THESIS

DEFACEMENT ATTACK

LECTURER: NGUYEN DUC THAI

GROUP: 3
CLASS: CC01

OVERVIEW

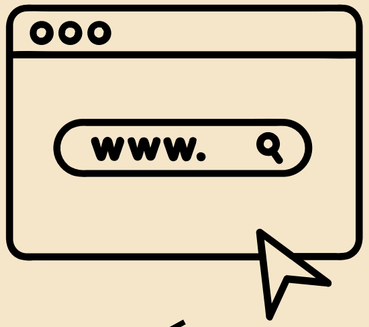
- INTRODUCTION
- PROBLEM
- RECOMMENDATIONS
- IMPLEMENTATION
- RESULTS
- CONCLUSION

INTRODUCTION

Attackers

Malicious code

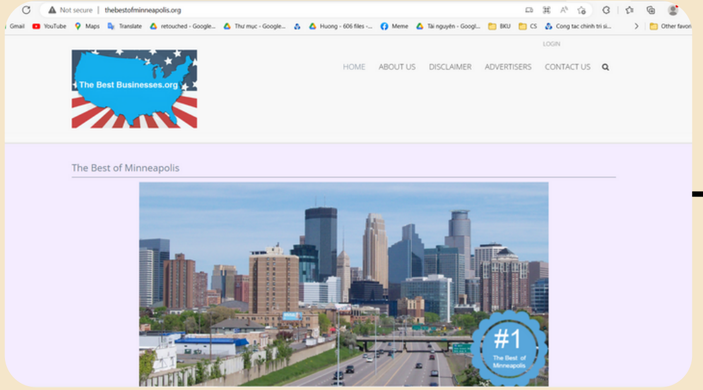
Legitimate webpage

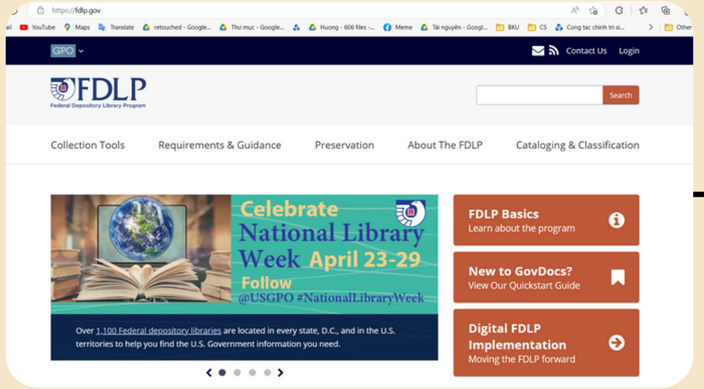


Defaced webpage

UNAUTHORIZED modification of web pages

INTRODUCTION



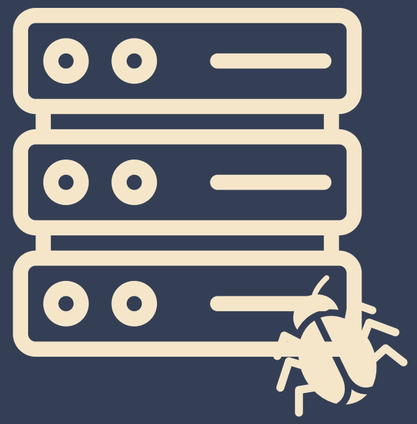


CONSEQUENCES

Availability

Reputation

WHY?



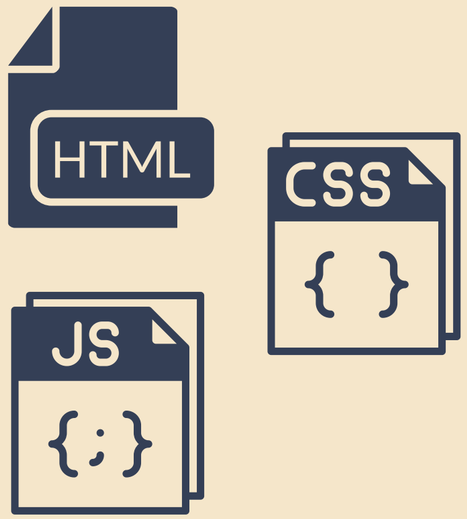
Weak server

Weak Adminisitration

No system update

Static Website

Client Side

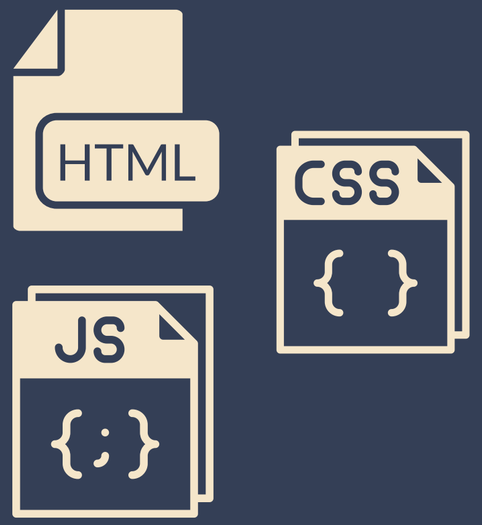


- ***No interactive sessions***
- Clients can't reach database

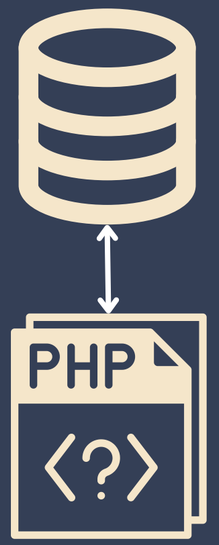
--> ***Less vulnerable***

Dynamic Website

Client Side



Server Side



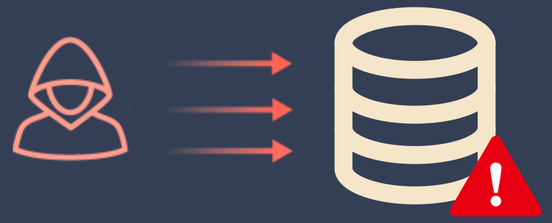
- ***Service request*** or ***query*** to **DATABASE**
- Can't know if user is attacker or normal

