iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** VI **Month of publication:** June 2021

DOI: https://doi.org/10.22214/ijraset.2021.35187

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

Social Engineering Penetration Testing

Vamshi Krishna Motru[1], Guntoju Deepak[2], Ch Mvn Sai Teja Prashanth[3], Ekke Karthik[4]
[1, 2, 3, 4]*UG Student, Department of Electronics and Communication Engineering, Chaitanya Bharathi Institute of Technology, Gandipet, Hyderabad, India*
[1, 2, 3, 4]*Maturi Venkata Subba Rao Engineering College, Nadergul, Hyderabad, India*

Abstract: ***In this universe of digitalization, the requirement for information protection and information security is very significant. The IT organizations today care for their information over everything. For organizations, information protection is additionally significant for any person. In any case, regardless of how secure the organization is, how cutting-edge is the innovation utilized, or how modern their products are, there's as yet a weakness in each area known as 'Human'.The ability of gathering sensitive information from a person is known as Social Engineering. Social Engineering exceeds a variant security danger as it has demonstrated to be one of the simplest, least expensive, and vigorous and profoundly fruitful ways for criminals to accomplish their finishes. This paper depicts social engineering, progressed techniques utilized,and their effect on associations. This paper can help the security analysts to acquire experiences into social engineering from an alternate point of view, and specifically, upgrade the current and future investigation on social engineering monitor mechanisms.***
Keywords: Digitalization, Sensitive Information, Social Engineering, Countermeasures

I. INTRODUCTION

Social engineering is the craft of controlling individuals to reveal delicate Information with the goal of playing out a malignant action. Social engineering penetration testing includes utilizing different methods to deceive the employees of the objective association into unveiling sensitive data or perform activities that make security weaknesses that can be additionally exploited by the attacker. The goal of performing social engineering penetration testing is to test the qualities and shortcomings of human variables in a security chain inside the association. It likewise checks the responsibility of the representatives towards ensuring the association's sensitive data, their mindfulness in regards to social weaknesses, their capacity to conform to security strategies, and the viability of the security preparation. A pen tester should initially get suitable approval from the association's administrators to perform social engineering. The pentester should accumulate all the pertinent data about the representatives and afterward carry out different social engineering methods to draw workers into uncovering the association's sensitive data. To succeed, the pen tester needs to take an uncommon interest in creating social engineering abilities and should be capable enough that the casualties don't see the misrepresentation. The pen tester needs to plan social engineering penetration tests that copy genuine assaults by utilizing different strategies that incorporate all techniques like telephone, email, or on the web and actual interruptions. After the consummation of the tests, the pen tester needs to create a full report of the discoveries and their moderation suggestions.

II. METHODOLOGIES

While thinking about security, clients are accepted to be the most vulnerable connection; in any case, numerous associations permit clients to have more than the needed advantages to play out their positions. Social engineering pen testing permits the pentester to test such sorts of clients and recognize the individuals who are vulnerable to social engineering strategies. Social engineering pen testing includes two distinct modes, to be specific off location testing and on location testing:

A. Off Location Testing

Off location testing includes testing representatives' security mindfulness during their day-by-day exercises. To perform off-site social engineering pen testing, first, the tester needs to accumulate openly accessible data about the association through uninvolved surveillance procedures. The tester can get significant data from the organization's site, web crawlers, social systems administration locales, the organization's yearly reports, and so forth. Strategies utilized in off-site social engineering incorporate the accompanying:

1) *Phishing:* Phishing is a procedure where the pen tester sends an email or gives a connection that dishonestly claims to be from a genuine site trying to get a client's close to home or record data. At the point when the client taps on the email connect, it diverts them to a phony page, where they are attracted into sharing sensitive subtleties, for example, address and Visa data without realizing that they are on a phishing site.

