POC

Target Name → Ideas for India
Target URL → https://www.ideasforindia.in
Target IP → 68.178.156.123
Status → static

Web Technology Used

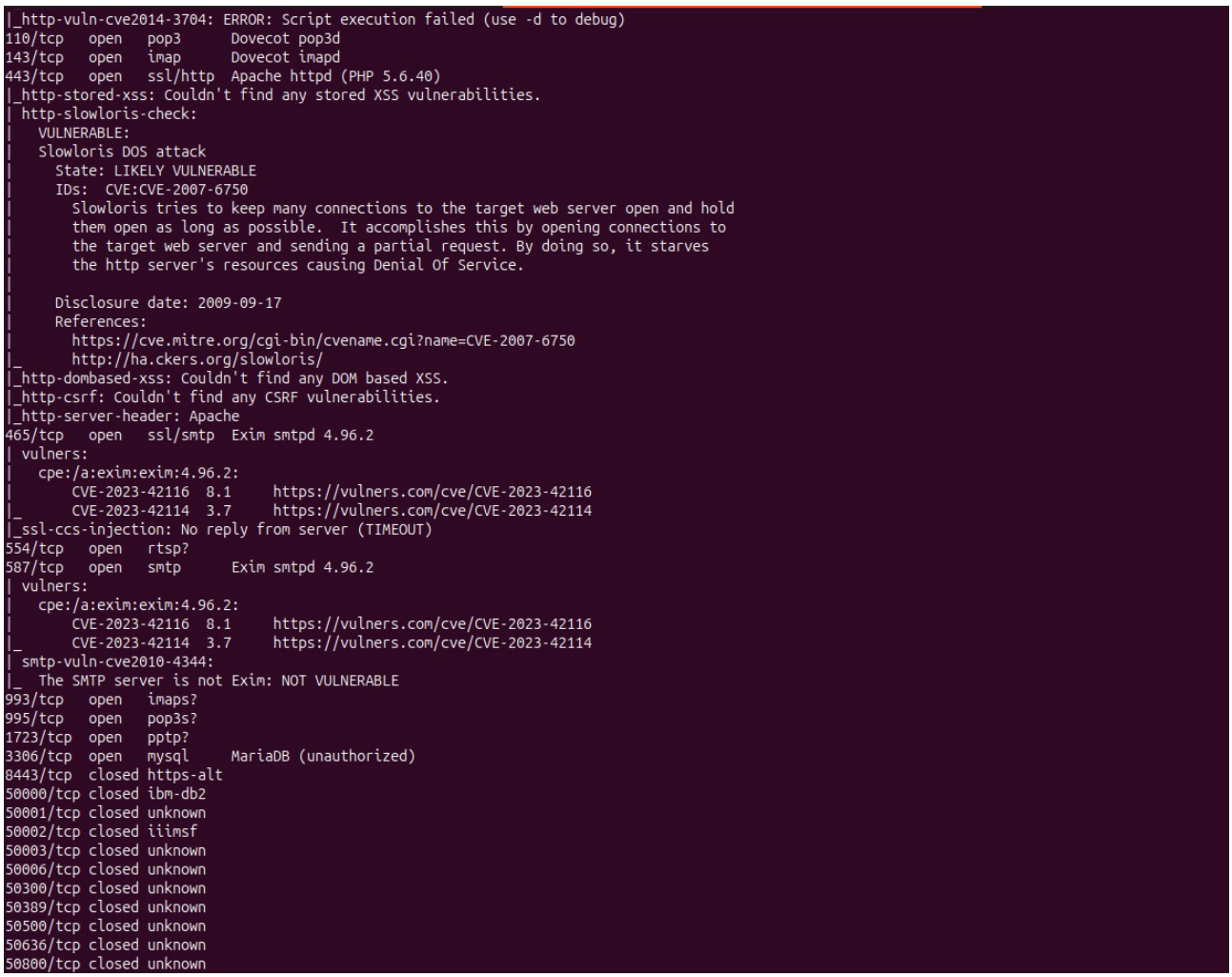
- HTML , CSS , JS ,PHP

Web Server

- Appache

Ports Discovery:

