Smart Internz

PROJECT NAME- MALWARE DETECTION AND CLASSIFICATION

PENTESTING OF MAIN WEBSITE - myntra.com

1)

Vulnerability Name - Anticlickjacking

CWE - CWE-355

OWASP Category - A09:2021 - Security Logging and Monitoring Failures/phishing attack

Description - Clickjacking, also known as a phishing attack is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they intend to click on the top-level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to another page, most likely owned by another application, domain, or both.

Business Impact - An attacker may also redirect the clicks to download malware or gain access to vital systems as a starting point for an advanced persistent threat (APT). This spells trouble for organizations that protect sensitive data and intellectual property.

Vulnerability Path:https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

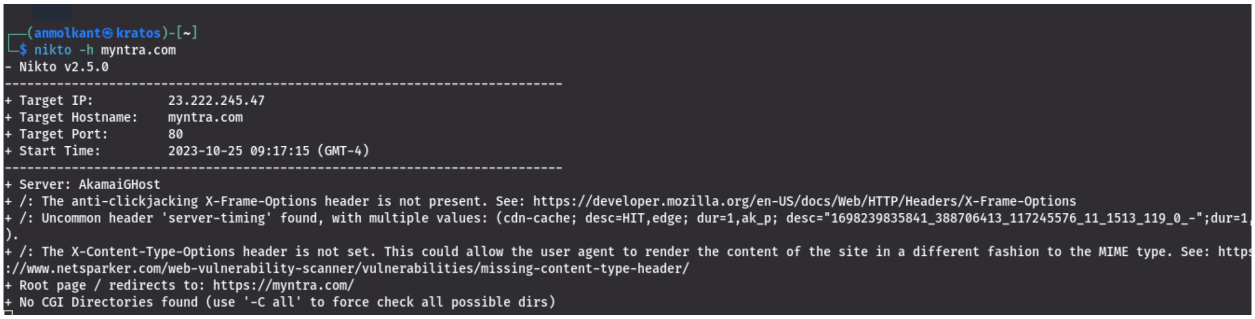
Steps To Reproduce:

1) **First, we need to open a tool called nikto which is used for vulnerability scanners and we use this tool for scan.**