©IJRASET: All Rights are Reserved

2) *Vishing:* Vishing (voice phishing or Voice over IP (VoIP) phishing) is a pantomime strategy where the pen tester utilizes VoIP innovation to fool people into uncovering their basic monetary and individual information. In this method, pen testers call workers, claiming to be a client or vendor who needs help and demands them for information. Pen testers for the most part pick nontechnical representatives and solicitation them to give essential information with respect to the organization. The testers can likewise utilize genuine names of vendors or clients related with the organization to persuade the workers. In the wake of acquiring their trust, pen testers attempt to assemble sensitive information.
3) *SMiShing:* In SMiShing (SMS Phishing), the SMS text informing framework is utilized to draw clients into moment activity, for example, downloading malware, visiting a vindictive website page, or calling a fake telephone number. SMiShing messages are created to incite a moment activity from the person in question, expecting them to uncover their own information and record subtleties.

B. On Location Testing

On location testing includes testing the actual security of an association and the security strategies set up. To perform nearby social engineering pen testing, the pen tester camouflages themselves as an approved individual to enter the objective premises.

1) *Baiting:* Baiting is a strategy wherein pen testers entice the objective client with something charming in return for significant data, for example, login details and other sensitive information. In this method, pen testers leave an actual gadget, for example, a USB streak drive containing pernicious records in areas where individuals can without much of a stretch discover them including parking garages, lifts, and washrooms. This physicalgadget is named with a real organization logo applicable to the objective client, which is utilized to fool them into finding and opening in systems of the orginazation. When the gadget is associated and opened by the person in question, a malignant document gets downloaded and the framework gets contaminated, which permits pen testers to assume responsibility for the casualty's framework.
2) *Reverse Social Engineering:* In reverse social engineering, the pen tester expects the job of an individual in authority with the goal that representatives ask them for information. The pen tester manipulates the inquiries that representatives pose in a way that the actual workers surrender the necessary information.
3) *Elicitation:* Elicitation is the strategy of extricating information from the casualty by bringing them into normal and incapacitating discussions. To evoke information, the pen tester needs to start an easygoing discussion with the objective client to remove information without causing them to understand that they are in effect socially designed.

III. IMPLEMENTATION

You'd receive an email with instructions to log into your bank. After login, you're instructed to click on this link https://yourBankWebsite.com/account?id=<script>[maliciousCodeHere]</script>

When you login, your bank's website server starts a session for you (usually lasting 10–15 minutes, after which you are automatically logged out). The session information (usually called a token) is stored in a cookie on your computer.If the hacker can get you to login, and then click the link he sent you, then maliciousCodeHere will run, and could send your session token to the hacker. This allows him to **steal your session**. He could then (in theory) create a cookie on his computer and store your session information in it. If that session is still active, he can visit your bank's website, and he'll be logged in as you, and can browse around, look at bank account information, and possibly even initiate a transfer or change your password.

Now, the site below is vulnerable to XSS, using which any attacker can use this official website as a phishing page to gain sensitive information from the victims. Here the URL will be the same as the original website as compared to the traditional social engineering attacks where the content will be the same but the URL will be a different one so with proper validation, we can ignore it and even the browser(Latest versions) will block it as a phishing site. But now the URL is the same as the original so even the website Administration will also be confused or misguided. So an attacker taking advantage of this can perform a social engineering attack on all of them.

To achieve it he uses the below as a sample malicious script to create a fake login in the official website.

```
<fieldset>
<legend>Login:</legend>
<label for="fname">User name:</label>
<form id="attack" action="https://a935720cda23.ngrok.io" method="GET">
<input type="text" name="pass" placeholder="User name">
```

©IJRASET: All Rights are Reserved

```
<br>
<br>
<label for="fname">Password:</label><br>
<form id="attack" action="https://a935720cda23.ngrok.io" method="GET">
<input type="password" name="pass" placeholder="Password"><br>
<button type="submit" onclick="attack">Submit
</fieldset>
```

