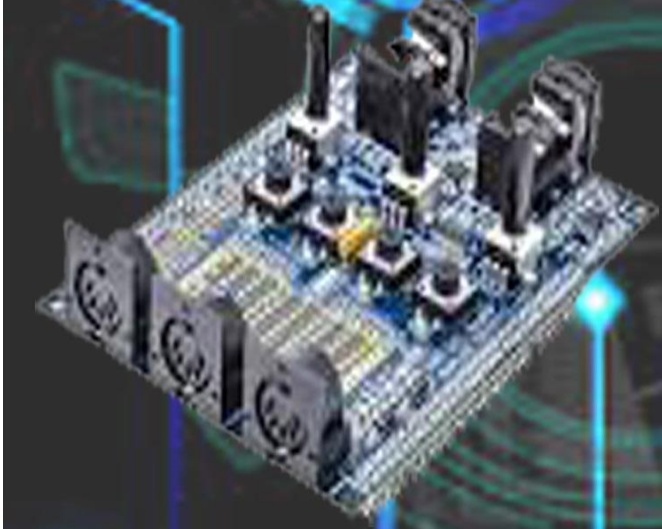
INFOLINE

VOLUME X ISSUE I JULY 2019



DEPARTMENT OF COMPUTER TECHNOLOGY AND INFORMATION TECHNOLOGY

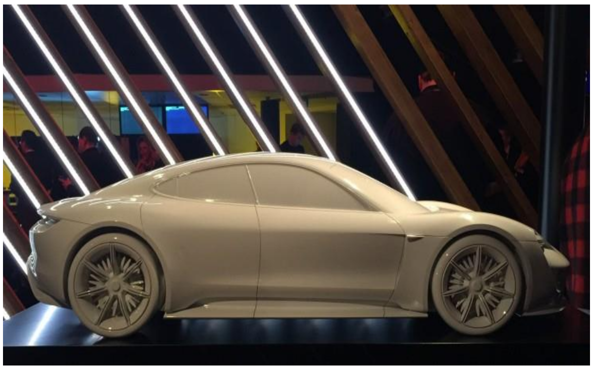
KONGU ARTS AND SCIENCE COLLEGE
(Autonomous)
Affliated to Bharathiar University,
Coimbatore
Approved by UGC and AICTE, New Delhi
Re-accredited by NAAC, DBT STAR College Scheme
An ISO 9001 : 2015 Certified Institution
Nanjanapuram, Erode - 638 107

INFOLINE

EDITORIAL BOARD

CONTENTS

MACHINE LEARNING WILL ADVANCE ARTIFICIAL INTELLIGENCE (AI)



Artificial Intelligence (AI) innovations will continue to bring scientific breakthroughs, in part, thanks to the vast amounts of data that new technologies have been collecting and is now available. In 2019, Machine Learning and Artificial Intelligence will be embedded in the business platform creating and enabling smart business operations.

In the Artificial Intelligence space, China is going to leave the U.S. emerging as a leader in AI developments and applications. Advances in Machine Learning technology and algorithm training will result in new and more advanced AI. Autonomous vehicles and robotics are the two industries that will see the most rapid developments during 2019.

In 2019, it is going to be a convergence of Artificial Intelligence, Machine Learning, and Deep Learning in business applications. As AI and learning technologies get to work together in order to reach better results AI will have greater accuracy at all levels. So far, humans have only developed Narrow Artificial Intelligence. A superior AI, though is in the future of mankind. How far should humans go with AI development is still a subject of controversy.

S.AISWARYA
III B.Sc. (Computer Technology)

SOCIAL MEDIA AND DIGITAL WELLBEING

The International Gaming Research Unit, at Nottingham Trent University has published a useful summary of research into the risks of excessive or problematic use of social media during adolescence. In a nutshell, anxiety, depression, stress, loneliness, hostility, distraction, procrastination, obesity, diabetes, sleep disorders and poor dietary habits have all been linked to excessive or problematic social media use.

The short report is balanced, leading with the insight that social media can also offer important psychological benefits such as facilitating emotional support, community building and self-expression. In addition, the report also points out that much of the research to date has been exploratory, small scale and only offers correlational evidence. So any conclusions from the research should be tentative.

Finally, report also makes the key point that much of this early research on social media and wellbeing has focused on overall time spent on social media, and that this may be unhelpful since the impact of social media may depend on particular social media activities (e.g. browsing vs posting) rather than overall time.

- Social media can contribute to increases in overall screen time which has been linked to serious physical conditions such as obesity and diabetes.
- Social media can contribute to increases in overall smartphone use which has been associated with negative outcomes, such as impaired social interactions, social isolation, as well as both somatic and mental health problems, including anxiety, depression and stress.
- It is linked to physical problems such as sleep deficit and poor dietary habits in some adolescents.
- It is linked to social problems such as such loneliness and hostility in some adolescents.
- It is linked to psychological problems such as anxiety and depression in some adolescents.
- It is linked to other psychological problems such as cognitive impairment, with symptoms of distraction, procrastination and attention deficit hyperactivity disorder (ADHD) in some adolescents.
- Social media use is linked to symptoms associated with substance-related addictions and behavioural addictions, such as gambling addiction among some adolescents.
- Young adolescents and those with a personality profile that includes elevated extraversion or neuroticism may be more at risk from addictive appeal of social media
- Social media use is linked to emotional states such as fear or missing out (FOMO) and separation anxiety with smartphones (nomophobia no mobile phone phobia).

A.TAMILHARIHARAN
III B.Sc. (Computer Technology)

CRYPTOJACKING

CryptoJacking is the top Cybersecurity threat for mining cryptocurrencies in 2018. According to McAfee report, it grows approximately 630 percent in the first quarter of 2018. The security researchers also found that, the fake Adobe Flash updates to push mining the cryptocurrencies through Malware.

As we all know Cryptocurrencies boom is on rise. In just few months, many cryptocurrencies have reached their all time high and given hefty returns to their investors. So some of the Hackers are now finding ways to capitalizing these crypto coins by stealing it from user's wallets. CryptoJacking is the process of using your computer silently to mine cryptocurrencies. It's quite similar to Ransomware. In Ransomware, your computer device infects through a file extension. But in Cryptojacking it infects your computer through a browser.

