Network Analysing Report
Using Wireshark

1. Exclusive Summary:

1.1. Introduction: Network protocol analysis is the process of capturing, decoding, and interpreting the data packets that travel across a network. A data packet is a unit of information that contains a header and a payload. The header contains information such as the source and destination addresses, the protocol type, and the sequence number. The payload contains the actual data, such as text, images, or audio.

Network protocol analysis tools can capture and display these packets in a readable format, allowing you to examine the details of each packet and how they interact with each other. This device or software is called a network analyzer, sniffer, or packet capture tool. **Wireshark** is a cross-platform network analysis tool used to capture packets in real-time. Wireshark includes filters, flow statistics, colour coding, and other features that allow you to get a deep insight into network traffic and to inspect individual packets. In a network system, each URL is called a request while the data sent back to you is called a response. Response can be simple XML or JSON or any other media type and contains either a status ("ok", "error", etc.) or data (e.g. a list of items). Wireshark has many uses, including troubleshooting networks that have performance issues. Cybersecurity professionals often use Wireshark to trace connections, view the contents of suspect network transactions and identify bursts of network traffic. It's a major part of any IT pro's toolkit.

Network protocol analysis can help you identify and resolve network performance issues, such as latency, packet loss, jitter, or bandwidth utilization. By analyzing the packets, you can determine the root cause of the problem, such as a faulty device, a misconfigured router, a congested link, or a malicious attack. You can also use network protocol analysis to optimize your network performance, such as by adjusting the quality of service (QoS) settings, load balancing, or routing protocols. Network protocol analysis can also help you ensure network security, compliance, and forensics, by detecting and preventing unauthorized access, data breaches, or cyberattacks.

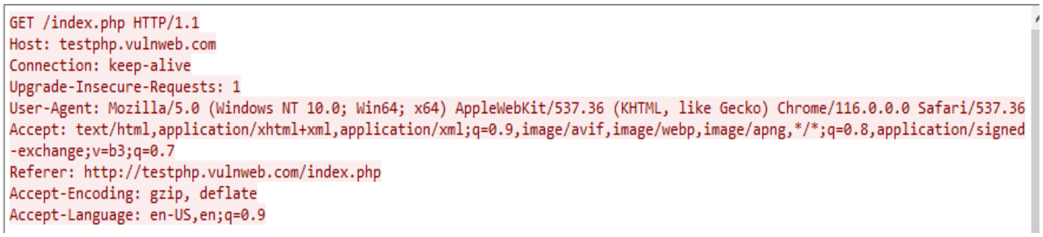
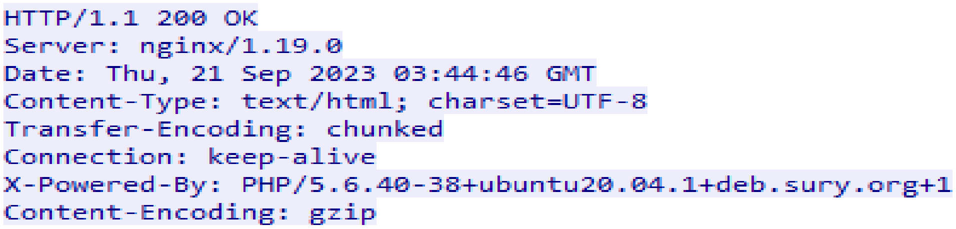
1.2 Objective: The website (http://testphp.vulnweb.com/) hosts intentionally vulnerable web applications. One can use these applications to understand how programming and configuration errors lead to security breaches. This website is created to help anyone test Acunetix but one may also use it for manual penetration testing or for educational purposes. As it is helpful for learning about vulnerabilities such as SQL Injection, Cross-site Scripting (XSS), Cross-site Request Forgery (CSRF), and many more. & this security issue is related to network.

If we analysis the network which is used to run the website, we can determine the likelihood of a threat to the network that will help reducing cyber attack. We can also detect irregular network activities or abnormal traffic patterns.

