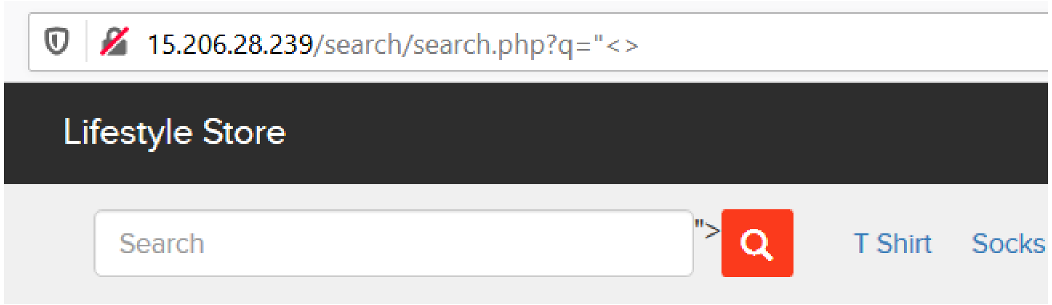
- https://spanning.com/blog/open-redirection-vulnerability-web-based-application-security-part-1/#:~:text=Understanding%20the%20Unvalidated%20Redirects%20Vulnerability&text=However%2C%20it%20can%20be%20misused,data%20and%20credibility%20into%20jeopardy.
- https://www.netsparker.com/blog/web-security/open-redirection-vulnerability-information-prevention/

14.Cross site scripting

Cross site scripting	The below mentioned urls are vulnerable to temporary and stored XSS • Affected urls Temporary -http://13.127.179.208/search/search.php?q=(here) Stored- http://13.127.179.208/products/details.php?p_id=(all id)

Observations

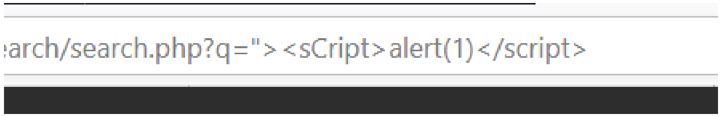
- In the search bar when I entered “<> I found this



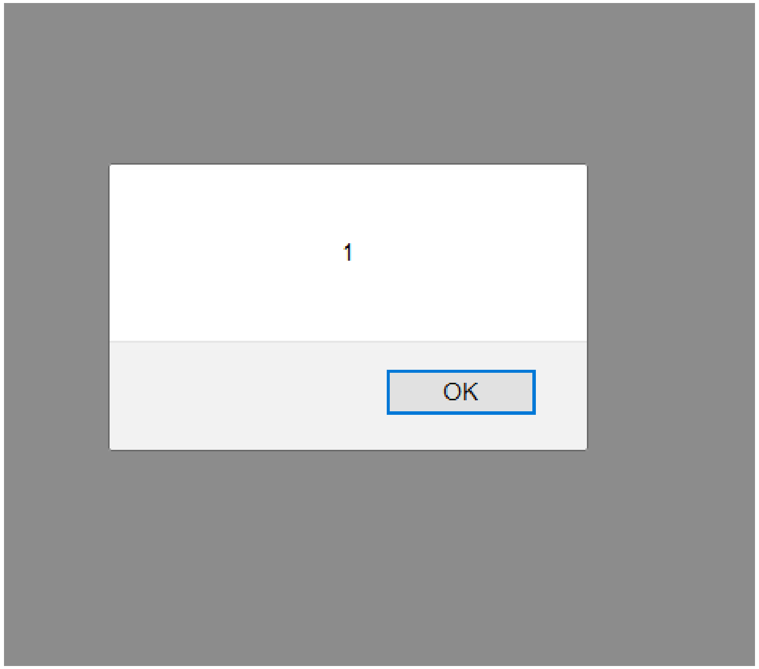
15.206.28.239/search/search.php?q="<>

POC

- When I entered the script popup code it was executed



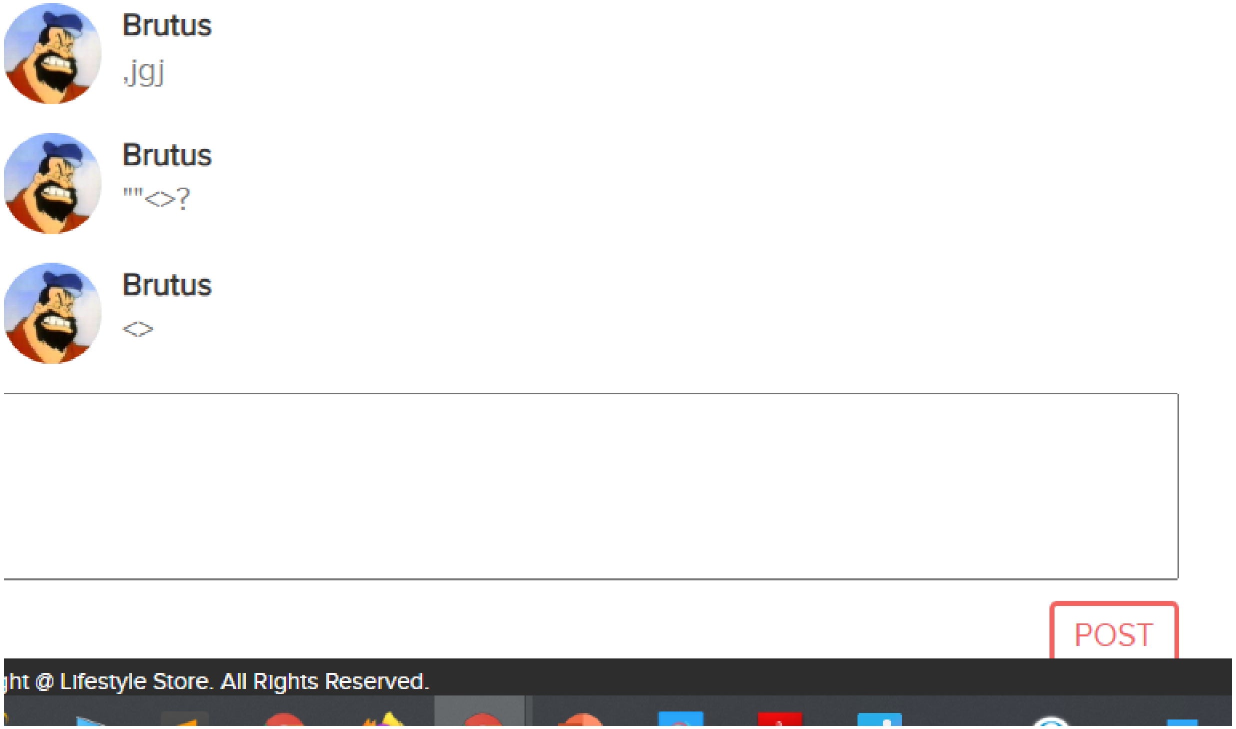
```
arch/search.php?q="><sCript>alert(1)</script>
```



