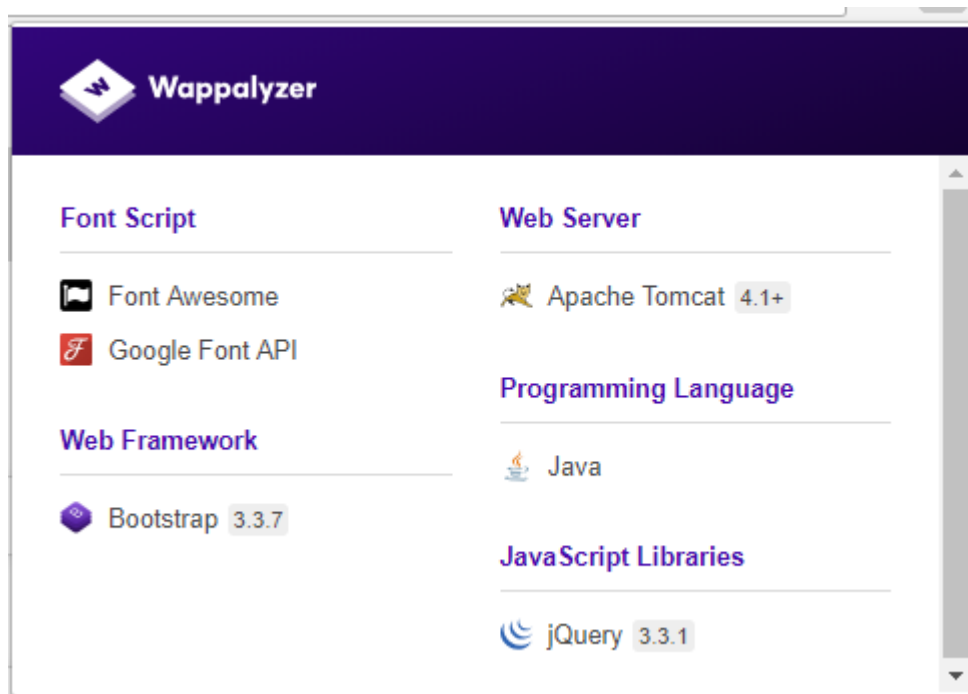


Name of the domain---http://www.way2sms.com

Who IS??

Domain Name: WAY2SMS.COM
Registry Domain ID: 288804034_DOMAIN_COM-VRSN
Registrar WHOIS Server: Whois.bigrock.com
Registrar URL: http://www.bigrock.com
Updated Date: 2014-01-16T10:29:19Z
Creation Date: 2005-12-17T12:34:58Z
Registry Expiry Date: 2019-12-17T12:34:58Z
Registrar: BigRock Solutions Limited
Registrar IANA ID: 1495
Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com
Registrar Abuse Contact Phone: +1.2013775952
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS1.WAY2DNS.NET
Name Server: NS2.WAY2DNS.NET
DNSSEC: unsigned

Wappalyzer



1) 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.way2sms.com/.

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.


The screenshot shows the way2sms website with a navigation bar at the top containing the logo, 'FREE SMS', 'BUSINESS', and 'PRICING' links, along with a phone number and email support. The main content area has three columns: 'SEND FREE SMS' with a list of features, 'LOGIN TO WAY2SMS' with input fields for mobile number and password, and 'REGISTER NOW' with a list of benefits. The mobile number field contains '+91 9890097689' and has a red error message below it. The password field is masked with dots. There are 'LOGIN' and 'REGISTER' buttons at the bottom of their respective sections.

```
POST /re-login HTTP/1.1
Host: www.way2sms.com
Content-Length: 44
Accept: */*
Origin: http://www.way2sms.com
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.84 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://www.way2sms.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: __gads=ID=324b9044e5f97fee:T=1520922463:S=ALNI_MbNqcmMIew1BZ54L6pM0mrV_F1Hxg; _ga=GAL.2.1034986302.1520922464; JSESSIONID=A03-B06D214A8327A9A6953C2A8C29CF34
Connection: close

mobileNo=9890097689&password=iuydhd&CatType=
```


```
POST /re-login HTTP/1.1
Host: www.way2sms.com
Content-Length: 42
Accept: */*
Origin: http://www.way2sms.com
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.84 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://www.way2sms.com/Logout
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: __gads=ID=324b9044e5f97fee:T=1520922463:S=ALNI_MbNqcmMiew1B254L6pM0mrV_FlHXg; __ga=GAL.2.1034986302.1520922464; JSESSIONID=A03-B06D214A8327A9A6953C2AE8C29CE734;
_gid=GAL.2.283969116.1533494904; _gat=1
Connection: close


mobileNo=9500080113&password=8834&CatType=
```


 **way2sms**
#india's #1 SMS platform


FREE SMS

BUSINESS

 How to send bulk SMS campaign ?