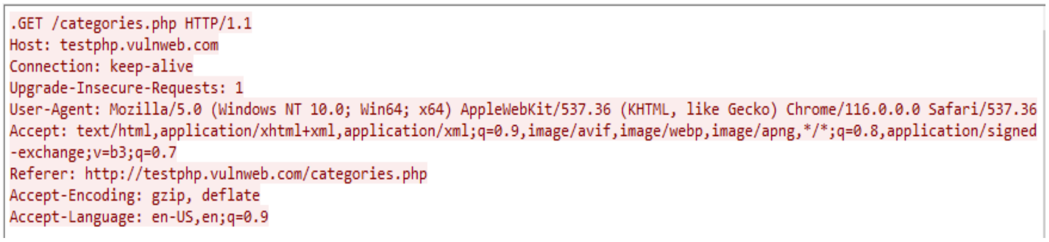
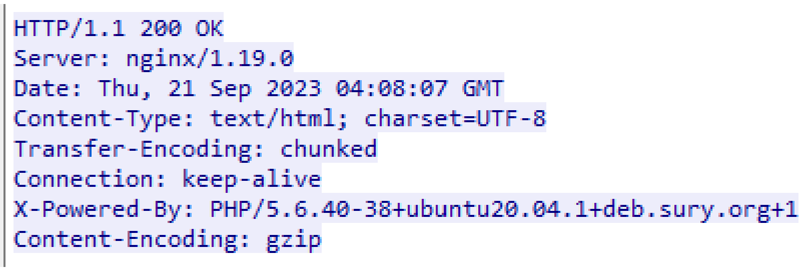
1.3 Scope of Work: http://testphp.vulnweb.com/

2 Details Observation(s)

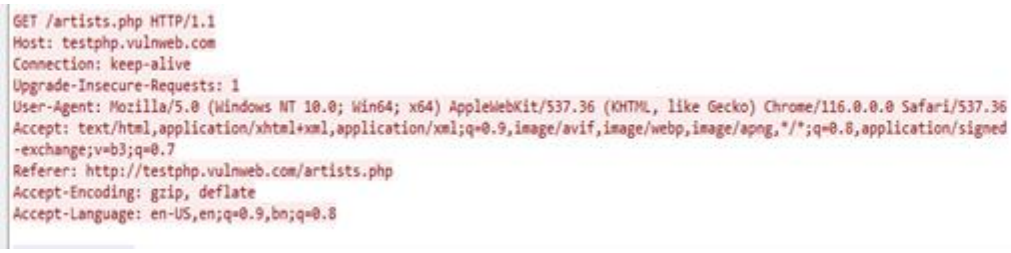
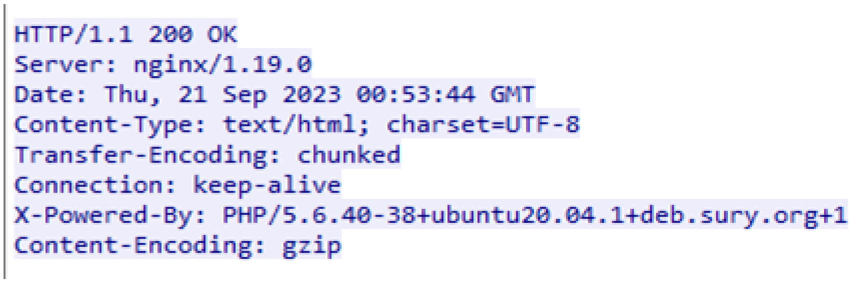
2.1 Description of Observation (Tabular form)

