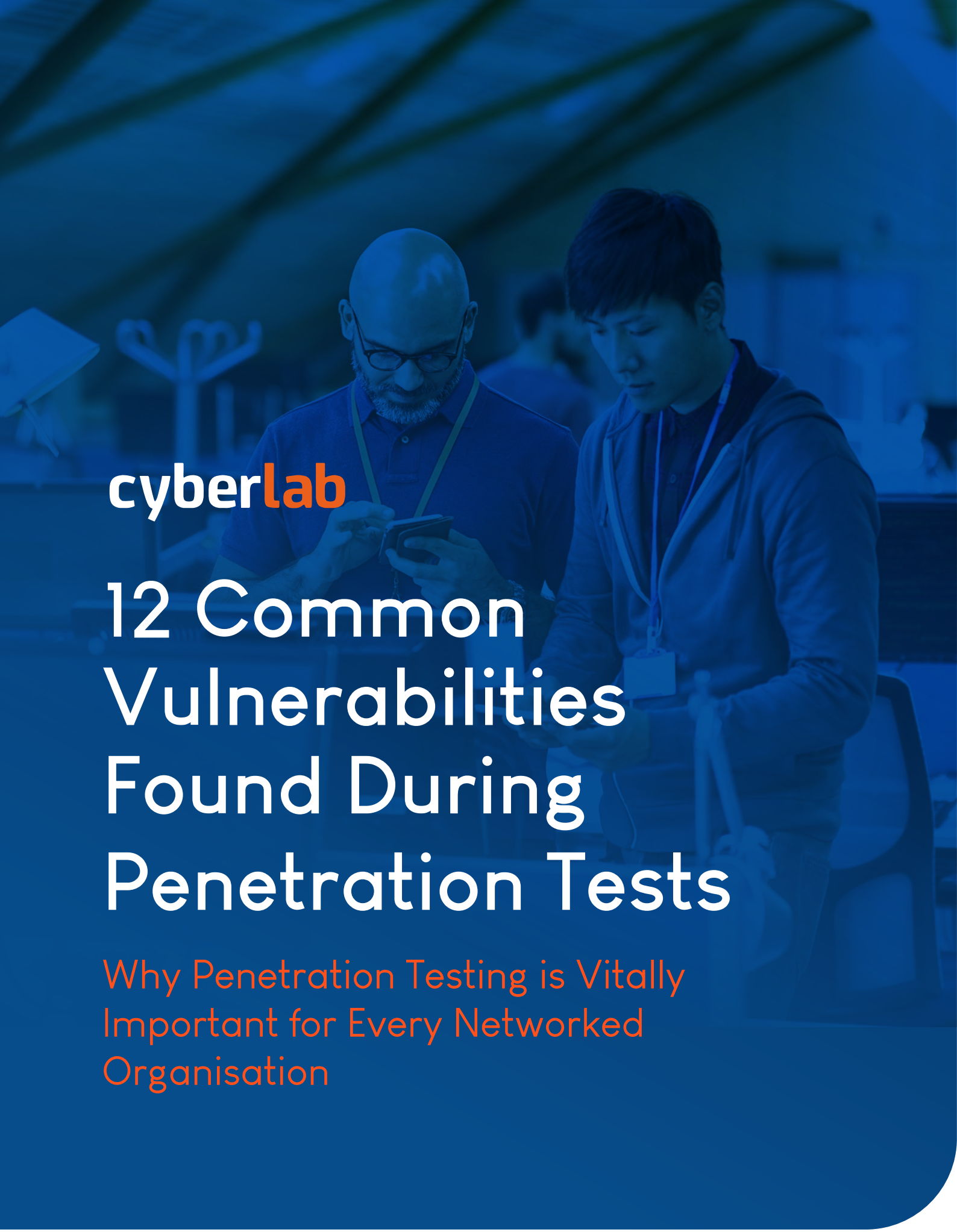


cyberlab

12 Common Vulnerabilities Found During Penetration Tests

Why Penetration Testing is Vitally Important for Every Networked Organisation

Introduction

Penetration testing is a critical part of any organisation's security strategy. It involves simulated attacks on the organisation's network and systems to identify vulnerabilities and weaknesses that hackers could exploit. Penetration testing helps organisations identify their security gaps and take proactive measures to address them before malicious actors use them.

When choosing a third-party organisation to perform a penetration test, it's important to consider certain criteria. In our experience, it's common for penetration test reports to uncover both expected and unexpected issues, some of which could be alarming.

