**Софтуерни технологии**

**Курсов проект**

**Име:** Георги Гинев

**Фак. номер:** 471218052

**Анализ на уязвимост и атаки касаещи груповият проект**

1. **Brute force attack**

Brute force attack е метод за получаване на почти всеки вид тайна дигитална информация. Тя се базира на метод, при който атакуващия тества множество от предварително дефинирани стойности, докато намери правилните. Най-често за този процес се използва автоматизиран софтуер, който по зададени правила генерира тези стойности и/или използва и набор от книжовни думи от речниците , за да тества дали паролата Ви не съдържа някоя съществуваща дума.

Бихме могли да се защити от този вид атака с няколко метода. Най-очевидният е паролата и името да бъдат различни от admin, administrator, 12345 и подобни. Добавяне на **CAPTCHA** би лимитирало автоматичните опити за налучкване на името или паролата.

Друг вариант за защита от този вид атака е блокиране на акаунта след определен брой опити за вход. По този начин само собственика на акаунта ще може да го отключи като му бъде изпратено писмо по имейл.

1. **HTTP floods**

Още познати като DDoS атаки. Това са атаки с цел ограничаване, затрудняване или прекъсване на достъпа на потребителите до дадената услуга. В зависимост от протокола, по който се атакува собственика на услугата, атаката може да се предотврати. Ако атаката се изпраща по TCP протокол, тя може да бъде предотвратена като се лимитира възможността на дадено IP да се свързва с това на собственика. Ако атаката е по UDP протокол и интернет връзката на собственика на услугата е по-слаба от тази на атакуващия, то собственикът няма да може да се защити, единственият вариант, по който може да се опита да се защити е на по-високо ниво(неговият доставчик) да се предприемат мерки за филтриране на изпратените празни пакети от атакуващия.

В днешно време има десетки хостинг компании с инвестирани хиляди левове в защити и интернет свързаност, които са далеч по-сигурни да поддържат нашите сайт, отколкото ние на нашият домашен компютър да го правим.

1. **Cross site scripting**

“Cross-Site Scripting” е изключително опасна и често срещана атака, при която на базата на технологичен пропуск злонамерените лица инжектират на сървъра JavaScript код, позволяващ да се промени съдържанието на уеб приложението, както и да се получи неоторизиран достъп до съхранена на сървъра информация. Хакерът не атакува директно избраната жертва, а използва този пропуск като междинен механизъм за изпращането на зловреден код

Злонамерените скриптове, използвани при XSS, могат да получат достъп до данни на потребителя, да създадат нови HTTP заявки към посочени от хакерите цели, както и да модифицират съдържанието на HTML страниците.

XSS атака може да доведе до следните нежелани последствия:

* Кражба на потребителски профили;
* Достъп до историята на въведени в браузъра на целевия потребител адреси;
* Достъп до клипборда (clipboard) на операционната система;
* Ефективен отдалечен контрол на браузъра на атакувания потребител;
* Сканиране на приложения и системи;
* Кражба на бисквитки на потребителя (пренасочване на браузъра към предварително зададен от хакера URL);
* Модифициране на страници за въвеждане на данни и други.

При този тип неправомерен достъп, застрашени са всички сайтове, които визуализират входяща информация. Такива са блогове, форуми, книги за гости, приложенията за електронна поща. Ако тази входяща информация не е правилно валидирана, се получава уязвимост от XSS атаки.

За да се предотврати една XSS атака от програмиста е нужно да спазва едно единствено правило: „Никога не вярвай на потребителя“ – строго проверявай данните въведени от потребителя.

Големи XSS дупки в един сайт биха могли да се намерят със софтуера **burp suite**.

1. **Ransomware**

Рансъмуер (ransomware) е вид злонамерен софтуер (малуер), който може да блокира достъпа до системата или да криптира потребителските файлове. Това обикновено е придружено от съобщение с искане на откуп – единственият начин според хакерите, за да получите достъп до системата си или ключ за декриптиране. Именно оттук идва и наименованието на този зловреден код – „ransom“, което от английски език буквално означава откуп.

Рансъмуерът може да бъде криптиращ данните или не, може да засегне цялата система или само определени файлове. При всички случаи целта е изнудване на засегнатия.