Observation Title (Test Case)	Verification of nav-item ‘home’ by clicking on it from the navigation menu
Reference No	TC001
Host Name	testphp.vulnweb.com
Test Data	http://testphp.vulnweb.com/index.php
Proof of Concept	Reproducing Steps: 1. Goto the URL “http://testphp.vulnweb.com/” 2. Identify the navigation menu 3. Click on the nav-item “home” 4. Open Wireshark 5. Look for http://testphp.vulnweb.com/index.php 6. Then right click >Follow>TCP Stream
Request	 GET /index.php HTTP/1.1 Host: testphp.vulnweb.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 Referer: http://testphp.vulnweb.com/index.php Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
Response	 HTTP/1.1 200 OK Server: nginx/1.19.0 Date: Thu, 21 Sep 2023 03:44:46 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 Content-Encoding: gzip
Analysis	1. Transmission Control Protocol, Src Port: 49884, Dst Port: 80, Seq: 648, Ack: 277, Len: 516 2. Internet Protocol Version 4, Src: 192.168.1.195, Dst: 44.228.249.3 3. Frame 315: 570 bytes on wire (4560 bits), 570 bytes captured (4560 bits) on interface \Device\NPF_{B2F39B3B-01F5-4FB7-BAB6-C642BE981D95}, id 0

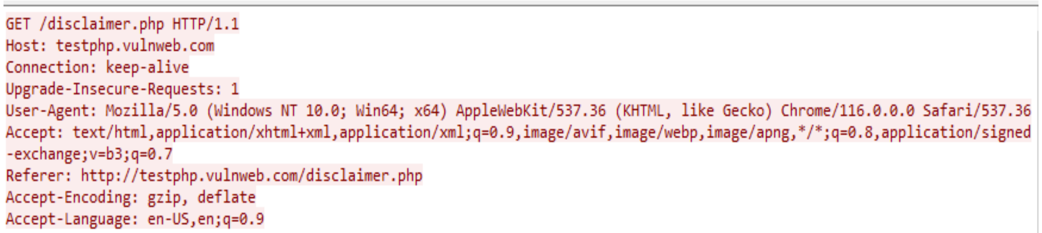
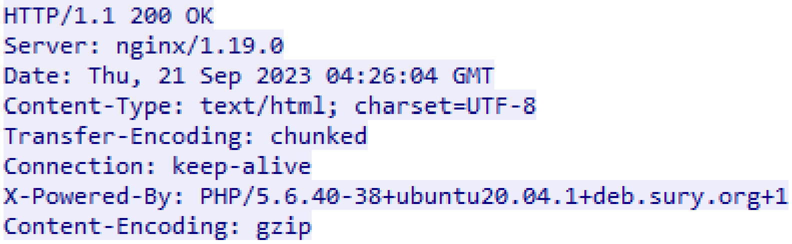
2.2 Description of Observation (Tabular form)

Observation Title (Test Case)	Verification of nav-item ‘categories’ by clicking on it from the navigation menu
Reference No	TC002
Host Name	testphp.vulnweb.com
Test Data	http://testphp.vulnweb.com/categories.php
Proof of Concept	Reproducing Steps: 1. Goto the URL “http://testphp.vulnweb.com/” 2. Identify the navigation menu 3. Open Wireshark 4. Click on the nav-item “categories” 5. Look for http://testphp.vulnweb.com/categories.php 6. Then right click >Follow>TCP Stream
Request	 .GET /categories.php HTTP/1.1 Host: testphp.vulnweb.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed -exchange;v=b3;q=0.7 Referer: http://testphp.vulnweb.com/categories.php Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
Response	 HTTP/1.1 200 OK Server: nginx/1.19.0 Date: Thu, 21 Sep 2023 04:08:07 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 Content-Encoding: gzip
Analysis	1. Transmission Control Protocol, Src Port: 49998, Dst Port: 80, Seq: 2, Ack: 1, Len: 500 2. Internet Protocol Version 4, Src: 192.168.1.195, Dst: 44.228.249.3 3. Frame 8: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface \Device\NPF_{B2F39B3B-01F5-4FB7-BAB6-C642BE981D95}, id 0