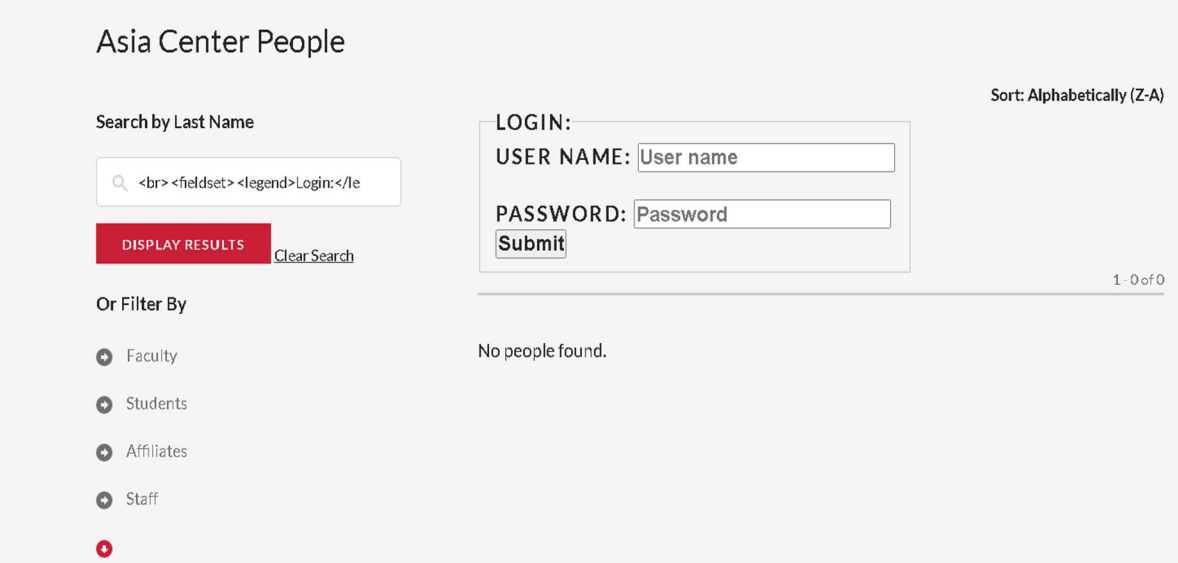


Fig 1.1 Vulnerable website with stored XSS

Ngrok provides a real-time web UI where you can introspect all HTTP traffic running over your tunnels. Replay any request against your tunnel with one click. Ngrok is a useful utility to create secure tunnels to locally hosted applications using a reverse proxy. It is a utility to expose any locally hosted application over the web. So by using Ngrok, an attacker creates a local port as a server and gets a HTTP and HTTPS link with that local port. Here its port 80