--> ***More vulnerable***

PROBLEM

DEFACEMENT ATTACKS TECHNIQUES

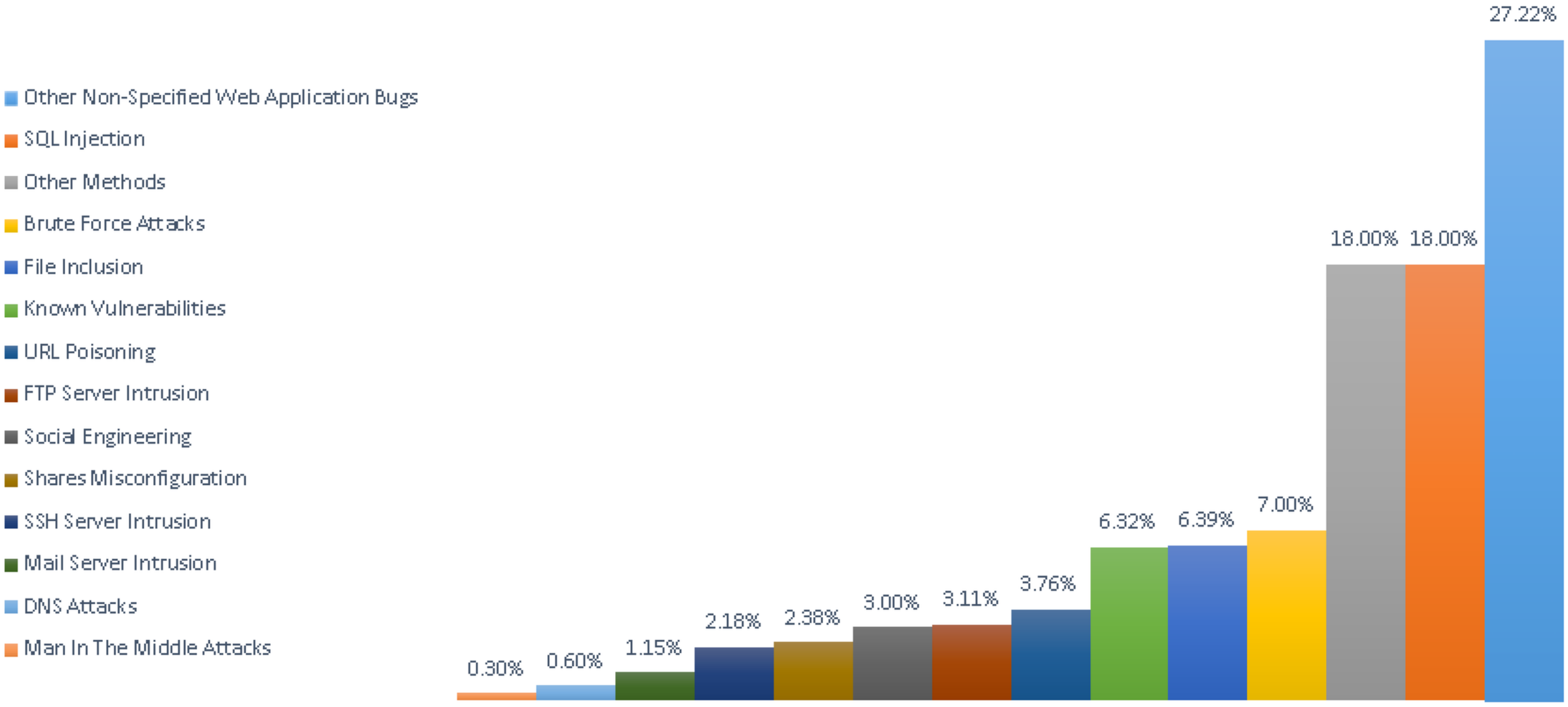
SQL Injection



Brute-force attack

File Inclusion

Cross-site scripting (XSS)


Other Non-Specified Web Application Bugs
SQL Injection
Other Methods
Brute Force Attacks
File Inclusion
Known Vulnerabilities
URL Poisoning
FTP Server Intrusion
Social Engineering
Shares Misconfiguration
SSH Server Intrusion
Mail Server Intrusion
DNS Attacks
Man In The Middle Attacks
0.30%
0.60%
1.15%
2.18%
2.38%
3.00%
3.11%
3.76%
6.32%
6.39%
7.00%
18.00%
18.00%
27.22%

DEFACEMENT DETECTION

ANOMALY-BASED DETECTION

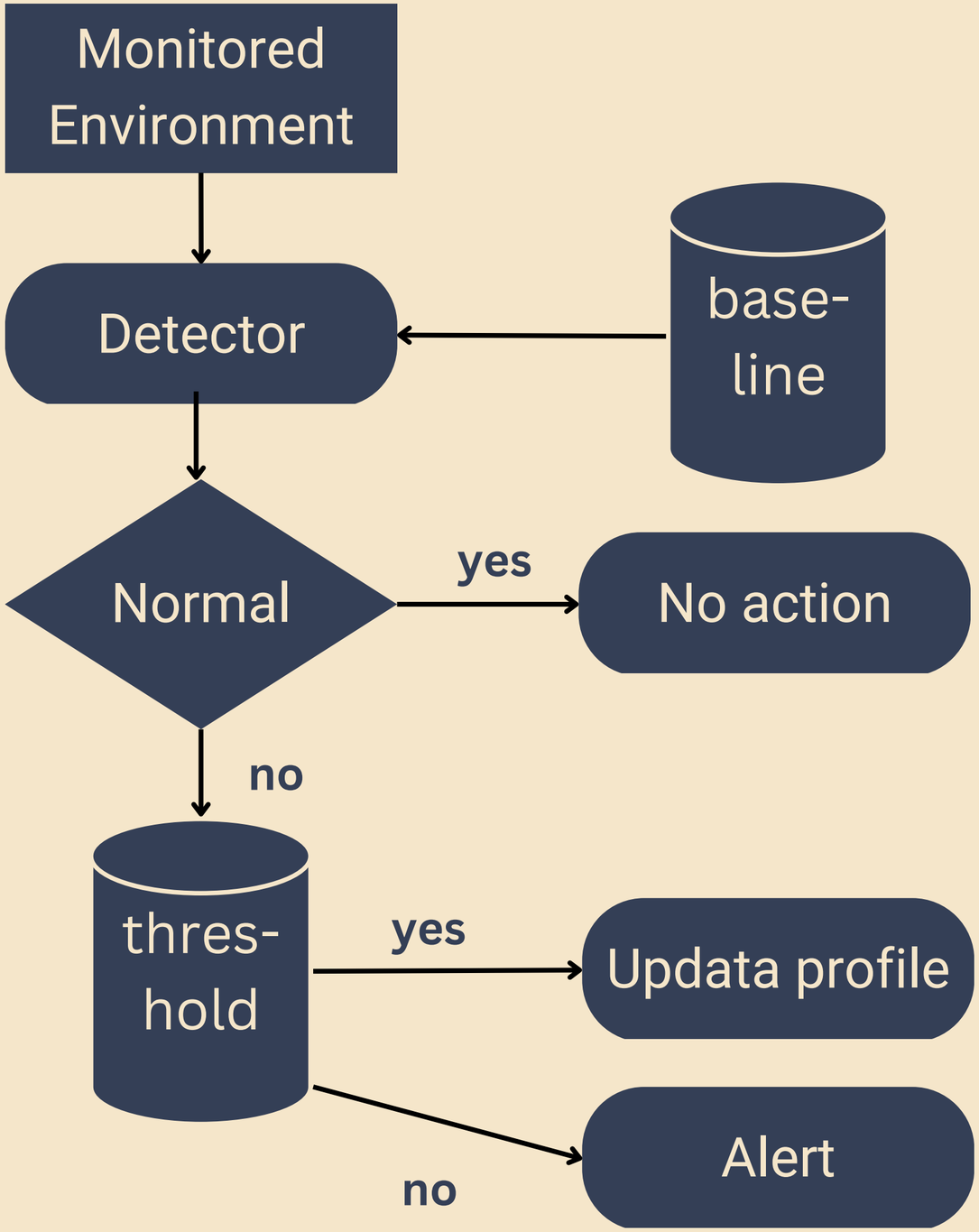
Anomaly-based detection detects changes in behavior

