MINI PROJECT

Project 14 website: http://testphp.vulnweb.com/

SUBMITTED TO: - SUBMITTED BY: -

IBM ANANT KUMAR (GROUP-14)

University Roll No.-181530004

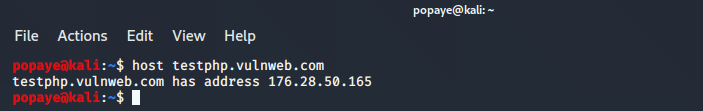
ABSTRACT

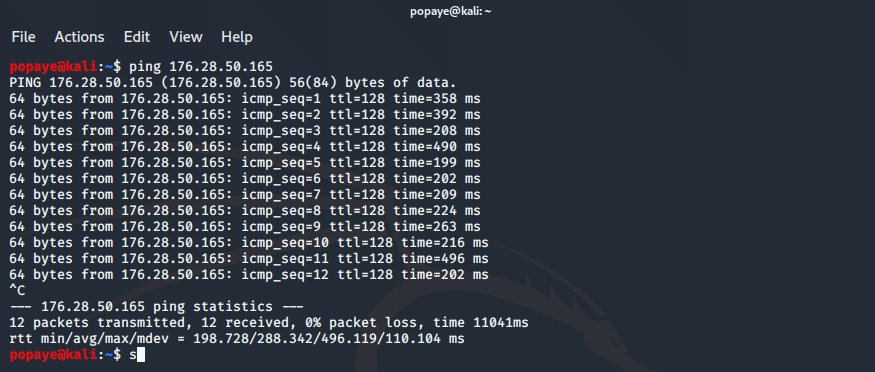
As many Web applications are developed daily and used extensively. It becomes important for developers and testers to improve these application securities. Pen testing, is a technique that helps developers and testers to ensure that the security levels of their Web application are at acceptable level to be used safely. Different tools are available for pen testing Web application; in this paper we have used many tools like dirb,dirbuster,nmap,nikto and burpsuit etc for the enumeration of vulnerabilities in the given Web site - http://testphp.vulnweb.com/

**Reconnaissance**

Host Discovery

One of the very first steps in any network reconnaissance mission is to reduce a (sometimes huge) set of IP ranges into a list of active or interesting hosts. Scanning every port of every single IP address is slow and usually unnecessary. Of course what makes a host interesting depends greatly on the scan purposes. Network administrators may only be interested in hosts running a certain service, while security auditors may care about every single device with an IP address. An administrator may be comfortable using just an ICMP ping to locate hosts on his internal network, while an external penetration tester may use a diverse set of dozens of probes in an attempt to evade firewall restrictions.

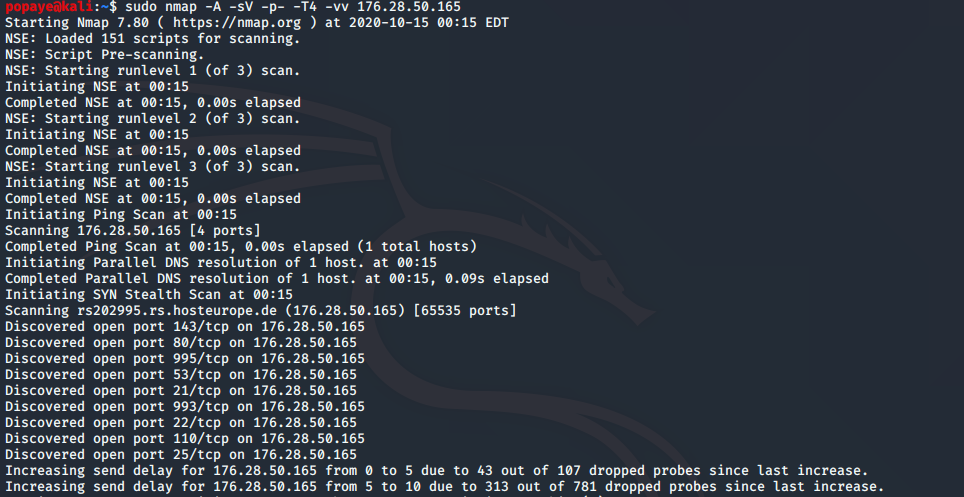




Nmap

Nmap is a network mapper that has emerged as one of the most popular, free network discovery tools on the market. Nmap is now one of the core tools used by network administrators to map their networks. The program can be used to find live hosts on a network, [perform port scanning](https://www.varonis.com/blog/port-scanning-techniques/" \t "_blank), ping sweeps, OS detection, and version detection.

A number of recent cyberattacks have re-focused attention on the type of network auditing that Nmap provides. Analysts have pointed out that the recent Capital One hack, for instance, [could have been detected sooner](https://www.sightline.com/how-the-capital-one-hack-could-have-been-detected-sooner/" \t "_blank) if system administrators had been monitoring connected devices.



Web Server Scanning with Nikto Scanner

There is a number of [online vulnerability scanner](https://geekflare.com/saas-web-vulnerability-scanner/) to test your web applications on the Internet. However, if you are looking to test Intranet applications or in-house applications, then you can use the Nikto web scanner.

[Nikto](https://github.com/sullo/nikto" \t "_blank) is an open-source scanner and you can use it with any web servers (Apache, Nginx, IHS, OHS, Litespeed, etc.). Sounds like a perfect in-house tool for web server scanning. It is capable of scanning for over 6700 items to detect misconfiguration, risky files, etc. and some of the features include;

You can save the report in HTML, XML, CSV

It supports SSL

Scan multiple ports on the server

[Find subdomain](https://geekflare.com/find-subdomains/)

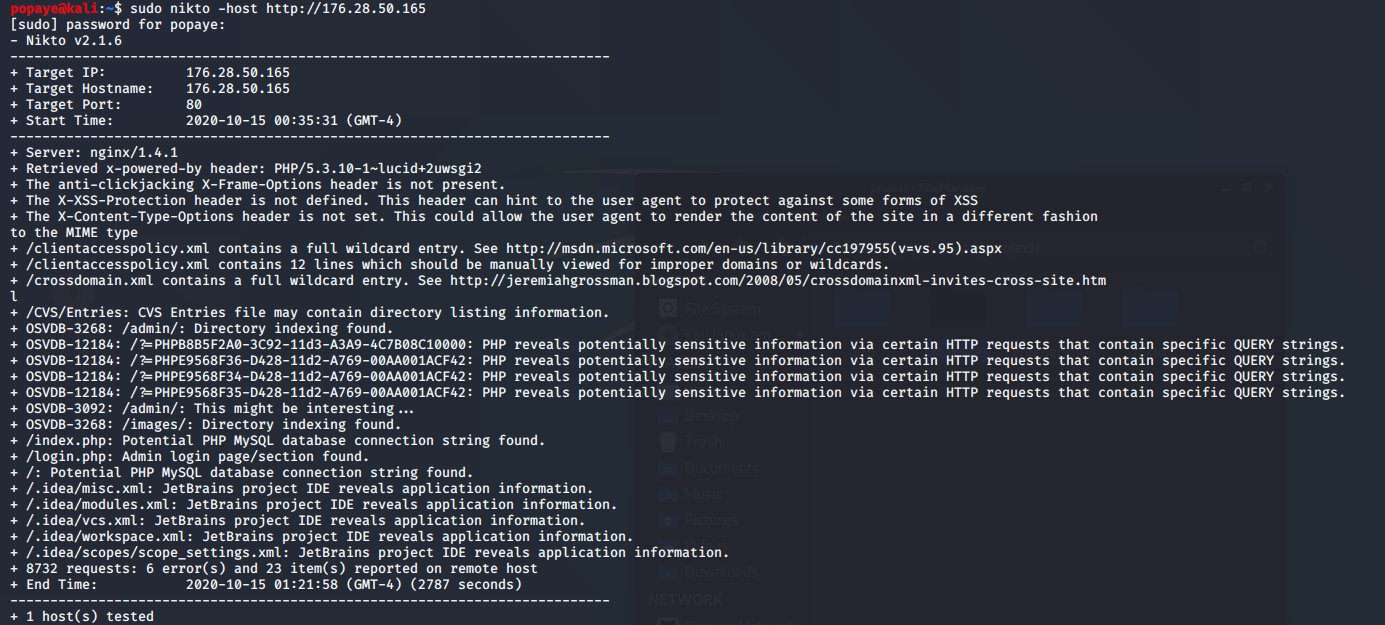
Apache user enumeration

Checks for outdated components

Detect parking sites

Using Nikto Scan in Kali linux

Go to Applications >> Vulnerability Analysis and click nikto



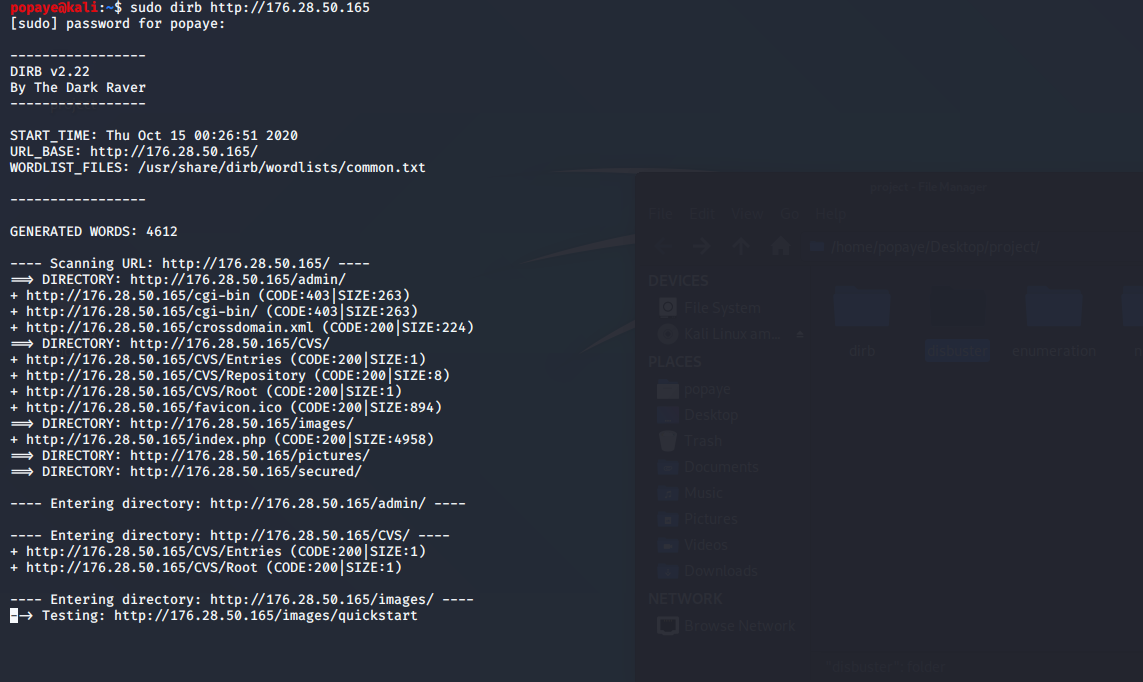
Directory scanning with gobuster, dirbuster and dirb

DIRB

DIRB is a Web Content Scanner. It looks for existing (and/or hidden) Web Objects. It basically works by launching a dictionary based attack against a web server and analyzing the response.

DIRB comes with a set of preconfigured attack wordlists for easy usage but you can use your custom wordlists. Also DIRB sometimes can be used as a classic CGI scanner, but remember is a content scanner not a vulnerability scanner.

DIRB main purpose is to help in professional web application auditing. Specially in security related testing. It covers some holes not covered by classic web vulnerability scanners. DIRB looks for specific web objects that other generic CGI scanners can’t look for. It doesn’t search vulnerabilities nor does it look for web contents that can be vulnerable.



