Sri Lanka Institute of Information Technology

ASSIGNMENT 01

IT3070 - Information Assurance & Security - 2019

Submitted by:

1. IT17102810 – D.D.H Kulathunga.
2. IT17090636 – W.W.S.R.M.U.Pasan.

01.Distributed denial of service attack.

Allegro - Worksheet 10		Information Asset Risk Worksheet			
Information Asset Risk	Threat	Information Asset	Company's web hosting servers.		
		Area of Concern	DDos Attacks.		
		(1) Actor *Who would exploit the area of concern or threat?*	Intruder.		
		(2) Means *How would the actor do it? What would they do?*	DDoS is an acronym for distributed denial of service. A DDoS attack is a malicious attempt to make a server or a network resource unavailable to users. It is achieved by saturating a service, which results in its temporary suspension or interruption. A DDoS attack, uses multiple connected devices often executed by botnets or, on occasion, by individuals who have coordinated their activity.		
		(3) Motive *What is the actor's reason for doing it?*	Intentional (ideology, business feuds, boredom, extortion, cyber warfare).		
		(4) Outcome *What would be the resulting effect on the information asset?*	☐ **Disclosure** ❑ **Destruction** ❑ **Modification** ☐ **Interruption**		
		(5) Security Requirements *How would the information asset's security requirements be breached?*	Servers will be inaccessible causing total system failure.		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	☐ **High** **75%**	❑ **Medium** **50%**	❑ **Low** **25%**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value (0-10)**	**Score**
So if there's a DDos attack, Servers going to shut down. So at that time,websites hosted by company's servers will	Reputation & Customer Confidence	8	6.0

	be down. Customers lose trust in the company, because of this failure, clients might leave this company.	Financial	5	3.75
	Customers will be disappointed about the loss of service, if clients get legal action against the company, the company might have to pay a fine.	Productivity	3	2.25
		Safety & Health	0	0.0
	Because of the shutdown servers and also downed websites there is going to be loss of productivity. And the company will lose its reputation.	Fines & Legal Penalties	3	2.25
		User Defined Impact Area	0	0.0
			Relative Risk Score	**14.25**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

❑ **Accept**	❑ **Defer**	☑ **Mitigate**	❑ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Identify the DDoS attack early.	Then you run your own servers, then you need to be able to identify when you are under attack. That's because the sooner you can establish that problems with your website are due to a DDoS attack, the sooner you can stop the DDoS attack. To be in a position to do this, it's a good idea to familiarize yourself with your typical inbound traffic profile, the more you know about what your normal traffic looks like, the easier it is to spot when its profile changes. Most DDoS attacks start as sharp spikes in traffic, and it's helpful to be able to tell the difference between a sudden surge of legitimate visitors and the start of a DDoS attack.
Overprovision bandwidth.	It generally makes sense to have more bandwidth available to your Web server than you ever think you are likely to need. That way, you can accommodate sudden and unexpected surges in traffic that could be a result of an advertising campaign, a special offer or even a mention of your company in the media. Even if you overprovision by 100 percent -- or 500 percent -- that likely won't stop a DDoS attack. But it may give you a few extra minutes to act before your resources are overwhelmed completely.
Defend at the network perimeter.	There are a few technical measures that can be taken to partially mitigate the effect of an attack, especially in the first minutes and some of these are quite simple. For example, the company can, ● rate limit your router to prevent your Web server from being overwhelmed, ● add filters to tell your router to drop packets from obvious sources of attack, ● timeout half-open connections more aggressively,

	• drop spoofed or malformed packages, • set lower SYN, ICMP, and UDP flood drop thresholds.
Getting help from a DDoS mitigation specialist.	For very large attacks, it's likely that your best chance of staying online is to use a specialist DDoS mitigation company. These organizations have large-scale infrastructure and use a variety of technologies, including data scrubbing, to help keep your websites online. You may need to contact a DDoS mitigation company directly, or your hosting company or service provider may have a partnership agreement with one to handle large attacks.
Set Concurrent Connections Limit	This will regulate DDoS assaults automatically. This establishes the user pool quantity. It can be wise region, IP wise, etc. configured. This automatically mitigates DDoS attacks.

