www.secupent.com

SECUPENT

Aim to Secure the modern internet

Office:
House# 1066, Road# 7, Avenue# 7
Mirpur DOHS, Dhaka-1216
Call: +880-1681274842
Email: service@secupent.com

WEBSITE PENETRATION TESTING

Do you know in the modern era websites and related applications are tantalizing dishes for the cyber criminals? If you have already known then obviously you are thinking about protecting your site with virtual shield what we call security. A website Penetration testing is a made-up task in order to find any flaw or loophole in your web application. It is a methodological approach to identify the loopholes in your web application. Your website is your appearance of business. So it should be keep neat and clean as a part of fulfilling corporate objective.

Our Specialty

We know Business begets risk and you just entered the right place. We have more than four years of experience of web app penetration testing era. We are trusted, honest and provide better quality! Moreover, we value our clients minimizing business risk and saving cost and time. We deliver you

- Minimizing business risk and saving cost.
- We have team of experts who're specialized on Penetration Testing Service and OWASP member working day and night for solving problems and protecting you from potential future threats.
- CVE, OSVDB and Zero-Day Exploit Testing.
- Patch Management and Bug Fixing.
- Full Source Code Inspection, White Box, Black Box and Grey Box testing.
- Threat Modeling & Security Review.
- Post Exploitation & Final Report.
- Manual & Auto Scanning and Vulnerability Identification.

Office:
House# 1066, Road# 7, Avenue# 7, Mirpur DOHS, Dhaka-1216
Mobile: +880-1681274842, Email: service@secupent.com

SECUPENT
Aim to Secure the modern internet

NETWORK PENETRATION TESTING

For a business, Network is like a nervous system for exchanging processed information. If you look at the network over the world, you can see a complex spider web like net active 24X7. Modern networking system connects people within seconds regardless of your location. So it is natural that criminals will set their focus on your network to tap information on the way while you are bypassing your data to another destination. And Cyber criminals are also waiting for you. That's the reason you need secured network. Penetration Testing is such a methodical test that it is forged from the perspective of an intruder in order to find any loophole or flaw in your Network System. As you are busy with your business and handling clients, there is hardly any time to concentrate on security. No problem!!! We are prepared with our experts here as you're helping hand and guaranteeing your network security while you are doing business with your customers.

Our Service:

Now the purpose of our service is to identify what type of resources are exposed to the outer world determining the security risk involved in it & detecting the possible types of attack. We minimize your IT security burden, cost and save time by adding a better value to your investment. For you to apprehend properly we are listing our services.

- We discover known and unknown (Zero-Day) vulnerabilities of your system before someone gets access of it.
- We test all software and devices install in your network as like router, IPS, IDS, firewall, switch, DNS, FTP, Mail, SharePoint, access point, all services ports etc.
- CVE, OSVDB and Zero-Day Exploit Testing.
- Threat Modeling & Security Review.
- Post Exploitation & Final Report.
- Our service also includes WEP/WPA Cracking and Cloud environmentpenetration testing.
- Black box and white box test is our usual service.
- Penetration testing also helps your business to comply like PCI DSS, HIPAA and ISO127001.

Office:
House# 1066, Road# 7, Avenue# 7, Mirpur DOHS, Dhaka-1216
Mobile: +880-1681274842, Email: service@secupent.com

SECUPENT
Aim to Secure the modern internet

SERVER PENETRATION TESTING

It's the method of testing the areas of weakness in server systems in terms of security that are put to test to determine, if 'weak-point' is indeed exists, that can be broken into or not. There are a handful of reasons for performing a penetration test for your server. Vulnerabilities need to be identified by both the penetration tester and the vulnerability scanner. The steps are similar for the security tester and an unauthorized attacker. The attacker may choose to proceed more slowly to avoid detection, but some penetration testers will also start slowly so that the target company can learn where their detection threshold is and make improvements.

Our services:

- On-demand penetration Testing based on your system.
- Hardware and software Exploits Development.
- SQL and NoSQL Database Security.
- CVE, OSVDB and Zero-Day Exploit Testing.
- Application and hardware level firewall set-up and configuration.
- IDS Testing & Set-up.
- Server OS vulnerability testing.
- System Upgrade, update based on demand.
- Server service Port Scanning and vulnerability check.
- Fuzzing Service port.
- DOS & DDOS attack testing and mitigation.

