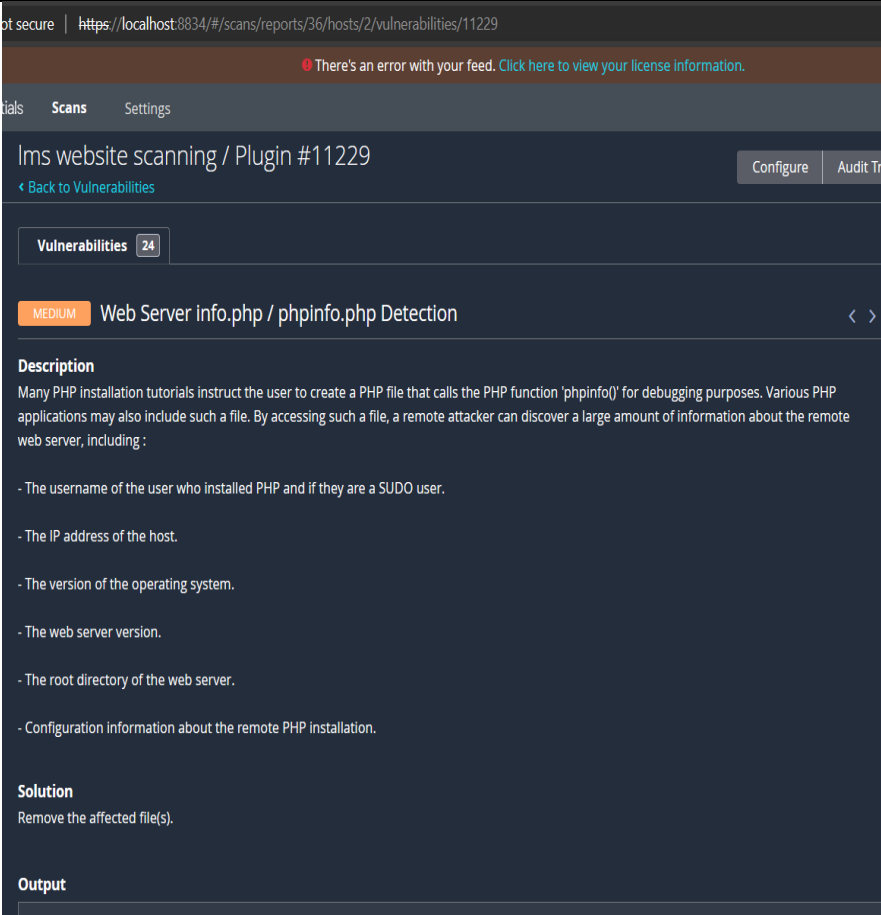


Title: Hidden File Found	
Description:	
Phpinfo.php page Detection, it includes admin detail and other installed and supported software information.	
Affected Resources	Severity
<a href="#">phpinfo() (aristopharma.co.in)</a>	<b>Critical</b>
Impact	
By accessing such a file, a remote attacker can discover a large amount of information about the remote web server, including:-	
<ul style="list-style-type: none"> <li>- The root directory of the web server.</li> <li>- Configuration information about the remote PHP installation.</li> </ul>	
Recommendation	
Remove the affected file	
Tool Used	References
Nessus	<a href="https://www.php.net/manual/en/function.phpinfo.php">https://www.php.net/manual/en/function.phpinfo.php</a>
POC	
 <p>The screenshot displays a Nessus vulnerability report for the 'Web Server info.php / phpinfo.php Detection' plugin (ID #11229). The severity is marked as 'MEDIUM'. The description explains that many PHP installation tutorials instruct users to create a PHP file that calls the 'phpinfo()' function for debugging purposes, which can reveal sensitive information about the remote web server. The report lists several pieces of information discovered, including the username of the user who installed PHP, the IP address of the host, the version of the operating system, the web server version, the root directory of the web server, and configuration information about the remote PHP installation. A solution is provided: 'Remove the affected file(s)'. The output section is also visible but contains no data.</p>	

## Title: Insure Communication

### Description:

Insecure Communication over http request leads to packet capturing and reveal the information over network.

### Affected Resources

<http://lms.aristopharma.co.in/>

### Severity

High

### Impact

The attacker can get victim passwords , can do MITM attacks.