Yet this is the purpose of a penetration test (or 'pen test'), as we'll call it. If a pen test contains a few surprising results for network administrators who may previously have thought their network security was water-tight, it's undoubtedly a good thing.

As a Crest-accredited and highly experienced penetration testing provider, CyberLab has some of the business's most technically accomplished and experienced engineers. To produce this report, we asked them to tell us about the most common vulnerabilities they uncover in their daily pen testing activities.

Read 12 Common Vulnerabilities Found During Penetration Testing to:

Help you make a business case for penetration testing.

Learn more about the sorts of vulnerabilities that you might unknowingly be allowing on your network.

Prepare your team for the sorts of results your penetration tester might uncover.

Part 1 of the report covers the most common administrative security vulnerabilities: weak passwords, unpatched systems, lack of network segmentation, weak authentication mechanisms, misconfigured services, lack of / broken access controls, social engineering and insufficient logging & monitoring.

Part 2 covers more in-depth technical vulnerabilities: cross-site scripting (XSS), SQL injection, lack of encryption and weak mobile device security.

Recap on the Importance of Penetration Testing

If your business handles data or customer details, collects financial information, develops commercially sensitive intellectual property or is simply aware of the risks posed by some of the less savoury elements on the internet – you'll want penetration testing.

Pen Testing is a type of security assessment desgined to replicate the actions taken by a malicious actor (hacker) but in an ethical manner. It may also be sometimes referred to as ethical hacking. Usually, part of the definition of pen testing offered by CREST (the security accreditation authority) says:

"Penetration testing looks to exploit known vulnerabilities but should also use the expertise of the tester to identify specific weaknesses - unknown vulnerabilities - in an organisation's security arrangements."

Below, we're going to reveal some of those 'specific weaknesses and unknown vulnerabilities' that our CREST-accredited security engineers have uncovered during their penetration testing work.

Common Vulnerabilities Found in Penetration Tests

ften, vulnerabilities uncovered by a Pen Test Engineer would require sophisticated hacking capabilities in order for a breach to take place. In some cases, user interaction may be required to succeed, whereas others may stay completely under the radar.

Nonetheless, many emanate from a network or system weakness of the sort that attackers specifically seek to exploit.

Other vulnerabilities such as weak passwords, default access credentials being left in place and out of date systems come about as a result of poor administrative practice, while others still are down to lax physical access issues which may allow those with malicious intent to steal sensitive data or devices right from under the noses of employees.

Let's look at the 12 most common vulnerabilities discovered by CyberLab penetration testing engineers in the course of their work.

Part 1: Common Administrative Vulnerability Findings

Weak Passwords

Weak passwords are one of the most common vulnerabilities found during a penetration test. An attacker can easily guess or crack a weak password using a brute force attack. This is especially true if the user is using a common word or phrase, a password that contains personal information or easily guessable patterns.

What's the danger?

One of the main dangers of weak passwords is that an attacker can access sensitive information, systems, and applications. Once an attacker has access, they can move laterally within the network and cause extensive damage. In addition, if the user is using the same password for multiple accounts, this can also lead to a domino effect where the attacker can access other systems and applications.

To address this issue, organisations should enforce password policies that require complex passwords and regular password changes. Businesses can also implement Multi-factor authentication (MFA) to provide an additional layer of security. It's also essential to educate users on the importance of strong passwords and the risks associated with password reuse. Regular training and awareness campaigns can help users understand the impact of their actions on the organisation's security.

Unpatched Systems

Unpatched systems are a serious risk to an organisation's security posture. With every patch that goes uninstalled, the system becomes increasingly vulnerable to known exploits and attacks. This is because security researchers often discover vulnerabilities and then make them public, making it easier for attackers to take advantage of them.

What's the danger?

One of the main dangers of weak passwords is that an attacker can access sensitive information, systems, and applications. Once an attacker has access, they can move laterally within the network and cause extensive damage. In addition, if the user is using the same password for multiple accounts, this can also lead to a domino effect where the attacker can access other systems and applications.

To address this issue, organisations should enforce password policies that require complex passwords and regular password changes. Businesses can also implement Multi-factor authentication (MFA) to provide an additional layer of security. It's also essential to educate users on the importance of strong passwords and the risks associated with password reuse. Regular training and awareness campaigns can help users understand the impact of their actions on the organisation's security.

There are many reasons why internal software systems may not be patched, including a fear of breaking the network.