Office:
House# 1066, Road# 7, Avenue# 7, Mirpur DOHS, Dhaka-1216
Mobile: +880-1681274842, Email: service@secupent.com

SECUPENT
Aim to Secure the modern internet

ADVANCE CMS SECURITY

Why CMS Security

WordPress, Joomla, Magento are most popular content management system in this time because of easy customization and user friendly user interface. They are also most targeted application by Hackers. Hundreds of thousands of Joomla, WordPress sites are hacked, compromised, defaced and data leaked by attackers (Mostly known as hackers). Last year Over 100,000 WordPress sites were infected with malicious malwares, reminding everyone just how vulnerable they are. So if you are CMS users then you must need to update from its security threats.

Our Features:

- Full Penetration Test report
- Discover all risk of your CMS
- Check all CVE, OSVDB, CWE and Zeroday exploits.
- Remove backdoor, Google Blacklist, Shell, and Malware etc. from your CMS.
- Check all of known vulnerability line by line of your code, such as: SQL Injection, XSS, LFI, CSRF, RCC etc.
- Brute-force and DOS attack.
- Scan content and bad URLs and perimeters.
- Monitor DNS
- Any new updated vulnerability report for core CMS or plugins.
- On demand Patch Management Solution
- Premium support (24×7/365 Days our support teams are awake for you!)

Office:
House# 1066, Road# 7, Avenue# 7, Mirpur DOHS, Dhaka-1216
Mobile: +880-1681274842, Email: service@secupent.com

SECUPENT
Aim to Secure the modern internet

EXPLOIT DEVELOPMENT

Exploit is some kind of script designed for taking advantage of the vulnerability. It is the most potential threat for any system or network. There are two kinds of exploits, one is Zeroday another is Non-Zeroday.

Zeroday Exploits means they are not listed in any known database like CVE or OSVDB. Even they are 100% unknown for vendors and users.

Non-Zeorday Exploits are known, they are already listed in database and vendors know about it. But maybe they were patch in new version not in previous version. In this case many users still have risk on it. Maximum time almost 80% users are not aware from update their system daily. So there is chance they can be exploit via knows Exploit aka Non-Zeorday Exploits.

In SECUPENT we can build useful exploits for you with 100% secured Non-Disclosure Agreement.

Our Features are:

- Zero-day and Non Zero-day (one-day) exploit development Service.
- On Demand exploit development service.
- General Agreement and Non-disclosure Agreement basis exploit Service.
- We already have the availability of many Zero-day and Non Zero-day (one-day) both kinds of exploits.
- We support all remote andlocal exploit development service.
- We support all kind of WebApps including CMS and Control Panels.
- Support Network related exploits as like router, IDS, firewall exploits
- Support Software services in servers with software and services.
- And we also can provide you user level exploits like browsers, media player related exploit services.

Office:
House# 1066, Road# 7, Avenue# 7, Mirpur DOHS, Dhaka-1216
Mobile: +880-1681274842, Email: service@secupent.com

CLOUD SECURITY

Cloud computing is phenomenon in current IT industry. Many of organizations use SaaS, PaaS, and IaaS etc. But there are many security issues associated with cloud infrastructures. Cloud computing poses several data protection risks such as since service providers can access data stored in the cloud storage at any time, they can pass sensitive information to third parties. In some cases, it may be difficult for the cloud customers (in its role as data controller) to effectively check the data handling practices of the cloud provider and thus to be sure that the data is handled in proper way. This problem is exacerbated in cases of multiple transfers of data, e.g., between federated clouds. On the other hand, some cloud providers do provide information on their data handling practices. Some also offer certification summaries on their data processing and data security activities and the data controls they have in place, e.g., SAS70 certification.

Our Services in Cloud Security areas are:

- Software as a Service (SaaS) penetration testing service
- Platform as a Service (PasS) penetration testing service
- Infrastructure as a Service (Iaas) penetration testing service
- Cloud ERP Security Solution
- AWS, Digital Ocean, Soft layer, Rackspace, Azure Optimizing and testing
- Fully managed service in cloud environment with firewall, log manager, monitoring system etc.
- Cloud Data Security and Data Protection Checking failure of mechanism
- Port Scan, vulnerability detection
- CVE, OSVDB SCAN and Details.
- And your own security demand

Office:
House# 1066, Road# 7, Avenue# 7, Mirpur DOHS, Dhaka-1216
Mobile: +880-1681274842, Email: service@secupent.com

