

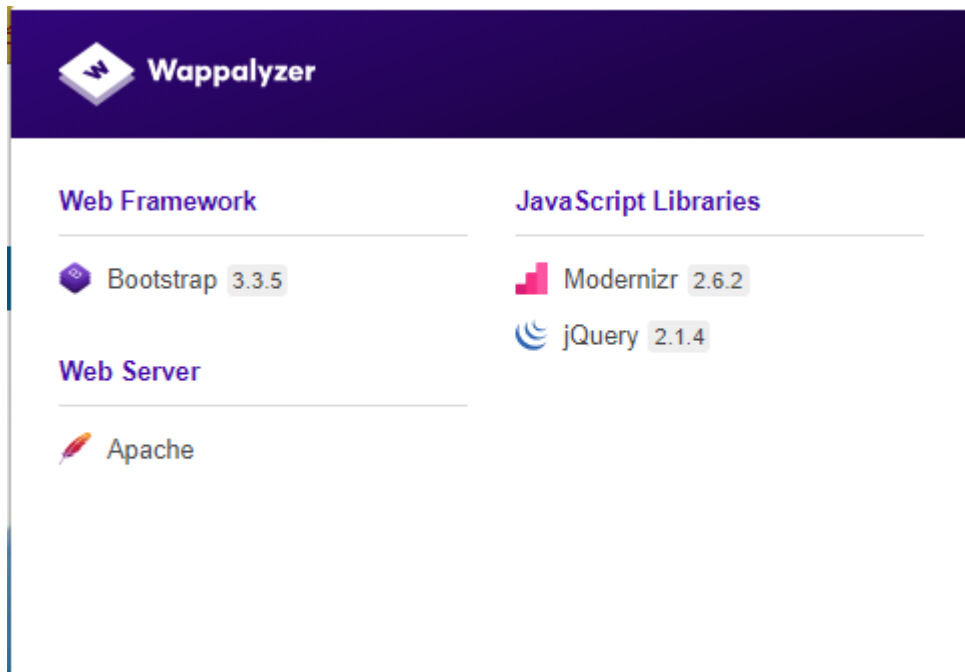
URL: <http://www.nagarjunauniversity.ac.in/index.htm>

Address: 23.238.226.105

Who Is?

Domain Name: NAGARJUNAUNIVERSITY.AC.IN
Registry Domain ID: D13286-AFIN
Registrar WHOIS Server:
Registrar URL: <http://www.ernet.in>
Updated Date: 2016-02-16T12:10:14Z
Creation Date: 2003-04-24T21:04:17Z
Registry Expiry Date: 2019-04-24T21:04:17Z
Registrar Registration Expiration Date:
Registrar: ERNET India
Registrar IANA ID: 800068
Domain Status: ok
Registrant State/Province: Andhra Pradesh
Registrant Country: IN
Name Server: NS1.NAGARJUNAUNIVERSITY.AC.IN
Name Server: NS2.NAGARJUNAUNIVERSITY.AC.IN
DNSSEC: unsigned

Wappalyzer



The image is a screenshot of the Wappalyzer web application. It features a dark purple header with the Wappalyzer logo and name. Below the header, the page is divided into three sections: 'Web Framework', 'Web Server', and 'JavaScript Libraries'. Each section lists the detected technology and its version number. The 'Web Framework' section shows Bootstrap 3.3.5. The 'Web Server' section shows Apache. The 'JavaScript Libraries' section shows Modernizr 2.6.2 and jQuery 2.1.4.

Category	Technology	Version
Web Framework	Bootstrap	3.3.5
	Web Server	Apache
JavaScript Libraries	Modernizr	2.6.2
	jQuery	2.1.4

Data sent is in plain text:

This site is sending data in Plain text format when intercepted using burp suite the data is seen in plain text. The URL of this page <http://www.nagarjunauniversity.ac.in/anuqas.php>.

Severity: High


Type: Validation

Vulnerability description:







The site is possible vulnerable to SQL injection attacks. This is one of the most common attacks currently being used. This vulnerability allows the attacker to alter back-end SQL statements by manipulation the user input.

Impact:

The attacker may execute arbitrary SQL statements on the vulnerable system which will compromise the integrity of the site.



ACHARYA NAGARJUNA UNIVERSITY
ఆచార్య నాగార్జున విశ్వవిద్యాలయం
Since 1976 **NAAC 'A'** ISO 9001:2015



HOME ABOUT ANU ADMINISTRATION LIBRARY AFFILIATED COLLEGES RESULTS SPORTS DOWNLOADS MAIL CDE

Name

harry

Mobile Number

1234567890

E-Mail ID

abc@gmail.com

Consultant

asdfghjklpoiuytrew

Submit


Request Response

Raw Params Headers Hex

```
POST /anuqasa.php HTTP/1.1
Host: www.nagarjunauniversity.ac.in
Content-Length: 80
Cache-Control: max-age=0
Origin: http://www.nagarjunauniversity.ac.in
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://www.nagarjunauniversity.ac.in/anuqas.php
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close

namef=harry&nof=C34567890&emailf=abc4@gmail.com&consf=asdfghjklSubmit=Submit
```

<http://www.nagarjunauniversity.ac.in/nriform.php> another form where the



Dr.K. Gangadhar Rao
Coordinator
Contact: 0863-2346284
Email: anunricell@gmail.com

Application

Name of the NRI :	harry
Email Id :	abc@gmail.com
Present Position :	ceo
Expertise :	developer
Department can collaborate :	astronomy
How they associate with ANU :	friend
Possible visit timings :	10:00
Contributions expected to provide to ANU :	23476