1

Observations

- In the comment section of every product items the comment was stored



Brutus
,jgj

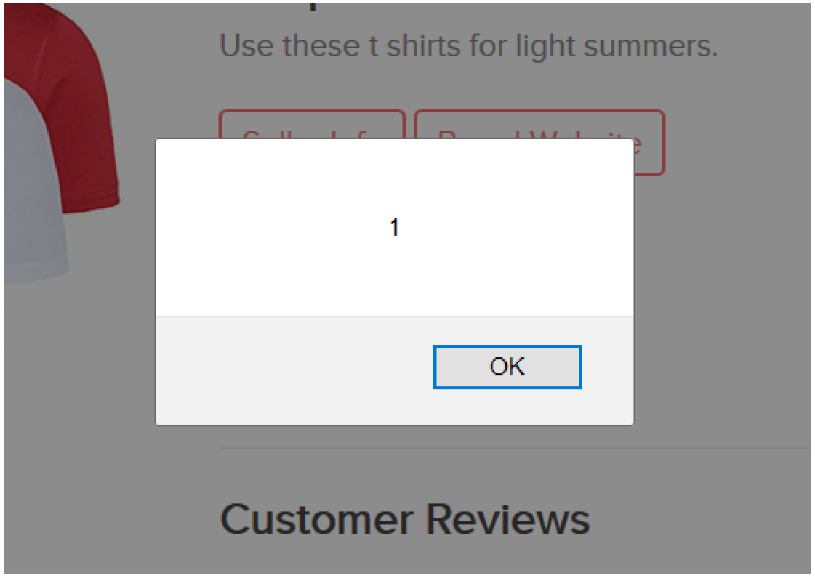
Brutus
""<>?

Brutus
<>

ht @ Lifestyle Store. All Rights Reserved.

POC

- When I entered the script pop up code it was executed and stored



Use these t shirts for light summers.

1

Customer Reviews

Business impact- severe

- Hacker can access any user credentials by injecting ***malicious*** scripts
- He can even change the html format of website

Recommendations

- By escaping user input. Escaping data means taking the data an application has received and ensuring it's secure before rendering it for the end user
- Validating input is the process of ensuring an application is rendering the correct data and preventing malicious data from doing harm to the site, database, and users
- A third way to prevent cross-site scripting attacks is to sanitize user input. Sanitizing data is a strong defense, but should not be used alone to battle XSS attacks

References

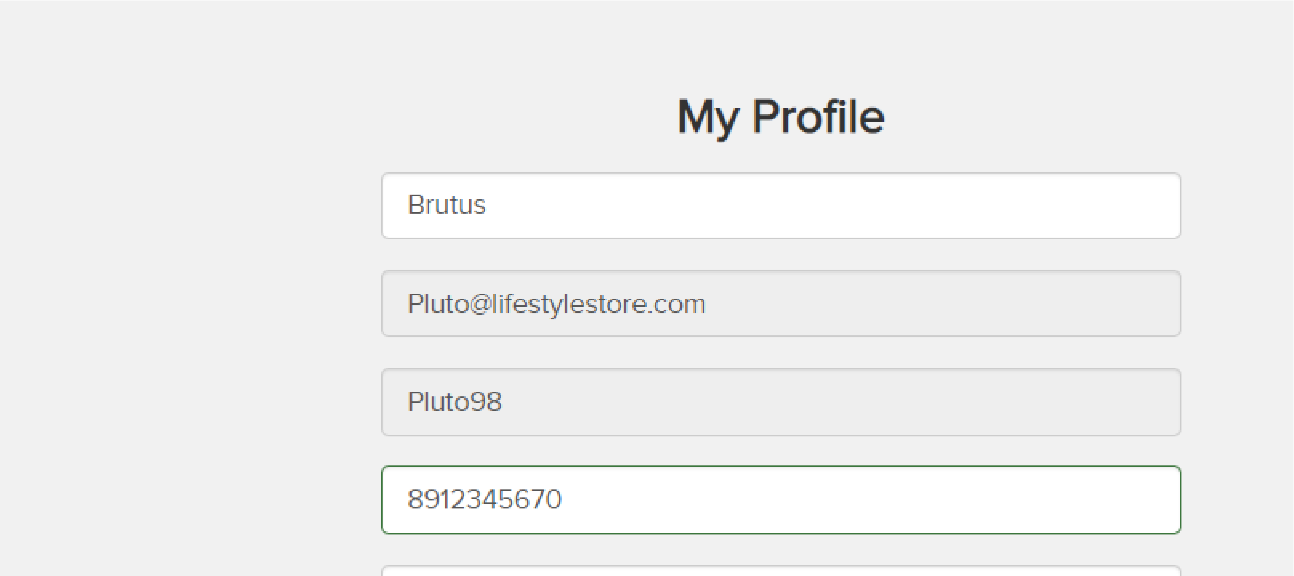
- https://www.checkmarx.com/2017/10/09/3-ways-prevent-xss/
- https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html
- https://owasp.org/www-community/attacks/xss/

15.Client side filter bypass

Client side filter bypass	The url given below is vulnerable to client side filter bypass • Afected url http://13.127.179.208/profile/3/edit/

