SNAPSEC

A Cybersecurity and Penetration testing company.

SNAPSEC

A Cybersecurity and Penetration testing company.

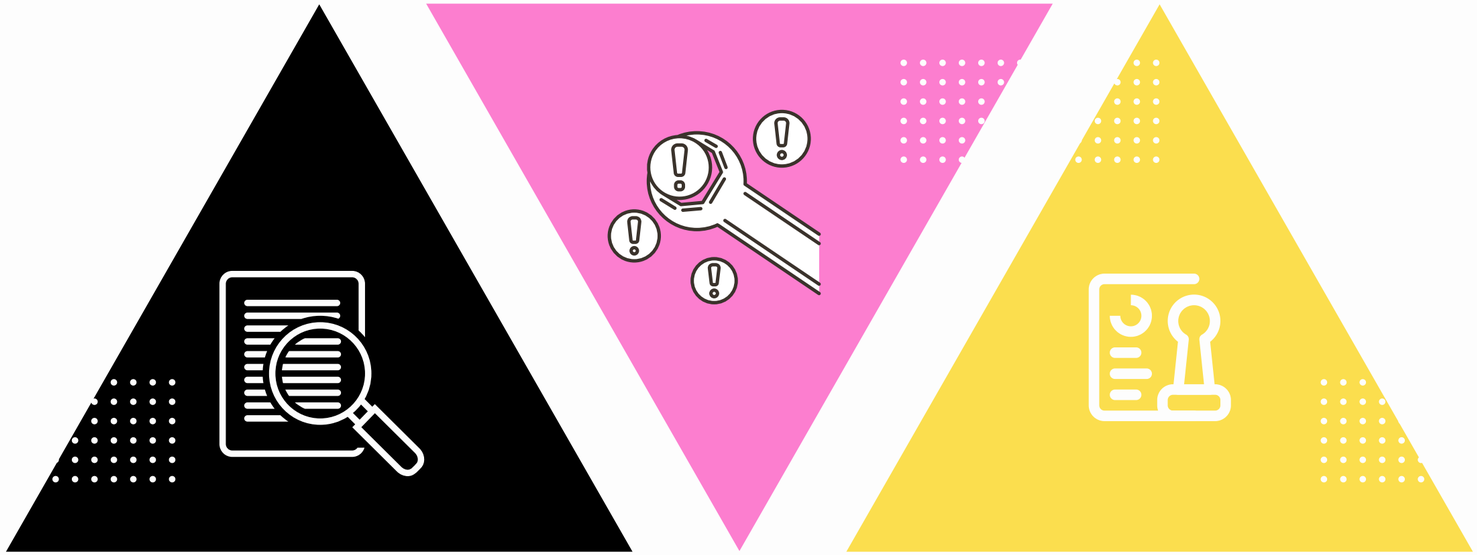
WHO WE ARE?

"OUR MISSION IS TO PROVIDE HIGH QUALITY PENETRATION TESTING SERVICES TO OUR CLIENTS"

In terms of handling and processing information, modern web applications have become much more complex and gigantic. This undoubtedly increases the complexity of the business logic and application logic within these applications. It is, therefore, necessary for us to use modern community-driven approaches, methodologies, and tactics to test these modern web applications, and to encourage our team members to go beyond known vulnerability classes and attack the application and business logic within these vulnerabilities to ensure the quality of our services.

THE PROCESS

NDA SIGNED



Find & Report

We identify security flaws in your assets and provide you with a comprehensive report on them.

Fix

We assist you in resolving those issues.

Confirm

We check to see if the security issues have been resolved properly and can be bypassed.

OUR SERVICES

OUR MOST POPULAR SERVICES.

1. Web Application Vulnerability assesment and Penetration Testing (VAPT)
2. Mobile Application Penetration Testing. IOS / Androd
3. API Security Testing.
4. Infrastructure Penetration Testing.
5. Vulnerability Scanning.
6. Access Control Model Evaluation (Role Based Testing)
7. Continuous Security Testing

ACKNOWLEDGEMENTS

OUR WORK IS THE PRESENTATION OF OUR CAPABILITIES.

