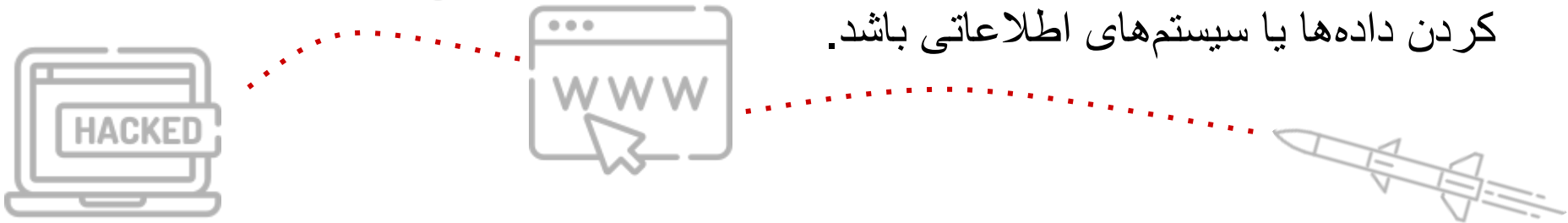
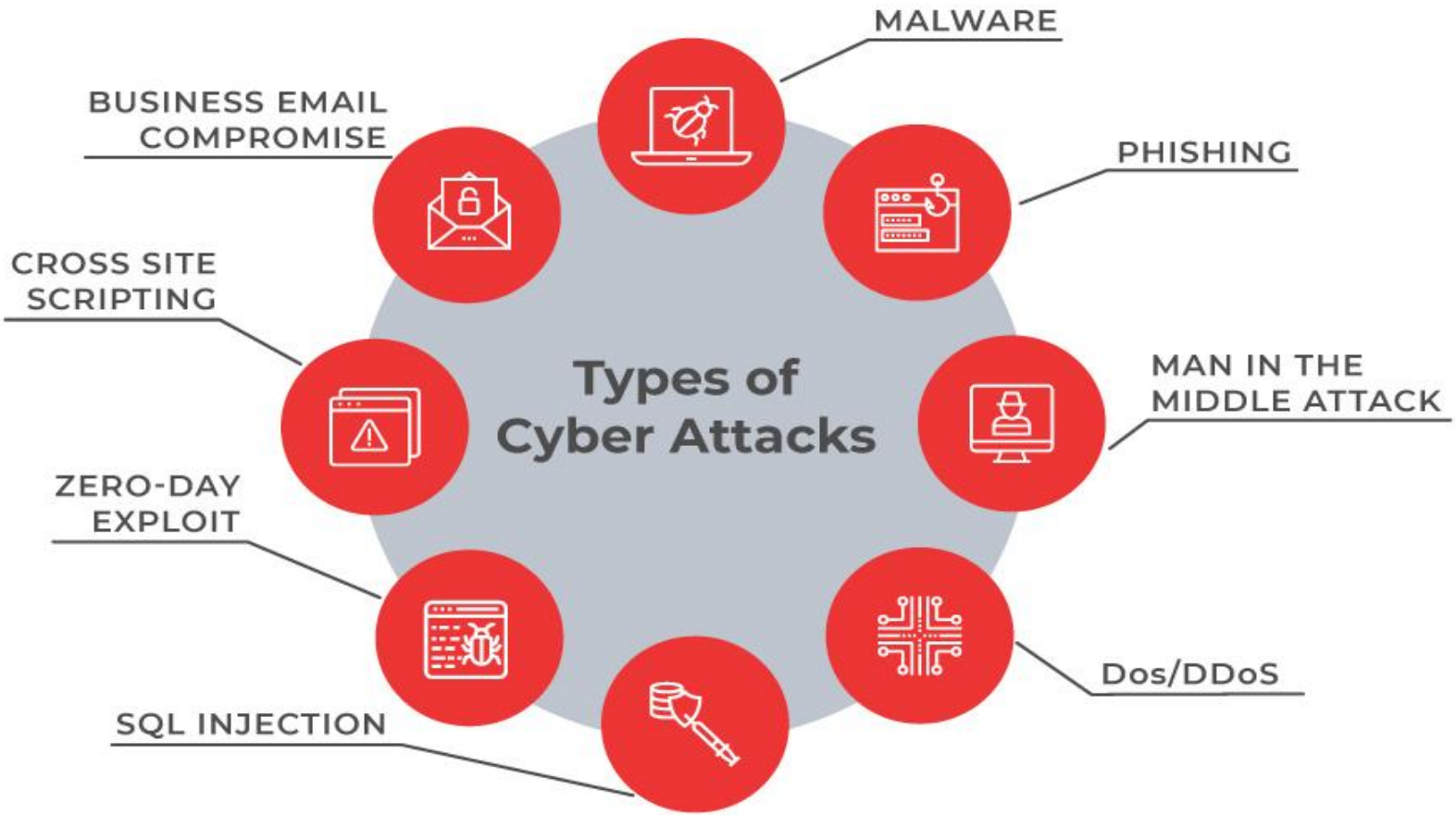
Attacks To Websites

The attacks on your website can take many forms, and the attackers behind them can be amateurs or coordinated professionals.