Observations

- After changing the information I was able to change it again via client side filter bypass



My Profile

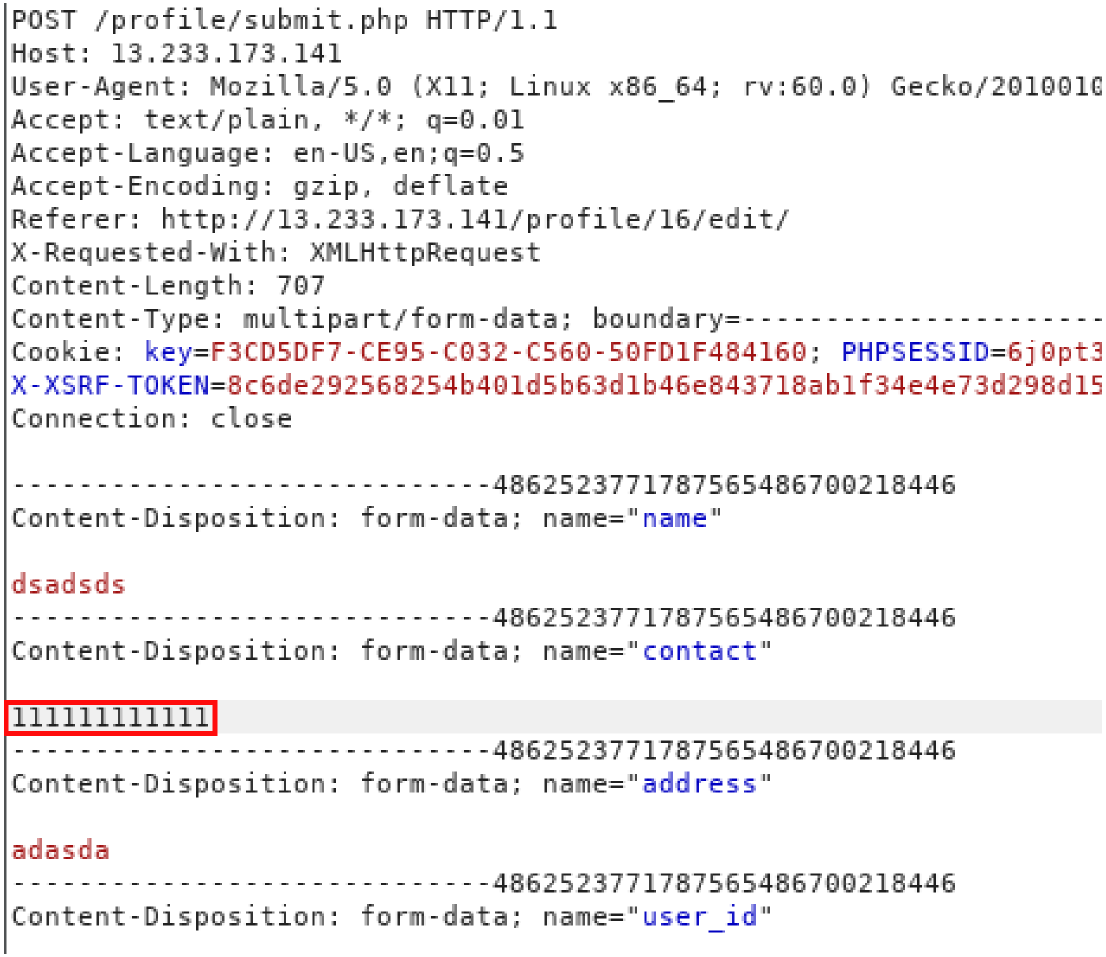
Brutus

Pluto@lifestylestore.com

Pluto98

8912345670

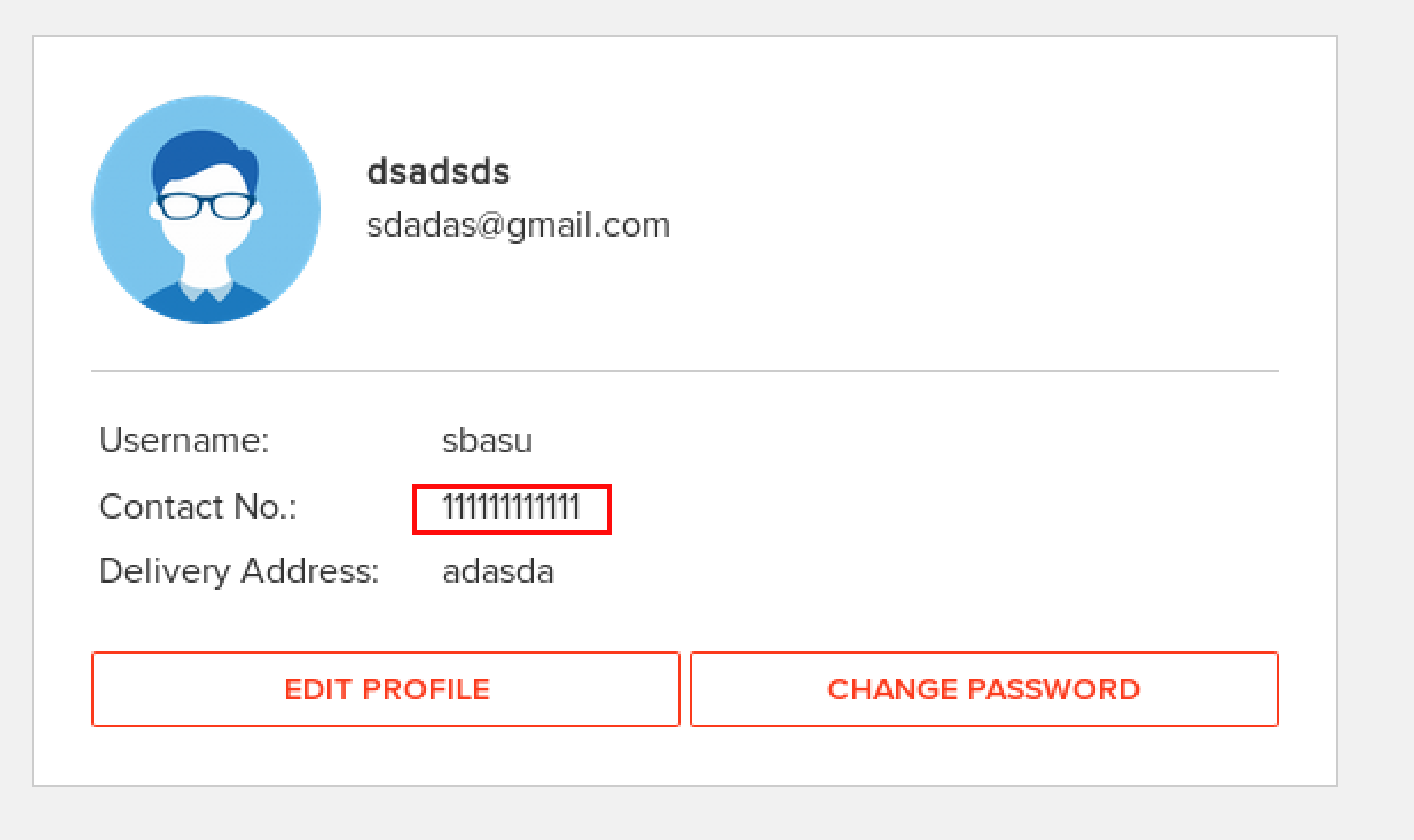
POC



```
POST /profile/submit.php HTTP/1.1
Host: 13.233.173.141
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/2010010
Accept: text/plain, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://13.233.173.141/profile/16/edit/
X-Requested-With: XMLHttpRequest
Content-Length: 707
Content-Type: multipart/form-data; boundary=----------------------
Cookie: key=F3CD5DF7-CE95-C032-C560-50FD1F484160; PHPSESSID=6j0pt3
X-XSRF-TOKEN=8c6de292568254b401d5b63d1b46e843718ab1f34e4e73d298d15
Connection: close

-----------------------------48625237717875654867002184446
Content-Disposition: form-data; name="name"

dsadsds
-----------------------------48625237717875654867002184446
Content-Disposition: form-data; name="contact"

111111111111
-----------------------------48625237717875654867002184446
Content-Disposition: form-data; name="address"

adasda
-----------------------------48625237717875654867002184446
Content-Disposition: form-data; name="user_id"
```