SIGNATURE-BASED DETECTION

Signature-based detection detects learnt patterns

MACHINE-LEARNING TECHNIQUES

Advanced anomaly-based techniques



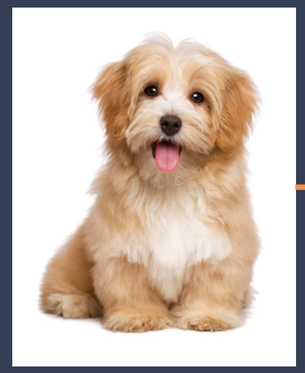
ANOMALY-BASED DETECTION

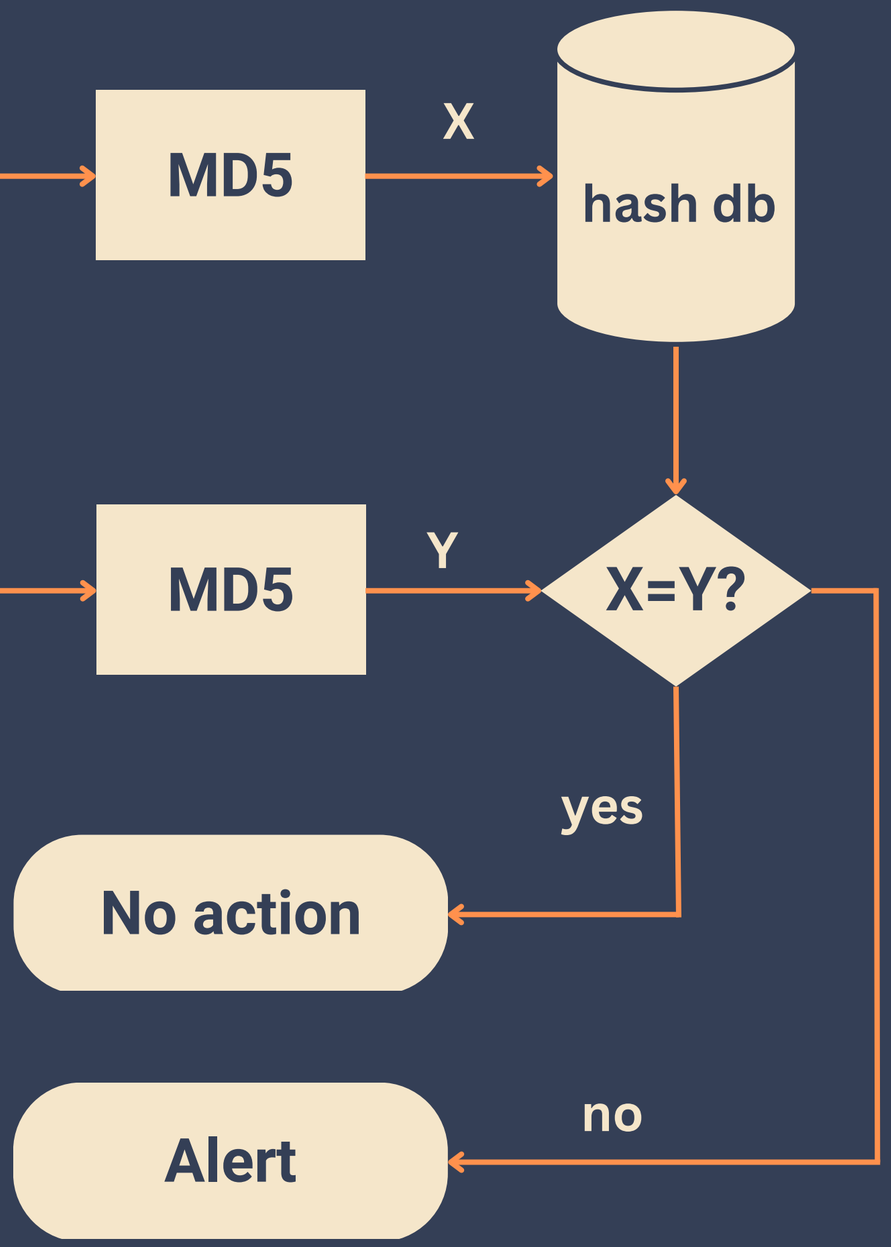
- Training the system with a baseline
- Comparing the current content with the baseline
- Triggering the alert

EXAMPLE: CHECKSUM COMPARISION

- Retrieve stored hash value
- Calculating the current hash value
- Comparing and alerting

Preserving ***INTEGRITY***





EXAMPLE: CHECKSUM COMPARISION

- Retrieve stored hash value
- Calculating the current hash value
- Comparing and alerting

Preserving ***INTEGRITY***

Advantages:

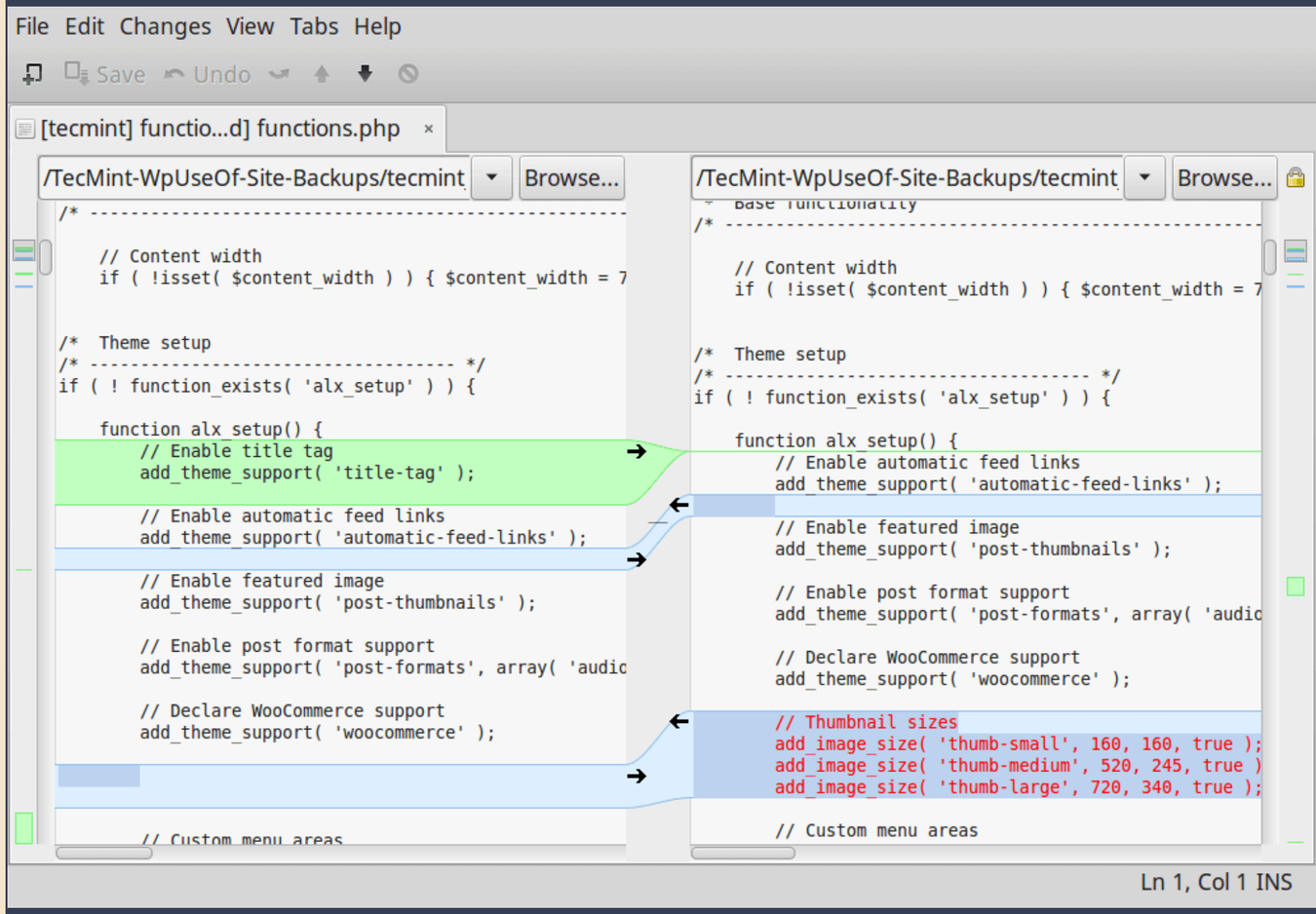
- Simple to implement
- Quick response
- Work well for static website

Disadvantages:

- False alarm
- Difficult to implement for dynamic website

EXAMPLE: DIFF COMPARISION

- Search the differences between two web pages
- Based on the ***content*** of the website, not the HTML code
- Determine a threshold to discard defacement



EXAMPLE:
DIFF COMPARISION

Advantages:

- Suitable for dynamic webpage if the threshold is determined
- Work well with static website

Disadvantages:

- False alarm
- Difficult to determine the threshold

- Generating a DOM tree from HTML code
- Comparing the structure of the HTML code based on the DOM tree
- Triggering the alarm

EXAMPLE: DOM ANALYSIS

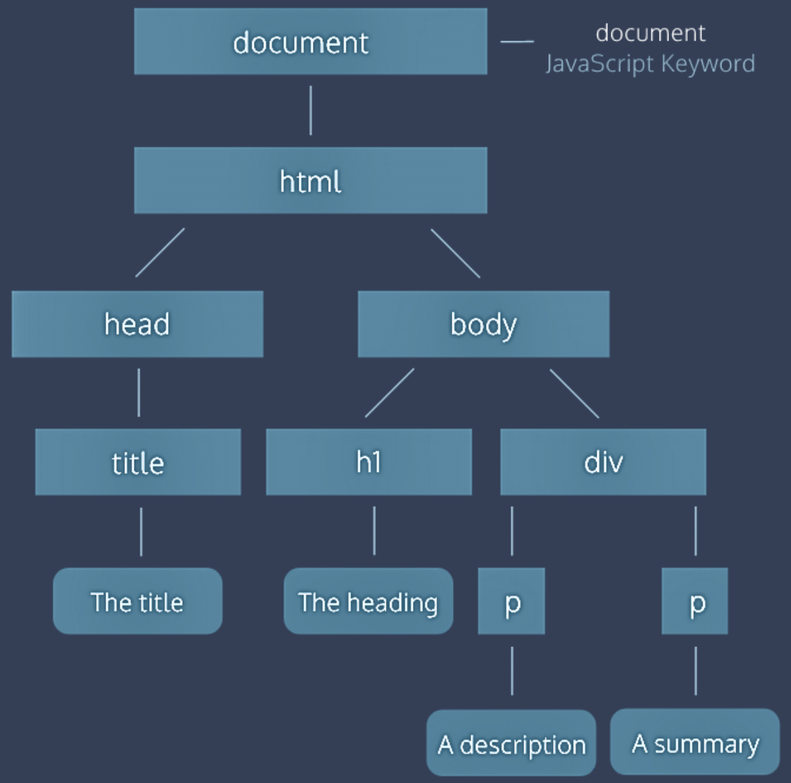
HTML File

```
<html>
    <head>
      <title>The title</title>
    </head>

    <body>
      <h1>The heading</h1>
      <div>
          <p>A description</p>
          <p>A summary</p>
      </div>
    </body>
</html>
```

DOM

Document Object Model



Advantages:

- Simple to implement
- No need to determine the threshold

Disadvantages:

- Can only find differences HTML files' structure

EXAMPLE: DOM ANALYSIS

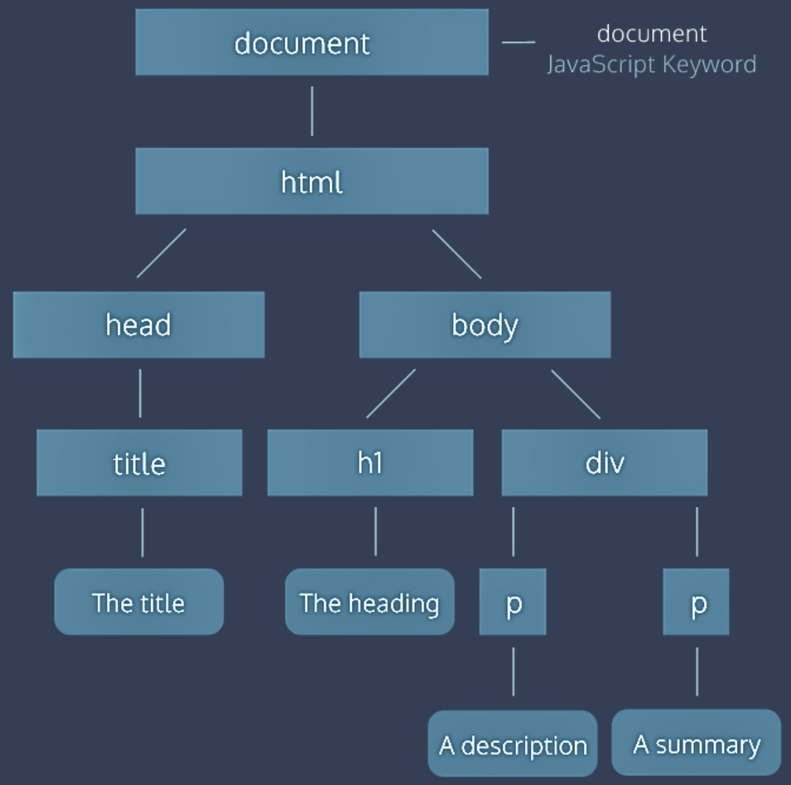
HTML File

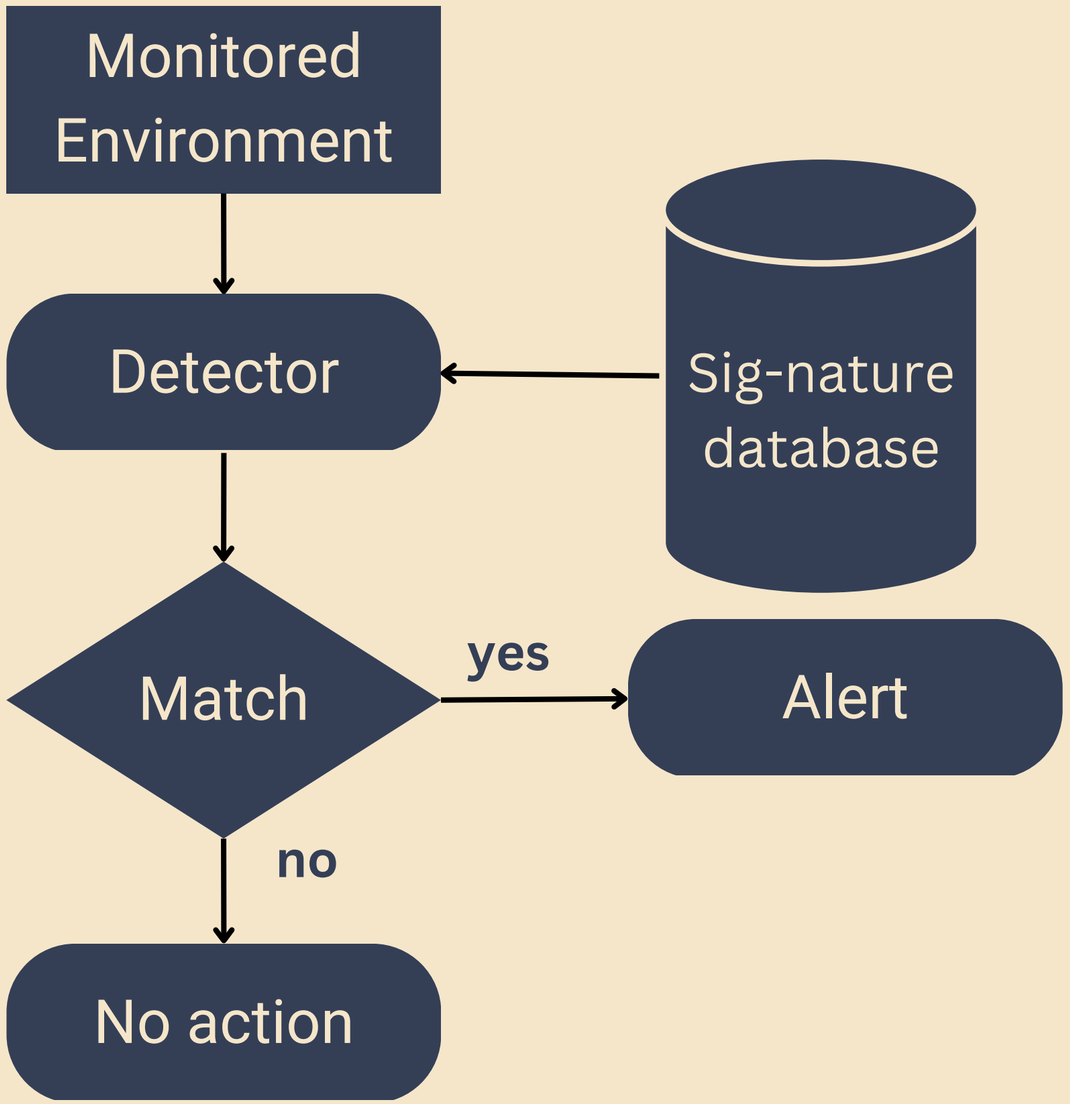
```
<html>
    <head>
      <title>The title</title>
    </head>

    <body>
      <h1>The heading</h1>
      <div>
          <p>A description</p>
          <p>A summary</p>
      </div>
    </body>
</html>
```

