ŠOLSKI CENTER VELENJE

ELEKTRO IN RAČUNALNIŠKA ŠOLA VELENJE

Trg mladosti 3, 3320 Velenje

MLADI RAZISKOVALCI ZA RAZVOJ ŠALEŠKE DOLINE

RAZISKOVALNA NALOGA

VDIRANJE IN MOTIVI ZA TEM

Tematsko področje:

Avtorja:

Žiga Deutschbauer, 4. letnik

Elijah Hlastan, 4. letnik

Mentor:

Iztok Osredkar

Velenje, 2018

Raziskovalna naloga je bila opravljena na ŠC Velenje, Elektro in računalniška šola, v šolskem letu 2017/2018

Mentor: Iztok Osredkar

Datum predstavitve:

KLJUČNA DOKUMENTACIJSKA INFORMACIJA

ŠD ŠC Velenje, šolsko leto 2017/2018

KG informacijska varnost/vdori v sisteme/heker

AV DEUTSCHBAUER, Žiga/HLASTAN, Elijah

SA OSREDKAR, Iztok

KZ 3320 Velenje, SLO, Trg mladosti 3

ZA ŠC Velenje

LI 2018

IN **VDIRANJE IN MOTIVI ZA TEM**

TD Raziskovalna naloga

OP 6, 30 str., 24 sl., 14 vir.

IJ SLO

JI SLO/EN

AI Živimo v informacijski dobi, kjer so nam podatki bolj dostopni kod kadarkoli. Informacije lahko dobimo že z nekaj kliki, na majhni napravi v našem žepu. Čeprav nam je to prineslo veliko prednosti, je ob temu razkrilo veliko pomanjkljivost - varovanje osebnih podatkov pred zlorabo. Kako dobimo podatke? Kakšni so ti podatki? Ali so nevarni? Vse to sva se spraševala in se nato odločila, da iz tega narediva raziskovalno nalogo.

V raziskovalni nalogi sva raziskala različne načine pridobivanja podatkov, na naši šolski mreži. Preverjala sva kakšne podatke lahko pridobiva in kakšne napade potrebujeva izvesti.

KEY WORD DOCUMENTATION

DN ŠC Velenje, school year 2017/2018

CX information security/hacking in systems/hacker

AU DEUTSCHBAUER, Žiga/HLASTAN, Elijah

AA OSREDKAR, Iztok

PP 3320 Velenje, SLO, Trg mladosti 3

PB ŠC Velenje

PY 2018

TI **HACKING AND THE MOTIVES BEHIND IT**

DT Research work

NO 6, 30 p., 24 fig., 14 ref.

LA SLO

AL SLO/EN

AB We live in an information age, where data is more available to us than ever. We can get information with just a few clicks on a small device in our pocket. Although this gave us a lot of advantages, it also revealed a big disadvantage – protection of personal data. How do we get data? What is this data? Is it dangerous? Because we had so many questions, we decided to write a research paper on this topic.

In it we research different ways of getting data, within our school network. We checked what kind of data we can gather and what type of attacks are necessary.

Kazalo vsebine

Kazalo slik

1 Uvod

V zadnjih nekaj desetletjih je naš planet doživel tehnološki razcvet. Tehnologija nas obdaja povsod in podatki so dostopni komurkoli s povezavo do svetovnega spleta. Kljub temu se pogosto ne zavedamo kakšne podatke pošiljamo v svetovno medmrežje in pogosto zaničujemo možnost zlorabe naših osebnih podatkov. Prav te zlorabe in napadi se iz leta v leto povečujejo, nepridipravi pa si za tarče vse bolj pogosto izbirajo prav osebe, ki pošljejo v svetovni svet malo preveč, kot bi potrebovali.

Ker se ta tema postavlja vse bolj v ospredje in nama je varnost in zasebnost zelo pomembna, sva se odločila narediti raziskovalno nalogo. Želela sva preveriti kako lahko "hekerji" pridobijo naše osebne podatke, predvsem pa kakšne namene bi nekdo imel pri pridobivanju takšnih informacij.

1.1 Namen raziskovalne naloge

V raziskovalni nalogi sva želela preveriti stanje varnosti računalniških sistemov na naši šoli. Obema je varnost zelo pomembna, zato sva jo hotela testirati v ustanovi, kjer preživiva veliko časa. Še bolj pa upava, da bi ta raziskovana naloga pomagala ljudem razumeti, kakšne nevarnosti prinaša tehnologija in kako se pred njimi bolje zaščititi.

1.2 Hipoteze

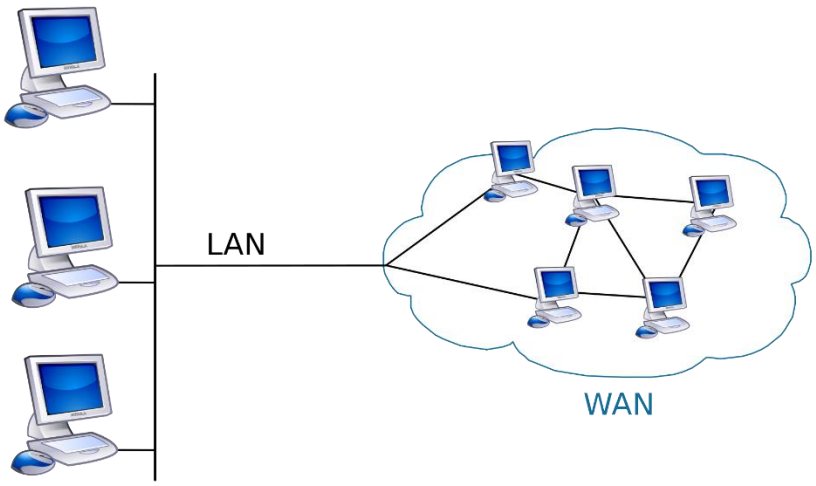
Da bi dosegla najine cilje sva si postavila naslednje hipoteze:

1. Vsak podatek je lahko nevaren.
2. Šola ima veliko zaupnih podatkov, ki bi jih lahko nekdo izkoristil
3. Varnost na šoli ni primerna za poslovanje z takšnimi podatki.

2 Pregled gradiva

2.1 Tipi napadov

Računalniški napadi se ves čas spreminjajo in vsak dan se najde več novih ranljivosti znotraj sistemov in nove napade na te sisteme zato lahko rečemo, da se kibernetske napade preprosto delijo na globalne in lokalne napade.



Slika 1 Primer globalnega in lokalnega omrežja

(Vir slike: https://commons.wikimedia.org/wiki/File:LAN_WAN_scheme.svg)

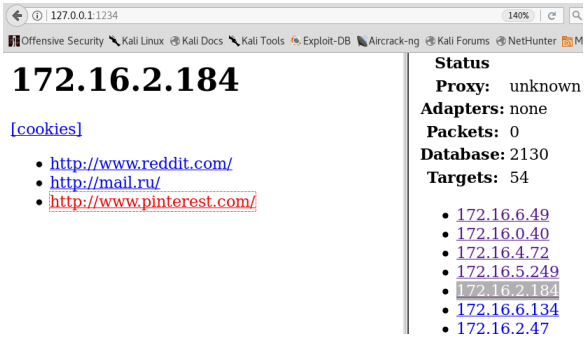
2.2 Lokalni napadi

Lokalno omrežje (LAN), je osnovni gradnik vsakega računalniškega omrežja. Sestavljeno je iz dveh ali več naprav, ki so vse povezani med seboj. Njihova značilnost je, da so zasebna omrežja in se nahajajo znotraj neke zgradbe ali območja katera lahko sega tudi do nekaj kilometrov.

