

Forum:[Hack Forums](#)

Thread: [FIND WEBSITES WITH WEAK CIPHERS \(Vulnerable\)](#)

Bingo121 - February 2, 2024, 10:28 pm

I have been looking ways to find websites with weak Ciphers like outdated TLS and RC4 algos, I tried by google dorks , shodan , sslabs etc.. But are there any inclusive and specific methods which might be really helpful that I might be missing out. Thanks for your time.

Nemo5 - February 27, 2024, 6:26 am

You can employ automated scanning tools such as Nessus, Qualys SSL Labs, or OpenVAS to perform comprehensive vulnerability assessments on websites. These tools can detect outdated encryption protocols and weak cipher suites automatically.

You can also erform manual testing using tools like OpenSSL or Nmap to check for supported cipher suites and TLS versions on target websites.

You can also examine SSL/TLS certificates associated with websites to determine the supported encryption algorithms and TLS versions.

You can also explore public databases and repositories of vulnerable websites or historical data on SSL/TLS configurations. Websites like Censys or Internet-wide scan projects may provide valuable insights into the prevalence of weak ciphers and outdated TLS versions.

You can also engage with the cybersecurity community through mailing lists or online platforms to exchange knowledge and insights regarding identifying websites with weak encryption.

Euaggelistes - February 27, 2024, 6:30 am

(Feb 27, 2024 07:26 AM)Nemo5 Wrote: [\[CITE\]](#) You can employ automated scanning tools such as Nessus, Qualys SSL Labs, or OpenVAS to perform comprehensive vulnerability assessments on websites. These tools can detect outdated encryption protocols and weak cipher suites automatically.

You can also erform manual testing using tools like OpenSSL or Nmap to check for supported cipher suites and TLS versions on target websites.

You can also examine SSL/TLS certificates associated with websites to determine the supported encryption algorithms and TLS versions.

You can also explore public databases and repositories of vulnerable websites or historical data on SSL/TLS configurations. Websites like Censys or Internet-wide scan projects may provide valuable insights into the prevalence of weak ciphers and outdated TLS versions.

You can also engage with the cybersecurity community through mailing lists or online platforms to exchange knowledge and insights regarding identifying websites with weak encryption.

^^^ Very nice suggestions.

dopedoxy - March 7, 2024, 10:32 am

(Feb 27, 2024 07:26 AM)Nemo5 Wrote: [\[CITE\]](#) You can employ automated scanning tools such as Nessus, Qualys SSL Labs, or OpenVAS to perform comprehensive vulnerability assessments on

websites. These tools can detect outdated encryption protocols and weak cipher suites automatically.

You can also perform manual testing using tools like OpenSSL or Nmap to check for supported cipher suites and TLS versions on target websites.

You can also examine SSL/TLS certificates associated with websites to determine the supported encryption algorithms and TLS versions.

You can also explore public databases and repositories of vulnerable websites or historical data on SSL/TLS configurations. Websites like Censys or Internet-wide scan projects may provide valuable insights into the prevalence of weak ciphers and outdated TLS versions.

You can also engage with the cybersecurity community through mailing lists or online platforms to exchange knowledge and insights regarding identifying websites with weak encryption.

?