

Client:  
Testphp.vulnweb.com

Audited by : NIKUL PATEL  
(ShadowFox Security)

Task Level: Beginner level

Security audit for Testphp.vulnweb.com

Prepared and audited by **NIKUL**  
**PATEL** Team ShadowFox Batch 1

(June)

## Table of contents

1. Introduction .....	
2. Planning and Scoping .....	
3. Task 1 .....	
4. Task 2 .....	
5. Task 3 .....	

## Introduction:

**Testphp.vulnweb.com** is a deliberately vulnerable web application created by Acunetix for security testing and educational purposes. It is used by security professionals, developers, and students to practice and learn about web application security vulnerabilities.

## Key Features:

1. **Purpose:** A testing ground for web vulnerabilities, helping users understand how these can be exploited and fixed.
2. **Vulnerabilities:** Contains intentional flaws like SQL injection, cross-site scripting (XSS), file inclusion, and command injection.
3. **Educational Tool:** Provides hands-on learning for penetration testing, vulnerability assessment, and secure coding.
4. **Ethical Use:** Designed for educational purposes only, and should not be used against real- world systems without permission.
5. **Accessibility:** Freely accessible online for anyone interested in web security.
6. **Up-to-Date:** Regularly maintained to reflect current security trends.
7. **Community:** Supported by a community that shares knowledge and challenges in web security testing.

## Technical Information:

- **Server-Side Scripting:** Uses PHP.
- **Database:** Utilizes MySQL or a similar relational database.
- **Web Server:** Runs on a server like Apache or Nginx that supports PHP.

## Planning and Scoping the test:

**Testphp.vulnweb.com** is not a real online store. Instead, it's an example PHP application designed to be intentionally vulnerable to web attacks.

### Purpose:

- **Testing:** It's made for testing with Acunetix, a web security tool.
- **Learning:** It helps you see how developer mistakes and poor configurations can allow someone to hack into a website.

This site is a safe place to learn about and practice web security.

All the possible attacks that can be tested here are:

1. SQL Injection
2. Cross site scripting (XSS)
3. Cross-Site request forgery
4. Man-in-the-Middle attack

Client:  
Testphp.vulnweb.com

Audited by : NIKUL PATEL  
(ShadowFox Security)

Implementing the attack:

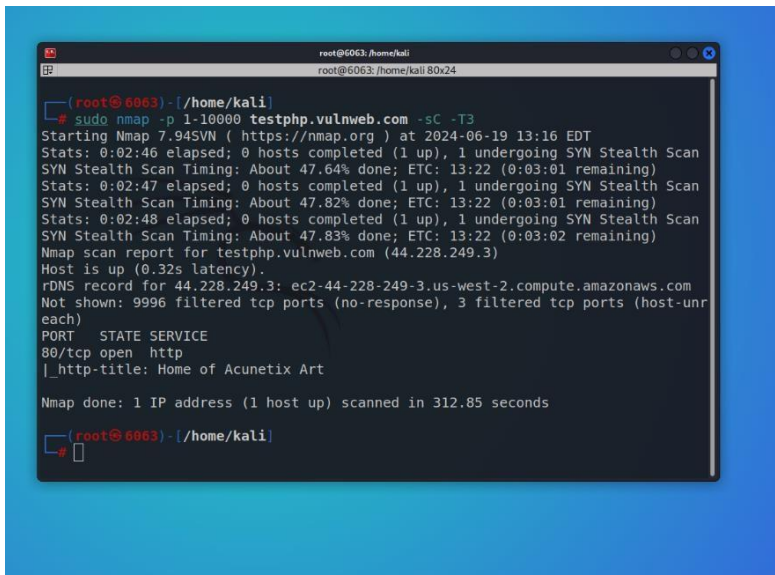
Task 1: Find all the ports that are open on the website  
<http://testphp.vulnweb.com/>

Requirements: Operating System, nmap, stable internet connection.