### Recommendation

Do not allow the website open in http request ,use SSL Certificate

### Tool Used

WireShark

### References

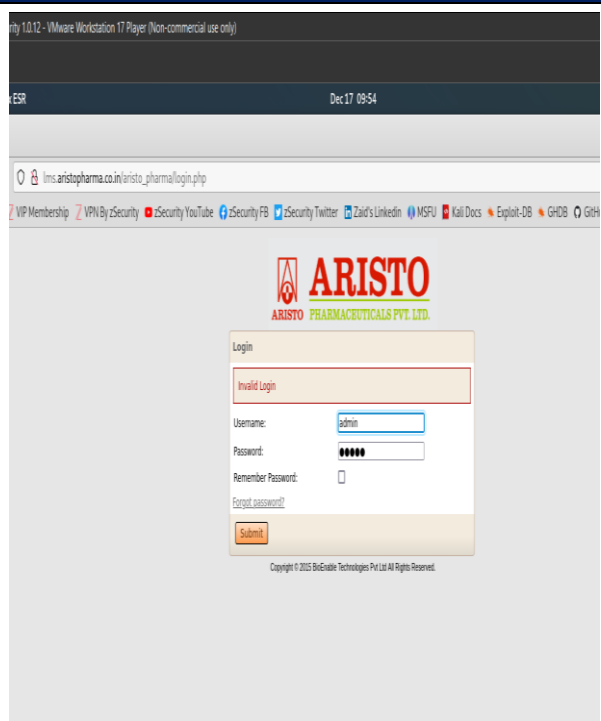
[M3: Insecure Communication | OWASP Foundation](#)


### POC

```
Wireshark - Packet 28 - eth0
Frame 28: 674 bytes on wire (5392 bits), 674 bytes captured (5392 bits) on inter
Ethernet II, Src: VMware_9e:83:3a (00:0c:29:9e:83:3a), Dst: VMware_f3:ec:38 (00:
Internet Protocol Version 4, Src: 192.168.150.128, Dst: 110.173.184.231
Transmission Control Protocol, Src Port: 56848, Dst Port: 80, Seq: 1, Ack: 1, Le
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "btnSubmit" = "Login"
Form item: "username" = "admin"
Form item: "password" = "admin"

0000  00 50 56 f3 ec 38 00 0c 29 9e 83 3a 00 00 45 00  .PV.8.).:..E
0010  02 94 eb cb 40 00 40 06 cd da c0 a8 96 80 6e ad  .@_@.....n
0020  b8 e7 de 10 00 50 80 c9 c2 83 5a ec 3d e1 50 18  .P...Z=P
0030  fa f0 81 44 00 00 50 4f 53 54 20 2f 61 72 69 73  .D.PO ST /aris
0040  74 6f 5f 70 68 61 72 6d 61 2f 6c 6f 67 69 6e 2e  to_pharm a/login.
0050  70 68 70 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f  php HTTP /1.1..Ho
0060  73 74 3a 20 6c 6d 73 2e 61 72 69 73 74 6f 70 68  st: lms. aristoph
0070  61 72 6d 61 2e 63 6f 2e 69 6e 0d 0a 55 73 65 72  arma.co. in .User
0080  2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f  -Agent: Mozilla/
0090  35 2e 30 20 28 58 31 31 3b 20 4c 69 6e 75 78 20  5.0 (X11; Linux
00a0  78 38 36 5f 36 34 3b 20 72 76 3a 39 31 2e 30 29  x86_64; rv:91.0)
00b0  20 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 31 20  Gecko/2.0.0.101
00c0  46 69 72 65 66 6f 78 2f 39 31 2e 30 0d 0a 41 63  Firefox/ 91.0. Ac
00d0  63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c  cept: te xt/html,
00e0  61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d  applicat ion/xhtm
00f0  6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f  l+xml,ap plicatio
0100  6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67  n/xml;q= 0.9,imag
0110  65 2f 77 65 62 70 2c 2a 2f 2a 3b 71 3d 30 2e 38  e/webp,* /*;q=0.8
0120  0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67  .Accept -Languag

No. 28 - Time: 0.709183217 - Source: 192.168.150.128 - Destin...o_pharma/login.php HTTP/1.1 (application/x-www-form-urlencoded)
```