GOBUSTER

Some of the directories and files found during dirbuster scan in the given website are as follows: -

Directories found during testing:

Dirs found with a 200 response:

/images/

/admin/

/pictures/

/AJAX/

/Mod\_Rewrite\_Shop/

/hpp/

/Flash/

/Mod\_Rewrite\_Shop/images/

/secured/

Dirs found with a 403 response:

/cgi-bin/

Files found during testing:

Files found with a 200 response:

/index.php

/search.php

/login.php

/product.php

/disclaimer.php

/signup.php

/categories.php

/cart.php

/artists.php

/guestbook.php

/AJAX/index.php

/Mod\_Rewrite\_Shop/index.php

/Flash/add.swf

/hpp/index.php

/AJAX/categories.php

/Mod\_Rewrite\_Shop/buy.php

/Mod\_Rewrite\_Shop/details.php

/logout.php

/hpp/test.php

/404.php

/AJAX/titles.php

/Mod\_Rewrite\_Shop/rate.php

/AJAX/artists.php

/hpp/params.php

/secured/index.php

Files found with a 302 response:

/comment.php

/userinfo.php

/redir.php

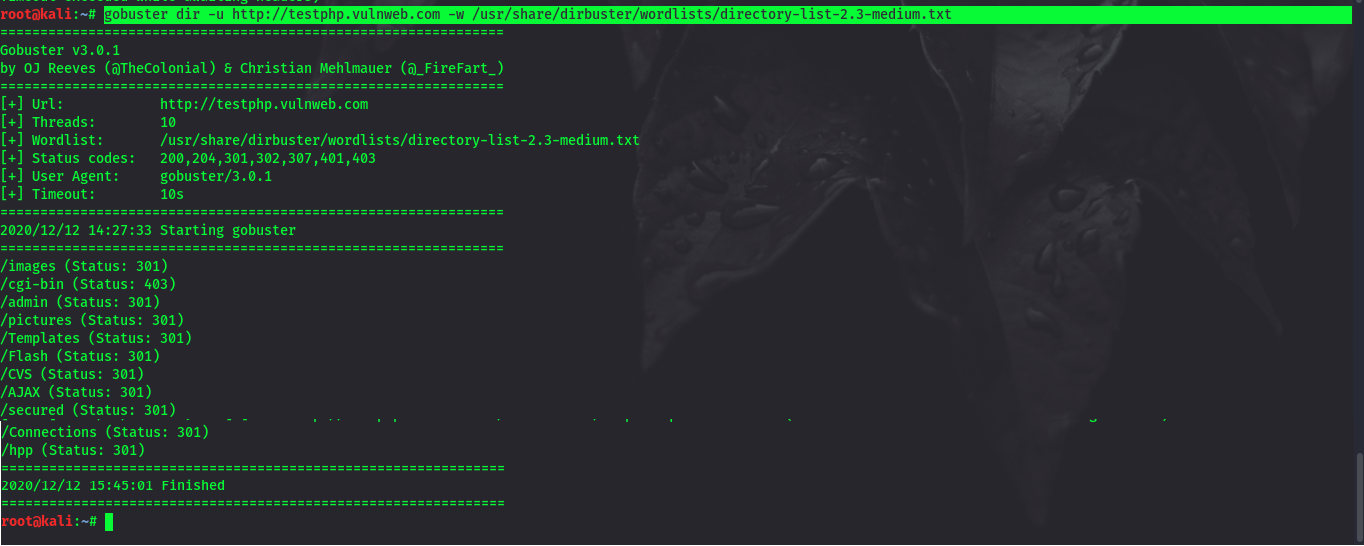
DIRBUSTER

One of the first steps in attacking a [web application](https://null-byte.wonderhowto.com/how-to/hacking-web-apps/) is enumerating hidden directories and files. Doing so can often yield valuable information that makes it easier to execute a precise attack, leaving less room for errors and wasted time. There are many tools available to do this, but not all of them are created equally. Gobuster, a directory scanner written in [Go](https://www.amazon.de/Programming-Language-Addison-Wesley-Professional-Computing-ebook/dp/B0184N7WWS/?tag=wnbde-21&language=en_GB" \t "_blank), is definitely worth exploring.

Traditional directory [brute-force](https://null-byte.wonderhowto.com/how-to/brute-force-nearly-any-website-login-with-hatch-0192225/) scanners like [DirBuster](https://null-byte.wonderhowto.com/how-to/hack-like-pro-find-directories-websites-using-dirbuster-0157593/) and [DIRB](https://null-byte.wonderhowto.com/how-to/hack-like-pro-hack-web-apps-part-7-finding-hidden-objects-with-dirb-0168596/) work just fine, but can often be slow and prone to errors. [Gobuster](https://tools.kali.org/web-applications/gobuster" \t "_blank) is a Go implementation of these tools and is offered in a convenient command-line format.

The main advantage Gobuster has over other directory scanners is speed. As a programming language, Go is known to be fast. It also has excellent support for [concurrency](https://www.amazon.de/Concurrency-Go-Tools-Techniques-Developers-ebook/dp/B0742NH2SG/?tag=wnbde-21&language=en_GB" \t "_blank) so that Gobuster can take advantage of multiple threads for faster processing.

The one downfall of Gobuster, though, is the lack of [recursive](https://knowyourmeme.com/photos/1246322-sweet-jesus-pooh-thats-not-honey" \t "_blank) directory searching. For directories more than one level deep, another scan will be needed, unfortunately. Often this isn't that big of a deal, and other scanners can step up and fill in the gaps for Gobuster in this area.



PHP VERSION

url:

http://testphp.vulnweb.com/secured/phpinfo.php

Sensitive informations:

This page may output a large amount of information about the current state of PHP using phpinfo() function. This includes information about PHP compilation options and extensions, the PHP version, server information and environment (if compiled as a module), the PHP environment, OS version information, paths, master and local values of configuration options, HTTP headers, and the PHP License. Remediation Remove the file from production systems.

|  |
| --- |
| [PHP Logo](http://www.php.net/)  PHP Version 5.1.6 |

|  |  |
| --- | --- |
| System | FreeBSD svn.local 6.2-RELEASE FreeBSD 6.2-RELEASE #0: Fri Jan 12 10:40:27 UTC 2007 [root@dessler.cse.buffalo.edu:/usr/obj/usr/src/sys/GENERIC i386](mailto:root@dessler.cse.buffalo.edu:/usr/obj/usr/src/sys/GENERIC%20i386) |
| Build Date | Jul 30 2007 12:20:01 |
| Configure Command | './configure' '--enable-versioning' '--enable-memory-limit' '--with-layout=GNU' '--with-config-file-scan-dir=/usr/local/etc/php' '--disable-all' '--enable-libxml' '--with-libxml-dir=/usr/local' '--enable-reflection' '--enable-spl' '--program-prefix=' '--enable-fastcgi' '--with-apxs2=/usr/local/sbin/apxs' '--with-regex=php' '--with-zend-vm=CALL' '--disable-ipv6' '--prefix=/usr/local' 'i386-portbld-freebsd6.2' |
| Server API | Apache 2.0 Handler |
| Virtual Directory Support | Disabled |
| Configuration File (php.ini) Path | /usr/local/etc/php.ini |
| Scan this dir for additional .ini files | /usr/local/etc/php |
| additional .ini files parsed | /usr/local/etc/php/extensions.ini |
| PHP API | 20041225 |
| PHP Extension | 20050922 |
| Zend Extension | 220051025 |
| Debug Build | No |
| Thread Safety | Disabled |
| Zend Memory Manager | Enabled |
| IPv6 Support | Disabled |
| Registered PHP Streams | php, file, http, ftp, https, ftps, compress.zlib |
| Registered Stream Socket Transports | tcp, udp, unix, udg, ssl, sslv3, sslv2, tls |
| Registered Stream Filters | string.rot13, string.toupper, string.tolower, string.strip\_tags, convert.\*, consumed, convert.iconv.\*, zlib.\* |

|  |
| --- |
| [Zend logo](http://www.zend.com/)This program makes use of the Zend Scripting Language Engine: Zend Engine v2.1.0, Copyright (c) 1998-2006 Zend Technologies |

[PHP Credits](http://testphp.vulnweb.com/secured/phpinfo.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000)

Configuration

PHP Core

|  |  |  |
| --- | --- | --- |
| Directive | Local Value | Master Value |
| allow\_call\_time\_pass\_reference | On | On |
| allow\_url\_fopen | On | On |
| always\_populate\_raw\_post\_data | Off | Off |
| arg\_separator.input | & | & |
| arg\_separator.output | & | & |
| asp\_tags | Off | Off |
| auto\_append\_file | *no value* | *no value* |
| auto\_globals\_jit | On | On |
| auto\_prepend\_file | *no value* | *no value* |
| Browscap | *no value* | *no value* |
| default\_charset | *no value* | *no value* |
| default\_mimetype | text/html | text/html |
| define\_syslog\_variables | Off | Off |
| disable\_classes | *no value* | *no value* |
| disable\_functions | *no value* | *no value* |
| display\_errors | On | On |
| display\_startup\_errors | Off | Off |
| doc\_root | *no value* | *no value* |
| docref\_ext | *no value* | *no value* |
| docref\_root | *no value* | *no value* |
| enable\_dl | On | On |
| error\_append\_string | *no value* | *no value* |
| error\_log | *no value* | *no value* |
| error\_prepend\_string | *no value* | *no value* |
| error\_reporting | 2039 | 2039 |
| expose\_php | On | On |
| extension\_dir | /usr/local/lib/php/20050922 | /usr/local/lib/php/20050922 |
| file\_uploads | On | On |
| highlight.bg | #FFFFFF | #FFFFFF |
| highlight.comment | #FF8000 | #FF8000 |
| highlight.default | #0000BB | #0000BB |
| highlight.html | #000000 | #000000 |
| highlight.keyword | #007700 | #007700 |
| highlight.string | #DD0000 | #DD0000 |
| html\_errors | On | On |
| ignore\_repeated\_errors | Off | Off |
| ignore\_repeated\_source | Off | Off |
| ignore\_user\_abort | Off | Off |
| implicit\_flush | Off | Off |
| include\_path | .: | .: |
| log\_errors | Off | Off |
| log\_errors\_max\_len | 1024 | 1024 |
| magic\_quotes\_gpc | Off | Off |
| magic\_quotes\_runtime | Off | Off |
| magic\_quotes\_sybase | Off | Off |
| mail.force\_extra\_parameters | *no value* | *no value* |
| max\_execution\_time | 30 | 30 |
| max\_input\_time | 60 | 60 |
| memory\_limit | 8M | 8M |
| open\_basedir | *no value* | *no value* |
| output\_buffering | *no value* | *no value* |
| output\_handler | *no value* | *no value* |
| post\_max\_size | 8M | 8M |
| precision | 12 | 12 |
| realpath\_cache\_size | 16K | 16K |
| realpath\_cache\_ttl | 120 | 120 |
| register\_argc\_argv | On | On |
| register\_globals | Off | Off |
| register\_long\_arrays | On | On |
| report\_memleaks | On | On |
| report\_zend\_debug | On | On |
| safe\_mode | Off | Off |
| safe\_mode\_exec\_dir | *no value* | *no value* |
| safe\_mode\_gid | Off | Off |
| safe\_mode\_include\_dir | *no value* | *no value* |
| sendmail\_from | *no value* | *no value* |
| sendmail\_path | /usr/sbin/sendmail -t -i | /usr/sbin/sendmail -t -i |
| serialize\_precision | 100 | 100 |
| short\_open\_tag | On | On |
| SMTP | localhost | localhost |
| smtp\_port | 25 | 25 |
| sql.safe\_mode | Off | Off |
| track\_errors | Off | Off |
| unserialize\_callback\_func | *no value* | *no value* |
| upload\_max\_filesize | 2M | 2M |
| upload\_tmp\_dir | *no value* | *no value* |
| user\_dir | *no value* | *no value* |
| variables\_order | EGPCS | EGPCS |
| xmlrpc\_error\_number | 0 | 0 |
| xmlrpc\_errors | Off | Off |
| y2k\_compliance | On | On |
| zend.ze1\_compatibility\_mode | Off | Off |