Kot vam že ime pove, lokalni napad je napad kateri je uporaben samo znotraj lokalnih omrežij. Kot je bilo prej omenjeno, napadi se spreminjajo vsak dan zato tudi znotraj lokalnih napadov poznamo več vrst napad. Najbolj znani napadi so prisluškovanje (evesdropping), sniffing (sledenju paketkom), napad posredovalnika (MITM), Data modification, DOS (Denial of service), Compromised key attack…

2.2.1 Prisluškovanje

Kot vam že v imenu piše, prisluškovanje je napad pri katerem lahko napadalec bere paketke drugih naprav znotraj istega omrežja. S posebnio programsko opremo lahko tudi napadalec bere sporočila ali celo posluša pogovore uporabnikov.



(vir slike: lasten)

Slika 2 Primer prisluškovanje

2.2.2 Sniffing

Napad sniffing je proces pri katerem lahko napadalec analizira vse leteče pakete in iz njih črpa podatke kot so gesla ali uporabniških imen

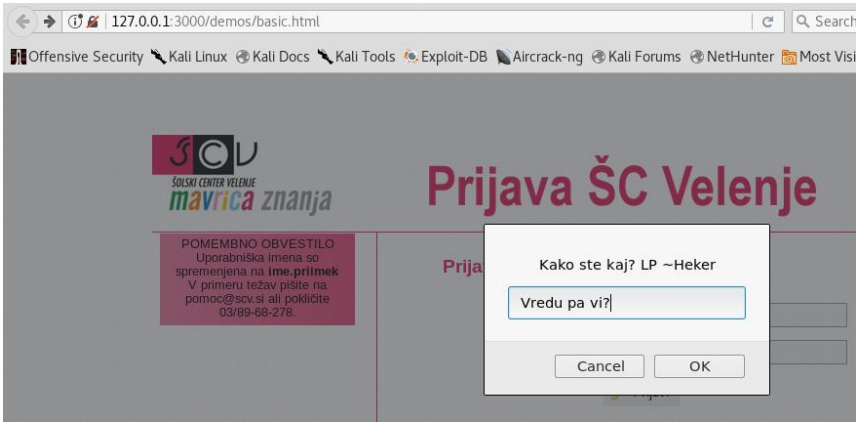
```
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "username" = "Ime.Priimek"
  Form item: "loginAttempt" = "0"
  Form item: "password" = "geslo"
  Form item: "login" = "Prijavi"
```

Slika 3 Primer ukradenega paketka

(vir slike: lasten)

2.2.3 Napad posrednika

Znotraj omrežja imajo vsi paketki, ki se prenašajo, vedno začetno in končno postajo. Napadalec lahko z določeno programsko opremo vstopi med potjo paketkov. Z paketkami katerih sprejme lahko napadalec preusmeri žrtev na željeno spletno stran. Z primerno programsko opremo napadalec lahko tudi manipulira kaj dela žrtev na določenih spletnih straneh.



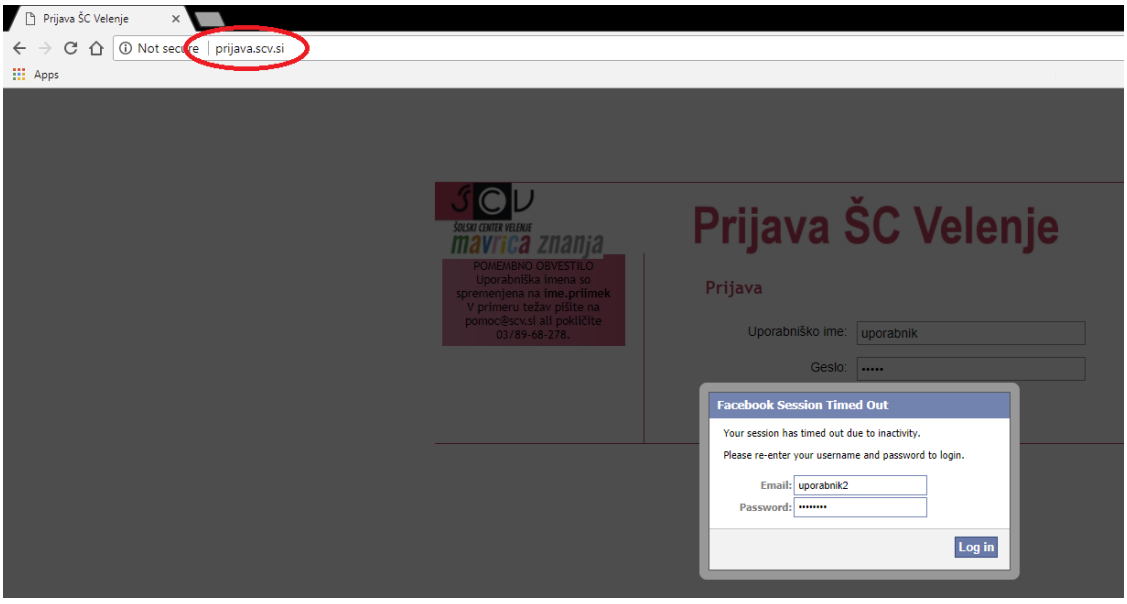
Slika 4 Primer manipuliranja z spletnih straneh preko posredovanja

(vir slike: lasten)

Slika 5 Manipuliranje vsebine na spletnih straneh

(Vir video posnetka znotraj slike: https://www.youtube.com/watch?v=dQw4w9WgXcQ)

(vir slike: lasten)



Slika 6 Primer manipulacije ljudji z uporabo posredovalnika

(vir slike: lasten)

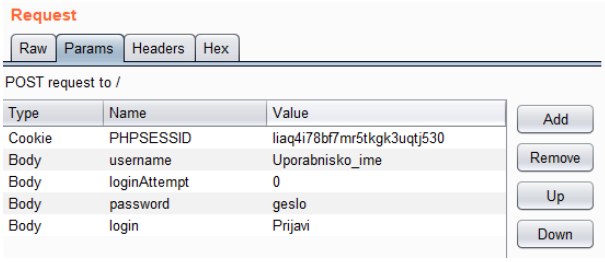
2.2.4 Data modification

Data modification je napad in proces pri katerem napadalec spremeni že leteče podatke znotraj paketkov.

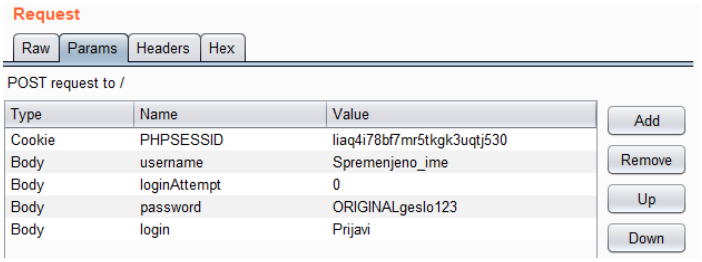
```
POST / HTTP/1.1
Host: prijava.scv.si
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://prijava.scv.si/
Content-Type: application/x-www-form-urlencoded
Content-Length: 68
Cookie: PHPSESSID=liaq4i78bf7mr5tkgk3uqtj530
Connection: close
Upgrade-Insecure-Requests: 1
DNT: 1

username=Uporabnisko_ime&loginAttempt=0&password=geslo&login=Prijavi
```

Slika 7 Primer paketka med prestregom

(vir slike: lasten)