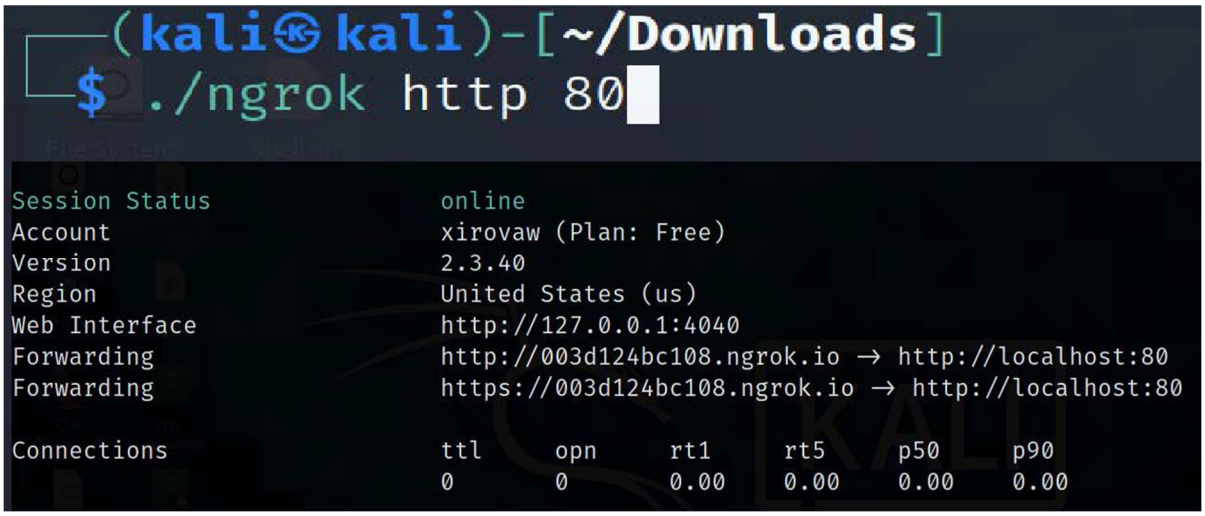


Fig 1.2 Hosting Ngrok

The figure above shows the localhost:80 routed/forwarding to a server which is hosted globally. And to listen to all the communication, attackers need a port listener. Netcat is a utility that reads and writes data across network connections, using the TCP or UDP protocol. It is designed to be a reliable "back-end" tool, used directly or driven by other programs and scripts. By using the below command, port 80 is set as a listening port.

©IJRASET: All Rights are Reserved

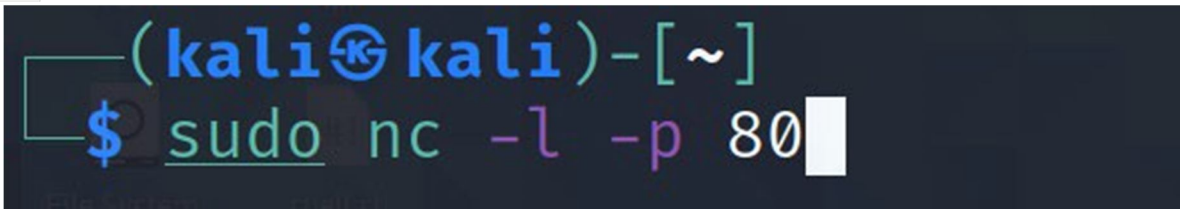


Fig 1.3 Port Listener

Anyone visiting this site will be triggered with this attacker created login and all usernames and passwords entered will be directly pushed to the Netcat listener. Here username=”Admin” and Password=”Admin@123” was entered by a victim visiting this website.