Lack of Network Segmentation

Network segmentation is an essential security measure that separates different parts of the network to limit the spread of a potential breach. However, penetration testers often find that networks lack proper segmentation, enabling attackers to move laterally through the network once they have gained access.

What's the danger?

One of the biggest dangers associated with a lack of network segmentation is that it makes it easier for attackers to spread malware or conduct a successful attack. For example, suppose an attacker gains access to one system on an unsegmented network. In that case, they can use that access to move laterally through the network, potentially compromising additional systems and data.

To mitigate the risk of a potentially successful attack that exploits a lack of network segmentation, organisations should implement network segmentation strategies that limit the scope of an attack.

This can include segmenting the network into smaller, more manageable subnetworks, implementing firewalls and other security measures to control access between segments, as well as regularly reviewing and updating network access policies and processes to ensure the segmentation strategy remains effective.

Additionally, organisations should ensure that they have adequate security monitoring and incident response procedures in place to detect and respond to any potential breaches.

This can include monitoring network traffic, user activity, and system logs for signs of suspicious activity, as well as conducting regular vulnerability assessments and tests such as VLAN Hopping assessments to identify and address potential weaknesses and ensure that lateral movement between networks is not possible.

Weak Authentication Mechanisms

Weak authentication mechanisms are a significant vulnerability that can allow attackers to gain unauthorised access to systems, applications, and data. Common weaknesses include the use of plain text passwords, weak encryption protocols, and failure to enforce password complexity requirements.

What's the danger?

One of the biggest dangers of weak authentication mechanisms is that attackers can easily exploit them. For example, attackers may use brute-force techniques to guess weak passwords or intercept authentication credentials that are transmitted over an insecure network.

To address this vulnerability, organisations should implement robust authentication mechanisms that make it difficult for attackers to guess or steal credentials. This can include the use of multi-factor authentication, which requires users to provide multiple forms of identification, such as a password and a fingerprint or smart card.

Additionally, organisations should regularly review and update their authentication mechanisms to ensure they remain effective against emerging threats. This can include monitoring for new vulnerabilities in authentication protocols and updating software and hardware as needed.

By implementing strong authentication mechanisms, organisations can significantly reduce the risk of unauthorised access and protect their sensitive data and systems from attackers.

Misconfigured Services

Misconfigured services are a significant security risk that can leave organisations vulnerable to attacks. For example, penetration testers often find that services such as web servers, databases, and email servers are misconfigured, which can enable attackers to gain unauthorised access to sensitive data or execute malicious code.

What's the danger?

One of the biggest dangers associated with misconfigured services is that attackers can exploit them in various ways. For example, attackers may use misconfigured web servers to execute cross-site scripting (XSS) attacks or exploit misconfigured databases to extract sensitive information.

To address this vulnerability, organisations should ensure that all services are properly configured according to best practices and security standards. This can include implementing secure configurations for web servers, databases, and email servers and regularly reviewing and updating these configurations to ensure they remain effective against emerging threats.

Organisations should also implement ongoing monitoring and auditing of their services to identify any potential misconfigurations or vulnerabilities. This can include using automated tools to scan for misconfigurations or conducting regular manual reviews of service configurations.

By taking proactive steps to address misconfigured services, organisations can significantly reduce the risk of attacks and protect their sensitive data and systems from exploitation.

Lack of / Broken Access Controls

Lack of access controls is a severe security issue that can leave organisations vulnerable to unauthorised access and data breaches. Penetration testers often find that organisations do not have effective access control mechanisms or are the controls are not being properly utilised.

What's the danger?

The danger associated with this vulnerability is that unauthorised users can gain access to sensitive data and systems, potentially leading to data breaches, intellectual property theft, and other serious security incidents. Attackers can exploit this vulnerability in various ways, such as exploiting unsecured credentials, exploiting weak passwords, or bypassing authentication mechanisms altogether.

To address this vulnerability, organisations should implement access control policies and procedures that limit access to sensitive data and systems based on the principle of least privilege. This means granting users only the minimum level of access necessary to perform their job functions and nothing more.

Broken Access Controls refer to situations where access controls are in place, but they are not functioning as intended or can be bypassed. This can occur when developers or administrators do not fully understand the risks associated with certain types of access controls or do not implement them correctly. Attackers can exploit these vulnerabilities by finding ways to bypass the access controls, such as by using stolen credentials, exploiting flaws in the authentication process, or manipulating data to trick the system into granting access.