DOM

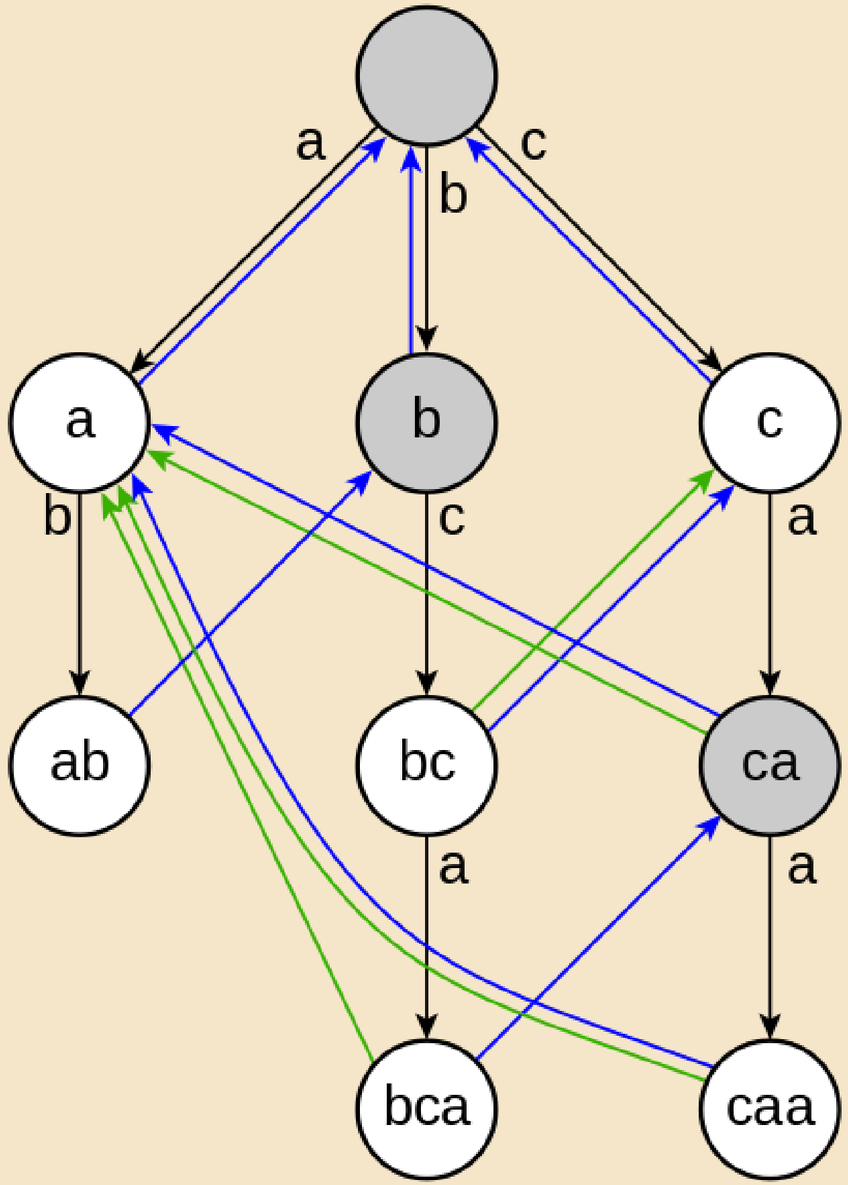
Document Object Model





SIGNATURE-BASED DETECTION

- Works on pattern
- Can only detect known attack
- Fast and efficient for well-known attacks only
- Cannot detect new kinds of threat

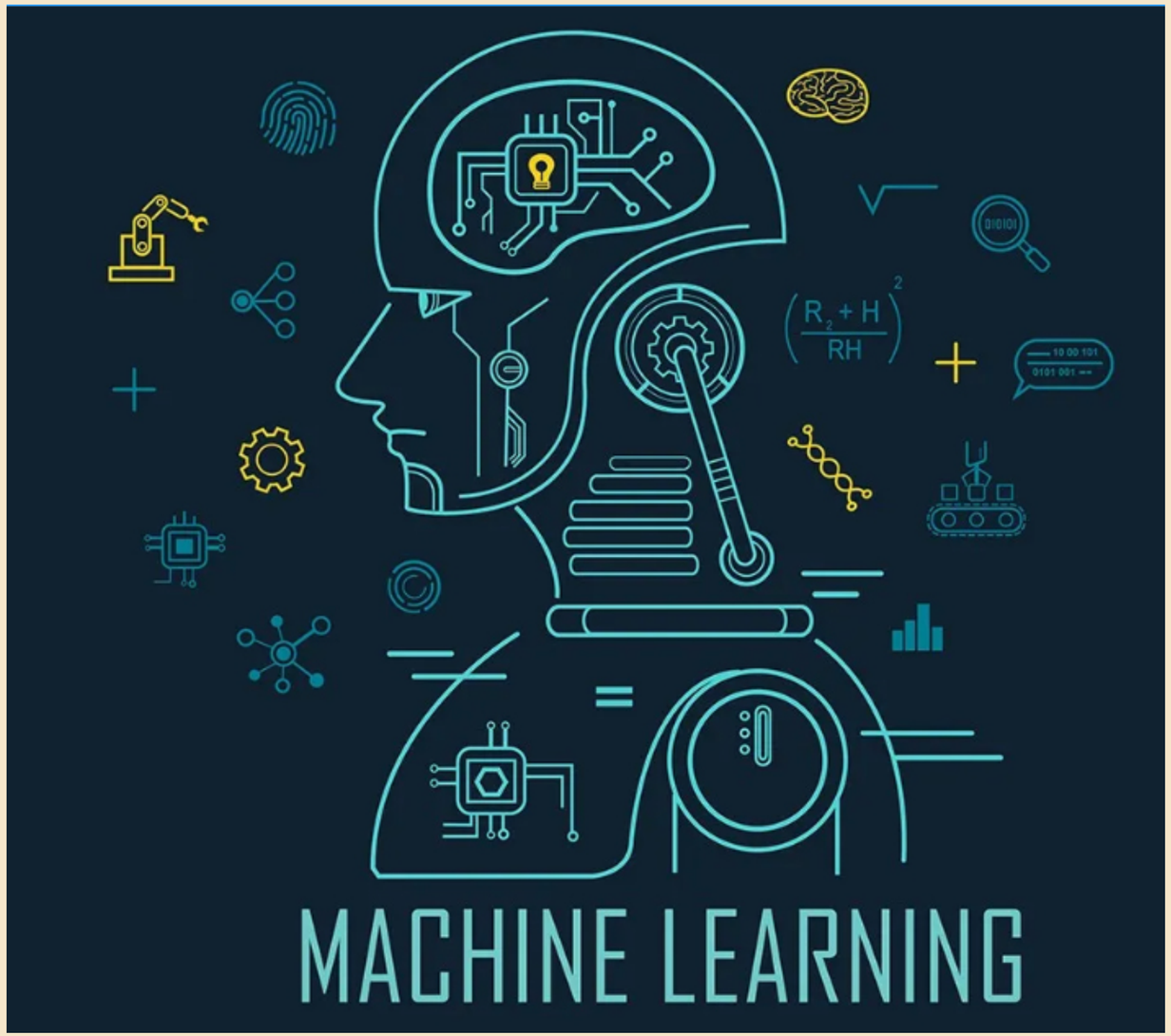


SIGNATURE-BASED DETECTION

- Collect signature attacks (string patterns, hacker signatures, ...)
- Generate a trie from the dictionary
- Use Aho–Corasick algorithm to match signatures in the string

