	Dr D Y Patil Pratishthan's Dr. D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune		DI No.: ACAD/DI/72
Academic Year: 2021-22	Weekly Report Format for Internship		Revision : 00 Dated : 20/11/2019
Term – II	Department : Computer Engineering		Date of Preparation : 3/01/2022

Weekly Report for Internship

Roll No: TACO19108

Name of the Student: Ojus Jaiswal


Name of the Company: T A L A K U N C H I Networks Pvt. Ltd.

Domain of Internship: Cyber Security (Ethical Hacking)

Name of the Internal Guide: Mrs. Nalini Jagtap

Name of the External Guide: Mrs. Poojitha Nandimandalam

Duration of Internship: 2 Months

 DYP <small>DR. D. Y. PATIL INSTITUTE OF ENGINEERING, MANAGEMENT AND RESEARCH</small>	Dr D Y Patil Pratishthan's Dr. D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune		DI No.: ACAD/DI/72
Academic Year: 2021-22	Weekly Report Format for Internship		Revision : 00 Dated : 20/11/2019
Term – II	Department : Computer Engineering		Date of Preparation : 3/01/2022

Week - IV

Dates: 31 January, 2022 to 6 February, 2022

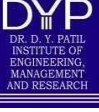
Description of work done till date:

In fourth week, we were given project no. 2 i.e., Scanning using OWASP ZAP. In this project we have to use OWASP ZAP tool which automates the process of finding vulnerabilities in website. In this tool we have to just give URL of website and the tool will automatically test for various vulnerabilities. Then it gives us detailed report of tests done and vulnerabilities found.

We were first told to attend sessions from LMS which will cover basics regarding the topic. Then after completion of sessions from LMS, live hands-on lecture was conducted in which the instructor showed us practical implementation of project. Then doubt session was conducted for clearing our doubts and to check if we were facing any problem in project execution.

Student Sign

Internal Guide Sign

	Dr D Y Patil Pratishthan's Dr. D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune		DI No.: ACAD/DI/72
Academic Year: 2021-22	Weekly Report Format for Internship		Revision : 00 Dated : 20/11/2019
Term – II	Department : Computer Engineering		Date of Preparation : 3/01/2022

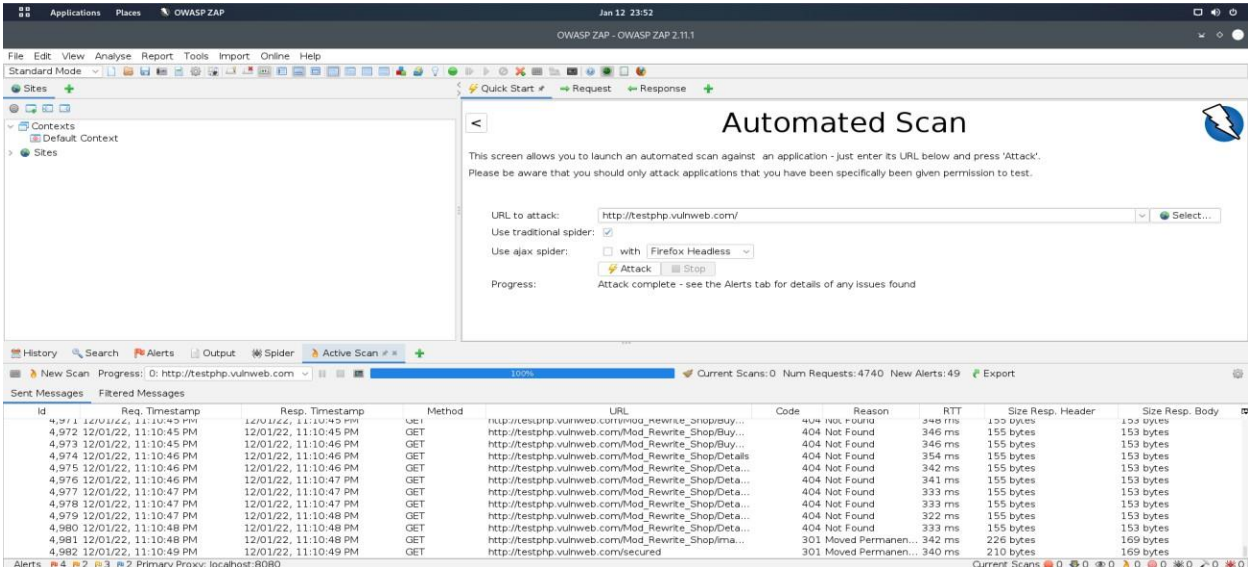
Supporting Documents:

Project 2

Scanning using OWASP ZAP

Task 1 :- Take some website (vulnerable website). Scan using OWASP ZAP Tool (quick/automated). Set of vulnerabilities - make a report with mitigations.

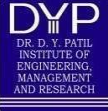
Solution :-

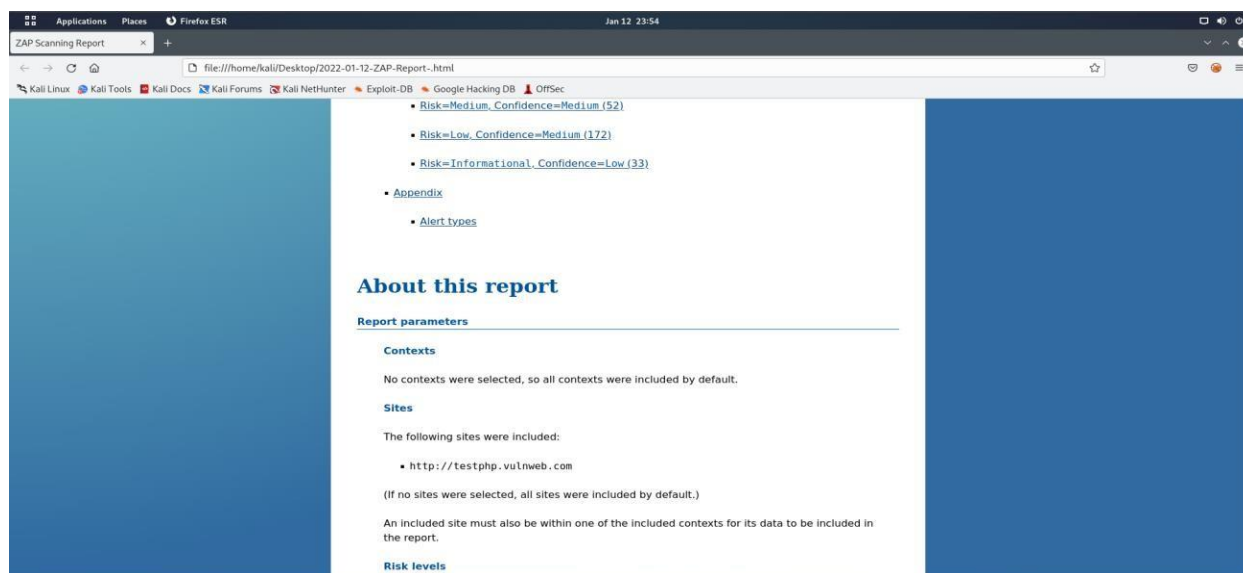


The screenshot shows the OWASP ZAP interface during an automated scan. The 'Automated Scan' window is active, displaying the URL 'http://testphp.vulnweb.com/' and the scan progress at 100%. Below the scan window, a table lists the scan results, including request timestamps, methods, URLs, codes, reasons, and response sizes.