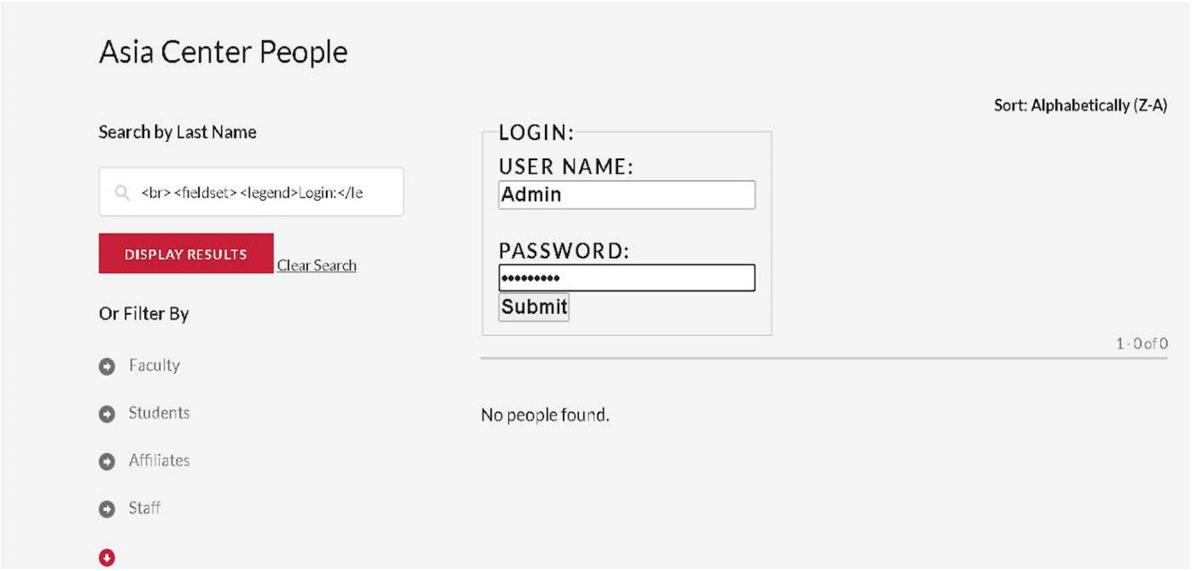


Fig 1.4 Official website with Fake login page

Immediately after the victim enters his/her credentials they reflect in the attackers netcat so by this the attacker is misguiding the users to login using this vulnerability to perform social engineering attack.

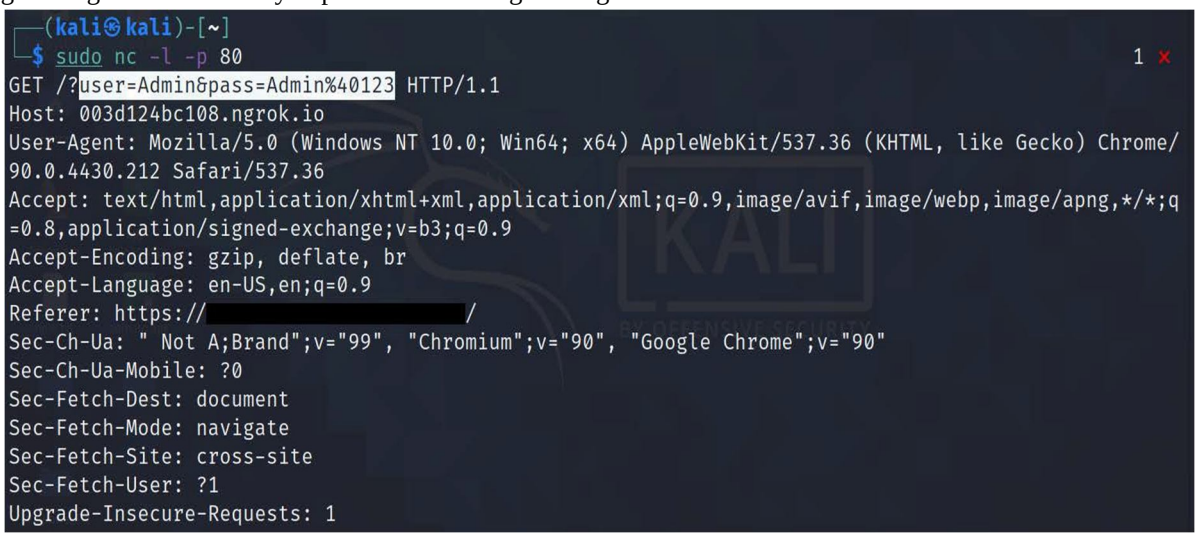


Fig 1.5 Attacker captured request

Now each user can browse to the search results page will see the link injected by the offender. If an unsuspecting consumer trusts the packages and clicks at the injected hyperlink it now contains, he's all of sudden seeing content material from an attacker-controlled login page.

©IJRASET: All Rights are Reserved

IV. COUNTERMEASURES

A. Train employees/help table to ne'er reveal passwords or alternative info by phone. Enforce policies for the front office and help desk personnel.
B. Train technical support executives and system directors to never reveal Passwords and other information by phone or email.
C. Implement strong credential, token or biometric authentication; training: and strict monitoring by security guards.
D. Employee training, best practices, and checklists for using passwords. Ensure that all guests are escorted by employee or relevant personnel.
E. Educate vendors about social engineering.
F. Lock and monitor the mailroom, including employee training.
G. Keep phone closets, server rooms, etc. locked at all times and keep equipment inventory updated.
H. Train executives to never reveal identity, passwords, or other confidential information by phone or email.
I. Keep all trash in secured and monitored areas, shred important data, and erase magnetic media.