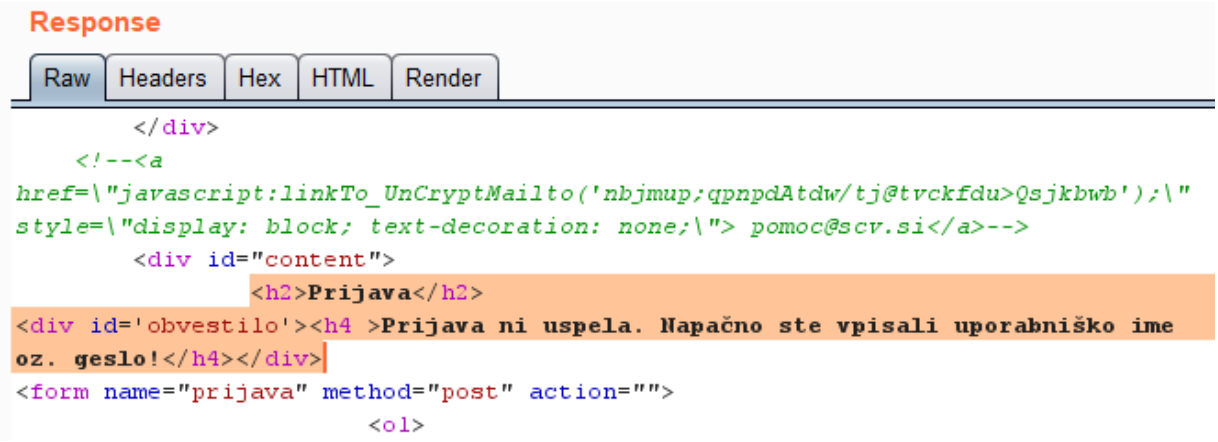
Slika 9 Primer vnešenih podatkov uporabnika



Slika 8 Primer spreminjanja podatkov

(vir slike 7: lasten)

(vir slike 8: lasten)



Slika 10 Primer odgovora pri pristregu napačnih podatkov

(vir slike: lasten)

2.2.5 DoS

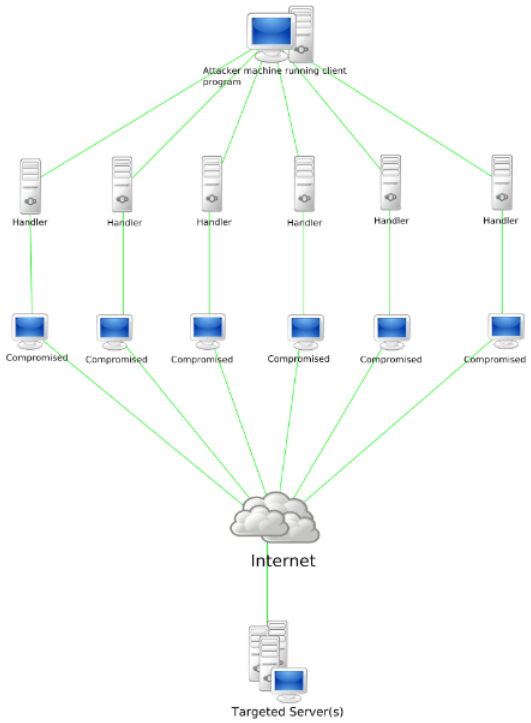
Zavrnitev storitev (Ang. Denial of Service) je napad pri katerem napadalec pošilja veliko količino podatkov preko določenega protokola z namenom, da bi prekinili/zaustavili določene internetne storitve. “to down a service”

2.3 Globalni napadi

Globalno omrežje (WWW) je storitev na internetu, ki uporabnikom sistema omogoča, da si na različnih krajih ogledujejo hipertekst, grafiko, zvok in video.

2.3.1 DDoS

DDoS je zelo podoben DoS napadu ampak razlika med njima je to, da je DDoS (Distributed Denile of Service) globalni napad. Druga razlika med njima je to, da DDoS ni učinkovita če ni več računalnikov kateri hkrati izvajajo enak napad, na isto tarčo. Namen DDoS napada je enak kot pri DoS napadu in sicer da napadalec zruši neko internetno storitev (npr. Strežnik, spletno stran ipd.)



Slika 11 Primer omrežja

(Vir slike: https://en.wikipedia.org/wiki/Denialofservice_attack#/media/File:Stachledraht_DDos_Attack.svg)

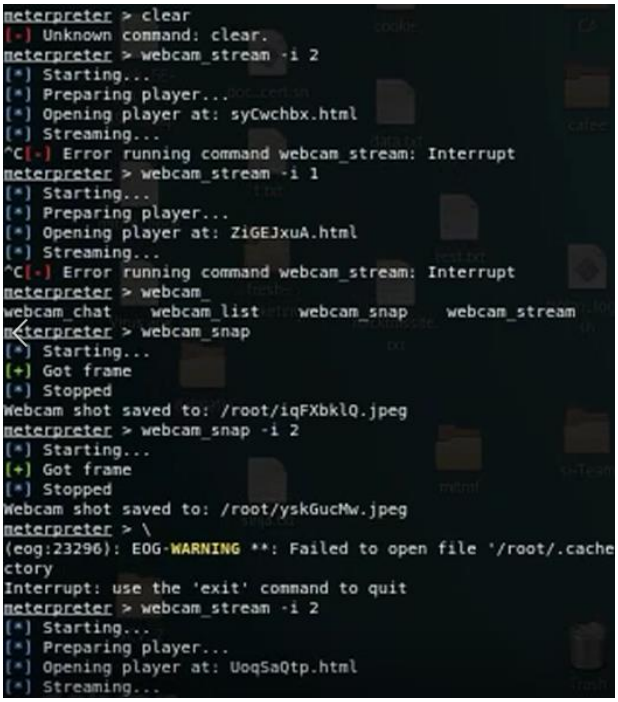
2.3.2 Izsiljevanje

Programi za izsiljevanje (Ransomware) so po navadi programi, ki jih heker podtakne na kakršen koli način na žrtvin računalnik, nato vse podatke na računalniku prekopira, kopije enkriptira in original izbriše. Napadalec potem izsiljuje žrtev za denar in grozi, da bo zbrisal vse podatke če žrtev ne odplača določeno količino denarja.

2.3.3 Reverse Engineering

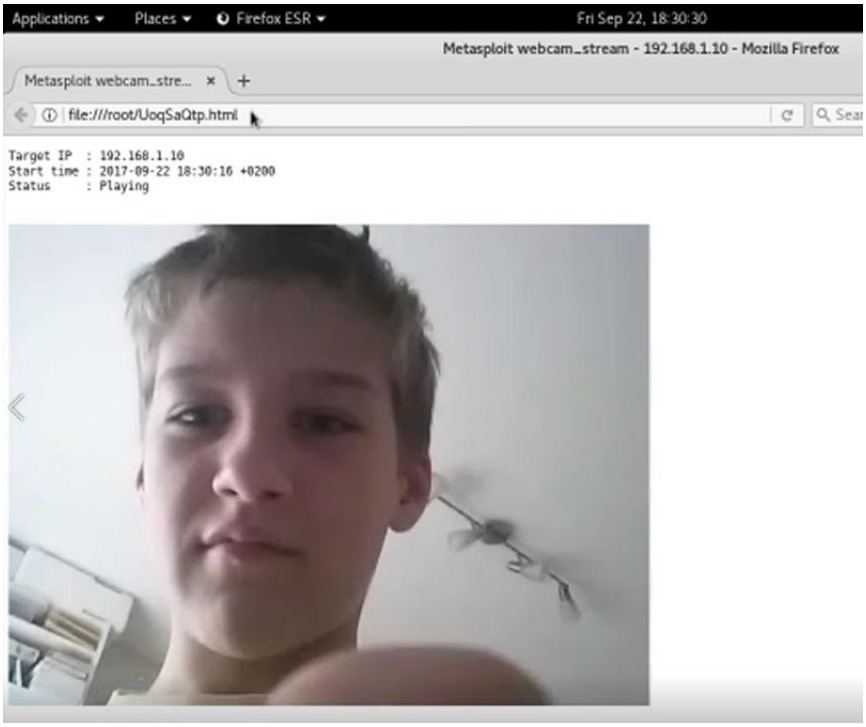
To je napad namenjena za pridobivanje dostopa do računalnika/strežnika z uporabo programov drugih podjetij. Napadalec za ta napad potrebuje veliko znanja, ko pride do področja programiranja. Zakaj? Ta napad deluje tako, da napadalec "razbije" program dokler ne pride do kode. Ko ima kodo lahko heker znotraj programa doda, nekaj zlonamernih linij kode preko katerih lahko heker vstopi do naprave. Ta napad deluje na globalnem in tudi na lokalnem nivoju. V praksi je dokaj težko izvesti taksen napa, ker ima večina naprav vgrajeni antivirusni programi, za odstranjevanje zlonamernih programov in lahko zaznajo številnih vrst virusov ali zlonamerne kode.