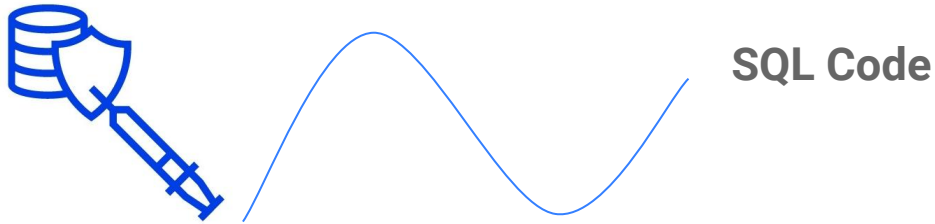
By Group #14

حمله سایبری هر نوع اقدام تهاجمی است، که با استفاده از روش‌های مختلف، سایت‌ها، سیستم‌های اطلاعات کامپیوتری، زیرساخت‌ها، شبکه‌های کامپیوتری یا کامپیوترهای شخصی را هدف قرار می‌دهند. این حملات ممکن است به منظور سرقت، تغییر یا نابود کردن داده‌ها یا سیستم‌های اطلاعاتی باشد.

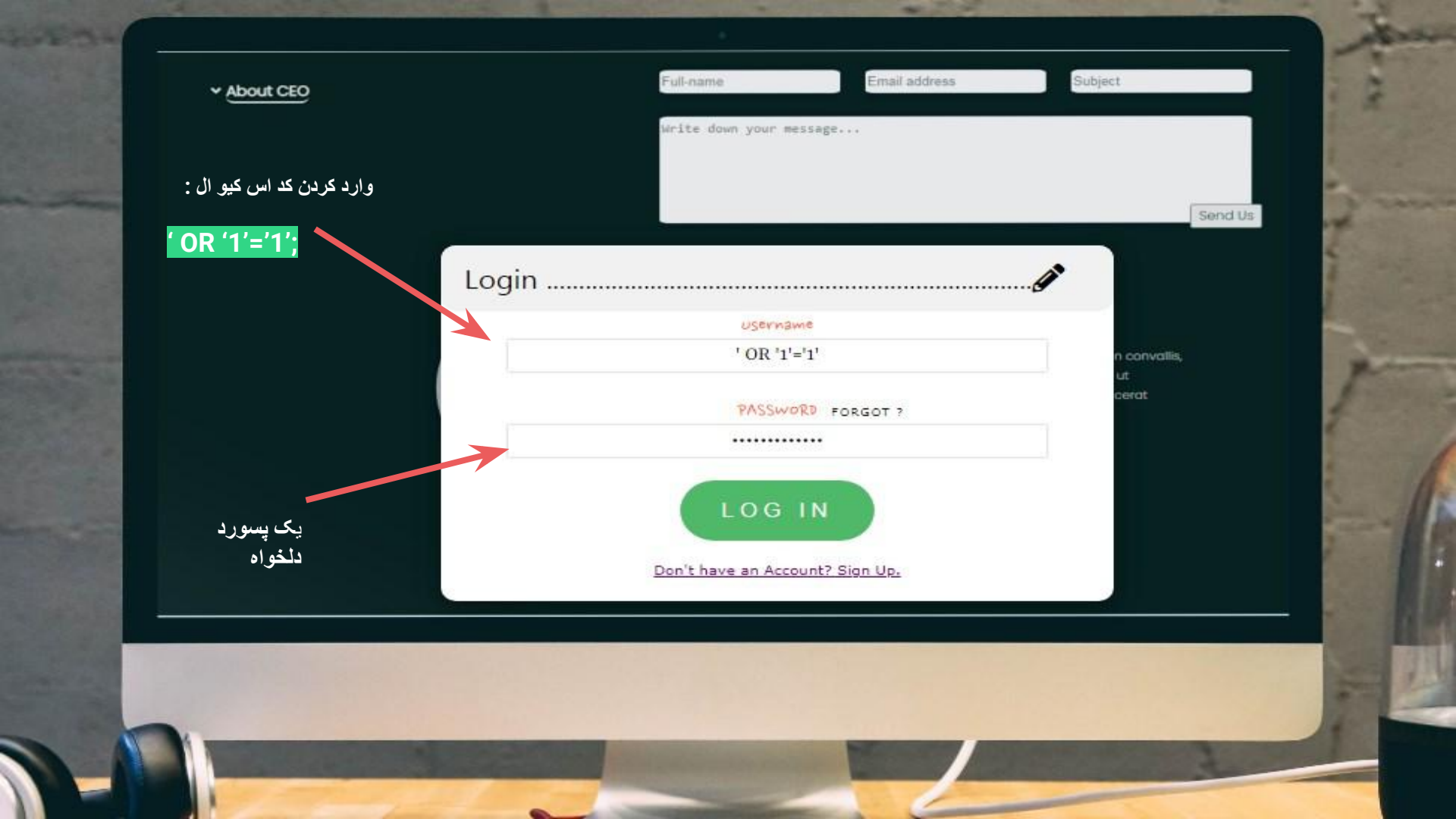



Types of Cyber Attacks
MALWARE
PHISHING
MAN IN THE MIDDLE ATTACK
Dos/DDoS
SQL INJECTION
ZERO-DAY EXPLOIT
CROSS SITE SCRIPTING
BUSINESS EMAIL COMPROMISE

SQL Injection Attacks



تزریق SQL یک حمله‌ی رایج به وب سایت‌های مبتنی بر پایگاه داده است. حتماً می‌دانید وب‌سایت‌های داینامیک، عموماً باید به یک دیتابیس متصل شوند تا بتوانند میان کاربران سایت و سرور ارتباط برقرار کنند (مثلاً بتوانند داده‌هایی را ذخیره کنند). این نوع از انواع حملات سایبری زمانی اتفاق می‌افتد که هکر یک Query SQL (کدی به زبان دیتابیس سایت) را از طریق فیلدهای ورودی، مثل فرم Sign Up یا Login، وارد سایت کند.