As we all know many Cryptocurrencies are Mineable. So Cybercriminals are using your computer to mine Cryptocurrency. Hackers are also trying to do some phishing via email by sending you a malicious link in the email that silently execute cryptomining code in your computer background. And by hijacking the website they could even insert malicious code in the victim's browser. CryptoJackers are now approaching Ad companies to insert malicious ad code to display it to a wide number of users.

CoinHive is the company which developed the script for Cryptojacking as a revenue alternative.

How does it Work?

- CryptoJackers are using JavaScript on a web-page to mine crypto coins.
- In browser mining, there is no need to install any software. They are just required to visit that particular website.
- There is no way to detect malicious link immediately, because it does not affect website performance.
- It runs silently.

CryptoJacking is on Rise

"Crypto mining is in its infancy. There is a lot of room for growth and evolution," says Marc Laliberte, threat analyst at network security solutions provider WatchGuard Technologies. He notes that Coinhive is easy to deploy and generated $300 thousand in its first month.

How to detect CryptoJacking?

There are some basic ways to detect cryptojacking in your Computer:

- If your computer is running very slow and giving poor performance.
- If CPU is heating excessively.
- We can also detect it via network monitoring tools.
- There are many artificial intelligence companies which analyzes network data to detect CryptoJacking.

According to report, CryptoJacking attacks in UK have surged by 1200 percent in just few months. Earlier in Feburary, Information Commissioner's office attacked by cybercriminals after insert a crypto mining scripts into a browser plugin. More than 1400 currencies have existence in the crypto market. Privacy focuses cryptocurrency called Monero is commonly mined by Cryptojackers. Recently Tesla was hacked for CryptoJacking, there are many open source plugins that allow without a password.

How can we Protect?

- Install Ad blocker and Cryptomining Protection Extensions in your Browser.
- In Chrome, there is a popular protection extension called No Coin to block Coinhive mining.
- Ad blocker plus has capability to detect cryptomining scripts.
- Always Keep your computer and browser updated.
- Use Anti-Ransomware protection tools along with your Antivirus.

P.VIJAYA SHREE
III B.Sc. (Information Technology)

AUGMENTED REALITY (AR) AND VIRTUAL REALITY (VR)

Advances in Augmented Reality (AR), Virtual Reality (VR), and Mixed Reality (MR), all of which can be summarized in R+, will continue to be at the forefront of attention during 2019 with some fascinating new practical applications for industries. R+, which once was only found in video gaming, has been quickly advancing to become a useful tool in industries such as engineering design, manufacturing, healthcare, space exploration, and many others.

In 2019, Virtual Reality is going to open up to innovative industrial applications that will change how people work and collaborate across geographies. Augmented Reality has been rising in the Virtual Reality's shadow for the past year. But in 2019, AR is set to grow exponentially.

S.PRAKASH
III B.Sc. (Information Technology)

INTELLIGENT APPS: THE NEXT GENERATION OF APPLICATIONS

The next generation of mobile applications will be the result of multiple worlds colliding: when application development meets artificial intelligence, the Internet of Things and big data analytics, intelligent apps are the outcome. Put simply, these are apps that continually learn from user interactions and other data sources to become even more relevant and useful.

Chatbots, virtual assistants and recommendation engines on e-commerce sites are just some examples of intelligent applications. While it’s difficult to formulate a catch-all definition of smart apps, they have a number of typical features:

Data-driven

Intelligent apps combine and process multiple data sources such as IoT sensors, beacons or user interactions and turn an enormous quantity of numbers into valuable insights.

Contextual and relevant:

Intelligent apps make much smarter use of a device’s features to proactively deliver highly relevant information and suggestions. Users will no longer have to go to their apps. Instead, the apps will come to them.

Continuously adapting

Thanks to machine learning, intelligent apps continuously adapt and improve their output.

Action-oriented

By anticipating user behaviours with predictive analytics, smart applications deliver personalized and actionable suggestions.

Omnichannel

Progressive web applications (PWAs) are increasingly blurring the lines between native apps and mobile web applications.

B. A. AKSHAYA SHREE
II B.Sc. (Computer Technology)

INTRUSION DETECTION SYSTEM

A system that tries to identify attempts to hack or break into a computer system or to misuse it. IDSs may monitor packets passing over the network, monitor system files, monitor log files, or set up deception systems that attempt to trap hackers. Computer systems have become more vulnerable to intrusions than ever. Intrusion Detection is a security technology that allows not only the detection of attacks, but also attempts to provide notification of new attacks unforeseen by other components. Intrusion detection is an important component of a security system, and it complements other security technologies.

How does an IDS work?

While there are several types of IDS's, the most common types work the same. They analyze network traffic and log files for certain patterns. What kind of patterns you may ask? While a firewall will continually block a hacker from connecting to a network, most firewalls never alert an administrator.

The administrator may notice if he/she checks the access log of the firewall, but that could be weeks or even months after the attack. This is where an IDS comes into play. The attempts to pass through the firewall are logged, and IDS will analyze its log. At some point in the log there will be a large number of request-reject entries. An IDS will flag the events and alert an administrator. The administrator can then see what is happening right after or even while the attacks are still taking place. This gives an administrator the advantage of being able to analyze the techniques being used, source of attacks, and methods used by the hacker.

Following are the types of intrusion detection systems:

1) **Host-Based Intrusion Detection System (HIDS)**: Host-based intrusion detection systems or HIDS are installed as agents on a host. These intrusion detection systems can look into system and application log files to detect any intruder activity.

2) **Network-Based Intrusion Detection System (NIDS)**: These IDSs detect attacks by capturing and analyzing network packets. Listening on a network segment or switch, one network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment, thereby protecting those hosts. Network-based IDSs often consist of a set of single-purpose sensors or hosts placed at various points in a network. These units monitor network traffic, performing local analysis of that traffic and reporting attacks to a central management console.

