George David <gd861721@gmail.com>

Responsible Disclosure of Security Vulnerabilities in pulse.in

1 message

George David <gd861721@gmail.com> Thu, Aug 10, 2023 at 11:55 AM
To: hiroshan@pulse.in, "support@pulse.in" <support@pulse.in>

Hello Development or security team,

I hope you are doing well. My name is George David. I am writing to inform you about security vulnerabilities I have found in the **pulse. in** and **support. pulse. in**. I believe in responsible disclosure and want to give you the information you need to address these issues effectively. if you are not a concerned person please forward this to the respective team.

Vulnerable URL: https://www.pulse.in/
http://support.pulse.in/

1.SQL Injection Vulnerability:
I have discovered a potential SQL injection vulnerability in the [Website Name] website. Through improper input validation, it appears that an attacker could exploit this vulnerability to gain unauthorized access to the database. I have attached a Proof of Concept (PoC) demonstrating the vulnerability in action. To replicate the PoC, please use the following steps to reproduce.

Steps to reproduce:
1. Go to http://support.pulse.in/
2. in the username input field type **'OR 1=1##**
3. in the Password input field type any random letters
4. Hit the login button
5. it will log in to the admin account

Impact
An attacker can access the ticketing system with admin privilege, they can see your customer details and ticketing queries and answer them disrespectfully it could be severe and P1
level bug.

suggestion
1. Use proper input validation
2. Use prepared statements in your DB connection

2. Email Spoofing Vulnerability:
I found an email spoofing vulnerability that could potentially allow malicious actors to send emails that appear to originate from the pulse.in email addresses. This could lead to phishing attacks and the spread of misinformation. To illustrate this issue, I have included a PoC where an email is spoofed to seem like it's from a support@pulse.in and marketing@pulse.in

Steps to reproduce:
1. To verify the pulse doesn't have valid SPF/TXT records go to https://www.kitterman.com/spf/validate.html
2. in domain name input field type **pulse.in** then click get SPF records(if any) button
3. you can see no valid SPF record found of either type TXT or type SPF
4. now go to https://emkei.cz/
5. put in from a name like admin or anything
6. put in from email like suppot@pulse.in or admin@pulse.in or hr@pulse.in or contact@pulse.in or marketing@pulse.in
7. To email, give your email address (for testing purposes I use a temporary email as the receiver email)
8. Add subject and message then verify the captcha and Hit send
9. you can see the mail from the pulse domain

Impact
if an attacker performs email spoofing in your domain it makes you weak in front of your customers it will make a bad impression
it could be possible for phishing and many other social engineering attacks

suggestion
maintain proper SPF/TXT records

3. Clickjacking Bug:
I also detected a clickjacking vulnerability on your website, where an attacker could trick users into clicking on hidden or

invisible elements that perform unintended actions. I have attached a PoC video showcasing this vulnerability in action and the steps to reproduce it.

Steps to reproduce:

1. create an HTML file with the following code:

```
<!DOCTYPE html>
<html>
<head>
<title>hack</title>
</head>
<body>
<iframe src="https://www.pulse.in/" width="500px" height="500px"></iframe>
</body>
</html>
```

4. run this HTML file in your Browser
5. it will open the pulse website in your local file

Impact

clickjacking will be a potential threat in a particular context. It could be possible to phish and fake embedded websites.

suggestion

Add X-frame and other security headers

4. Path Traversal Vulnerability

A Path Traversal Vulnerability (also known as Directory Traversal or Directory Climbing) is a type of security vulnerability that occurs when an attacker can manipulate input to access files or directories that are located outside of the intended scope of the application. This can lead to unauthorized access to sensitive files or directories on a web server or in a file system.

Steps to Reproduce:

1. Go to support. pulse.in
2. right click pulse logo then click open image in the new tab
3. it will open the pulse logo in a new tab
4. The URL looks like http://support.pulse.in/assets/img/dummy/with-pulse3.gif
5. Remove the image name and reload
6. The URL is http://support.pulse.in/assets/img/dummy/
7. it shows a directory of all images used on the website.
8. do the process again and again like: http://support.pulse.in/assets/img/ and http://support.pulse.in/assets/
9. it will list your digital certificates and cryptographic key information

Impact

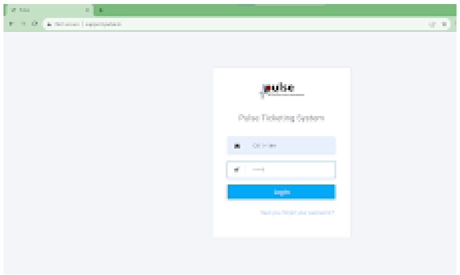
It could lead to unauthorized data disclosure, Data loss, and DOS attack in many cases

Suggestion

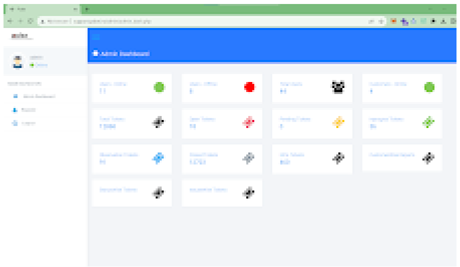
1. Avoid direct user input in file paths
2. Use Absolute Paths
3. Use WAF