About CEO
Full-name
Email address
Subject
Write down your message...
Send Us
وارد کردن کد اس کیو ال :
' OR '1'='1';
Login
username
' OR '1'='1'
PASSWORD
FORGOT ?
LOG IN
Don't have an Account? Sign Up.
یک پسورد
دلخواه

PHP Code Of The Login

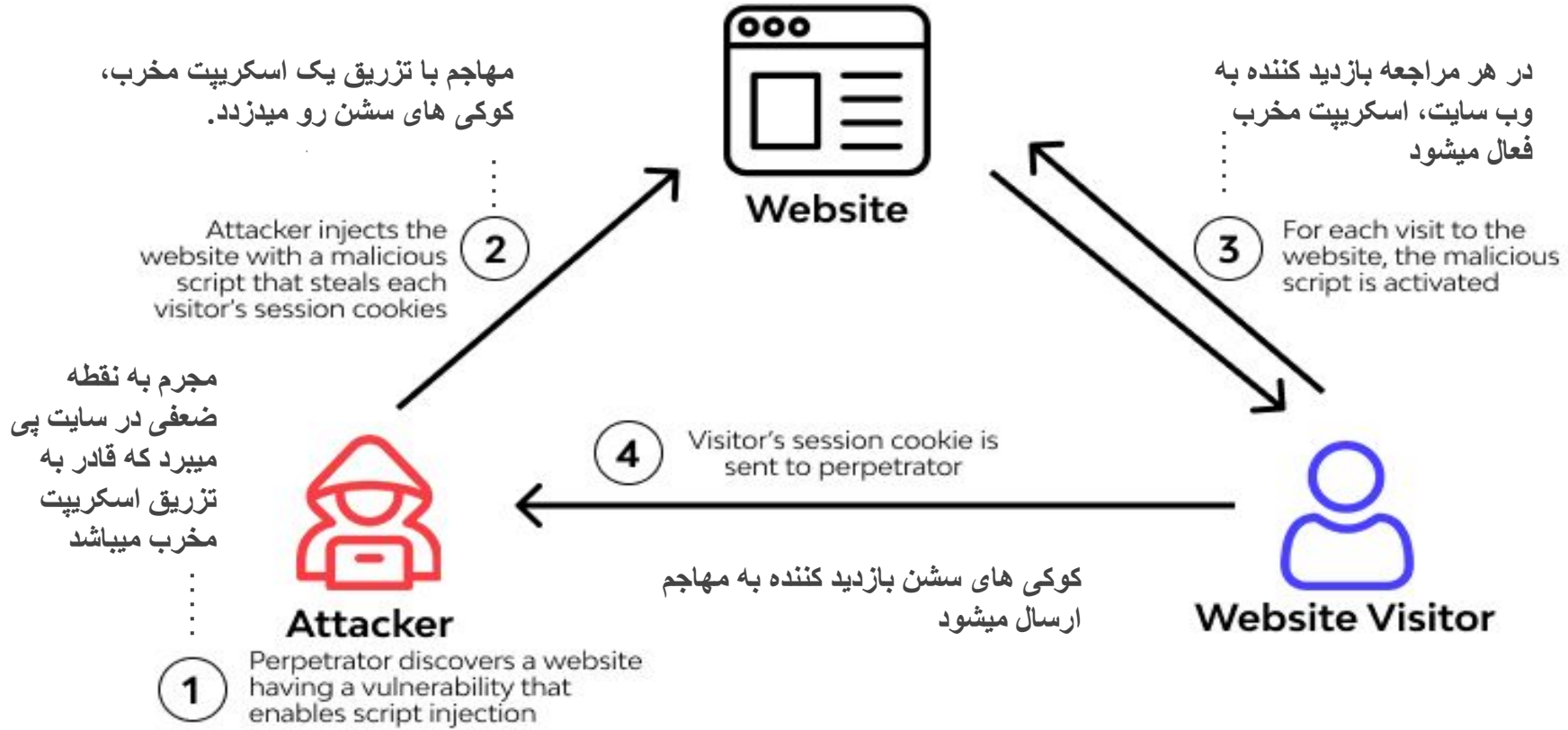
```
<?php

if(isset($_POST['submit'])){

    $username=$_POST['u_name'];   //یوزرنیمی که کاربر وارد کرده است در متغیر یوزرنیم ریخته میشود
    $pass=$_POST['pass'];   //پسوردی که کاربر وارد کرده است در متغیر "پس" ریخته میشود

    include_once 'includes/dbcon.php';

    $sql="SELECT * FROM subscribers WHERE uid= '$username' ;" ;
    $result=mysqli_query($conn, $sq);
```