Some important topics comes under intrusion detection are as follows :

Signatures: Signature is the pattern that you look for inside a data packet. A signature is used to detect one or multiple types of attacks. For example, the presence of “scripts/iisadmin” in a packet going to your web server may indicate an intruder activity. Signatures may be present in different parts of a data packet depending upon the nature of the attack.

Alerts: Alerts are any sort of user notification of an intruder activity. When an IDS detects an intruder, it has to inform security administrator about this using alerts. Alerts may be in the form of pop-up windows, logging to a console, sending e-mail and so on. Alerts are also stored in log files or databases where they can be viewed later on by security experts.

Logs: The log messages are usually saved in file.Log messages can be saved either in text or binary format.

False Alarms: False alarms are alerts generated due to an indication that is not an intruder activity. For example, misconfigured internal hosts may sometimes broadcast messages that trigger a rule resulting in generation of a false alert. Some routers, like Linksys home routers, generate lots of UPnP related alerts. To avoid false alarms, you have to modify and tune different default rules. In some cases you may need to disable some of the rules to avoid false alarms.

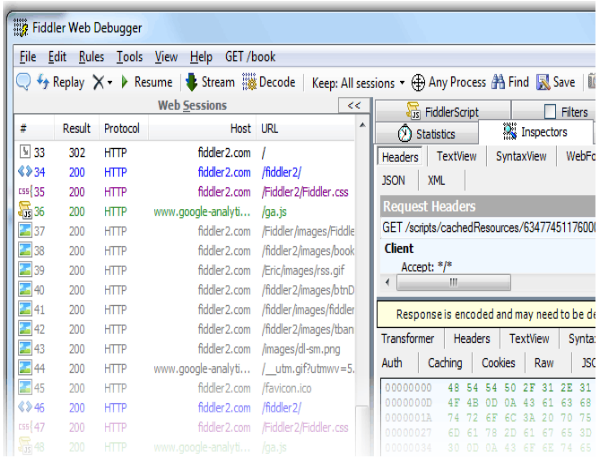
Sensor: The machine on which an intrusion detection system is running is also called the sensor in the literature because it is used to "sense" the network.

Snort

Snort is a very flexible network intrusion detection system that has a large set of pre-configured rules. Snort also allows you to write your own rule set. There are several mailing lists on the internet where people share new snort rules that can counter the latest attacks.

K.SURESHKUMAR
II B.Sc. (Computer Technology)

WEBSITE SECURITY TOOLS



#	Result	Protocol	Host	URL
33	302	HTTP	fiddler2.com	/
34	200	HTTP	fiddler2.com	/fiddler2/
35	200	HTTP	fiddler2.com	/Fiddler2/Fiddler.css
36	200	HTTP	www.google-analyti...	/ga.js
37	200	HTTP	fiddler2.com	/Fiddler/images/Fiddle
38	200	HTTP	fiddler2.com	/fiddler2/images/book
39	200	HTTP	fiddler2.com	/Eric/images/rss.gif
40	200	HTTP	fiddler2.com	/fiddler2/images/btnD
41	200	HTTP	fiddler2.com	/fiddler/images/fiddler
42	200	HTTP	fiddler2.com	/fiddler2/images/tban
43	200	HTTP	fiddler2.com	/images/dl-sm.png
44	200	HTTP	www.google-analyti...	/__utm.gif?utmwv=5.
45	200	HTTP	fiddler2.com	/favicon.ico
46	200	HTTP	fiddler2.com	/fiddler2/
47	200	HTTP	fiddler2.com	/Fiddler2/Fiddler.css
48	200	HTTP	www.google-analyti...	/ga.js

Request Headers

GET /scripts/cachedResources/63477451176000

Client

Accept: */*

Response is encoded and may need to be de

```
00000000  48 54 54 50 2F 31 2E 31
0000000D  4F 4B 0D 0A 43 61 63 68
0000001A  74 72 6F 6C 3A 20 70 75
00000027  6D 61 78 2D 61 67 65 3D
00000034  30 0D 0A 43 6F 6E 74 65
```

Fiddler

Fiddler is a free web debugging proxy which logs all HTTP(s) traffic between your computer and the Internet. Use it to debug traffic from any application that supports a proxy like IE, Chrome, Safari, Firefox, Opera, and more. Fiddler steps in to help you record all the HTTP and HTTPS traffic that passes between your computer and the Internet. Fiddler supports a wide range of filters such as "hide a session", "highlight interesting traffic", "breakpoint for manipulation on a session", "block traffic from sending" and more that can save you loads of time and efforts.

You can store the HTTP(s) traffic you captured though Fiddler to an archive (SAZ file) and reload it later, even from a different computer.

GoLismero

It is an Open Source security tools that can run their own security tests and manage a lot of well known security tools (OpenVas, Wfuzz, SQLMap, DNS recon, robot analyzer…) take their results. The framework also collects and unifies the results of well known tools: sqlmap, xsser, openvas, dnsrecon, theharvester

WebScarab

It is a framework for analysing applications that communicate using the HTTP and HTTPS protocols. It is written in Java, and is thus portable to many platforms. WebScarab has several modes of operation, implemented by a number of plugins. In its most common usage, WebScarab operates as an intercepting proxy, allowing the operator to review and modify requests created by the browser before they are sent to the server, and to review and modify responses returned from the server before they are received by the browser. WebScarab is able to intercept both HTTP and HTTPS communication. The operator can also review the conversations (requests and responses) that have passed through WebScarab.

Bricks

It's a web application security learning platform built on PHP and MySQL. The project focuses on variations of commonly seen application security issues. Each 'Brick' has some sort of security issue which can be leveraged manually or using automated software tools. The mission is to 'Break the Bricks' and thus learn the various aspects of web application security.Bricks is a completely free and open source project brought to you by OWASP.

Panoptic

It is a tool that searches for commonly known files through LFI vulnerabilities. Local file inclusion is a vulnerability that allows the attacker to read files that are stored locally through the web application. To get started, you will need Python 2.6+. Panoptic display the found file paths and it can save the actual files as well.