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	Pure-FTPd
22/tcp	open	ssh	OpenSSH 8.0 (protocol 2.0)
80/tcp	open	http	Apache httpd (PHP 5.6.40)
110/tcp	open	pop3	Dovecot pop3d
143/tcp	open	imap	Dovecot imapd
443/tcp	open	ssl/http	Apache httpd (PHP 5.6.40)
465/tcp	open	ssl/smtp	Exim smtpd 4.96.2
554/tcp	open	rtsp?	
587/tcp	open	smtp	Exim smtpd 4.96.2
993/tcp	open	imaps?	
995/tcp	open	pop3s?	
1723/tcp	open	pptp?	
3306/tcp	open	mysql	MariaDB (unauthorized)



Common CVE found

- FTP {Pure-FTPd}: CVE:CVE-2010-1938 || Risk factor: High
- SSH : CVE-2023-38408 || CVE-2020-15778 || CVE-2019-16905 || CVE-2021-41617 || CVE-2023-51385 || CVE-2023-48795 || CVE2020-14145 || CVE-2016-20012 || CVE-2021-36368
- HTTP {Apache httpd (PHP 5.6.40)}: CVE:CVE-2007-6750 (dos)
- HTTPS : same as above
- SMTP {smtpd 4.96.2} : CVE-2023-42116 || CVE-2023-42114 || cve2010-4344

Missing Headers

Strict-Transport-Security	HTTP Strict Transport Security is an excellent feature to support on your site and strengthens your implementation of TLS by getting the User Agent to enforce the use of HTTPS. Recommended value "Strict-Transport-Security: max-age=31536000; includeSubDomains".
Content-Security-Policy	Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
X-Frame-Options	X-Frame-Options tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking. Recommended value "X-Frame-Options: SAMEORIGIN".
Referrer-Policy	Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
Permissions-Policy	Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.

Shodan Report

Singapore

68.178.156.123

Regular View | Raw Data

© MapTiler © OpenStreetMap contributors

// TAGS: starttls

// LAST SEEN: 2024-10-07

General Information

Hostnames	ideasforindia.in www.ideasforindia.in prod.bom1.secureserver.net 123.156.178.68.host.secureserver.net
Domains	IDEASFORINDIA.IN SECURESERVER.NET
Country	Singapore
City	Singapore
Organization	GoDaddy.com, LLC
ISP	GoDaddy.com, LLC
ASN	AS26496

Web Technologies

Analytics
- Google Analytics

CDN
- cdnjs
- Cloudflare

Ecommerce
- Abicart

JavaScript Libraries
- jQuery 2.1.4
- jQuery Migrate

Tag Managers
- Google Tag Manager

Widgets
- Twitter

Vulnerabilities

All ports | Latest

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

2024

CVE-2024-4577

falseIn PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows, if the system is set up to use certain code pages, Windows may use "Best-Fit" behavior to replace characters in command line given to Win32 API functions. PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc.

2022

CVE-2022-31629

falseIn PHP versions before 7.4.31, 8.0.24 and 8.1.11, the vulnerability enables network and same-site attackers to set a standard insecure cookie in the victim's browser which is treated as a `__Host-` or `__Secure-` cookie by PHP applications.

CVE-2022-31628

falseIn PHP versions before 7.4.31, 8.0.24 and 8.1.11, the phar uncompressor code would recursively uncompress "quines" gzip files, resulting in an infinite loop.

2020

CVE-2020-11579

5.0 An issue was discovered in Chadha PHPKB 9.0 Enterprise Edition. installer/test-connection.php (part of the installation process) allows a remote unauthenticated attacker to disclose local files on hosts running PHP before 7.2.16, or on hosts where the MySQL ALLOW LOCAL DATA INFILE option is enabled.

2019

CVE-2019-9641

7.5 An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_TIFF.

CVE-2019-9639

5.0 An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_MAKERNOTE because of mishandling the data_len variable.

CVE-2019-9638

5.0 An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_MAKERNOTE because of mishandling the maker_note->offset relationship to value_len.

CVE-2019-9637

5.0 An issue was discovered in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. Due to the way rename() across filesystems is implemented, it is possible that file being renamed is briefly available with wrong permissions while the rename is ongoing, thus enabling unauthorized users to access the data.

2018

CVE-2018-19396

5.0 ext/standard/var_unserializer.c in PHP 5.x through 7.1.24 allows attackers to cause a denial of service (application crash) via an unserialize call for the com, dotnet, or variant class.

CVE-2018-19395

5.0 ext/standard/var.c in PHP 5.x through 7.1.24 on Windows allows attackers to cause a denial of service (NULL pointer dereference and application crash) because com and com_safearray_proxy return NULL in com_properties_get in ext/com_dotnet/com_handlers.c, as demonstrated by a serialize call on COM("WScript.Shell").

