

Forum:[Hack Forums](#)

Thread: [How to exploit a website vulnerability hash disclosure - mac osx salted sha-1?](#)

Arass - September 9, 2023, 12:10 am

Hello, I'm studying to become an information security specialist, I was given the task to crack our the site. I checked the site for vulnerability using Owasp ZAP, Nmap and :

Owasp Zap:

Alerts

Name , Risk Level, Number of Instances

Hash Disclosure - Mac OSX salted SHA-1, High, 2
Absence of Anti-CSRF Tokens, Medium, 104
Content Security Policy (CSP) Header Not Set, Medium, 102
Cookie Without Secure Flag, Low, 3
Cookie without SameSite Attribute, Low, 6
Cross-Domain JavaScript Source File Inclusion, Low, 7
Strict-Transport-Security Header Not Set, Low, 102
Content-Type Header Missing, Informational, 2
Information Disclosure - Sensitive Information in URL ,Informational, 102
Re-examine Cache-control Directives, Informational, 1
Retrieved from Cache, Informational, 102
User Controllable HTML Element Attribute (Potential XSS), Informational, 1

Nmap:

Port, State (toggle closed [0] | filtered [0]), Service, Reason

22	tcp	open	ssh	syn-ack
80	tcp	open	http	syn-ack
443	tcp	open	https	syn-ack
5223	tcp	open	hqvirtgrp	syn-ack
8070	tcp	open	ucs-isc	syn-ack
8893	tcp	open	ddi-tcp-6	syn-ack
8894	tcp	open	ddi-tcp-7	syn-ack

How can I exploit these vulnerabilities? Please help me! Thank you in advance!!

DramaKing - September 9, 2023, 4:55 am

Social engineering and CSRF or XSS, DNS spoofing, HTTPS downgrade attack, and packet sniffing. A vulnerability scanner like OpenVAS will detect any known vulnerabilities in the server, not just the HTML.

As for the Hash Disclosure, it's probably a false positive. There should have been a URL given.