digital hands®

How Cybercriminals Are Attacking Healthcare Organizations

Cybercriminals are taking advantage of the global pandemic. One study showed that since the introduction of COVID-19 vaccines, healthcare organizations suffer 187 million web application attacks monthly.

To put it simply, cybercriminals are launching hundreds, possibly thousands of attacks on your most public-facing digital assets. Your organization's websites, web applications, and web services such as APIs are constantly under siege due to critical vulnerabilities which provide easy access for hackers.

01

Most Common Vulnerability - XSS (Cross-site scripting) Attacks

How it works:
Attackers inject malicious scripts on your trusted web pages. When an unsuspecting victim visits your infected site, the victim's browser doesn't recognize the malicious script and executes it. The script then allows the attacker to steal session cookies.

Sensitive data entered into forms on vulnerable sites can also be stolen, for example credit card info and its CVC info. Or, via JavaScript, hackers can transform information on a specific website page, like changing the details of a bank transfer.

XSS or cross-site scripting is the most common type of web application attacks, consisting of 28% of the total web-related vulnerabilities seen in 2020. These types of attacks are common in web applications written in JavaScript and CSS.

02

SQL Injection Attacks

How it works:
SQL injections happen when an attacker inserts or "injects" an SQL query via input data fields. For example, a hacker could insert malicious code via your organization's 'new patient' registration form. Once inserted, the SQL query executes in the back-end database, giving the attacker access to the server. They can then either control your application, retrieve other patients' records, or even alter original data from the linked database.

Applications using SQL databases such as MySQL, Oracle, and SQL Server are especially susceptible to SQL injections.

03

Broken Authentication

How it works:
To distinguish and identify users, web applications use session cookies. Once a user enters their login and password information, special identifiers are saved in a specific storage, which the program sends to the server with every query for a page of the app.

If an attacker manages to steal this identifier, and there are no other security measures in place to perform other checks such as for the session's IP address or for multiple connections in a session, the intruder could potentially access the system with the stolen user's account.

According to the OWASP Top 10, a broken authentication vulnerability is one of the most critical weaknesses in web applications.

04

Security Mis-configurations

To properly secure your web applications, all infrastructure elements—for example application frameworks and servers—must be properly configured. Organizations often use default settings for server components, which opens themselves up to leaks.

For example, attackers can steal session cookies via JavaScript in an XSS attack because of the Cookie HttpOnly setting, which is disabled by default. A server that is configured correctly with the Cookie HttpOnly setting enabled would make it impossible to receive a session cookie via JavaScript.

Similar weaknesses can be found in default settings in database servers like Redis, Memcached and so on. The default settings of these database servers allow hackers to easily infiltrate, read and modify data.

Properly securing your web applications and fixing these vulnerabilities is difficult even for large organizations with dedicated IT resources.

Hiring a good Managed Security Service Provider (MSSP) to augment your existing security infrastructure is a quick and cost-effective way to ensure that your web applications are fully secure and meet regulatory compliance standards.

ENSURING YOUR ORGANIZATION IS SECURE WITH DIGITAL HANDS CYGUARD™ WEB APPLICATION SHIELDING

Digital Hands is a trusted, award-winning MSSP and cybersecurity leader with extensive security expertise offering advanced protection, detection, and remediation services.

CyGuard™ Web Application Shielding is Digital Hands' fully managed web application security service. With CyGuard™ Web Application Shielding, you immediately mitigate the vulnerabilities in your applications and secure them against modern cyber attackers without changing a single line of code.

Our team achieves this by correcting insecure behavior with customized code objects and shields that we place in front of your applications. This shield secures the vulnerabilities in all your applications so that they cannot be exploited, regardless of the source code—saving you precious resources which you can use to strengthen your business.

To learn more about application shielding and Digital Hands' composable security service, download the full white paper here or visit www.digitalhands.com.

digital hands®