Step 1: Running the nmap scan for finding potential loopholes for entry points Command:

Sudo nmap -p 1-10000 testphp.vulnweb.com -sC -T3

POC:



```
root@6063:/home/kali
root@6063:/home/kali 80x24

(root@6063) - [/home/kali]
# sudo nmap -p 1-10000 testphp.vulnweb.com -sC -T3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-19 13:16 EDT
Stats: 0:02:46 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 47.64% done; ETC: 13:22 (0:03:01 remaining)
Stats: 0:02:47 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 47.82% done; ETC: 13:22 (0:03:01 remaining)
Stats: 0:02:48 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 47.83% done; ETC: 13:22 (0:03:02 remaining)
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.32s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 9996 filtered tcp ports (no-response), 3 filtered tcp ports (host-unr
each)
PORT      STATE SERVICE
80/tcp    open  http
|_http-title: Home of Acunetix Art

Nmap done: 1 IP address (1 host up) scanned in 312.85 seconds

(root@6063) - [/home/kali]
#
```

Client:  
Testphp.vulnweb.com

Audited by : NIKUL PATEL  
(ShadowFox Security)

## Port Scanning Findings:

PORT STATE SERVICE

80/tcp open http

|\_http-title: Home of Acunetix Art

## Vulnerability:

Cryptographic Failure (Severity: Medium)

The site does not use HTTPS, which is a more secure communication protocol than HTTP.

Without HTTPS, data transmission is not encrypted, making it possible for attackers to intercept and read the information being sent. This vulnerability increases the risk of man-in-the-middle attacks, which can be highly problematic for organizations.

The attacks which can be possible

1. Man-in-the-middle-attack
2. Network tracerouting
3. Packet sniffing

Later in task 3 we will try to understand how the packets could be sniffed over unsecure http traffic.

Task 2: Brute force the website <http://testphp.vulnweb.com/> and find the directories that are present in the website.

Requirements: Operating System, Dir buster or go buster, stable internet connection

Step 1: Brute forcing the available directories using drib tool

**Dirb** is a command-line tool used in web security assessments to discover hidden web content

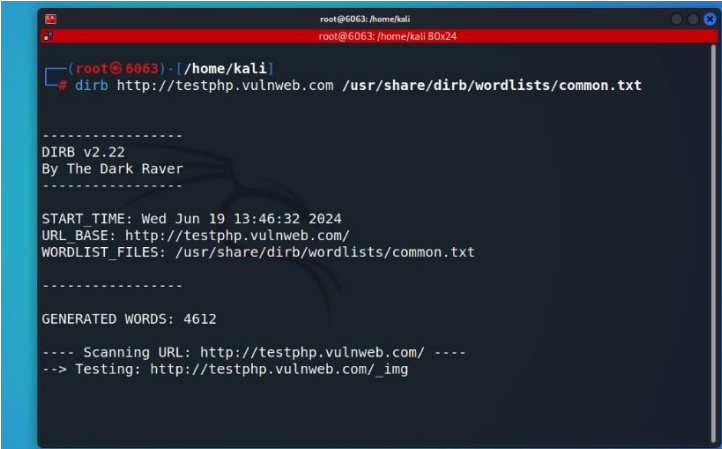
Command:

Client:  
Testphp.vulnweb.com

Audited by : NIKUL PATEL  
(ShadowFox Security)