Za primer sem z dovoljenjev preko navadne android aplikacije iz google trgovine vstopil v android mobilno napravo od brata.



Slika 12 Primer konzole preko katerega smo vdirali v mobilno napravo

(vir slike: lasten)

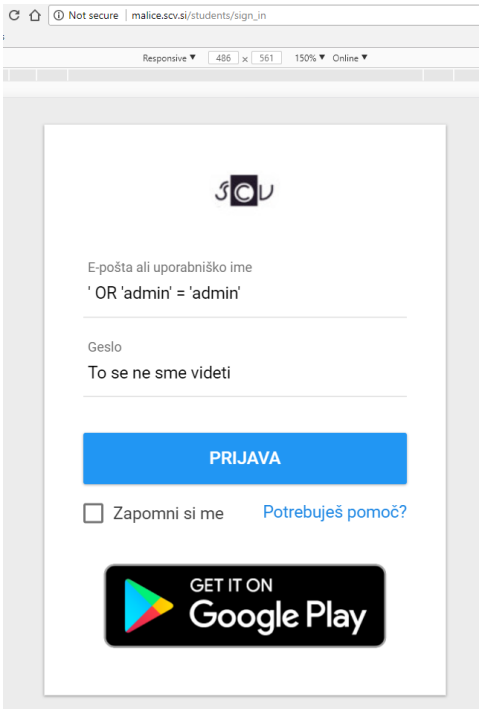


Slika 13 Primer manipuliranja telefona in snemanje "v živo" s kamero ogrožene mobilne naprave

(vir slike: lasten)

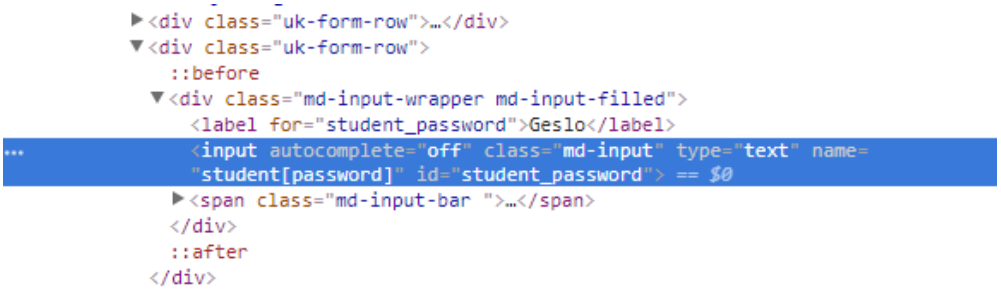
2.3.4 XSS

XSS (cross site scripting) je napad pri katerem heker manipulira kodo, ki se izvaja na določenemu strežniku za svoje namene (npr. Spletna stran za oddajanje naloge v soli …). napadalec lahko napiše določeno sintakso znotraj teh polj, na spletni strani. Ker se koda izvede na strežniku, bo ko heker napise kakšno sintakso za izpis celotne podatkovne baze strežnik izvedel to kodo. Ta napad se da preprosto preprečiti tako da administrator strežnika naredi, da se vsa vsebina znotraj vnosnih polj pretvori v niz znakov (ang. string), katero računalnik razume kot navadno besedilo in ne kot izvršljivo kodo.



Slika 14 Primer spreminjanje kode na spletni strani

(vir slike: lasten)



Slika 15 Primer spremenjene kode

(vir slike: lasten)

Znotraj vsakega brskalnika lahko spreminjamo kodo spletne strani (ampak samo na naši strani) Z pomoč tega lahko veliko krat razkrijemo skrite dele znotraj spletnih straneh katerih lahko izkoristimo.

2.4 Programska oprema

Programska oprema je najpomembnejše orodje, ki ga lahko ima heker. Večina, današnjih orodji se je razvila iz orodji za testiranje varnosti in spremljanje prometa na omrežjih, spletnih straneh … Le ta je bila nato predelana v programe za zlonamerno uporabo, vendar pa obstaja še veliko programov, ki so bili oz. so napisani od začetka.

Pri hekanju se programska oprema deli na to zakaj se uporablja, saj ima več načinov uporabe.

Najpomembnejši programi so tisti, ki nam omogočajo zbiranje podatkov. Le ti se uporablja predvsem ob pripravi na napad. Programi v tej kategoriji so namenjeni predvsem zbiranju čim več informacij o žrtvi in sistemu, ki ga napadamo. Informacije, ki jih pridobimo, lahko vključujejo programsko in strojno opremo, ki jo žrtev uporablja. Včasih je dovolj le brskalnik in dostop do spleta, saj lahko veliko uporabnih informacij o žrtvi najdemo prav tam.

Ko smo pridobili čim več informacij o žrtvi, nastopijo programi, ki so specializirani za iskanje napak in šibkih točk sistema, ki ga napadamo. Večina takšnih programov deluje na ta način, da so povezani na podatkovno bazo že najdenih napak v razni programski in strojni opremi.

Ko heker pridobi informacije in identificira napake v sistemu, ki ga žrtev uporablja, lahko prične z napadom. Programska oprema, ki jo uporablja pri samem napadu je odvisna od samega sistema, napak v njem in pa tudi namena hekerja.

Pod programsko oprem, ki jo uporabljajo hekerji sodijo tudi virusi, črvi trojanski konji … Takšna oprema se deli predvsem na dva dela: tisti, ki pridejo z nekim drugim programom in tista, ki je samostojen program.

2.4.1 Operacijski sistem

Pri vdiranju je najbolj pomemben del računalnika vedno operacijski sistem (krajše OS). Imamo 3 glavne operacijske sisteme kateri obstajajo.

Windows:

Najbolj znan in najbolj razširjen OS je Windows, ki ga je razvil Bill Gates, ustanovitelj in CEO podjetja Microsoft. Windows OS je namenjen za skoraj vse, uporablja se v podjetjih, (dopisi)

MAC OS:

MAC OS in Linux sta si zelo podobna. MAC OS je zgrajen po BSD kodi in Linux je neodvisen razvoj Unix-podobnemu sistemu. To pomeni, da sta si oba zelo podobna ampak nista binarno kompatibilna. MAC OS je tudi zgrajen s pomočjo zaprto kodnih knjižnic, Linux pa je v celoti zasnovan iz odprtokodnih knjižnicah. Zaradi uporabe zaprto kodnih knjižnic, je vdiranje s pomočjo

MAC OS bistveno težje. Odprtokodni operacijski sistemi se uporabljajo samo zato, ker nudijo več možnosti za razvoj takih programskih orodij.

