

Vulnerability Assessment and Penetration Testing For

[Yourxxxx.co.in](#)

Disclosure Statement

This document contains sensitive information about the computer security environment, practices, current vulnerabilities and weaknesses for the client security infrastructure, and proprietary tools and methodologies from our team.

Report Details

Title	Vulnerability Assessments Report for yourxxx.co.in	
Author	<ul style="list-style-type: none">• A.K.M. Mohiuddin• Md. Rezaul Karim Razu	<ul style="list-style-type: none">• Review & Correction• Test & Report
Project Duration	01/04/2023 – 01/06/2023	



Vulnerability Assessment and Penetration Testing

What is VA & PT?

VA: A vulnerability assessment is a systematic review of security weaknesses in an information system. It evaluates if the system is susceptible to any known

vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed.

Examples of threats that can be prevented by vulnerability assessment include:

1. [SQL injection](#), [XSS](#) and other code injection attacks.
2. Escalation of privileges due to faulty authentication mechanisms.
3. Insecure defaults – software that ships with insecure settings, such as a guessable admin password.

There are several types of vulnerability assessments. These include:

1. **Host assessment** – The assessment of critical servers, which may be vulnerable to attacks if not adequately tested or not generated from a tested machine image.
2. **Network and wireless assessment** – The assessment of policies and practices to prevent unauthorized access to private or public networks and network-accessible resources.
3. **Database assessment** – The assessment of databases or big data systems for vulnerabilities and misconfigurations, identifying rogue databases or insecure dev/test environments, and classifying sensitive data across an organization's infrastructure.
4. **Application scans** – The identifying of security vulnerabilities in web applications and their source code by automated scans on the front-end or static/dynamic analysis of source code.



1. Acunetix

Acunetix is a web vulnerability scanner that features advanced crawling technology to find vulnerabilities to search every type of web page—even those that are password protected.

2. Burp Suite

Burp Suite is a web vulnerability scanner that is frequently updated, and integrates with bug tracking systems like Jira for simple ticket generation.

3. Nmap

Nmap is an open source, free security scanner that is also used by organizations for network discovery, inventory, managing service upgrade schedules, and monitoring host or service uptime.

Target Sub-Domain List
<ol style="list-style-type: none">1. www.yourxxxx.co.in2. yourxxxx.co.in3. airfxxx.net4. krishnatraxxxx.com5. b2b.xxxxxxxx.com6. oaaviaxxxx.com7. www.oaavxxxx.com8. aviation.ktsclxxxxx.com9. api.xxxxxworld.com10. xxxxxworld.com11. www.xxxxworld.com12. crm.xxxxworld.com

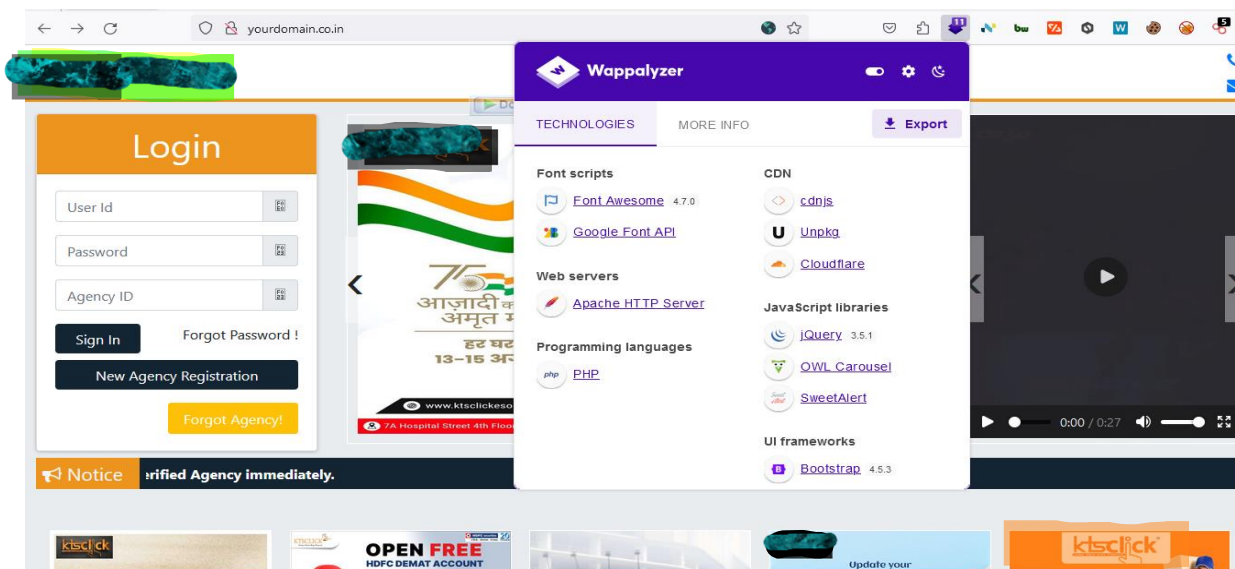
Test 1: Discover Web Application Default Content

Test 1.1: Identify Functionality

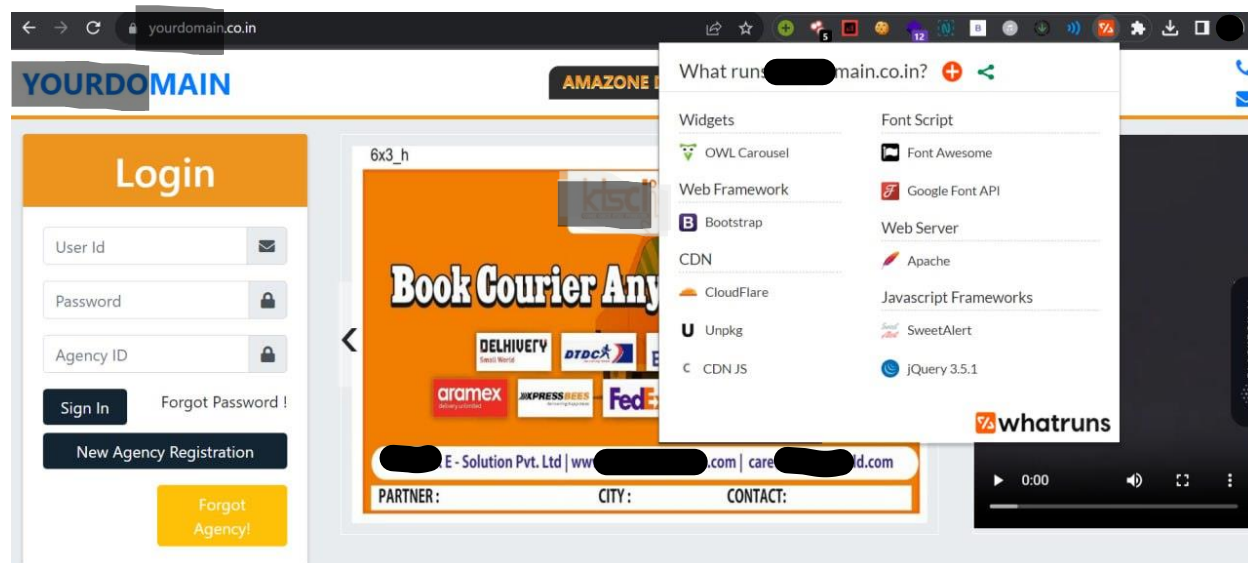
Target Organization	xxxxx E Solution Pvt Ltd,
URL	www.yourxxxxx.co.in
Target Application	yourxxxxx.co.in
List of Functions it is Designed to Perform	<ol style="list-style-type: none">1. PostgreSQL DB (14.1-14.5)2. Php 7.4.233. jQuery 3.5.14. Bootstrap 4.5.3
Key Security Mechanisms in an Application	<ol style="list-style-type: none">1. TLSV1.12. Cdnjs.cloudflare.com
Tools/Services Used	<ol style="list-style-type: none">1. wappalyzer2. whatruns

Results Analysis:

Below Some Information leakage Found.