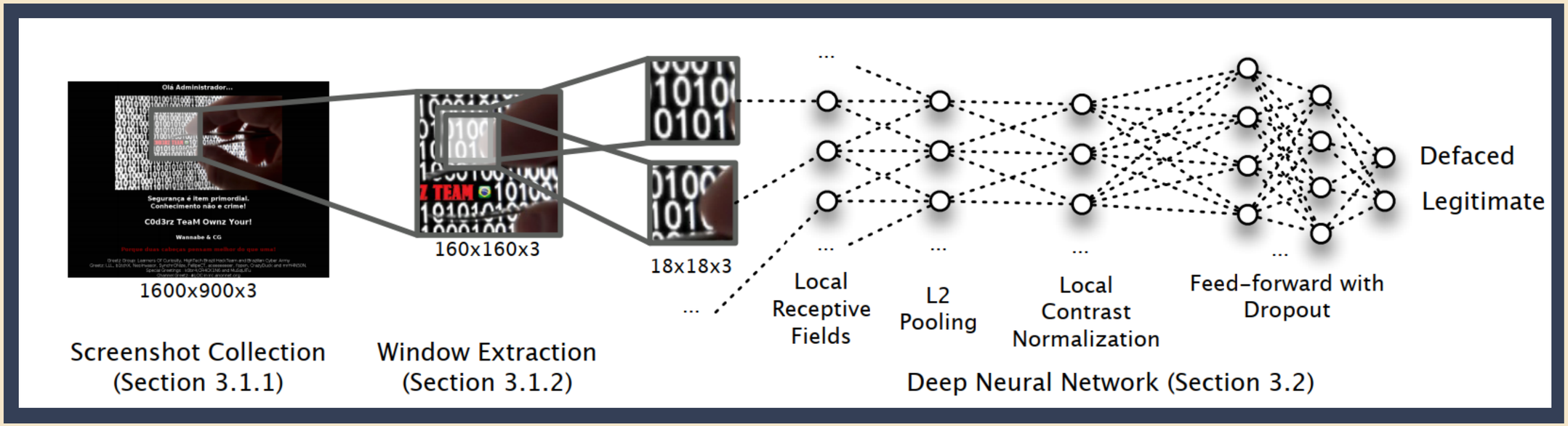
COMPARISON

ANOMALY-BASED DETECTION • Work on behaviour • Trigger when the rule is break • Generate false alarm a lot	**SIGNATURE-BASED DETECTION** • Work on patterns • Detect only known attacks • Rarely generate false alarm



MACHINE-LEARNING -BASED TECHNIQUES

- Advanced anomaly-based detection
- Using different machine learning methods (CNN, RF, GBD,...)
- High accuracy, low false alarm



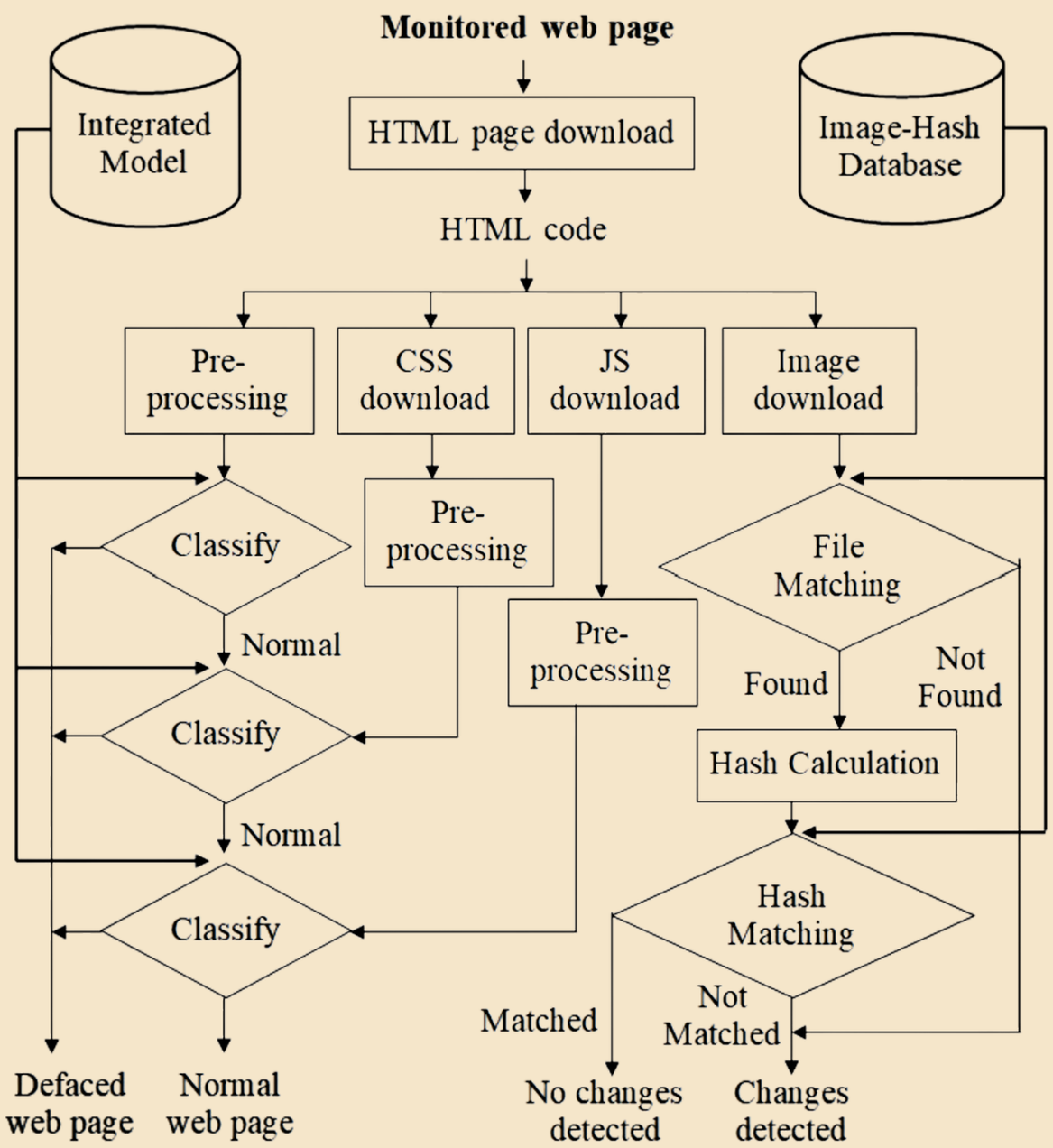
MEERKAT'S MODEL

TRAINING PHASE

- Extract the 160×160 window from each screenshot
- The windows are used to learn the classifier's parameters

DETECTION PHASE

- Capture screenshot from website
- Detect anomalies via the sliding window and the classifier