 897805

 Support


sumaila
+919500080113


- Send Sms
- Language Sms
- Group Sms
- Future Sms
- Sent Sms
- Address Book


Send SMS


Instant Delivery , No.1 service provider in India.

+91

Mobile Number

 Contacts

 Greeting Sms

 Smile's

Enter Message

Remaining Characters 140

SEND SMS

2) Web Browser XSS Protection Not Enabled

Severity :Medium

Type: Post and Get

Vulnerability description

Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server

Solution for the vulnerability

Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'.



About Way2SMS

We are India's largest free messaging destination, helping over 50 Million users to connect with their families and friends and also in saving their mobile bills. We have over 15,000 new users joining us daily and that makes us the fastest growing messaging destination in India.

- Over 50 million registered users across 120 countries, trust our platform for seamless communication.
- We have been featured in the top 50 sites in India constantly.
- Featured in top 10 most searched keywords in India ? Google Zeitgeist Award.

Feel free to contact us at support@way2online.com



Get In Touch With Us

Way2SMS Users Get In Touch With Us

Write your questions, issues to **support at way2online dot com**

- Please mention your registered mobile number while writing to us.
- Remember, we may not reply to all your mails due to the volume of mails we handle every day. We reply to only important mails.

Advertising Inquiries

For Banner advertising, Social Media advertising, Electronic direct mailer (EDM) or click to call advertising opportunities email us on [hello at way2online dot com](mailto:hello@way2online.com)

CEO: Write To Me

I'm always interested to hear from anyone who wishes to get in touch with me. Whether you have a partnership proposal, or a killer idea to share with me, or just to poke me and say

3) X-Content-Type-Options Header Missing

Severity :LOW

Type : GET

Vulnerability Description:

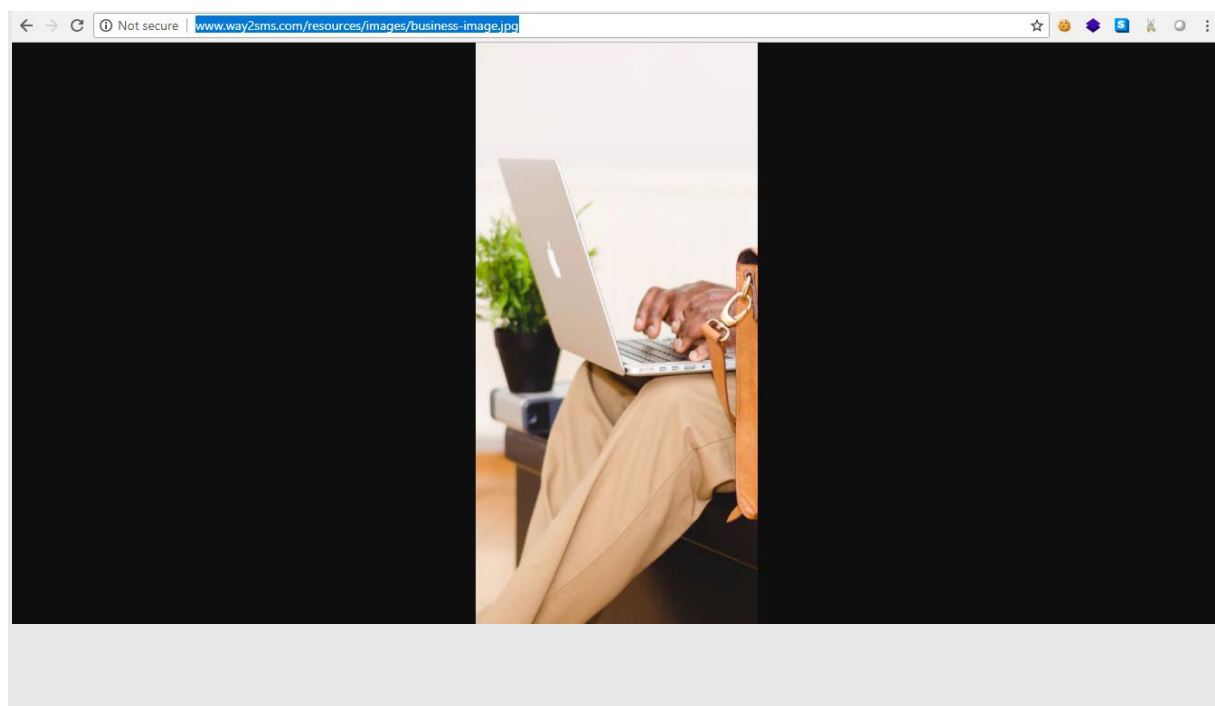
The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