POC

- Original info was changed



dsadsds

sdadas@gmail.com

Username: sbasu

Contact No.: 111111111111

Delivery Address: adasda

Business impact-high

- This would only trouble the users which will be giving bad feed back on you website

Recommendations

- Cookies should be used .
- Referrer headers should be used
- Proper security checks should be done

References

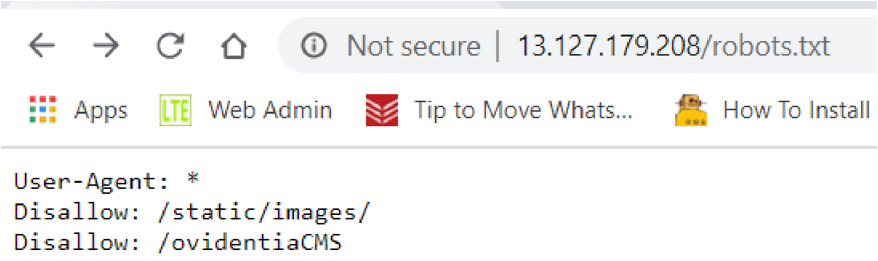
- https://portswigger.net/support/using-burp-to-bypass-client-side-javascript-validation
- https://www.slideshare.net/SamBowne/cnit-129s-ch-5-bypassing-clientside-controls

16.Directory listing

Directory listing	The url given below is listing the directories • Affected url http://13.127.179.208/static/images/

Observations

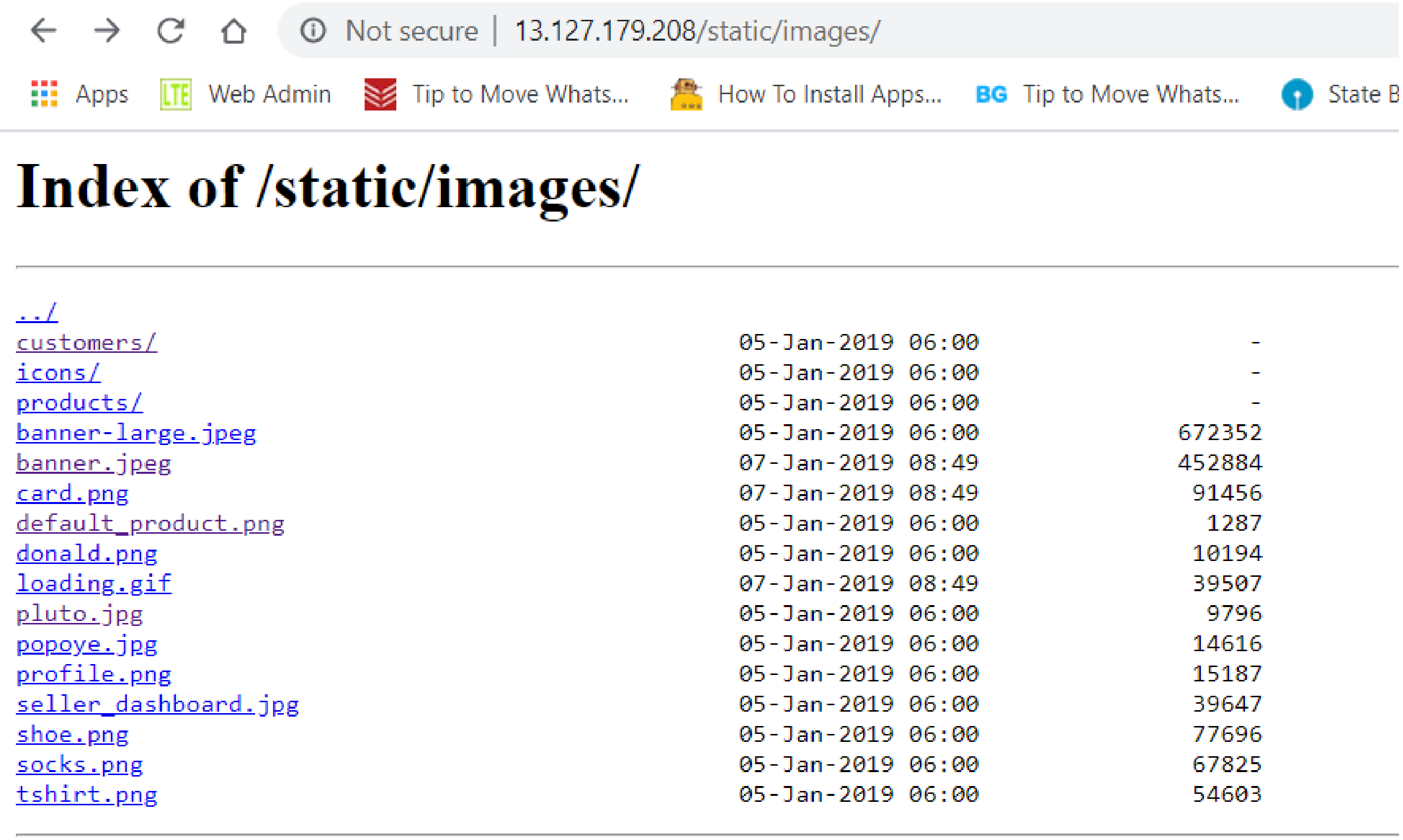
- In robots.txt file I found static/images/



```
User-Agent: *
Disallow: /static/images/
Disallow: /ovidentiaCMS
```

