101domain® Corporate Brand Services

CYBER SECURITY

Reducing Opportunities for Attack on Your Corporate Infrastructure with Cloudflare

You've built your business and your brand. Now how do you secure and protect it?

CYBER SECURITY

CONTENTS

INTRODUCTION

This whitepaper will walk you through the four most common web infrastructure vulnerabilities that exist today. These threats, when unaddressed, leave your organization open to attacks with potentially devastating consequences. We'll show you real-world examples of these attacks in action and present one easy to use, simple to install, and comprehensive solution to reduce your attack opportunities and improve your overall speed, performance, and reliability.

DOS & DDOS ATTACKS

WHAT IS A DOS/DDOS ATTACK?

A Denial-of-Service Attack, also known as a DOS attack, is a cyberattack that seeks to make a network resource like your website, server, or surrounding infrastructure unavailable to users. A Distributed Denial-of-Service Attack (DDoS) uses multiple compromised computer systems to overwhelm a targeted service with a flood of Internet traffic.

Simply put, a DDoS attack is like an unexpected traffic jam clogging up the highway, preventing regular traffic from arriving at its destination.

CONSEQUENCES OF A DDOS ATTACK

DDoS attacks are a primary concern in Internet security today because it uses up all of the network bandwidth a company should be spending on legitimate users to prevent the online business from operating as usual. Preventing legitimate users and customers from accessing your website can be extremely damaging. DDoS attacks can harm your company's reputation and negatively impact site revenue by cutting off online purchases. Also, they can be extremely costly to remedy.

DDOS PROTECTION WITH CLOUDFLARE

We explored how DDoS attacks function, and now for the juicy part—how they can be stopped. There are preventative measures you can take to avoid becoming the next victim of a DDoS attack. The number one is investing in a DDoS mitigation service. Cloudflare is one of the largest DDoS mitigation providers on the market, with a network of servers around the world powerful enough to protect against the strongest recorded DDoS attacks.

Cloudflare is the middleman between your server and the rest of the Internet, intercepting web traffic to ensure only clean requests are coming through. **From a high level, Cloudflare is like a water filtration system that automatically filters out malicious requests before they can even reach your website.**

THERE ARE 4 STAGES OF MITIGATING A DDOS ATTACK WITH CLOUDFLARE

1. Detection – Detect the fingerprint of an attack as it occurs

Cloudflare oversees over 11M HTTP requests a second—with each server in the global network checking IP reputation, common attack patterns, and previous data for indications of various types of DDoS attacks and filter requests accordingly.

2. Response – Drop malicious traffic at the network edge

Cloudflare responds to incoming identified threats by intelligently dropping malicious bot traffic and absorbing the rest of the traffic. The network can mitigate the attempted attack using Web Application Firewall (WAF) page rules.

3. Routing – Route traffic across multiple Data Centers

Cloudflare intelligently routes traffic to a network of servers worldwide, breaking the remaining traffic into manageable chunks and preventing denial-of-service.

4. Adaption – Use machine learning to adapt to the attack pattern

Cloudflare uses machine learning to analyze the enormous amount of Internet traffic passing through the network to learn and improve continuously. The information is used to harden the Cloudflare network against future attacks and protect other users.

DIRECT PAYLOAD ATTACKS

WHAT IS A DIRECT PAYLOAD ATTACK?

In the context of a cyberattack, a payload is the attack element that causes harm to the victim. Viruses, worms, and malware are all examples of attack vectors containing a malicious payload waiting to be triggered. You can also find payloads in email attachments. **Symantec has reported that one in every 359 emails contains a malicious payload, and this ratio is trending upward.**

The most common types of Direct Payload Attacks are Injection Attacks and Brute Force Attacks.