Whatruns view:




Test 1.2: Perform Basic Website Footprinting using Netcraft

Target Organization	ktclicksolution
URL	www.ktclicksolution.com
IP addresses	<ol style="list-style-type: none"> 103.174.51.5 103.0.0.0-103.255.255.255 103.174.50.0-103.174.51.255 103.174.51.5

DNS Information	1. ns1.[REDACTED]infotechltd.com 2. srv1.[REDACTED]server.com 3. whois.namecheap.com
Server-side Technology	1. Apache 2.2 2. PostgreSQL DB 14.1- 14.5
Client-side Technology	1. HTML 2. CSS 3. JavaScript
Background Information	Site Title: [REDACTED] luation Site Rank: 0/10 Primary Language: HTML, CSS, JS, WordPress 4.7.5 Date first seen: September 2016
Tools/Services Used	1. Netcraft

Results Analysis:


[LEARN MORE](#)
[REPORT FRAUD](#)

Network

Site	http://www.ktscliquesolution.com	Domain	[REDACTED].com
Netblock Owner	Flarezen Ltd.	Nameserver	ns1.[REDACTED]rd.com
Hosting company	bdixdns.com	Domain registrar	[REDACTED]ock.com
Hosting country	BD	Nameserver organisation	whois.namecheap.com
IPv4 address	103.174.51.5 (VirusTotal)	Organisation	15 Crooked Lane , 3rd Floor , Kolkata, kolkata, 700069, India
IPv4 autonomous systems	AS138358	DNS admin	[REDACTED]ch@gmail.com
IPv6 address	Not Present	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	Not Present	DNS Security Extensions	unknown
Reverse DNS	srv1.balanceserver.com		

IP delegation

IPv4 address (103.174.51.5)

IP range	Country	Name	Description
::ffff:0:0:0:0/96	United States	IANA-IPv4-MAPPED-ADDRESS	Internet Assigned Numbers Authority

Test 1.3: Perform Web Enumeration Using Whatweb

Target Organization	a2familybazarbd.com
URL	a2familybazarbd.com
Targeted Server	1. ns1.g21bd.com
Identified Information using Whatweb	Platform: WP CMS Platform: WordPress 5.2.8 IP address, Country: 103.174.51.5 Plugins & their libraries used: WPBakery, ContackForm 7 Cookies: gridcookie=grid
Tools/Services used	1. whatweb

Results Analysis:

SELECT ANALYSIS TOOL

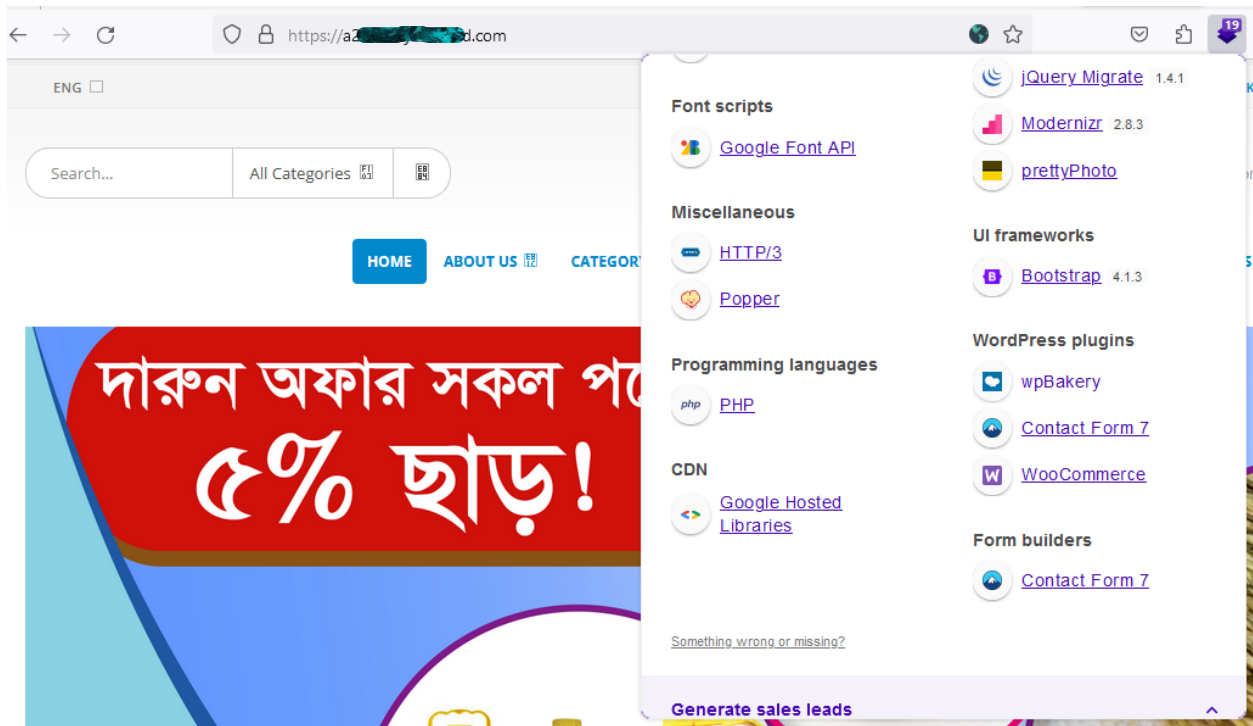
Passive Web Site Analysis (WhatWeb) ▼

Start Scan

http://[redacted]com [301 Moved Permanently] IP[103.174.51.5], RedirectLocation[https://[redacted]com/], UncommonHeaders[x-redirect-by], x-pingback[http://a2familybazarbd.com/xmlrpc.php]

https://[redacted]com/ [200 OK] Email[a2familybazar@gmail.com,ajax-loader@2x.gif], HTML5, IP[103.174.51.5], MetaGenerator[Powered by LayerSlider 5.6.9 - Multi-Purpose, Responsive, Parallax, Mobile-Friendly Slider Plugin for WordPress.,Powered by WPBakery Page Builder - drag and drop page builder for WordPress.], PoweredBy[LayerSlider,WPBakery], Script[text/javascript,text/template], maybe Sophos-Email-Appliance, Title[Family Bazar Online - [redacted] Bazar Online], UncommonHeaders[link,alt-svc], WordPress, X-UA-Compatible[IE=edge], x-pingback[https://[redacted]com/xmlrpc.php]

```
(venom@kali)-[~]
$ whatweb -a 3 103.174.51.5
http://103.174.51.5 [200 OK] Bootstrap[3.3.6,3.3.7], Cookies[cl-bypass-cache], HTML5,
HTTPServer[imunify360-webshield/1.21], HttpOnly[cl-bypass-cache], IP[103.174.51.5],
jQuery[1.12.4,3.6.3], PoweredBy[Imunify360], Script, Title[Captcha], UncommonHeaders[
cf-edge-cache]
```



Test 1.4: Analyze the HTML source Code

Target Organization	[REDACTED]
URL	http://www.[REDACTED].com
Target Website	www.[REDACTED].com
Tools/Services Used	View page sources