ID	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
4,971	12/01/22, 11:10:45 PM	12/01/22, 11:10:45 PM	GET	http://testphp.vulnweb.com/Mod_Rewrite_ShopBuy...	404	Not Found	346 ms	155 bytes	153 bytes
4,972	12/01/22, 11:10:45 PM	12/01/22, 11:10:45 PM	GET	http://testphp.vulnweb.com/Mod_Rewrite_ShopBuy...	404	Not Found	346 ms	155 bytes	153 bytes
4,973	12/01/22, 11:10:45 PM	12/01/22, 11:10:46 PM	GET	http://testphp.vulnweb.com/Mod_Rewrite_ShopBuy...	404	Not Found	346 ms	155 bytes	153 bytes
4,974	12/01/22, 11:10:46 PM	12/01/22, 11:10:46 PM	GET	http://testphp.vulnweb.com/Mod_Rewrite_ShopDetails...	404	Not Found	354 ms	155 bytes	153 bytes
4,975	12/01/22, 11:10:46 PM	12/01/22, 11:10:46 PM	GET	http://testphp.vulnweb.com/Mod_Rewrite_ShopDetails...	404	Not Found	342 ms	155 bytes	153 bytes
4,976	12/01/22, 11:10:46 PM	12/01/22, 11:10:47 PM	GET	http://testphp.vulnweb.com/Mod_Rewrite_ShopDetails...	404	Not Found	341 ms	155 bytes	153 bytes
4,977	12/01/22, 11:10:47 PM	12/01/22, 11:10:47 PM	GET	http://testphp.vulnweb.com/Mod_Rewrite_ShopDetails...	404	Not Found	333 ms	155 bytes	153 bytes
4,978	12/01/22, 11:10:47 PM	12/01/22, 11:10:47 PM	GET	http://testphp.vulnweb.com/Mod_Rewrite_ShopDetails...	404	Not Found	333 ms	155 bytes	153 bytes
4,979	12/01/22, 11:10:47 PM	12/01/22, 11:10:48 PM	GET	http://testphp.vulnweb.com/Mod_Rewrite_ShopDetails...	404	Not Found	322 ms	155 bytes	153 bytes
4,980	12/01/22, 11:10:48 PM	12/01/22, 11:10:48 PM	GET	http://testphp.vulnweb.com/Mod_Rewrite_ShopDetails...	404	Not Found	333 ms	155 bytes	153 bytes
4,981	12/01/22, 11:10:48 PM	12/01/22, 11:10:48 PM	GET	http://testphp.vulnweb.com/Mod_Rewrite_ShopDetails...	301	Moved Permanen...	342 ms	226 bytes	169 bytes
4,982	12/01/22, 11:10:49 PM	12/01/22, 11:10:49 PM	GET	http://testphp.vulnweb.com/secured	301	Moved Permanen...	340 ms	210 bytes	169 bytes

Alerts: 4 #2 #3 #2 Primary Proxy: localhost:8080

 <p>DR. D. Y. PATIL INSTITUTE OF ENGINEERING, MANAGEMENT AND RESEARCH</p>	<p align="center">Dr D Y Patil Pratishthan's Dr. D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune</p>		<p align="center">DI No.: ACAD/DI/72</p>
<p>Academic Year: 2021-22</p>	<p align="center">Weekly Report Format for Internship</p>		<p>Revision : 00 Dated : 20/11/2019</p>
<p align="center">Term – II</p>	<p align="center">Department : Computer Engineering</p>		<p>Date of Preparation : 3/01/2022</p>



Academic Year:
2021-22

Weekly Report Format for Internship

Revision : 00
Dated : 20/11/2019

Term – II

Department : Computer Engineering

Date of Preparation : 3/01/2022

Applications Places Firefox ESR Jan 12 23:54

ZAP Scanning Report

file:///home/kali/Desktop/2022-01-12-ZAP-Report-.html

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Included: High, Medium, Low, Informational

Excluded: None

Confidence levels

Included: User Confirmed, High, Medium, Low

Excluded: User Confirmed, High, Medium, Low, False Positive

Summaries

Alert counts by risk and confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

	Confidence				Total
	User Confirmed	High	Medium	Low	
High	0 (0.0%)	18 (6.0%)	22 (7.4%)	2 (0.7%)	42 (14.0%)
Medium	0 (0.0%)	0 (0.0%)	52 (17.4%)	0 (0.0%)	52 (17.4%)
Low	0	0	172	0	172

Applications Places Firefox ESR Jan 12 23:55

ZAP Scanning Report

file:///home/kali/Desktop/2022-01-12-ZAP-Report-.html

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Risk	(0.0%)	(0.0%)	(57.5%)	(0.0%)	(57.5%)
Informational	0 (0.0%)	0 (0.0%)	0 (0.0%)	33 (11.0%)	33 (11.0%)
Total	0 (0.0%)	18 (6.0%)	246 (82.3%)	35 (11.7%)	299 (100%)

Alert counts by site and risk

This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.

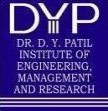
Alerts with a confidence level of "False Positive" have been excluded from these counts.

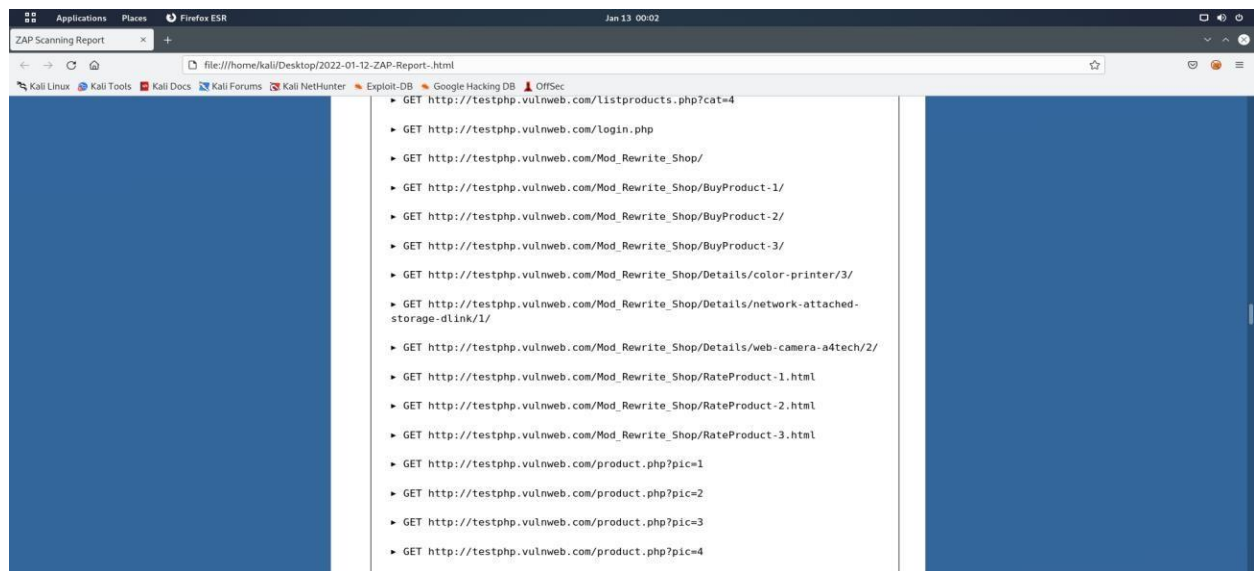
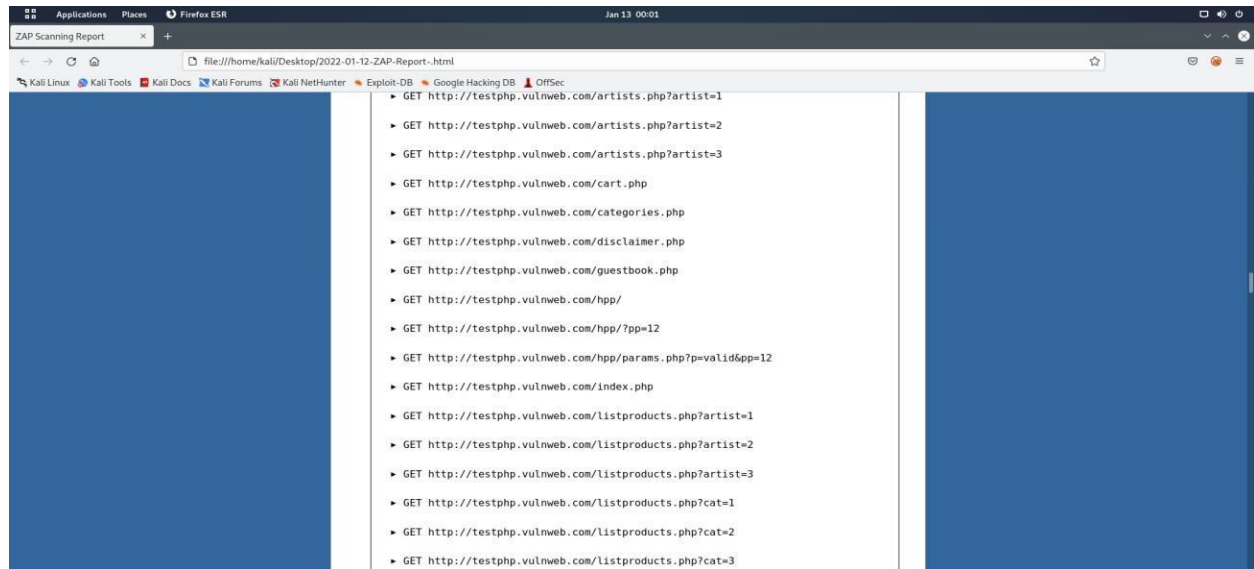
(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)

