Penetration Test Report: hackforums.net

Date: 2023-07-08

Prepared By: Robot Security

Unique HTTP/HTTPs Subdomains Identified: 16

14 of 16 Subdomains using Cloudflare

admin@robotsecurity.com

Date: 2023-07-08

Penetration Test Report: hackforums.net

During the preliminary stage of our penetration test, a thorough initial scan was performed, which identified a total of 16 unique response subdomains. Further examination of these subdomains revealed a noteworthy statistic: 14 of them were found to be utilizing Cloudflare as a means of security and performance enhancement. There are 2 subdomains that are potentially leaking important server IP addresses. This is a significant observation that warrants further discussion, due to the possible exposure or leakage of information related to the servers hosting your website. Cloudflare, as a leading provider of content delivery network services, DDoS mitigation, Internet security, and distributed domain-name-server services, offers robust protection for many websites. However, the reliance on this tool also introduces certain considerations. The most salient concern is that of Distributed Denial of Service (DDoS) attacks, a common threat in the digital landscape. DDoS attacks involve overwhelming a network with traffic, which, if successful, can lead to extended periods of downtime. This can cause significant disruption to your visitors, impairing their ability to access your website and potentially compromising their experience. Moreover, it's vital to consider that the identified subdomains could be hosting additional sensitive data or critical functionalities. If these areas were to be compromised due to vulnerabilities, it might not only lead to data breaches but also to malfunctions in essential website operations. Such breaches could lead to a slew of issues ranging from regulatory penalties to reputational damage. In the end, while Cloudflare offers substantial security benefits, it is crucial that we remain vigilant to the potential risks and vulnerabilities associated with its use. The purpose of this penetration test is not only to uncover potential vulnerabilities but also to provide you with a deeper understanding of your digital security landscape so you can better protect your operations in the future.

Domain	Cloudflare	Wordpress	.htaccess	.git/HEAD	.env	phpinfo.php	robots.txt	sitemap.xml	humans.txt	security.txt	crossdomain.xml	downloads	backups	/.well-known/
http://apidocs.hackforums.net	✓	✗	✗	–	–	–	✗	✗	✗	✗	✗	✗	✗	✗
http://pay.hackforums.net	✓	✗	✗	–	–	–	✗	✗	✗	✗	✗	✗	✗	✗
http://www.hackforums.net	✓	✗	✗	–	–	–	✗	✗	✗	✗	✗	✗	✗	✗
http://email.hackforums.net	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗
http://tracking.hackforums.net	✓	✗	✗	–	–	–	✗	✗	✗	✗	✗	✗	✗	✗
http://wiki.hackforums.net	✓	✗	✗	–	–	–	✗	✗	✗	✗	✗	✗	✗	✗
http://btcpay.hackforums.net	✓	✗	✗	–	–	–	✗	✗	✗	✗	✗	✗	✗	✗
http://hackforums.net	✓	✗	✗	–	–	–	✗	✗	✗	✗	✗	✗	✗	✗
https://apidocs.hackforums.net	✓	✗	✗	–	–	–	✗	✗	✗	✗	✗	✗	✗	✗
https://pay.hackforums.net	✓	✗	✗	–	–	–	✓	✗	✓	✓	✗	✗	✗	✗
https://www.hackforums.net	✓	✗	✗	–	–	–	✓	✗	✓	✓	✗	✗	✗	✗
https://email.hackforums.net	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗
https://tracking.hackforums.net	✓	✗	✗	–	–	–	✓	✗	✓	✓	✗	✗	✗	✗
https://wiki.hackforums.net	✓	✗	✗	–	–	–	✓	✗	✓	✓	✗	✗	✗	✗
https://btcpay.hackforums.net	✓	✗	✗	–	–	–	✗	✗	✗	✗	✗	✗	✗	✗
https://hackforums.net	✓	✗	✗	–	–	–	✓	✗	✗	✗	✗	✗	✗	✗

Legend:
✓: Exists
✗: Doesn't Exist
–: 403 Error (Forbidden or False Positive)