2017

CVE-2017-8923

7.5 The zend_string_extend function in Zend/zend_string.h in PHP through 7.1.5 does not prevent changes to string objects that result in a negative length, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact by leveraging a script's use of .= with a long string.

CVE-2017-7963

5.0 The GNU Multiple Precision Arithmetic Library (GMP) interfaces for PHP through 7.1.4 allow attackers to cause a denial of service (memory consumption and application crash) via operations on long strings. NOTE: the vendor disputes this, stating "There is no security issue here, because GMP safely aborts in case of an OOM condition. The only attack vector here is denial of service. However, if you allow attacker-controlled, unbounded allocations you have a DoS vector regardless of GMP's OOM behavior.

CVE-2017-7272

5.8 PHP through 7.1.11 enables potential SSRF in applications that accept an fsockopen or pfsockopen hostname argument with an expectation that the port number is constrained. Because a :port syntax is recognized, fsockopen will use the port number that is specified in the hostname argument, instead of the port number in the second argument of the function.

2015

CVE-2015-9253

6.8 An issue was discovered in PHP 7.3.x before 7.3.0alpha3, 7.2.x before 7.2.8, and before 7.1.20. The php-fpm master process restarts a child process in an endless loop when using program execution functions (e.g., passthru, exec, shell_exec, or system) with a non-blocking STDIN stream, causing this master process to consume 100% of the CPU, and consume disk space with a large volume of error logs, as demonstrated by an attack by a customer of a shared-hosting facility.

2013

CVE-2013-2220

7.5 Buffer overflow in the radius_get_vendor_attr function in the Radius extension before 1.2.7 for PHP allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a large Vendor Specific Attributes (VSA) length value.

2007

CVE-2007-3205

5.0 The parse_str function in (1) PHP, (2) Hardened-PHP, and (3) Suhosin, when called without a second parameter, might allow remote attackers to overwrite arbitrary variables by specifying variable names and values in the string to be parsed. NOTE: it is not clear whether this is a design limitation of the function or a bug in PHP, although it is likely to be regarded as a bug in Hardened-PHP and Suhosin.

Open Ports

21 | 443 | 587 | 993 | 995 | 2083 | 2086

// 21 / TCP -1487623700 | 2024-09-15T05:13:45.579143

Pure-FTPd


```
220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 1 of 50 allowed.
220-Local time is now 22:13. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
530 Login authentication failed
214-The following SITE commands are recognized
 ALIAS
 CHMOD
 IDLE
 UTIME
214 Pure-FTPd - http://pureftpd.org/
211-Extensions supported:
 UTF8
 EPRT
 IDLE
 MDTM
 SIZE
 MFMT
 REST STREAM
 MLST type*;size*;sizd*;modify*;UNIX.mode*;UNIX.uid*;UNIX.gid*;unique*;
 MLSD
 PRET
 AUTH TLS
 PBSZ
 PROT
 TVFS
 ESTA
 PASV
 EPSV
 ESTP
211 End.
```


SSL Certificate


```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 8314214583358865166 (0x7362061ceb7a3f0e)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=Arizona, L=Scottsdale, O=Starfield Technologies, Inc., OU=http:\/\/certs.starfieldtech.com\/repository\/, CN=Starfield Secure Certificate Authority - G2
        Validity
            Not Before: Feb 16 18:19:23 2024 GMT
            Not After : Mar 19 18:19:23 2025 GMT
        Subject: CN=*.prod.bom1.secureserver.net
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    ...
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://crl.starfieldtech.com/sfig2s1-677.crl
            X509v3 Certificate Policies:
                Policy: 2.16.840.1.114414.1.7.23.1
                  CPS: http://certificates.starfieldtech.com/repository/
                Policy: 2.23.140.1.2.1
            Authority Information Access:
                OCSP - URI:http://ocsp.starfieldtech.com/
                CA Issuers - URI:http://certificates.starfieldtech.com/repository/sfig2.crt
            X509v3 Authority Key Identifier:
                25:45:81:68:50:26:38:3D:3B:2D:2C:BE:CD:6A:D9:B6:3D:B3:66:63
            X509v3 Subject Alternative Name:
                DNS:*.prod.bom1.secureserver.net, DNS:prod.bom1.secureserver.net
            X509v3 Subject Key Identifier:
                30:E4:C8:96:D1:87:69:29:47:D9:70:F2:86:08:47:1D:B8:23:DE:98
            CT Precertificate SCTs:
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log ID    : 4E:75:A3:27:5C:9A:10:C3:38:5B:6C:D4:DF:3F:52:EB:
                                1D:F0:E0:8E:1B:8D:69:C0:B1:FA:64:B1:62:9A:39:DF
                    Timestamp : Feb 16 18:19:24.536 2024 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256
                                ...
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log ID    : 7D:59:1E:12:E1:78:2A:7B:1C:61:67:7C:5E:FD:F8:D0:
                                87:5C:14:A0:4E:95:9E:B9:03:2F:D9:0E:8C:2E:79:B8
                    Timestamp : Feb 16 18:19:24.783 2024 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256
                                ...
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log ID    : CC:FB:0F:6A:85:71:09:65:FE:95:9B:53:CE:E9:B2:7C:
                                22:E9:85:5C:0D:97:8D:B6:A9:7E:54:C0:FE:4C:0D:B0
                    Timestamp : Feb 16 18:19:24.933 2024 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256
                                ...
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        ...
```