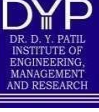
Site	Risk			Informational (>= Informational)
	High (= High)	Medium (>= Medium)	Low (>= Low)	
http://testphp.vulnweb.co	42 (42)	52 (94)	172 (266)	33 (299)

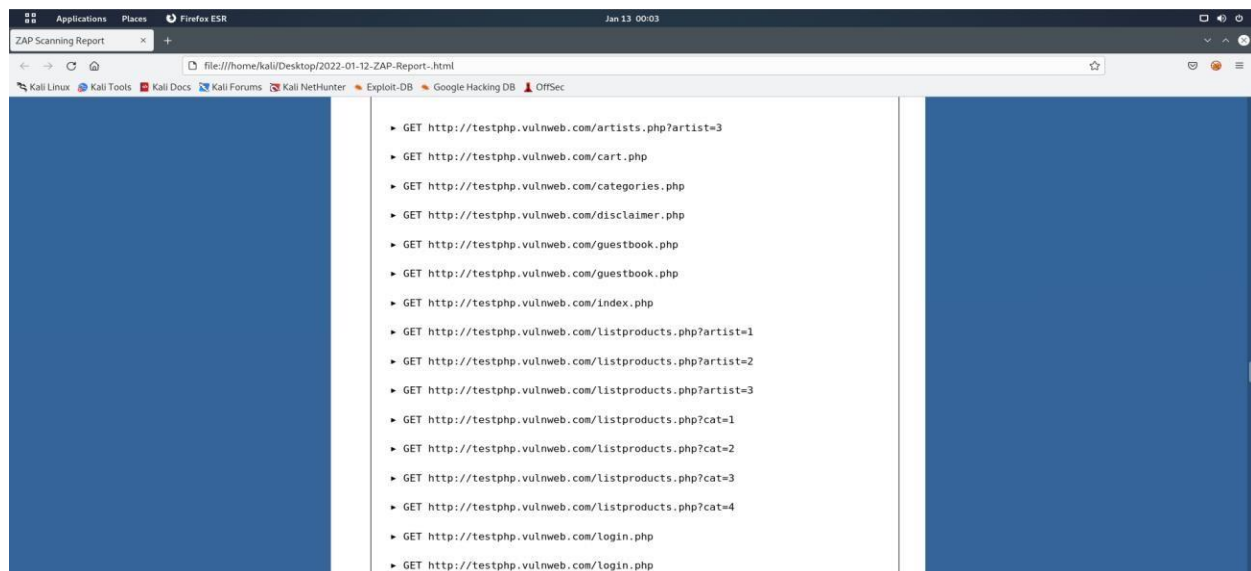
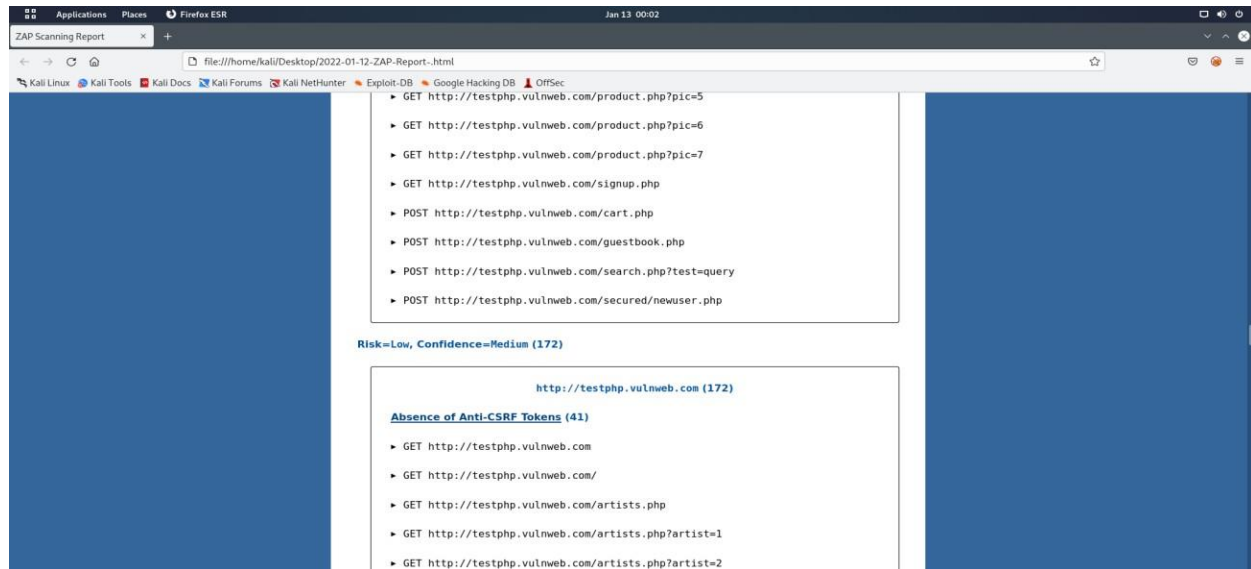
Alert counts by alert type

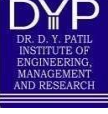
This table shows the number of alerts of each alert type, together with the alert type's risk level.