Title: Found Open Ports	
Description:	
Open Ports are revealing the Service Version that the server is running On.	
Affected Resources	Severity
http://lms.aristopharma.co.in/	High
Impact	
The attacker can use this version for finding exploits (pentesting using Metasploit)	
Recommendation	
Please the in Production that the relevant ports are required, keep the server up to date	
Tool Used	References
NMAP	<a href="#">WSTG - Latest</a>   <a href="#">OWASP Foundation</a>
POC	
 Kali 2022 x64 Customized by zSecurity 1.0.12 - VMware Workstation 17 Player (Non-commercial use only)	
Player ▾    ▾ ⏏ ⏏ ⏏	
Applications Places Terminator	
<pre> root@kali:~# nmap -sV 110.173.184.231 Starting Nmap 7.92 ( https://nmap.org ) at 2023-12-17 09:52 EST Nmap scan report for 110.173.184.231 Host is up (0.0046s latency). Not shown: 995 filtered tcp ports (no-response) PORT      STATE SERVICE      VERSION 21/tcp    open  tcpwrapped 80/tcp    open  http         Apache httpd 2.2.15 ((CentOS)) 554/tcp   open  rtsp? 1723/tcp  open  pptp? 3306/tcp  open  mysql        MySQL 5.1.73 </pre>	

Title: Absence of Anti-CSRF Tokens	
Description:	
No Anti-CSRF tokens were found in a HTML submission form.	
Affected Resources	Severity
http://lms.aristopharma.co.in/	<b>MEDIUM</b>
Impact	
A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim.	
Recommendation	
Use anti-CSRF packages such as the OWASP CSRFGuard.	
Tool Used	References
ZAP PROXY	<a href="https://cwe.mitre.org/data/definitions/352.html">https://cwe.mitre.org/data/definitions/352.html</a>
POC	

```

GET http://lms.aristopharma.co.in/aristo_pharma/login.php HTTP/1.1
host: lms.aristopharma.co.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
  
```

```

HTTP/1.1 200 OK
Date: Sun, 17 Dec 2023 12:56:39 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.3
Set-Cookie: PHPSESSID=rfdtmrisa4hpttjqnkeap42v7; path=/
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Content-Length: 5512
Connection: close
Content-Type: text/html; charset=Windows-1252

<!--[if IE]>
<link REL="stylesheet" href="styles/defaultIE.css" type="text/css">

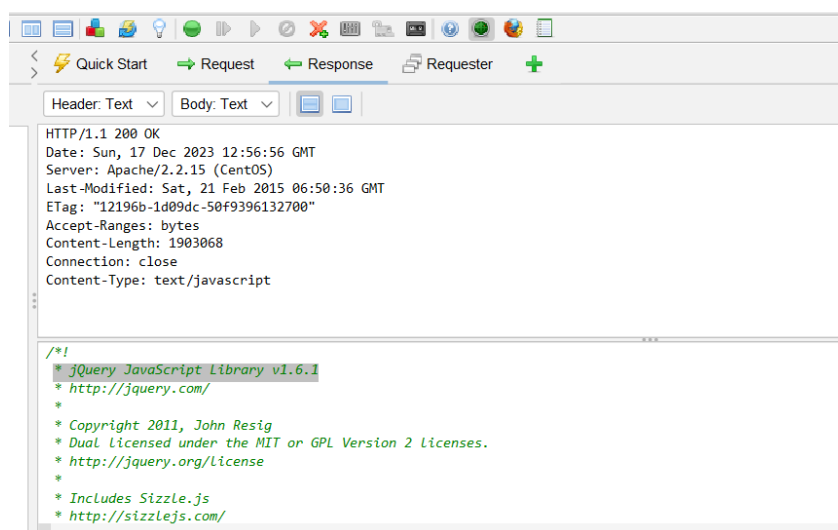
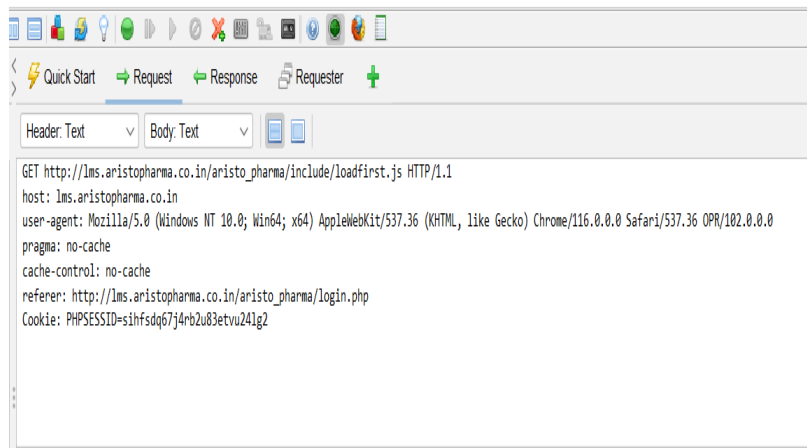
<link REL="stylesheet" href="styles/Purific10range/styleIE.css" type="text/css">

<link REL="stylesheet" href="pagestyles/LoginIE.css" type="text/css">

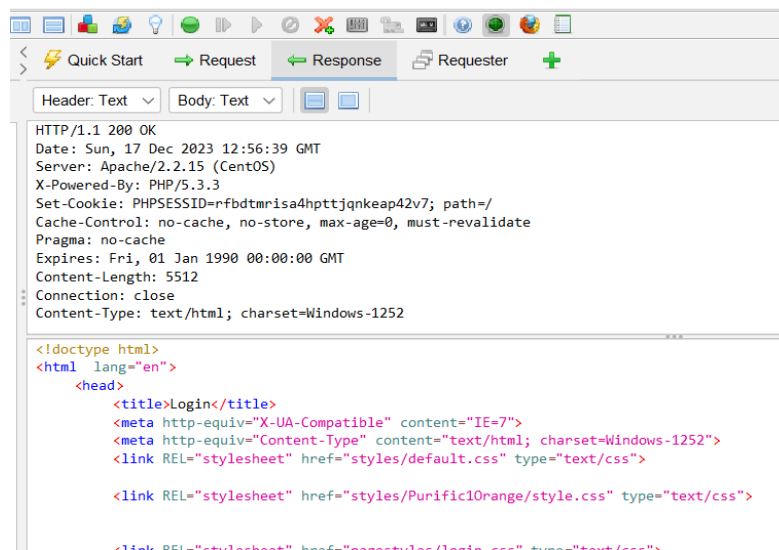
<![endif]-->
</head>

<body class="Purific10range page-login">
<script type="text/javascript" src="include/loadfirst.js"></script><script type="text/javascript" src="include/lang/English.js"></script><form method
  