Linux:

Četudi MAC OS uporablja jedra, ki so podobna sistemu Linux, je se vedno zelo drugačen od ostalih OS na trgu. Za Windows OS plačaš za licence, MAC OS dobiš samo zraven Apple-ovih produktov. Linux pa je odprtokoden in zastonj. Ker je odprtokoden OS, lahko kdor koli programira in razvija zanj. Zato večina hekerjev uporablja prav ta sistem. Veliko njegovih distribucij obstajajo (npr. Ubuntu, Debian, Tailes …). Najbolj razširjena distribucija Linuxa, ki jo uporabljajo hekerji, je Kali Linux.

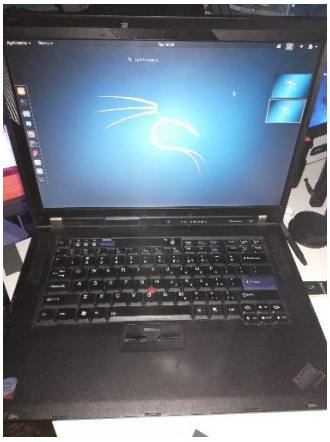
Kali Linux je lahek hkrati pa močan OS kateri je najbolj znan po njegovi uporabi. Kali Linuxa so razvili hekerji za hekerje.

2.5 Strojna oprema

Računalniki ne delujejo brez svoje strojne opreme, ampak ali je res, da potrebujemo najboljšo strojno opremo za kibernetske napade? Odgovor je lahko ja in ne.

Ja: vdiranje v računalnike lahko uporabi res močne komponente za računalnike kot so močan procesor za hitrejšo generiranje kombinacij gesel pri brute force napadu, dovolj spomina v RAM za začasno shranjevanje in analizo paketkov pri napad posrednika ali pa dovolj prostora na ROM za shranjevanje programske opreme za napade. (dopiši)

Ne: kibernetske napade ne potekajo samo preko običajnega računalnika ampak heker lahko uporabi običajne IoT komponente za izvajanje določene napade (npr. Raspberry PI Mikrokrmilnik za pasivno prisluškovanje podatkov na omrežju, navadni USB za skrivno kopiranje podatkov iz računalnika ali pa tudi običajni android telefon za INTENZIVNO in MOČNE brezžične napade).



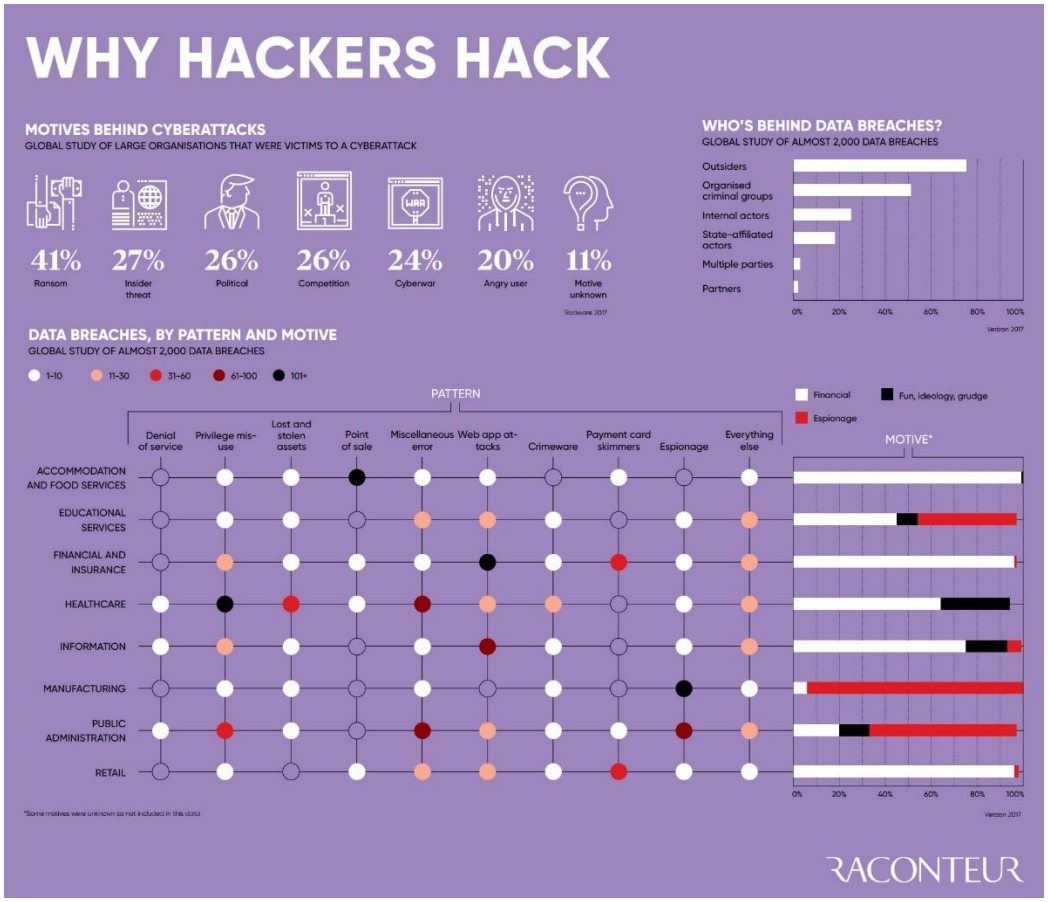
Slika 16 Primer Lenovo ThinkPad R61

(vir slike: lasten)

2.6 Ljudje

V zgodovini računalništva je bilo veliko ljudi, ki je hotelo z raznimi tehnikami, pridobiti podatke in jih uporabiti za škodoželjne namene. Prav tako kot tehnike so se razlikovali motivi teh ljudi.

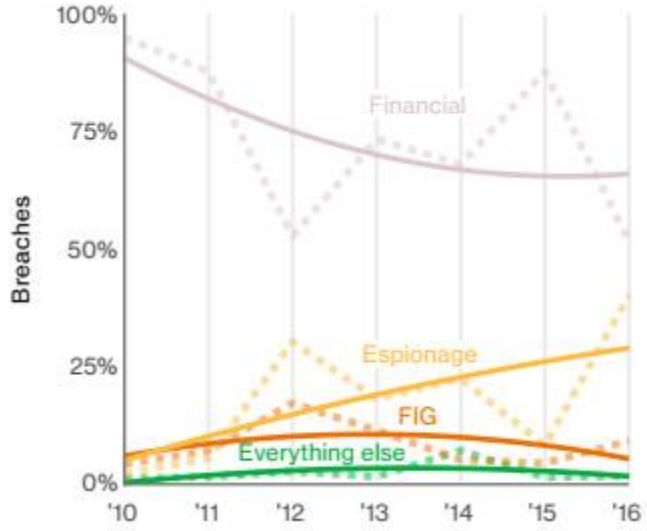
Stran "Visual capitalist" je objavila podatek, da so leta 2016 hekerski napadi povzročili za 450 milijard dolarjev škode, motive za te napade pa pripisujejo največ finančnim vzrokom. Podjetje Racounter je objavilo graf, ki nam kaže motive za napade, ki so se zgodili v letu 2016. V veliki večini so to izsiljevanja (41 %), sledi jim grožnja iz znotraj(27 %), tej tesno sledijo politični motivi in konkurenčnost (oba 26 %), nato pa so tu tudi kibernetske vojne(24 %) in nezadovoljni uporabniki (20 %). Od 11 % napadov pa je motiv neznan.