dirb <http://testphp.vulnweb.com> --wordlist=usr/share/dirb/common.txt

POC:



```
root@6063:/home/kali
root@6063:/home/kali 80x24

(root@6063)-[/home/kali]
# dirb http://testphp.vulnweb.com /usr/share/dirb/wordlists/common.txt

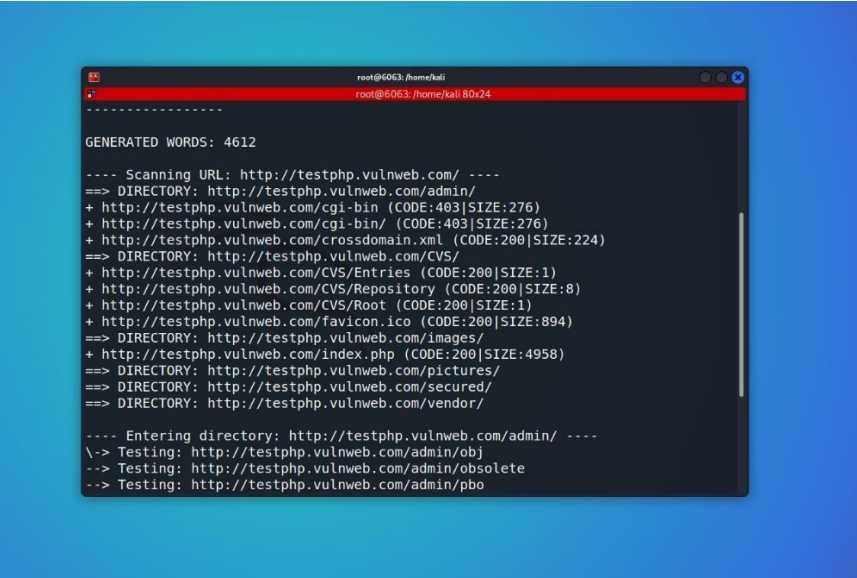
-----
DIRB v2.22
By The Dark Raver
-----

START TIME: Wed Jun 19 13:46:32 2024
URL_BASE: http://testphp.vulnweb.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

---- Scanning URL: http://testphp.vulnweb.com/ ----
--> Testing: http://testphp.vulnweb.com/_img
```



```
-----
GENERATED WORDS: 4612

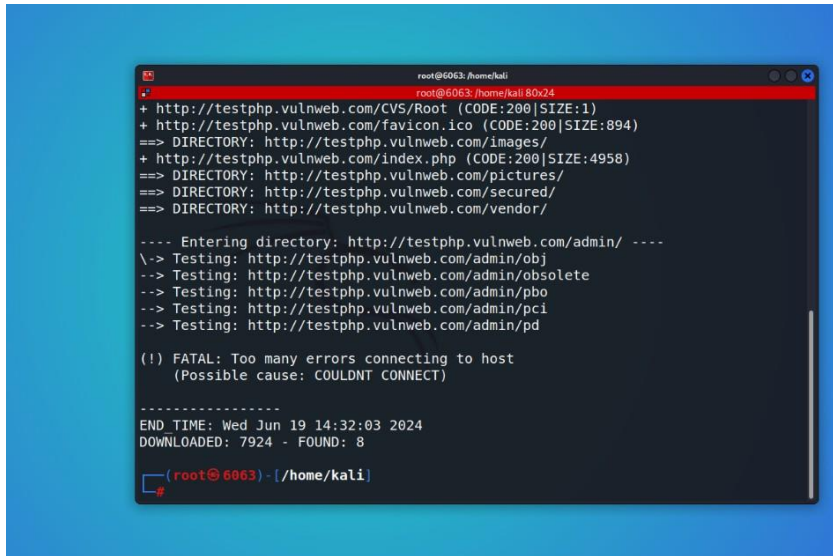
---- Scanning URL: http://testphp.vulnweb.com/ ----
==> DIRECTORY: http://testphp.vulnweb.com/admin/
+ http://testphp.vulnweb.com/cgi-bin (CODE:403|SIZE:276)
+ http://testphp.vulnweb.com/cgi-bin/ (CODE:403|SIZE:276)
+ http://testphp.vulnweb.com/crossdomain.xml (CODE:200|SIZE:224)
==> DIRECTORY: http://testphp.vulnweb.com/CSV/
+ http://testphp.vulnweb.com/CSV/Entries (CODE:200|SIZE:1)
+ http://testphp.vulnweb.com/CSV/Repository (CODE:200|SIZE:8)
+ http://testphp.vulnweb.com/CSV/Root (CODE:200|SIZE:1)
+ http://testphp.vulnweb.com/favicon.ico (CODE:200|SIZE:894)
==> DIRECTORY: http://testphp.vulnweb.com/images/
+ http://testphp.vulnweb.com/index.php (CODE:200|SIZE:4958)
==> DIRECTORY: http://testphp.vulnweb.com/pictures/
==> DIRECTORY: http://testphp.vulnweb.com/secured/
==> DIRECTORY: http://testphp.vulnweb.com/vendor/

---- Entering directory: http://testphp.vulnweb.com/admin/ ----
\> Testing: http://testphp.vulnweb.com/admin/obj
--> Testing: http://testphp.vulnweb.com/admin/obsolete
--> Testing: http://testphp.vulnweb.com/admin/pbo
```