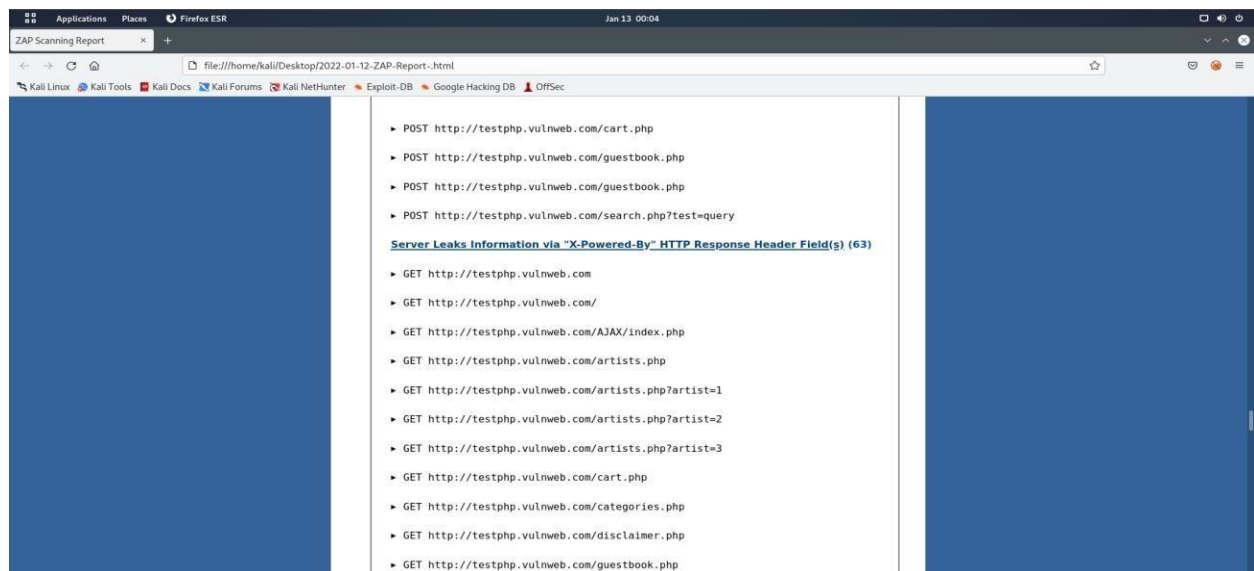
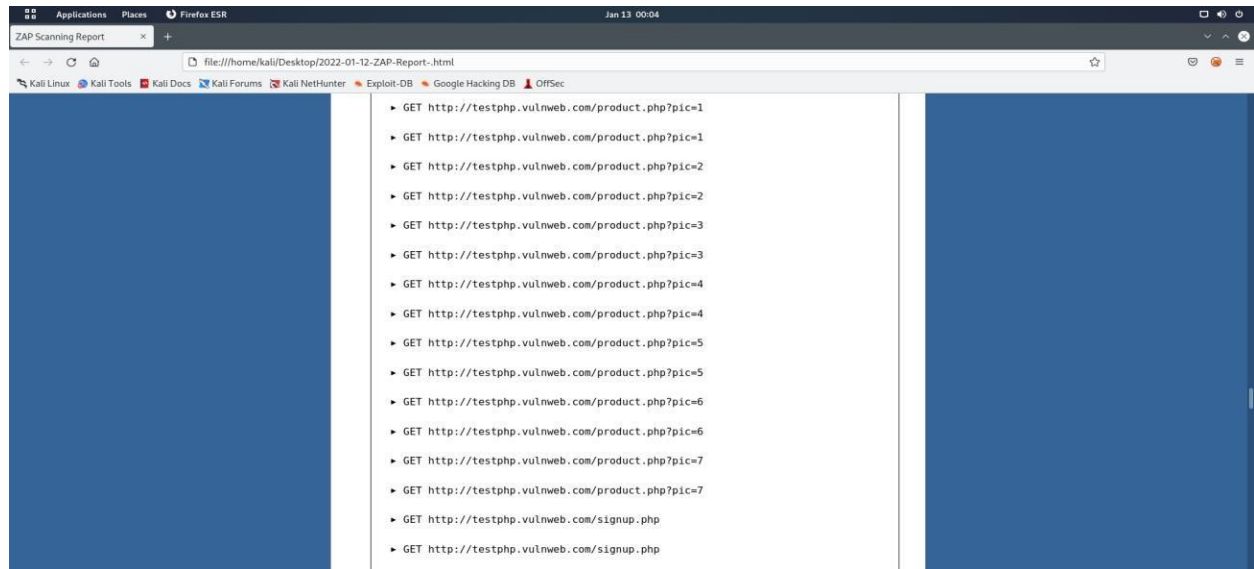
	<p align="center">Dr D Y Patil Pratishthan's Dr. D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune</p>		<p align="center">DI No.: ACAD/DI/72</p>
<p>Academic Year: 2021-22</p>	<p align="center">Weekly Report Format for Internship</p>		<p>Revision : 00 Dated : 20/11/2019</p>
<p align="center">Term – II</p>	<p align="center">Department : Computer Engineering</p>		<p>Date of Preparation : 3/01/2022</p>

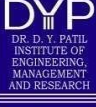


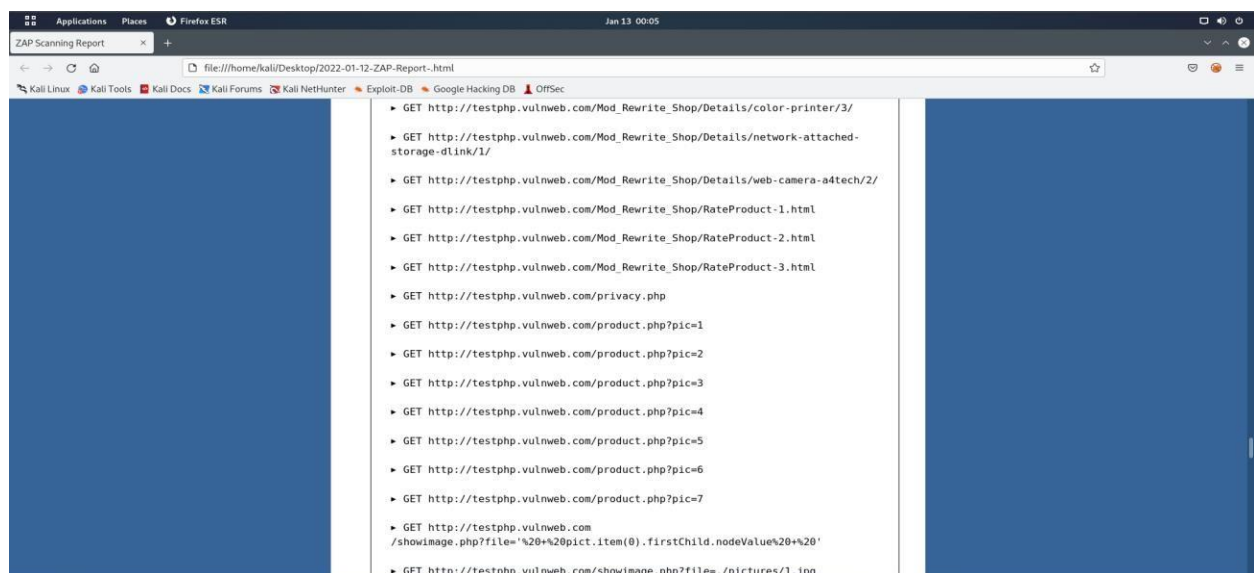
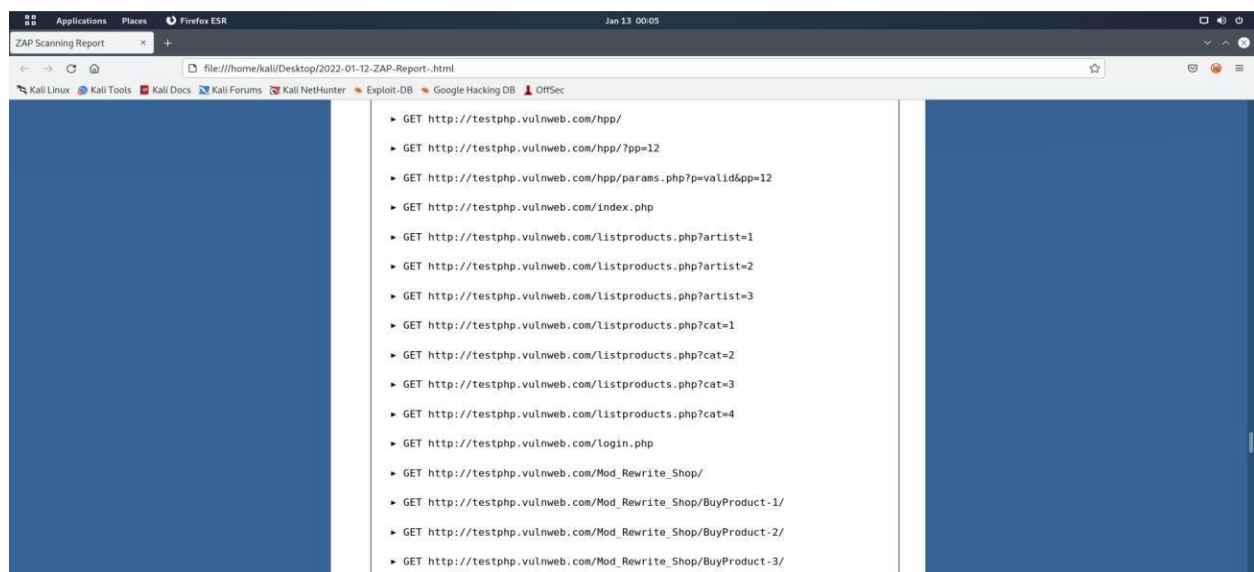
	<p align="center">Dr D Y Patil Pratishthan's Dr. D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune</p>		<p align="center">DI No.: ACAD/DI/72</p>
<p>Academic Year: 2021-22</p>	<p align="center">Weekly Report Format for Internship</p>		<p>Revision : 00 Dated : 20/11/2019</p>
<p align="center">Term – II</p>	<p align="center">Department : Computer Engineering</p>		<p>Date of Preparation : 3/01/2022</p>