ModSecurity

It is a web application firewall that can work either embedded or as a reverse proxy. It provides protection from a range of attacks against web applications and allows for HTTP traffic monitoring, logging and real-time analysis.

K.SURESHKUMAR
II B.Sc. (Computer Technology)

KEYLOGGER

Keylogger is a software program or hardware device that is used to monitor and log each of the keys a user types into a computer keyboard. The user who installed the program or hardware device can then view all keys typed in by that user. Because these programs and hardware devices monitor the keys typed in a user can easily find user passwords and other information a user may not wish others to know about.

Keyloggers, as a surveillance tool, are often used by employers to ensure employees use work computers for business purposes only. Unfortunately, keyloggers can also be embedded in spyware allowing your information to be transmitted to an unknown third party.

About keyloggers

A keylogger is a program that runs in the background, recording all the keystrokes. Once keystrokes are logged, they are hidden in the machine for later retrieval, or shipped raw to the attacker. The attacker then peruses them carefully in the hopes of either finding passwords, or possibly other useful information that could be used to compromise the system or be used in a social engineering attack. For example, a keylogger will reveal the contents of all e-mail composed by the user. Keylogger is commonly included in rootkits.

A keylogger normally consists of two files: a DLL which does all the work and an EXE which loads the DLL and sets the hook. Therefore when you deploy the hooker on a system, two such files must be present in the same directory.

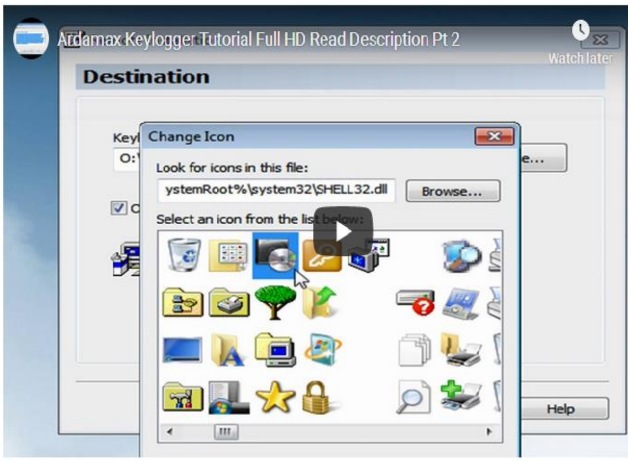
- There are other approaches to capturing info about what you are doing.
- Some keyloggers capture screens, rather than keystrokes. Other keyloggers will secretly turn on video or audio recorders, and transmit what they capture over your internet connection.

A keyloggers might be as simple as an exe and a DLL that are placed on a machine and invoked at boot via an entry in the registry. Or a keyloggers could be which boasts these features:

- Stealth: invisible in process list Includes kernel keylogger driver that captures keystrokes even when user is logged off (Windows 2000 / XP) ProBot program files and registry

Tools

Ardamax Keylogger is a keystroke recorder that captures user’s activity and saves it to an encrypted log file. The log file can be viewed with the powerful Log Viewer. Use this tool to find out what is happening on your computer while you are away, maintain a backup of your typed data automatically or use it to monitor your kids. Also you can use it as a monitoring device for detecting unauthorised access. Logs can be automatically sent to your e-mail address, access to the keylogger is password protected. Besides, Ardamax Keylogger logs information about the Internet addresses the user has visited.


Ardamax Keylogger Tutorial Full HD Read Description Pt 2
Watch later
Destination
Change Icon
Look for icons in this file:
ystemRoot%\system32\SHELL32.dll
Browse...
Select an icon from the list below:
Help

This invisible spy application is designed for 2000, XP, 2003, Vista and Windows 7.

- Security allows you to protect program settings, Hidden Mode and Log file.
- Application monitoring keylogger will record the application that was in use that received the keystroke.
- Time/Date tracking , it allows you to pinpoint the exact time a window received a keystroke.
- Powerful Log Viewer you can view and save the log as a HTML page or plain text with keylogger Log Viewer.
- Small size Ardamax Keylogger is several times smaller than other programs with the same features. It has no additional modules and libraries, so its size is smaller and the performance is higher.
- Ardamax Keylogger fully supports Unicode characters which makes it possible to record keystrokes that include characters from Japanese, Chinese, Arabic and many other character sets.
- It records every keystroke. Captures passwords and all other invisible text.

Other Features

- Windows 2000/2003/XP/Vista/Windows 7 support
- Monitors multi-user machines
- Automatic startup
- Friendly interface
- Easy to install

Perfect Keylogger for Windows 98/2000/XP/Vista and Windows 7

- The latest, improved and most stealth version of Perfect Keylogger is now available only after purchase. To protect the product from abuse and improve its quality for the registered users, we no longer offer the trial version of the latest builds. The localized versions of Perfect Keyloger and 64-bit version are also available after purchase. The last public version is still available, but keep in mind that it’s not the latest and may be flagged by security software.

S.HARITHA
II B.Sc. (Information Technology)

CROSS SITE SCRIPTING (XSS)

It is a very common vulnerability found in Web Applications, Cross Site Scripting (XSS) allows the attacker to INSERT malicious code, There are many types of XSS attacks, I will mention 3 of the most used. This kind of vulnerability allows an “attacker” to inject some code into the applications affected in order to bypass access to the website or to apply “phishing” on falls users.

This technique is also used for website Hacking.

Types of XSS:

There are actually three types of Cross-Site Scripting, commonly named as:

- DOM-Based XSS
- Non-persistent XSS
- Persistent XSS

DOM-Based XSS

The DOM-Based Cross-Site Scripting allow to an attacker to work not on a victim website but on a victim local machine: the various operative system usually includes “since born” some HTML pages created for differents aims, but as long as the humans do mistakes this HTML pages often can be exploited due to code vulnerabilities.

The DOM-Based XSS exploits these problems on users local machines in this way:

- The attacker creates a well built malicious website.
- The ingenious user opens that site. The user has a vulnerable page on his machine.
- The attacker’s website sends commands to the vulnerable HTML page.
- The vulnerable local page executes that commands with the user’s privileges on that machine.
- The attacker easily gain control on the victim computer.