Client:  
Testphp.vulnweb.com

Audited by : NIKUL PATEL  
(ShadowFox Security)



```
root@6063: /home/kali
+ http://testphp.vulnweb.com/ CVS/Root (CODE:200|SIZE:1)
+ http://testphp.vulnweb.com/favicon.ico (CODE:200|SIZE:894)
==> DIRECTORY: http://testphp.vulnweb.com/images/
+ http://testphp.vulnweb.com/index.php (CODE:200|SIZE:4958)
==> DIRECTORY: http://testphp.vulnweb.com/pictures/
==> DIRECTORY: http://testphp.vulnweb.com/secured/
==> DIRECTORY: http://testphp.vulnweb.com/vendor/

---- Entering directory: http://testphp.vulnweb.com/admin/ ----
\-> Testing: http://testphp.vulnweb.com/admin/obj
--> Testing: http://testphp.vulnweb.com/admin/obsolete
--> Testing: http://testphp.vulnweb.com/admin/pbo
--> Testing: http://testphp.vulnweb.com/admin/pci
--> Testing: http://testphp.vulnweb.com/admin/pd

(!) FATAL: Too many errors connecting to host
(Possible cause: COULDNT CONNECT)

-----
END TIME: Wed Jun 19 14:32:03 2024
DOWNLOADED: 7924 - FOUND: 8

root@6063 - [ /home/kali ]
```

Traversing all the paths of testphp.vulnweb.com

Access to the ADMIN login panel:

Got the access to the database  
(Severity : Critical)

==>DIRECTORY: http://testphp.vulnweb.com/admin/

Forbidden by the WAF Firewall:

+ http://testphp.vulnweb.com/cgi-bin (CODE:403|SIZE:276)

+ http://testphp.vulnweb.com/cgi-bin/ (CODE:403|SIZE:276)

Status code 200 OK paths:

+ http://testphp.vulnweb.com/crossdomain.xml (CODE:200|SIZE:224)

Reveals information about nginx server and it's version (nginx/1.19.0)  
(Severity=Low-Medium)

Access to the directories available at website like

1. Root
2. Entries
3. Repository
4. Favicon.ico
5. Index.php

Client:  
Testphp.vulnweb.com

Audited by : NIKUL PATEL  
(ShadowFox Security)

(Severity: High)

==> DIRECTORY: http://testphp.vulnweb.com/CVS/

+ http://testphp.vulnweb.com/CVS/Entries (CODE:200|SIZE:1)

+ http://testphp.vulnweb.com/CVS/Repository (CODE:200|SIZE:8)

+ http://testphp.vulnweb.com/CVS/Root (CODE:200|SIZE:1)

+ http://testphp.vulnweb.com/favicon.ico (CODE:200|SIZE:894)

==> DIRECTORY: http://testphp.vulnweb.com/images/

+ http://testphp.vulnweb.com/index.php (CODE:200|SIZE:4958)

==> DIRECTORY: http://testphp.vulnweb.com/pictures/

==> DIRECTORY: http://testphp.vulnweb.com/secured/

==> DIRECTORY: http://testphp.vulnweb.com/vendor/

END\_TIME: Wed Jun 19 14:32:03 2024

DOWNLOADED: 7924 - FOUND: 8

Date:11/06/2024

Task 3: Make a login in the website <http://testphp.vulnweb.com/> and intercept the network traffic using Wireshark and find the credentials that were transferred through the network.

Requirements: Operating System, Wireshark, Stable Internet Connection, basic understanding of Wireshark and packet capturing.

Wireshark is a tool that helps you see what's happening on a computer network.

It captures all the data passing through and lets you look closely at each piece of information, like a detective examining clues. You can see where data comes from, where it's going, and what kind of data it is, like emails or web pages

Client:  
Testphp.vulnweb.com

Audited by : NIKUL PATEL  
(ShadowFox Security)

This website is prone to man-in-the-middle attack. The attacker can use this vulnerability to sniff the packets transfer over the http protocol.

However, here is the POC

POC:

Step1: on the signup page and try to login with default credentials that are provided below.