POC

- Listed directories



Index of /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
```

Business impact-high

- These directories will be useful for the attacker to collect information about the website

To plan a attack

Recommendations

- Disable these listed directories

References

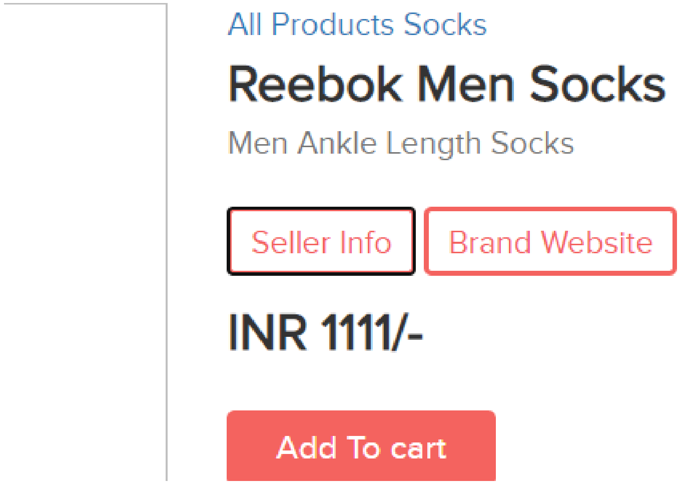
- https://www.acunetix.com/blog/articles/directory-listing-information-disclosure/

17.Personnel identifiable information-leakage

Personnel identifiable information	The url given below has PII-leakage • Affected url http://13.127.179.208/products/details.php?p_id=(all)

Observations

In every product pages the seller info option is available



All Products Socks

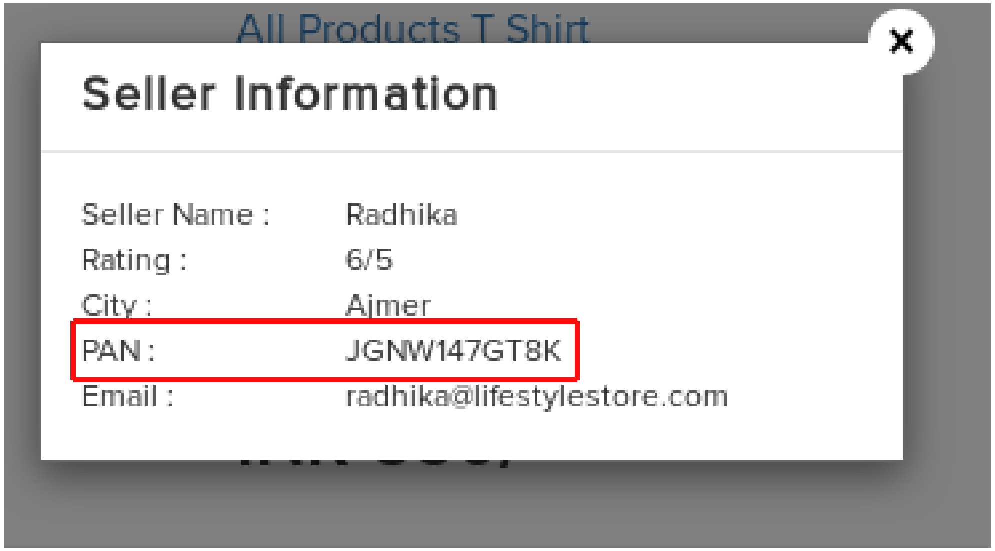
Reebok Men Socks

Men Ankle Length Socks

INR 1111/-

POC

- Pan card details are also shown



Seller Information

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

Business impact - high

- Providing the Seller information may uninterest people to buy the item
- It may also cause social engineering attacks on seller

Recommendations

- Remove the pan card details
- Only show required information about anyone

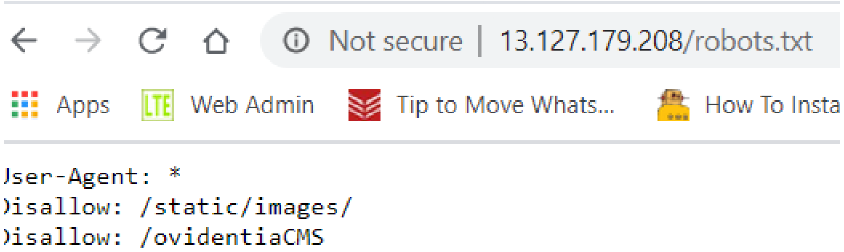
References

- https://www.imperva.com/learn/data-security/personally-identifiable-information-pii/
- https://hackerone.com/reports/374007

18.Default and debug files

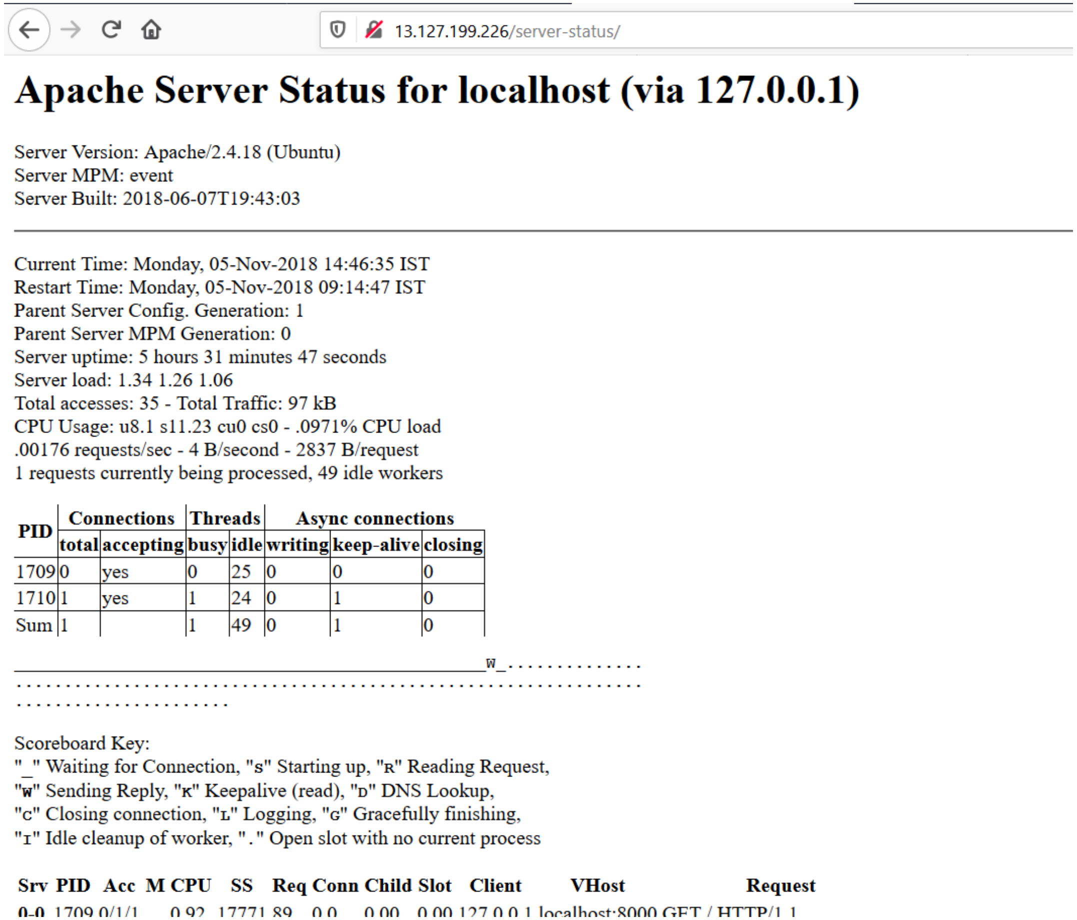
Default and debug files	Below mentione url has many default and debug files • Affected url http://13.127.179.208/ • Default pages 1. robots.txt 2. server-status 3. phpinfo.php 4. composer.json 5. userlist.txt

POC