HOANG'S MULTI-LAYER MODEL

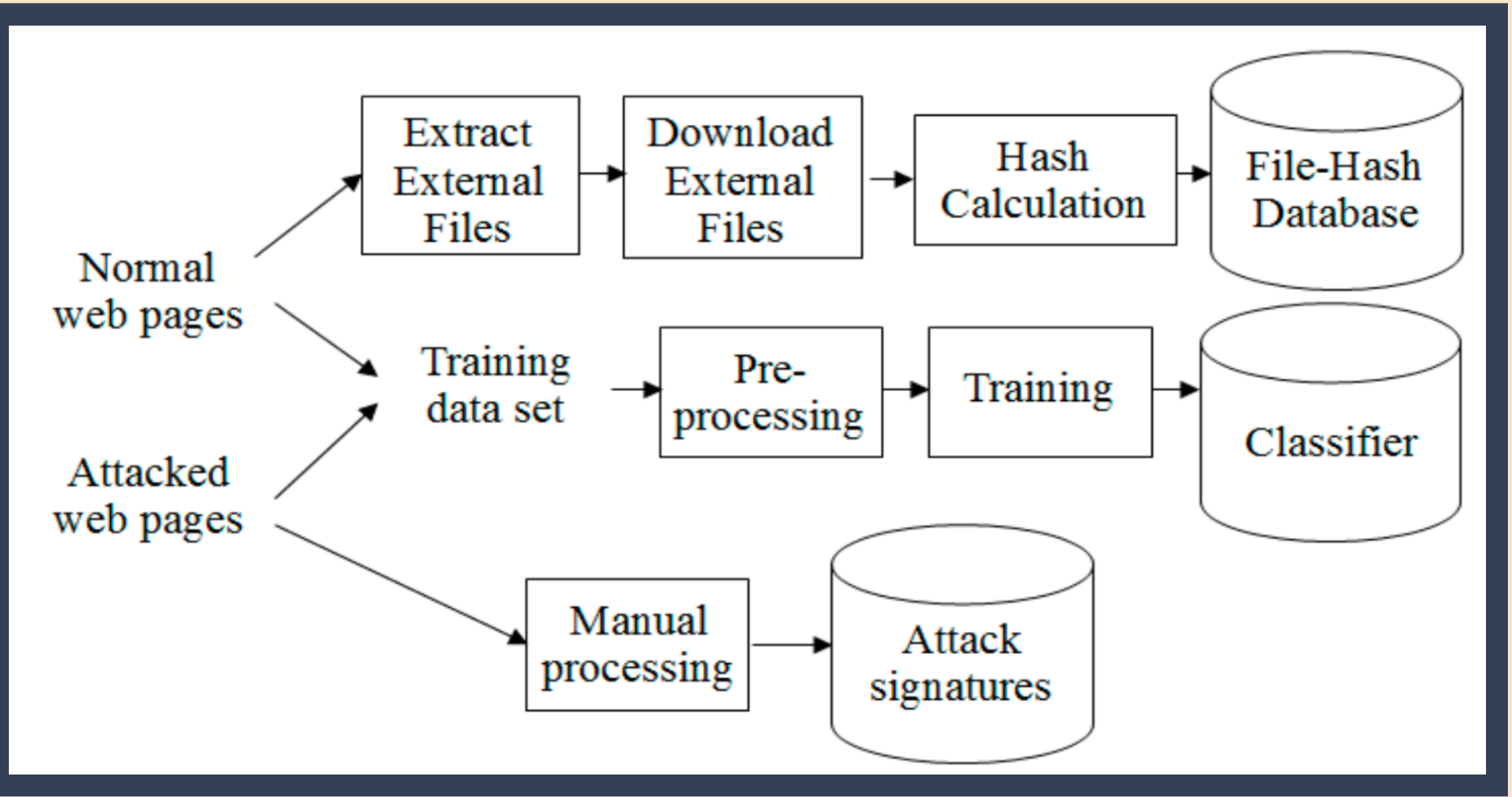
- Use BiLSTM/Efficientnet for 2 classifier layers that train on content + code
- Use hash-based checking for external files

OUR APPROACH

DATASET

- 1700 defaced (Zone.h)
- 2500 benign (Kaggle)

Problem: crawler blocked by captcha

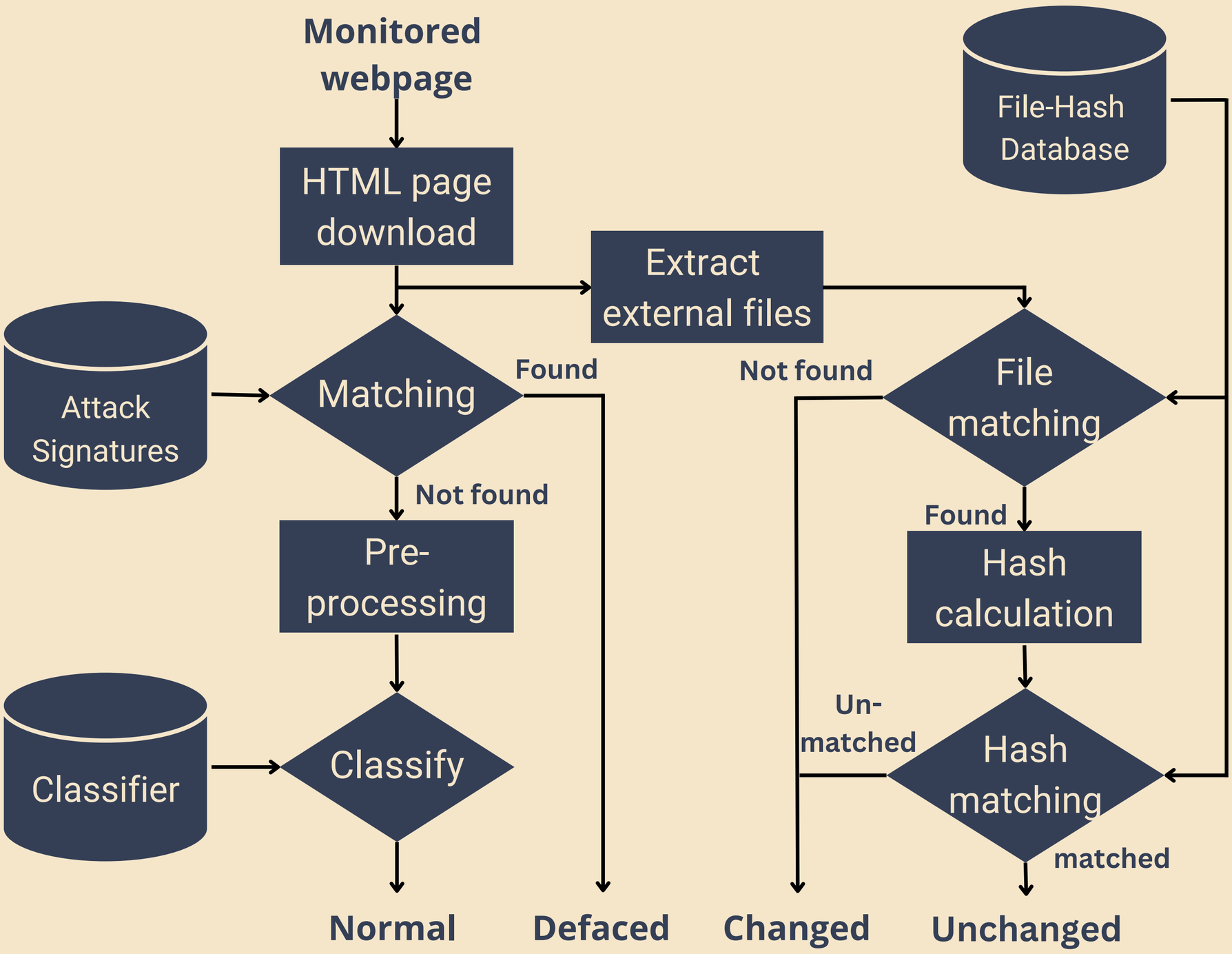


TRAINING

accuracy: 93.7

loss: 47.0835

HYBRID DETECTION



SUMMARY

In this session, we:

- Introduced defacement techniques
- Discuss defacement detection techniques
- Propose our hybrid model

THANK YOU

GROUP: 3 CLASS: CC01