* **Какви щети може да причини т.нар. „рансъмуер“?**

Истината е, че последните години станахме свидетели на няколко по-сериозни атаки, щетите от които бяха огромни. Ако смятате, че загубата на вашите снимки или документи е голяма щета, представете си какъв е ефектът за големите корпорации или държавни учреждения, засегнати от т.нар. криптовируси. „Ефектите“ от инфекция с подобен злонамерен код се изразяват в една или няколко от следните прояви:

* + Криптиране на файлове върху твърдия диск. Обикновено засегнати биват често използваните файлове – снимки, офис документи, видео клипове, бази данни и т.н. Криптираните файлове са неизползваеми и декриптирането им често пъти е невъзможно.
  + Криптиране на сектора за начално зареждане (Master Boot Record – MBR).
  + Заключване на екрана. В този случай потребителските файлове не са криптирани, но достъпът до тях отново е невъзможен – системата по един или друг начин бива „заключена“. Обикновено „заключването“ на компютъра е придружено от съобщение с искане за откуп, след заплащане на който „засегнатия ще получи ключ“. Неслучайно използваме „“, защото такъв обикновено не получаваме.
  + Кражба на лични данни. Злонамереният софтуер може да изпрати до трети страни различни данни – потребителски имена, пароли, снимки, документи и др. Потребителят дори може да бъде изнудван с тях.
  + Блокиране или деинсталиране на антивирусен и антималуер софтуер. Често пъти рансъмуер кодът се опитва (и успява) да саботира инсталирания защитен софтуер, чрез цялостното му блокиране или спиране на определени модули.
  + Блокиране (заключване) на интернет браузъра.
* **Как да се предпазим от рансъмуер?**

На първо място инсталирайте надеждна антивирусна програма. Убедете се, че продуктът, който използвате е лицензиран (не кракнат) и разполага с механизъм за откриване на подобен тип злонамерен код. Уверете се, че операционната система и инсталираните приложения са актуални (обновени до последната версия). Тук от решаващо значение е инсталирането на всички критични обновления на Windows. Обновяването на операционната система в повечето случаи е с цел „закърпване“ на пропуски в сигурността, както и отстраняване на различни проблеми. Същото важи и за инсталираните програми. Бъдете внимателни към съмнителни имейли, особено ако към същите има прикачени файлове или линкове. Не отваряйте прикачени файлове от непознати податели, проверявайте имейл адреса дори и на тези, които изглеждат надеждни. Винаги сканирайте с подходящ антивирусен софтуер всички външни носители на данни, които поставяте – USB флаш памети, карти памет, компакт дискове, DVD и т.н. Правете периодичен бекъп (резервно копие) на най-важните си файлове на външен носител – преносим твърд диск, който не е постоянно свързан или флаш памет. В последните години актуални станаха т.нар. облачни услуги, които са отлична алтернатива. Въпреки това не препоръчваме използването им за качване на строго конфиденциална информация. Практиката ни показва, че компакт дисковете и DVD дисковете са може би най-надеждният носител на данни, що се отнася до създаване на периодични резервни копия на най-важните файлове. Записаните данни на диск (CD или DVD, без опция за повторен запис) не могат да бъдат неволно изтрити, модифицирани и напрактика не могат да бъдат заразени от вируси или друг зловреден код.

1. **SQL Injection**

SQL Injector е техника за инжектиране на код който се използва за атака. Тя позволява да вземеш информацията на една база данни. Първите признаци за уязвимост се появяват когато потребителят който използва SQL Injection въведе знаци които не могат да се филтрират правилно.

Пример за това е когато в input поле се въвежда парола и формата се изпраща на backend-а. Тук трябва да се вметне изразът „Никога не вярвай на потребителя“. Ако потребителят изпрати израз “ **‘ or ‘1’=’1** “ и потребителското име се знае, то при проверката в sql дали този потребител съществува изразът ще бъде : SELECT \* FROM users WHERE name=’admin’ AND password=” **‘ or ‘1’=’1** ”. Изразът password=” **‘ or ‘1’=’1** ” ще бъде винаги true. Тогава „хакерът“ спокойно може да влезе в администраторския акаунт и да направи каквото си пожелае.

* Как да се защитим от **SQL Injection**?
  + Стъпка 1: Не вярвай на това, което въвеждат потребителите.
  + Стъпка 2: Използвай най-новите технологии. При PHP вместо MYSQLi да се изполва PDO.
  + Стъпка 3: Не се опитвайте да създавате защита от нулата. Десетки програмисти са посветили месеци в разработка на библиотеки за тази цел. Почти невъзможно е да измислите нещо, което вече не е измислено за ограниченият ви период от време.
  + Стъпка 4: Сканирайте редовно за нередности. Скенер за това е Acumetix.