//$username= ' OR '1'='1'

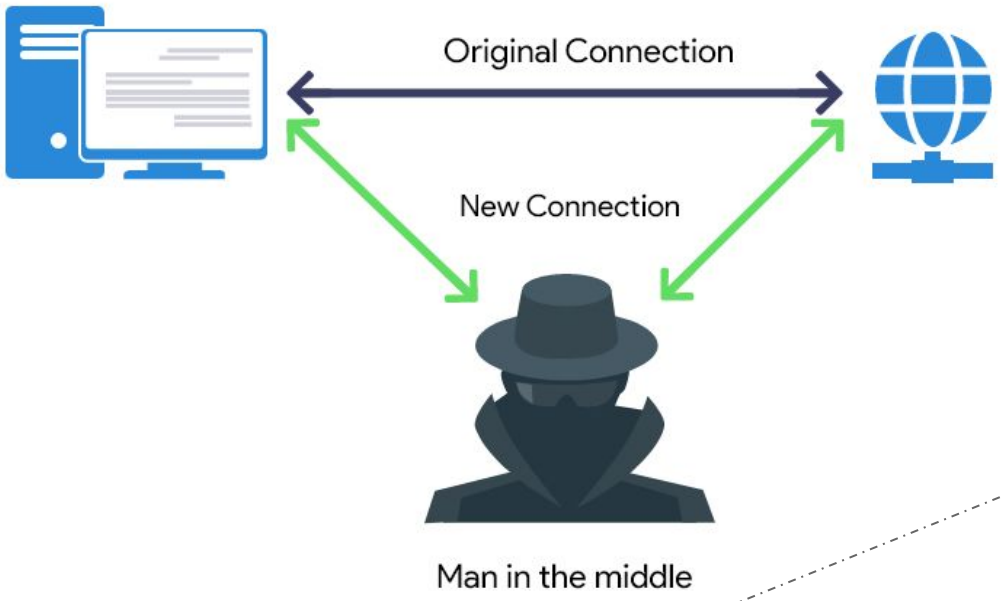
// $sql="SELECT * FROM subscribers WHERE uid=' ' OR '1'='1' ; ";

XSS Attacks

Type : **Stored cross-site scripting**



Man In The Middle Attacks



حملات **Man-in-the-Middle** در میان سایت هایی رایج است که داده های خود را هنگام انتقال از کاربر به سرورها رمزگذاری نکرده اند. به‌عنوان کاربر، می‌توانید با بررسی اینکه آیا **URL** وب سایت با **HTTPS** شروع می‌شود، که در آن «S» به معنای رمزگذاری شدن داده‌ها است، یک خطر بالقوه را شناسایی کنید.

مهاجمان از نوع حمله **Man-in-the-Middle** برای جمع آوری اطلاعات (اغلب حساس) استفاده می کنند. هکر داده ها را هنگام انتقال بین دو طرف رهگیری می کند. اگر داده ها رمزگذاری نشده باشند، مهاجم می تواند به راحتی اطلاعات شخصی، ورود به سیستم یا سایر جزئیات حساس را که بین دو مکان در اینترنت حرکت می کنند، بخواند.

Phishing Attacks

فیشینگ یکی دیگر از روش‌های حمله است که مستقیماً وب‌سایت‌ها را هدف قرار نمی‌دهد، اما ما نمی‌توانیم آن را از فهرست خارج کنیم، زیرا همچنان می‌تواند یکپارچگی سیستم شما را به خطر بیندازد. فیشینگ، طبق گزارش جرایم اینترنتی FBI، از رایج ترین جرایم سایبری مهندسی اجتماعی است.

ابزار استاندارد مورد استفاده در فیشینگ ایمیل است. مهاجمان معمولاً خود را به عنوان فردی که نیستند پنهان می کنند و سعی می کنند قربانیان خود را به اشتراک گذاری اطلاعات حساس یا انتقال بانکی وادار کنند. این نوع حملات شامل آدرس های ایمیل جعلی، وب سایت های به ظاهر معتبر و زبان متقاعد کننده است. حمله فیشینگ هدفمند به عنوان Spear phishing شناخته می شود.

More On Phishing Attacks

یکی دیگر از تکنیک‌هایی که هکرها برای اضافه‌کردن اعتبار به داستان خود استفاده می‌کنند کلونینگِ وب‌سایت است. آنها وب‌سایت‌های قانونی را کپی می‌کنند تا شما را به وارد کردن اطلاعات شخصی یا اطلاعات ورود به سیستم وادار کنند و شما بدون اینکه متوجه باشید هرچه دارید را در اختیار آنها قرار دهید.