Non-Persistent: The non-persistent XSS are actually the most common vulnerabilities that can be found on the Net. It’s commonly named as “non-persistent” because it works on an immediate HTTP response from the victim website: it shows up when the web page get the data provided by the attacker’s client to automatically generate a result page for the attackers himself. Standing on this the attacker could provide some malicious code and try to make the server execute it in order to obtain some result.

The most common applying of this kind of vulnerability is in Search engines in website: the attacker writes some arbitrary HTML code in the search textbox and, if the website is vulnerable, the result page will return the result of these HTML entities.

Persistent: The persistent XSS vulnerabilities are similar to the second type (Non-persistent XSS), because both works on a victim site and tries to hack users information and the difference is that in websites vulnerable to Persistent XSS the attacker doesn't need to provide the crafted url to the users, because the website itself permits to users to insert fixed data into the system: this is the case for example of "guestbooks".

Usually the users use that kind of tool to leave messages to the owner of the website and at a first look it doesn't seem something dangerous, but if an attacker discover that the system is vulnerable can insert some malicious code in his message and let ALL visitors to be victims of that.

This works when the tool provided (the guestbook in the example) doesn't do any check on the content of the inserted message: it just inserts the data provided from the user into the result page.

How to Find Cross Site Scripting (XSS) Vulnerabilities

To start finding these Vulnerabilities you can start checking out Blogs, Forums, Shoutboxes, Comment Boxes, Search Box's, there are too many to mention.

Using 'Google Dorks' to make the finding easier, Ok if you wanna get cracking, go to google.com and type `inurl:"search.php?q="` now that is a common page and has a lot of results. Also note that most sites have XSS Vulnerabilities, it's just having a good eye, and some good knowledge on how to bypass their filtration.

Basics of XSS

The methods that commonly used in XSS is :

```
<script>alert("Priyanshu")</script>
```

now this will alert a popup message, saying "Priyanshu" without quotes.

So, use `"search.php?q="` and you can simply try the following on a website with the same thing,

```
http://website.com/search.php?q=<script>alert("Priyanshu")</script>
```

There are good chances of it working, but don't be worried if it don't, just try different sites. You can insert HTML not just javascript.

```
http://website.com/search.php?q=<br><b
r><b><u>Priyanshu</u></b>
```

If you see the bold text on the page and newlines then you knows it’s vulnerable.

How to Deface a Website using XSS ?

The first one being IMG SCR, now for those of you who don’t know HTML, IMG SCR is a tag, that displays the IMAGE linked to it on the web page.

```
<html><body><IMG
SRC="http://website.com/yourDefaceIMAG
E.png"></body></html>
```

insert the following code to make the picture display on the page.

```
<IMG
SRC="http://site.com/yourDefaceIMAGE.p
ng">
```

The other tags are not needed has the page will already have them. It helps to make your picture big so it stands out and it is clear that the site got hacked. Another method is using FLASH videos, its the same has the method below but a more stylish deface.

```
<EMBED SRC="http://site.com/xss.swf"
```

That will execute the flash video linked to it. Or maybe using a pop or redirection as :

```
<script>window.open("https://hackerson
lineclub.com/")</script>
```

There are many others ways that you can found using Google or other website. My purpose is to make you understand the concept.

D.KRISHNAKUMAR
II B.Sc. (Information Technology)

SOUNDWAVE TECHNOLOGY: THE NEW FRONTIER IN DIGITAL PAYMENT SPACE

On November 8, 2016, Prime Minister Narendra Modi announced the scrapping of Rs 500 and Rs 1,000 currency notes in a revolutionary attempt to combat the issues of black money, corruption, and the outflow of money funding illegal activities and terrorism. Following the demonetisation drive, the Indian government has been working relentlessly to promote the usage of digital payment solutions.

With a phenomenal rise in the ownership of smartphones and introduction of easy-to-use payment methods like BHIM UPI and Aadhaar-linked payments, India has already ventured into its journey towards becoming a cashless economy. According to the statistics provided by the Reserve Bank of

India (RBI), as many as 523.23 million cashless transactions worth Rs 93.63 lakh took place in November 2016 itself. Furthermore, the country has witnessed a robust rise in the number of debit and credit card hold .

To begin with, digital payment solutions are largely designed for smartphones, and the smartphone penetration in India is just 24%, according to a global survey conducted by The Pew Research Center. Moreover, only a fraction of smartphone holders in the country are well-acquainted with technologies such as RFID, Infrared, Bluetooth and NFC. Moreover, upon taking into consideration factors like poor network coverage, low disposable income, and lack of cognisance, a smartphone's usage often gets l .

Soundwave technology

The force to reckon with in the digital payment ecosystem Prior to the implementation of demonetisation, cash was the most widely used payment method in India. The reason for cash being the king for Indian consumers is simple; ease of availability and simplicity of usage. Universally accessible, there is no requirement for a ground-level infrastructure to use cash. On the other hand, mobile and online payments typically require a digital device enabled.

However, with the 4th Industrial Revolution dawning upon us, where modern technologies are blurring the lines between the physical, digital and biological spheres, things are looking up for companies in the digital payments sector as well. Soundwave technology, for example, is one such development that is addressing these challenges head-on. This technology facilitates a universally scalable and cost-effective means of payment by leveraging the benefits of cash-based and digital payment methods.

It enables transactions on smart as well as feature phone. Makes the transaction faster, seamless in smart phone and also enable feature phone users to do transaction without internet dependency. In addition to all of this, soundwave-based payments are entirely secure, which can be a relief amidst the rising incidents of cyber frauds and security. Relatively inexpensive to deploy, soundwave technology holds the potential to create major transformational disruptions in the digital payment space. As more and more people turn to mobile wallets and UPI-based payment apps, the government's dream of making India a major cashless economy may soon turn into a reality. And, with 668.3 million users projected to rely on Soundwave technology by 2021, usage of cash as a mode of payment could possibly become rare in near future, if not obsolete.