The 'downloads' directory was found to be exposed on the subdomain 'http://email.hackforums.net'. This could potentially allow unauthorized access to sensitive data. It is recommended to restrict public access to this directory or remove it if it's not necessary. The 'downloads' directory was found to be exposed on the subdomain 'https://email.hackforums.net'. This could potentially allow unauthorized access to sensitive data. It is recommended to restrict public access to this directory or remove it if it's not necessary.
Subdomain: email.hackforums.net | IP: 94.23.161.19 | Ports: 25,80,443,465,587,2525,2526

Date: 2023-07-08

Penetration Test Report: hackforums.net

During the process of evaluating your website's security, one of the key steps is to identify the different services operating on the server or computer where your website is hosted. This is like checking what programs are running in the background of your personal computer. Often, a single server may host multiple websites, much like a large office building might house several different companies. While this can be efficient, it can also present security risks. If any of the other websites on the same server are compromised, it could potentially put your own website at risk too. Think of this as if one company in the office building leaves a door unlocked, allowing a thief to enter. Once inside, the thief could also gain access to other companies in the same building. In a similar way, if another website on your server is hacked, the attacker might 'pivot', that is, use this compromised site as a springboard to infiltrate and manipulate your website's files. Another aspect to consider in this 'security audit' are the services like SSH (Secure Shell), RDP (Remote Desktop Protocol), SMB (Server Message Block), and FTP (File Transfer Protocol) that are running on your server. These services are like different doors into your 'office building' - they are necessary for operation, but each can also be a potential entry point for hackers. Exploits, which are ways hackers find to bypass security measures, can target these services. Some of these exploits are known as '0days' which means they are brand new and unknown to security professionals, making them particularly dangerous. Even if these '0days' aren't in play, if your server's software isn't kept updated, it could be vulnerable to older, known attacks - similar to how an old, rusty lock might be easier for a thief to pick. Regularly updating your software and monitoring the other websites hosted on your server are critical steps to ensure your website's security. By understanding these risks and taking the necessary precautions, you can greatly reduce the likelihood of your website being compromised.

166 unique database entries were discovered for your doman. Passwords, phone numbers, email addresses are all contained within these breaches from other websites that have been hacked in the past. It's important that your employees all use unique credentials for work and for each website to avoid credential stuffing attacks. This could be a very serious issue. Your site appearing in leaked databases indicates that at some point, the security of your website or one of the services it uses was compromised. Immediate action should be taken to investigate and rectify this issue.

Penetration Test Report: hackforums.net

WiFi Network Vulnerabilities for Company Offices

Wireless networks, commonly referred to as WiFi, have become ubiquitous in modern offices due to their ease of setup and use. However, this convenience can introduce a host of vulnerabilities that could potentially compromise an organization's sensitive data. An improperly secured WiFi network can expose your company to various attack vectors. Firstly, a rogue access point (AP) could be set up by an attacker to mimic a legitimate network, enticing employees to connect and thus enabling data interception. Secondly, encryption protocols like WEP (Wired Equivalent Privacy) and WPA (WiFi Protected Access) are susceptible to cracking techniques. The newer WPA2 and WPA3 protocols provide stronger security, but only if correctly implemented and regularly updated. Lastly, WiFi networks are susceptible to de-authentication attacks, wherein the attacker disconnects a legitimate user from the network and possibly establishes a man-in-the-middle attack, intercepting the user's communications when they attempt to reconnect.

Man-in-the-Middle (MitM) Attacks

A Man-in-the-Middle (MitM) attack is a type of cybersecurity threat where an attacker secretly intercepts and potentially alters the communications between two parties who believe they are directly communicating with each other. This attack can occur in several ways. One common method is via an unsecured or poorly secured WiFi network, where the attacker can easily place themselves between the communication of the user and the network. In another form, known as IP spoofing, the attacker can deceive the system into believing it's interacting with a known, trusted entity. MitM attacks can result in unauthorized access to sensitive information, such as login credentials, financial information, and confidential company data, leading to significant business damage, including financial loss, reputation damage, and regulatory penalties.

