Authentication

تعريفها

هي عملية بتتأكد من إنك فعلا الشخص الي انت بتدعيه، يعني باختصار لما تكون عايز تدخل على صفحة مارك زوكربيرج ف صفحة اللوجين بتطلب منك الـ credentials الي بتثبت إنك مارك وبتعمل عملية Authenticationيعني تشوف الـ credentials صحيحة ولا لا.

- Authentication is the process of verifying the identity of a given user or client. In other words, it involves making sure that they really are who they claim to be. At least in part, websites are exposed to anyone who is connected to the internet by design. Therefore, robust authentication mechanisms are an integral aspect of effective web security.

أسباب حدوثها

ثغرات الـ Authentication بتحصل نتيجة حاجتين:

- ضعف آلية الـ authentication وعدم حمايتها بالشكل الصحيح ضد هجوم الBrute Force Attack
- نتيجة لـ Logic flows أو عدم كتابة الكود بالشكل الصحيح وبالتالي بيحصل عملية bypass وده بيُسمى بالـ Broken authentication.

مدي تأثير ثغرات الـ Authentication

- يمكن أن يكون تأثير ثغرات المصادقة شديدة للغاية. بمجرد أن يتخطى المهاجم المصادقة أو يفرض طريقه الوحشي إلى حساب مستخدم آخر، يكون لديه حق الوصول إلى جميع البيانات والوظائف الموجودة في الحساب المخترق. إذا كان بإمكانهم اختراق حساب ذي امتيازات عالية، مثل مسؤول النظام، فيمكنهم التحكم الكامل في التطبيق بالكامل واحتمال الوصول إلى البنية التحتية الداخلية.

مناطق حدوثها

ثغرات صفحة الـPassword based-login.

-هنا الموقع بيعتمد على إن اليوزر إما بيسجل حساب جديد بيوزر نيم فريد وباسورد سري محدش يعرفه غيره أو حسابه بياخد عن طريق الادمن وبرضو محدش يعرف الصلاحيات غيره وبالتالي لو الـ Attacker عرف الباسورد هيقدر يدخل على حساب الضحية وده ممكن يحصل بكذا طريقة:

- الـ Brute force Attack لل يوزر نيم أو الباسورد أو الاتنين مع بعض: بتحاول تدخل على صفحة شخص وأنت مش authenticated حتى لو الداتا المهمة مخفية ف ممكن يظهر اليوزر نيم والي غالبا بيكون هو الي بيسجل بيه الدخول، وبص على الـ response أحيانا بيحصل discolse للاميل أو اليوزر نيم.
- الـ Username Enumeration غالبا بتحصل في صفحة الـ login لما بتدخل username صحيح وباسورد غلط ف يقولك الباسورد غلط، أو صفحة إنشاء حساب ف لما بتكتب اميل أو يوزر نيم يقولك ده موجود ف كده بتسهل عملية البروت فورس.

Brute Force

معظم التطبيقات عشان تمنع الـ Attacker من إنه ينفذ هجوم الـ Brute force ويقدر من خلاله يخمن اليوزر نيم أو الباسورد ف بتعمل حاجة من أتنين:

- تقفل الحساب بعد عدة محاولات ولكن لو سجلت الدخول صح بيعيد مرات المحاولة تاني وبالتالي تقدر تتخطاها عن طريق إنك تجرب مرات معينة غلط وبعدين تسجل الدخول وهكذا.
- بيحظر الـ IP الي جاي منه الريكوستس ودي بتتخطاها من خلال الـ X-Forwarded-For وخلافه.

HTTP Basic Authentication

في النوع ده من المصادقة بعد ما تكتب اليوزر نيم والباسورد، بيرد السيرفر بـ Authorization token وبيحطه في الـ Headersوبتكون قيمته عبارة عن username:password و.base64

- مشكلته إن الـ Token بيتبعت مع كل ريكوست داخل التطبيق.
- مشكلة تانية وهو إن النوع ده معندهوش حماية ضد الـ Brute force attack وبالتالي سهل ع المهاجم يخمن توكين يوزر تاني.
- أحيانا النوع ده مش بيوصلك لصفحات مهمة وبتكون حاجات عادية ولكن ممكن فيما بعد يدمجها مع حاجة تاني وهجوم تاني ويقدر ينفذ حاجة كبيرة ويوصل لداتا مهمة.