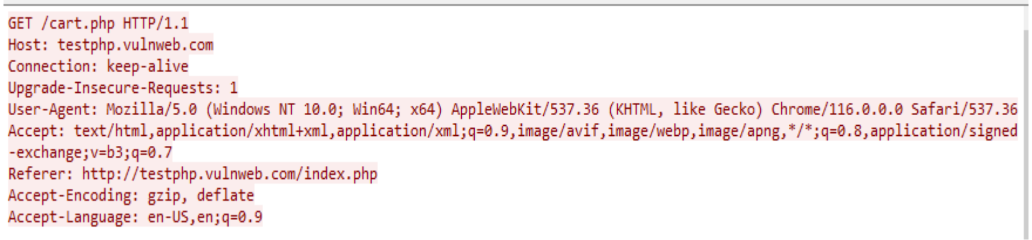
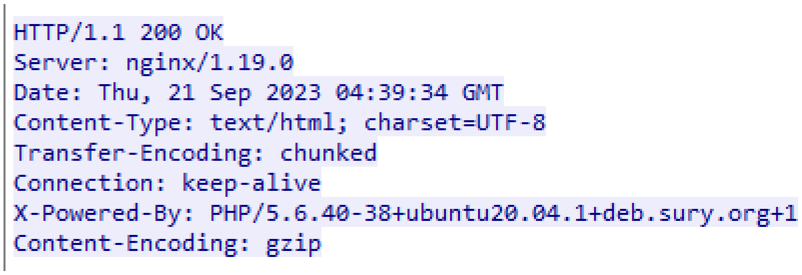
2.3 Description of Observation (Tabular form)

Observation Title (Test Case)	Verification of nav-item ‘artists’ by clicking on it from the navigation menu
Reference No	TC003
Host Name	testphp.vulnweb.com
Test Data	http://testphp.vulnweb.com/artists.php
Proof of Concept	Reproducing Steps: 1. Goto the URL “http://testphp.vulnweb.com/” 2. Identify the navigation menu 3. Open Wireshark 4. Click on the nav-item “artists” 5. Look for http://testphp.vulnweb.com/artists.php 6. Then right click >Follow>TCP Stream
Request	 GET /artists.php HTTP/1.1 Host: testphp.vulnweb.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 Referer: http://testphp.vulnweb.com/artists.php Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9,bn;q=0.8
Response	 HTTP/1.1 200 OK Server: nginx/1.19.0 Date: Thu, 21 Sep 2023 00:53:44 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 Content-Encoding: gzip
Analysis	1. Transmission Control Protocol, Src Port: 50046, Dst Port: 80, Seq: 1483, Ack: 7813, Len: 494 2. Internet Protocol Version 4, Src: 192.168.1.195, Dst: 44.228.249.3 3. Frame 879: 548 bytes on wire (4384 bits), 548 bytes captured (4384 bits) on interface \Device\NPF_{B2F39B3B-01F5-4FB7-BAB6-C642BE981D95}, id 0

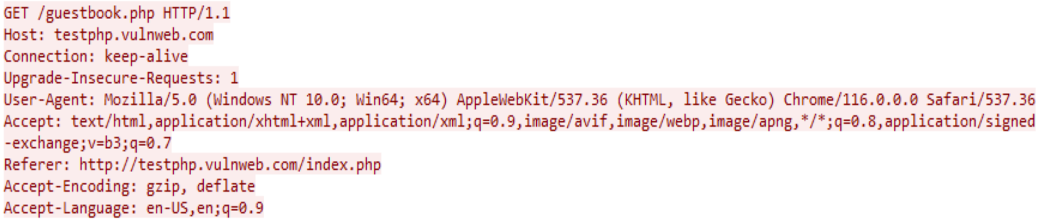
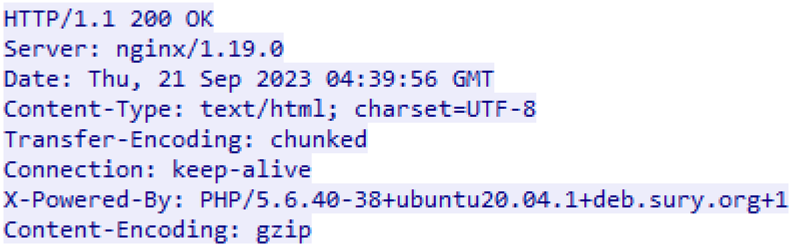
2.4 Description of Observation (Tabular form)