Rubber Duckies/OMG Cables

Rubber duckies and OMG cables are physical hacking tools that represent a significant security risk, often overlooked in cybersecurity strategies. A Rubber Ducky, technically known as a keystroke injection tool, resembles a typical USB drive but acts as an automated keyboard, executing pre-programmed keystroke sequences at superhuman speeds, making it capable of installing malware, exfiltrating data, or otherwise compromising a system in seconds. Similarly, an O.MG cable mimics a standard charging cable but contains an embedded chip allowing an attacker to remotely execute commands on the connected device. Both tools underscore the risk of hardware-based attacks, requiring robust physical security measures to supplement cyber defenses.

Employees Targeted at Home for Escalation Within the Company

As the world becomes more interconnected, employees' home networks have become an increasingly attractive target for threat actors aiming to compromise a company's internal systems. These attackers exploit the often lower security standards of home networks to gain access to work devices and sensitive data. By doing this, they can potentially escalate their privileges within the company's IT system through various techniques such as credential theft, malware installation, or spear-phishing attacks. This form of cyber-attack is often part of an Advanced Persistent Threat (APT) strategy, where the attacker gains access and retains a foothold for an extended period, often undetected. As remote work grows more common, businesses must consider the vulnerabilities presented by employees' home networks as part of their overall cybersecurity strategy, implementing measures like VPNs, multi-factor authentication, and comprehensive employee training to mitigate these risks.

Date: 2023-07-08

Penetration Test Report: hackforums.net

Parameters extracted which could be exploitable

As digital technology advances, web applications have become more complex and dynamic. They rely heavily on parameters to function correctly and to offer interactive experiences to their users. Parameters in a web application are like input boxes that communicate user's choices to the system. These parameters can be seen in URLs or in the body of HTTP requests, and can range from user IDs, product IDs, search keywords, to user input and many others. While parameters are vital to web applications, they also pose a significant security risk. Unvalidated or improperly handled parameters can lead to various forms of cyber attacks, including Local File Inclusion (LFI), Remote File Inclusion (RFI), Remote Code Execution (RCE), Cross-Site Scripting (XSS), and SQL Injection (SQLI). LFI and RFI attacks involve manipulating parameters to include files from the local server or a remote server. If successful, these attacks can lead to unauthorized access to sensitive data or even allow the attacker to execute arbitrary code. RCE is an attack that leverages vulnerabilities in an application to execute malicious code on the server. If an attacker can manipulate parameters and cause the server to execute this code, they can gain full control over the server. XSS attacks manipulate parameters to inject malicious scripts into webpages viewed by other users. These scripts can then be used to steal sensitive information from users who visit these pages. SQLI attacks manipulate parameters to interfere with the application's SQL queries. This can lead to unauthorized access to the database, data corruption, or even data loss. Given the potential damage these attacks can cause, it is crucial to check and sanitize parameters in web applications. This involves validating and sanitizing user input, employing secure coding practices, implementing appropriate security headers, and utilizing web application firewalls. By doing so, businesses can significantly reduce their vulnerability to these types of attacks, protecting their assets and their users' data in the process. In today's interconnected world, comprehensive parameter checks and robust cybersecurity practices are not just optional—they are essential in maintaining the integrity, functionality, and reputation of a business.