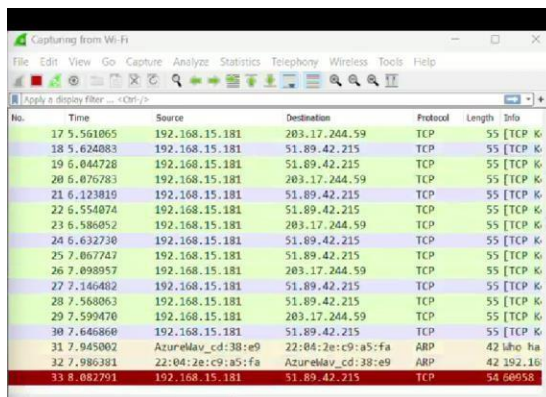
The screenshot displays a web browser window on the left and a Wireshark packet capture window on the right. The browser window shows the login page of 'Acunetix acuart'. The page has a search bar, navigation links (home, categories, artists, disclaimer, your cart, guestbook, AJAX Demo), and a login section. The login section includes fields for 'Username' (containing 'nikul') and 'Password' (containing 'test'), and a 'login' button. Below the login fields, there is a message: 'You can also signup here. Signup disabled. Please use the username test and the password test.' The Wireshark window is titled 'Capturing from Wi-Fi' and shows a list of captured packets. The selected packet is a TCP packet from 192.168.15.181 to 203.17.244.59, port 80, with a length of 55 bytes. The packet details pane shows the following structure: Ethernet II, Src: 22:04:2e:c9:a5:fa (22:04:2e:c9:a5:fa), Dst: 08:00:20:3a:ff:fe (08:00:20:3a:ff:fe), Internet Protocol Version 6, Src: fe80::2004:40:c1:003a:bb75:61b3, Dst: fe80::2004:2e:c9:a5:fa, Internet Control Message Protocol v6.

Step2: Make sure to turn on the Wireshark to capture the packets before pressing login.

Date:11/06/2024

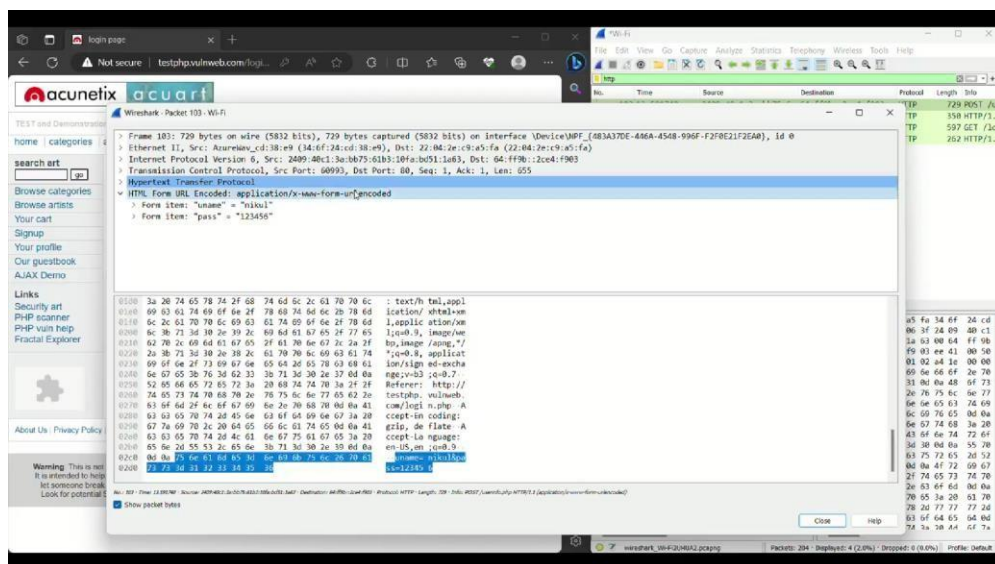
Client:  
Testphp.vulnweb.com

Audited by : NIKUL PATEL  
(ShadowFox Security)



No.	Time	Source	Destination	Protocol	Length	Info
17	5.561065	192.168.15.181	203.17.244.59	TCP	55	[TCP K...
18	5.624083	192.168.15.181	51.89.42.215	TCP	55	[TCP K...
19	6.044728	192.168.15.181	51.89.42.215	TCP	55	[TCP K...
20	6.076783	192.168.15.181	203.17.244.59	TCP	55	[TCP K...
21	6.123819	192.168.15.181	51.89.42.215	TCP	55	[TCP K...
22	6.554074	192.168.15.181	51.89.42.215	TCP	55	[TCP K...
23	6.586052	192.168.15.181	203.17.244.59	TCP	55	[TCP K...
24	6.632730	192.168.15.181	51.89.42.215	TCP	55	[TCP K...
25	7.067747	192.168.15.181	51.89.42.215	TCP	55	[TCP K...
26	7.098957	192.168.15.181	203.17.244.59	TCP	55	[TCP K...
27	7.146482	192.168.15.181	51.89.42.215	TCP	55	[TCP K...
28	7.568053	192.168.15.181	51.89.42.215	TCP	55	[TCP K...
29	7.599470	192.168.15.181	203.17.244.59	TCP	55	[TCP K...
30	7.646808	192.168.15.181	51.89.42.215	TCP	55	[TCP K...
31	7.945002	AzureMav.cd:38:e9	22:04:2e:c9:a5:fa	ARP	42	Who ha...
32	7.986381	22:04:2e:c9:a5:fa	AzureMav.cd:38:e9	ARP	42	192.16...
33	8.082791	192.168.15.181	51.89.42.215	TCP	54	60958