```
Jser-Agent: *
)isallow: /static/images/
)isallow: /ovidentiaCMS
```

POC



13.127.199.226/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 cs0 - .0971% CPU load
.00176 requests/sec - 4 B/second - 2837 B/request
1 requests currently being processed, 49 idle workers

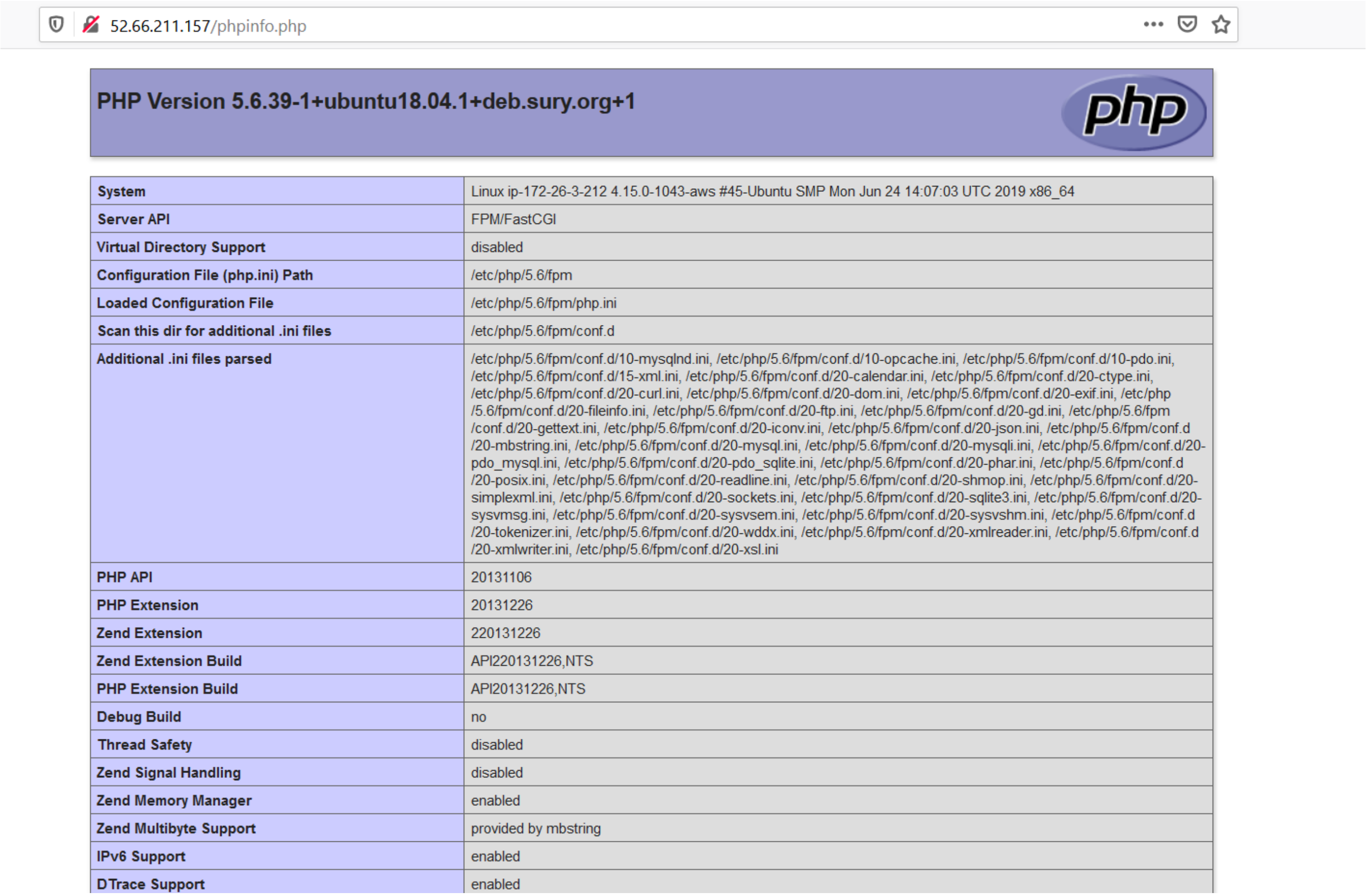
PID	Connections		Threads		Async connections		
	total	accepting	busy	idle	writing	keep-alive	closing
1709	0	yes	0	25	0	0	0
1710	1	yes	1	24	0	1	0
Sum	1		1	49	0	1	0