apache2handler

|  |  |
| --- | --- |
| Apache Version | Apache/2.2.3 (FreeBSD) DAV/2 PHP/5.1.6 mod\_ssl/2.2.3 OpenSSL/0.9.7e-p1 |
| Apache API Version | 20051115 |
| Server Administrator | [root@localhost.localdomain](mailto:root@localhost.localdomain) |
| Hostname:Port | acuart:0 |
| User/Group | www(80)/80 |
| Max Requests | Per Child: 10000 - Keep Alive: on - Max Per Connection: 100 |
| Timeouts | Connection: 300 - Keep-Alive: 5 |
| Virtual Server | Yes |
| Server Root | /usr/local |
| Loaded Modules | core prefork http\_core mod\_so mod\_authn\_file mod\_authn\_dbm mod\_authn\_anon mod\_authn\_default mod\_authn\_alias mod\_authz\_host mod\_authz\_groupfile mod\_authz\_user mod\_authz\_dbm mod\_authz\_owner mod\_authz\_default mod\_auth\_basic mod\_auth\_digest mod\_file\_cache mod\_cache mod\_disk\_cache mod\_include mod\_filter mod\_charset\_lite mod\_deflate mod\_log\_config mod\_logio mod\_env mod\_mime\_magic mod\_cern\_meta mod\_expires mod\_headers mod\_usertrack mod\_setenvif mod\_version mod\_ssl mod\_mime mod\_dav mod\_status mod\_autoindex mod\_asis mod\_info mod\_cgi mod\_dav\_fs mod\_vhost\_alias mod\_negotiation mod\_dir mod\_imagemap mod\_actions mod\_speling mod\_userdir mod\_alias mod\_rewrite mod\_php5 |

|  |  |  |
| --- | --- | --- |
| Directive | Local Value | Master Value |
| engine | 1 | 1 |
| last\_modified | 0 | 0 |
| xbithack | 0 | 0 |

ctype

|  |  |
| --- | --- |
| ctype functions | Enabled |

curl

|  |  |
| --- | --- |
| CURL support | Enabled |
| CURL Information | libcurl/7.15.5 OpenSSL/0.9.7e zlib/1.2.3 |

|  |  |  |
| --- | --- | --- |
| Directive | Local Value | Master Value |
| date.default\_latitude | 31.7667 | 31.7667 |
| date.default\_longitude | 35.2333 | 35.2333 |
| date.sunrise\_zenith | 90.583333 | 90.583333 |
| date.sunset\_zenith | 90.583333 | 90.583333 |
| date.timezone | *no value* | *no value* |

dom

|  |  |
| --- | --- |
| DOM/XML | Enabled |
| DOM/XML API Version | 20031129 |
| libxml Version | 2.6.26 |
| HTML Support | Enabled |
| XPath Support | Enabled |
| XPointer Support | Enabled |
| Schema Support | Enabled |
| RelaxNG Support | Enabled |

exif

|  |  |
| --- | --- |
| EXIF Support | Enabled |
| EXIF Version | 1.4 $Id: exif.c,v 1.173.2.5 2006/04/10 18:23:24 helly Exp $ |
| Supported EXIF Version | 0220 |
| Supported filetypes | JPEG,TIFF |

ftp

|  |  |
| --- | --- |
| FTP support | Enabled |

gd

|  |  |
| --- | --- |
| GD Support | Enabled |
| GD Version | bundled (2.0.28 compatible) |
| FreeType Support | Enabled |
| FreeType Linkage | with freetype |
| FreeType Version | 2.2.1 |
| T1Lib Support | Enabled |
| GIF Read Support | Enabled |
| GIF Create Support | Enabled |
| JPG Support | Enabled |
| PNG Support | Enabled |
| WBMP Support | Enabled |
| XPM Support | Enabled |
| XBM Support | Enabled |

libxml

|  |  |
| --- | --- |
| libXML support | Active |
| libXML Version | 2.6.26 |
| libXML streams | Enabled |

mssql

|  |  |
| --- | --- |
| MSSQL Support | enabled |
| Active Persistent Links | 0 |
| Active Links | 0 |
| Library version | FreeTDS |

mysql

|  |  |
| --- | --- |
| MySQL Support | enabled |
| Active Persistent Links | 0 |
| Active Links | 0 |
| Client API version | 5.1.11-beta |
| MYSQL\_MODULE\_TYPE | *no value* |
| MYSQL\_SOCKET | /tmp/mysql.sock |
| MYSQL\_INCLUDE | *no value* |
| MYSQL\_LIBS | *no value* |

|  |  |  |
| --- | --- | --- |
| Directive | Local Value | Master Value |
| mysql.allow\_persistent | On | On |
| mysql.connect\_timeout | 60 | 60 |
| mysql.default\_host | *no value* | *no value* |
| mysql.default\_password | *no value* | *no value* |
| mysql.default\_port | *no value* | *no value* |
| mysql.default\_socket | *no value* | *no value* |
| mysql.default\_user | *no value* | *no value* |
| mysql.max\_links | Unlimited | Unlimited |
| mysql.max\_persistent | Unlimited | Unlimited |
| mysql.trace\_mode | Off | Off |

openssl

|  |  |
| --- | --- |
| OpenSSL support | Enabled |
| OpenSSL Version | OpenSSL 0.9.7e-p1 25 Oct 2004 |

posix

|  |  |
| --- | --- |
| Revision | $Revision: 1.70.2.3 $ |

Reflection

|  |  |
| --- | --- |
| Reflection | Enabled |
| Version | $Id: php\_reflection.c,v 1.164.2.33 2006/03/29 14:28:42 tony2001 Exp $ |

session

|  |  |
| --- | --- |
| Session Support | Enabled |
| Registered save handlers | files user |
| Registered serializer handlers | php php\_binary |

|  |  |  |
| --- | --- | --- |
| Directive | Local Value | Master Value |
| session.auto\_start | Off | Off |
| session.bug\_compat\_42 | On | On |
| session.bug\_compat\_warn | On | On |
| session.cache\_expire | 180 | 180 |
| session.cache\_limiter | nocache | nocache |
| session.cookie\_domain | *no value* | *no value* |
| session.cookie\_lifetime | 0 | 0 |
| session.cookie\_path | / | / |
| session.cookie\_secure | Off | Off |
| session.entropy\_file | *no value* | *no value* |
| session.entropy\_length | 0 | 0 |
| session.gc\_divisor | 100 | 100 |
| session.gc\_maxlifetime | 1440 | 1440 |
| session.gc\_probability | 1 | 1 |
| session.hash\_bits\_per\_character | 4 | 4 |
| session.hash\_function | 0 | 0 |
| session.name | PHPSESSID | PHPSESSID |
| session.referer\_check | *no value* | *no value* |
| session.save\_handler | files | files |
| session.save\_path | *no value* | *no value* |
| session.serialize\_handler | php | php |
| session.use\_cookies | On | On |
| session.use\_only\_cookies | Off | Off |
| session.use\_trans\_sid | 0 | 0 |

SQLite

|  |  |
| --- | --- |
| SQLite support | Enabled |
| PECL Module version | 2.0-dev $Id: sqlite.c,v 1.166.2.13 2006/04/18 14:30:15 iliaa Exp $ |
| SQLite Library | 2.8.17 |
| SQLite Encoding | iso8859 |

|  |  |  |
| --- | --- | --- |
| Directive | Local Value | Master Value |
| sqlite.assoc\_case | 0 | 0 |

standard

|  |  |
| --- | --- |
| Regex Library | Bundled library enabled |
| Dynamic Library Support | Enabled |
| Path to sendmail | /usr/sbin/sendmail -t -i |

|  |  |  |
| --- | --- | --- |
| Directive | Local Value | Master Value |
| assert.active | 1 | 1 |
| assert.bail | 0 | 0 |
| assert.callback | *no value* | *no value* |
| assert.quiet\_eval | 0 | 0 |
| assert.warning | 1 | 1 |
| auto\_detect\_line\_endings | 0 | 0 |
| default\_socket\_timeout | 60 | 60 |
| safe\_mode\_allowed\_env\_vars | PHP\_ | PHP\_ |
| safe\_mode\_protected\_env\_vars | LD\_LIBRARY\_PATH | LD\_LIBRARY\_PATH |
| url\_rewriter.tags | a=href,area=href,frame=src,input=src,form=,fieldset= | a=href,area=href,frame=src,input=src,form=,fieldset= |
| user\_agent | *no value* | *no value* |

xml

|  |  |
| --- | --- |
| XML Support | active |
| XML Namespace Support | active |
| libxml2 Version | 2.6.26 |

xmlreader

|  |  |
| --- | --- |
| XMLReader | Enabled |

xmlwriter

|  |  |
| --- | --- |
| XMLWriter | Enabled |

xsl

|  |  |
| --- | --- |
| XSL | enabled |
| libxslt Version | 1.1.17 |
| libxslt compiled against libxml Version | 2.6.26 |
| EXSLT | enabled |
| libexslt Version | 1.1.17 |

Additional Modules

|  |
| --- |
| Module Name |

Environment

|  |  |
| --- | --- |
| Variable | Value |
| LD\_LIBRARY\_PATH | /usr/local/lib: |
| HOME | / |
| PATH | /sbin:/bin:/usr/sbin:/usr/bin |

PHP Variables

|  |  |
| --- | --- |
| Variable | Value |
| \_SERVER["HTTP\_HOST"] | Acuart |
| \_SERVER["HTTP\_USER\_AGENT"] | Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.11) Gecko/20071127 Firefox/2.0.0.11 |
| \_SERVER["HTTP\_ACCEPT"] | text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,\*/\*;q=0.5 |
| \_SERVER["HTTP\_ACCEPT\_LANGUAGE"] | en-us,en;q=0.5 |
| \_SERVER["HTTP\_ACCEPT\_ENCODING"] | gzip,deflate |
| \_SERVER["HTTP\_ACCEPT\_CHARSET"] | ISO-8859-1,utf-8;q=0.7,\*;q=0.7 |
| \_SERVER["HTTP\_KEEP\_ALIVE"] | 300 |
| \_SERVER["HTTP\_CONNECTION"] | keep-alive |
| \_SERVER["PATH"] | /sbin:/bin:/usr/sbin:/usr/bin |
| \_SERVER["SERVER\_SIGNATURE"] | *no value* |
| \_SERVER["SERVER\_SOFTWARE"] | Apache/2.2.3 (FreeBSD) DAV/2 PHP/5.1.6 mod\_ssl/2.2.3 OpenSSL/0.9.7e-p1 |
| \_SERVER["SERVER\_NAME"] | Acuart |
| \_SERVER["SERVER\_ADDR"] | 192.168.0.5 |
| \_SERVER["SERVER\_PORT"] | 80 |
| \_SERVER["REMOTE\_ADDR"] | 192.168.0.26 |
| \_SERVER["DOCUMENT\_ROOT"] | /var/www/acuart/ |
| \_SERVER["SERVER\_ADMIN"] | [root@localhost.localdomain](mailto:root@localhost.localdomain) |
| \_SERVER["SCRIPT\_FILENAME"] | /var/www/acuart/secured/phpinfo.php |
| \_SERVER["REMOTE\_PORT"] | 11493 |
| \_SERVER["GATEWAY\_INTERFACE"] | CGI/1.1 |
| \_SERVER["SERVER\_PROTOCOL"] | HTTP/1.1 |
| \_SERVER["REQUEST\_METHOD"] | GET |
| \_SERVER["QUERY\_STRING"] | *no value* |
| \_SERVER["REQUEST\_URI"] | /secured/phpinfo.php |
| \_SERVER["SCRIPT\_NAME"] | /secured/phpinfo.php |
| \_SERVER["PHP\_SELF"] | /secured/phpinfo.php |
| \_SERVER["REQUEST\_TIME"] | 1201867164 |
| \_SERVER["argv"] | Array |
| \_SERVER["argc"] | 0 |
| \_ENV["LD\_LIBRARY\_PATH"] | /usr/local/lib: |
| \_ENV["HOME"] | / |
| \_ENV["PATH"] | /sbin:/bin:/usr/sbin:/usr/bin |