M.BHAVAN
I B.Sc. (ComputerTechnology)

AMAZON CLOUDFRONT

Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment. CloudFront is integrated with AWS both physical locations that are directly connected to the AWS global infrastructure, as well as other AWS services. CloudFront works seamlessly with services including AWS Shield for DDoS mitigation, Amazon S3, Elastic Load Balancing or Amazon EC2 as origins for your applications, and Lambda@Edge to run custom code closer to customers' users and to customize the user experience. Lastly, if you use AWS origins such as Amazon S3, Amazon EC2 or Elastic Load Balancing, you don't pay for any data transferred between these services and CloudFront.

You can get started with the Content Delivery Network in minutes, using the same AWS tools that you're already familiar with: APIs, AWS Management Console, AWS CloudFormation, CLIs, and SDKs. Amazon's CDN offers a simple, pay-as-you-go pricing model with no upfront fees or required long-term contracts, and support for the CDN is included in your existing AWS Support subscription.

Benefits

Fast and global

The Amazon CloudFront content delivery network (CDN) is massively scaled and globally distributed. The CloudFront network has 188 points of presence (PoPs), and leverages the highly-resilient Amazon backbone network for superior performance and availability for your end users.

Security at the Edge

The Amazon CloudFront content delivery network (CDN) is massively scaled and globally distributed. The CloudFront network has 188 points of presence (PoPs), and leverages the highly-resilient Amazon backbone network for superior performance and availability for your end users.

Amazon CloudFront is a highly-secure CDN that provides both network and application level protection. Your traffic and applications benefit through a variety of built-in protections such as AWS Shield Standard, at no additional cost. You can also use configurable features such as AWS Certificate Manager (ACM) to create and manage custom SSL certificates at no extra cost.

Highly Programmable

Amazon CloudFront features can be customized for your specific application requirements. Lambda@Edge functions, triggered by CloudFront events, extend your custom code across AWS locations worldwide, allowing you to move even complex application logic closer to your end users to improve responsiveness. The CDN also supports integrations with other tools and automation interfaces for today's DevOps and CI/CD environments by using native APIs or AWS tools.

Deep Integration with AWS

Amazon CloudFront features can be customized for your specific application requirements. Lambda@Edge functions, triggered by CloudFront events, extend your custom code across AWS locations worldwide, allowing you to move even complex application logic closer to your end users to improve responsiveness. The CDN also supports integrations with other tools and automation interfaces for today's DevOps and CI/CD environments by using native APIs or AWS tools.

Amazon CloudFront is integrated with AWS services such as Amazon S3, Amazon EC2, Elastic Load Balancing, Amazon Route 53, and AWS Elemental Media Services . They are all accessible via the same console and all features in the CDN can be programmatically configured by using APIs or the AWS Management Console.

R.SHOBIKA
I B.Sc. (ComputerTechnology)

COMPUTER-AIDED KNITTING

New research from the Computer Science and Artificial Intelligence Laboratory uses machine learning to customize clothing designs. The oldest known knitting item dates back to Egypt in the Middle Ages, by way of a pair of carefully handcrafted socks. Although handmade clothes have occupied our closets for centuries, a recent influx of high-tech knitting machines have changed how we now create our favorite pieces.

These systems, which have made anything from Prada sweaters to Nike shirts, are still far from seamless. Programming machines for designs can be a tedious and complicated ordeal: When you have to specify every single stitch, one mistake can throw off the entire garment. In a new pair of papers, researchers from MIT’s Computer Science and Artificial Intelligence Laboratory (CSAIL) have come up with a new approach to streamline the process: a new system and design tool for automating knitted garments.

In one paper, a team created a system called “InverseKnit”, that translates photos of knitted patterns into instructions that are then used with machines to make clothing. An approach like this could let casual users create designs without a memory bank of coding knowledge, and even reconcile issues of efficiency and waste in manufacturing.

“As far as machines and knitting go, this type of system could change accessibility for people looking to be the designers of their own items," says Alexandre Kaspar, CSAIL PhD student and lead author on a new paper about the system. “We want to let casual users get access to machines without needed programming expertise, so they can reap the benefits of customization by making use of machine learning for design and manufacturing.”

In another paper, researchers came up with a computer-aided design tool for customizing knitted items. The tool lets non-experts use templates for adjusting patterns and shapes, like adding a triangular pattern to a beanie, or vertical stripes to a sock.

InverseKnit

Automation has already reshaped the fashion industry as we know it, with potential positive residuals of changing our manufacturing footprint as well. To get InverseKnit up and running, the team first created a dataset of knitting instructions, and the matching images of those patterns. They then trained their deep neural network on that data to interpret the 2-D knitting instructions from images.

This might look something like giving the system a photo of a glove, and then letting the model produce a set of instructions, where the machine then follows those commands to output the design. When testing InverseKnit, the team found that it produced accurate instructions 94% of the time.

“Current state-of-the-art computer vision techniques are data-hungry, and they need many examples to model the world effectively,” says Jim McCann, Assistant Professor in the Carnegie Mellon Robotics Institute. “With InverseKnit, the team collected an immense dataset of knit samples that, for the first time, enables modern computer vision techniques to be used to recognize and parse knitting patterns.”

While the system currently works with a small sample size, the team hopes to expand the sample pool to employ InverseKnit on a larger scale. Currently, the team only used a specific type of acrylic yarn, but they hope to test different materials to make the system more flexible.

A tool for knitting

While there’s been plenty of developments in the field such as Carnegie

Mellon's automated knitting processes for 3-D meshes these methods can often be complex and ambiguous. The distortions inherent in 3-D shapes hamper how we understand the positions of the items, and this can be a burden on the designers.

To address this design issue, Kaspar and his colleagues developed a tool called "CADKnit", which uses 2-D images, CAD software, and photo editing techniques to let casual users customize templates for knitted designs. The tool lets users design both patterns and shapes in the same interface. With other software systems, you'd likely lose some work on either end when customizing both.

The team tested the usability of CADKnit by having non-expert users create patterns for their garments and adjust the size and shape. In post-test surveys, the users said they found it easy to manipulate and customize their socks or beanies, successfully fabricating multiple knitted samples. They noted that lace patterns were tricky to design correctly and would benefit from fast realistic simulation.