Step3: Analyze the captured packets and apply filter for specific http packets.



Wireshark - Packet 103 - Wi-Fi

Frame 103: 720 bytes on wire (5832 bits), 720 bytes captured (5832 bits) on interface \Device\NPF\_{483A370C-466A-4568-990F-F2F0E21F2EAB}, Id 0

Ethernet II, Src: AzureMav.cd:38:e9 (34:6f:24:cd:38:e9), Dst: 22:04:2e:c9:a5:fa (22:04:2e:c9:a5:fa)

Internet Protocol Version 6, Src: 2409:40c1:3a:b675:61b3:10fa:b51:1a83, Dst: 64:ff9b::2c04:f903

Transmission Control Protocol, Src Port: 60993, Dst Port: 80, Seq: 1, Ack: 1, Len: 655

Hypertext Transfer Protocol

HTML Form URL Encoded: application/x-www-form-urlencoded

Form item: "uname" = "nikul"

Form item: "pass" = "123456"

0100 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c : text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8,application/javascript;q=0.7

0100 69 03 61 74 69 6f 6e 2f 78 68 34 6d 6e 2b 79 6d : /static/js/dhtmlvm

0110 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 79 6d : ,application/xml

0200 6c 38 71 3d 10 2e 39 2c 69 6d 61 67 65 2f 77 65 : /js/0.9.1\_image/w

0210 62 78 2c 69 6d 61 67 65 2f 61 78 6e 67 2c 2a 2f : /js/image/comp.7

0220 2a 38 71 3d 30 2e 38 2c 61 79 70 6c 69 63 61 74 : /\*q=0.8,applicat

0230 69 6f 6e 2f 73 69 67 6e 65 64 2d 65 78 63 68 61 : ion/sign-ed-excha

0240 6e 67 65 3b 76 3d 62 33 3b 71 3d 30 2e 37 6d 6a : ngs;q=0.3;q=0.2

0250 52 65 66 65 72 65 72 3a 20 68 74 74 70 3a 2f 2f : Referer: http://

0260 34 65 73 74 70 68 78 2e 78 75 6c 6e 77 65 82 2c : testphp.vulnweb.

0270 61 6f 6d 2f 4c 6f 67 69 6e 2b 78 68 78 6d 6a 41 : /cm/legit.php-A

0280 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 : ccept-in coding: A

0290 67 7a 69 70 3c 20 64 65 66 6c 61 74 65 6a 6a 41 : gip, de flate-A

0300 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 : cept-la nguage:

0310 65 6e 2d 55 53 2c 65 6e 3b 71 3d 30 2e 39 6d 6a : en-us,en;q=0.0

0320 6d 6a 3b 6f 63 61 63 63 63 63 63 63 63 63 63 63 : /js/0.9.1\_image/w

0330 61 74 11 12 13 14 15 16 17 18 19 20 21 22 23 24 : /js/0.9.1\_image/w

Warning: This is not a warning! It is intended to help you find potential security issues. Look for potential security issues.

"In this scenario, the credentials we used to log in are exposed and easily readable within the packet."

Client:  
Testphp.vulnweb.com

Audited by : NIKUL PATEL  
(ShadowFox Security)

### Resources Used:

1. Operating System (Windows or Linux) Linux Preferred
2. Wireshark (Packet Sniffer)
3. Nmap (Network mapper)
4. Internet
5. OSINT (Open-Source Intelligence gathering)

Client:  
Testphp.vulnweb.com

Audited by : NIKUL PATEL  
(ShadowFox Security)