Solutions for vulnerabilities found in the test website:

Vulnerabilities found:

- ICMP Timestamp Request Remote Date Disclosure
- Common Platform Enumeration (CPE)
- Device Type
- Host Fully Qualified Domain Name (FQDN) Resolution
- Nessus SYN scanner
- Nessus Scan Information
- OS Identification
- Service Detection (HELP Request)
- TCP/IP Timestamps Supported
- Traceroute Information

Possible Solutions:

Solutions for ICMP Timestamp Request Remote Date Disclosure

- Block incoming and outgoing ICMP timestamp requests and replies. This is the most effective way to mitigate the vulnerability and can be done using a firewall.
- Use a different time synchronization protocol. Instead of relying on ICMP timestamps, use a more secure protocol such as NTP.
- Keep your operating system and network devices up to date. Software updates often include security patches that can help to mitigate vulnerabilities.

Solutions for Common Platform Enumeration (CPE)

- Restrict access to CPE information. Only allow authorized users to access CPE information. This can be done by configuring your network firewall or by using a web application firewall (WAF).
- Use a honeypot to detect and deceive attackers. A honeypot is a fake system that is designed to attract and trap attackers. By deploying a honeypot, you can collect information about the attacker's methods and targets.

Solutions for Host Fully Qualified Domain Name (FQDN) Resolution

- Use a DNS cache server. A DNS cache server can store frequently accessed DNS records, which can improve performance and security.
- Use a DNS firewall. A DNS firewall can filter out malicious DNS requests, which can help to protect your network from attacks.
- Use DNSSEC. DNSSEC is a security extension to the DNS protocol that can help to authenticate and verify DNS records.

Solutions for Nessus SYN scanner

- Use a firewall to block unauthorized access to the Nessus scanner.
- Use a Nessus policy to restrict the scope of the scanner.
- Use a Nessus credential management system to manage access to credentials.

Solutions for Nessus Scan Information

- Store Nessus scan results in a secure location.
- Only allow authorized users to access Nessus scan results.
- Encrypt Nessus scan results.

Solutions for OS Identification

- Use a firewall to block unauthorized OS fingerprinting requests.
- Use a security information and event management (SIEM) system to monitor for OS fingerprinting attempts.
- Keep your operating system and network devices up to date. Software updates often include security patches that can help to mitigate vulnerabilities.

Solutions for Service Detection (HELP Request)

- Block incoming HELP requests. This can be done using a firewall.
- Restrict access to the services that are advertised by HELP requests. Only allow authorized users to access these services.
- Use a security information and event management (SIEM) system to monitor for HELP requests.

Solutions for TCP/IP Timestamps Supported

- Disable TCP/IP timestamps on systems that do not need them.

- Use a firewall to block incoming and outgoing TCP/IP timestamp requests.
- Keep your operating system and network devices up to date. Software updates often include security patches that can help to mitigate vulnerabilities.

Solutions for Traceroute Information

- Block incoming traceroute requests. This can be done using a firewall.
- Restrict access to the network devices that are exposed to traceroute requests. Only allow authorized users to access these devices.
- Use a security information and event management (SIEM) system to monitor for traceroute requests.