PHP License

|  |
| --- |
| This program is free software; you can redistribute it and/or modify it under the terms of the PHP License as published by the PHP Group and included in the distribution in the file: LICENSE  This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  If you did not receive a copy of the PHP license, or have any questions about PHP licensing, please contact license@php.net. |

WEB VULNERABILITIES

On scanning the given website we founded many web vulnerabilities some are listed below

**1.SQL INJECTION**

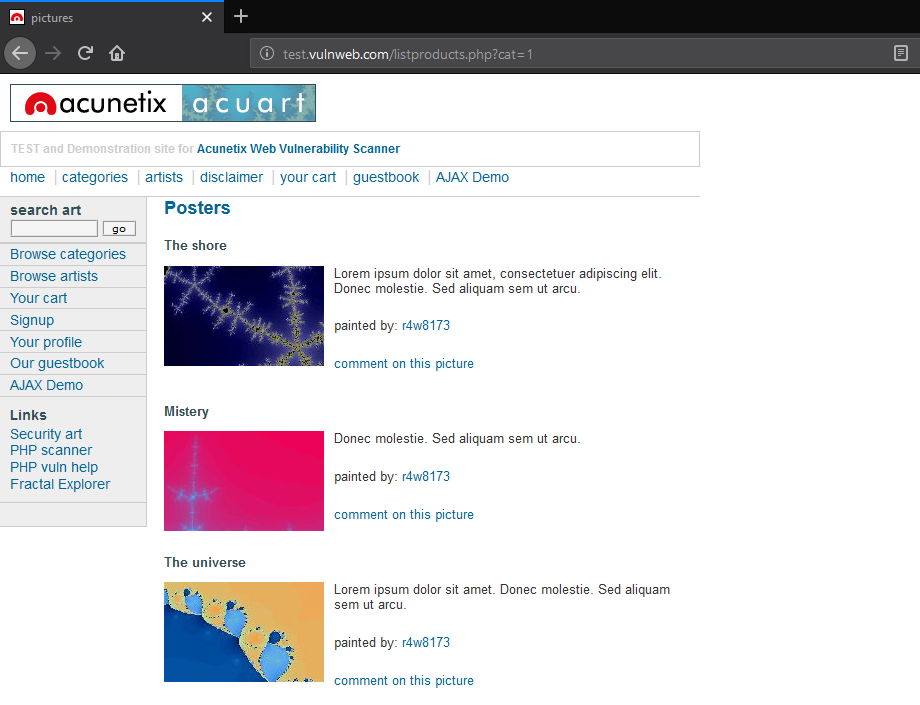
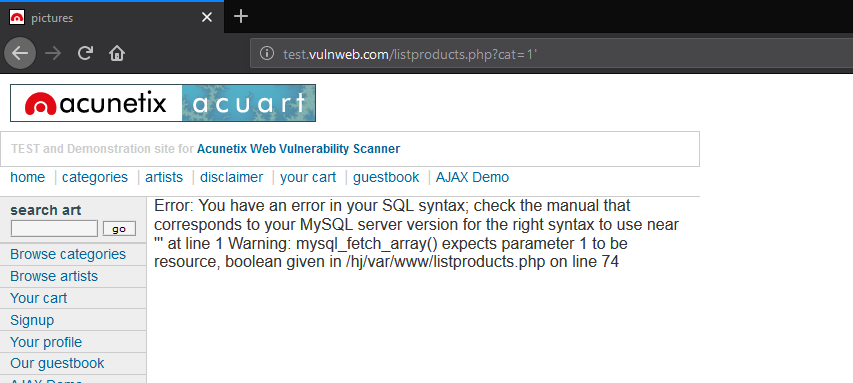
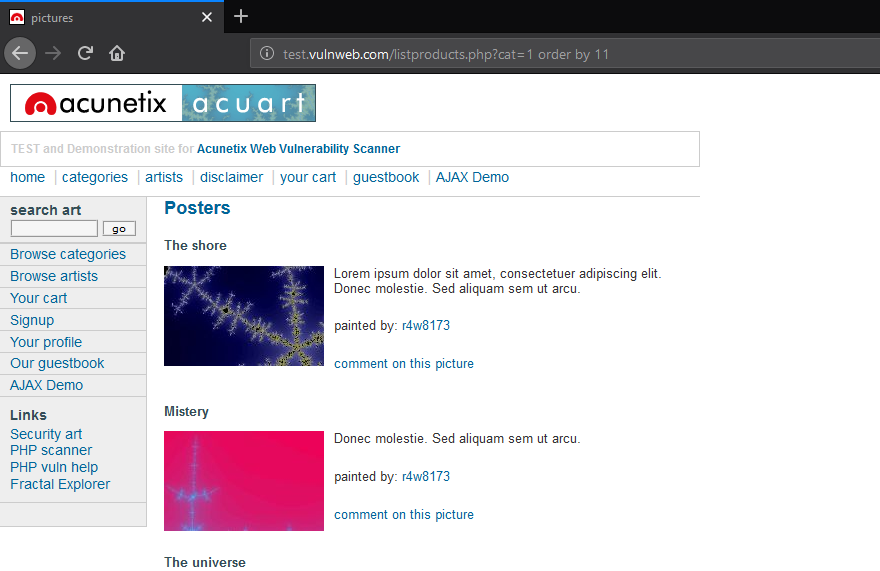
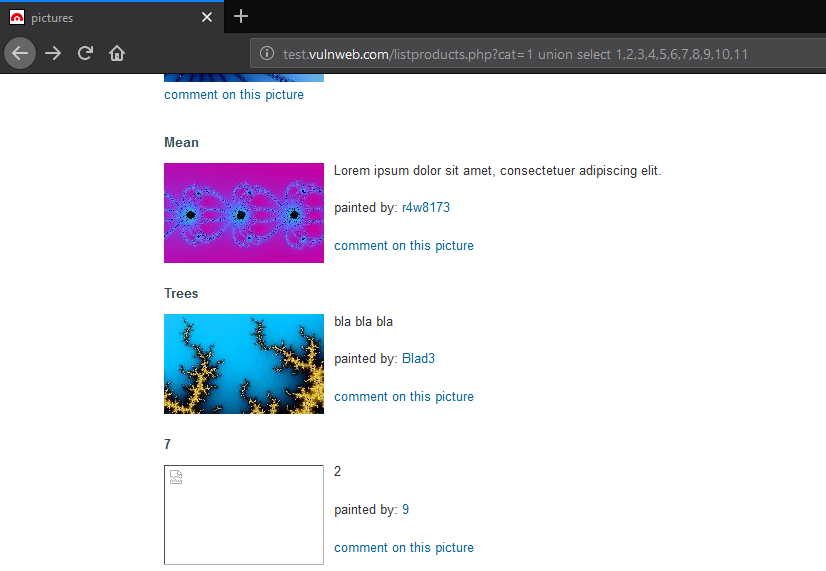
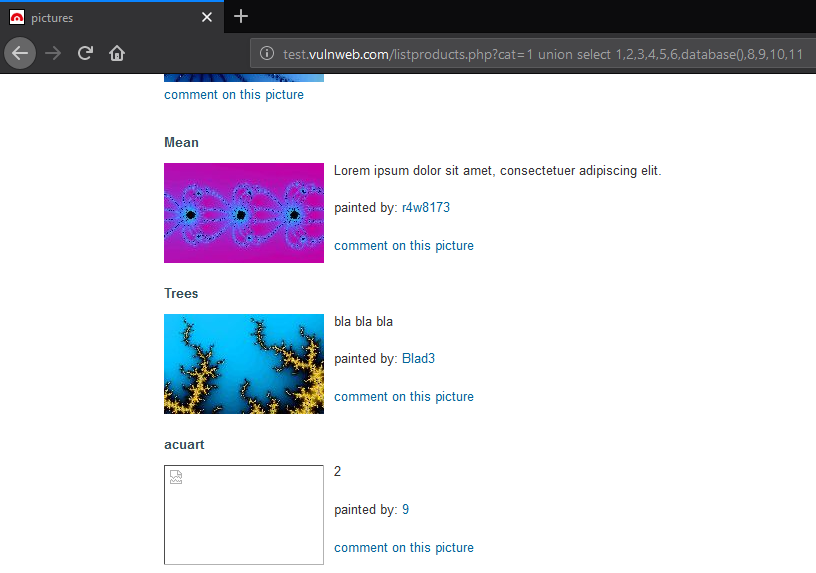
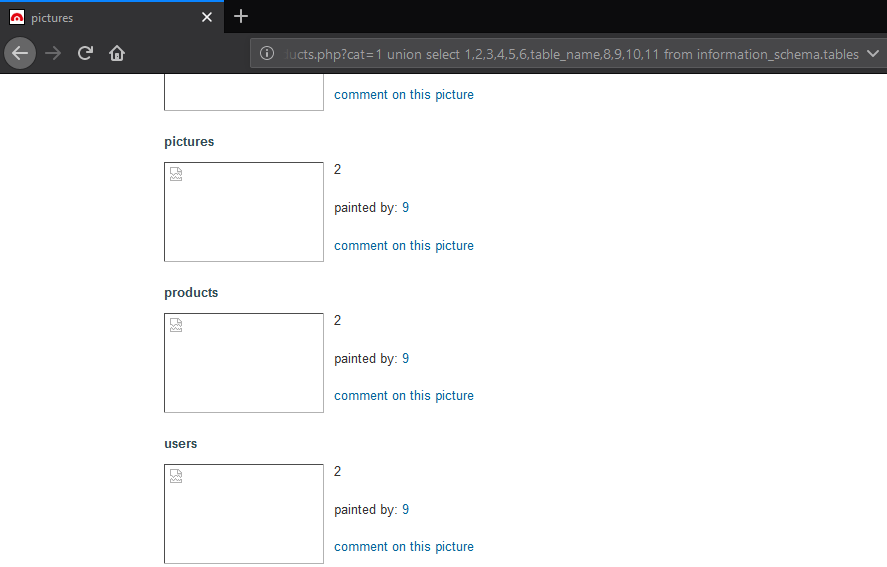
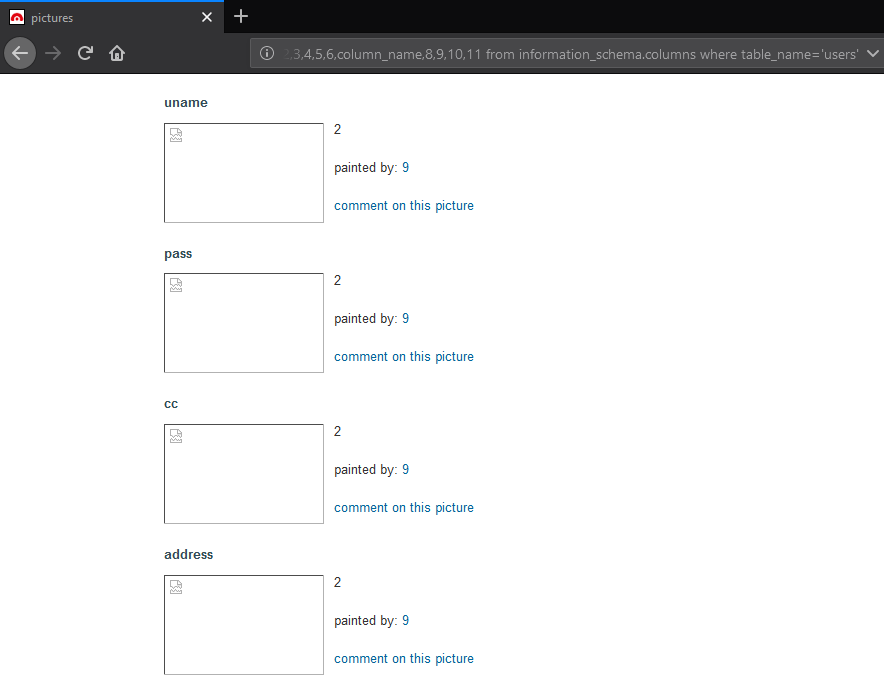
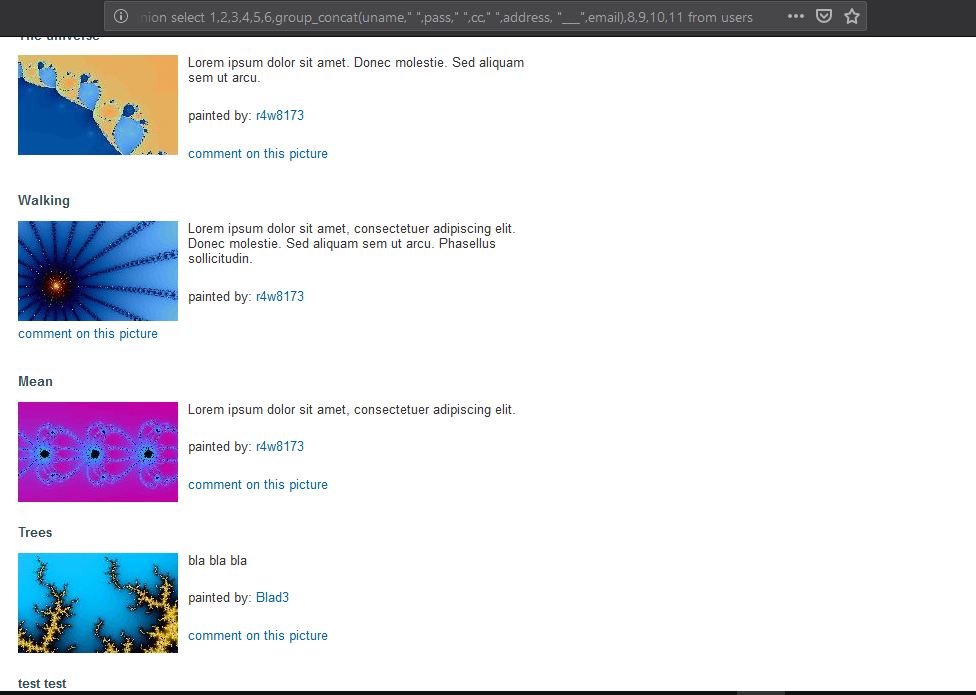
Description: - SQL Injection (SQL) is a type of web application vulnerability where an attacker can manipulate and submit a SQL command to retrieve the database information. This type of attack mostly occurs when a web application executes by using the user-provided data without validating or encoding it.