V. CONCLUSIONS

Social engineering is a manner by which an interloper can gain admittance to your data assets without being a specialized, organization, or security master. The attacker can utilize numerous strategies either to trick the casualty into giving the data he needs to acquire passage or to get the data without the casualty's information. Social engineering can be a danger to the security of any association. It is critical to comprehend the meaning of this danger and the manners by which it very well may be shown. Really at that time can fitting counter-measures be utilized and kept everything under control to ensure an organization. Reporting is the last step. The pen tester should list every one of the aftereffects of the social engineering pen test in the report. While producing the report, the pen tester ought to consider the intended interest group of the report. By and large, as a rule, the crowd contains the senior administration of the association. The report should address every one of the important viewpoints relating to the underlying arranging and perusing, target ID, tests led, and recognized vulnerabilities. Alongside the recognized vulnerabilities, the report should likewise incorporate the suggestions and countermeasures needed to alleviate the distinguished vulnerabilities and defeat future assaults.

REFERENCES

[1] Wenke Lee, Bo Rotoloni, “Emerging cyber threats, trends and technologies”, Technical report, Institute for Information Security and Privacy, 2016.
[2] Nabie Y Conteh, Paul J Schmick, “Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks”, International Journal of Advanced Computer Research, Vol.6 pp.23- 31, 2016
[3] “Hacking the human operating system: The role of social engineering within cybersecurity”, Technical report, Intel Security, 2015.
[4] Andrea Cullen, Lorna Armitage, “The social engineering attack spiral (seas). In Cyber Security And Protection Of Digital Services (Cyber Security)”, 2016 International Conference On, pp.1-6, IEEE, 2016.
[5] Avoiding Social Engineering and Phishing Attacks, Cyber Security Tip ST04-014, by Mindi McDowell, Carnegie Mellon University, June 2007.
[6] The Risk of Social Engineering on Information Security, A Survey of IT Professionals,September 2011.
[7] “Social engineering fraud: questions and answers”, Technical report, Interpol, December 2015.
[8] Katharina Krombholz, Heidelinde Hobel, Markus Huber, Edgar Weippl, “Advanced social engineering attacks”, Journal of Information Security and applications, Vol.22, pp.113-122, 2015.
[9] Parker Graeme, Shala Vlerar, “Social engineering and risk from cyber-attacks”, Technical report, PECB, March 2016.
[10] Rabinovitch E., “Staying Protected from Social Engineering," Communications Magazine, IEEE, Volume: 45, Issue: 9, Digital Object Identifier: 10.1109/MCOM.2007.4342845, Publication Year: 2007, Page(s): 20 –21.