LIST OF COMPANIES WE HAVE HELPED IN PAST:

- Typeform
- Lark Technologies
- Box BB
- Agorapulse
- Zendesk Sell
- Citrix Systems Private
- Lucid Software
- Amplitude, Inc.
- Grammarly
- PlanGrid
- Zendesk
- Officevibe
- Statuspage
- Hibob
- Bill.com
- Auth0
- Samsara
- Campaign Monitor
- Atlassian
- Sophos
- DocuSign
- Twilio
- waitwhile
- Workiva
- Dialpad
- Parsable
- Mailgun
- Home-Connect
- Infobip
- 7Geese
- Sailthru
- SoundCloud
- Blue Jeans Network
- Opsgenie
- Vidio.com
- Peakon
- Kenna Security
- Smartsheet
- Upwork
- doxo
- Snowflake
- mixmax
- Coinbase
- 8x8 Bounty
- CRITEO
- Miro
- Chaturbate
- Clever
- GSOFT
- OpenSea
- Yahoo!
- Dell Technologies
- SEEK
- BetterHelp
- Frame.io
- Mailchimp
- Brex
- Conveyor
- GoPro
- Dialpad VDP
- Contentful
- HOVER
- Kiwi.com
- Schoology
- Udacity
- Workable

For more information on our public work, Visit:

https://bugcrowd.com/snapsec

https://hackerone.com/snapsec

OUR WORK

OVER THE LAST 2 YEARS.

HELPED: 64+ ORGINISATIONS

SECURITY REPORT: 1000

- Helped **Typeform** by identifying and reporting More than **100** security issues to them.
- Helped **Auth0** by identifying and reporting More than **50** security issues to them.
- Helped **Samsara** by identifying and reporting More than **50** security issues to them.
- Helped **Hibob** by identifying and reporting More than **44** security issues to them.
- Helped **Zendesk** by identifying and reporting More than **20** security issues to them.
- Helped **Atlassian** by identifying and reporting More than **40** security issues to them.
- Helped **Sophos** by identifying and reporting More than **10** security issues to them.
- Helped **Box** Technologies by identifying and reporting More than 40 security issues to them.
- **and more 60+ Companies.**

Public Appearances

Our team have spoken about ApPsec a couple of times.

OWASP

Talk - BASH and RECON V1

Null0x01

Getting Started in Appsec and Bug bounties.