https://hackforums.net/forumdisplay.php?fid=32&datecut;=FUZZ
http://hackforums.net/forumdisplay.php?fid=249&page;=FUZZ
http://www.hackforums.net:80/forumdisplay.php?fid=17&sortby;=FUZZ
http://www.hackforums.net/index.php/member.php?action=FUZZ
http://www.hackforums.net/forumdisplay.php?fid=25&datecut;=FUZZ
https://hackforums.net/postactivity.php?uid=FUZZ
http://www.hackforums.net:80/index.php/member.php?action=FUZZ
https://hackforums.net/private.php?action=send&uid;=FUZZ
https://wiki.hackforums.net/index.php?title=8480&redirect;=FUZZ
http://www.hackforums.net:80/archive/index.php/misc.php?action=FUZZ
https://hackforums.net/misc.php?action=agreement/../https://adf.ly/?id=FUZZ
http://hackforums.net/misc.php?action=markread&fid;=FUZZ
https://hackforums.net/contracts.php?action=disputes&uid;=FUZZ
https://wiki.hackforums.net/edit/Template:High-risk?oldid=FUZZ
https://hackforums.net/xmlhttp.php?action=edit_subject&my;_post_key=FUZZ
http://www.hackforums.net/memberlist.php?by=FUZZ
http://hackforums.net/member.php?action=FUZZ
http://www.hackforums.net/misc.php?action=username_history&uhuid;=FUZZ
https://hackforums.net/syndication.php?type=atom1.0&fid;=FUZZ
https://hackforums.net/blog.php?page=FUZZ
https://hackforums.net/marketcp.php?action=FUZZ
https://wiki.hackforums.net/load.php?lang=en&modules;=FUZZ
http://www.hackforums.net/ipcheck.php?action=iplookup&ipaddress=FUZZ
http://hackforums.net:80/member.php?action=FUZZ
https://hackforums.net/flyover.php?action=login&provider;=FUZZ
https://www.hackforums.net/member.php?action=register&referrer=FUZZ
https://hackforums.net/disputedb.php?action=view&did;=FUZZ
https://hackforums.net/cdn-cgi/challenge-platform/h/g/orchestrate/managed/v1?ray=FUZZ
http://www.hackforums.net:80/myps.php?action=donate&username;=FUZZ
https://hackforums.net/repsgiven.php?uid=FUZZ
http://www.hackforums.net/cdn-cgi/l/*/http://www.hackforums.net/cdn-cgi/l/chk_captcha?id=1bb353a043241061&recaptcha;_challenge_field=FUZZ
https://www.hackforums.net/ipcheck.php?action=FUZZ
https://hackforums.net/alerts.php?action=view&id;=FUZZ
http://www.hackforums.net/search.php?action=FUZZ
http://www.hackforums.net:80/misc.php?action=FUZZ
http://hackforums.net:80/forumdisplay.php?fid=10&datecut;=FUZZ
http://www.hackforums.net:80/index.cfm?fuseaction=music.showDetails&friendid;=FUZZ
http://hackforums.net:80/postactivity.php?uid=FUZZ
http://www.hackforums.net/archive/index.php/forum-10-446.html?action=FUZZ
https://hackforums.net/member.php?action=logout&logoutkey;=FUZZ