1. **Cross site request forgery**

CSRF е широко използвана уязвимост в уеб приложенията. Тази атака, атакуващия може да наруши цялостта на потребителската сесия с уеб страница, като инжектира заявка по мрежата посредством браузъра на потребителя. Политиката на сигурност на browser-ите позволява уеб адресите да изпращат HTTP заявка до който и да е мрежови адрес.

Накратко: CSRF е мястото, където злонамерен уеб сайт ще се опита да издаде действия по отношение на друг сайт, без знанието на потребителя от него, настъпили.

Имаме следната ситуация. Направилисте си регистрация в някой сайт за онлайн банкиране ОК, няма проблеми. Дали сте отметка на „Запомни ме“, когато сте се вписали. Сега.. да предположим, че имате опция за лесно прехвърляне на пари между хората. Т.е. искам да кажа прехвърляте си пари от Адриян до Петкан. (например) При трансфера, ако се загледате може да забележите нещо от вида на: banka.com/transfer.php?To=46346442634?cena=1000.

Какво всъщност правите с горния линк? Правите трансфер до клиентски номер: 46346442634, на стойност 1000 $/лв/евро – все тая. Всъщност. Трансфера ще е успешно до Петкан – няма проблеми ние искахме да му преведем дадената сума, НО ако имаме някой зъл хакер, който иска да ни манипулира и не само нас, но и всички хора, които имат регистрация във въпросния сайт. Може да ни прехвърли парите ни в неговата сметка. Това може, да стане ако сайта е уязвим към CSRF. Виждате някакъв безобиден сайт, но всъщност е „заразен“. Който прави горната манипулация и се прехвърлят парите.

Този проблем е известен като (CSRF) и това е потенциален проблем във всеки един динамичен уеб сайт. Докато кражба на пари е краен пример, CSRF може да се използва, за да открадне „бисквитки“ от един уеб сайт или да публикувате нежелана поща коментари по блогове, изтриване на албуми, снимки, без потребителят да е наясно, че това го правят от друг сайт(злонамерен).

Действия на уеб сайтове винаги са свързани с форми – влизане в системата, прехвърляне на пари или публикуване на коментар в блога. Решение на проблема CSRF е да се генерира уникален ключ(token), когато потребител посети страницата с формата.

1. **Packet sniffing**

Същността на Packet sniffing атаката е програма или устройство, улавящо мрежовия трафик специфична за дадената информация.

Целта от всичко това е да се открадне нещо – пароли, email-и, файлове по мрежата и други.

Изисква се пакет, който да извършва „подслушването“ на информацията.

Видове sniffing атаки са:

* **Пасивни -** реализират дейността си чрез/през хъб. Много трудно могат да бъдат проследени по мрежата. Вече не се използват.
* **Активни –** „подслушването“ се осъществява чрез суич. Лесно могат да бъдат открити. Разчитат на „инжектирането“ на ARP пакети в мрежата, които предизвикват трафик.

Средства за извършване на sniffing атаки.

* **MSN Sniffer** – платена версия, служи за улавяне на MSN чат в мрежата, записва разговорите автоматично.
* **BetSetMan** – платена версия, но има и безплатна, която позволява създаването на 6 профила включващи пълна мрежова конфигурация, възможност за ръчна промяна на местоположението в мрежата.
* **SMAC** – платена версия, но има и безплатна, която служи за смяна на MAC адреса, за Windows 2000/XP/Vista
* **Други**

Мерки, които можем да предприемем, за да се защитим от такъв вид атака.

* Да се наложи ограничение на физическия достъп до мрежата.
* Да се използва криптиране.
* Да се използва статичен IP адрес и статична ARP таблица.
* Само оторизирани потребители да могат да работят с мрежата.
* Да се използва IPv6 вместо IPv4
* Да се използват криптирани сесии, като SSH, SCP и SSL.
* Да се използват PGP и S/MIPE, VPN, IPSec, TLS, OTP.
* Да се използва HTTPS за защита.
* Да не се използват услуги на незащитени мрежи.
* Да се вземат под внимание мрежовото устройство, което ще използва.
* Да се внимава, когато се споделят папки и услуги по мрежата.