// 443 / TCP -582657689 | 2024-09-24T18:29:05.174711

Apache httpd

Ideas for India - for more evidence based policy


```
HTTP/1.1 200 OK
Date: Tue, 24 Sep 2024 18:29:03 GMT
Server: Apache
X-Powered-By: PHP/5.6.40
Expires: Wed, 17 Aug 2005 00:00:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: 884362f5c3eafb1b91aeb0c9f7beb71=htjqq05ks54v0k82cpca1ed1j1; path=/; HttpOnly
X-Content-Type-Options: nosniff
Upgrade: h2,h2c
Connection: Upgrade
Last-Modified: Tue, 24 Sep 2024 18:29:03 GMT
Vary: Accept-Encoding
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8
```


SSL Certificate


```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            03:08:b5:d4:4c:c8:95:6c:9c:b5:c3:60:9a:04:b2:d1:0a:78
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Let's Encrypt, CN=R10
        Validity
            Not Before: Aug  2 01:56:51 2024 GMT
            Not After : Oct 31 01:56:50 2024 GMT
        Subject: CN=www.ideasforindia.in
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    ...
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Subject Key Identifier:
                E1:F1:8D:5E:5A:59:A5:09:48:7B:19:13:2C:6B:D8:67:38:E9:EA:4C
            X509v3 Authority Key Identifier:
                BB:BC:C3:47:A5:E4:BC:A9:C6:C3:A4:72:0C:10:8D:A2:35:E1:C8:E8
            Authority Information Access:
                OCSP - URI:http://r10.o.lencr.org
                CA Issuers - URI:http://r10.i.lencr.org/
            X509v3 Subject Alternative Name:
                DNS:ideasforindia.in, DNS:www.ideasforindia.in
            X509v3 Certificate Policies:
                Policy: 2.23.140.1.2.1
            CT Precertificate SCTs:
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log ID    : DF:E1:56:EB:AA:05:AF:B5:9C:0F:86:71:8D:A8:C0:32:
                                4E:AE:56:D9:6E:A7:F5:A5:6A:01:D1:C1:3B:BE:52:5C
                    Timestamp : Aug  2 02:55:21.080 2024 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256
                                ...
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log ID    : 48:B0:E3:6B:DA:A6:47:34:0F:E5:6A:02:FA:9D:30:EB:
                                1C:52:01:CB:56:DD:2C:81:D9:BB:BF:AB:39:D8:84:73
                    Timestamp : Aug  2 02:55:21.589 2024 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256
                                ...
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        ...
```


CVE-2019-9641 | CVE-2017-8923 | CVE-2013-2220 | CVE-2020-11579 | CVE-2019-9639 | 11 more

// 587 / TCP 763351817 | 2024-10-02T04:19:05.309949

Exim smtpd 4.96.2


```
220-bom1plmcpnl503320.prod.bom1.secureserver.net ESMTP Exim 4.96.2 #2 Tue, 01 Oct 2024 21:18:08 -0700
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
250-bom1plmcpnl503320.prod.bom1.secureserver.net Hello rlrkmf7uln5.org [224.237.27.242]
250-SIZE 52428800
250-8BITMIME
250-PIPELINING
```