HTML Source Code

```

1  <!DOCTYPE html>
2  <!--[if lt IE 10 ]>
3  <html lang="en-US" prefix="og: http://ogp.me/ns#" class="old-ie no-js">
4  <![endif]-->
5  <!--[if !(IE 6) | !(IE 7) | !(IE 8) ]><!-->
6  <html lang="en-US" prefix="og: http://ogp.me/ns#" class="no-js">
7  <!--<![endif]-->
8  <head>
9  <meta charset="UTF-8" />
10 <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">
11 <link rel="profile" href="http://ogp.org/xfn/11" />
12 <link rel="pingback" href="http://www.kt[REDACTED].com/xmlrpc.php" />
13 <title>Home - [REDACTED]</title>
14
15
16 <!-- Facebook Pixel Code -->
17 <script>
18 !function(f,b,e,v,n,t,s){if(f.fbq)return;n=f.fbq=function(){n.callMethod?
19 n.callMethod.apply(n,arguments):n.queue.push(arguments)};if(!f._fbq)n=
20 n.push=n; n.loaded=!0;n.version='2.0'; n.queue=[];t=b.createElement(e);t.async=!0;
21 t.src=v;s=b.getElementsByTagName(e)[0];s.parentNode.insertBefore(t,s)}(window,
22 document,'script','https://connect.facebook.net/en_US/fbevents.js');
23 fbq('init', '192859374636672' );
24 fbq('track', 'PageView');
25
26 </script>
27 <noscript></noscript>
30 <!-- DO NOT MODIFY -->
31 <!-- End Facebook Pixel Code -->
32
33 <!-- This site is optimized with the Yoast SEO plugin v9.5 - https://yoast.com/wordpress/plugins/seo/ -->
34 <link rel="canonical" href="http://www.kt[REDACTED].com/" />
35 <meta property="og:locale" content="en_US" />
36 <meta property="og:type" content="website" />
37 <meta property="og:title" content="Home - [REDACTED]" />
38 <meta property="og:url" content="http://www.kt[REDACTED].com/" />
39 <meta property="og:site_name" content="kt[REDACTED]ion" />
40 <meta name="twitter:card" content="summary_large_image" />
41 <meta name="twitter:title" content="Home - kt[REDACTED]ion" />
42 <script type="application/ld+json">{"@context":"https://schema.org","@type":"WebSite","id":"ht[REDACTED]","url":"http://www.kt[REDACTED].com/","name":"k[REDACTED]"}</script>
43 <script type="application/ld+json">{"@context":"https://schema.org","@type":"Organization","url":"http://www.kt[REDACTED].com/","sameAs":["http://www.kt[REDACTED].com/","http://www.kt[REDACTED].com/","http://www.kt[REDACTED].com/"],"id":"http://www.kt[REDACTED].com/"}</script>

```

Test 1.5: Check the HTTP and HTML processing by the browser

Target Organization	[REDACTED]
URL	http://www.kt[REDACTED].com/

Results Analysis:

Analyzed HTTP and HTTPS Request Headers

ew Help Burp Suite Professional v2023.8 - Temporary Project - Licensed to Z

er Repeater Collaborator Sequencer Decoder Comparer Logger Orga

initions | Scope settings

image and general binary content; hiding 4xx responses; hiding empty folders

Contents

Host	Method	URL	Params	Status co...	Length	MIME type
http://www.██████████...	GET	/wp-content/plugin...	✓	200	28724	script
http://www.██████████...	GET	?s={search_term_str...	✓			
http://www.██████████...	GET	/about-us/				
http://www.██████████...	GET	/amazon-easy-store/				
http://www.██████████...	GET	/bulk-sms/				
http://www.██████████...	GET	/careers/				
http://www.██████████...	GET	/click-tatkal-money/				
http://www.██████████...	GET	/comments/feed/				
http://www.██████████...	GET	/contact-us/				

Request

Pretty Raw Hex

```
1 GET
2 /wp-content/plugins/revslider/public/assets/js/extensions/revoluti
on.extension.slideanim.min.js?version=5.3.1.4 HTTP/1.1
3 Host: www.██████████.com
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/117.0
5 Accept: text/javascript, application/javascript,
application/ecmascript, application/x-ecmascript, */*; q=0.01
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 X-Requested-With: XMLHttpRequest
9 Connection: close
10 Referer: http://www.██████████.com/
11 Cookie: devicePixelRatio=1; _fbp=fb.1.1693296846462.1268089039;
time=9/3/2023, 3:44:56 PM; twkr_idm_key=CcobwFrQi9Yf15rtJuMfz
12
```

Inspector

0 highlights

Test 1.6: Identify the Technology used to Build Target Website

Target Organization	[REDACTED]ution
URL	http://www.[REDACTED]solution.com/
Identified the Technology used to Build Target Website	Added below
Tools/Services Used	Built with extension

Results Analysis:

The screenshot shows the BuiltWith website interface for the target URL <https://ktscliquesolution.com/>. The page is titled "ktscliquesolution.COM" and features a navigation bar with tabs: Technology Profile, Detailed Technology Profile, Meta Profile, Performance Profile, and Relationship. The main content area is divided into sections: Contact Information, Publicly Listed Contacts, and Website Information.

Contact Information:

- Company Name:** [REDACTED]ution. A link "Find People on LinkedIn" is provided.
- Address:** Esplanade, 700062 WB, India.
- Telephone:** (Field is empty).

Publicly Listed Contacts:

Name	Level
Anil Sharma	C-Suite

Website Information: (Field is empty).

A watermark "Burp Suite Professional v2.1.1 licensed to [REDACTED] Davl ab Ci" is visible in the bottom right corner of the screenshot.

IP Address History & Relationships

KTSCCLICKESOLUTION.COM IP History and other websites that have shared IP addresses with KTSCCLICKESOLUTION.COM. Click the IP addresses to see more information.

KTSCCLICKESOLUTION.COM	207.172.214.206	174.138.164.250	103.174.51.5
antofagasta.bedbron.com		174.138.164.250	
alexandria.bedbron.com		174.138.164.250	
akroncantan.bedbron.com		174.138.164.250	
albuquerque.bedbron.com		174.138.164.250	
altoona.bedbron.com		174.138.164.250	
abidjan.bedbron.com		174.138.164.250	
alicante.bedbron.com		174.138.164.250	
aurangabad.bedbron.com		174.138.164.250	
augusta.bedbron.com		174.138.164.250	
ahmedabad.bedbron.com		174.138.164.250	
albany.bedbron.com		174.138.164.250	
anaheim.bedbron.com		174.138.164.250	

Widgets

 CrUX Dataset	Dec 2022	Aug 2023	
 CrUX Top 50m	Dec 2022	Aug 2023	
 Yoast SEO Premium WordPress Plugins	Feb 2019	Aug 2023	\$
 Fontello Fonts	May 2023	Aug 2023	\$
 Ultimate Social Media WordPress Plugins	Feb 2019	Aug 2023	\$
 ConvertPlug WordPress Plugins	Feb 2019	Aug 2023	\$
 Wordpress Plugins	Nov 2016	Aug 2023	
 Google Font API Fonts	Nov 2016	Aug 2023	
 Contact Form 7 Feedback Forms and Surveys	Nov 2016	Aug 2023	
 Slider Revolution WordPress Plugins	Aug 2017	Aug 2023	
 LayerSlider Responsive WordPress Plugins	Aug 2017	Aug 2023	
 Recent Tweets Widget for WordPress WordPress Plugins	Aug 2017	Aug 2023	
 Font Awesome Fonts	Aug 2017	Aug 2023	
 Visual Composer Ultimate Addons WordPress Plugins	Aug 2017	Aug 2023	
 Google Plus One Platform	Aug 2017	Aug 2023	

Test 2: Discover Web Application Hidden Content, Manually browse the target

Test 2.1: Identify the Sitemap of Target Website

Target Organization	Y●●●●●●●●.co.in
URL	You●●●●●●●●.co.in
Information collected	1. Found hidden link.
Tools/Services Used	1. What web.net

1) internal link found.