Date: 2023-07-08

Penetration Test Report: hackforums.net

https://hackforums.net/search.php?message=FUZZ
http://www.hackforums.net/member.php?action=profile&anticache;=FUZZ
http://hackforums.net:80/misc.php?action=markread&fid;=FUZZ
http://www.hackforums.net:80/downloads.php?action=FUZZ
http://www.hackforums.net:80/calendar.php?action=dayview&calendar;=FUZZ
http://hackforums.net:80/online.php?sortby=FUZZ
https://hackforums.net/usercp.php?action=FUZZ
https://hackforums.net/myps.php?action=history&uid;=FUZZ
https://hackforums.net/https://hackforums.net/member.php?action=FUZZ
http://hackforums.net/private.php?action=send&uid=FUZZ
http://hackforums.net/captcha.php?imagehash=FUZZ
http://hackforums.net:80/memberlist.php?sort=FUZZ
http://www.hackforums.net:80/myawards.php?awid=FUZZ
http://www.hackforums.net/refer.php?action=details&uid;=FUZZ
http://www.hackforums.net:80/games.php?action=rate&gid;=FUZZ
http://hackforums.net/reputation.php?action=FUZZ
http://hackforums.net/ipcheck.php?action=iplookup&ipaddress=FUZZ
https://wiki.hackforums.net/api.php?action=FUZZ
http://www.hackforums.net:80/archive/index.php/ipcheck.php?action=iplookup&ipaddress;=FUZZ
https://hackforums.net/gamecp.php?action=profile&uid;=FUZZ
http://www.hackforums.net:80/reputation.php?uid=FUZZ
http://hackforums.net/refer.php?action=details&my;_post_key=FUZZ
https://wiki.hackforums.net/edit/Walt_Disney™?oldid=FUZZ
http://www.hackforums.net/modcp.php?action=editprofile&uid;=FUZZ
http://hackforums.net/archive/forumdisplay.php?fid=FUZZ
http://www.hackforums.net:80/ipcheck.php?action=FUZZ
http://hackforums.net/myps.php?action=FUZZ
https://hackforums.net/https://hackforums.net/forumdisplay.php?fid=FUZZ
http://hackforums.net:80/myvouch.php?uid=FUZZ
https://hackforums.net/https://www.coinpayments.net/index.php?ref=FUZZ
http://www.hackforums.net/forum/index.php?topic=FUZZ
https://wiki.hackforums.net/edit/Trust?oldid=FUZZ
http://www.hackforums.net/reputation.php?uid=FUZZ
https://www.hackforums.net/?__cf_chl_tk=FUZZ
https://hackforums.net/fonts/font-awesome-4.7.0/fonts/fontawesome-webfont.svg?v=FUZZ
http://www.hackforums.net:80/member.php?action=profile&uid;=FUZZ
http://hackforums.net:80/reputation.php?uid=FUZZ
http://hackforums.net:80/refer.php?action=FUZZ
http://www.hackforums.net:80/index.php/misc.php?action=FUZZ
http://www.hackforums.net/managegroup.php?action=joinrequests&gid;=FUZZ
http://hackforums.net:80/search.php?action=finduser&uid;=FUZZ
http://www.hackforums.net:80/archive/member.php?action=profile&uid;=FUZZ
http://hackforums.net/online.php?page=FUZZ
http://www.hackforums.net/archive/index.php/forum-10-460.html?action=FUZZ
https://hackforums.net/gtag/destination?id=FUZZ
http://www.hackforums.net:80/private.php?action=send&uid;=FUZZ
http://www.hackforums.net//ipcheck.php?action=FUZZ
https://hackforums.net/?__cf_chl_captcha_tk__=FUZZ
https://hackforums.net/https://hackforums.net/search.php?action=FUZZ
https://hackforums.net/sportsbook.php?page=FUZZ
http://www.hackforums.net/online.php?page=FUZZ
http://www.hackforums.net/hover.php?data=FUZZ
https://hackforums.net/myawards.php?awid=FUZZ