After I analyzed your site I know you are the leading telecommunications solutions 👍
I am committed to ensuring the security and integrity of online platforms, which is why I wanted to bring these issues to your attention. As a token of appreciation for my efforts, I am interested in discussing the possibility of a bounty or recognition for helping secure the pulse.in platform. This could be a financial reward, an acknowledgment in your security hall of fame, or any other appropriate form of recognition.
I am willing to cooperate with your team to help resolve these issues and enhance the security of the pulse platform. If you require further details or assistance in reproducing these issues, please don't hesitate to contact me. I have attached all POC screenshots and videos with this mail.
Thank you for your time and consideration. I look forward to the opportunity to contribute to a safer online environment for all users.

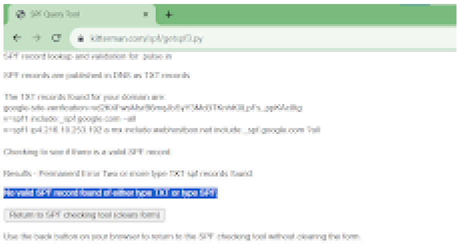
15 attachments



pulse sqli poc1.png
43K



pulse sqli poc2.png
95K



SPF record lookup and validation for: pulse.in

SPF records are published in DNS as TXT records.

The TXT records found for your domain are:
google-site-verification=[illegible]
v=spf1 include:_spf.google.com ~all
v=spf1 ip4:218.19.253.192 a mx include:webhostbox.net include:_spf.google.com ?all

Checking to see if there is a valid SPF record.

Results - PermError Error Two or more type TXT spf records found.

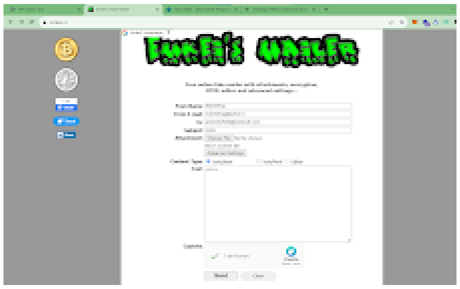
No valid SPF record found of either type TXT or type SPF.

Return to SPF checking tool (clears form)

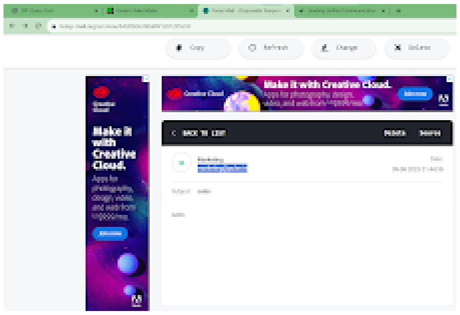
Use the back button on your browser to return to the SPF checking tool without clearing the form.

pulse es poc2.png
43K

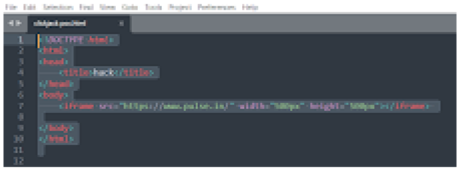
pulse es poc1.png
106K



pulse es poc3.png
234K



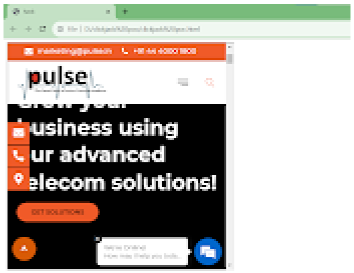
pulse es poc4.png
589K



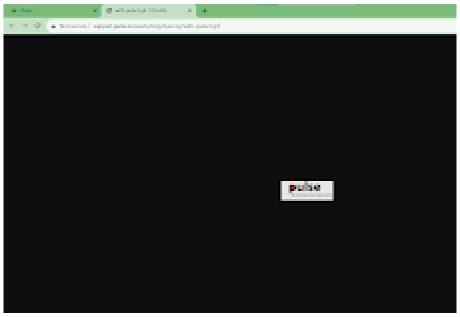
```
<!DOCTYPE html>
<html>
<head>
    <title>hack</title>
</head>
<body>
    <iframe src="https://www.pulse.in/" width="500px" height="500px"></iframe>

</body>
</html>
```

pulse cj poc1.png
27K



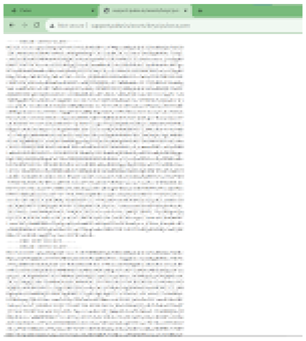
pulse cj poc2.png
74K



pulse pt poc1.png
29K

Index of /assets/img/dummy

pulse pt poc2.png
158K



pulse pt poc3.png
204K

pulse sqli poc.mp4
596K

pulse email spoofing poc.mp4
6336K

pulse clickjack poc.mp4
1947K

pulse pt poc.mp4
1838K