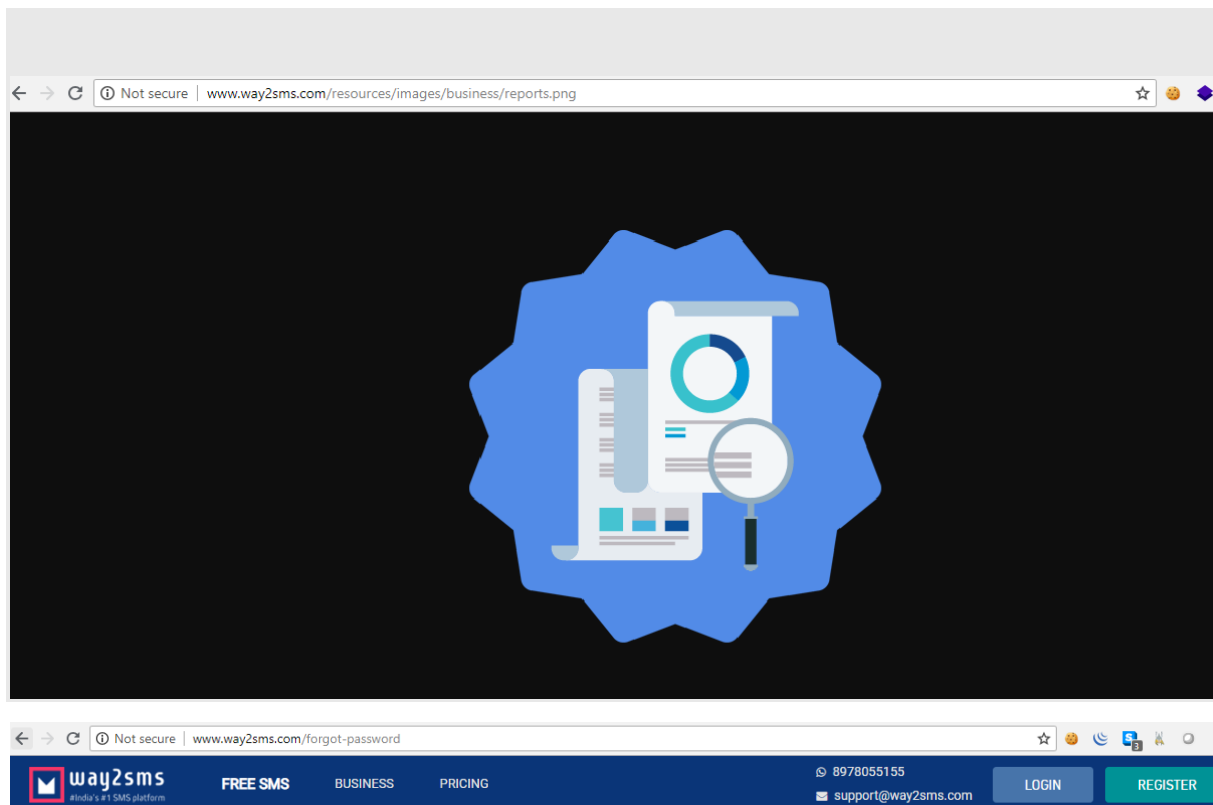
Solution for the vulnerability :

Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.

If possible , ensure that the end user uses a standards-complaint and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web applications/web server to not perform the MIME-attack

Irrelavent pages being displayed because of this vulnerability






Forgot Password

Send Password To My Mobile

Mobile Number

Enter the code shown below

Q P a J r z



Send my Password