Justification of probability and Severity values

Attribute	Value	Justification
(6) Probability	75%	Probability is high because there are many DDoS attacks around and cost for initiating this type of attack is very low.
Reputation & Customer Confidence	8	Reputation will be highly Damaged. Due to the down time of systems, Clients will lose the trust about the company and it's systems. Therefore, the high impact value is given (8/10)
Financial	5	Clients might lose their sensitive data from the attack. It is cost effective to take measures to minimize the occurrence of such attacks. And the company might have to recover the client's loses, due to the legal processes. Therefore, an average value is given (5/10)

Productivity	5	Productivity of the company's web hosting services goes down with this. But because of this company is having BYOD concept, the other parts of the company's work might go on as usual .There for the impact on productivity is medium (5/10)
Safety & Health	0	There is no impact on safety and health. Therefore, no value is given (0/10)
Fines & Legal Penalties	3	Since the attack is an external attack the chances of getting fines are less. There is a possibility for being charged with penalties for insufficient risk mitigation methods which leads to loss of data. Therefore, a low value is given (3/10)
User Defined Impact Area	0	There are no User Defined Impact Areas. Therefore, no value is given (0/10)

02.Data Steal.

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Threat	Information Asset	Projects files and data		
		Area of Concern	Our company is having BYOD (Bring your own device) concept. So we brought our own devices to work in the office. personal laptops and other devices are having access to our file transfer protocol which include all the projects and sensitive stuff. So if someone stole my laptop and find out a way to hack my password, he will get access to all sensitive data of the company.		
		(1) Actor *Who would exploit the area of concern or threat?*	Intruder		
		(2) Means *How would the actor do it? What would they do?*	So after intruder get access to my laptop, that person can copy all the sensitive data. change the data, delete highly valuable data, also he can add a virus into the system so that no one can access the projects files again.		
		(3) Motive *What is the actor's reason for doing it?*	Intentional		
		(4) Outcome *What would be the resulting effect on the information asset?*	☐ **Disclosure** ☐ **Destruction** ☐ **Modification** ❑ **Interruption**		
		(5) Security Requirements *How would the information asset's security requirements be breached?*	Maybe intruder wants to give company data into a third party or he wants to hack the system so that he can get to know what is happening inside the company		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High** **(75%)**	☑ **Medium** **(50%)**	❑ **Low** **(25%)**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
After gain access by the intruder, company security will eventually go down, and because of that clients trustworthy will reduce. This will definitely affect the reputation of the company. Sometimes companies can't find who is the intruder and how the intruder done this breach. So in order to find out, the company has to pay third parties to find out who did this. This will affect the financial state of the company	Reputation & Customer Confidence	7	3.5
	Financial	4	2.0

	Because of lost client confidence, clients will no longer give their projects for the company. So productivity will go down.	Productivity	3	1.5
		Safety & Health	0	0
	And if a client take legal actions for losing his data, the company has to face many financial problems (Hiring Lawyers), of course they will lose their profits also.	Fines & Legal Penalties	2	1
		User Defined Impact Area	0	0
			Relative Risk Score	**8.0**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

❑ **Accept**	❑ **Defer**	☑ **Mitigate**	❑ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Stop using own device for company work	Management should stop this concept of using own device for company works. This all happened due to having company works inside personal devices. We take personal devices everywhere. So there is a high risk of data breach using our personal devices.
File transfer protocol block	when an intruder try to attempt to the system file transfer protocol, We can set a maximum number of attempts to log into the protocol. So when the intruder try to enter our protocol using different IP's we can block the entire protocol.
Use monitoring tools to monitor file transfer protocol and server changes	Using protocol monitoring tools, companies can identify every single thing done to the file server including the intruder location.
Always keep backups on cloud servers	It's a good thing of having different cloud servers to backup company data. So whether there was an attack, we can easily get those backups using those cloud servers