©IJRASET: All Rights are Reserved

AUTHORS PROFILE

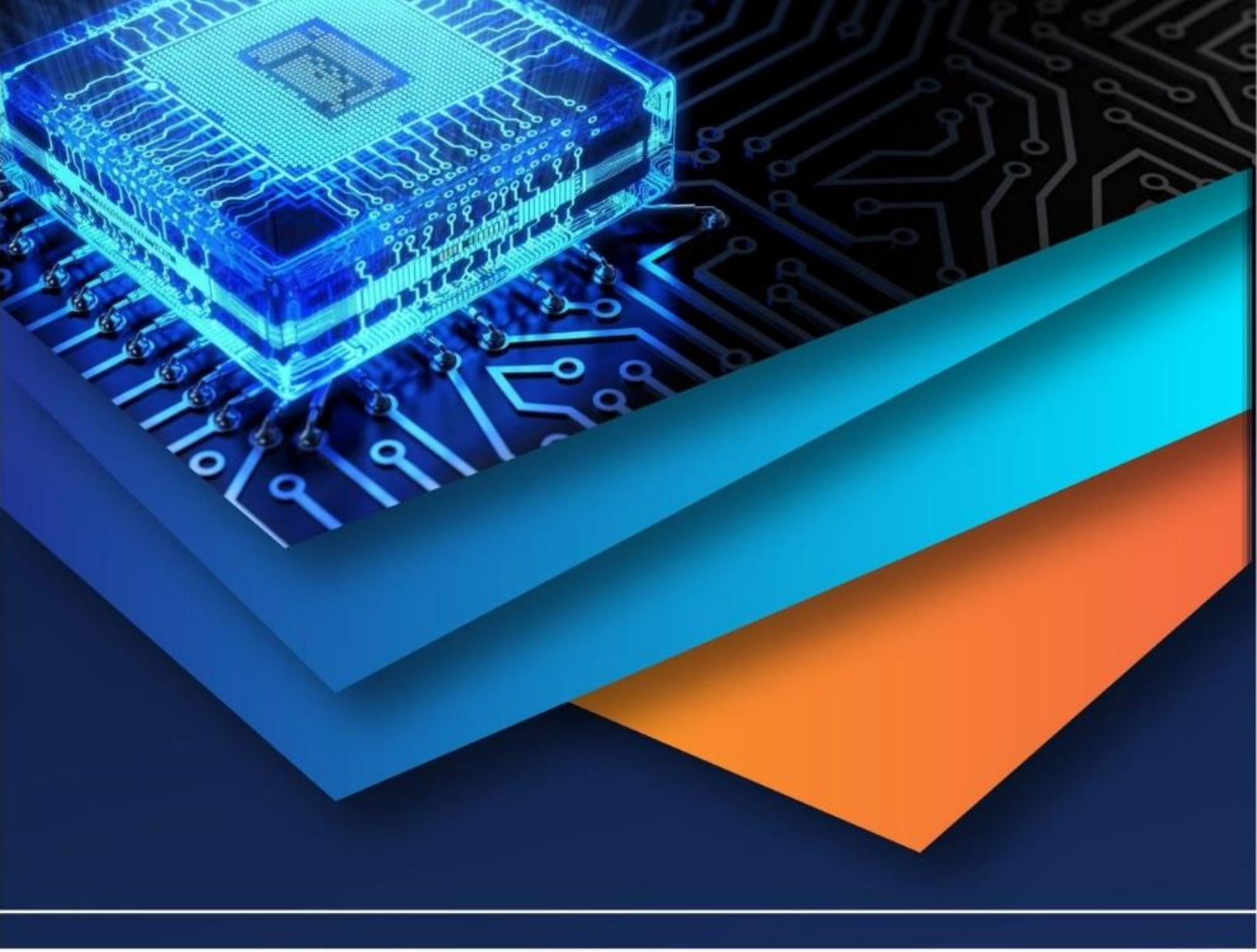
Vamshi krishna Motru is a cyber security enthusiast. He has a strong knowledge of cybersecurity and proficient in risk analysis and vulnerability assessment and penetration testing. He was also featured in different MNC'c like Mastercard, Pinterest, TripAdvisor, Atlassian, DELL and Secured over 35+ companies.

Ch Mvn Sai Teja Prashanth is an Ardent Security Researcher and Bug Bounty Hunter. He has good experience in Web-app security, Android-app security, and Vulnerability Assessment and Penetration testing. He has been featured in MNC's like United Nations, Netflix, Indeed, Swiggy, Big basket, and many more.

Guntoju Deepak is a cyber security Ninja. He has experience in OSINT, malware analysis, Android security and VAPT. He has been featured in organization like Bitdefender, DELL, Western Union, Statuspage, Cloudways, $(ISC)^2$, Kenna Security.

Ekke Karthik is a cybersecurity researcher and instructor. He has good knowledge of web- VAPT and his research areas include android testing, social engineering attacks, and methodologies. He also secures hall of fame in Blue jeans network, Naspers, Western Union, Sophos, Ibotta, Under Armour, Tello, Statuspage, Bit Discovery.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)