Observation Title (Test Case)	Verification of nav-item ‘disclaimer’ by clicking on it from the navigation menu
Reference No	TC004
Host Name	testphp.vulnweb.com
Test Data	http://testphp.vulnweb.com/disclaimer.php
Proof of Concept	Reproducing Steps: 7. Goto the URL “http://testphp.vulnweb.com/” 8. Identify the navigation menu 9. Open Wireshark 10. Click on the nav-item “disclaimer” 11. Look for http://testphp.vulnweb.com/disclaimer.php 12. Then right click >Follow>TCP Stream
Request	 GET /disclaimer.php HTTP/1.1 Host: testphp.vulnweb.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 Referer: http://testphp.vulnweb.com/disclaimer.php Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
Response	 HTTP/1.1 200 OK Server: nginx/1.19.0 Date: Thu, 21 Sep 2023 04:26:04 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 Content-Encoding: gzip
Analysis	1. Transmission Control Protocol, Src Port: 50059, Dst Port: 80, Seq: 501, Ack: 2814, Len: 500 2. Internet Protocol Version 4, Src: 192.168.1.195, Dst: 44.228.249.3 3. Frame 105: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface \Device\NPF_{B2F39B3B-01F5-4FB7-BAB6-C642BE981D95}, id 0

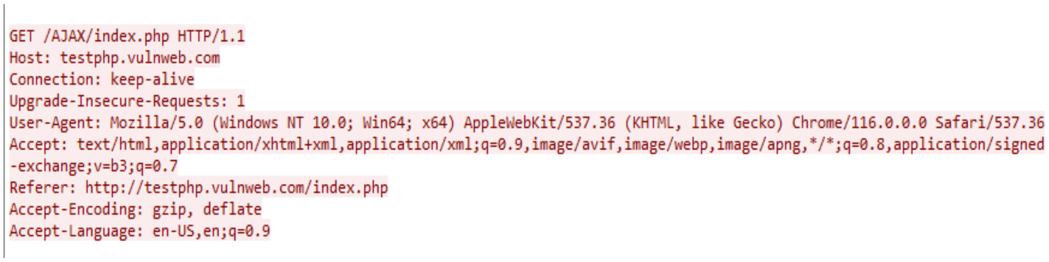
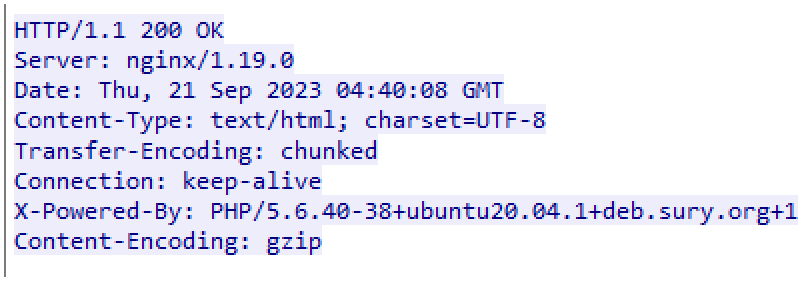
2.5 Description of Observation (Tabular form)

Observation Title (Test Case)	Verification of nav-item ‘your cart’ by clicking on it from the navigation menu
Reference No	TC005
Host Name	testphp.vulnweb.com
Test Data	http://testphp.vulnweb.com/cart.php
Proof of Concept	Reproducing Steps: 13. Goto the URL “http://testphp.vulnweb.com/” 14. Identify the navigation menu 15. Open Wireshark 16. Click on the nav-item “your cart” 17. Look for http://testphp.vulnweb.com/cart.php 18. Then right click >Follow>TCP Stream
Request	 GET /cart.php HTTP/1.1 Host: testphp.vulnweb.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 Referer: http://testphp.vulnweb.com/index.php Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
Response	 HTTP/1.1 200 OK Server: nginx/1.19.0 Date: Thu, 21 Sep 2023 04:39:34 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 Content-Encoding: gzip
Analysis	1. Transmission Control Protocol, Src Port: 50105, Dst Port: 80, Seq: 1, Ack: 1, Len: 489 2. Internet Protocol Version 4, Src: 192.168.1.195, Dst: 44.228.249.3 3. Frame 58: 543 bytes on wire (4344 bits), 543 bytes captured (4344 bits) on interface \Device\NPF_{B2F39B3B-01F5-4FB7-BAB6-C642BE981D95}, id 0