Slika 17 Graf podjetja Raconteur, ki pikazuje razloge vdorov

(Vir slike: http://www.visualcapitalist.com/hackers-hack-motives-behind-cyberattacks/)

Še bolj pa je zanimiv graf podjetja Verizon, ki je razdelila motive na finančne, vohunske in FIG (zabava (fun), ideologija (ideology) in zamere (grudge)). Na spodnjem grafu so prikazani motivi od leta 2010 do 2016. Vidimo lahko, da je delež napadov z finančnim namenom vpadel, njegovo mesto pa so prevzeli vohunski nameni.



Slika 18 Graf podjetja Verizion, ki prikazuje vzroke vdorov od leta 2010 do 2016

(Vir slike http://www.visualcapitalist.com/hackers-hack-motives-behind-cyberattacks/)

Glede na motive lahko hekerje delimo tudi na bele, sive in črne. Beli hekerji so tisti, ki uporabljajo svoje znanje zato, da pomagajo preprečevati napade preden se lahko zgodijo. Po navadi je njihova identiteta znana. Črni hekerji so pravo nasprotje, saj svoje znanje uporabljajo za osebno rast, največkrat na ilegalne načine. Sivi se znajdejo med njima saj skušajo pomagati z tem, da izboljšajo varnost, vendar po navadi na nezakonite načine.

Čeprav so hekerji po navadi skriti in svoje identitete ne želijo deliti so se v zgodovini pojavili ljudje oziroma skupine, ki so postali slavni. Prvi, ki pride na pamet je Kevin Mitnick. Svojo hekersko pot je začel že leta 1981, ko je ukradel računalniške priročnike iz telefonskega podjetja Pacific Bell. Naslednjo leto je vdrl v severno ameriško obrambo. Po še nekaj napadih so ga prejeli in aretirali. Ko so ga odpustili, je še enkrat vdrl v telefonsko podjetje, omenjeno prej. Njegova posebnost je bila, da svojih vdorov ni izkoristil temveč je le pokazal, da lahko to stori. Trenutno ima svoje podjetje, ki se ukvarja s svetovanjem za varnost.

Zelo znana je tudi skupina Anonymous. Najbolj znani po njihovih maskah, začetki te hekerske skupine so bili v letu 2003 na spletni strani »4chan«. Od takrat dalje je bila skupina aktivna pri napadih nekaterih zelo znanih podjetji in spletnih strani, kot so »Amazon«, »PayPal« in »Sony«. Čeprav je ameriška obveščevalna služba uspela aretirati nekaj posameznikov skupine, Anonymous zaradi ne organiziranosti še vedno deluje.

Verjeto malo manj znan kot prejšnja dva je tudi Jonathan James. Uspelo mu je veliko napadov, njegov najbolj znan pa je vdor v agencijo NASA. Ukradel je veliko podatkov in programske, kode, ki po ocenah znašajo 1.7 milijonov dolarjev. NASA je po tem napadu zaustavila njihovo omrežje kar jim je naredilo še več stroškov. Vendar pa za tega hekerja prihodnost ni bila tako svetla, saj je v letu 2008 naredil samomor, zaradi domnevno lažnih obtožb proti njemu.

(Vir zivljenjepisa: knjiga GHOST IN THE WIRES – avtor Kevin Mitnik in William L. Simon)

2.7 Preprečevanje napadov

Z porastom napadov se je potrebno znati pravilno zavarovati. Obstaja več različnih načinov, kako se obraniti, za navadnega uporabnika pa je najboljša obramba pamet. Nasveti kot so "Ne nalagaj neznanih programov", "Ne odpiraj sumljivih e-pošt", so sicer stari vendar nas obvarujejo pred večino napadov iz spleta. Pri obrambi pred raznimi napadi za navadnega uporabnika nastopijo še požarni zid in razni antivirusni programi, ki nas ščitijo pred večino okužb.

Pri podjetjih nastopi tu še pravilna izbira programske in strojne opreme, enkripcija, omejitev dostopa nepooblaščenim osebam in redna menjava gesel.

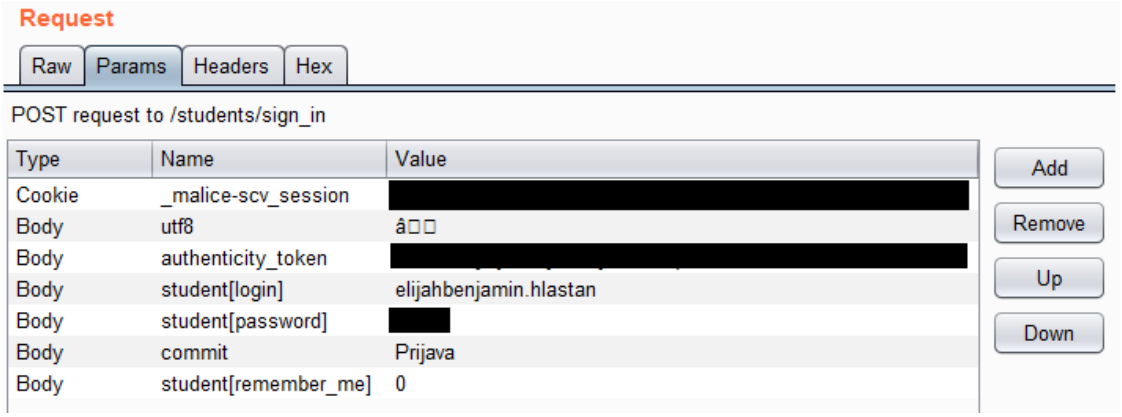
Nove tehnologije pa so že na obzorju, saj veliko strokovnjakov meni, da bi lahko uporabili umetno inteligenco za boljše varovanje in analizo vdorov.

3 Metode

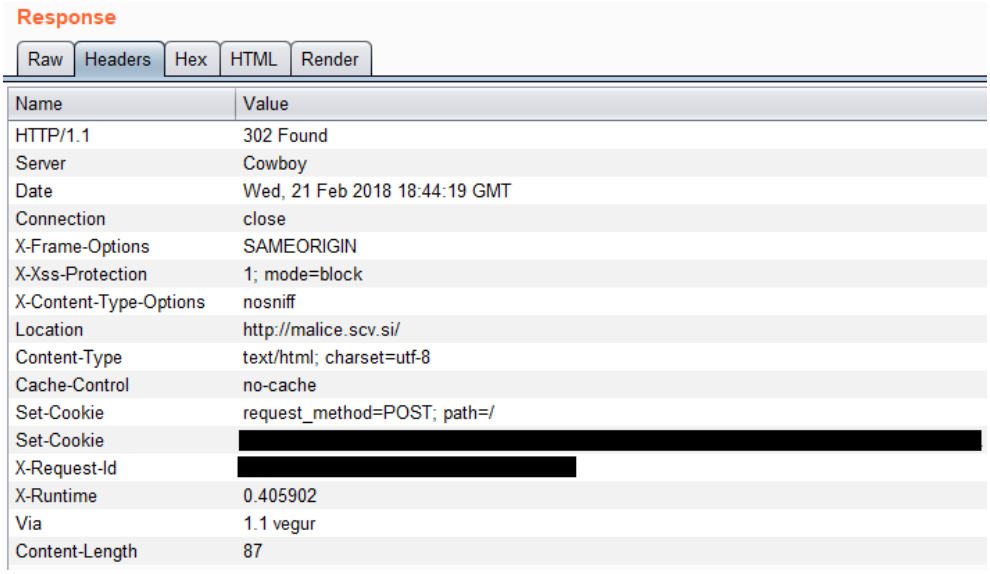
Da bi dosegla cilje najine naloge, sva se odločila, da bova vdore izvedla na naši šoli – Elektro in računalniška šola Velenje. Odločila sva se, da bova izvedla naslednje napade:

3.1 Sniffing

Naša šola ima več sto dijakov in dijakinj. Vsak dijak ima malice na šoli. Da lahko nekdo je, morajo se prijaviti preko spleta in izberejo hrano. Ob pritisku gumba prijavi se podatki uporabnika pošljejo preko našega omrežja. Mi lahko tega prisluškujemo. Z uporabo primernega programskega oprema bi lahko prebrali vsa gesla vseh uporabnikov portal za malice.