This attack can give access to sensitive information like customer information credit card numbers, trade secrets, personal data and more.

This attack allows an attacker to add, modify and delete data stored in the database.

How to Perform This Attack?

Steps to follow – (Performing this attack on a intentionally vulnerable application - <http://test.vulnweb.com/listproducts.php?cat=1>)

1. Open the above link in the Firefox browser
2. To test if this web application is vulnerable to SQL injection or not we put a quote(’) at the end of URLAs error occurs here, this means this website is vulnerable to SQL injection attack.
3. To know how many columns are present in the table we use order by We get to know that this page has 11 columns in the table
4. To know which column is vulnerable in the table we use union queryWe get to know that 7 and 9 column are vulnerable
5. To know the database name we use database() at the place of column numberWe get to know that acuart is the database name
6. To know the tables name present in the database we do the followingWe get to know various tables name but from these users table might be useful to us
7. To know the columns name we do the followingThese columns are very useful to use to get sensitive information
8. To fetch the data we do the followingWe get to know username and password of user.

**We have performed Brute Force Attack!!!!**

**Remediation**

1. Whitelisting is the best practice to validate input against blacklisting whenever it is practicable.
2. Do not create SQL queries with string concatenation. Instead use prepared statements or stored procedures.

**2.File Upload**

File Inclusion vulnerability allows an attacker to include a file, usually exploiting a “dynamic file inclusion” mechanism implemented in the target application. The vulnerability occurs due to the use of user-supplied input without proper validation.

This can lead to something as outputting the contents of the file, but depending on the severity, it can also lead to:

1.Code execution on the web server

2.Code execution on the client-side such as JavaScript which can lead to other attacks such as cross site scripting (XSS)

3.Denial of Service (DoS)

4.Sensitive Information Disclosure

**Local file inclusion (LFI)** is the process of including files, that are already locally present on the server, through the exploiting of vulnerable inclusion procedures implemented in the application. This vulnerability occurs, for example, when a page receives, as input, the path to the file that has to be included and this input is not properly sanitized, allowing directory traversal characters (such as dot-dot-slash) to be injected.

Directory:

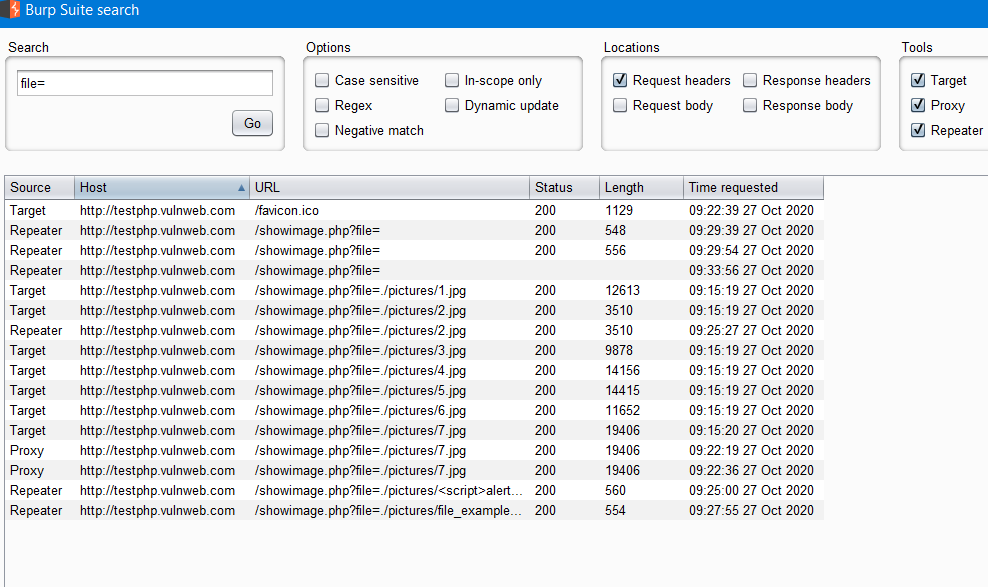
/showimage.php?file=./pictures/7.jpg

url: <http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg>

go to:

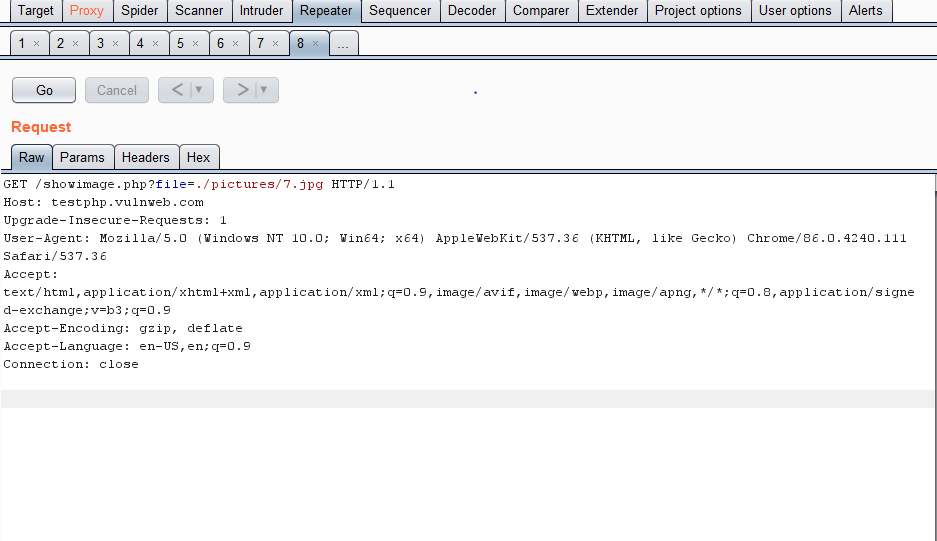
search in burpsuite to modify the request header i.e.

file=



The go to any link and then changes the file path to check whether it has file upload vulnerability or not

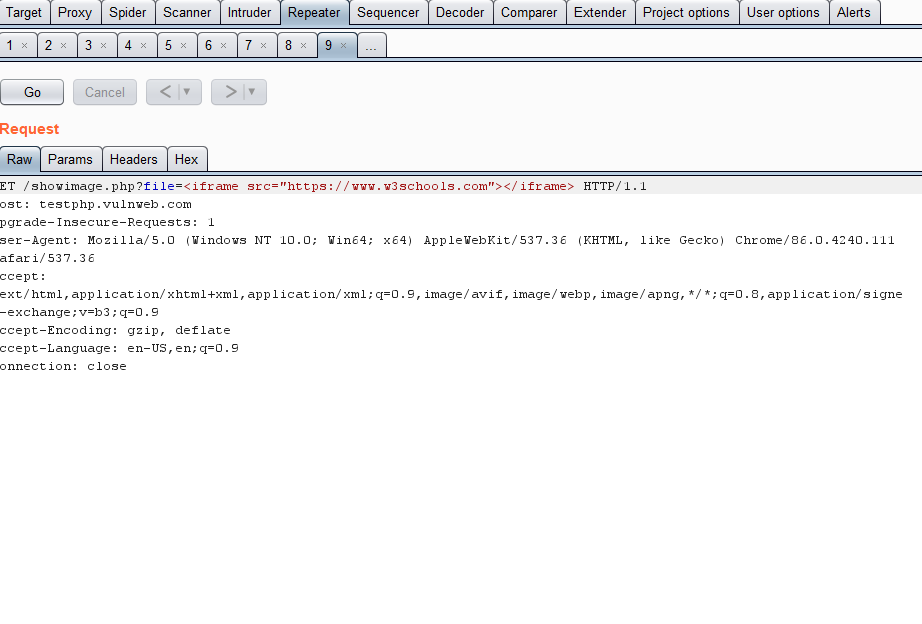
Send this request to the repeater to modify the request.