Linked Pages

Summary

Internal Link Count	10
External Link Count	4

▼ Internal Links

- /
- /
- /
- /account/registration
- /
- /faqs
- /privacy_policy
- /terms_condition
- /contact_us
- /about_us

Crawl Rules

User-agent *

Block Lists

AdGuard	✓	Not Blocked
AdGuard Family	✓	Not Blocked
CleanBrowsing Adult	✓	Not Blocked
CleanBrowsing Family	✓	Not Blocked
CleanBrowsing Security	✓	Not Blocked
CloudFlare	✓	Not Blocked
CloudFlare Family	✓	Not Blocked
Comodo Secure	✓	Not Blocked
Google DNS	✓	Not Blocked
Neustar Family	✓	Not Blocked

Test 2.2: Crawl a Website to Identify Its Files, Directories, Folders

Target Organization	██████████
URL	www.██████████.in.co.in
Target Website	██████████.co.in
Tools/Services Used	Acunetix
Found	Directory

Results:

Scan

Full Scan - https://██████████.co.in/

Stop Scan

Pause Scan

Full Scan - https://██████████.co.in/

Scan Information

Vulnerabilities

Site Structure

Events

https://██████████.co.in/

https://██████████.co.in/

fragments

account

admin

assets

images

index.php

lib

newassets

system

uploads

about_us

composer.json

contact_us

faqs

index.html

index.php

https://██████████.co.in/

0 5 8 11

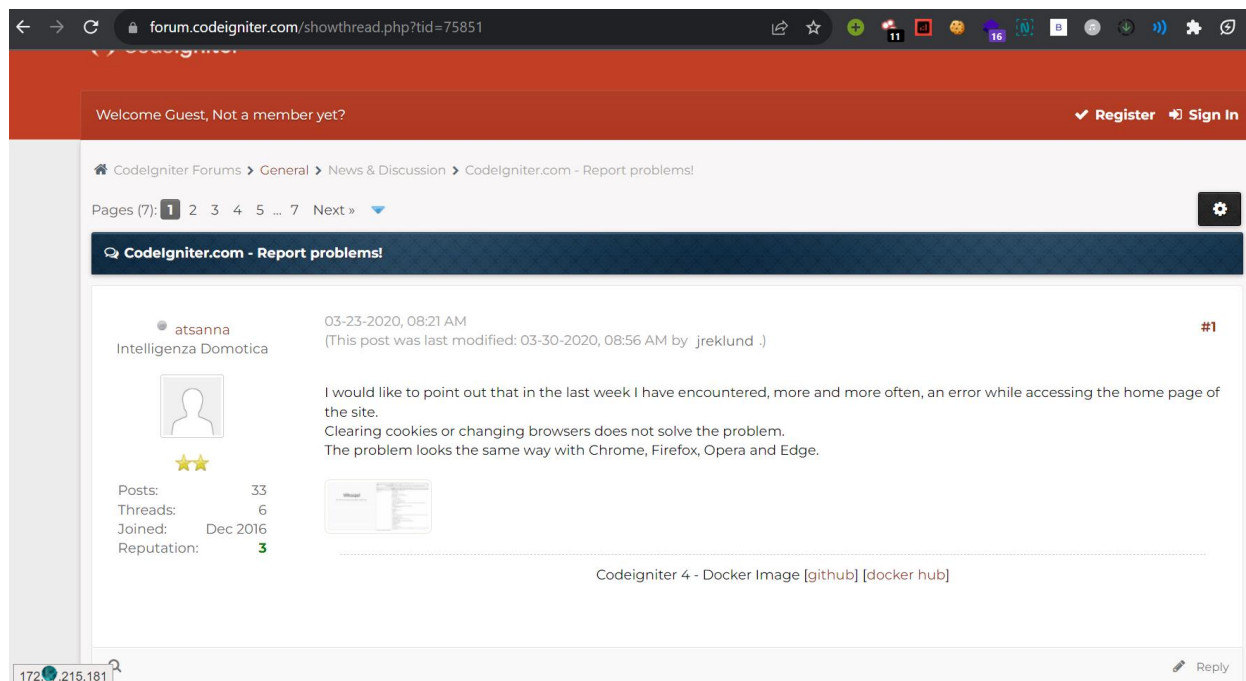
Severity	Vulnerability	Parameter	Status
	Development configuration files		Open
	PHPinfo pages		Open
	TLS/SSL Sweet32 attack		Open
	TLS/SSL Weak Cipher Suites		Open
	Vulnerable JavaScript libraries		Open
	Clickjacking: X-Frame-Options header missing		Open
	Cookies with missing		

4) When we go this link we found secret conversation.



```
{
  "description": "The CodeIgniter framework",
  "name": "codeigniter/framework",
  "type": "project",
  "homepage": "http://codeigniter.com",
  "license": "MIT",
  "support": {
    "forum": "http://forum.codeigniter.com/",
    "wiki": "https://github.com/bcit-ci/CodeIgniter/wiki",
    "irc": "irc://irc.freenode.net/codeigniter",
    "source": "https://github.com/bcit-ci/CodeIgniter"
  },
  "require": {
    "php": ">=5.2.4"
  },
  "require-dev": {
    "mikey179/vfsStream": "1.1.*"
  }
}
```

5) Visit this link <http://forum.codeigniter.com/> we are found a very **critical** vulnerability Private message.



Test 3: Conduct Web Vulnerability Scanning

Test 3.1: Conduct Web Vulnerability Assessment

Target Organization	https://[REDACTED].co.in	
Web Application Vulnerability Scanners used	<ol style="list-style-type: none"> 1. Acunetix 2. Rustscan 	
Successfully performed vulnerability scanning	<input type="checkbox"/> YES	<input type="checkbox"/> NO
Tools/Services Used	<ol style="list-style-type: none"> 1. Acunetix 2. Rustscan 	

Results: Here we are given the Acunetix Scanning Report.

Analysis:

The screenshot displays the Acunetix web interface. The top navigation bar includes the Acunetix logo, user role (Administrator), and notification icons. The left sidebar contains a menu with options like Dashboard, Targets, Vulnerabilities, Scans, Reports, Users, Scan Profiles, Network Scanner, Issue Trackers, Email Settings, Engines, Excluded Hours, and Proxy Settings. The main content area shows a scan report for the target https://[REDACTED].co.in/. The report includes a progress bar, a summary of scan information, and a list of latest alerts. The summary shows a scan duration of 31m 54s, 31,630 requests, an average response time of 505ms, and 87 paths identified. The latest alerts list includes vulnerable JavaScript libraries, outdated JavaScript libraries, possible sensitive directories, possible server path disclosure (Unix), and PHPinfo pages.

Scan Information	Vulnerabilities	Site Structure	Events
Full Scan - https://[REDACTED].co.in/			
Scan Duration	31m 54s	Requests	31,630
Average Response Time	505ms	Paths Identified	87
Target Information	<p>Address: https://[REDACTED].co.in/</p> <p>Server: Apache</p> <p>Operating System: Unknown</p> <p>Identified Technologies: PHP</p> <p>Responsive: Yes</p>		
Latest Alerts	<ul style="list-style-type: none"> Vulnerable JavaScript libraries (Sep 3, 2023, 11:44:37 AM) Outdated JavaScript libraries (Sep 3, 2023, 11:40:56 AM) Possible sensitive directories (Sep 3, 2023, 11:40:45 AM) Possible server path disclosure (Unix) (Sep 3, 2023, 11:39:05 AM) PHPinfo pages (Sep 3, 2023, 11:39:05 AM) 		

Report: Here we are given the Nmap Scanning Report.

```
└─# nmap -F 34.117.134
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-18 01:24 EDT
Nmap scan report for 134.93.34.bc.googleusercontent.com (34.117.134)
Host is up (0.12s latency).
Not shown: 75 filtered tcp ports (no-response), 16 filtered tcp ports (admin-prohibited)
PORT      STATE SERVICE
21/tcp    closed ftp
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
3000/tcp   closed ppp
5432/tcp   open  postgresql
8080/tcp   closed http-proxy
8081/tcp   closed blackice-icecap
8888/tcp   open  sun-answerbook

Nmap done: 1 IP address (1 host up) scanned in 9.26 seconds
```

Rust scan: Open port with service version

```

Completed NSE at 01:14, 0.75s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 01:14
Completed NSE at 01:14, 1.15s elapsed
Nmap scan report for 134.117.93.34.bc.googleusercontent.com (34.93.117.134)
Host is up, received timestamp-reply ttl 57 (0.089s latency).
Scanned at 2023-08-29 01:11:23 EDT for 164s

PORT      STATE SERVICE      REASON      VERSION
22/tcp    open  ssh          syn-ack ttl 57 OpenSSH 8.0 (protocol 2.0)
40/tcp    open  ftp          syn-ack ttl 57 Pure-FTPd
888/tcp   open  accessbuilder? syn-ack ttl 57
5432/tcp  open  postgresql   syn-ack ttl 56 PostgreSQL DB 14.1 - 14.5
8888/tcp  open  http         syn-ack ttl 56 nginx

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 164.91 seconds

Raw packets sent: 9 (372B) | Rcvd: 6 (260B)