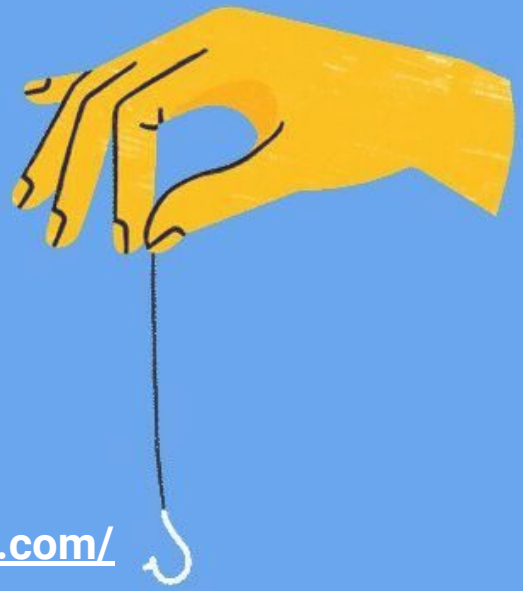
برای مثال، تصور کنید که شما وارد صفحه‌ای به آدرس www.facebok.com شده‌اید. بدون اینکه به چیزی شک کنید اطلاعات ورود به حساب فیسبوک خودتان را وارد می‌کنید و از قضا ممکن است وارد حساب فیسبوک خود هم بشوید. اما در این لحظه هکر به حساب ارزشمند فیسبوک شما دسترسی پیدا کرده بدون اینکه شما روحتان هم خبر داشته باشد. یک بار دیگر نگاه دقیقی به آدرس بیندازید. این آدرس یک آدرس شبیه به آدرس اصلی Facebook است و احتمالا دقیقاً شبیه سایت اصلی طراحی شده، اما خود آن نیست. این نوع هک در ایران بسیار اتفاق افتاده و قربانیان اطلاعات حساب خود را در درگاه‌های پرداختی وارد کرده‌اند که در واقع صفحه‌ی پرداخت اصل و مطمئنی نبوده است و هکر توانسته حساب آنها را خالی کند.

اگر می‌خواهید توانایی خود را در شناخت حمله فیشینگ محک بزنید و هم یک سری نکته‌ی کاربردی در این رابطه یاد بگیرید در این آزمون گوگل شرکت کنید:

Can you spot when you're being phished?

Identifying phishing can be harder than you think. Phishing is an attempt to trick you into giving up your personal information by pretending to be someone you know. Can you tell what's fake?

TAKE THE QUIZ



www.phishingquiz.withgoogle.com/

Fake email for exp. from a website or your boss, ...

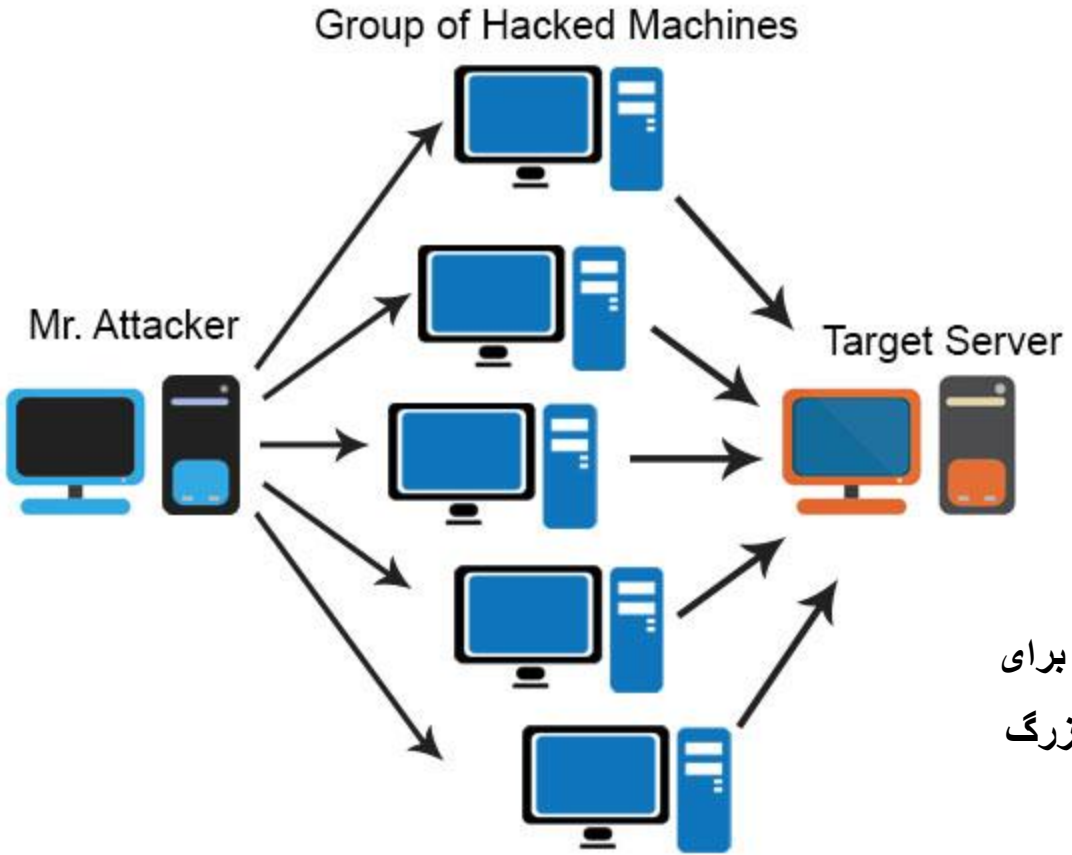
PHISHING Attacks

Denial-of-Service (DoS) Attacks

تصور کنید که هر روز یک عده زیادی وارد رستوران شما شوند، صندلی‌ها را اشغال کنند و بدون اینکه سفارش دهند و پولی به شما پرداخت کنند تمام مدت در رستوران بمانند. اگرچه این افراد هفت‌تیر نمی‌کشند یا گاوصندوق شما را خالی نمی‌کنند اما مانع از ورود مشتریان واقعی به رستوران شما می‌شوند و درنتیجه هیچ درآمدی نخواهید داشت.