Date: 2023-07-08

Penetration Test Report: hackforums.net

http://www.hackforums.net/postactivity.php?uid=FUZZ
http://hackforums.net/search.php?action=finduser&uid;=FUZZ
https://hackforums.net/reputation.php?uid=2481137&page;=FUZZ
http://www.hackforums.net/private.php?action=read&pmid;=FUZZ
https://hackforums.net/member.php/robots.txt?action=profile&uid;=FUZZ
https://wiki.hackforums.net/edit/Viral_Dragon?oldid=FUZZ
http://www.hackforums.net/polls.php?action=FUZZ
http://www.hackforums.net:80/repsgiven.php?uid=FUZZ
http://www.hackforums.net/cdn-cgi/l/chk_captcha?id=FUZZ
http://www.hackforums.net/myps.php?action=donate&my;_post_key=FUZZ
https://hackforums.net/attachment.php?thumbnail=FUZZ
http://hackforums.net/attachment.php?thumbnail=FUZZ
http://www.hackforums.net/archive/index.php/forum-10-427.html?action=FUZZ
https://hackforums.net/https://hackforums.net/misc.php?action=markread&my;_post_key=FUZZ
http://hackforums.net/polls.php?action=FUZZ
http://hackforums.net:80/polls.php?action=FUZZ
https://hackforums.net/forumdisplay.php/robots.txt?fid=FUZZ
https://hackforums.net/blog/member.php?action=FUZZ
http://hackforums.net:80/myawards.php?uid=FUZZ
http://www.hackforums.net/showteam.php/member.php?action=FUZZ
http://www.hackforums.net/captcha.php?action=regimage&imagehash;=FUZZ
http://www.hackforums.net:80/archive/index.php/private.php?action=FUZZ
http://www.hackforums.net:80/index.php/forumdisplay.php?fid=FUZZ
http://www.hackforums.net:80/polls.php?action=FUZZ
https://hackforums.net/refer.php?action=details&uid;=FUZZ
http://hackforums.net/myawards.php?uid=FUZZ
http://hackforums.net:80/private.php?action=send&uid;=FUZZ
http://www.hackforums.net/disputedb.php?useruid=FUZZ
http://www.hackforums.net/?id=FUZZ
https://hackforums.net/index.php?action=FUZZ
https://hackforums.net/convo.php?do=FUZZ
https://hackforums.net/cdn-cgi/challenge-platform/h/b/orchestrate/managed/v1?ray=FUZZ
https://hackforums.net/debug/bootstrap?id=FUZZ
http://www.hackforums.net:80/archive/index.php/forumdisplay.php?fid=FUZZ
https://hackforums.net/blog/misc.php?action=help&hid;=FUZZ
https://hackforums.net/pagead/landing?gclid=FUZZ
https://wiki.hackforums.net/edit/Judge_Dredd?oldid=FUZZ
http://www.hackforums.net/attachment.php?thumbnail=FUZZ
http://www.hackforums.net/downloads.php?action=FUZZ
https://hackforums.net/hackuman.php?ajax=FUZZ
https://hackforums.net/captcha.php?action=FUZZ
https://hackforums.net/salestag.php?action=FUZZ
https://hackforums.net/tools.php?action=FUZZ
https://hackforums.net/robots.txt/member.php?action=FUZZ
https://hackforums.net/https://hackforums.net/sportsbook.php?action=FUZZ
https://www.hackforums.net/myawards.php?awid=FUZZ
http://hackforums.net:80/archive/index.php/ipcheck.php?action=iplookup&ipaddress;=FUZZ
https://hackforums.net/ipcheck.php?action=FUZZ
https://hackforums.net/editpost.php?pid=FUZZ
http://www.hackforums.net:80/memberlist.php?by=FUZZ
https://hackforums.net/online.php?action=FUZZ
https://hackforums.net/scratchcard.php?action=FUZZ
http://www.hackforums.net:80/refer.php?action=FUZZ

Date: 2023-07-08

Penetration Test Report: hackforums.net

https://www.hackforums.net/misc.php?action=username_history&uhuid;=FUZZ
http://www.hackforums.net//attachment.php?aid=FUZZ
https://hackforums.net/newreply.php?ajax=FUZZ
http://www.hackforums.net/archive/index.php/forum-10-147.html?action=FUZZ
https://wiki.hackforums.net/edit/ViewsFromThe6ix?oldid=FUZZ
http://www.hackforums.net/archive/index.php/forum-10-326.html?action=FUZZ
http://www.hackforums.net/myawards.php?awid=FUZZ
http://www.hackforums.net/myvouch.php?uid=FUZZ
http://www.hackforums.net:80/attachment.php?aid=FUZZ
https://hackforums.net/https://adf.ly/?id=FUZZ
http://www.hackforums.net/repsgiven.php?uid=FUZZ
http://www.hackforums.net:80/announcements.php?aid=FUZZ
https://hackforums.net/fonts/font-awesome-4.7.0/fonts/fontawesome-webfont.eot?v=FUZZ
https://btcpay.hackforums.net/login?ReturnUrl=FUZZ
http://www.hackforums.net:80/myvouch.php?uid=FUZZ
http://www.hackforums.net:80/search.php?action=FUZZ
https://wiki.hackforums.net/edit/Omniscient?oldid=FUZZ
https://hackforums.net/https://localbitcoins.com/?ch=FUZZ
https://hackforums.net/https://hackforums.net/syndication.php?type=FUZZ
http://www.hackforums.net:80/index.php?title=FUZZ
http://hackforums.net:80/coins.php?action=FUZZ

admin@robotsecurity.com