```
________________________________________________W_...............
..................................................................
......................
```

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	0/1/1		0.92	17771	89	0.0	0.00	0.00	127.0.0.1	localhost:8000	GET / HTTP/1.1

POC

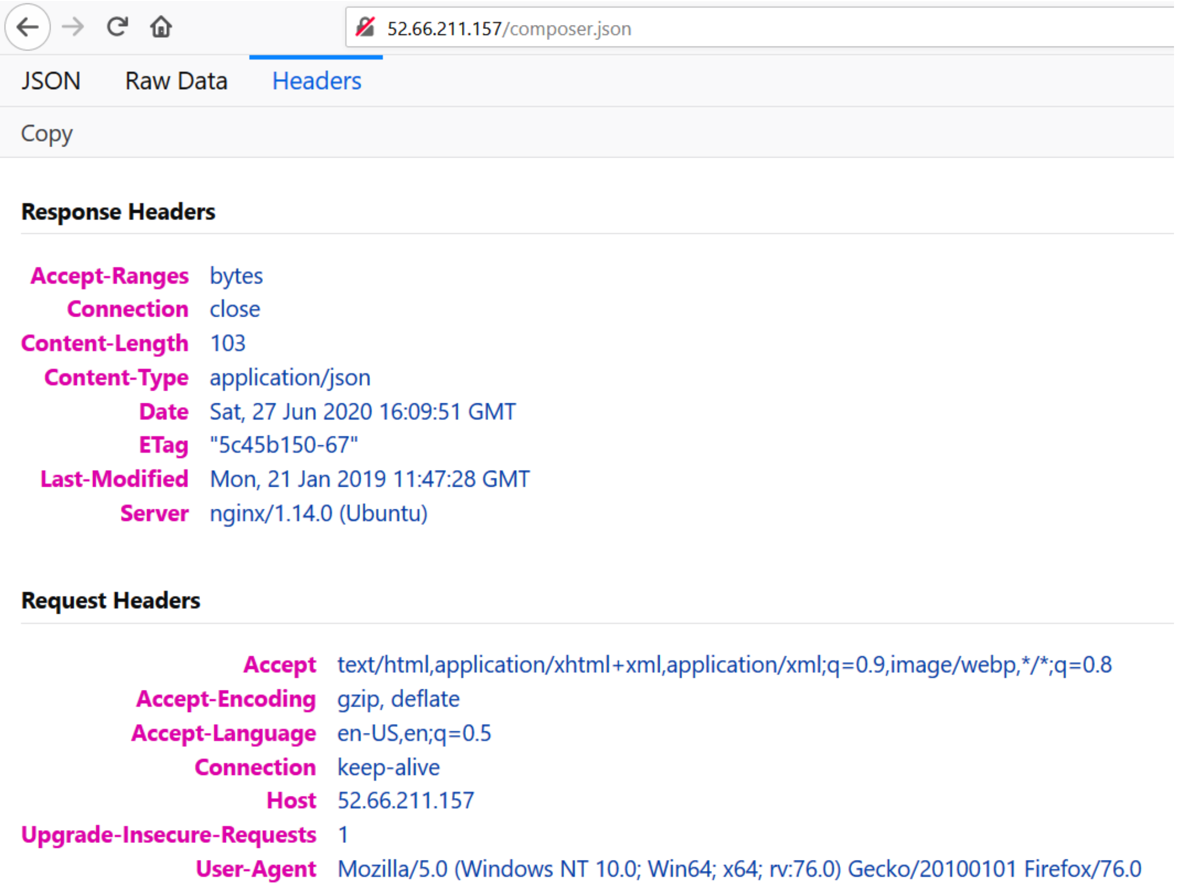


52.66.211.157/phpinfo.php

PHP Version 5.6.39-1+ubuntu18.04.1+deb.sury.org+1

System	Linux ip-172-26-3-212 4.15.0-1043-aws #45-Ubuntu SMP Mon Jun 24 14:07:03 UTC 2019 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-mysqlnd.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-xml.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-json.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-sysvmsg.ini, /etc/php/5.6/fpm/conf.d/20-sysvsem.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

POC



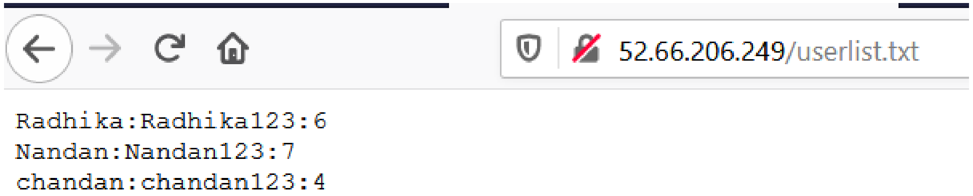
Response Headers