Justification of probability and Severity values

Attribute	Value	Justification
(6) Probability	50%	Probability is medium because stealing someone's personal device is not happening usually. But if that happens then the attack can be harmful.
Reputation & Customer Confidence	7	Reputation will be highly damaged. because when a client find out their personal details are breached, that will highly affect a company's reputation (7/10)
Financial	4	Company might lose their sensitive data from the attack. It is cost effective to take measures to minimize the occurrence of such attacks. Therefore, an average value is given (4/10)
Productivity	3	If an intruder gain access to our file system, then he will definitely change some of our files and maybe release sensitive data. So at this time the company has to spend their resources to find out who did this attacks, and how intruder did this. So at that time, productivity will go down (3/10)
Safety & Health	0	There is no impact on safety and health. Therefore, no value is given (0/10)
Fines & Legal Penalties	2	Because of the attack clients can take legal actions against the company, So company has to face those legal actions (Hiring Lawyers)(2/10)

User Defined Impact Area	0	There are no User Defined Impact Areas. Therefore, no value is given (0/10)

03.Power Interruption.

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Threat	Information Asset	Project Files and Data		
		Area of Concern	This company has no power generator or any power backup plan. Because of that when there is a power failure, company work stops.		
		(1) Actor *Who would exploit the area of concern or threat?*	N/A		
		(2) Means *How would the actor do it? What would they do?*	This company is a startup company, So they have small power backup only for servers not for company computers, so if there was a power failure, internet connection stops and due to that staff can't access the File transfer protocol. File transfer protocol is the protocol where all the company files are stored. when power is down company staff can't do any changes to the company documents and files.		
		(3) Motive *What is the actor's reason for doing it?*	Natural disaster		
		(4) Outcome *What would be the resulting effect on the information asset?*	☐ **Disclosure** ❑ **Destruction** ❑ **Modification** ☑ **Interruption**		
		(5) Security Requirements *How would the information asset's security requirements be breached?*	Not having powerful power backup		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	☑ **High** **(75%)**	❑ **Medium** **(50%)**	❑ **Low** **(25%)**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
This company has no any backup plan. So if there any power failure, File server gonna shut down. So at that time, if a client call and ask for a change in a website. Company can't do that quickly. Because they need to stay until the power come online. That makes this company reputation looks bad and customers trust gonna lose. Because of this failure, clients gonna leave this company. Company revenue falls down.	Reputation & Customer Confidence	9	6.75
	Financial	7	5.25

	At that time all the computers will shut down. So the company can't do any work. This will directly affect the productivity of the company. File server will be interrupted due to this reason.	Productivity	5	3.75
		Safety & Health	0	0
	There can be an immediate change on a site requested by a client. Due to no power, the company can't help that client at that moment. Company must be ready for this kind of situations. Now the client can take legal actions against the company. That will cost money for the company	Fines & Legal Penalties	3	2.25
		User Defined Impact Area	0	0
			Relative Risk Score	**18**

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
❑ **Accept**	❑ **Defer**	☑ **Mitigate**	❑ **Transfer**
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*		
Buy a new powerful power backups that can be used for entire company	This company only have small power generators. Those generators won't help to backup the computers inside the company. So in order to keep all the computers running when there was a power failure, company needs to get a high performance power generators. Those new powerful generators will keep the computers running whenever there is a power failure.		
get portable WIFI routers, so that they can be used whenever power is down	Portable wifi routers help to keep computers with uninterrupted network connection. Having this kind of gadgets helps when there is a power failure.		