```

Test 3.2: Perform Web Application Fuzz Testing

Target Organization	
URL	https://yourdomain.co.in/demo https://yourdomain.co.in/NewILR http://yourdomain.co.in/favicon.ico

	http://yourid@yourdomain.co.in http://yourid@yourdomain.co.in https://yourdomain.co.in/terms_condition https://yourdomain.co.in/about_us https://yourdomain.co.in/demo https://yourdomain.co.in/NewILR http://yourdomain.co.in/favicon.ico https://yourdomain.co.in/account/registration
Tools/Services Used	<ol style="list-style-type: none"> 1. Nmap 2. Wfuzz 3. ffuf

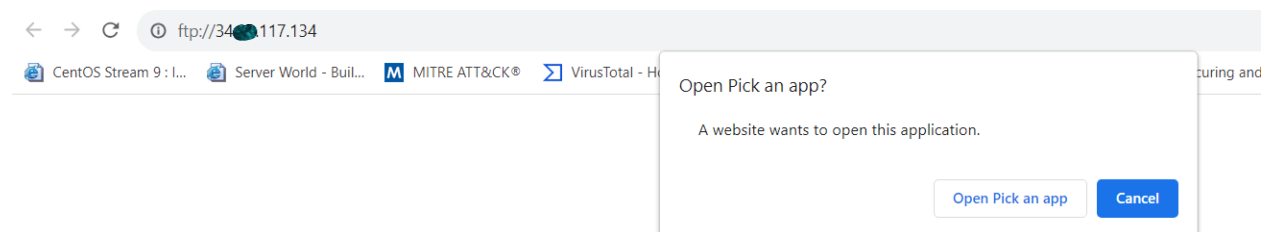
Test 4: Identify the Attack Surface Area

Test 4.1: Map the Attack Surface

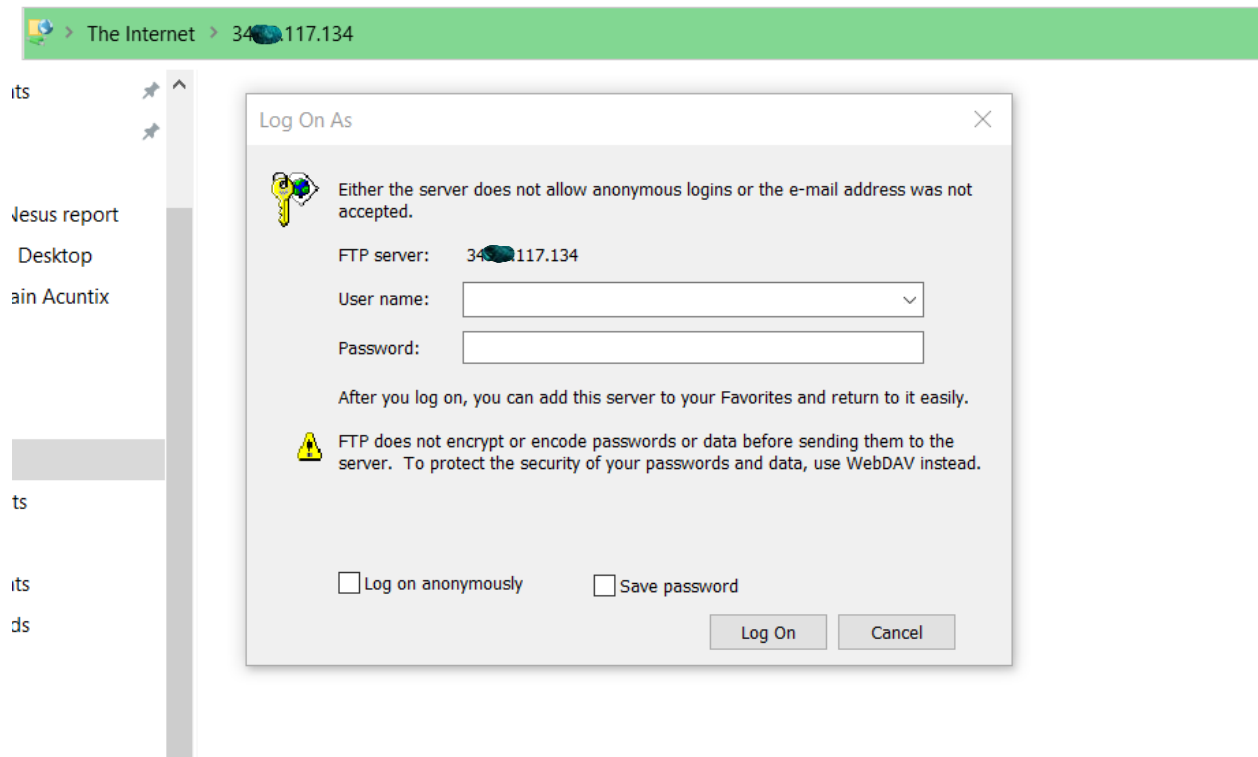
Target Organization	yourdomain
URL	yourdomain.co.in
Target Web Application	http://yourdomain.co.in/
Information Collected	Added below
Identified Attack Surface	FTP, CPanel
Tools/Services Used	Nmap, Web

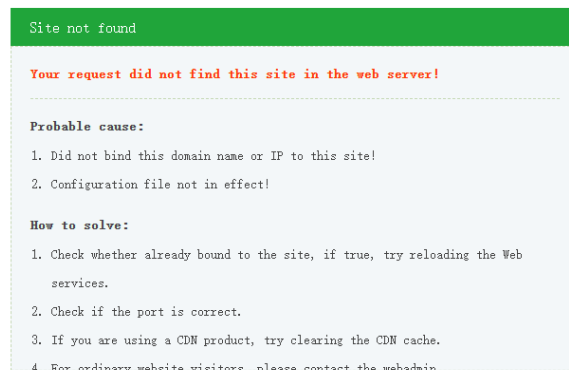
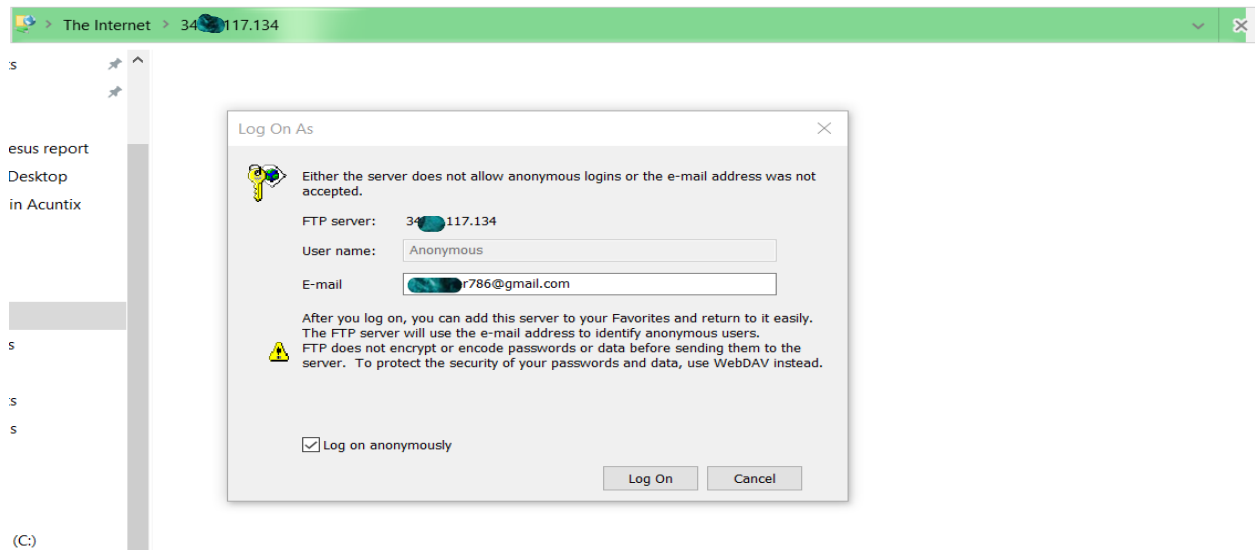
Results Analysis:

```
# wget -m --no-passive ftp://anonymous:anonymous@34.93.117.134:40
--2023-08-28 05:28:36-- ftp://anonymous:*password*@34.93.117.134:40/
=> '34.93.117.134:40/.listing'
Connecting to 34.93.117.134:40 ... connected.
Logging in as anonymous ... id
Login incorrect.
```