However the system is only a first step towards full garment customization. The authors found that garments with complicated interfaces between different parts such as sweaters didn't work well with the design tool. The trunk of sweaters and sleeves can be connected in various ways, and the software didn't yet have a way of describing the whole design space for that.

Furthermore, the current system can only use one yarn for a shape, but the team hopes to improve this by introducing a stack of yarn at each stitch. To enable work with more complex patterns and larger shapes, the researchers plan to use hierarchical data structures that do not incorporate all stitches, just the necessary ones.

N.R SHARMILA
I B.Sc. (Computer Technology)

STREAMING MEDIA

Streaming media is multimedia that is constantly received by and presented to an end-user while being delivered by a provider. The verb "to stream" refers to the process of delivering or obtaining media in this manner the term refers to the delivery method of the medium, rather than the medium itself, and is an alternative to file downloading, a process in which the end-user obtains the entire file for the content before watching or listening to it.

A client end-user can use their media player to start playing digital video or digital audio content before the entire file has been transmitted. Distinguishing delivery method from the media distributed applies specifically to telecommunications networks, as most of the delivery systems are either inherently streaming (e.g. radio, television, streaming apps) or inherently non-streaming (e.g. books, video cassettes, audio CDs). For example, in the 1930s, elevator music was among the earliest popular music available as streaming media; nowadays Internet television is a common form of streamed media. The term "streaming media" can apply to media other than video and audio, such as live closed captioning, ticker tape, and real-time text, which are all considered "streaming text".

Live streaming is the delivery of Internet content in real-time much as live television broadcasts content over the airwaves via a television signal. Live internet streaming requires a form of source media (e.g. a video camera, an audio interface, screen capture software), an encoder to digitize the content, a media publisher, and a content delivery network to distribute and deliver the content. Live streaming does not need to be recorded at the origination point although it frequently is.

There are challenges with streaming content on the Internet. If the user does not have enough bandwidth in their Internet connection, they may experience stops, lags, or slow buffering of the content. Some users may not be able to stream certain content due to not having compatible computer or software systems. Some popular streaming services include the video sharing website YouTube, Netflix, Amazon Video and Vudu which stream films and television shows Spotify and Apple Music which stream music; and the video game live streaming sites Twitch and mixer.

VARSHA R
III B.Sc. (Information Technology)

TECHNOLOGIES FOR THE SIXTH GENERATION CELLULAR NETWORK

Future wireless data networks will have to reach higher transmission rates and shorter delays, while supplying an increasing number of end devices. For this purpose, network structures consisting of many small radio cells will be required. To connect these cells, high-performance transmission lines at high frequencies up to the terahertz range will be needed. Moreover, seamless connection to glass fiber networks must be ensured, if possible. Researchers of Karlsruhe Institute of Technology (KIT) use ultra-rapid electro-optical modulators to convert terahertz data signals into optical signals. This is reported in Nature Photonics.

While the new 5G cellular network technology is still tested, researchers are already working on technologies for the next generation of wireless data transmission. "6G" is to reach far higher transmission rates, shorter delays, and an increased device density, with artificial intelligence being integrated. On the way towards the sixth generation cellular network, many challenges have to be mastered regarding both individual components and their interaction. Future wireless networks will consist of a number of small radio cells to quickly and efficiently transmit large data volumes. These cells will be connected by transmission lines, which can handle tens or even hundreds of gigabits per second per link. The necessary frequencies are in the terahertz range, i.e. between microwaves and infrared radiation in the electromagnetic spectrum. In addition, wireless transmission paths have to be seamlessly connected to glass fiber networks. In this way, the advantages of both technologies, i.e. high capacity and reliability as well as mobility and flexibility, will be combined.

Scientists of the KIT Institutes of Photonics and Quantum Electronics (IPQ), Microstructure Technology (IMT), and Radio Frequency Engineering and Electronics (IHE) and the Fraunhofer Institute for Applied Solid State Physics IAF, Freiburg, have now developed a promising approach to converting data streams between the terahertz and optical domains. As reported in nature photonics, they use ultra-rapid electro-optical modulators to directly convert a terahertz data signal into an optical signal and to directly couple the receiver antenna to a glass fiber. In their experiment, the scientists selected a carrier frequency of about 0.29 THz and reached a transmission rate of 50 Gbit/s.

"The modulator is based on a plasmonic nanostructure and has a bandwidth of more than 0.36 THz," says Professor Christian Koos, Head of IPQ and Member of the Board of Directors of IMT. "Our results reveal the great potential of nanophotonic components for ultra-rapid signal processing." The concept demonstrated by the researchers will considerably reduce technical complexity of future radio base stations and enable terahertz connections with very high data rates several hundred gigabits per second are feasible.

With a quantum coprocessor in the cloud, physicists from Innsbruck, Austria, open the door to the simulation of previously unsolvable problems in chemistry, materials research or high-energy physics. The research groups led by Rainer Blatt and Peter Zoller report in the journal *Nature* how they simulated particle physics phenomena on 20 quantum bits and how the quantum simulator self-verified the result for the first time.

Many scientists are currently working on investigating how quantum advantage can be exploited on hardware already available today. Three years ago, physicists first simulated the spontaneous formation of a pair of elementary particles with a digital quantum computer at the University of Innsbruck. Due to the error rate, however, more complex simulations would require a large number of quantum bits that are not yet available in today's quantum computers. The analog simulation of quantum systems in a quantum computer also has narrow limits. Using a new method, researchers around Christian Kokail, Christine Maier und Rick van Bijnen at the Institute of Quantum Optics and Quantum Information (IQOQI) of the Austrian Academy of Sciences have now surpassed these limits. They use a programmable ion trap quantum computer with 20 quantum bits as a quantum coprocessor, in which quantum mechanical calculations that reach the limits of classical computers are outsourced. "We use the best features of both technologies," explains experimental physicist Christine Maier. "The quantum simulator takes over the computationally complex quantum problems and the classical computer solves the remaining tasks."