Justification of probability and Severity values

Attribute	Value	Justification
(6) Probability	75%	Probability is high, because in Sri Lanka there was a high probability of losing power. So as a company they need to be prepared for that kind of situations. If they are not

		ready. They have to face many consequences.
Reputation & Customer Confidence	9	Reputation will be highly damaged. Due to power failure company can't access the file protocol. So if a client asks for a change on their site, they can't do it immediately. So the customer reputation is going to be highly damaged. (9/10)
Financial	7	company might lose their clients trustworthy, and also productivity goes down. Company couldn't finish projects within the time period. So due to those problems this company may face lots of financial troubles(7/10)
Productivity	5	if this power failure happens then definitely productivity goes down. Because at that time no one can do anything at the office. So it's high risk. (5/10)
Safety & Health	0	There is no impact on safety and health. Therefore, no value is given (0/10)
Fines & Legal Penalties	3	There is a high probability of taking legal actions by clients due to this power failure. Because at that time no changes can be done to their site. (2/10)
User Defined Impact Area	0	There are no User Defined Impact Areas. Therefore, no value is given (0/10)

04.SQL Injection Attack .

Allegro - Worksheet 10		Information Asset Risk Worksheet			
Information Asset Risk	Threat	Information Asset	Employee Management System (EMS)		
		Area of Concern	SQL Injection Attacks		
		(1) Actor *Who would exploit the area of concern or threat?*	Internal Intruder.		
		(2) Means *How would the actor do it? What would they do?*	To make an SQL Injection attack, an attacker must first find vulnerable user inputs within the web page or web application. A web page or web application that has a SQL Injection vulnerability uses such user input directly in an SQL query. The attacker can create input content. Such content is often called a malicious payload and is a key part of the attack. After the attacker sends this content, malicious SQL commands are executed in the database.		
		(3) Motive *What is the actor's reason for doing it?*	Intentional		
		(4) Outcome *What would be the resulting effect on the information asset?*	☐ **Disclosure** ☐ **Modification**	☐ **Destruction** ☐ **Interruption**	
		(5) Security Requirements *How would the information asset's security requirements be breached?*	To find out other people's salary and private informations and to change intruder's overtime details, bonus salary amounts and leaves		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	☐ **High** **75%**	☐ **Medium** **50%**	☐ **Low** **25%**
	(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*		(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
			Impact Area	**Value (0-10)**	**Score**
	Intruder will access the database and make changes in the records using SQL Injections. Sometimes they will change		Reputation & Customer Confidence	3	1.50

	not only their personal details but also other employee's details. So because of that employee's trust will reduce and they will think that this changes done by the company itself. So again company reputation will go down. Company needs to find out who is doing these things. So they need some expertise and more human resources. That will affect the company's financial state.	Financial	2	1.00
	Because of these kind of attacks company needs to spend resources and more attention to find out how this happened and who is doing these things. So eventually productivity will go down.	Productivity	2	1.00
		Safety & Health	0	0.00
	Sometimes the employee will take legal actions due to this case, at that time the company has to face financial troubles	Fines & Legal Penalties	0	0.00
	Employees think that these changes are made by the company. So they lost their trust in the company. Because of employee lack of trust and confidence productivity will go down eventually.	Employee Trust	5	2.50
			Relative Risk Score	**6.00**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

❑ **Accept**	❑ **Defer**	☑ **Mitigate**	❑ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Firewall.	Consider a web application firewall (WAF) either software or appliance based to help filter out malicious data. Good ones will have a comprehensive set of default rules, and make it easy to add new ones whenever necessary. A WAF can be particularly useful to provide some security protection against a particular new vulnerability before a patch is available.
Reduce your attack surface.	Get rid of any database functionality that you don't need to prevent a hacker taking advantage of it. For example, the xp_cmdshell extended stored procedure in MS SQL spawns a Windows command shell and passes in a string for execution, which could be very useful indeed for a hacker. The Windows process spawned by **xp_cmdshell** has the same security privileges as the SQL Server service account.