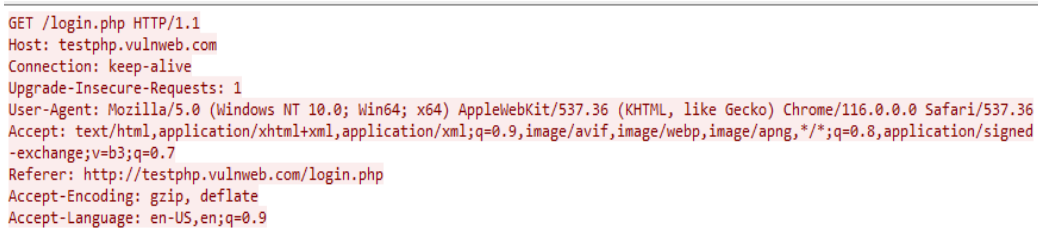
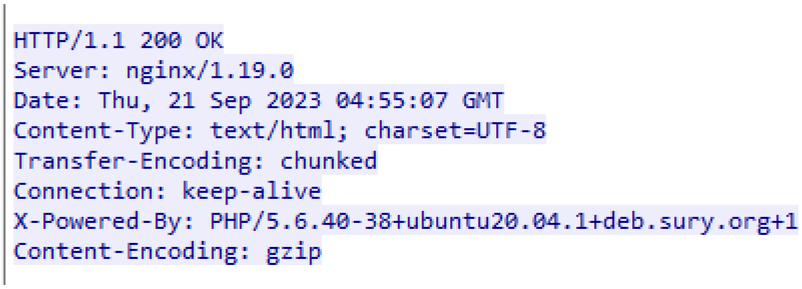
2.6 Description of Observation (Tabular form)

Observation Title (Test Case)	Verification of nav-item ‘guestbook’ by clicking on it from the navigation menu
Reference No	TC006
Host Name	testphp.vulnweb.com
Test Data	http://testphp.vulnweb.com/guestbook.php
Proof of Concept	Reproducing Steps: 1. Goto the URL “http://testphp.vulnweb.com/” 2. Identify the navigation menu 3. Open Wireshark 4. Click on the nav-item “guestbook” 5. Look for http://testphp.vulnweb.com/guestbook.php 6. Then right click >Follow>TCP Stream
Request	 GET /guestbook.php HTTP/1.1 Host: testphp.vulnweb.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 Referer: http://testphp.vulnweb.com/index.php Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
Response	 HTTP/1.1 200 OK Server: nginx/1.19.0 Date: Thu, 21 Sep 2023 04:39:56 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 Content-Encoding: gzip
Analysis	1. Transmission Control Protocol, Src Port: 50105, Dst Port: 80, Seq: 490, Ack: 2560, Len: 494 2. Internet Protocol Version 4, Src: 192.168.1.195, Dst: 44.228.249.3 3. Frame 157: 548 bytes on wire (4384 bits), 548 bytes captured (4384 bits) on interface \Device\NPF_{B2F39B3B-01F5-4FB7-BAB6-C642BE981D95}, id 0