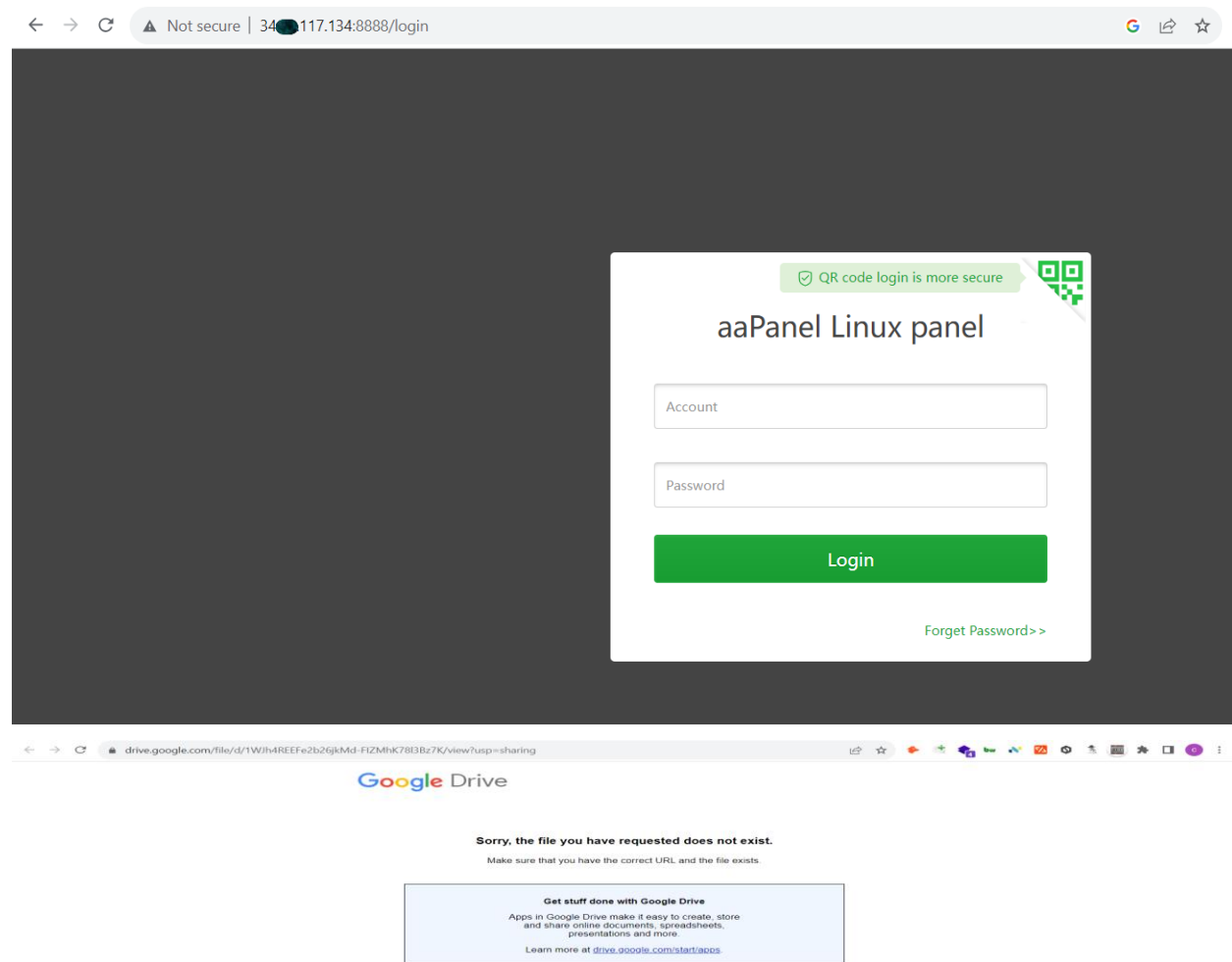


Tried to access via Ftp





Tried to access CPanel



<https://help.dreamhost.com/hc/en-us/articles/216363167-Deny-access-to-a-site-with-an-htaccess-file>

Deny access to an entire website

The following code prevents anyone from viewing your website. Visitors will instead see a **403** when viewing your website.

Apache 2.2

```
Order deny,allow
Deny from all
```

Apache 2.4

```
Require all denied
```

Deny access to files

Denying access to specific file extensions

The following code forces any file ending in .inc to throw a 403 Forbidden error when visited:

Apache 2.2

```
<Files ~ "\.inc$"
  Order Allow,Deny
  Deny from All
</Files>
```

<https://help.dreamhost.com/hc/en-us/articles/216363167-Deny-access-to-a-site-with-an-htaccess-file>

Apache 2.4

```
<FilesMatch "\.(inc)$"
  Require all denied
</FilesMatch>
```

Denying access to "hidden" files

File names beginning with a dot are considered "hidden" by UNIX. Usually, you don't want to serve them to visitors.

DreamHost already disallows retrieving **.htaccess** and **.htpasswd**, but you can recursively deny all access to all hidden files by placing the following into a top-level **.htaccess**:

```
RedirectMatch 403 /\..*$
```

Deny access to folders

Denying access to a directory listing

If you don't have an index file in your directory, all of your files are listed in a directory list for anyone to view. The following code forces this directory listing to throw a 403 Forbidden error instead when visited:

```
Options -Indexes
```

List of Inject Codes

OpenVAS report

Host	High	Medium	Low	Log	False Positive
34.117.134 ai.net	4	13	2	0	0
Total: 1	4	13	2	0	0

Vendor security updates are not trusted.

Overrides are off. Even when a result has an override, this report uses the actual threat of the result.

Information on overrides is included in the report.

Notes are included in the report.

This report might not show details of all issues that were found.

Issues with the threat level "Log" are not shown.

Issues with the threat level "Debug" are not shown.

Issues with the threat level "False Positive" are not shown.

Only results with a minimum QoD of 70 are shown.

This report contains all 19 results selected by the filtering described above. Before filtering there were 139 results.

2 Results per Host

2.1 34.117.134

Host scan start Sat Sep 2 06:39:15 2023 UTC

Host scan end Sat Sep 2 12:39:00 2023 UTC

Service (Port)	Threat Level
443/tcp	High
22/tcp	Medium
443/tcp	Medium
8888/tcp	Medium
80/tcp	Medium
general/icmp	Low
general/tcp	Low

2.1.1 High 443/tcp

High (CVSS: 7.5)

NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

Summary

...continued from previous page ...
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.
Vulnerability Detection Result 'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol: TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32) TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32) 'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32) TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
Solution: Solution type: Mitigation The configuration of this services should be changed so that it does not accept the listed cipher suites anymore. Please see the references for more resources supporting you with this task.
Affected Software/OS Services accepting vulnerable SSL/TLS cipher suites via HTTPS.
Vulnerability Insight These rules are applied for the evaluation of the vulnerable cipher suites: - 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).
Vulnerability Detection Method Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS OID:1.3.6.1.4.1.25623.1.0.108031 Version used: 2023-07-20T05:05:17Z
References cve: CVE-2016-2183 cve: CVE-2016-6329 cve: CVE-2020-12872 url: https://bettercrypto.org/ url: https://mozilla.github.io/server-side-tls/ssl-config-generator/ url: https://sweet32.info/ cert-bund: WID-SEC-2022-2226 cert-bund: WID-SEC-2022-1955 cert-bund: CB-K21/1094 cert-bund: CB-K20/1023 cert-bund: CB-K20/0321 cert-bund: CB-K20/0314

High (CVSS: 7.5)
 NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

Summary

This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

Vulnerability Detection Result

'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:

TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

Solution:

Solution type: Mitigation

The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.

Please see the references for more resources supporting you with this task.