Use appropriate privileges.	Don't connect to your database using an account with admin-level privileges unless there is some compelling reason to do so. Using a limited access account is far safer, and can limit what a hacker is able to do.
Don't divulge more information than you need to	hackers can learn a great deal about database architecture from error messages, so ensure that they display minimal information. Use the "RemoteOnly" customErrors mode (or equivalent) to display verbose error messages on the local machine while ensuring that an external hacker gets nothing more than the fact that his actions resulted in an unhandled error.
Buy better software	Make code writers responsible for checking the code and for fixing security flaws in custom applications before the software is delivered. SANS suggests you incorporate terms from this sample contract into your agreement with any software vendor.

Justification of probability and Severity values

Attribute	Value	Justification
(6) Probability	50%	SQL Injection is an old attack. These kinds of attacks are now rare, because most frameworks are using inbuilt security system.
Reputation & Customer Confidence	3	Reputation will be damaged. But not high, Because using SQL injection attacks are very easy to identify and very easy to solve. (3/10)
Financial	2	Because of changing intruder personal details such as changing salary details will make company to pay for that particular intruder. as an example. If the intruder increase his salary, company should have to pay that salary. (2/10)

Productivity	2	Because of these kind of attacks employees confidence will reduce and because of that eventually employers productivity will go down (2/10)
Safety & Health	0	There is no impact on safety and health. Therefore, no value is given (0/10)
Fines & Legal Penalties	0	There are no impact on fiines & legal penalties. Therefore, no value is given (0/10)
Employee trust	5	Employers are one of the important stakeholders within a company. So keeping them motivated will increase productivity. But with these kind of attacks, their confidence and trust into the company will be reduced and maybe employee turnover will be increased also (5/10)

05.Spear Phishing attack.

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Threat	Information Asset	Clients information , Company's sensitive information.		
		Area of Concern	Spear Phishing attack.		
		(1) Actor *Who would exploit the area of concern or threat?*	Intruder.		
		(2) Means *How would the actor do it? What would they do?*	Attackers collect information from social media about potential targets, including their personal and professional relationships and other personal details. The attacker uses this information to craft a personalized message that looks and sounds authentic to convince the target to respond to the sender's request. The sender may request that the user reply directly to the email, or the message may include a malicious link or attachment that installs malware on the target's device, or directs the target to a malicious website that is set up to trick them into giving sensitive information like passwords, account information.		
		(3) Motive *What is the actor's reason for doing it?*	Two motives lie behind spear phishing: stealing money and/or getting secrets.		
		(4) Outcome *What would be the resulting effect on the information asset?*	☐ **Disclosure** ☐ **Destruction** ❑ **Modification** ❑ **Interruption**		
		(5) Security Requirements *How would the information asset's security requirements be breached?*	If an intruder got those details, he/she can sell those details to other rival companies on purpose of earning money is one way of doing these attacks for.		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	☐ **High** **75%**	☐ **Medium** **50%**	❑ **Low** **25%**
	(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*		(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
			Impact Area	**Value**	**Score**

	Because of Lack of security awareness, will loss the Client confidence and company's sensitive data.	Reputation & Customer Confidence	8	4..0
		Financial	5	2.50
	If the customers take legal action against the company, even if the company is not directly liable for the theft of their loss, justifying and providing legal services may cost some resources.	Productivity	0	0.0
		Safety & Health	0	0.0
	Client will be disappointed about leaking their data to a third party, this will bring a negative impact to the company. (Loss of reputation)	Fines & Legal Penalties	2	1.00
		User Defined Impact Area	0	0.0
			Relative Risk Score	**7.50**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