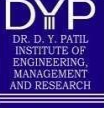


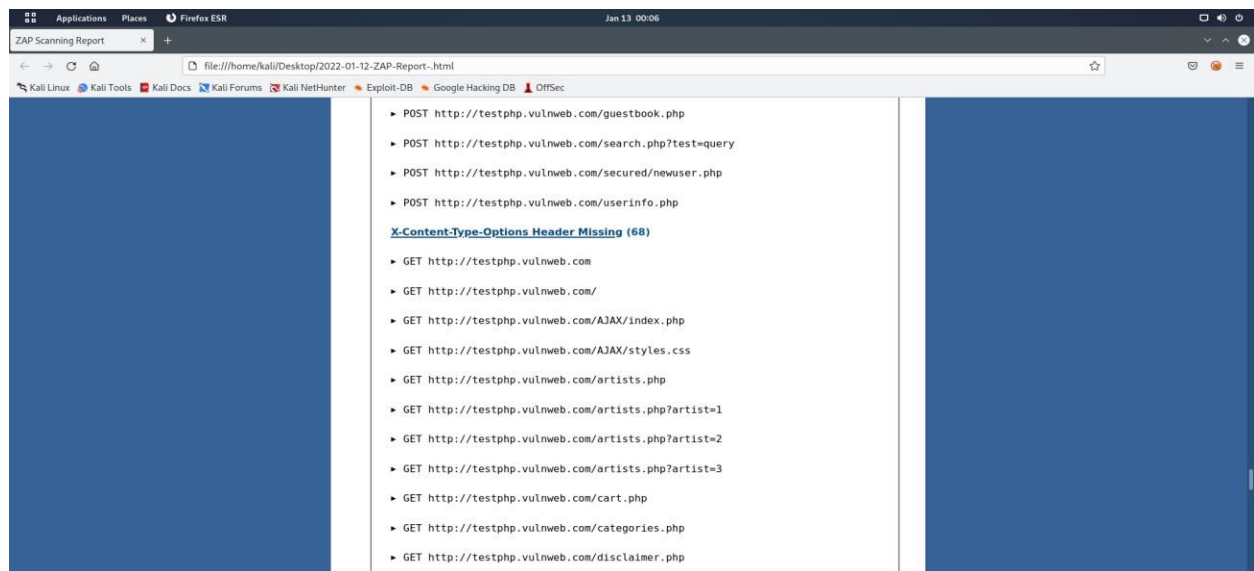
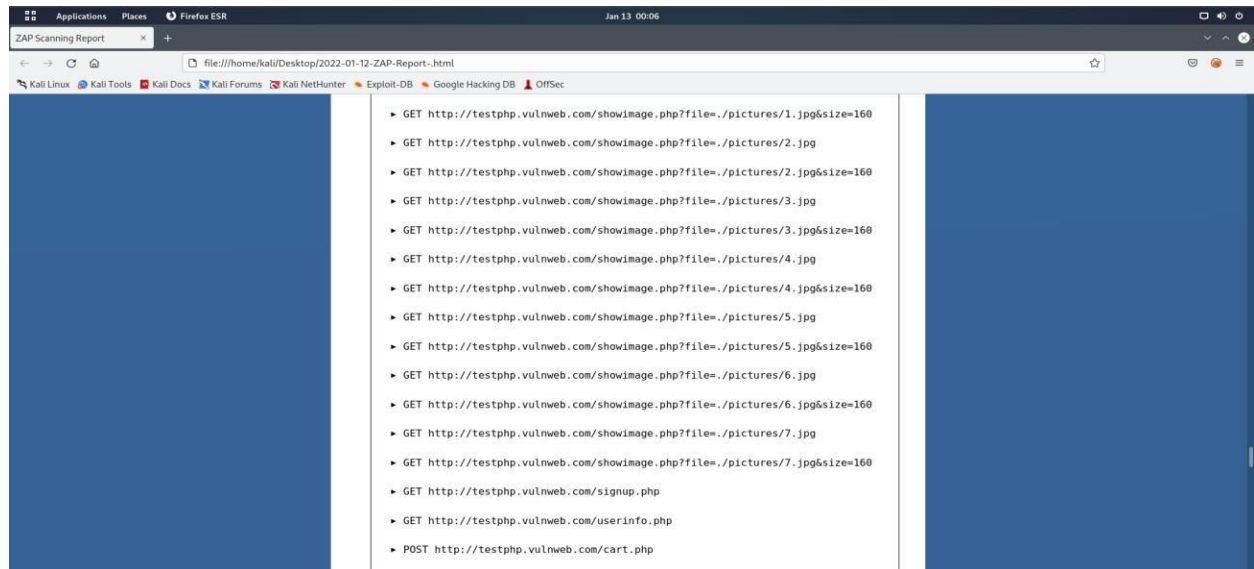
	Dr D Y Patil Pratishthan's Dr. D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune		DI No.: ACAD/DI/72
Academic Year: 2021-22	Weekly Report Format for Internship		Revision : 00 Dated : 20/11/2019
Term – II	Department : Computer Engineering		Date of Preparation : 3/01/2022