Organisations should also ensure that access controls are properly enforced and monitored. This can include using role-based access controls, implementing two-factor authentication, and regularly reviewing access logs and audit trails to identify suspicious activity.

By implementing adequate access controls and regularly checking that those controls are functioning properly, organisations can significantly reduce the risk of unauthorised access and protect their sensitive data and systems from exploitation. campaigns can help users understand the impact of their actions on the organisation's security.

Social Engineering

Social engineering attacks pose a serious threat to organisations, as they target the human element of security. Unlike other types of cyber attacks that exploit technical vulnerabilities, social engineering attacks rely on deception and manipulation to trick employees into divulging sensitive information or granting access to systems.

This vulnerability is compounded by the fact that many employees are not adequately trained to identify and avoid social engineering attacks, making them susceptible to these types of attacks.

What's the danger?

The danger of social engineering attacks is that they can be used to steal sensitive information, such as login credentials or financial data, from employees who may not even realise they are being manipulated.

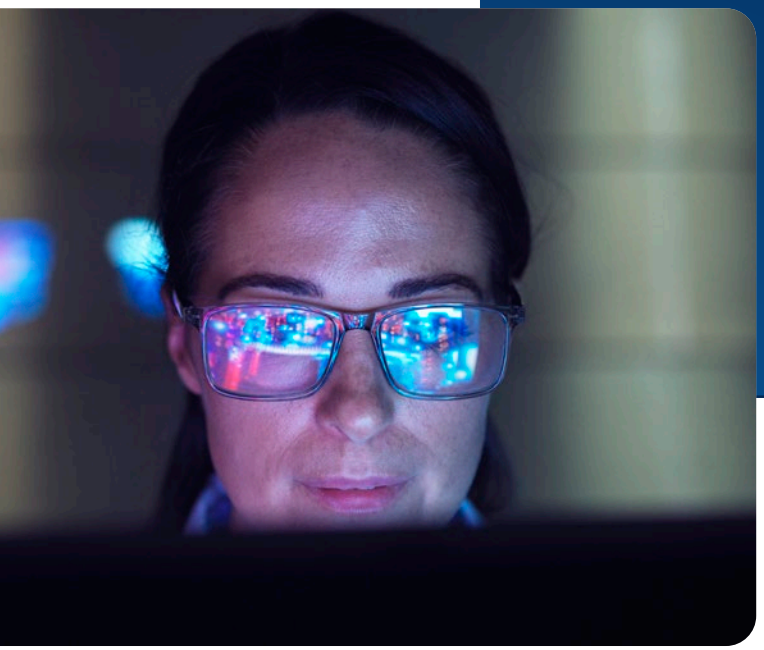
Attackers can use a variety of tactics, such as phishing emails, pretexting, or baiting, to gain access to systems and data. In some cases, attackers may even use social engineering techniques to gain physical access to a facility, allowing them to bypass security controls and steal sensitive information.

Social engineering attacks can have serious consequences for organisations, including financial losses, reputational damage, and legal or compliance issues.

For example, a successful social engineering attack could result in the theft of customer data, which could lead to costly fines or lawsuits. In addition, the impact of a social engineering attack on an organisation's reputation could be long-lasting, making it difficult to regain the trust of customers and partners.

To mitigate the risk of social engineering attacks, organisations should implement comprehensive security awareness training programs that educate employees about social engineering risks and best practices for identifying and avoiding these types of attacks. This training should include simulated phishing exercises to test employees' awareness and reinforce the importance of following security protocols.

By taking proactive steps to address misconfigured services, organisations can significantly reduce the risk of attacks and protect their sensitive data and systems from exploitation.



Insufficient Logging & Monitoring

Insufficient logging and monitoring is a security vulnerability that poses a significant risk to organisations. Logging and monitoring are crucial for identifying and responding to security incidents in a timely manner.

Without proper logging and monitoring, organisations may be unaware of potential security breaches and their impact, allowing attackers to maintain access to systems and data undetected. This can result in the loss of valuable information, damage to an organisation's reputation, and significant financial losses.

What's the danger?

One of the primary dangers of insufficient logging and monitoring is that it can lead to a delayed response to security incidents. If an organisation is not aware that a breach has occurred, they cannot respond promptly to contain the damage and prevent further access by attackers.

Furthermore, organisations that fail to adequately monitor their systems and data may struggle to identify the scope and severity of a security incident, making it more difficult to respond effectively.