❑ **Accept**	❑ **Defer**	☐ **Mitigate**	❑ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Educate employees.	Addressing phishing threats requires more than building or deploying a security solution. Company need to invest in employee security awareness training to teach how to recognize and respond to phishing attacks. Intermedia's security team runs an employee security education program called 'Hacktober' designed to simulate cyber threats to build awareness around phishing attacks. The program has seen great success, with significantly fewer employees clicking on a phishing email year over year.
Filtering email and implement anti-phishing protection.	Traditional email security solutions include anti-spam and anti-virus filters, which are great at mitigating known threats. Unfortunately, most of these solutions have no counter measures for spear phishing emails. Since spear phishing emails usually contain no malware and are almost never spam, they are often getting past these traditional security filters. Effective anti-phishing protection should include checks for domain spoofing, impersonation, and the ability to flag suspicious content within externally originated email.
Run frequent backup.	Over 90% of phishing emails contain ransomware (malware capable of blocking user access to files and systems), making a successful attack hugely disruptive for your business. Organizations need to get users back to work quickly by getting them access to the latest versions of uninfected files. Having a cloud-based file back-up solution is critical to keeping users productive during a ransomware attack.

Deploy a data loss prevention solution.	CEO fraud or 'whaling' attacks impersonate an executive to trick the recipient into making a wire transfer or disclosing sensitive information such as W-2 forms. Data Loss Prevention offers outbound email protection against leakage of valuable, sensitive, and proprietary data. For example, IT department can set up a policy to block outbound email containing W-2 forms.
Keep software up to date.	Running regular updates of both your operating system and security software helps to fix security vulnerabilities being exploited by hackers. While viruses might be delivered via email, they can spread across your network using gaps in security caused by outdated software. Next time a security update pops up, make sure to take a few minutes to 'Install Now' rather than selecting the tempting 'Remind Me Later'.

Justification of probability and Severity values

Attribute	Value	Justification
(6) Probability	50%	Probability is medium because most of the browsers have anti-virus and scam prevention tools and recommend users to use when they login to a financial application.But there are some people who are not aware of using these tools and the risk, therefore a medium chance of a spear phishing attack is there.

Reputation & Customer Confidence	8	Reputation will be highly damaged. Due to the leak of client details and also company's sensitive information, Clients will lose confidence about the company and it's system. Therefore, the high impact value is given (8/10)
Financial	5	Company might lose their sensitive data from the attack. It is cost effective to take measures to minimize the occurrence of such attacks. Therefore, an average value is given (5/10)
Productivity	0	There is no impact on productivity. Therefore, no value is given (0/10)
Safety & Health	0	There is no impact on safety and health. Therefore, no value is given (0/10)
Fines & Legal Penalties	2	There is a lesser chance of getting legal fines since the possible controls using firewalls and other methods are used. But due to the possibility of undiscovered loophole a lesser value is given (2/10)
User Defined Impact Area	0	There are no User Defined Impact Areas. Therefore, no value is given (0/10)

References

[1]"DDoS Attack Types & Mitigation Methods | Imperva", *Learning Center*, 2019. [Online]. Available: https://www.imperva.com/learn/application-security/ddos-attacks/. [Accessed: 08- Sep- 2019].

[2]2019. [Online]. Available: https://www.esecurityplanet.com/network-security/5-tips-for-fighting-ddos-attacks.html [Accessed: 08- Sep- 2019].

[3]"5 steps to reducing the risks of spear-phishing attacks", *Intermedia's Business Cloud Blog*, 2019. [Online]. Available: https://www.intermedia.net/blog/2017/08/28/5-steps-to-reducing-the-risks-of-spear-phishing-attacks/. [Accessed: 08- Sep- 2019].

[4]"What is SQL Injection (SQLi) and How to Prevent It", *Acunetix*, 2019. [Online]. Available: https://www.acunetix.com/websitesecurity/sql-injection/. [Accessed: 08- Sep- 2019].

[5]"10 Ways to Prevent or Mitigate SQL Injection Attacks", *Enterprisenetworkingplanet.com*, 2019. [Online]. Available: http://www.enterprisenetworkingplanet.com/netsecur/article.php/3866756/10-Ways-to-Prevent-or-Mitigate-SQL-Injection-Attacks.htm. [Accessed: 08- Sep- 2019].