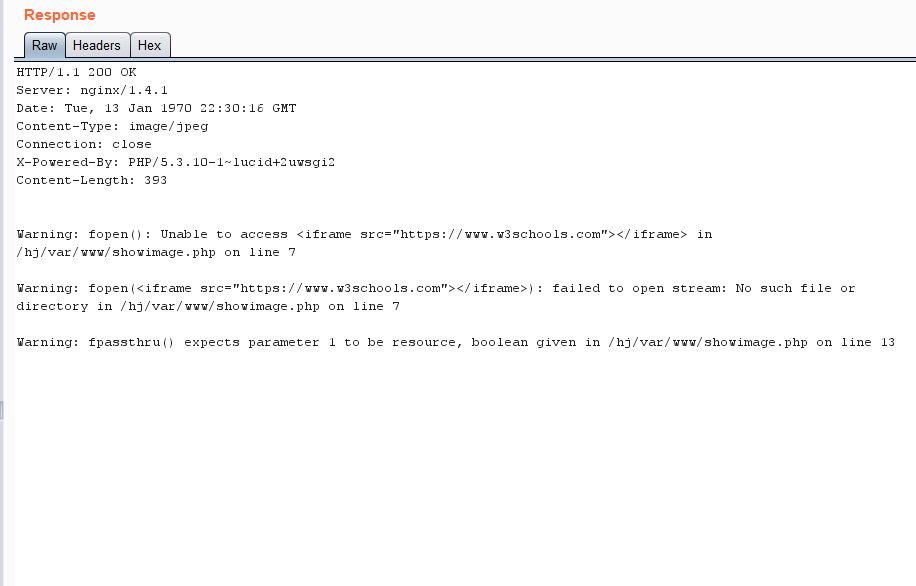


Apply this payload:

<iframe src=” https://www.3schools.com”> </iframe>

Modifies request:

Response:



Hence this response shows warning i.e. unable to access that means it does not have file upload vulnerability.

**Remediation**

As the main cause is improper input validation, suggestions mainly revolve around sanitizing the input received.

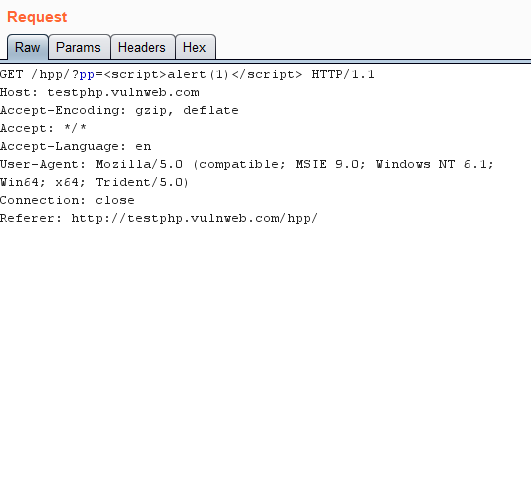
1. Accept only characters and numbers for file names (A-Z 0-9). Blacklist all the special characters which are not of any use in a filename.

2. Limit the API to allow inclusion of files only from one allowed directory so that directory traversal can also be avoided.

**3.Http parameter pollution attack**

Client-side HTTP parameter pollution (HPP) vulnerabilities arise when an application embeds user input in URLs in an unsafe manner. An attacker can use this vulnerability to construct a URL that, if visited by another application user, will modify URLs within the response by inserting additional query string parameters and sometimes overriding existing ones. This may result in links and forms having unexpected side effects. For example, it may be possible to modify an invitation form using HPP so that the invitation is delivered to an unexpected recipient.

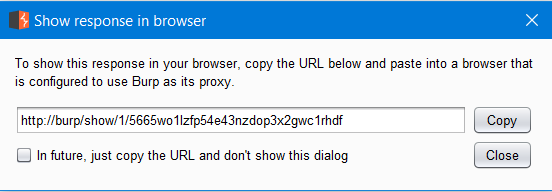
The security impact of this issue depends largely on the nature of the application functionality. Even if it has no direct impact on its own, an attacker may use it in conjunction with other vulnerabilities to escalate their overall severity.

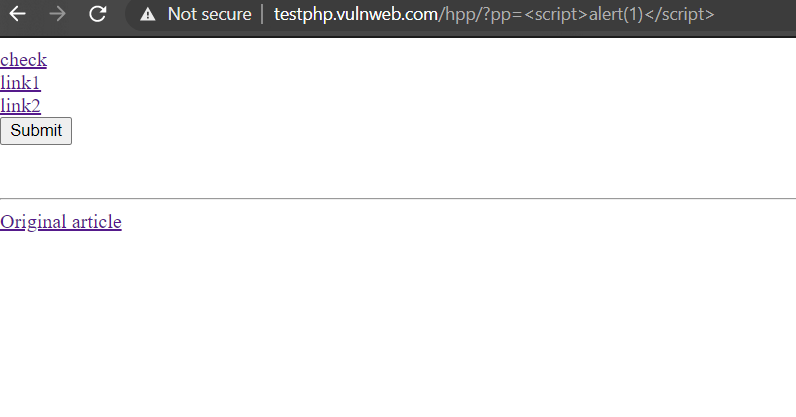


Then check response



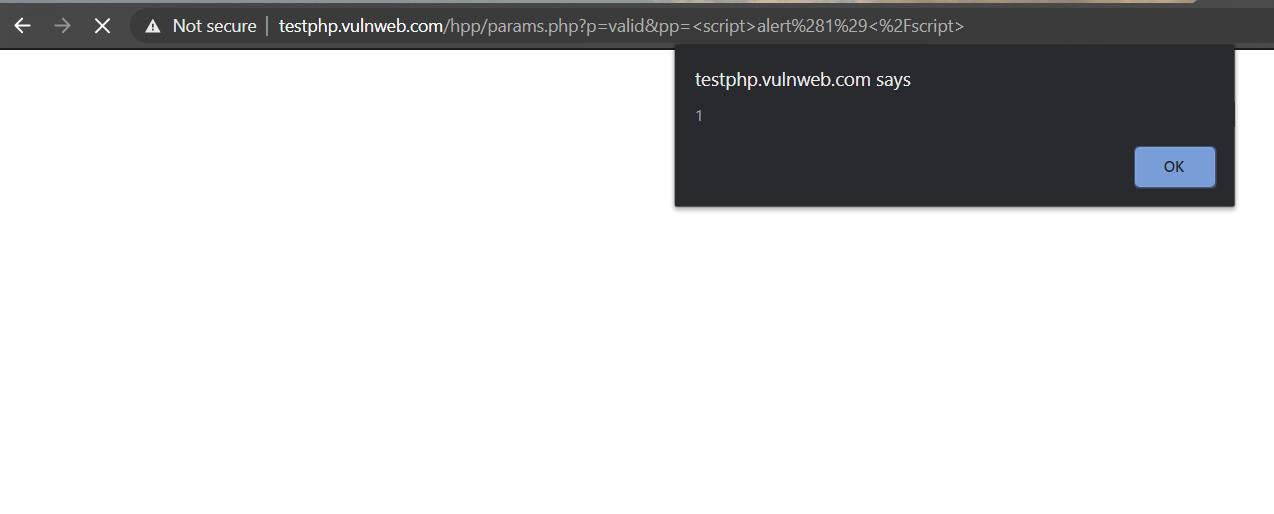
Then check response in browser.





Then click on link1 and link2

Then we get it works



We surely changed or injected payload in the http request.

Remediation

Ensure that user input is URL-encoded before it is embedded in a URL.

Now intercept the request in burbsuite and then send it to the repeater and perform modification or manipulating http request by <script>alert(1)</script>

**4.Cross Site Scripting (XSS)**

**Overview**

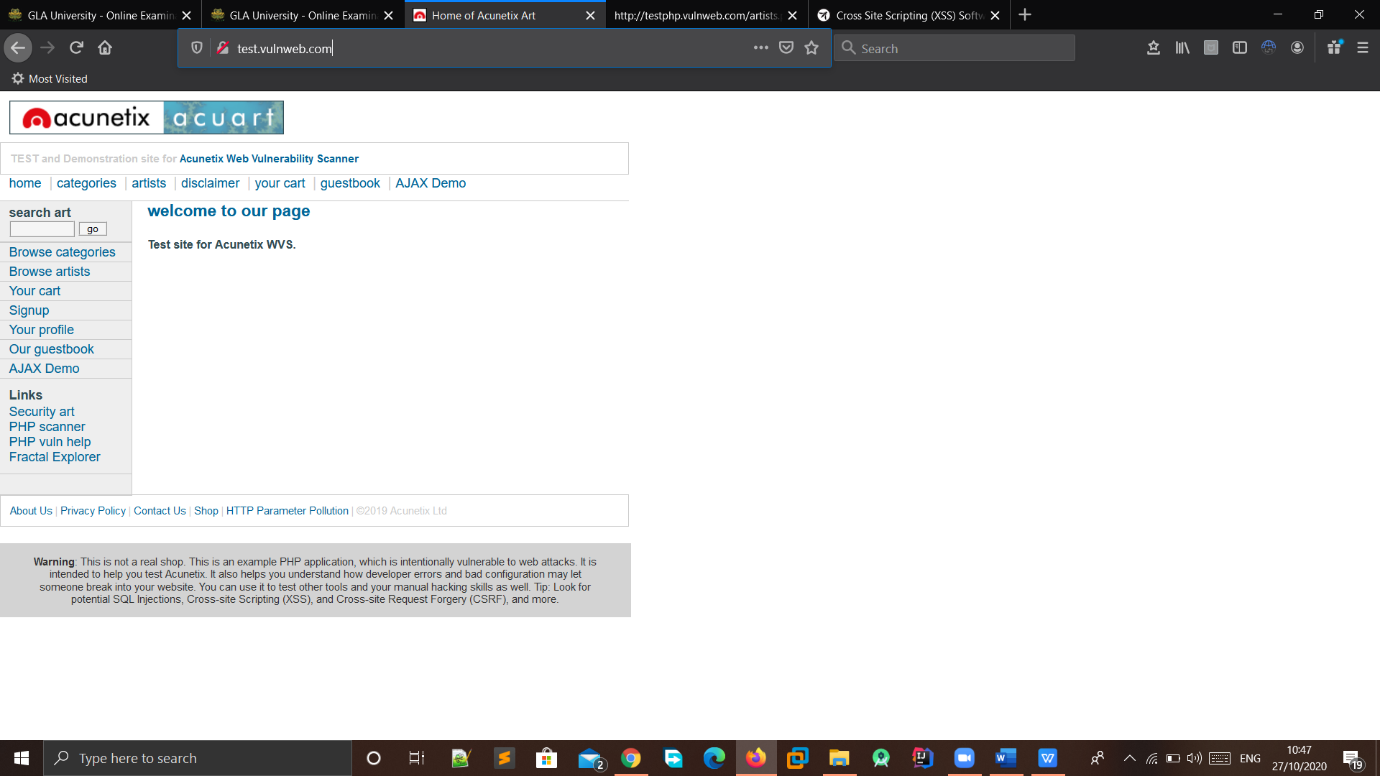
Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user’s browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.