VULNERABILITY MANAGEMENT

When we come to discuss the vulnerability, definitely something haunting arise in your mind. In terms of IT, vulnerability is a weakness or flaw which allows an attacker to gain unauthorized access into sensitive information database. Vulnerability Management is the cyclical and typical practice of identifying, classifying, remediating, and mitigating vulnerabilities. To exploit vulnerability, an attacker must have at least one applicable tool or technique that can connect to your system weakness. Yet, when exploited by very skilled attackers, these vulnerabilities can undermine an organization's defenses and expose it to significant damage. That's the reason we provide this services to our customer. In this case you just need to subscribe our services and rest of all work will be ours. We will monitor, test, check all vulnerability and security issues in your system and patch them in daily basis. So you can be safe from any attack from cyber criminals.

Our Features:

- A self-driven, on-demand service.
- Quick detection and vulnerability mitigation.
- 100% false positive detection, which will save many money and time.
- Our daily monitor includes zeroday which is rare in current industry.
- Manual & Auto vulnerability assessment report.
- CVE & OSVDB updates and patch all system software and services
- 100% Compatible with compliance like PCI DSS 3.0, ISO 127001:2013, and HIPAA etc.
- And 24X7X365 System vulnerability updates and Monitoring

Office:
House# 1066, Road# 7, Avenue# 7, Mirpur DOHS, Dhaka-1216
Mobile: +880-1681274842, Email: service@secupent.com

SECUPENT
Aim to Secure the modern internet

OWASP TOP 10

WHAT IS OWASP TOP 10?

The OWASP Top Ten is a list of the 10 most dangerous current Web application security flaws, along with effective methods of dealing with those flaws. OWASP (Open Web Application Security Project) is an organization that provides unbiased and practical, cost-effective information about computer and Internet applications.

WHY YOU NEED THAT?

OWASP (Open Web Application Security Project) has top 10 security flaws for website which can be exploited by cyber criminals. And this is highly slandered security testing for web application. So you can secure from unethical hackers with this security solutions.

We give you report all latest OWASP top 10 security updates. However if you want report based on previous one then it's also possible.

OWASP Top 10 – 2013 (New)

- A1 – Injection
- A2 – Broken Authenticion and Session Management
- A3 – Cross-Site Scripting (XSS)
- A4 – Insecure Direct Object References
- A5 – Security Misconfiguration
- A6 – Sensitive Data Exposure
- A7 – Missing Function Level Access Control
- A8 – Cross-Site Request Forgery (CSRF)
- A9 – Using Known Vulnerable Components
- A10 – Unvalidated Redirects and Forwards

Office:
House# 1066, Road# 7, Avenue# 7, Mirpur DOHS, Dhaka-1216
Mobile: +880-1681274842, Email: service@secupent.com

ISO/IEC 27001:2013

WHAT IS ISO?

The International Organization for Standardization (ISO) is an international standard-setting body composed of representatives from various national standards organizations. ISO founded on 23 February 1947, the organization promotes worldwide proprietary, industrial and commercial standards. It is headquartered in Geneva, Switzerland, and as of 2013 works in 164 countries.

WHAT IS IEC?

The International Electrotechnical Commission (IEC) is a non-profit, non-governmental international standards organization that prepares and publishes International Standards for all electrical, electronic and related technologies – collectively known as “electro technology”. IEC standards cover a vast range of technologies from power generation, transmission and distribution to home appliances and office equipment, semiconductors, fiber optics, batteries, solar energy, nanotechnology and marine energy as well as many others. The IEC also manages three global conformity assessment systems that certify whether equipment, system or components conform to its International Standards.

WHAT IS ISO/IEC 27001?

ISO 27001 is an information security standard, which is published by theInternational Organization for Standardization (ISO) and theInternational Electro technical Commission (IEC) under the joint ISO and IEC subcommittee, ISO/IEC JTC 1/SC 27. It is a specification for an information security management system (ISMS). Organizations which meet the standard may gain an official certification issued by an independent and accredited certification body on successful completion of a formal audit process.