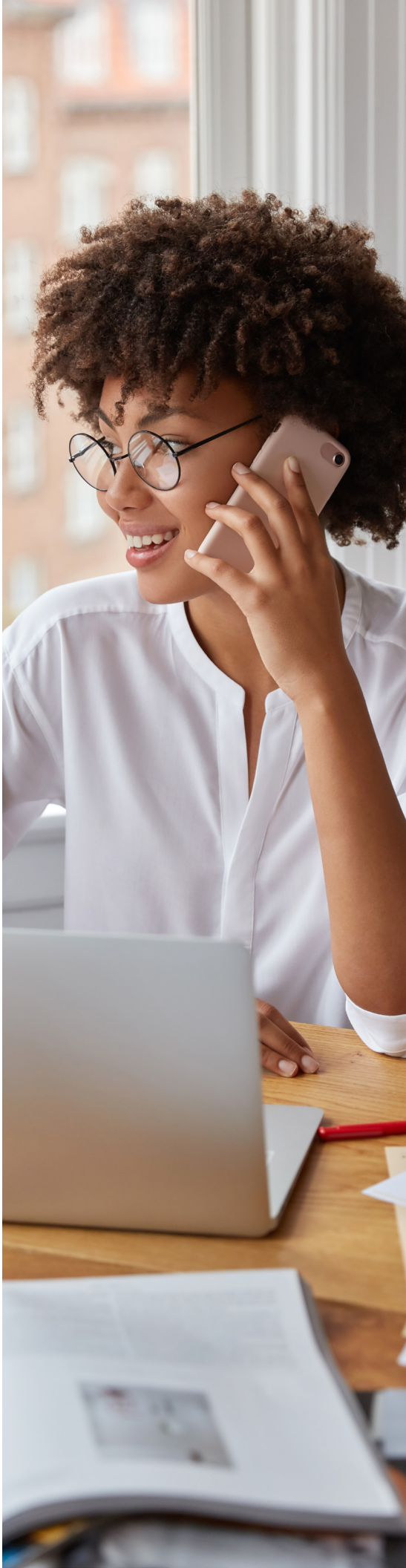
INJECTION ATTACKS

Cross-Site Scripting, also known as an XSS Payload Attack, attaches code onto a legitimate website that triggers when the victim loads the website. Attackers can insert malicious code in several ways. It is most popularly either added to the end of a URL or posted directly onto a page that displays user-generated content such as a web forum. In an XXS Payload Attack, the attacker can access APIs for data theft, identity theft, and other malicious purposes.

Database Injection, also known as Structured Query Language (SQL) Injection Attacks, targets a vulnerable Application Programming Interface or API to access a database or conduct other manipulative behaviors. SQL injections are easy to implement. An attacker will commonly use tools that automatically search through a website looking for forms to exploit, modify, retrieve, or destroy sensitive data.

BRUTE FORCE ATTACKS

A Brute Force Attack is a trial-and-error method used to decode sensitive data. The most common applications for brute force attacks are cracking passwords, encryption keys, and API keys. Brute force password attacks are often carried out by scripts or bots that target a website's login page, attempting different combinations until it finds the correct combination. You can think of it as a thief trying to break into a combo safe by attempting every possible combination of numbers until the safe opens.



CONSEQUENCES OF A DIRECT PAYLOAD ATTACK

There are a number of ways in which payloads can harm their victims and cause significant damage.

Data Theft
Prevalent is the theft of sensitive information such as login credentials or financial information through data breaches.

Activity Monitoring
A payload may serve to monitor user activity on a computer for spying, blackmail, or collecting consumer behavior, which can be sold to advertisers.

Display Advertisements
Some malicious payloads work to display persistent, unwanted ads such as pop-ups to the victim.

Deleting or Modifying Files
Files can be deleted or modified to either affect a computer's behavior or even disable the operating system from turning on or being used in any way.

Downloading New Files
Once triggered, some payloads will download large pieces of malicious software.

Running Background Processes
A payload can also be triggered to quietly run processes in the background, such as cryptocurrency mining or data storage.

CLOUDFLARE WAF SOLUTION

Cloudflare's Web Application Firewall (WAF) protects your web infrastructure from SQL injection, cross-site scripting (XSS), and other malicious content. Cloudflare WAF is fully-integrated with DDoS protection and blocks millions of attacks daily, automatically learning from each new threat. There are a few WAF options available in the Cloudflare Control Panel: Cloudflare Managed Ruleset, OWASP ModSecurity Core Rule Set, and Customer Requested Rules.

Cloudflare WAF runs ModSecurity rule sets out of the box, protecting you against the most critical web application security flaws that exist. As a cloud-based service, Cloudflare's WAF requires no hardware or software to install and maintain. You can deploy WAF with a single click, customizing it to meet your needs.