در حملات داس و دی‌داس هم IP های غیر واقعی وارد سایت شما می‌شوند، در کل سایت شما چرخ می‌زنند و بدون اینکه فایده‌ای داشته باشند ترافیک سایت را می‌خوردند و مانع ورود افراد واقعی به سایت شما می‌شوند. این کاربرهای غیر واقعی اگرچه به اطلاعات شما دسترسی ندارند اما جای کاربران واقعی را تنگ می‌کنند و اگر کل ظرفیت ترافیکی سایت شما را بگیرند، مانع از این می‌شوند که سایت شما برای کاربران واقعی بالا بیاید.

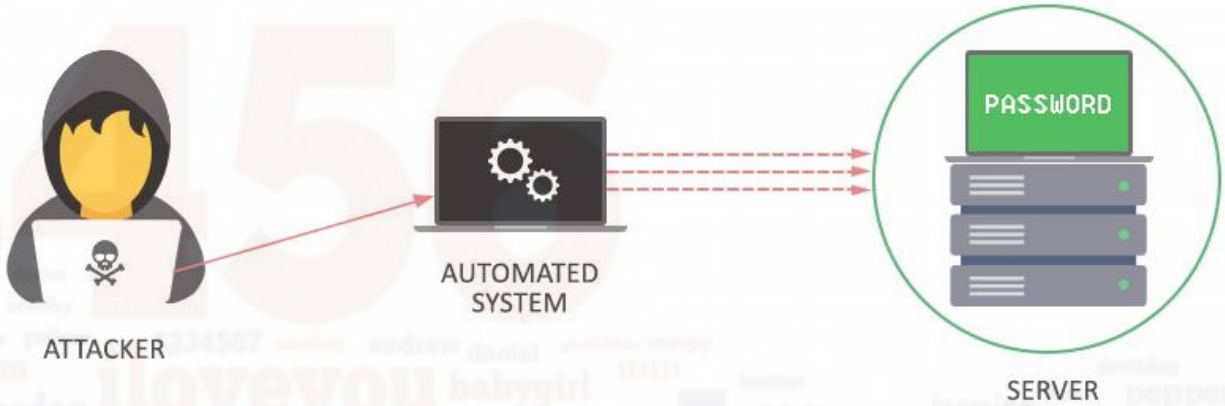
- ***Distributed Denial-of-Service (DDoS)***



حمله‌ی DDoS (distributed DoS)) هم حمله به منابع سیستم است، با این تفاوت که این حمله از تعداد زیادی از سیستم‌ها اتفاق می‌افتد. یعنی مبدا این حملات واحد نیست. معمولا حملات دی‌داس از طریق سیستم‌هایی انجام می‌شود که توسط نرم‌افزارهای مخربِ تحت کنترل مهاجم آلوده شده‌اند.

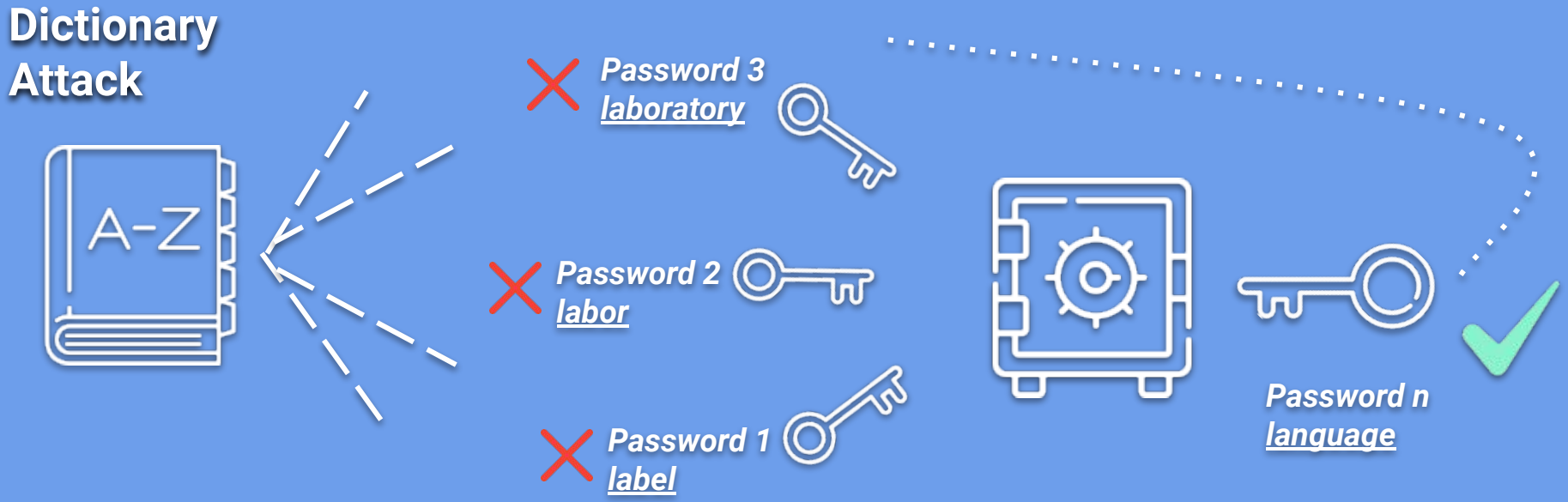
براساس تحقیقات در سال 2017، یک حمله DDoS برای مشاغل کوچک حدودا 123 هزار دلار و شرکت‌های بزرگ به طور متوسط 2.3 میلیون دلار هزینه دارد.

