اسلاید 1

سلام

با ارائه گروه 14 همراه باشید - اعضایه گروه ما : فاطمه آزاد - پویا کفاشی - مهدی حسن بیگی

موضوع ارائه ما حملات به وب سایت ها هستش

حملات به وب سایت ها می تونن شکل های مختلفی داشته باشن و مهاجمای پشت اون ها میتونن آماتور یا متخصصان هماهنگ باشن.

اسلاید 2

اول از همه حمله سایبری چیه ؟

حمله سایبری هر نوع اقدام تهاجمیه که با استفاده از روش‌های مختلف؛ سایت‌ها، سیستم‌های اطلاعات کامپیوتری، زیرساخت‌ها، شبکه‌های کامپیوتری یا کامپیوترهای شخصی رو هدف قرار می‌ده. این حمله ها ممکنه به منظور سرقت، تغییر یا از بین بردنه داده‌ها یا سیستم‌های اطلاعاتی باشه.

اسلاید 3

تو این اسلاید ما نام 8 تا از حمله ها رو میبریم که در ادامه این اسلاید به بررسی هرکدوم میپردازیم.

(دونه دونه شروع به خواندن اونا کن)

اسلاید 4

تزریق SQL یه حمله‌ی رایج به وب سایت‌های مبتنی بر پایگاه داده هستش. حتماً می دونید وب‌سایت‌هایه پویا عموماً باید به یه دیتابیس متصل باشن تا بتونن بین کاربرایه سایت و سرور ارتباط برقرار کنن (مثلاً بتوانن داده‌هایی رو ذخیره کنن). این نوع از حمله های سایبری زمانی اتفاق می‌افته

که هکر یه Query SQL (کدی به زبان دیتابیس سایت) رو از طریق فیلدهای ورودی، مثل فرم Sign Up یا Login، وارد سایت کنه.

اسلاید 5

اینجا ما یه فرم login طراحی کردیم که username و password رو از کاربر میگیره و در صورتی که کاربر معتبر باشه وارد حساب کاربریش میشه.

حالا فرض کنین که یه هکر قصد نفوذ به پایگاه داده ما رو داشته بشه و بیاد به جا username، بخشی از یه کد اس کیو ال مثل چیزی که تو اسلاید هایلایت سبز شده ***' OR '1'='1'*** رو وارد کنه و password رو هرچی که شد و دکمه Login رو هم در آخر بزنه.

اسلاید 6

بعد از زدن دکمه، username و password توسط کد سمت سرور ما درون متغیر هایی ریخته میشن. متغیر اس کیو ال به این باکس پایینه اسلاید تغییر شکل میده که یعنی تمام مشترکانی رو نمایش بده که username شون تهی هست، یا 1 برابر 1 هست، که چون 1 همیشه برابر1 هستش اطلاعات تمام مشترکان رو نشون میده.

اسلاید 7

خب اینجا ما به معرفی stored cross-site scripting که یه نوع حمله ی xss هستش میپردازیم.

این حمله رو به 4 مرحله تقسیم میکنیم.

مرحله اول اینه که مجرم به نقطه ضعفی در سایت پی میبره، که میتونه اسکریپت مخربی رو بهش تزریق کنه.

مرحله بعد یعنی مرحله 2، مهاجم با تزریق یه اسکریپت مخرب، کوکی های سشن رو میدزده.

تو مرحله 3، با مراجعه هر بازدید کننده به وب سایت، اسکریپت مخرب فعال میشه.

و تو مرحله نهایی کوکی های سشن بازدید کننده به مهاجم ارسال میشن.

اسلاید 8

حمله ای که تو این اسلاید معرفی میکنیم حمله ی Man-in-the-Middle هست که در میان سایت هایی رایجه که دادهاشون رو موقع انتقال از کاربر به سرورا رمزگذاری نکردن. به‌عنوان کاربرمیتونید ببینید که آیا URL وب سایت با HTTPS شروع می‌شه و یک خطر بالقوه رو شناسایی کنین («S» در HTTPS به معنای داده هایه رمزگذاری شده هستش).
مهاجم ها از نوع حمله Man-in-the-Middle برای جمع آوری اطلاعات (اغلب حساس) استفاده می کنن. هکر داده ها رو هنگام انتقال بین دو طرف رهگیری می کنه. اگر داده ها رمزگذاری نشده باشن، مهاجم می تونه به راحتی اطلاعات شخصی، ورود به سیستم یا سایر جزئیات حساس رو که بین دو مکان در اینترنت حرکت می کنن رو بخونه.

اسلاید 9

فیشینگ یکی دیگه از روش‌های حمله است که مستقیماً وب‌سایت‌ها را هدف قرار نمی‌ده، اما ما نمی‌تونیم اون رو از فهرست خارج کنیم، چون همچنان می‌تونه یکپارچگی سیستم رو به خطر بندازه.

