BRAHMA TEJA KALAPALA

Security Analyst – VAPT

9014970560 | k.brahmateja24@gmail.com | https://www.linkedin.com/in/brahma-teja-kalapala-b96aa424a

---

OBJECTIVE

Skilled and detail-oriented cybersecurity with hands-on experience in Vulnerability Assessment and Penetration Testing (VAPT). Proficient in identifying, analyzing, and mitigating security risks across diverse systems and networks. Committed to maintaining up-to-date knowledge of the latest vulnerabilities and attack vectors to proactively safeguard data and systems.

KEY SKILLS

1. Vulnerability Assessment
2. Penetration Testing
3. Application Security
4. Network Security
5. Malware
6. Metasploit
7. OWASP TOP 10
8. Burp Suite
9. Nmap
10. CSRF
11. SOC
12. SIEM

PROFESSIONAL EXPERIENCE

Kleap Institute of Information security   **From Jul 2024 – Dec 2024**

- **Security Analyst - VAPT**

Currently working as a Security Analyst Intern specializing in Vulnerability Assessment and Penetration Testing (VAPT) at the KLEAP Institute of Information Security (KIIS), I possess six months of hands-on experience in web application security and vulnerability assessment and Penetration Testing and Bug Bounty, SOC, SIEM, Information Security Certified Consultant (ISCC).

EDUCATION

QUALIFICATION	UNIVERSITY	YEAR
B.Tech (Computer science and Business Systems)	Qis College Of Engineering & Technology	2020 - 2024
Intermediate (M.P.C)	Narayana Jr college	2018 - 2020
SSC	ZPHS BOYS HIGH SCHOOL	2013 - 2018

CERTIFICATIONS

- Certified Penetration Tester
- Certified AppSec Practitioner (The SecOps Group)
- Certified Network Security Practitioner (The SecOps Group)
- Cyber Security Virtual Internship (Palo Alto)
- Introduction to Cyber Security (Palo Alto)
- Fundamentals of SOC (Palo Alto)
- Fundamentals of Network Security (Palo Alto)
- Ethical Hacking Essentials (EC-Council)
- Ethical Hacking (Internshala)

- **User names and Email I'Ds Bypassing:**
  http://testphp.vulnweb.com/
  Scenario: Attack on a Website Using CSRF to Change User Names and Emails.
    1. **Change a victim's username and email address Using Burp suit.**
    2. The attack modifies the victim's username and email in their account settings to those specified in the crafted request.
    3. Take same website in two different browsers and login, after one website use Burp proxy and on the intercept and change the username and Email and go to the request section and go to Engagement tools and select Generate CSRF POC and copy the html code and paste it in another browse which was you login the same website and refresh the browser and the username and Email changed.

- **OTPs Bypass:**

  https://www.instafinancials.com/
  Scenario: Attack on a Website Using CSRF to Bypass Phone Number and OTP.
    1. **Bypassing OTP and Phone Number Using Burp suite:**
    2. Enter the random number in section and capture the request in Burp suite.
    3. Do intercept to Response to this request, after you get POST request and go to response section and get a like "NEW USER" forward the request, finally phone number bypass successfully.
    4. Enter the random OTP in section and capture the request in Burp suite.
    5. Do intercept to Response to this request, after you get POST request and go to response section and get a like "d":2 and change it into 1, forward the request Finally phone number bypass successfully.
    6. For OTP Bypass "failure - success 0 - 1".

  https://wd103.myworkday.com/wday/authgwy/accenture/login-saml.htmld
  Scenario: Attack on a Website Using CSRF to Bypass Phone Number and OTP.
    1. **Bypassing OTP Using Burp suite:**
    2. Using credentials login on login page.
    3. Turn on the Burp suite and enter a random OTP and capture the request in the burp suite.
    4. In the request section Do intercept and send the forward the response.
    5. In the response section just Drop the section and turn off the burp suite and visit login page you successfully login.

Declaration:

I hereby declare that the information given above data is true to the best of my knowledge and belief and nothing has been concealed therein.