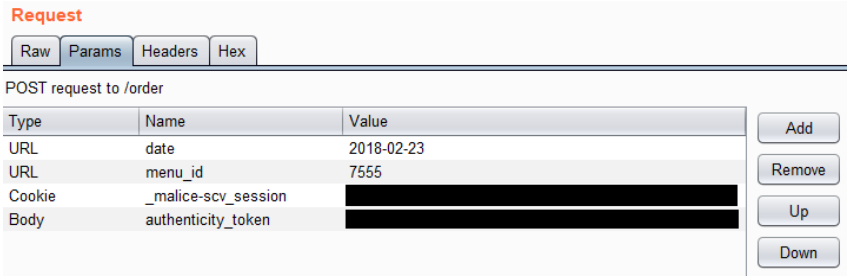
Slika 19 Primer kraje svojih podatkov



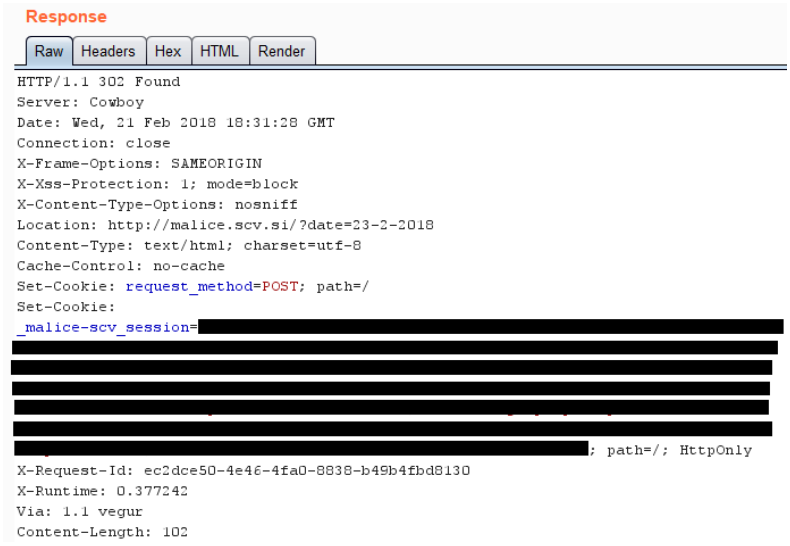
Slika 20 Primer Odgovora pri kraji svojih podatkov

3.2 Data modification

Paketki so sestavljeni iz ne samo uporabniškega imena in gesla ampak v našem primeru niz znakov katera reprezentira določen meni katera je na voljo tisti dan. Ujeti paketki smo lahko spreminjali kakor smo hoteli (npr. Nekdo hoče imeti četrtek margarito v šoli. Lepo se prijavi v portal in si spremeni malice na margarito. Ker omrežje ni bilo zavarovano med prijavo in med spremembo malice smo prestregli paket in spremenili malice na vegi meni.



Slika 21 Primer ID za specifično jed pri malici



Slika 22 Primer odgovora pri spreminjanju podatkov znotraj paketka

3.3 Napad posrednika

Navada dijakov v naši šoli je, da po uporabi šolskega računalnika vsi izbrišemo zgodovino in chache znotraj brskalnika, da ne pride do kraje naših podatkov. Ampak noben pa ne naredi kaj, da bi preprečili (branje naše zgodovina brskanja, chache, sessions,…)

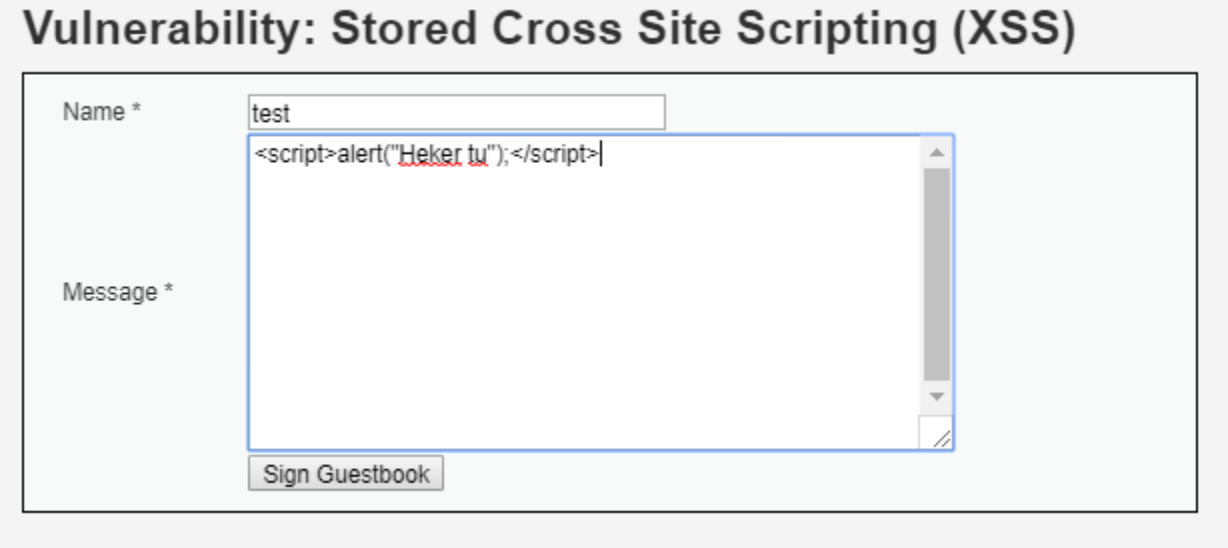
Vrstice za iskanje je zelo koristna stvar znotraj brskalnikov. Iščem nekaj? Sam napišem v vrstico in pritisnemo išči. Ob pritisku na spletno stran se nam spremeni vse znotraj vrstice. Če smo dovolj pozorni lahko opazimo, da je veliko vrednosti znotraj polja. Večino časa ne vemo kaj vse pomeni ampak, če dovolj podrobno pogledamo lahko vidimo, da se te vrednosti spreminjajo glede na kaj delamo na strani.

3.4 XSS

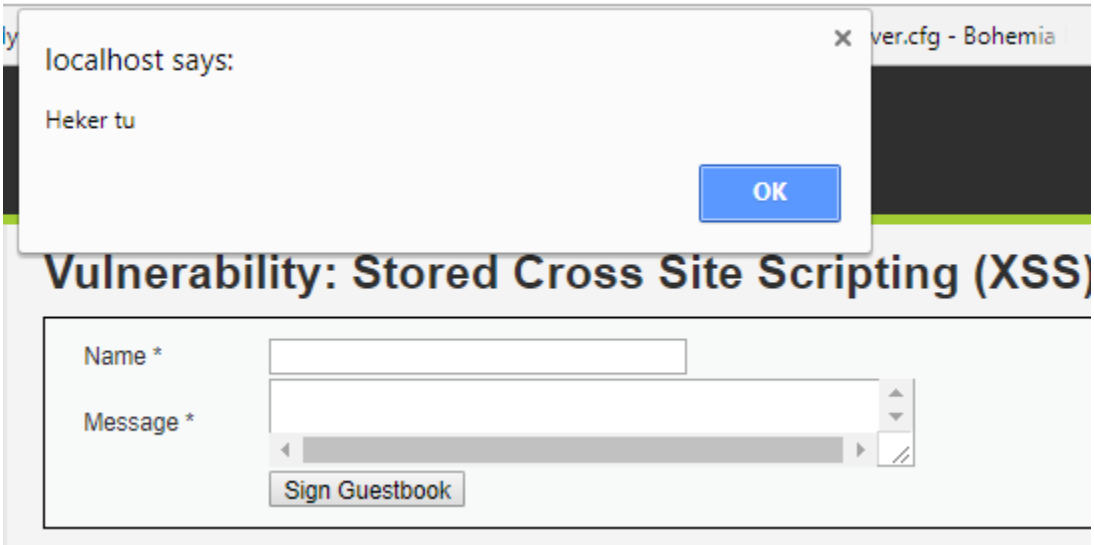
Spletne strani nikoli niso sestavljeni iz samo enega programskega jezika. Večina strani ima vsaj 4 različnih programskih jezikov. Nekatere za obliko strani, nekatere za logiko in nekatere za upravljanje z podatki. Večina strani tudi sprejemajo podatke od uporabnikov preko vnosnih polj. Če spletni portal ni zaščiten se potem tudi vneseni podatki tretirajo kot ukaze.