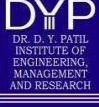


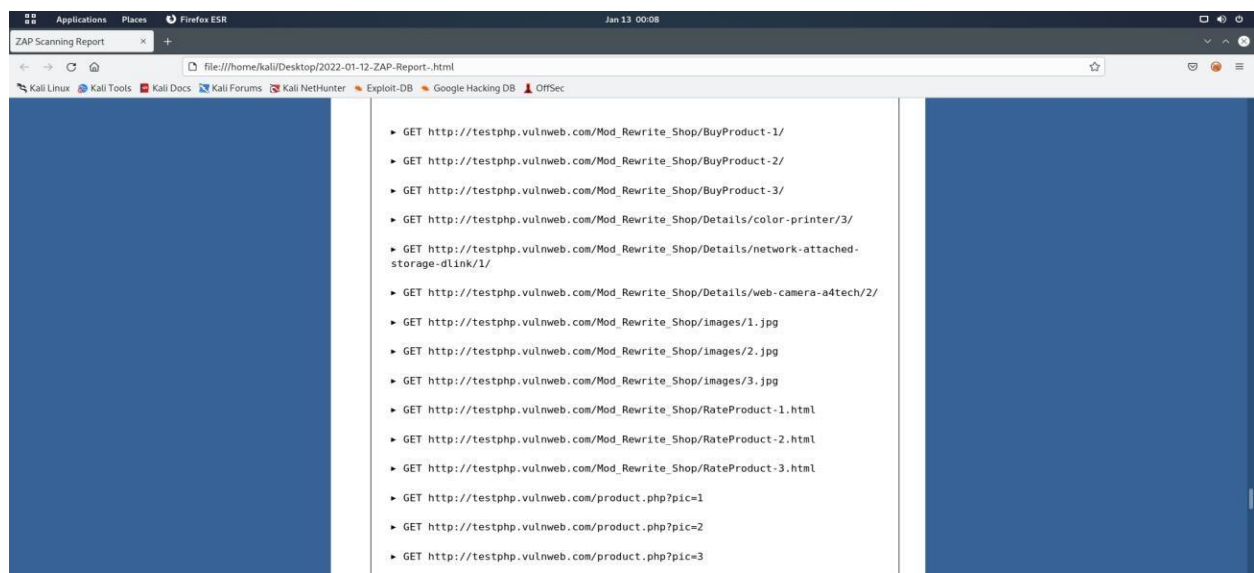
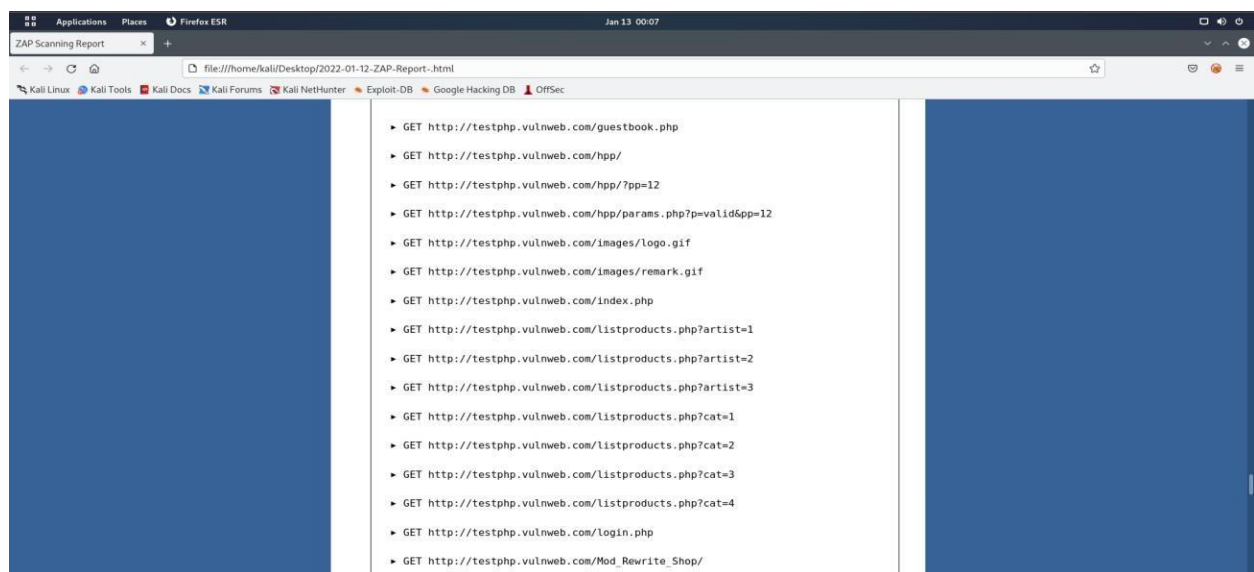
 <p>DR. D. Y. PATIL INSTITUTE OF ENGINEERING, MANAGEMENT AND RESEARCH</p>	<p align="center">Dr D Y Patil Pratishthan's Dr. D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune</p>		<p align="center">DI No.: ACAD/DI/72</p>
<p>Academic Year: 2021-22</p>	<p align="center">Weekly Report Format for Internship</p>		<p>Revision : 00 Dated : 20/11/2019</p>
<p align="center">Term – II</p>	<p align="center">Department : Computer Engineering</p>		<p>Date of Preparation : 3/01/2022</p>

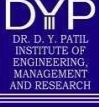


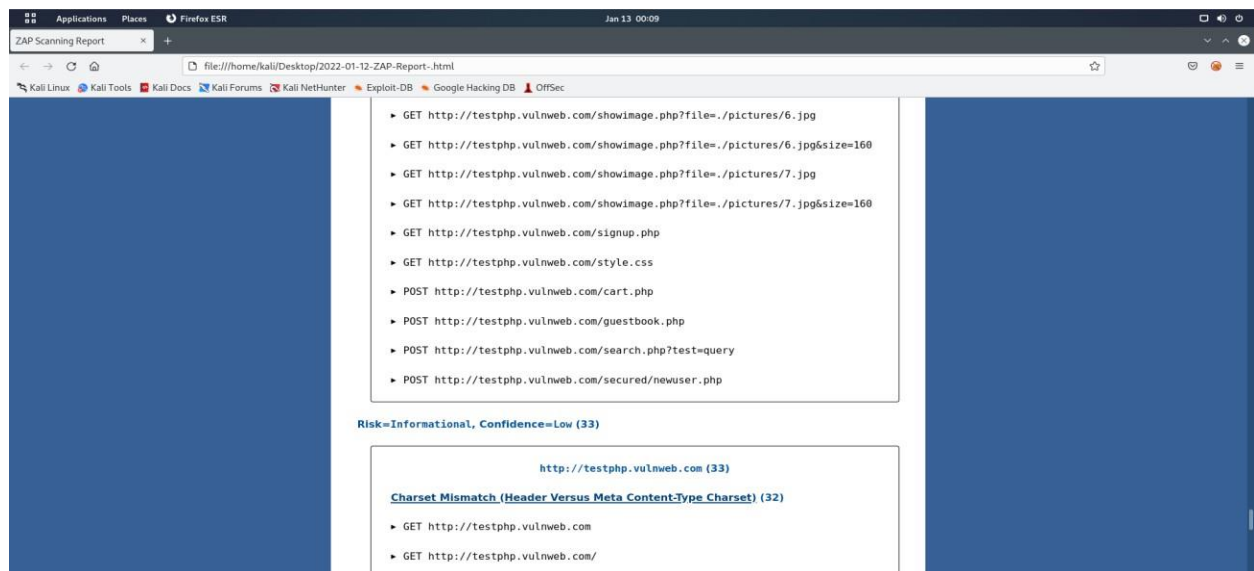
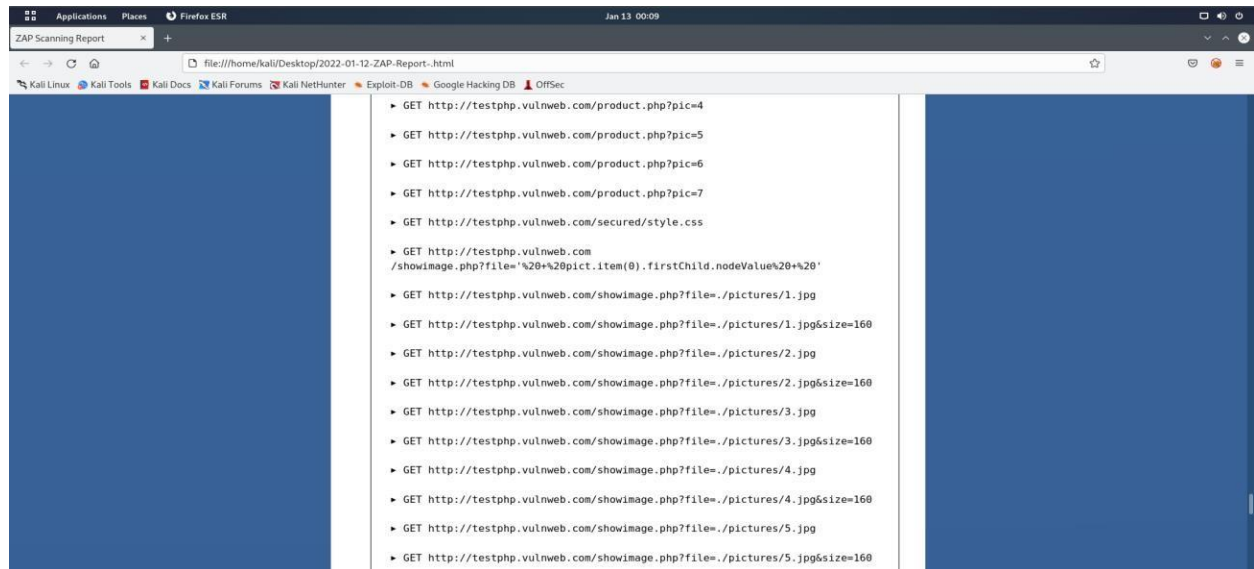
	<p style="text-align: center;">Dr D Y Patil Pratishthan's Dr. D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune</p>		<p style="text-align: center;">DI No.: ACAD/DI/72</p>
<p>Academic Year: 2021-22</p>	<p style="text-align: center;">Weekly Report Format for Internship</p>		<p>Revision : 00 Dated : 20/11/2019</p>
<p style="text-align: center;">Term – II</p>	<p style="text-align: center;">Department : Computer Engineering</p>		<p>Date of Preparation : 3/01/2022</p>