2) **Then we write a command to scan the web application.**

3) **We basically type a command that is nikto -h myntra.com**

4) **After that, we see some vulnerabilities which useful for us to hack the web application.**



```
┌──(anmolkant㉿kratos)-[~]
└─$ nikto -h myntra.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          23.222.245.47
+ Target Hostname:    myntra.com
+ Target Port:        80
+ Start Time:         2023-10-25 09:17:15 (GMT-4)
---------------------------------------------------------------------------
+ Server: AkamaiGHost
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'server-timing' found, with multiple values: (cdn-cache; desc=HIT,edge; dur=1,ak_p; desc="1698239835841_388706413_117245576_11_1513_119_0_-";dur=1,
).
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https
://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: https://myntra.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

2)

Vulnerability Name - No proper handling of user agents
(HTTP user agent. nse)

CWE: CWE- 209

OWASP Category: A04:2021 - Insecure Design

Description: Insecure design is a broad category representing different weaknesses, expressed as “missing or ineffective control design.” Insecure design is not the source for all other Top 10 risk categories. There is a difference between insecure design and insecure implementation. We differentiate between design flaws and implementation defects for a reason, they have different root causes and remediation.

Business Impact: Insecure design can be how you position servers in your network, the order of trust you put on your systems, the protections you include for other vulnerabilities (including using outdated practices, such as saving passwords in plaintext and more.

Vulnerability Path:https://nmap.org/book/nse.html

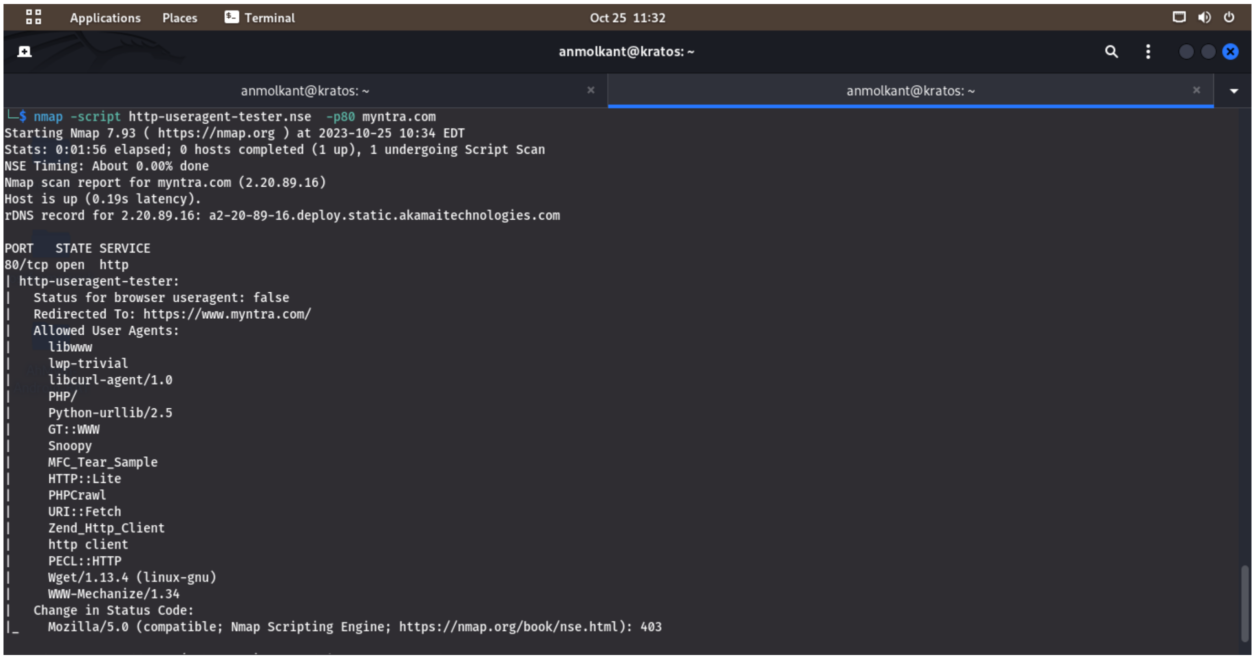
Steps to Reproduce:

1) **We use the Nmap tool to exploit a vulnerability.**

2) **Then we write a command that is nmap -script discovery myntra.com.**

3) **This command leads us to all the scripts of the HTTP service and in that script, we found a user agent vulnerability on this target.**

4) **We found many user-agents displayed along with their path and we can say that this kind of vulnerability comes under insecure design.**



```
└─$ nmap -script http-useragent-tester.nse  -p80 myntra.com
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-25 10:34 EDT
Stats: 0:01:56 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done
Nmap scan report for myntra.com (2.20.89.16)
Host is up (0.19s latency).
rDNS record for 2.20.89.16: a2-20-89-16.deploy.static.akamaitechnologies.com

PORT   STATE SERVICE
80/tcp open  http
| http-useragent-tester:
|   Status for browser useragent: false
|   Redirected To: https://www.myntra.com/
|   Allowed User Agents:
|     libwww
|     lwp-trivial
|     libcurl-agent/1.0
|     PHP/
|     Python-urllib/2.5
|     GT::WWW
|     Snoopy
|     MFC_Tear_Sample
|     HTTP::Lite
|     PHPCrawl
|     URI::Fetch
|     Zend_Http_Client
|     http client
|     PECL::HTTP
|     Wget/1.13.4 (linux-gnu)
|     WWW-Mechanize/1.34
|   Change in Status Code:
|_    Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html): 403
```