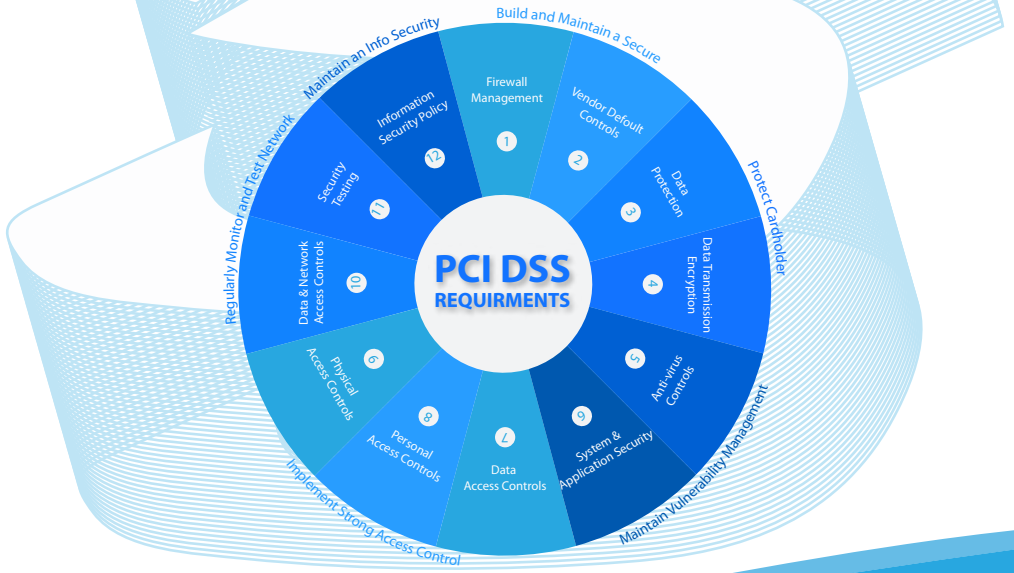
Office:
House# 1066, Road# 7, Avenue# 7, Mirpur DOHS, Dhaka-1216
Mobile: +880-1681274842, Email: service@secupent.com

PCI DSS 3.0

secupent.com
#secupent
/secupent
secupent

WHAT IS PCI DSS?

The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that all companies that process, store or transmitcredit card information maintain a secure environment. Essentially any merchant that has a Merchant ID (MID).The Payment Card Industry Security Standards Council (PCI SSC) was launched on September 7, 2006 to manage the ongoing evolution of the Payment Card Industry (PCI) security standards with focus on improving payment account security throughout the transaction process. The PCI DSS is administered and managed by the PCI SSC (www.pcisecuritystandards.org), an independent body that was created by the major payment card brands (Visa, MasterCard, American Express, Discover and JCB.).



Office:
House# 1066, Road# 7, Avenue# 7, Mirpur DOHS, Dhaka-1216
Mobile: +880-1681274842, Email: service@secupent.com

SECUPENT
Aim to Secure the modern internet

CWE/SANS TOP 25

WHAT IS CWE/SANS TOP 25

The 2011 CWE/SANS Top 25 Most Dangerous Software Errors is a list of the most widespread and critical errors that can lead to serious vulnerabilities in software. They are often easy to find, and easy to exploit. They are dangerous because they will frequently allow attackers to completely take over the software, steal data, or prevent

Insecure Interaction between Components

- SQL Injection
- OS Command Injection
- Cross-site Scripting
- Unrestricted Upload of File with Dangerous Type
- Cross-Site Request Forgery (CSRF)
- URL Redirection to Untrusted Site ('Open Redirect')

Risky Resource Management

- Classic Buffer Overflow
- Path Traversal
- Download of Code Without Integrity Check
- Inclusion of Functionality from Untrusted Control Sphere
- Use of Potentially Dangerous Function
- Incorrect Calculation of Buffer Size
- Uncontrolled Format String
- Integer Overflow or Wraparound

Porous Defenses

- Missing Authentication for Critical Function
- Missing Authorization
- Use of Hard-coded Credentials
- Missing Encryption of Sensitive Data
- Reliance on Untrusted Inputs in a Security Decision
- Execution with Unnecessary Privileges
- Incorrect Authorization
- Incorrect Permission Assignment for Critical Resource
- Use of a Broken or Risky Cryptographic Algorithm
- Improper Restriction of Excessive Authentication Attempts
- Use of a One-Way Hash without a Salt

Office:
House# 1066, Road# 7, Avenue# 7, Mirpur DOHS, Dhaka-1216
Mobile: +880-1681274842, Email: service@secupent.com

SARBANES-OXLEY ACT

Sarbanes–Oxley Act of 2002 (SOX)

The Sarbanes–Oxley Act of 2002 (SOX) commonly called Sarbanes–Oxley, Sarbox or SOX, is a United States federal law that set new or expanded requirements for all U.S. public company boards, management and public accounting firms. There are also a number of provisions of the Act that also apply to privately held companies, for example the willful destruction of evidence to impede a Federal investigation.