فیشینگ، طبق گزارش جرایم اینترنتی FBI، از رایج ترین جرایم سایبری مهندسی اجتماعیه.

ابزار استاندارد مورد استفاده در فیشینگ ایمیله. مهاجما معمولاً به عنوان فردی که نیستن پنهان میشن و سعی می کنن قربانی هاشون رو به اشتراک گذاری اطلاعات حساس یا انتقال بانکی وادار کنن. این

نوع حمله ها شامل آدرس های ایمیل جعلی، وب سایت های به ظاهر معتبر و زبان متقاعد کننده هستن.

اسلاید 10

یکی دیگه از تکنیک‌هایی که هکرا برای اضافه‌کردن اعتبار به داستانشون استفاده می‌کنن کلونینگِ وب‌سایت هستش. اونا وب‌سایتایه قانونی رو کپی می‌کنن تا شما رو به وارد کردنه اطلاعات شخصی یا اطلاعات ورود به سیستم وادار کنن و شما بدون اینکه متوجه باشین هرچی دارین رو در اختیار اونا قرار میدین.

برای مثال، فرض کنین که شما قصد ورود به اکانت فیسبوکتون رو دارین و به آدرس www.facebok.com رفتین.

بدون اینکه به چیزی شک کنین اطلاعات ورود به حساب فیسبوک خودتون رو وارد می‌کنین و احتمالا، ممکنه وارد حساب فیسبوک خودتون هم بشین اما الان دیگه هکر به حساب فیسبوکتون دسترسی پیدا کرده، بدون اینکه روحتون هم خبر داشته باشد. یک بار دیگه آدرس وب سایتی که رفتیم رو نگاه کنین. این آدرس، یه آدرس شبیه به آدرس اصلیه فیسبوکه و احتمالا دقیقاً شبیه سایت اصلی فیسبوک طراحی شده، اما خود اون نیست، همونطور که میبینین یه o کم داره. این نوع هک در ایران بسیار اتفاق افتاده و قربانی ها اطلاعات حساب خودشون رو تو درگاه‌های پرداختی ای وارد کردن که در واقع صفحه ی پرداخت اصل نبوده و هکر تونسته حسابشون رو خالی کنه.

اسلاید 11

خب حالا اگر کسی می‌خواد تواناییه خودشو تو شناخت حمله های فیشینگ محک بزنه و یه سری نکته‌ی کاربردی در این رابطه یاد بگیره، با فیلترشکن بره تو این سایت "فیشینگ کوییز" از گوگل که کاملا معتبره .

پیشنهاد میکنم حتما تستشو بدین.

اسلاید 12

اینجا یه طنز از حمله فیشینگ رو میبینین. هکر با خودش میخنده و میگه که یکم ماهی گیری کنم و بعد یه ایمیل تقلبی مثلا از وب سایتی رو به یکی میزنه و منتظر میشه طرف یوزرنیم پسوردشو وارد کنه و صیدش کنه.

اسلاید 13

خب میرسیم به حمله ی Denial of Service یا همون DoS

تصور کنین هر روز یک عده زیادی وارد رستوران شما میشن، صندلیا رو اشغال میکنن و بدون اینکه سفارش بدن و پولی به شما پرداخت کنن تمام مدت تو رستوران بمونن. این افراد هفت‌تیر نمی‌کشن یا گاوصندوق شما رو خالی نمی‌کنن اما مانع از ورود مشتریایه واقعی به رستوران شما می‌شون و باعث میشن که هیچ درآمدی نداشته باشین .

تو حمله های داس و دی‌داس، **IP** هایه غیر واقعی وارد سایت می‌شن، تو کل سایت چرخ می‌زنند و بدون اینکه فایده‌ای داشته باشن ترافیک سایت رو می‌خورن و مانع ورود افراد واقعی به سایت می‌شن. با اینکه این کاربرای غیر واقعی به اطلاعات شما دسترسی ندارن اما جایه کاربرای واقعی رو تنگ می‌کنن و اگر کل ظرفیت ترافیکی سایت رو بگیرن، مانع از این می‌شن که سایت برای کاربران واقعی بالا بیادش.

اسلاید 14

حمله‌ی دی‌داس هم حمله به منابع سیستمه، با این تفاوت که این حمله از تعداد زیادی از سیستما صورت میگیره. یعنی مبدا این حملات واحد نیست. معمولا حمله های دی‌داس از طریق سیستم‌هایی انجام می‌شه که توسط نرم‌افزارهایه مخربِه تحت کنترل مهاجم آلوده شدن.

بد نیست بدونین که براساس تحقیقات انجام شده تو سال 2017، یه حمله ی دی داس برای مشاغل کوچیک حدودا 123 هزار دلار؛ و شرکت‌های بزرگ به طور متوسط 2.3 میلیون دلار هزینه داره.