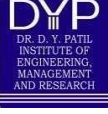


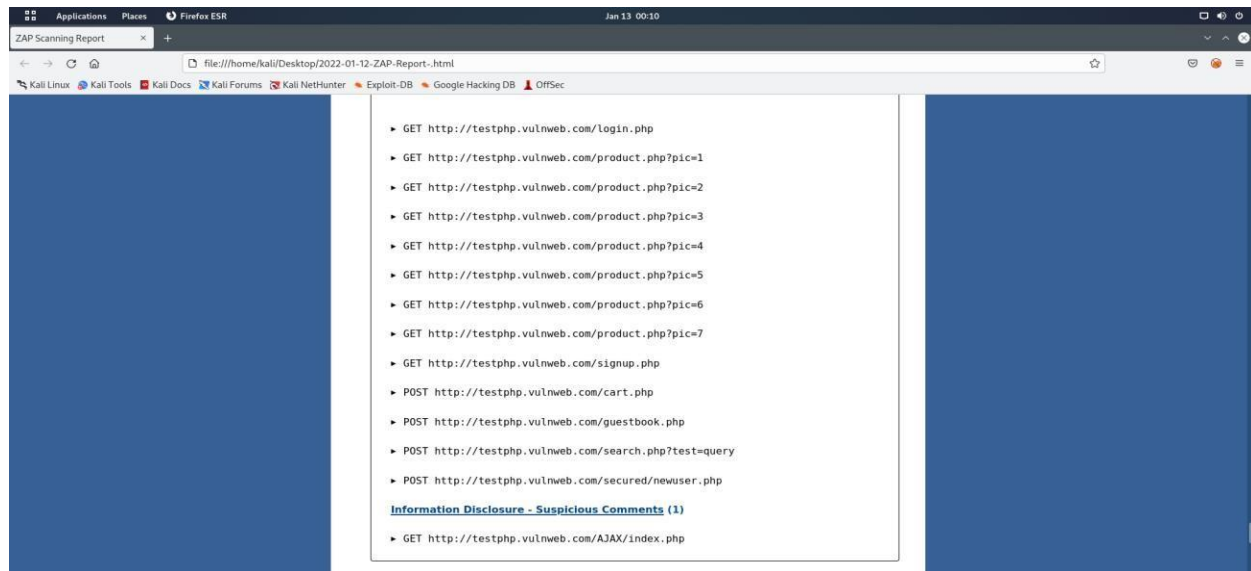
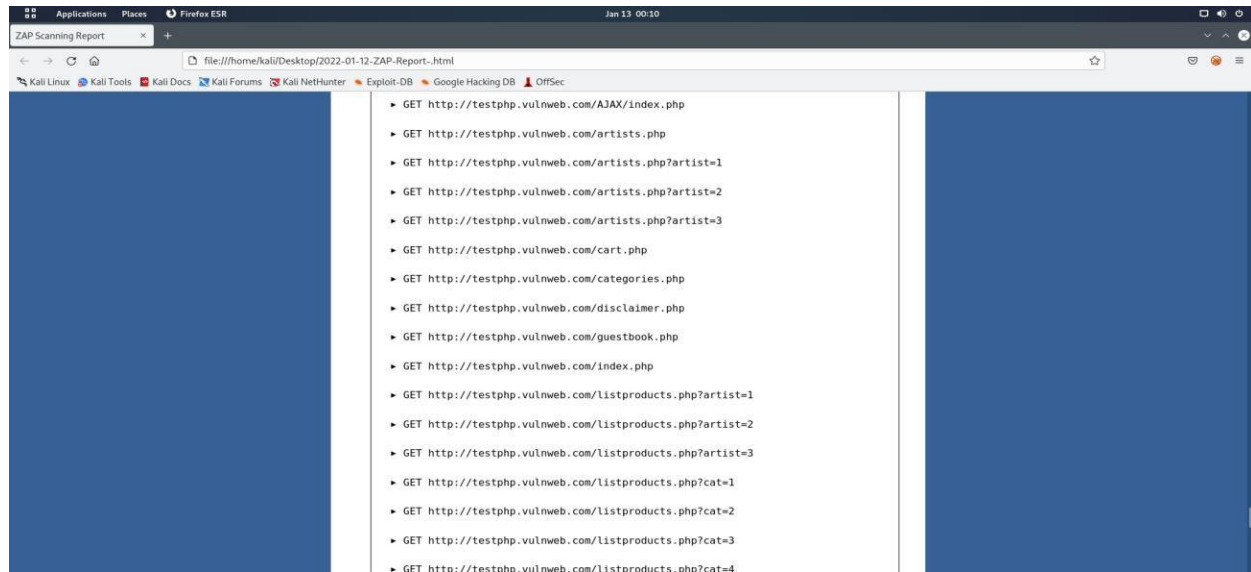
	<p style="text-align: center;">Dr D Y Patil Pratishthan's Dr. D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune</p>		<p style="text-align: center;">DI No.: ACAD/DI/72</p>
<p>Academic Year: 2021-22</p>	<p style="text-align: center;">Weekly Report Format for Internship</p>		<p>Revision : 00 Dated : 20/11/2019</p>
<p style="text-align: center;">Term – II</p>	<p style="text-align: center;">Department : Computer Engineering</p>		<p>Date of Preparation : 3/01/2022</p>

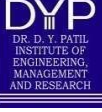


	<p style="text-align: center;">Dr D Y Patil Pratishthan's Dr. D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune</p>		<p style="text-align: center;">DI No.: ACAD/DI/72</p>
<p>Academic Year: 2021-22</p>	<p style="text-align: center;">Weekly Report Format for Internship</p>		<p>Revision : 00 Dated : 20/11/2019</p>
<p style="text-align: center;">Term – II</p>	<p style="text-align: center;">Department : Computer Engineering</p>		<p>Date of Preparation : 3/01/2022</p>



	Dr D Y Patil Pratishthan's Dr. D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune		DI No.: ACAD/DI/72
Academic Year: 2021-22	Weekly Report Format for Internship		Revision : 00 Dated : 20/11/2019
Term – II	Department : Computer Engineering		Date of Preparation : 3/01/2022



	<p align="center">Dr D Y Patil Pratishthan's Dr. D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune</p>		<p align="center">DI No.: ACAD/DI/72</p>
<p>Academic Year: 2021-22</p>	<p align="center">Weekly Report Format for Internship</p>		<p>Revision : 00 Dated : 20/11/2019</p>
<p align="center">Term – II</p>	<p align="center">Department : Computer Engineering</p>		<p>Date of Preparation : 3/01/2022</p>

Player Applications Places Firefox ESR Jan 13 00:11

ZAP Scanning Report

file:///home/kali/Desktop/2022-01-12-ZAP-Report-.html

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Appendix

Alert types

This section contains additional information on the types of alerts in the report.