Za testiranje kako deluje ta napad smo sami poskušali izvesti podobne napade znotraj razvojnega okolja DVWA (Damn Vulnerable Web Application). DVWA je bil razvit z namenom da bi ljudje izobrazili o novejših ranljivosti spletnih aplikacij.

(Vir orodja: http://www.dvwa.co.uk/)



Slika 23 Primer XSS napad znotraj DVWA orodje



Slika 24 Primer uspešen izveden XSS napad

4 Rezultati

Kaj smo ugotovili od vsakega napada? Kot smo videli. Šola ima veliko ljudi, veliko podatkov, veliko naprav in veliko varnostnih lukenj. Šola lahko to preprosto popravi

Ugotovila sva, da je pri varnostnih sistemih še vedno najšibkejši člen človek. Najini napadi, kjer sva sprva pridobila nepomembne informacije (kot na primer geslo za malico), so se prelevili v veliko nevarnost, ko je imel nekdo enako geslo za malico in za e-pošto.

Ugotovila sva tudi, da tehnologija in varnost zelo tesno sledita vdorom in napakam in je večina vdorov možnih zaradi človeškega faktorja.

Prišla sva do zaključka, da čeprav živimo v svetu, v katerem nas obdaja tehnologija, se potrebujejo ljudje še bolj izobraziti na temo varnosti na omrežjih, saj lahko s preprostimi nasveti, izognemo večini napadov.

Veliko varnostne napak se lahko popravi na zelo preprost način. Večina napade kateri so izveden na lokalnem omrežju se da popraviti samo z navadnimi certifikati ali pa navadne metode kriptiranja podatkov v podatkovni bazi.

5 Zaključek

Najini napadi so tako že na začetku obrodili sadove. Tudi podatki, ki sva jih pridobila niso bili zanemarljivi. Tako sva že na začetku najinega raziskovanja podvomila v varnost podatkov na naši šoli, saj sva z preprostimi metodami pridobila kar nekaj gesel. Ko sva že mislila, da bova lahko tretjo hipotezo z lahkoto potrdila, sva naletela na eAsistent, kjer se hranijo ocene in bi bil eden največjih tarč za napad, vendar nama vanj ni uspelo vdreti, ker ne spada pod okvir šole in za vdiranje vanj nisva imela dovoljenja. Pri tem sva tudi ugotovila, da so v sistemu zapisani pomembni podatki, ki bi jih lahko nekdo izkoristil, skozi šolo pa se pretakajo tudi osebni podatki učencev. Zataknilo se nama je pri prvi hipotezi. Sprva se nama nekaj, kot je geslo za šolsko malico, ni zdelo nevarno, vendar sva kar hitro ugotovila, da ima veliko ljudi ista gesla na več spletnih portalih in straneh, kot so socialna omrežja ali pa osebne e-pošte. To pa so že večji posegi v zasebnost saj na teh portalih kroži veliko osebnih podatkov, kar nas pripelje v šibkost v vsakem varnostnem sitemu – človek. Veliko strani omogoča prijavo z dvema korakoma (na primer: geslo in potrditev iz že znane naprave), vendar nam to nič ne pomaga, če se pozabimo odjaviti od javnega računalnika. S temi mislimi sva končala najino raziskovanje, prvi dve hipotezi pa sva potrdila, tretjo pa delno potrdila.

6 ZAHVALA

Rada bi se zahvalila mentorju Iztoku Osredkarju, za pomoč pri izdelavi raziskovalne naloge, ter dobre ideje ob trenutkih, ko jih nisva imela. Velika zahvala gre tudi ravnatelju šolskega centra Velenja Simonu Konečniku, za zaupanje v naju in dovoljenje pri testiranju njihove varnosti. Prav tako se zahvaljujeva najinim staršem, ki so naju podpirali in spodbujali. Zahvala gre tudi Elektro in računalniški šoli Velenje, ki nama je omogočila izdelavo in izvedbo najine raziskave.

7 Viri

Elektronski viri

- Vrste omrežji. (online). Dostopno na spletnem naslovu: http://wiki.fmf.uni-lj.si/wiki/Vrste_omre%C5%BEja
- Breščak, B. Lokalna omrežja. E-računalništvo (online). Dostopno na spletnem naslovu: http://www.s-sers.mb.edus.si/gradiva/rac/moduli/upravljanje_ik/21_lan/01_datoteka.html
- Desjardins, J. Why hackers hack: Motives behind cyberattacks. Visual capitalist (online). Dostopno na spletnem naslovu http://www.visualcapitalist.com/hackers-hack-motives-behind-cyberattacks/
- http://aic.gov.au/media_library/publications/htcb/htcb006.pdf
- Top ten greatest hackers. Kaspersky (online). Dostopno na spletnem naslovu: https://usa.kaspersky.com/resource-center/threats/top-ten-greatest-hackers
- Lee, J. 10 of the world's most famous hackers & what happened to them. Makeuseof (online). Dostopno na spletnem naslovu: https://www.makeuseof.com/tag/5-of-the-worlds-most-famous-hackers-what-happened-to-them/
- Calypitix, Wht motivates hackers? Money, secrets, fun. Calyptix security (online). Dostopno na spletnem naslovu: https://www.calyptix.com/top-threats/motivates-hackers-money-secrets-fun/
- Motivations of a criminal hacker. Microsoft (online). Dostopno na spletnem naslovu: https://msdn.microsoft.com/en-us/library/cc505924.aspx
- Hacking: motives, methods and how to protect your web site. Technologi.st (online). Dostopno na spletnem naslovu: https://www.technologi.st/comment/hacking-motives-methods-and-how-to-protect-your-web-site/#.Wm929qinFPY
- OConnel, J. 10 most notorious hackers of all time. Hacked (online). Dostopno na spletnem naslovu: https://hacked.com/hackers/
- Buckle up for a bumpy 2018 as cyber extortion hits new hights. Racounter (online). Dostopno na spletnem naslovu: https://www.raconteur.net/sponsored/buckle-up-for-a-bumpy-2018-as-cyber-extortion-hits-new-highs
- Cyber crime. FBI (online). Dostopno na spletnem naslovu: https://www.fbi.gov/investigate/cyber
- Papadopoulos, L. How Watson Ai is helping companies stay ahead of hackers and cybersecurity attacks. IBM (online). Dostopno na spletni povezavi: https://www.ibm.com/blogs/watson/2017/08/how-watson-ai-is-helping-companies-stay-ahead-of-cybersecurity-attacks/

Knjižni viri

- GHOST IN THE WIRES, avtor Kevin Mitnik in William L. Simon