2016. All Rights Reserved to Acharya Nagarjuna University, Nagarjuna Nagar, Guntur - 522 510 ., Andhra Pradesh, India. Ph.No: 0863-22346114, Fax:0863-2293320

```
POST /nriform.php HTTP/1.1
Host: www.nagarjunauniversity.ac.in
Content-Length: 152
Cache-Control: max-age=0
Origin: http://www.nagarjunauniversity.ac.in
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://www.nagarjunauniversity.ac.in/nriform.php
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close

name=harry&email=abc%40gmail.com&position=ceo&expertise=developer&department=astronomy&amu=friend&visit=10%3A00&contribution=23476&snext=&snext=Submit
```

X-Frame-Options Header Not Set

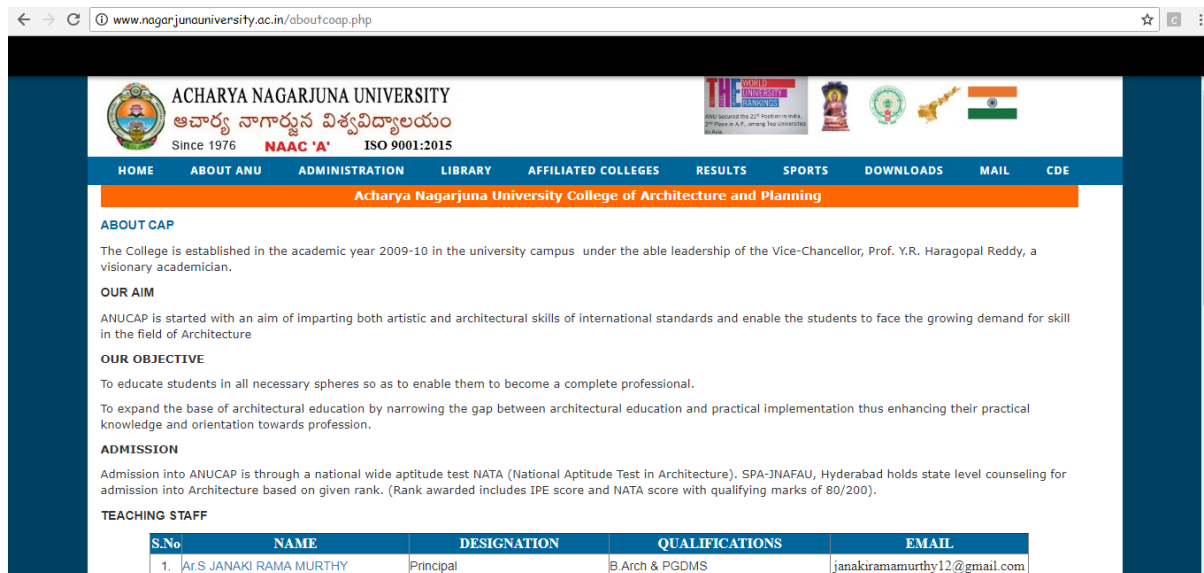
Severity: Medium

Vulnerability Description:

X-Frame-Options header is not included in the HTTP response to protect against 'Clickjacking' attacks.

Solution:

Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).



The screenshot shows the website of Acharya Nagarjuna University. The header includes the university's name in English and Telugu, its founding year (1976), and accreditation (NAAC 'A' and ISO 9001:2015). The navigation menu lists various sections: HOME, ABOUT ANU, ADMINISTRATION, LIBRARY, AFFILIATED COLLEGES, RESULTS, SPORTS, DOWNLOADS, MAIL, and CDE. The main content area is titled 'Acharya Nagarjuna University College of Architecture and Planning' and contains information about the college's establishment, aims, objectives, and admission process. A table of teaching staff is also present.

S.No	NAME	DESIGNATION	QUALIFICATIONS	EMAIL
1.	Ar.S JANAKI RAMA MURTHY	Principal	B.Arch & PGDMS	janakiramamurthy12@gmail.com

PHP allow_url_fopen enabled

Severity: Medium

Vulnerability Description:


The PHP configuration directive allow_url_fopen is enabled, which allows data retrieval from remote location.

Solution:

Disable allow_url_fopen from php.ini

URL: <http://www.nagarjunauniversity.ac.in/phpinfo.php>

This URL will display all the information including 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.

PHP Version 5.5.32	
	
System	Linux nagarjunauniversity.ac.in 3.10.0-327.4.5.el7.x86_64 #1 SMP Mon Jan 25 22:07:14 UTC 2016 x86_64
Build Date	Feb 20 2016 03:28:00
Configure Command	'./configure' '--disable-fileinfo' '--disable-opcache' '--enable-bcmath' '--enable-calendar' '--enable-ftp' '--enable-gd-native-ttf' '--enable-libxml' '--enable-pdo=shared' '--enable-sockets' '--prefix=/usr/local' '--with-apxs2=/usr/local/apache/bin/apxs' '--with-curl=/opt/curlssl' '--with-freetype-dir=/usr' '--with-gd' '--with-imap=/opt/php_with_imap_client' '--with-imap-ssl=/usr' '--with-jpeg-dir=/usr' '--with-kerberos' '--with-libdir=lib64' '--with-libxml-dir=/opt/xml2/' '--with-mcrypt=/opt/libmcrypt' '--with-mysql=/usr' '--with-mysql-sock=/var/lib/mysql/mysql.sock' '--with-pcre-regex=/opt/pcre' '--with-pdo-mysql=shared' '--with-pdo-sqlite=shared' '--with-pic' '--with-png-dir=/usr' '--with-xpm-dir=/usr' '--with-zlib' '--with-zlib-dir=/usr'
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/lib
Loaded Configuration File	/usr/local/lib/php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20121113
PHP Extension	20121212
Zend Extension	220121212
Zend Extension Build	API220121212,NTS