ATHENIAN PROJECT

BY CLOUDFLARE

The Interactive Guide to Protecting Your Election Website

1 INTRODUCTION

Cloudflare is on a mission to help build a better Internet.

Cloudflare is one of the world's largest networks. Today, businesses, nonprofits, bloggers, and anyone with an Internet presence uses our network to make their websites, apps, and anything connected to the Internet fast and secure. More than 20 million Internet properties are protected by Cloudflare, and our network is growing by tens of thousands per day. Cloudflare powers requests for ~10% of the Fortune 1000.

As one of the world's largest networks, we believe it is our duty to help protect the most vulnerable voices and most critical institutions on the Internet.

In September 2017, the U.S. Department of Homeland Security informed 21 states that their voter registration files or public election websites had been the target of cyber attacks.

Among their many responsibilities, state and local officials are often responsible for election websites, which are increasingly the primary source of critical voter information, such as where to vote, how to vote, and who is running for office. Just like every other Internet property, election websites need to be fast, they need to be reliable, they need to be secure. Yet, scarce budgets too often prevent governments from getting the right resources to prevent attacks and stay online.

We created the Athenian Project to ensure that state and local governments have the highest level of protection and reliability, so that their constituents can access election information and voter registration.

The Athenian Project offers Cloudflare's Enterprise level of protection to state and local election websites for free. As part of this project, we are introducing this Interactive Guide to Protecting Your Election Website so that you are aware of the vulnerabilities and how Athenian Project protects you from them.

Taking the steps included in this guide helps us all ensure that the Internet remains a vital resource for elections.

2 WHY ELECTION WEBSITES CAN BE TARGETS

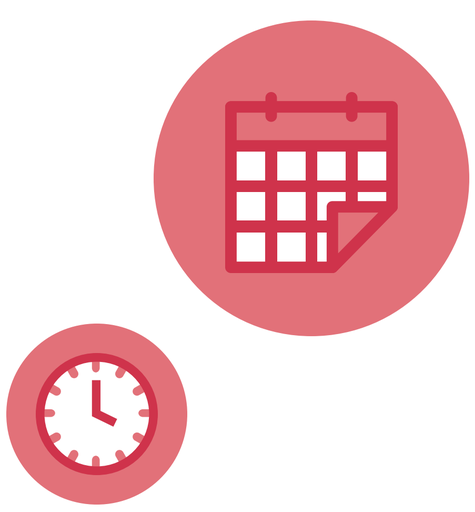
Election websites serve a powerful role in democratic elections.

They provide crucial information to people before, during, and after elections. Election websites can also be targets of attack and can face vulnerabilities due to peaks in traffic.

Here are just some of the ways that vulnerabilities can interfere with a smooth democratic election:

Before elections

Security and performance vulnerabilities can cause these sites to become unavailable or to spread false information about how to register to vote and the specific state and local measures that will be on the ballot.



During elections

Security and performance vulnerabilities can prevent citizens who visit election websites from accessing important information about where and when to vote.

After elections

Security and performance vulnerabilities can interfere with people who visit election websites after an election to see the results and get real-time updates.

3 VULNERABILITIES AND SAFEGUARDS - HOW TO PROTECT YOUR ELECTION WEBSITE

The Internet's open, distributed nature creates security and performance vulnerabilities for election websites.

Here's what you need to know to protect your Internet presence before any damage is done.

THREAT #1 Distributed Denial-of-Service (DDoS) attacks

THREAT #2 Data Theft

THREAT #3 Malicious Bots

THREAT #3 Website Availability

THREAT #1

Distributed Denial-of-Service (DDoS) attacks

What is it?

Bad actors can target election websites with denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks that target websites and network infrastructure. These attacks overwhelm available resources, often utilizing application layer (layer 7) attacks.

How Athenian Project protects your election website:

Protect your network

The first step in protecting against a DDoS attack is to ensure that multiple layers of security controls are able to protect your network. Example controls include utilizing a web application firewall or IP reputation database.

Block malicious traffic at the edge

A CDN provider will have insights into global traffic that would be impossible for individual websites to maintain. This knowledge is often fed into security actions. For example, Cloudflare employs a program called Gatebot, which automatically blocks bad traffic at the edge, preventing this traffic from reaching your origin.

THREAT #1

Distributed Denial-of-Service (DDoS) attacks

How Athenian Project protects your election website:

Protect your DNS

DNS, short for Domain Name System, is the phone book for the Internet. It associates an IP address with a corresponding URL address. Nearly every action you take on the Internet starts with a DNS request. For example, when you type ‘google.com’ into a web browser, DNS is the system that finds the numerical IP address behind the letters. Cloudflare can help protect DNS because our authoritative DNS servers run on the same 30Tbps network which protects more than 20 million Internet properties.

THREAT #2

Data Theft

What is it?

Election websites can be vulnerable to security breaches like SQL injection attacks, cross-site scripting, and cross-site forgery requests, which can lead to the theft of data, including voter data.

What's SQL injection?

Structured Query Language (SQL) Injection is a code injection technique used to modify or retrieve data from SQL databases. By inserting specialized SQL statements into an entry field, an attacker is able to execute commands that allow for the retrieval of data from the database.