To mitigate this risk, organisations should implement logging and monitoring systems that capture a broad range of security events, including failed login attempts, unusual user behaviour, and unauthorised access attempts.

These systems should be configured to alert security personnel in real-time when potential security incidents are detected, allowing them to respond promptly and minimise the impact of a breach.

Additionally, organisations should establish formal incident response procedures that outline the steps to be taken in the event of a security incident. These procedures should be regularly reviewed and updated to reflect changes in the threat landscape and the organisation's IT infrastructure.

Part 2: Common Technical Vulnerability Findings

Cross-Site Scripting (XSS)

Cross-site scripting (XSS) vulnerabilities can pose a significant threat to web applications and their users. These vulnerabilities occur when an application fails to validate user input or encode output properly, allowing attackers to inject malicious scripts into the application. Once injected, these scripts can be executed by unsuspecting users, leading to a range of potentially damaging consequences.

What's the danger?

The danger of XSS attacks is that they can be used to steal sensitive information, such as login credentials or financial data, from unsuspecting users. Attackers can also use XSS attacks to deface websites, distribute malware, or launch phishing attacks. In addition to causing harm to users and the application, successful XSS attacks can also harm an organisation's reputation and lead to costly legal or compliance issues.

To prevent XSS attacks, organisations should implement robust security measures, such as input validation and output encoding. Input validation ensures that user input is in the correct format and does not contain any malicious code, while output encoding ensures that any user input displayed on a web page is encoded correctly to prevent malicious code from being executed.

Another approach to preventing XSS attacks is to use content security policies (CSPs). CSPs allow organisations to specify which domains are allowed to execute scripts on their web pages, reducing the risk of unauthorised script execution. Additionally, organisations should keep their web applications up to date and perform regular security testing to identify and address any XSS vulnerabilities.

SQL Injection

SQL injection is one of the most common and dangerous vulnerabilities found in web applications. Attackers can use SQL injection to gain access to sensitive information, modify data, or even take control of the entire database server. This vulnerability occurs when user input is not properly sanitised and validated before being used in SQL queries. As a result, attackers can inject malicious SQL code into the application, allowing them to execute arbitrary commands on the database server.

What's the danger?

The danger of SQL injection lies in the fact that it can be challenging to detect and have significant consequences. Attackers can use SQL injection to steal sensitive data, such as usernames, passwords, and credit card numbers. They can also modify or delete data, causing data loss or system downtime. In severe cases, attackers can even take control of the entire database server, giving them unrestricted access to all data and resources on the server.

Organisations should implement security measures such as input validation and prepared statements to prevent SQL injection. Input validation involves checking user input for malicious characters and limiting the type and length of input allowed. Prepared statements involve parameterised queries, which separate user input from SQL code, preventing attackers from injecting malicious SQL code. Regular security assessments and application penetration testing can also help identify and address SQL injection vulnerabilities.

campaigns can help users understand the impact of their actions on the organisation's security.

Lack of Encryption

Encryption is an essential security measure that protects sensitive data from unauthorised access. Penetration testers often find that data is transmitted or stored without proper encryption, making it vulnerable to interception.

Sensitive data transmitted in plaintext, such as passwords or credit card information, can be intercepted by attackers who have gained access to the network or are monitoring network traffic. Sensitive data stored without proper encryption, such as personal information or financial data, can be accessed by attackers who gain unauthorised access to the storage location.

What's the danger?

Without proper encryption, sensitive data is at risk of interception and unauthorised access. Attackers who have gained access to the network or are monitoring network traffic can intercept sensitive data transmitted in plaintext, such as passwords or credit card information. Sensitive data stored without proper encryption, such as personal information or financial data, can be accessed by attackers who gain unauthorised access to the storage location.

To mitigate this risk, organisations should implement encryption for all sensitive data in transit and at rest. Encryption protocols such as SSL/TLS can be used for data in transit, while encryption algorithms such as AES or RSA can be used for data at rest. Properly managing encryption keys through policies and procedures is also crucial to ensuring that sensitive data remains protected.

This can include monitoring network traffic, user activity, and system logs for signs of suspicious activity, as well as conducting regular vulnerability assessments and tests such as VLAN Hopping assessments to identify and address potential weaknesses and ensure that lateral movement between networks is not possible.

Weak Mobile Device Security

Mobile devices have become an essential part of modern business operations, allowing employees to work from anywhere at any time. However, with the rise of mobile device usage, there has been a corresponding increase in mobile security risks. Penetration testers often find that organisations lack proper security controls for mobile devices, which can leave them vulnerable to attacks.