```
     Accept-Ranges  bytes
        Connection  close
    Content-Length  103
      Content-Type  application/json
              Date  Sat, 27 Jun 2020 16:09:51 GMT
              ETag  "5c45b150-67"
     Last-Modified  Mon, 21 Jan 2019 11:47:28 GMT
            Server  nginx/1.14.0 (Ubuntu)
```

Request Headers

```
                   Accept  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
          Accept-Encoding  gzip, deflate
          Accept-Language  en-US,en;q=0.5
               Connection  keep-alive
                     Host  52.66.211.157
Upgrade-Insecure-Requests  1
               User-Agent  Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:76.0) Gecko/20100101 Firefox/76.0
```

POC



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

Business impact - low

- It does not impact the website directly
- It only helps hacker to collect information

Recommendations

- Disable all these default pages

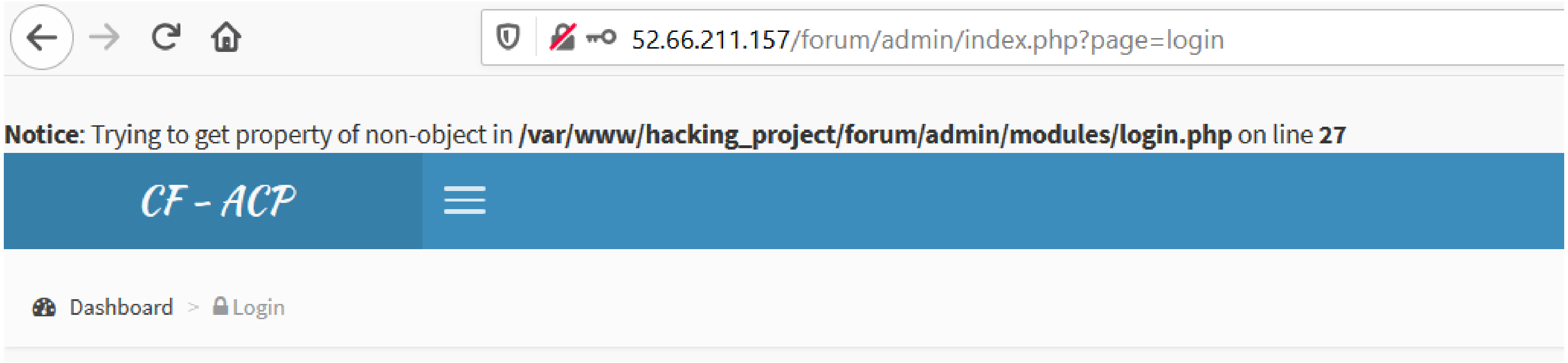
References

- https://www.indusface.com/blog/owasp-security-misconfiguration/
- https://hdivsecurity.com/owasp-security-misconfiguration

19.Descriptive error messages

Descriptive error messages	Below mentioned url shows Descriptive error messages • Affected url http://52.66.211.157/forum/admin/index.php?page=login http://52.66.206.249/?includelang=lang?’

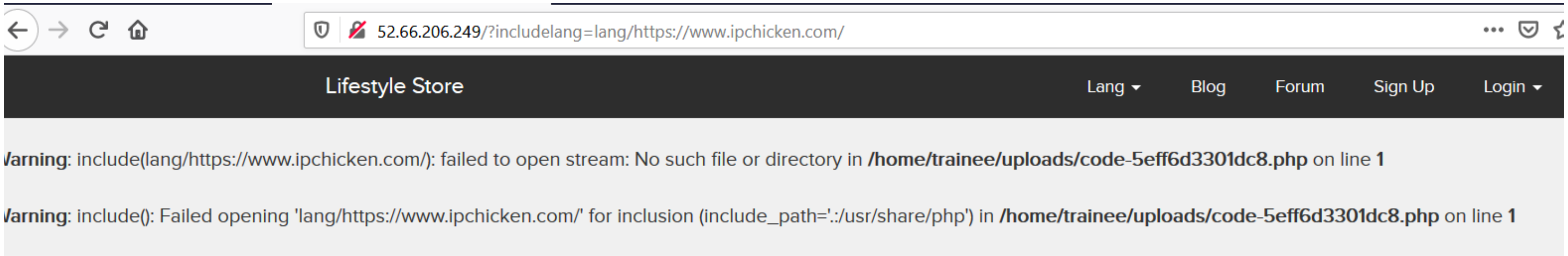
POC



52.66.211.157/forum/admin/index.php?page=login

Notice: Trying to get property of non-object in **/var/www/hacking_project/forum/admin/modules/login.php** on line **27**

POC



```
Varning: include(lang/https://www.ipchicken.com/): failed to open stream: No such file or directory in /home/trainee/uploads/code-5eff6d3301dc8.php on line 1

Varning: include(): Failed opening 'lang/https://www.ipchicken.com/' for inclusion (include_path='.:/usr/share/php') in /home/trainee/uploads/code-5eff6d3301dc8.php on line 1
```

Business impact-low

- It doesn’t harm the website directly
- But it is letting the hacker to know about the website architecture

Recommendations

- Block these kind of error pages to show up
- Only show simple error pages

References

- https://owasp.org/www-community/Improper_Error_Handling#:~:text=Description,to%20the%20user%20(hacker).
- https://cwe.mitre.org/data/definitions/209.html

THANK YOU

FOR FURTHER CLASSIFICATION / PATCH ASSISTANCE CONTACT - 8765858457