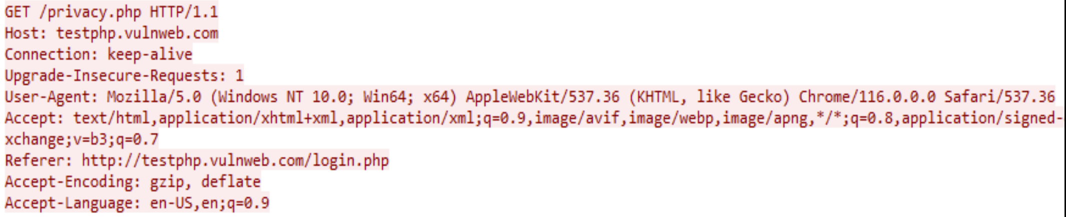
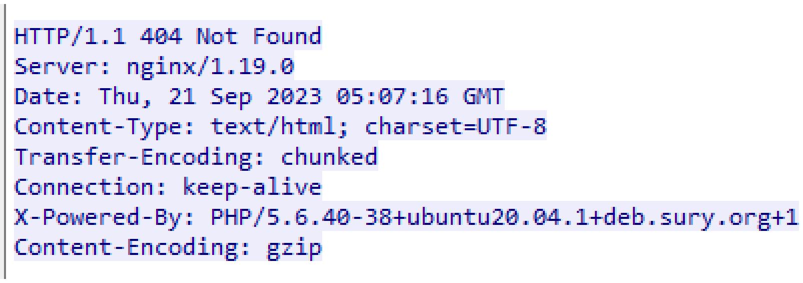
2.7 Description of Observation (Tabular form)

Observation Title (Test Case)	Verification of nav-item ‘AJAX Demo’ by clicking on it from the navigation menu
Reference No	TC007
Host Name	testphp.vulnweb.com
Test Data	http://testphp.vulnweb.com/AJAX/index.php
Proof of Concept	Reproducing Steps: 1. Goto the URL “http://testphp.vulnweb.com/” 2. Identify the navigation menu 3. Open Wireshark 4. Click on the nav-item “AJAX Demo” 5. Look for http://testphp.vulnweb.com/AJAX/index.php 6. Then right click >Follow>TCP Stream
Request	 GET /AJAX/index.php HTTP/1.1 Host: testphp.vulnweb.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 Referer: http://testphp.vulnweb.com/index.php Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
Response	 HTTP/1.1 200 OK Server: nginx/1.19.0 Date: Thu, 21 Sep 2023 04:40:08 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 Content-Encoding: gzip
Analysis	1. Transmission Control Protocol, Src Port: 50105, Dst Port: 80, Seq: 984, Ack: 5265, Len: 495 2. Internet Protocol Version 4, Src: 192.168.1.195, Dst: 44.228.249.3 3. Frame 286: 549 bytes on wire (4392 bits), 549 bytes captured (4392 bits) on interface \Device\NPF_{B2F39B3B-01F5-4FB7-BAB6-C642BE981D95}, id 0

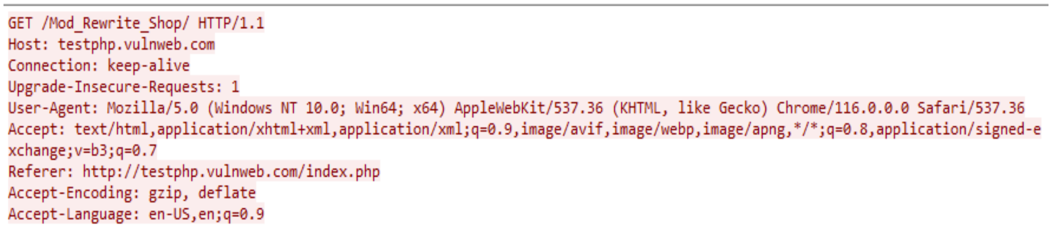
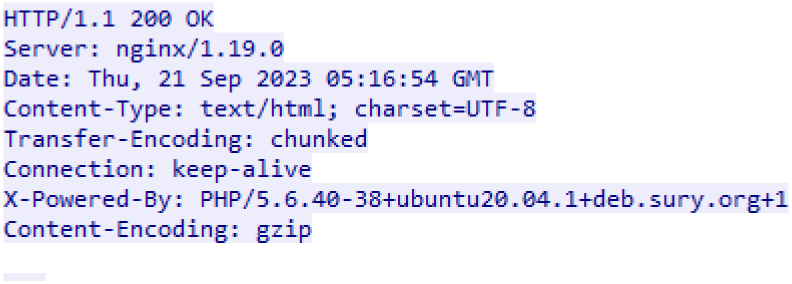
2.8 Description of Observation (Tabular form)