**How to perform This Attack?**

Steps to follow – (Performing this attack on a intentionally vulnerable application - <http://test.vulnweb.com/>)

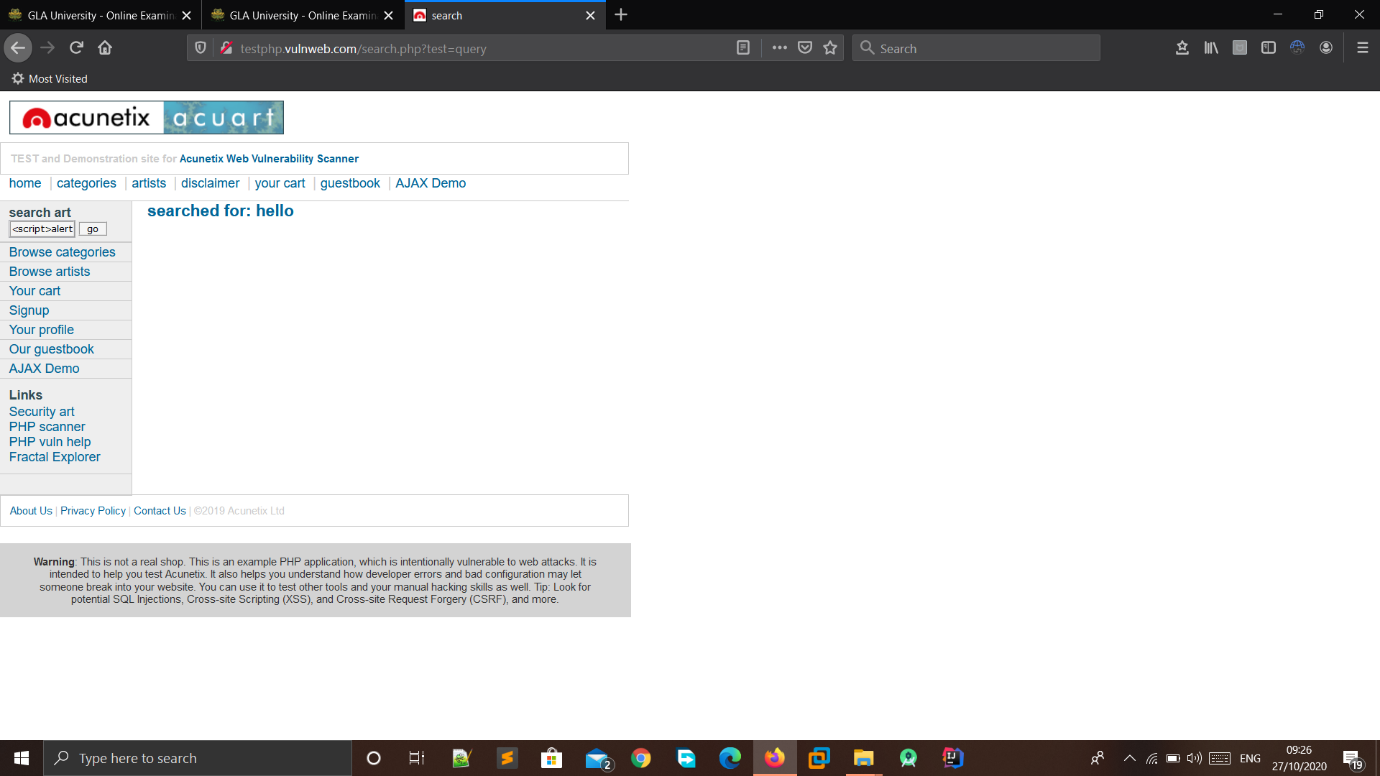
1. Open the above link in the Firefox browser

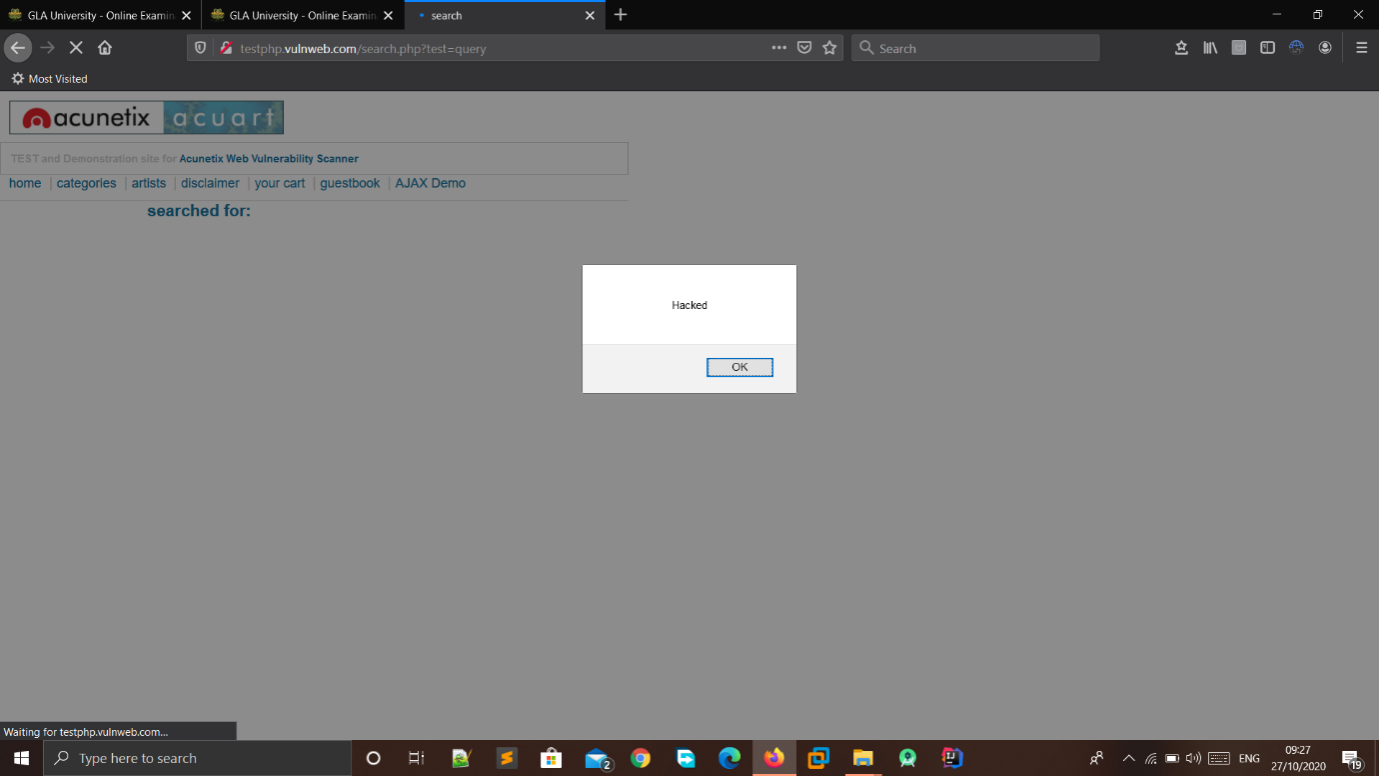


1. To test if this web application is vulnerable to XSS or not we put a Script in search bar

(“<script>alert(“Hacked”)</script>”)

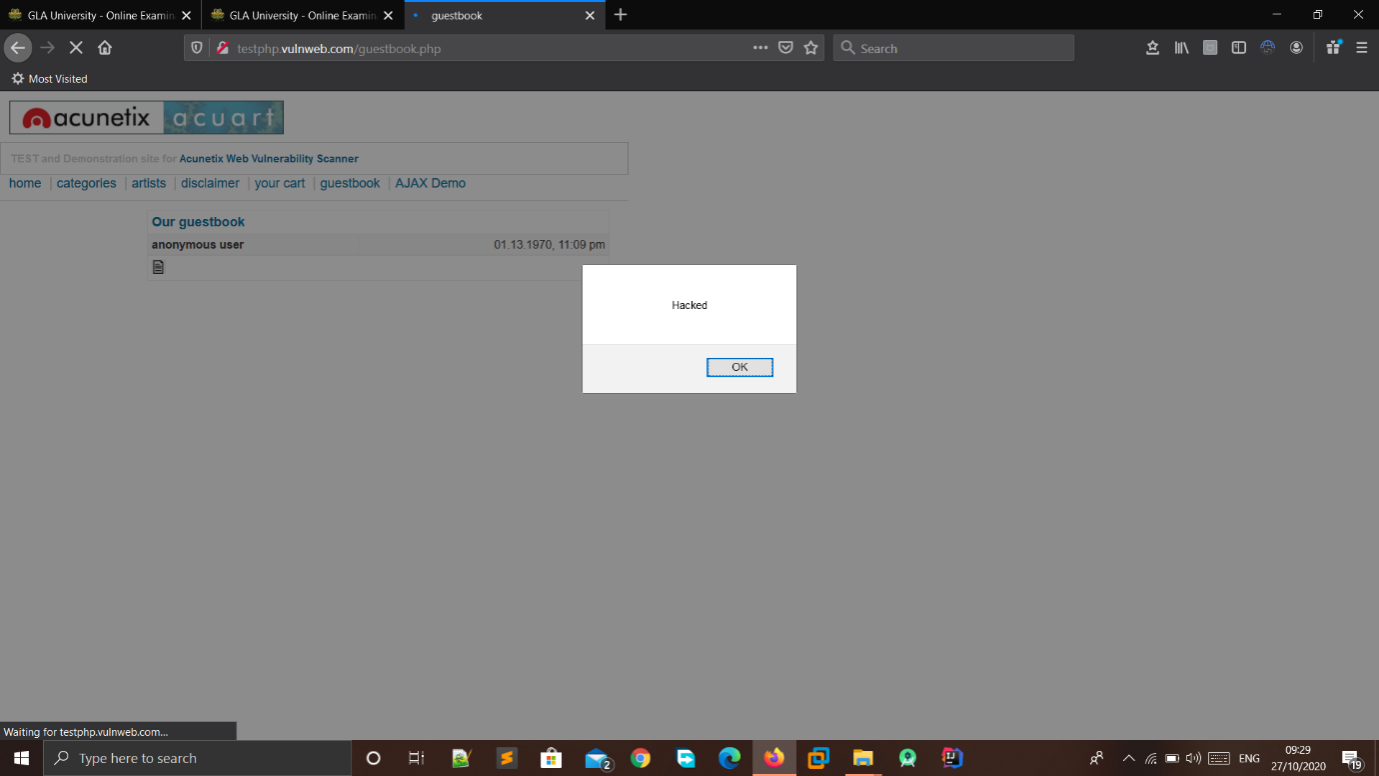
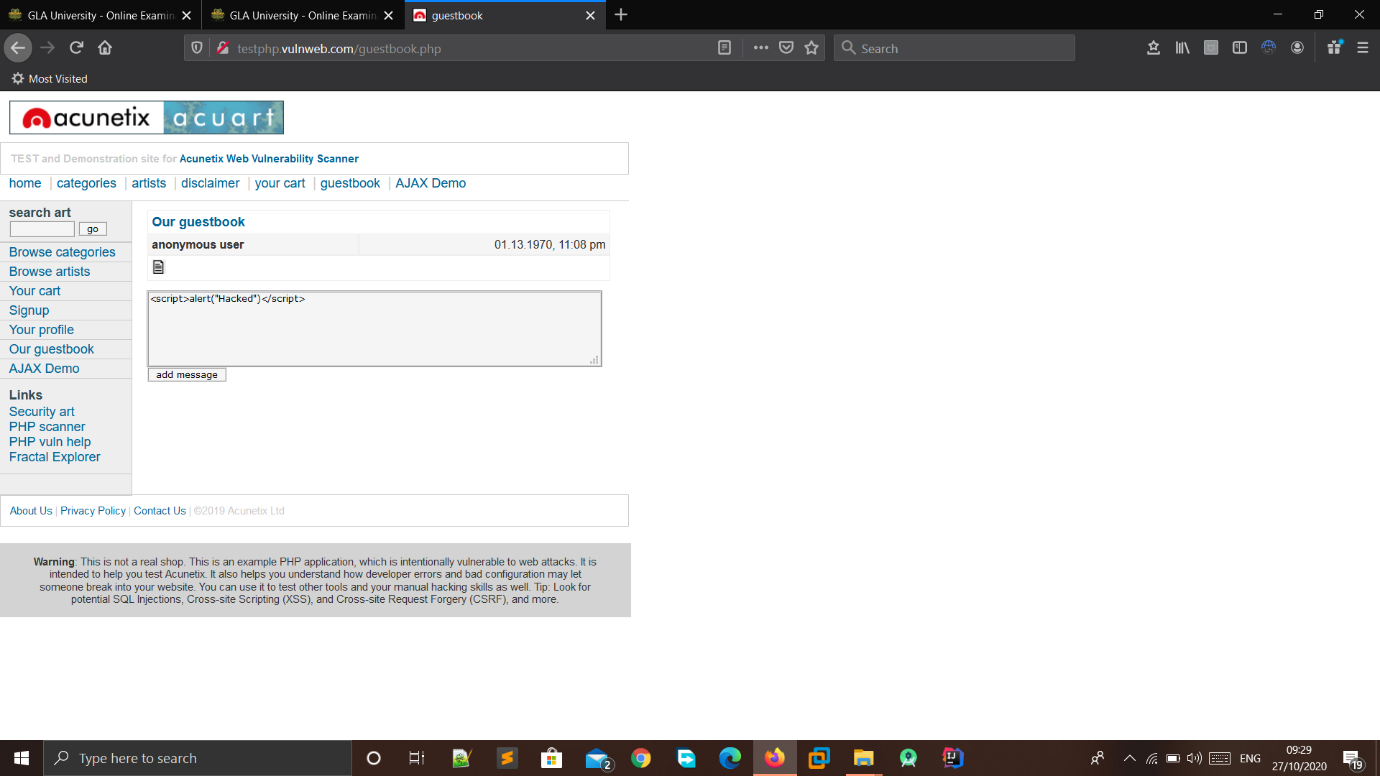
(<http://test.vulnweb.com/>)