```

Title: Vulnerable JS Library	
Description:	
jQuery JavaScript Library v1.6.1	
Affected Resources	Severity
http://lms.aristopharma.co.in/aristo_pharma/include/loadfirst.js	<b>MEDIUM</b>
Impact	
The identified library jquery, version 1.6.1 is vulnerable.	
Recommendation	
Use up to Date JS version	
Tool Used	References
ZAP PROXY	http://research.insecurelabs.org/jquery/test/
POC	



Title: Missing Anti-clickjacking Header	
Description:	
The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.	
Affected Resources	Severity
http://lms.aristopharma.co.in/aristo_pharma/login.php	MEDIUM
Impact	
Website page loading in an anonymous website using iFrame.	
Recommendation	
Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.	
Tool Used	References
ZAP PROXY	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
POC	



## Title: Content Security Policy (CSP) Header Not Set

### Description:

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks

### Affected Resources

http://lms.aristopharma.co.in/aristo\_pharma/login.php

### Severity

**MEDIUM**

### Impact

These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

### Recommendation

Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

### Tool Used

ZAP PROXY

### References

[https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing\\_Content\\_Security\\_Policy](https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy)

### POC

```
GET http://lms.aristopharma.co.in/aristo_pharma/login.php HTTP/1.1
host: lms.aristopharma.co.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

```
HTTP/1.1 200 OK
Date: Sun, 17 Dec 2023 12:56:39 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.3
Set-Cookie: PHPSESSID=rfdtmrisa4hpttjqnkeap42v7; path=/
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Content-Length: 5512
Connection: close
Content-Type: text/html; charset=Windows-1252

<!doctype html>
<html lang="en">
  <head>
    <title>Login</title>
    <meta http-equiv="X-UA-Compatible" content="IE=7">
    <meta http-equiv="Content-Type" content="text/html; charset=Windows-1252">
    <link REL="stylesheet" href="styles/default.css" type="text/css">
    <link REL="stylesheet" href="styles/Purific10range/style.css" type="text/css">
    <link REL="stylesheet" href="nanastyles/login.css" type="text/css">
```