(به علت کمبود وقت ما اسلایدهای مربوط به حملات BruteForce ، Dictionary و Drive by رو رد میکنیم و اگر شد برمیگردیم).

پرش به توضیحاته اسلاید 19

اسلاید 15

(در صورت کمبود وقت این اسلاید رو رد کن و بگو به علت کمبود وقت ما اسلاید مربوط به BruteForce رو رد میکنیم و اگر شد برمیگردیم).

یه رویکرد رایج هکرها برای حمله؛ پی بردن به کلمه‌ی عبور هستش . رمز عبور آدم ها رو می‌شه با گشتن میز کارشون، روش‌های هک MitN، استفاده از مهندسی اجتماعی، دسترسی به پایگاه دادهٔ یک سایت یا حدس زدن به دست آورد.

هکر ممکنه خودش یا به وسیله‌ی یه ربات سعی کنه با به‌کاربردن یه سری رشته‌کلمات، وارد اکانت طرف بشه؛ مثلا صفحه‌ی ورود به سایت رو باز میکنه و دائما با توجه به نام، عنوان شغلی، کدملی، شماره تلفن، و ... ، یوزرنیم و پسورد رو وارد می‌کنه و امیدواره بعد از مدتی بالاخره وارد اکانت طرف بشه.

اگر تو انتخاب رمزها نکات امنیتی رو رعایت نکرده باشین، احتمالا این کار چند روز یا حتی چند ساعت بیشتر برای هکر زمان نمیبره.

اسلاید 16

(در صورت کمبود وقت این اسلاید رو رد کن و بگو به علت کمبود وقت ما اسلاید مربوط به Dictionary Attack رو رد میکنیم و اگر شد برمیگردیم).

حمله دیکشنری در حقیقت نوعی حمله ی BruteForce هستش و اینطوریه که هکر یک لیست از کلمات کلیدی معمول که اکثر آدم‌ها از اونا استفاده می‌کنن رو داره و از اونها برای ورود به اکانت کاربری(بالفرض شما)، استفاده می‌کنه. مثلا اگر رمز صفحه تنظیمات مودم رو عوض نکردین و همان رمز دیفالت هستش، احتمالاً هکر با یوزرنیم و پسورد admin می‌تونه وارد صفحه تنظیمات

بشه و وای‌فای خونتون رو هک کنه.

اسلاید 17

(در صورت کمبود وقت این اسلاید رو رد کن و بگو به علت کمبود وقت ما این اسلاید و اسلاید بعد که مربوط به حمله Drive by هست رو رد میکنیم و اگر شد برمیگردیم).

Drive-by حمله مرسوم هکرها و یه روش معمول برای پخش نرم‌افزارهای مخرب یا همون Malware هستش. به این صورت که هکرا وب‌سایت‌های ناامن رو پیدا می‌کنن و اسکریپتی (کد) مخرب رو به کدایه یکی از صفحه ها اضافه می‌کنن. این اسکریپت ممکنه بدافزارها رو مستقیماً روی سیستم کسی که از سایت بازدید می‌کنه نصب کنه یا ممکنه قربانی رو به سایتی که تحت کنترل هکر هست هدایت کنه.

حمله Drive by به دانلود ناخواسته کد مخرب در سیستم ما اشاره داره و ما را در معرض حمله سایبری قرار می ده.

اسلاید 18

حتماً بارها برای شماها هم پیش اومده که زمان بازدیده یه وب‌سایت به صفحه‌ای دیگه ای Redirect میشین یا یه پنجره‌ی پاپ‌آپ براتون باز شود که اصلاً به سایتی که هستین، ربط نداره. برای مبتلا شدن لازم نیستش که روی چیزی کلیک کنیم، دانلود کنیم یا پیوست ایمیلی مخرب رو باز کنیم. ممکن است با کلیک یا بدون کلیک ما دانلود صورت بگیره. برخلاف حمله فیشینگ، حمله Drive-by به فعالیت کاربر، کلیکش یا باز کردنه ضمیمه ایمیل متکی نیستش.

اسلاید 19

اینجا میزان استفاده هکرها، از برخی از انواع حملات به وب سایت ها رو به صورت نسبی

روی یک چارت دونات مقایسه کردیم.

این چارت مربوط به حمله های نیمه ی دوم سال 2017 هست.

تو این چارت میبینید که بیشترین نوع از حمله هایه صورت گرفته توسط حمله ی cross site scripting یا همان xss بوده . تقریبا 39% کل حمله های اون زمانو تشکیل میداده .

تقریبا 25% حمله های اون زمانو حمله هایه sql injection تشکیل دادن و مقام دوم رو کسب کردن .

در مورد بقیه حمله ها هم درصد هر کدوم روی چارت مشخص هست و میتونین ببینین.

اسلاید 20

خب ارائه ما به پایان رسید

ممنون از همراهی شما