Brute -Force -Attacks

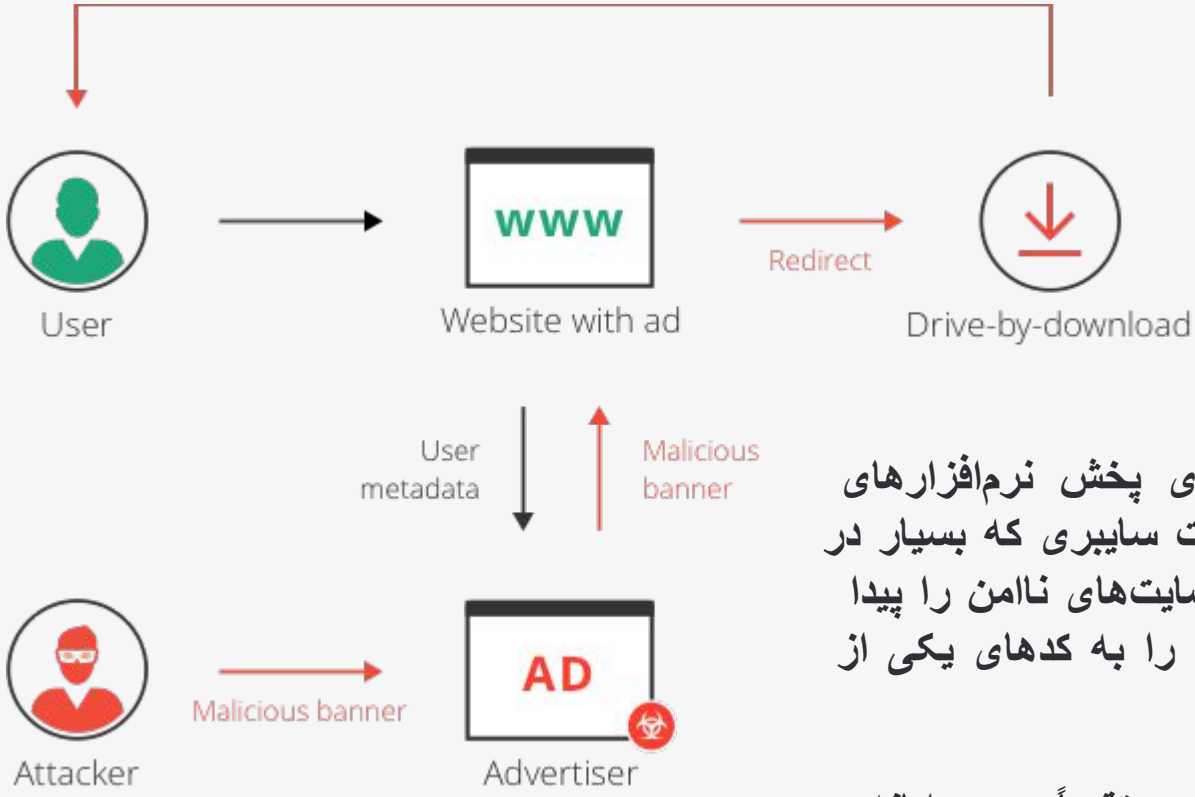


به‌دست آوردن کلمه‌ی عبور یک رویکرد شایع و البته کارآمد هکرها برای حمله است. رمز عبور افراد را می‌توان با جستجوی میز کار افراد، روش‌های هک MitN، استفاده از مهندسی اجتماعی، دسترسی به پایگاه دادهٔ یک سایت یا حدس زدن به دست آورد.

هکر ممکن است خودش یا به وسیله‌ی یک ربات سعی کند با به‌کاربردن یک سری رشته‌کلمات وارد حساب کاربری شما شود؛ مثلا در نظر بگیرید که صفحه‌ی ورود به سایتتان را باز کرده و دائما با توجه به نام، عنوان شغلی، کدملی، شماره تلفن، و ... ، یوزرنیم و پسورد وارد می‌کند و امیدوار است پس از مدتی بالاخره وارد سایت شود. اگر در انتخاب رمزها نکات امنیتی را رعایت نکرده باشید احتمالا این کار چند روز یا حتی چند ساعت بیشتر برای هکر زمان نبرد.



در یک حمله دیکشنری، هکر یک لیست از کلمات کلیدی معمول که اکثر آدم‌ها از آن استفاده می‌کنند، دارد و از آنها برای ورود به حساب استفاده می‌کند. مثلا اگر شما رمز صفحه تنظیمات مودم خود را عوض نکرده‌اید و همان رمز دیفالت است، احتمالاً هکر با یوزرنیم و پسورد admin می‌تواند وارد صفحه تنظیمات شود و وای‌فای خانه‌ی شما را هک کند.