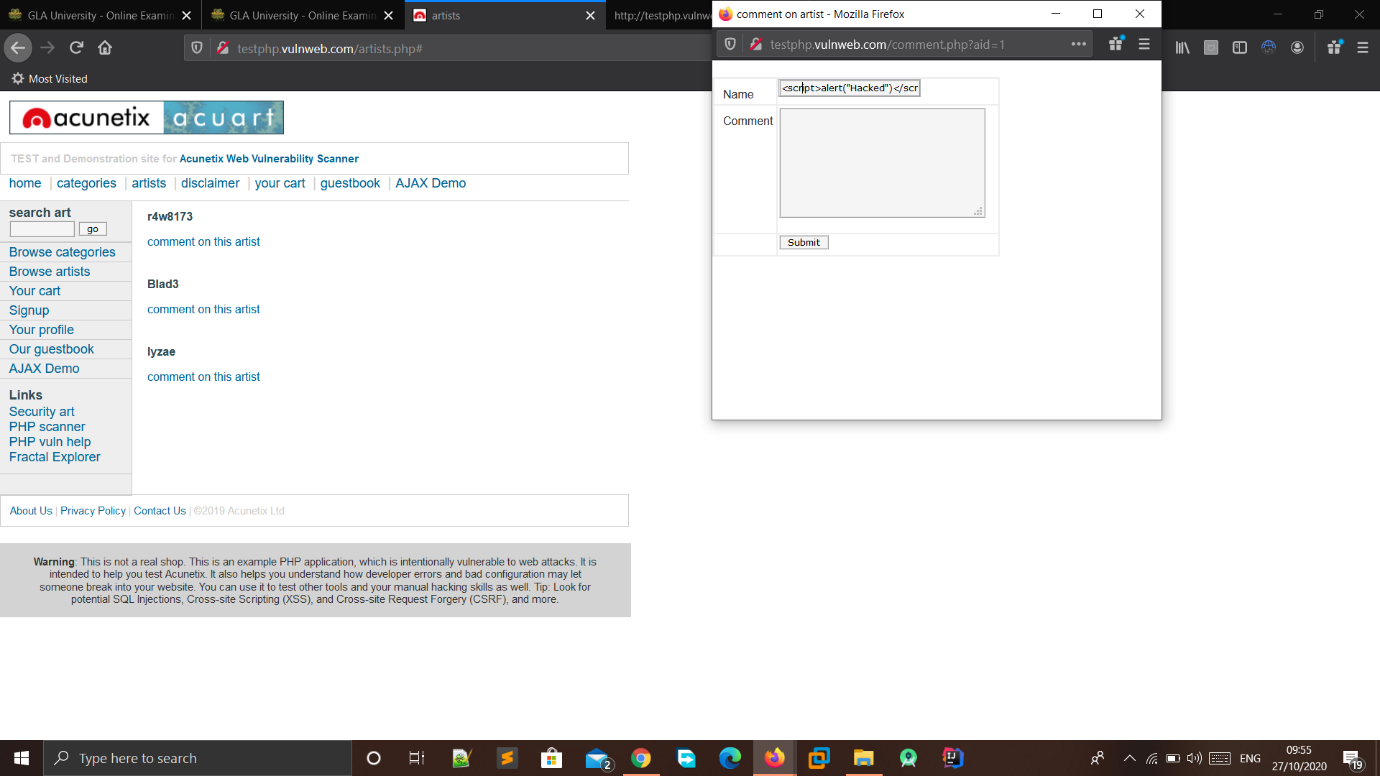
1. And also put the script in Message

(<http://test.vulnweb.com/guestbook.php>)



4.This type of script is also work in comment bar

(<http://test.vulnweb.com/comment.php?aid=1>)



**Remediations**

Sanitizing. A third way to prevent cross-site scripting attacks is to sanitize user input. Sanitizing data is a strong defense, but should not be used alone to battle XSS attacks. It’s totally possible you’ll find the need to use all three methods of prevention in working towards a more secure application.

5.SOURCE CODE DISCLOSURE

Obtaining the source code of server-side scripts grants the attacker deeper knowledge of the logic behind the web application, how the application handles requests and their parameters, the structure of the database, vulnerabilities in the code and source code comments.

Url:

<http://testphp.vulnweb.com/index.bak>

**<?PHP require\_once("database\_connect.php"); ?>**

<!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>

<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document\_title\_rgn" -->

<title>Home of WASP Art</title>

<!-- InstanceEndEditable -->

<link rel="stylesheet" href="style.css" type="text/css">

<!-- InstanceBeginEditable name="headers\_rgn" -->

<!-- here goes headers headers -->

<!-- InstanceEndEditable -->

<script language="JavaScript" type="text/JavaScript">

<!--

function MM\_reloadPage(init) { //reloads the window if Nav4 resized

if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {

document.MM\_pgW=innerWidth; document.MM\_pgH=innerHeight; onresize=MM\_reloadPage; }}

else if (innerWidth!=document.MM\_pgW || innerHeight!=document.MM\_pgH) location.reload();

}

MM\_reloadPage(true);

//-->

</script>

</head>

<body>

<div id="mainLayer" style="position:absolute; width:700px; z-index:1">

<div id="masthead">

<h1 id="siteName">ACUNETIX ART</h1>

<h6 id="siteInfo">TEST and Demonstration site for Acunetix Web Vulnerability Scanner</h6>

<div id="globalNav">

<a href="index.php">home</a> | <a href="categories.php">categories</a> | <a href="artists.php">artists

</a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> |

<a href="guestbook.php">guestbook</a>

</div>

</div>

<!-- end masthead -->

<!-- begin content -->

<!-- InstanceBeginEditable name="content\_rgn" -->

<div id="content">

<h2 id="pageName">welcome to our page</h2>

<div class="story">

<h3>Test site for WASP.</h3>

</div>

</div>

<!-- InstanceEndEditable -->

<!--end content -->

<div id="navBar">

<div id="search">

<form action="search.php" method="post">

<label>search art</label>

<input name="searchFor" type="text" size="10">

<input name="goButton" type="submit" value="go">

</form>

</div>

<div id="sectionLinks">

<ul>

<li><a href="categories.php">Browse categories</a></li>

<li><a href="artists.php">Browse artists</a></li>

<li><a href="cart.php">Your cart</a></li>

<li><a href="login.php">Signup</a></li>

<li><a href="userinfo.php">Your profile</a></li>

<li><a href="guestbook.php">Our guestbook</a></li>

<?PHP if **(isset($\_COOKIE["login"]))echo '<li><a href="../logout.php">Logout</a>'; ?></li>**

</ul>

</div>

<div class="relatedLinks">

<h3>Links</h3>

<ul>

<li><a href="http://www.acunetix.com">Security art</a></li>

<li><a href="http://www.eclectasy.com/Fractal-Explorer/index.html">Fractal Explorer</a></li>

</ul>

</div>

<div id="advert">

<p><img src="images/add.jpg" alt="" width="107" height="66"></p>

</div>

</div>

<!--end navbar -->

<div id="siteInfo"> <a href="http://www.acunetix.com">About Us</a> | <a href="redir.php?r=index.php">Site

Map</a> | <a href="privacy.php">Privacy Policy</a> | <a href="mailto:wasp@acunetix.com">Contact Us</a> | &copy;2004

Acunetix Ltd

</div>

<br>

</div>

</body>

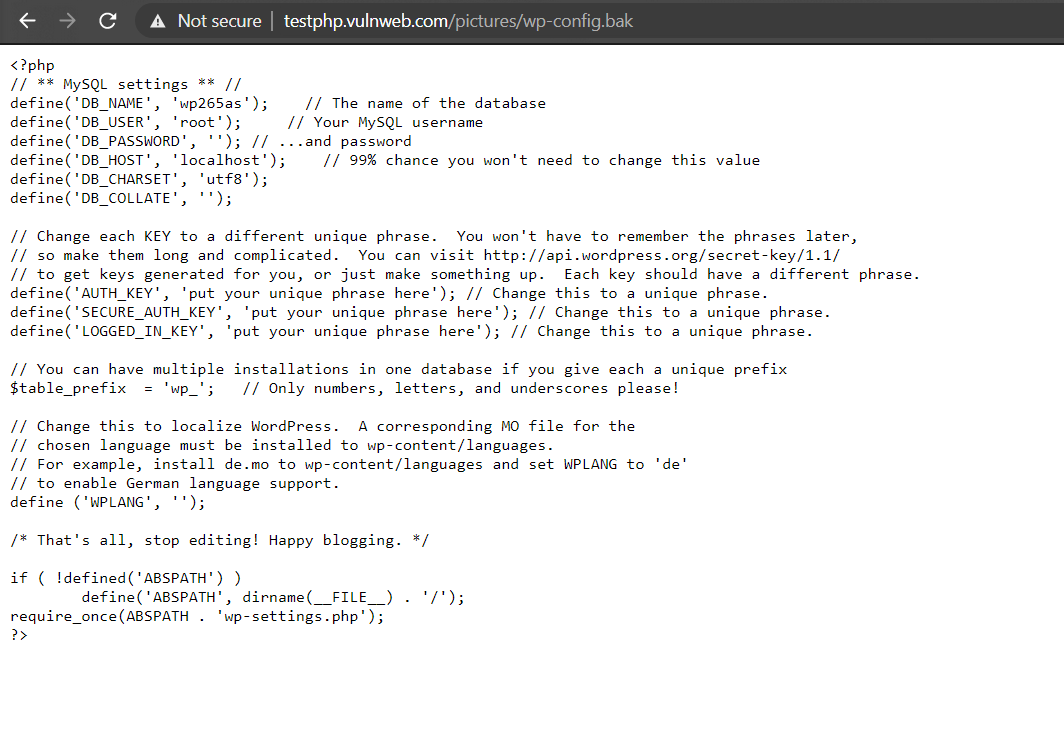
<!-- InstanceEnd --></html>

This code shows that this website uses php in database side .

2.

url:

http://testphp.vulnweb.com/pictures/wp-config.bak

gain

This shows that source code by database .

Due to this information attacker can exploit the database and can gain acces to the database and modify the entries or delete .

**Remediation:**

Review the cause of the code disclosure and prevent it from happening.