Toolbox for Quantum Modelers

The scientists use the variational method known from theoretical physics, but apply it on their quantum experiment. "The advantage of this method lies in the fact that we can use the quantum simulator as a quantum resource that is independent of the problem under investigation," explains Rick van Bijnen. "In this way we can simulate much more complex problems." A simple comparison shows the difference: an analog quantum simulator is like a doll's house, it represents reality. The programmable variational quantum simulator, on the other hand, offers individual building blocks with which many different houses can be built. In quantum simulators, these building blocks are entanglement gates and single spin rotations. With a classical computer, this set of knobs is tuned until the intended quantum state is reached. For this the physicists have developed a sophisticated optimization algorithm that in about 100,000 requests of the quantum coprocessor by the classical computer leads to the result. Coupled with extremely fast measurement cycles of the quantum experiment, the simulator at IQOQI Innsbruck becomes enormously powerful. For the first time, the physicists have simulated the spontaneous creation and destruction of pairs of elementary particles in a vacuum on 20 quantum bits. Since the new method is very efficient, it can also be used on even larger quantum simulators. The Innsbruck researchers plan to build a quantum simulator with up to 50 ions in the near future. This opens up interesting perspectives for further investigations of solid-state models and high-energy physics problems.

Built-in Self-Check

A previously unsolved problem in complex quantum simulations is the verification of the simulation results. "Such calculations can hardly or not at all be checked using classical computers. So how do we check whether the quantum system delivers the right result," asks the theoretical physicist Christian Kokail. "We have solved this question for the first time by making additional measurements in the quantum system. Based on the results, the quantum machine assesses the quality of the simulation," explains Kokail. Such a verification mechanism is the prerequisite for even more complex quantum simulations, because the necessary number of quantum bits increases sharply. "We can still test the simulation on 20 quantum bits on a classical computer, but with more complex simulations this is simply no longer possible," says Rick van Bijnen. "In our study, the quantum experiment was even faster than the control simulation on the PC. At the end, we had to take it out of the race in order not to slow down the experiment," says the physicist.

Innsbruck Quantum Cloud

This research achievement is based on the unique collaboration between experiment and theory at the Innsbruck Quantum Research Center. The expertise from years of experimental quantum research meets innovative theoretical ideas in Tyrol, Austria. Together, this leads to results that are recognized worldwide and establishes an internationally leading position of Innsbruck's quantum research. "15 years of very hard work have gone into this experiment," emphasizes experimental physicist Rainer Blatt. "It is very nice to see that this is now bearing such beautiful fruit." The theoretical physicist Peter Zoller adds: "We in Innsbruck are not only leaders in the number of available quantum bits, but have now also advanced into the field of programmable quantum simulation and were able to demonstrate for the first time the self-verification of a quantum processor. With this new approach, we are bringing the simulation of everyday quantum problems within reach."

SELVA BHARATHI A
III B.Sc. (Computer Technology)

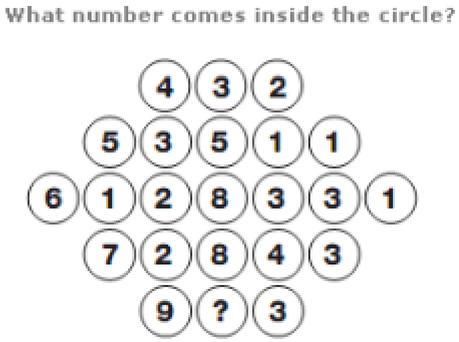
MATH PUZZLES

1. How to get a number 100 using four sevens(7's) and a one(1) ???

Answer 1:177-77=100

Answer 2: (7+7)*(7+ (1/7)) =100

2. By using your numerical and logical reasoning skills please try to figure out which number is missing in the questions below. The numbers around will give you the clues you need to solve the puzzle.

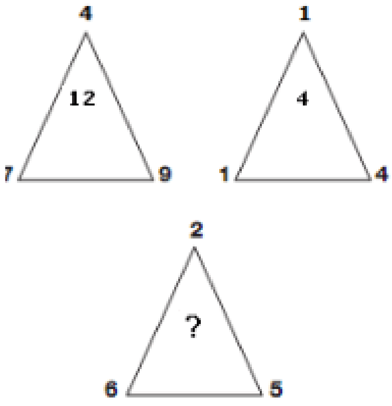

What number comes inside the circle?

Answer : 6

Explanation :

Looking at the diagram in rows, the central circle equals half the sum of the numbers in the other circles to the left and right of the centre.

3. Which number replaces the question mark?



Answer : 9

Explanation :

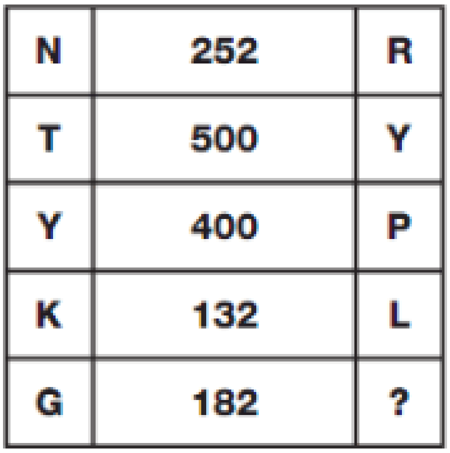
The number at the centre of each triangle equals the sum of the lower two numbers minus the top number.

4. The day before yesterday I was 25. The next year I will be 28. this is true only ine day in a year. What day is my birthday?

Answer:

My birthday is on December 31.
I am telling this on January 1.
Day before yesterday (dec 30):I am 25
Present day (January 1) :I am 26
This year december 31 :I will be 27.
Next year december 31 : I will be 28.

5. Which letter replaces the question mark?



N	252	R
T	500	Y
Y	400	P
K	132	L
G	182	?

Answer : Z

Explanation :

In each row, multiply the numerical values of the left and right hand letters, putting the result in the centre.

SINDUJA T

III B.Sc. (Computer Technology)

EVERYONE SHOULD HAVE THE OPPORTUNITY TO LEARN COMPUTER SCIENCE AT SCHOOL AND BEYOND

- SUNDAR PICHAI