# Vulnerability Scanning

In the age of growing vulnerability from an ever-increasing scale of cyber attacks, ensuring your website and web applications are secure has never been so important.

One of the easiest ways for malicious actors to leverage your website, app or network is through the exploitation of vulnerabilities in the back end of the relevant system. Whilst businesses of all sizes like to think they are completely secure, vulnerabilities will exist - so how can you ensure your platform is completely secure? One of the most simple and cost-efficient methods is vulnerability scanning.

## What is vulnerability scanning?

Vulnerability scanning helps to protect websites and web applications against attacks from hackers and cybercriminals.

Vulnerability scanning is the automatic process of assessing security vulnerabilities in hardware, website, applications and internal networks, through the analysis of multiple areas of code to ensure that there are no opportunities for areas to be exploited by cybercriminals.

Through analysing a website, application or network, the scanning software identifies possible security holes, vulnerabilities or misconfigurations, compiles these into an automatic report and sent to the relevant team. From this report, developers or engineers can identify the necessary elements which need attention, ensuring total security moving forward.

## How does vulnerability scanning work?

Vulnerability scanning can take shape in two main ways:

### Unauthenticated scans

These scans will find the weaknesses in your overall security

### Authenticated scans

These scans use privileged access to find further security weaknesses in pre-determined internal networks

Whichever type you choose, vulnerability scanning tools will use reference databases of known flaws, coding bugs, anomalies, configuration errors and potential routes into corporate networks that attackers can exploit. These databases are updated continually.

## Why should you consider vulnerability scanning?

Whilst you may regularly check the security of your networks and systems, there will be vulnerabilities that will naturally fall through the net.

In the age of increased cybercrime, more and more malicious actors are looking to utilise automated tools to identify and exploit known vulnerabilities and access unsecured systems before an organisation realises. Traditionally it was harder for hackers to explore your systems, but with the rise of automated tools, exploiting vulnerabilities has become relatively easy - every internet-facing organisation is at risk. With such a rise, this is why processes such as vulnerability scanning and patch management have become so essential.

## Why Hyve for vulnerability scanning?

We provide industry-leading security expertise to identify vulnerabilities and implement corrections. Our team of expert technical engineers scan your websites and web applications to look for open web application security vulnerabilities, such as cross-site scripting, SQL injection, broken authentication and more.

For a small management fee, our team of dedicated experts will correct any vulnerabilities for you, keeping your website or web application completely secure.