What's the danger?

Mobile devices are often unsecured, with weak passwords, outdated software, and unsecured Wi-Fi connections, making them vulnerable to cyber attacks. Attackers can exploit these weaknesses to gain unauthorised access to sensitive data, such as passwords, credit card information, and other confidential information.

Organisations should implement security policies and controls for mobile devices to mitigate the risk of mobile device security. One critical control is device encryption, which ensures that all data on the device is protected when it is lost or stolen. Mobile device management (MDM) solutions are also essential, as they allow organisations to manage and secure mobile devices remotely, enforcing security policies and monitoring for potential security threats.

Strong authentication mechanisms are another critical control for mobile devices. Organisations should require multi-factor authentication for all mobile devices, which requires users to provide two or more pieces of evidence to authenticate their identity. This can include a password or PIN, biometrics such as a fingerprint or facial recognition scan, and a security token or smart card.

Finally, it's vital to ensure that all mobile applications are secure and do not pose a risk to sensitive data. Organisations should conduct thorough security assessments of all mobile applications, including third-party apps, to identify and mitigate potential vulnerabilities. Additionally, all mobile applications should be tested regularly to ensure they remain secure and compliant with industry standards and best practices.

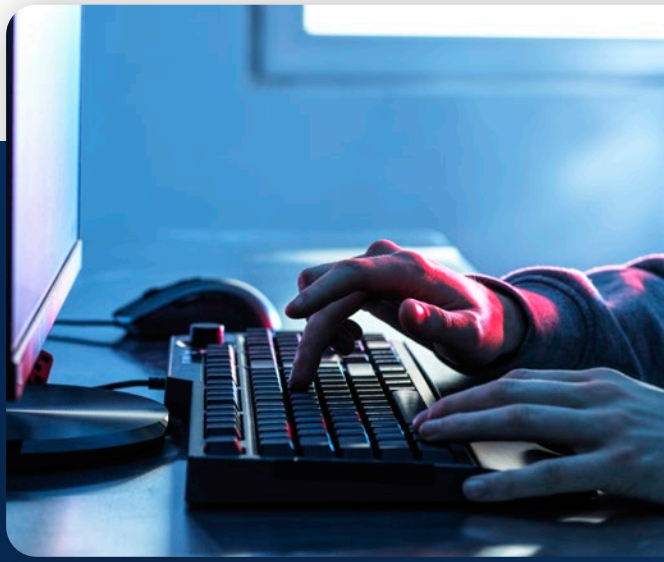
Conclusion

While the vulnerabilities we've covered in this eBook are just a sample of the many risks that modern businesses face, they're all too real and all too dangerous. The consequences of a successful attack can be devastating, from lost data and stolen funds to reputational damage and legal liabilities.

To truly protect your business, you need to be proactive about identifying and mitigating vulnerabilities before they can be exploited. That's where regular penetration testing comes in. By simulating real-world attacks and identifying weaknesses in your security infrastructure, penetration testing can help you to keep up with the ever-evolving threat landscape and minimise your risk of a breach.

At CyberLab, we have over 25 years of experience helping businesses of all sizes and industries improve their security posture through penetration testing and other cybersecurity services. We're committed to staying up to date on the latest threats and technologies, so you can focus on running your business with confidence.

So, if you're serious about protecting your business from cyber threats, don't hesitate to reach out to us. We'd be happy to answer any questions you have about penetration testing and help you develop a customised plan to keep your organisation safe and secure.



cyberlab

Find out more at **cyberlab.co.uk**

Our People. Our Platform. Protects You.

CyberLab is a specialist cyber security company that provides a wide range of security solutions and services.

Your one-stop cyber security advisor, the CyberLab team is equipped with the right technology, knowledge, and expertise to help businesses of all sizes, including large public sector organisations.

By leveraging world-class technology, decades of experience, and our vendor partnerships, we have helped to secure thousands of organisations across the UK.

Our unique Detect, Protect, Support approach makes us the perfect partner to review and reenforce your cyber security defences.

Speak With an Expert

hello@cyberlab.co.uk | cyberlab.co.uk

Awards and Accreditations

CREST

VA | PEN TEST

IASME CONSORTIUM

Assured Service Provider
in association with National Cyber Security Centre
CHECK Penetration Testing

CYBER ESSENTIALS CERTIFIED

CYBER ESSENTIALS CERTIFIED PLUS

cyberlab

cyberlab.co.uk