SOX requires the chief executive officers (CEO) and chief financial officers (CFO) of public companies to attest to the accuracy of financial reports (Section 302) and require public companies to establish adequate internal controls over financial reporting (Section 404). Passage of SOX resulted in an increased focus on IT controls, as these support financial processing and therefore fall into the scope of management's assessment of internal control under Section 404 of SOX.

302	404	409	802
Corporate Responsibility for Financial Reports	Management Assessment of Internal Controls	Real-time Issuer Disclosures	Criminal Penalties for Altering Documents

Office:
House# 1066, Road# 7, Avenue# 7, Mirpur DOHS, Dhaka-1216
Mobile: +880-1681274842, Email: service@secupent.com

INCIDENT RESPONSE

SECUPENT's Incident Response service for all kind of under attack websites, server, network and system. We provide very fast and proper solution. We just not provide only recover solution our services included protection from future threat. So being with SECUPENT is not only todays help, it's a long term support and service for you.

We will analyse your under attack website

Check all server logs, malware, all authentication logs, and determind total risk in your system.

Cleaning all hacked codes from your website

We will clean all maleware, shell, iframe injection code, backdoor & other exploits. And we will also check your codes for suspect vulnerabilities. Now we will help to secure your system

Now we will help to secure your system

We will check vulnerabilities in your website and give you available patch. We also analyse zero-day exploits and patch them. So you can get overall solutions by us.

Long term update and management services

We will provide your long term update and management services based on your demand. So you don't need to think about your future updates and attacks because we are with you.

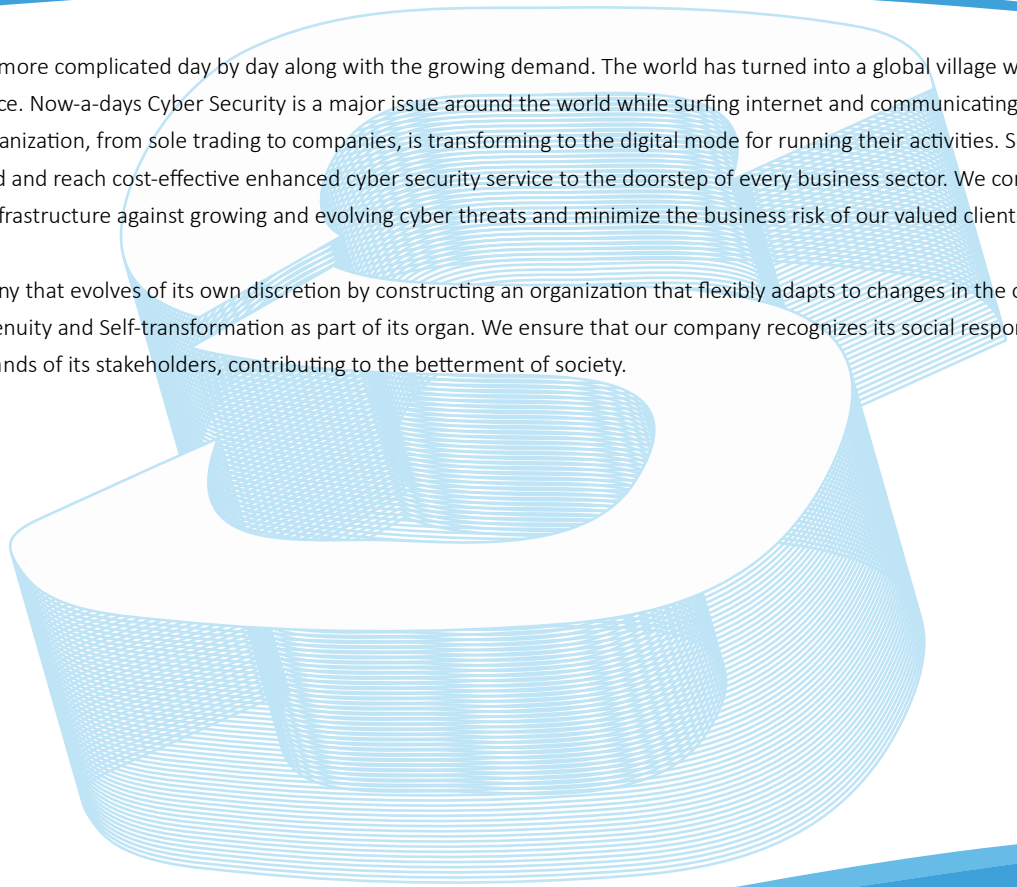
Office:
House# 1066, Road# 7, Avenue# 7, Mirpur DOHS, Dhaka-1216
Mobile: +880-1681274842, Email: service@secupent.com

