Twitter Thread by Harsh Bothra



Harsh Bothra
@harshbothra_



#Learn365 Day-6: Cross-Site Leaks

Goldmine to Learn: https://t.co/TsqGRWxPq7

Cross-Site Leaks/XS-Leaks is a less explored security issue that usually comes from Side-Channel Attacks. I found this an interesting vector but unusual.

(1/n)

#BugBountyTips #infosec #AppSec

(2/n)
This basically utilizes the web's core principle of composability in order to determine & extract useful information.

XS-Leaks take advantage of small pieces of information that are exposed during interactions between websites.

(3/n)
Cross-Site Oracle.

This can be considered as a querying mechanism. The information used for this attack is of binary form and called Oracles. It usually has an answer of "Yes" or "No". You can say True or False.

(4/n)
For Example: Does User Harsh Exists in the Application. Yes, means that the user is there in the application.
- An attacker requires to smartly form queries in order to successfully execute this attack and gain hold of sensitive information.

(5/n)
Some of the Attacks using Cross-Site leaks are:

1. XS-Search: An attacker try to abuse the query mechanism such as search functionality to leak and get hold of the user's

information.

Remediation
- Same Site Lax Cookies

(6/n)
Usual Exploitation Workflow:

1. Define a timeline when there is a Hit vs Miss
2. Start attacking the Querying Endpoint.
3. For Example: ?search=h (Throws a Hit)
search for the next word appended to `h` i.e. ?search=ha otherwise change the word i.e. ?search=b

(7/n)
2. Error Events

Based on the Error Message returned by the application, it may be possible to enumerate sensitive information. This is similar to user enumeration techniques.

Reference: https://t.co/2iIVT0xei2

(8/n)
3. Frame Counting
The window.length provides the number of frames in the window. This attribute can provide valuable information about a page to an attacker.

References: https://t.co/XjOZL3yiZF

(9/n)
3. Navigation Attacks
Reference: https://t.co/lS3LT80Foa

4. Cache Probing
- Workes based on detecting whether the web page was cached or not.
Ref: https://t.co/ejAdOHaIFG

5. ID Attribute
Ref: https://t.co/11lwLzE2DD

(10/n)

6. Post Message Broadcasts
a. Sharing Sensitive message with untrusted origins
b. Leaking information based on varying content or on the presence of a broadcast

7. Abusing Browser Features
- CORB (Cross-Origin Read Blocking)

- CORP (Cross-Origin Resource Policy)

(n/n)

8. Timing Attacks
- Clock Based
- Network Timing
- Execution Timing
- Hybrid Timing
- Connection Pool

Referneces
1. https://t.co/byryqh3bql
2. https://t.co/khunvHYDga
3. https://t.co/ssQ39okO55

I'll revisit this attack in near future & will try to find.