DNS CACHE POISONING

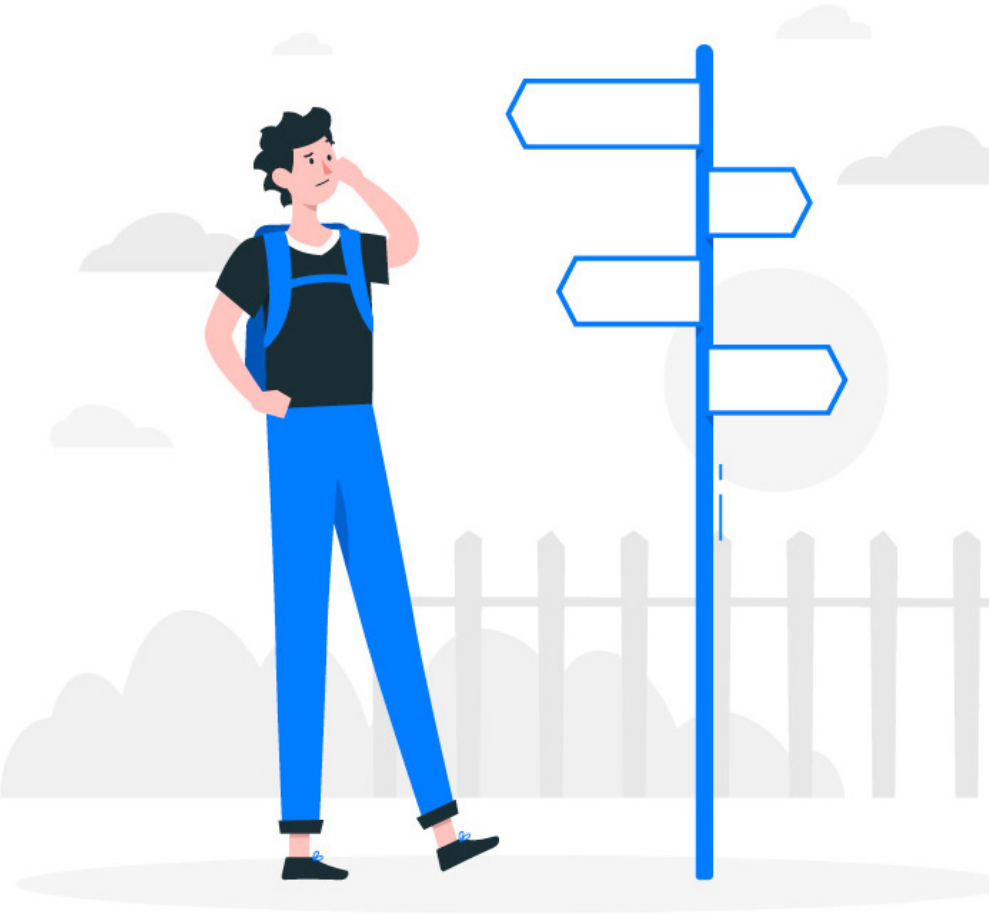
WHAT IS DNS CACHE POISONING?

Before you can understand DNS cache poisoning, you must first generally know how the Domain Name System (DNS) works. DNS is the backbone of the Internet. You can think of DNS as a massive global phone book that directs and routes all the calls that users and other devices make to each other day in and day out, 24/7/365.

DNS tells computers where to send and retrieve information – but it also accepts any address given to it, no questions asked. Attackers have exploited the flaws in the decades-old DNS infrastructure to conduct attacks such as DNS cache poisoning.

DNS Cache Poisoning also known as DNS Spoofing is the act of entering false information into a DNS cache so that users are directed to the wrong websites. A number of vulnerabilities make DNS poisoning possible, but there are ways to prevent it. A more secure DNS protocol called DNSSEC aims to solve some of these problems, but it has not been widely adopted yet.

Imagine DNS cache poisoning as a senior-year prank where high school seniors change out all the room numbers on their high school campus, so that the new students who don't know the campus layout yet will spend the next day getting lost and showing up in the wrong classrooms.



HOW DOES DNSSEC SOLVE THESE PROBLEMS?

Domain Name System Security Extensions (DNSSEC) adds a layer of trust on top of DNS by providing authentication before accepting an answer. You can think of DNSSEC as the Internet's non-spoofable caller ID. It guarantees traffic coming to your website is not intercepted by a hidden attacker, protecting both your web infrastructure and site visitor from attack.

Public/Private Key Encryption

DNSSEC implements a hierarchical digital signing policy across all layers of DNS. For example, in the case of a 'google.com' lookup, a root DNS server would sign a key for the .COM nameserver, and the .COM nameserver would then sign a key for google.com's authoritative nameserver.

Zone Signing

DNSSEC creates a chain of trust that travels up to the root zone. This chain of trust cannot be compromised at any layer of DNS. The root zone itself needs to be validated (proven to be free of tampering or fraud) to close the chain of trust. This is done using human intervention. In a Root Zone Signing Ceremony, selected individuals from around the world meet to sign the root DNSKEY RRset in a public and audited way.