Cross Site Scripting (DOM Based)

Source	raised by an active scanner (Cross Site Scripting (DOM Based))
CWE ID	79
WASC ID	8
Reference	<ul style="list-style-type: none"> http://projects.webappsec.org/Cross-Site-Scripting http://cwe.mitre.org/data/definitions/79.html

Cross Site Scripting (Reflected)

Source	raised by an active scanner (Cross Site Scripting (Reflected))
CWE ID	79
WASC ID	8
Reference	<ul style="list-style-type: none"> http://projects.webappsec.org/Cross-Site-Scripting http://cwe.mitre.org/data/definitions/79.html

Player Applications Places Firefox ESR Jan 13 00:11

ZAP Scanning Report

file:///home/kali/Desktop/2022-01-12-ZAP-Report-.html

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Remote OS Command Injection

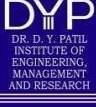
Source	raised by an active scanner (Remote OS Command Injection)
CWE ID	78
WASC ID	31
Reference	<ul style="list-style-type: none"> http://cwe.mitre.org/data/definitions/78.html https://owasp.org/www-community/attacks/Command_Injection

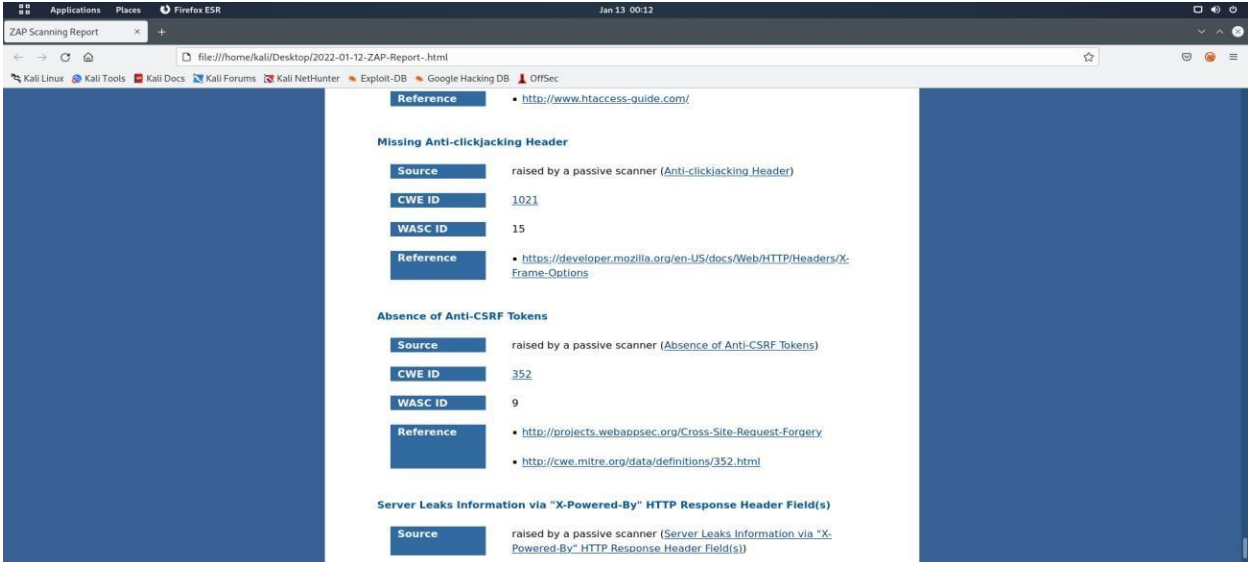
SQL Injection

Source	raised by an active scanner (SQL Injection)
CWE ID	89
WASC ID	19
Reference	<ul style="list-style-type: none"> https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

.htaccess Information Leak

Source	raised by an active scanner (.htaccess Information Leak)
CWE ID	94
WASC ID	14

	<p align="center">Dr D Y Patil Pratishthan's Dr. D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune</p>		<p align="center">DI No.: ACAD/DI/72</p>
<p>Academic Year: 2021-22</p>	<p align="center">Weekly Report Format for Internship</p>		<p>Revision : 00 Dated : 20/11/2019</p>
<p align="center">Term – II</p>	<p align="center">Department : Computer Engineering</p>		<p>Date of Preparation : 3/01/2022</p>



Reference

- <http://www.htaccess-guide.com/>

Missing Anti-clickjacking Header

Source raised by a passive scanner ([Anti-clickjacking Header](#))

CWE ID 1021

WASC ID 15

Reference

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

Absence of Anti-CSRF Tokens

Source raised by a passive scanner ([Absence of Anti-CSRF Tokens](#))

CWE ID 352

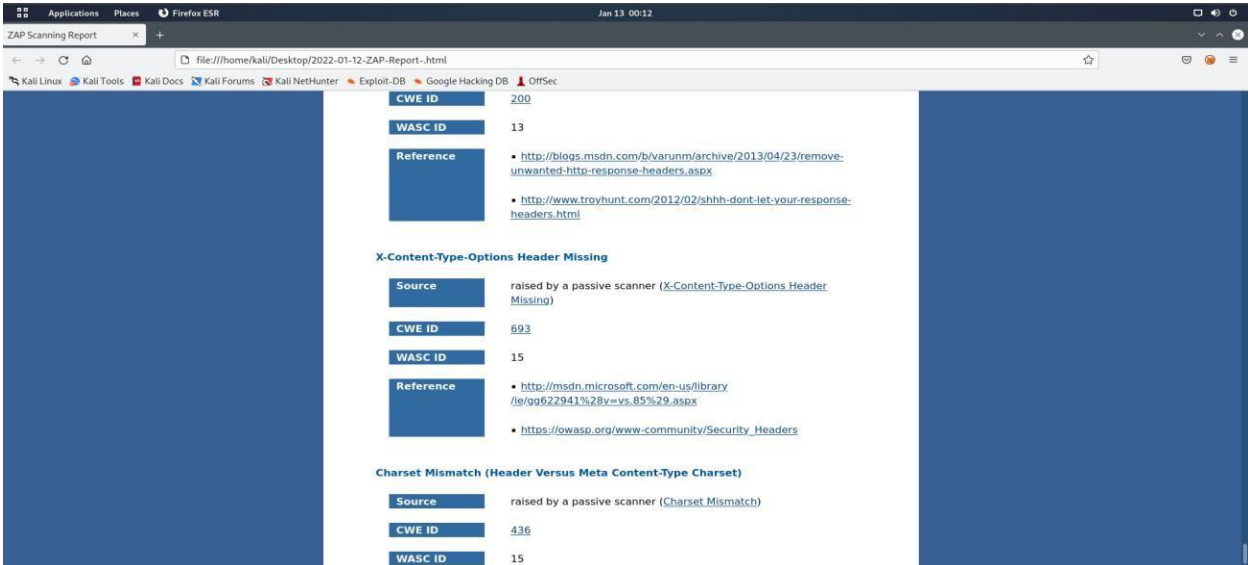
WASC ID 9

Reference

- <http://projects.webappsec.org/Cross-Site-Request-Forgery>
- <http://cwe.mitre.org/data/definitions/352.html>

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Source raised by a passive scanner ([Server Leaks Information via "X-Powered-By" HTTP Response Header Field\(s\)](#))



CWE ID 200

WASC ID 13

Reference

- <http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx>
- <http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html>

X-Content-Type-Options Header Missing

Source raised by a passive scanner ([X-Content-Type-Options Header Missing](#))

CWE ID 693

WASC ID 15

Reference

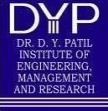
- <http://msdn.microsoft.com/en-us/library/ee6622941%28v=vs.85%29.aspx>
- <https://owasp.org/www-community/Security-Headers>

Charset Mismatch (Header Versus Meta Content-Type Charset)

Source raised by a passive scanner ([Charset Mismatch](#))

CWE ID 436

WASC ID 15

	Dr D Y Patil Pratishthan's Dr. D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune		DI No.: ACAD/DI/72
Academic Year: 2021-22	Weekly Report Format for Internship		Revision : 00 Dated : 20/11/2019
Term – II	Department : Computer Engineering		Date of Preparation : 3/01/2022