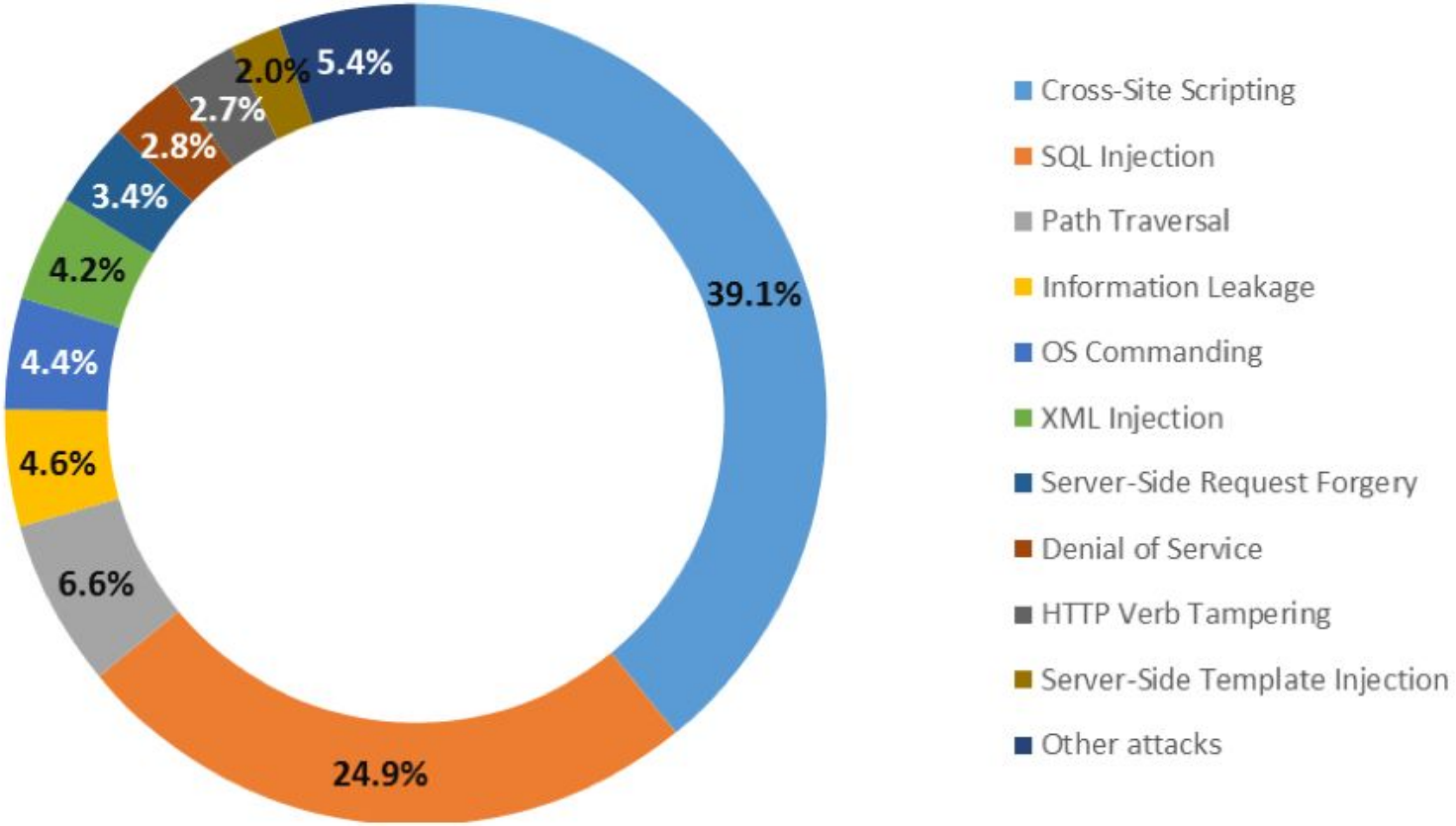
Drive-by Attack

Drive-by یک روش معمول برای پخش نرم‌افزارهای مخرب میباشد (یکی از انواع حملات سایبری که بسیار در سطح وب شایع است). هکرها وب‌سایت‌های ناامن را پیدا می‌کنند و یک اسکریپت (کد) مخرب را به کدهای یکی از صفحات اضافه می‌کنند.

این اسکریپت ممکن است بدافزارها را مستقیماً روی رایانه‌ی کسی که از سایت بازدید می‌کند نصب کند یا ممکن است قربانی را به یک سایت تحت کنترل هکر هدایت کند.

حتماً بارها شده که در هنگام بازدید از یک وب‌سایت به صفحه‌ای دیگر هدایت شوید یا یک پنجره‌ی پاپ‌آپ برای شما باز شود که اصلا به چیزی که دنبال می‌کنید، ارتباط ندارد. ممکن است با کلیک روی آن یا بدون کلیک شما یک چیزی دانلود شود. بر خلاف حمله فیشینگ، حمله Drive-by به فعالیت کاربر و کلیک او یا باز کردن ضمیمه ایمیل وابسته نیست.

Doughnut chart



Hacker: “We are Anonymous”