CLOUDFLARE DNSSEC

Cloudflare has easy to deploy DNSSEC. Cloudflare's one-click DNSSEC protects your users from attacks that can spoof or hijack your DNS records. The DNSSEC protocol verifies that a requested DNS record came from its authoritative name server and wasn't altered en-route via cache-poisoning, man-in-the-middle attacks, or other types of DNS forgeries.

THE DANGERS OF NOT USING ENCRYPTION

WHAT IS HTTPS ENCRYPTION?

SSL, or Secure Sockets Layer, is an encryption-based Internet security protocol that ensures privacy, authentication, and data integrity in Internet communications. SSL is the predecessor to the modern TLS encryption used today. A website that implements SSL/TLS has "HTTPS" in its URL instead of "HTTP."

SSL protects user privacy by encrypting any data between a user and a web server. Encryption via SSL ensures that attackers cannot intercept sensitive information such as credit card information, personally identifiable information, and passwords in transit.

ACHIEVING TLS & HTTPS WITH CLOUDFLARE

The Cloudflare Control Panel is an environment for your web infrastructure where you can quickly analyze, manage, and deploy performance and security settings in one place. When creating an encryption strategy for your web infrastructure, there are four elements to consider.

1. Ensuring that only updated cryptographic protocols are in use

Both TLS 1.0 and TLS 1.1 are insufficient for protecting information and securing payment card related traffic.

TLS 1.2 became the industry standard in 2008. Both the Payment Cards Industry Security Standards Council (PCI SSC) and the National Institute of Standards and Technology (NIST) endorse TLS 1.2 for tighter security on the web. Cloudflare can help you achieve PCI standard recommendations using TLS 1.2 and mitigate earlier TLS/SSL versions.

2. Disable deprecated encryption protocols

Using Cloudflare's minimum TLS version guarantees encrypted communications between a client and a web server via HTTPS. It replaces the now deprecated SSL protocol.

You can manage the TLS version that your domain uses as a part of the Cloudflare network by setting the Minimum TLS Version in the Cloudflare Control Panel.

Selecting a minimum TLS version ensures that all subsequent, newer versions of the protocol are also supported. TLS 1.0 is the version that Cloudflare sets by default for all customers using certificate-based encryption. It means that Cloudflare also accepts requests encrypted with all TLS versions beyond 1.0.

3. Removal of weak ciphers

Depending on the minimum TLS option specified in the Cloudflare Control Panel, Cloudflare either connects to an origin web server over HTTP or HTTPS. There is a list of origin server SSL ciphers that Cloudflare supports for TLS 1.3, TLS 1.2, and earlier TLS versions when connecting to your origin web server over HTTPS. You can remove weak ciphers in the Cloudflare Control Panel to further strengthen your encryption.

4. Disable or forward ports using encrypted protocols

It is simple to manage and update TLS versions and ensure that all requests are completed using HTTPS using the Cloudflare Control Panel.

SECURE WEB ACCLERATOR

101domain's Secure Web Accelerator powered by Cloudflare provides a scalable, easy-to-use, unified control environment to deliver security, performance, and reliability for corporate infrastructures. Add your domains to the Cloudflare network to reduce the opportunity for attacks, including DOS/DDoS, Direct Payload, DNS Cache Poisoning, and Deprecated Encryption Protocols.

Trusted by over 16% of the Fortune 1000, Cloudflare is the security solution that helps build a better Internet. To learn more please visit www.101domain.com/secure_web_accelerator.htm.

If you are interested in a free Technical Scan of your website to assess your web infrastructure's security and performance vulnerabilities, please contact a member of our Sales team at 877.983.6624.

CLOUDFLARE® SECURITY BENEFITS FOR ENTERPRISES

Ease of Use

No code changes required; the Cloudflare dashboard enables quick configuration in one deeply unified control panel.

Simple Installation

All your domains can be managed through the Cloudflare Control Panel. You get a dedicated solutions engineering team to help onboard and change your DNS records to Cloudflare with zero downtime.

Integrated Performance & Reliability

In addition to the security benefits of joining the Cloudflare global cloud network that spans over 200 cities in more than 100 countries, you also get access to other features such as CDN, Analytics, and Optimizations.

A PARTNER YOU CAN TRUST

With increased pressure for security on the Internet, it is essential to employ Cloudflare services on your web infrastructure.

If you would like more information or advice on implementing any of the security features mentioned, 101domain dedicated account managers and experienced engineers will be happy to assist you.

www.101domain.com
corporate@101domain.com
877.983.6624