Observation Title (Test Case)	Verification of nav-item ‘Signup’ by clicking on it from the navigation menu
Reference No	TC008
Host Name	testphp.vulnweb.com
Test Data	http://testphp.vulnweb.com/login.php
Proof of Concept	Reproducing Steps: 1. Goto the URL “http://testphp.vulnweb.com/” 2. Identify the navigation menu 3. Open Wireshark 4. Click on the nav-item “Signup” 5. Look for http://testphp.vulnweb.com/login.php 6. Then right click >Follow>TCP Stream
Request	 GET /login.php HTTP/1.1 Host: testphp.vulnweb.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed -exchange;v=b3;q=0.7 Referer: http://testphp.vulnweb.com/login.php Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
Response	 HTTP/1.1 200 OK Server: nginx/1.19.0 Date: Thu, 21 Sep 2023 04:55:07 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 Content-Encoding: gzip
Analysis	1. Transmission Control Protocol, Src Port: 50139, Dst Port: 80, Seq: 1, Ack: 1, Len: 490 2. Internet Protocol Version 4, Src: 192.168.1.195, Dst: 44.228.249.3 3. Frame 89: 544 bytes on wire (4352 bits), 544 bytes captured (4352 bits) on interface \Device\NPF_{B2F39B3B-01F5-4FB7-BAB6-C642BE981D95}, id 0

2.9 Description of Observation (Tabular form)

Observation Title (Test Case)	Verification of footer menu item “Privacy Policy” by clicking on it
Reference No	TC009
Host Name	testphp.vulnweb.com
Test Data	http://testphp.vulnweb.com/privacy.php
Proof of Concept	Reproducing Steps: 1. Goto the URL “http://testphp.vulnweb.com/” 2. Identify the navigation menu 3. Open Wireshark 4. Click on the nav-item “Privacy Policy” 5. Look for http://testphp.vulnweb.com/privacy.php 6. Then right click >Follow>TCP Stream
Request	 GET /privacy.php HTTP/1.1 Host: testphp.vulnweb.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 Referer: http://testphp.vulnweb.com/login.php Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
Response	 HTTP/1.1 404 Not Found Server: nginx/1.19.0 Date: Thu, 21 Sep 2023 05:07:16 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 Content-Encoding: gzip
Analysis	1. Transmission Control Protocol, Src Port: 50237, Dst Port: 80, Seq: 1, Ack: 1, Len: 492 2. Internet Protocol Version 4, Src: 192.168.1.195, Dst: 44.228.249.3 3. Frame 1504: 546 bytes on wire (4368 bits), 546 bytes captured (4368 bits) on interface \Device\NPF_{B2F39B3B-01F5-4FB7-BAB6-C642BE981D95}, id 0

2.10 Description of Observation (Tabular form)

Observation Title (Test Case)	Verification of footer menu item “Shop” by clicking on it
Reference No	TC0010
Host Name	testphp.vulnweb.com
Test Data	http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Proof of Concept	Reproducing Steps: 1. Goto the URL “http://testphp.vulnweb.com/” 2. Identify the navigation menu 3. Open Wireshark 4. Click on the nav-item “artists” 5. Look for http://testphp.vulnweb.com/Mod_Rewrite_Shop/ 6. Then right click >Follow>TCP Stream
Request	 GET /Mod_Rewrite_Shop/ HTTP/1.1 Host: testphp.vulnweb.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 Referer: http://testphp.vulnweb.com/index.php Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
Response	 HTTP/1.1 200 OK Server: nginx/1.19.0 Date: Thu, 21 Sep 2023 05:16:54 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 Content-Encoding: gzip
Analysis	1. Transmission Control Protocol, Src Port: 50291, Dst Port: 80, Seq: 1, Ack: 1, Len: 498 2. Internet Protocol Version 4, Src: 192.168.1.195, Dst: 44.228.249.3 3. Frame 121: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface \Device\NPF_{B2F39B3B-01F5-4FB7-BAB6-C642BE981D95}, id 0

3 Conclusion: We have analyzed the network which is used to browse the website. We also record every request & response of the network regarding this website. Then we have handed over the report to concerned team. Now we are waiting eagerly for their feedback.