SECUPENT
Aim to Secure the modern internet

OUR VISION

Today's Hi-tech world is getting more complicated day by day along with the growing demand. The world has turned into a global village where communication system came to second's distance. Now-a-days Cyber Security is a major issue around the world while surfing internet and communicating and storing sensitive data. Almost every business organization, from sole trading to companies, is transforming to the digital mode for running their activities. Secupent holds the motto to create a risk free Cyber World and reach cost-effective enhanced cyber security service to the doorstep of every business sector. We concentrate on Total Quality Management, protect critical infrastructure against growing and evolving cyber threats and minimize the business risk of our valued clients.

We will continue to be a company that evolves of its own discretion by constructing an organization that flexibly adapts to changes in the operating environment and incorporates corporate Ingenuity and Self-transformation as part of its organ. We ensure that our company recognizes its social responsibilities as a member of society, while fulfilling the demands of its stakeholders, contributing to the betterment of society.



Office:
House# 1066, Road# 7, Avenue# 7, Mirpur DOHS, Dhaka-1216
Mobile: +880-1681274842, Email: service@secupent.com

SECUPENT
Aim to Secure the modern internet

WHY YOU CHOOSE US

We are passionate, loyal and committed to you. At Secupent, we care about our clients because trust and commitment hold the key factor in every business relationship. We pride ourselves on going above and beyond the boundaries of typical customer service to truly exceed the expectations of those we work with. We build personal relationships with our clients and view ourselves as extensions of their business. As their partners, we work hard to help them succeed since the only true measure of our success is their own.

Not only are the people from our company experienced with Cyber Security, but we truly believe in what we do. We focus on strategies designed to increase your performance. Moreover, we provide you custom solution on your proper demand. That makes pentest more reliable and more perfect. We also follow all OWASP, PCI, ISO, and NIST Rules and Procedures that provides totally high quality solution that meets international demand.

Then why not experiencing the power of working with someone who is excited about what they can accomplish and who fully believes in the end goal!!! See for yourself the difference we've made for our clients. We are at your service 24/7 next to you. So, place your order and relax because rest is ours.

Office:
House# 1066, Road# 7, Avenue# 7, Mirpur DOHS, Dhaka-1216
Mobile: +880-1681274842, Email: service@secupent.com

SECUPENT
Aim to Secure the modern internet

ABOUT US

SECUPENT has been providing cyber security service and exploit development successfully with a highly experienced robust team since its inception and only one in local market. Here we put our limelight on quality assurance within binding time according to the taste of our valued clients.

We meet all of your security demand, provide you protection from your future threats and Restore your system from any security disaster. Every business entity wants to cut cost as low as possible keeping the expected quality at least. Bearing the Total Quality Management in mind, SECUPENT delivers the most accurate, complete and cost-effective website security solution available today. When most of the companies concentrate on protecting their networks, websites remain unprotected without defense and fall prey to the attack of cyber criminals. Consequently, the ramifications can be Leakage of data, Malware infection, Loss of consumer, fall of market share, failure to meet regulatory & clients' requirements etc. The truth is once affected, no company can afford to erase the black mark of a website attack overnight. SECUPENT provides many kinds of security solutions for Web and Network system. For example, our service encompasses Malware Analysis, Website Penetration test, Vulnerability Patching, Security Monitoring, Exploit development, software testing, CMS Penetration test, Cloud System Penetration test including SaaS, PaaS, IaaS platform, SAP Penetration test, Custom ERP Solution Penetration test, DDOS and DOS protection and many more. We provide our services on your demand. So, place your Order, sit back and relax because prevention does is better than cure!!!

Office:
House# 1066, Road# 7, Avenue# 7, Mirpur DOHS, Dhaka-1216
Mobile: +880-1681274842, Email: service@secupent.com

SECUPENT
Aim to Secure the modern internet