Affected Software/OS

Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

Vulnerability Insight

These rules are applied for the evaluation of the vulnerable cipher suites:

- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

Vulnerability Detection Method

Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

OID:1.3.6.1.4.1.25623.1.0.108031

Version used: 2023-07-20T05:05:17Z

References

cve: CVE-2016-2183

cve: CVE-2016-6329

cve: CVE-2020-12872

<p>High (CVSS: 7.5)</p> <p>NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS</p>
<p>Summary</p> <p>This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.</p>
<p>Vulnerability Detection Result</p> <p>'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:</p> <p>TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)</p> <p>TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)</p> <p>'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:</p> <p>TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)</p> <p>TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)</p>
<p>Solution:</p> <p>Solution type: Mitigation</p> <p>The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.</p> <p>Please see the references for more resources supporting you with this task.</p>
<p>Affected Software/OS</p> <p>Services accepting vulnerable SSL/TLS cipher suites via HTTPS.</p>
<p>Vulnerability Insight</p> <p>These rules are applied for the evaluation of the vulnerable cipher suites:</p> <p>- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).</p>
<p>Vulnerability Detection Method</p> <p>Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS</p> <p>OID:1.3.6.1.4.1.25623.1.0.108031</p> <p>Version used: 2023-07-20T05:05:17Z</p>
<p>References</p> <p>cve: CVE-2016-2183</p> <p>cve: CVE-2016-6329</p> <p>cve: CVE-2020-12872</p> <p>url: https://bettercrypto.org/</p>

<p>High (CVSS: 7.5)</p> <p>NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS</p>
<p>Summary</p> <p>This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.</p>
<p>Vulnerability Detection Result</p> <p>'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:</p> <p>TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)</p> <p>TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)</p> <p>'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:</p> <p>TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)</p> <p>TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)</p>
<p>Solution:</p> <p>Solution type: Mitigation</p> <p>The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.</p> <p>Please see the references for more resources supporting you with this task.</p>
<p>Affected Software/OS</p> <p>Services accepting vulnerable SSL/TLS cipher suites via HTTPS.</p>
<p>Vulnerability Insight</p> <p>These rules are applied for the evaluation of the vulnerable cipher suites:</p> <p>- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).</p>
<p>Vulnerability Detection Method</p> <p>Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS</p> <p>OID:1.3.6.1.4.1.25623.1.0.108031</p> <p>Version used: 2023-07-20T05:05:17Z</p>
<p>References</p> <p>cve: CVE-2016-2183</p> <p>cve: CVE-2016-6329</p> <p>cve: CVE-2020-12872</p>

Medium (CVSS: 5.3) NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)
Summary The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).
Vulnerability Detection Result The remote SSH server supports the following weak KEX algorithm(s): KEX algorithm Reason ----- diffie-hellman-group-exchange-sha1 Using SHA-1
Impact An attacker can quickly break individual connections.
Solution: Solution type: Mitigation Disable the reported weak KEX algorithm(s) - 1024-bit MODP group / prime KEX algorithms: Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.
Vulnerability Insight - 1024-bit MODP group / prime KEX algorithms: Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime. A nation-state can break a 1024-bit prime.
Vulnerability Detection Method Checks the supported KEX algorithms of the remote SSH server. Currently weak KEX algorithms are defined as the following: - non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime - ephemerally generated key exchange groups uses SHA-1 - using RSA 1024-bit modulus key Details: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH) OID:1.3.6.1.4.1.25623.1.0.150713 Version used: 2022-12-08T10:12:32Z

<p>Medium (CVSS: 6.4) NVT: Missing 'Secure' Cookie Attribute (HTTP)</p>
<p>Summary The remote HTTP web server / application is missing to set the 'Secure' cookie attribute for one or more sent HTTP cookie.</p>
<p>Vulnerability Detection Result The cookies: Set-Cookie: PHPSESSID=***replaced***; path=/ are missing the "Secure" cookie attribute.</p>
<p>Solution: Solution type: Mitigation Set the 'Secure' cookie attribute for any cookies that are sent over a SSL/TLS connection.</p>
<p>Affected Software/OS Any web application accessible via a SSL/TLS connection (HTTPS) and at the same time also accessible over a cleartext connection (HTTP).</p>
<p>Vulnerability Insight The flaw exists if a cookie is not using the 'Secure' cookie attribute and is sent over a SSL/TLS connection. This allows a cookie to be passed to the server by the client over non-secure channels (HTTP) and subsequently allows an attacker to e.g. conduct session hijacking attacks.</p>
<p>Vulnerability Detection Method Checks all cookies sent by the remote HTTP web server / application over a SSL/TLS connection for a missing 'Secure' cookie attribute. Details: Missing 'Secure' Cookie Attribute (HTTP) OID:1.3.6.1.4.1.25623.1.0.902661 Version used: 2023-01-17T10:10:58Z</p>
<p>References url: https://www.rfc-editor.org/rfc/rfc6265#section-5.2.5 url: https://owasp.org/www-community/controls/SecureCookieAttribute url: https://wiki.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-002)</p>

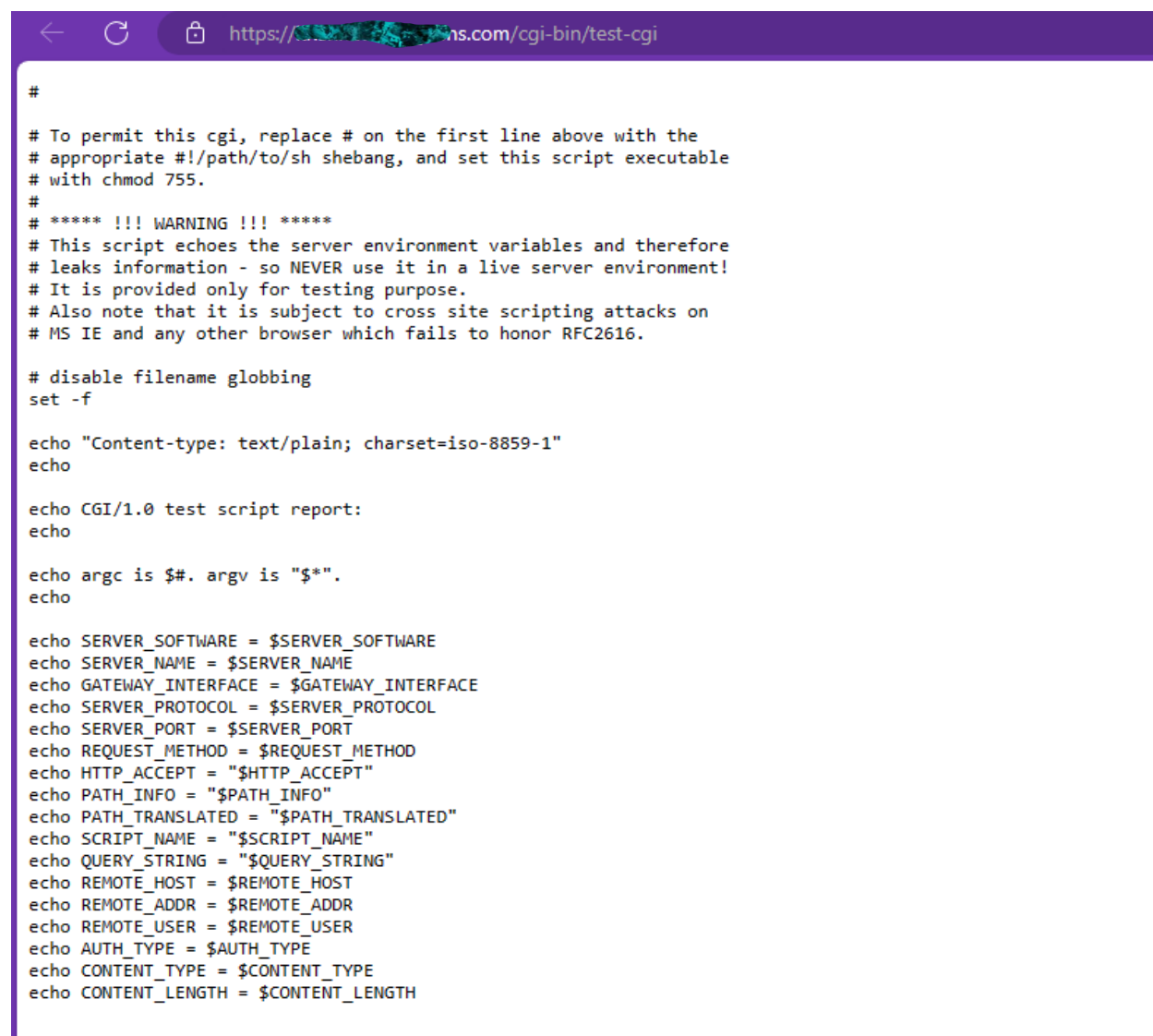
Server Misconfigurations

Any folder with images create a file Thumbs.db. Which contains image informations in it. An attacker can directly download it from the directory if it is on the hosting (www) directory by just visiting the link.