How Athenian Project protects your election website:

Use HTTPS encryption

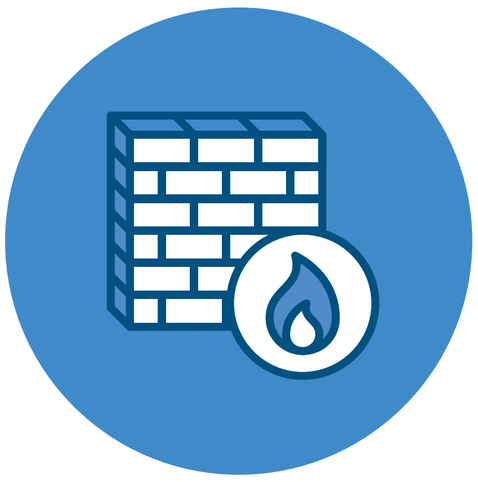
Protecting your website starts with strong encryption practices. Secure Sockets Layer, or SSL, is the first widely-adopted web encryption protocol. The latest protocol is called TLS, short for Transport Security Layer. Because data on the Internet is transferred across many locations, it is possible for bad actors to intercept packets of information as they move across the globe.

By using a cryptographic protocol, like TLS, websites ensure that only the intended recipient is able to decode and read the information, and intermediaries are prevented from decoding the contents of the transferred data.

THREAT #2

Data Theft

How Athenian Project protects your election website:



Use a Web Application Firewall

A Web Application Firewall (WAF) monitors, filters, and blocks HTTP traffic to a web application. Using a WAF protects your Internet property from common vulnerabilities like SQL injection attacks, cross-site scripting, and cross-site forgery requests.

Did you know?

Cloudflare develops automatic rules for our WAF based on intelligence we gather from our global network.

USE DNSSEC

If DNS is the phone book of the Internet, DNSSEC is the Internet's unspoofable caller ID. It guarantees a web application's traffic is safely routed to the correct servers so that a site's visitors are not intercepted by a hidden 'man-in-the-middle' attacker which can go unnoticed by site visitors, increasing the risk of phishing, malware infections, and personal data usage.

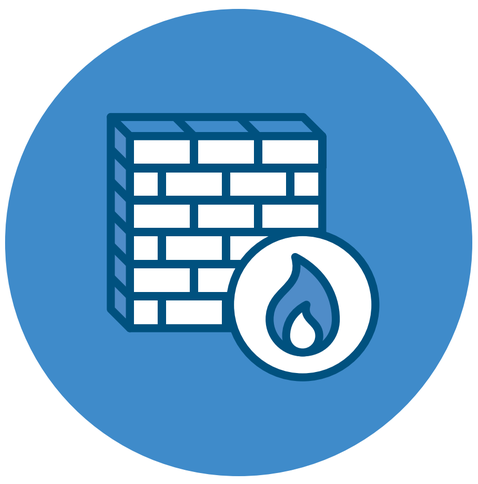
THREAT #3

Malicious Bots

What is it?

Bad actors can create bots that interfere with election websites. The most common types of abuse include content scraping and account takeover, which can lead to increases in operational costs and data loss.

How Athenian Project protects your election website:



Use a Web Application Firewall

A Web Application Firewall (WAF) filters, monitors, and blocks HTTP traffic to and from a web application. Using a WAF protects your internet property from common vulnerabilities like SQL injection attacks, cross-site scripting, and cross-site forgery requests.

Use an IP reputation database

IPs that perform malicious actions can be tracked with a global reputation system. An IP reputation database enables shared network intelligence and predictive security to identify and block abusive bots.

THREAT #4

Website Availability

What is it?

Oftentimes, election websites experience periods of high traffic, often referred to as network spikes. These spikes in traffic can overwhelm websites creating a poor user experience — at times, content on the website will slowly load; at other times, the content will not load at all.

Similarly, spikes in traffic can also lead to increased network infrastructure bills, due to higher network and server utilization. Using a CDN and caching will help offload resources from your server at all times, optimizing your website's resources and reducing the burden of spikes in traffic.

How Athenian Project protects your election website:

Reliable DNS

Reliable DNS providers like Cloudflare use vast networks of servers to ensure that your content is always reachable and decreases delays in resolving your DNS.

Anycast Content Delivery Network

Cloudflare is an Anycast CDN which quickly routes incoming traffic to the nearest data center with the capacity to process the request efficiently, handling surges in web traffic due to voter registration deadlines and election result updates.

THREAT #4

Website Availability

How Athenian Project protects your election website:

Perform country blocks at the edge

Oftentimes, election websites are looking to serve web traffic to countries in which the visitor is not a constituent. Being able to block specific countries frees up resources and prevents malicious attacks.

CDN/Caching

Serving static assets from a CDN provider will significantly offload resource load from your origin. This will allow for more processing power from your servers, especially during peak times, during the election or when results are published.

Knowing is half the battle

It’s important to monitor how your election website is performing. With Athenian Project, you have access to Cloudflare’s analytics platform, giving you full insight into performance, availability, and security of your election website.

Ok, you’re well on your way!

You now have the fundamentals of election website vulnerabilities and the steps you can take to make them secure and reliable.

4 HOW CAN I SIGN UP FOR ATHENIAN PROJECT?

We launched Athenian Project to help protect democratic elections.

If you run a state or local election website in the United States, we encourage you to apply. Athenian Project is for websites that administer elections. This includes sites that provide information related to voting and polling places, voter data, including voter registration or verification, or the reporting of election results.

If you feel that your website could benefit from the Athenian Project, reach out to us at Cloudflare and we can walk you through signing up your webpage and upgrading your service to Enterprise level.

VISIT AND APPLY AT:

HTTPS://WWW.CLOUDFLARE.COM/ATHENIAN

CLOUDFLARE®