DarkCON

Talk - Bash & Recon V2

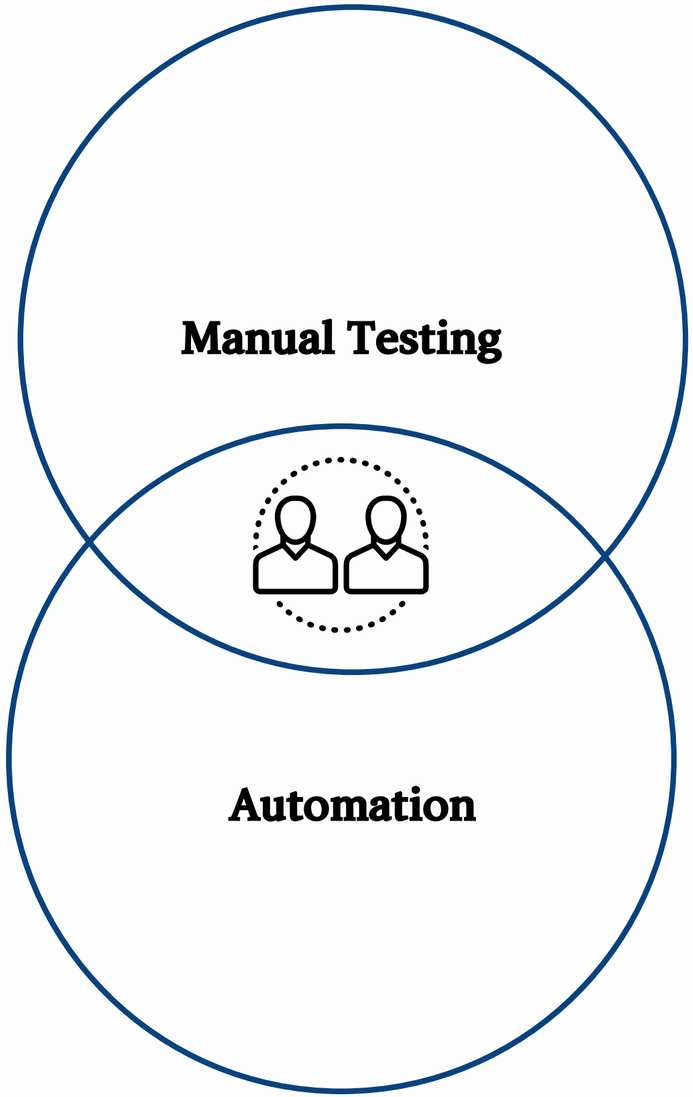
ThreatCON

Attacking Access Control Models in Modern Web Apps

[INDIA] CIO Business insider Magazine

TOP 10 Application Security Service Providers

OUR APPROACH



IN-DEPTH APPLICATION LOGIC TESTING	OUR TEAM IS CAPABLE OF PERFORMING IN-DEPTH APPLICATION LOGIC TESTING WHICH ALLOWS THEM TO FIND BUGS OUTSIDE OF KNOWN VULNERABILITY CLASSES.
BUSINESS LOGIC ISSUES	ATTACKING THE BUSINESS PERSPECTIVE OF AN APPLICATION REMAINS OUR PRIORITY DURING THE TESTING PHASE WHICH ALLOWS US TO ATTACK AND FIND ISSUES IN THE BUSINESS LOGIC OF THE APPLICATION.
MANUAL EXPLOITATION FOR MAXIMUM IMPACT.	EACH VULNERABILITY FOUND THROUGH AUTOMATION IS MANUALLY VERIFIED AND ESCALATED BY OUR TEAM MEMBERS BEFORE INCLUDING IT TO THE REPORT.

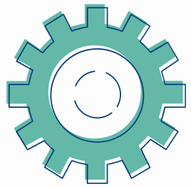
OPEN SOURCE TOOLS	WE CONTINUE TO KEEP TRACK OF NEW OPEN SOURCE SECURITY TOOLS AND USE THEM FOR SCANNING AND COLLECTING DATA ABOUT OUR TARGET.
COMMUNITY DRIVEN APPROACHES	OUR APPROACHES ARE COMMUNITY-DRIVEN, WHICH MEANS WE KEEP TRACKING NEW METHODOLOGIES, APPROACHES, AND WAYS TO ATTACK DIFFERENT TECHNOLOGIES.
ATTACK SURFACE REPORTS	WE PROVIDE OUR CLIENTS WITH A COMPREHENSIVE REPORT OF THEIR ATTACK SURFACE WHICH PROVIDES THEM PROVIDES YOU WITH THE DETAILS OF YOUR ORGANIZATION'S EXPOSED APPLICATIONS AND SERVERS TO A PUBLIC NETWORK. (WE CHARGE NOTHING FOR THIS)

WHAT DO WE LOOK FOR ?

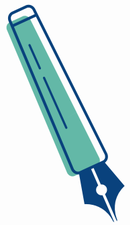
What do we Look for :

List of Vulnerabilities that we Look for

XSS



CSRF



SQLi

CORS issues

Logic Issues

IDOR

Email Misconfigrations

Cloud Misconfigrations

File Upload vulnerabilites

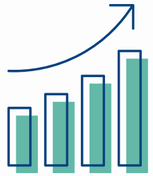
Open redirect

File Inclusion

Authorization Issues

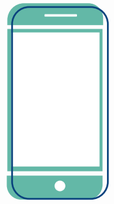
CI scanning

XSS



XSS

XSS



Authentication Issues

3rd party Misconfigrations

ClickJacking

Race Conditions

OUR TEAM

Technical TEAM

Imran Parray
CEO and Founder

Mubashir Parray
Security Lead

Adnan Shah
Junior Penetration Tester

Abdul Basit
Senior Penetration Tester

Waseem Raja
Junior Penetration Tester

Danish Bhat
Senior Penetration Tester

Imran Nissar
Senior Offensive Security Consultant

Sales Team

Shahnawaz Shafi
Director of Partnerships

Danish Ahmed
Sales and Marketing Director

Altaf Ahmed
Lead Generation Specialist

Marketing & Content

Hafeez Mir
Social Media Manager

Sahil Phalle
Intern | Content Writer

Web Developer

Saleem Yousuf
Full Stack Web Developer

THANK YOU.

QUESTIONS ?