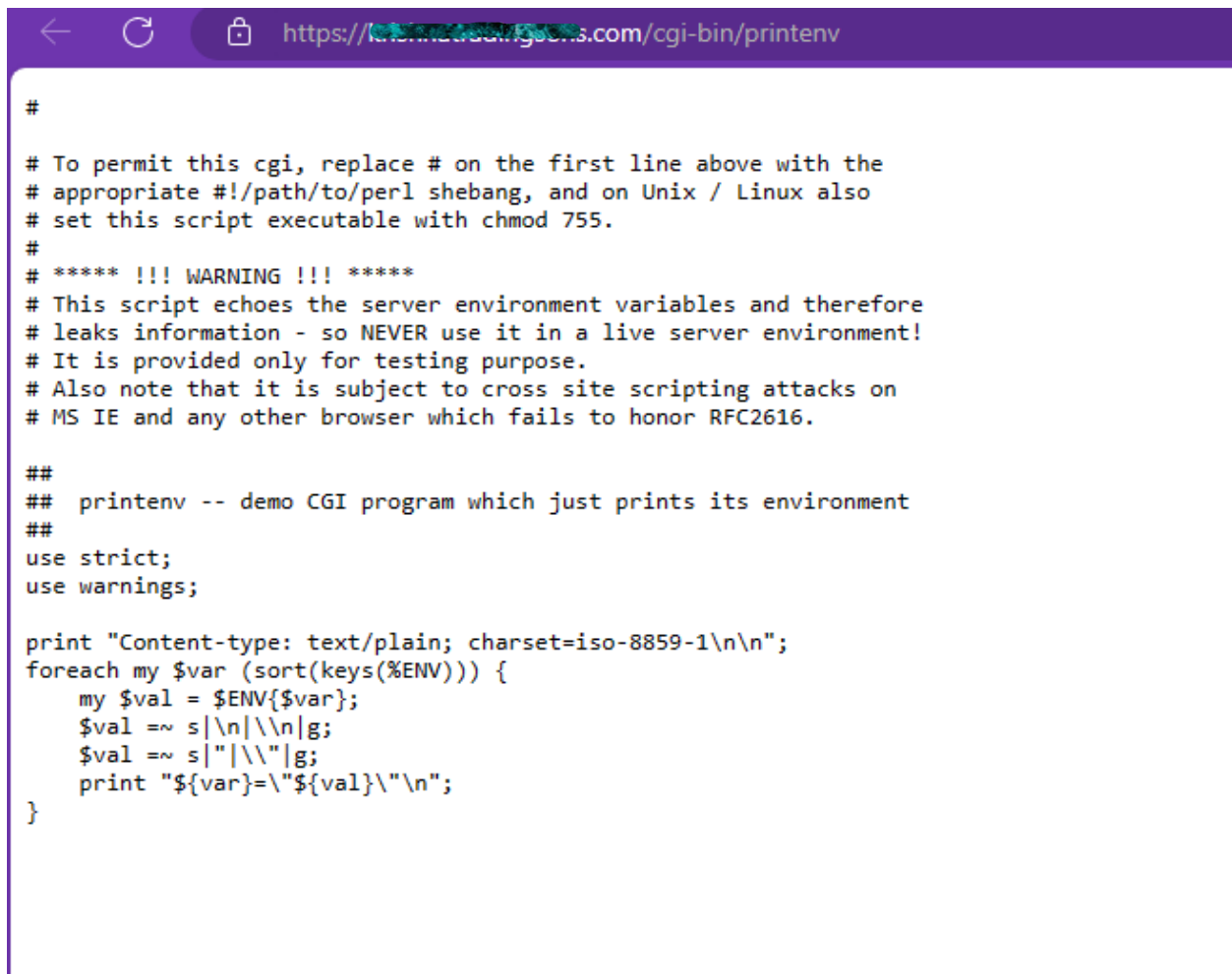
1. Step to reproduce:
2. 1. Open [https://\[redacted\].co.in/.../Thumbs.db](https://[redacted].co.in/.../Thumbs.db) It will automatically download Thumbs.db for this specific directory.
3. 2. Goto <https://thumbsdb.herokuapp.com/> and upload the file to see images on that directory.

Same URL:

- [https://\[redacted\].com/cgi-bin/printenv](https://[redacted].com/cgi-bin/printenv)
- [https://\[redacted\].com/cgi-bin/test-cgi](https://[redacted].com/cgi-bin/test-cgi)

A screenshot of a web browser window with a purple header bar. The address bar shows a URL starting with 'https://'. The main content area displays the output of a CGI script, which includes various status messages and environment variable listings.

```
#  
  
# To permit this cgi, replace # on the first line above with the  
# appropriate #!/path/to/sh shebang, and set this script executable  
# with chmod 755.  
#  
# ***** !!! WARNING !!! *****  
# This script echoes the server environment variables and therefore  
# leaks information - so NEVER use it in a live server environment!  
# It is provided only for testing purpose.  
# Also note that it is subject to cross site scripting attacks on  
# MS IE and any other browser which fails to honor RFC2616.  
  
# disable filename globbing  
set -f  
  
echo "Content-type: text/plain; charset=iso-8859-1"  
echo  
  
echo CGI/1.0 test script report:  
echo  
  
echo argc is $#. argv is "$*".  
echo  
  
echo SERVER_SOFTWARE = $SERVER_SOFTWARE  
echo SERVER_NAME = $SERVER_NAME  
echo GATEWAY_INTERFACE = $GATEWAY_INTERFACE  
echo SERVER_PROTOCOL = $SERVER_PROTOCOL  
echo SERVER_PORT = $SERVER_PORT  
echo REQUEST_METHOD = $REQUEST_METHOD  
echo HTTP_ACCEPT = "$HTTP_ACCEPT"  
echo PATH_INFO = "$PATH_INFO"  
echo PATH_TRANSLATED = "$PATH_TRANSLATED"  
echo SCRIPT_NAME = "$SCRIPT_NAME"  
echo QUERY_STRING = "$QUERY_STRING"  
echo REMOTE_HOST = $REMOTE_HOST  
echo REMOTE_ADDR = $REMOTE_ADDR  
echo REMOTE_USER = $REMOTE_USER  
echo AUTH_TYPE = $AUTH_TYPE  
echo CONTENT_TYPE = $CONTENT_TYPE  
echo CONTENT_LENGTH = $CONTENT_LENGTH
```



```
#
# To permit this cgi, replace # on the first line above with the
# appropriate #!/path/to/perl shebang, and on Unix / Linux also
# set this script executable with chmod 755.
#
# ***** !!! WARNING !!! *****
# This script echoes the server environment variables and therefore
# leaks information - so NEVER use it in a live server environment!
# It is provided only for testing purpose.
# Also note that it is subject to cross site scripting attacks on
# MS IE and any other browser which fails to honor RFC2616.

##
## printenv -- demo CGI program which just prints its environment
##
use strict;
use warnings;

print "Content-type: text/plain; charset=iso-8859-1\n\n";
foreach my $var (sort(keys(%ENV))) {
    my $val = $ENV{$var};
    $val =~ s|\n|\\n|g;
    $val =~ s|"|\\"|g;
    print "${var}=\"${val}\"\\n";
}
```

It does not have any direct risk or security impact. Although, it could leak sensitive data of other users with this exploit.