2FA Authentication

- بعض المواقع بتفضل إن عملية الـ Authentication تكون على خطوتين وده لزيادة الأمان، وأحنا عارفين إن عملية المصادقة نفسها بتقوم على 3 عوامل، ف المشهور إن عملية المصادقة الثنائية بتكون مزيج بين Something you know & Something you haveوف الغالب بيكون الباسورد وكود بيتبعت على الفون.
- لازم الـ 2 FA Authenticationتقوم على عاملين مختلفين مش عامل واحد بطريقتين مختلفتين، زي إنك تبعت رسالة على الميل ده مش 2 FA Authخالص لإن المهاجم لو عرف الباسورد هيعدي الخطوة الأولى وبالتالي ممكن يكون سهل يعرف الخطوة التانية.

الثغرات المحتملة وطرق تخطيها

1-عدم وجود عملية الRate limit

- الـ Rate limit هي آلية بتحدد كام ريكوست أو السرعة الي بتم بيها الريكوستس لـ IP معين أو session معين .

2-وجود الـ Rate limit ولكن يمكن تخطيه

أ- أحيانا بيكون في Silent Rate limit وده مش بيظهرلك فيه errors وبالتالي بتحتاج تقلل عدد الـ Threadلـ 1 وبعدين لـ 1 مع ,delay وده معناه إنه لو هيعملك block عشان بتبعت 2 ريكوست في الثانية ف أنت هتقلل بس ميعملش block لحد ما توصل للنتيجة النهائية.

ب- عدم تغير رمز الـ OTP المرسل لمدة محددة ومش بيتغير لكل ريكوست وبالتالي لو هو متاح لمدة 5 دقائق هيبقى سهل على المهاجم إنه يفضل يخمن الرقم لحد ما يوصله خلال الـ 5 دقائق.

ج- أحيانا بعد ما يعملك Block بيعيد عدد المرات لما تدوس ,resend code ف لو بيسمحلك لكل كود 3 محاولات وكل 30 ثانية بيبعت كود جديد ف تقدر تعمل.Brute Force

ء- ممكن يكون بيعتمد على الـ IP ف بعد عدد مرات محددة بيـ block الـ IP ف جرب تغير الـIP.

-3أحيانا بيكون في بارامتير فيه value خاصة باليوزر وبيـ create ع أساسها الـ OTP ف ممكن تـ createالـ OTP بإنك تغير الـ value لاميل تاني وبيعتله الـ OTP وتاخده وتسجل بيه وبالتالي بتكون عملت bypass للـ OTP بدون ما يبعتلك الـ OTP على رقم الاميل الأساسي.

-4تخطي 2 FAعن طريق خاصية الـ Remember me أو ما شابه، ولازم تحدد الطريقة الي بتحصل بيها عملية التذكر هل بيضيف cookie ولا بيكون جزء من السيشن ولا بيحفظها تبعا للـ IP ولا.local storage

أ- لو بيحفظها في الكوكي والقيمة بتكون متزايدة في سهل التخمين وبالتالي سهل تعمل تخطي للـ 2 FAلاميل تاني عن طريق الـ ,Brute Force لازم تكون قيمة عشوائية وكبيرة عشان يكون صعب تخمينها .

ب- لو بيحفظها تبعا للـ IP ف حاول تغير الـ ,IP وعشان تعرف هي مرتبطة بالـ IP ولا لا بتجرب تسجل الدخول بخاصية Remember meوبعدين تفتح نفس الاكونت من متصفح تاني أو متصفح مخفي وتشوف هيطلب منك الـ 2 FAولا لا، ده بيأثر إن لو حد معاك على نفس النيتورك هيقدر يتخطى الـ 2 FAبسهولة.

-5أحيانا بتكون صفحة المصادقة الثنائية عبارة عن URL With parameters ودي طبعا غير آمنة لإن ممكن توصلها بدون ما تدخل كلمة اليوزر نيم وكلمة السر، ف اتأكد إن صفحة الـ 2 FAمش صفحة منفصلة لوحدها بـ URL منفصل.

6-

-7تجاهل الـ 2 FAتحت ظروف معينة

أ- بعض المواقع بتعمل تسجيل دخول تلقائي بعد ما تعمل reset password وبالتالي لو مفعل 2 FAومطلبهاش منك بعد ما ترجع الباسورد ف كده أنت عملت bypass ليها.

ب- لما تربط حاسبك بموقع من مواقع التواصل الاجتماعي عشان تسهل عملية الدخول وبالتالي لما تيجي تسجل الدخول من حسابات السوشيال أحيانا بيعمل تجاهل للـ 2.FA

ج- في النسخة القديمة من التطبيقات، وهنا هو مش بيطلب الـ 2 FAلإن الإصدار بيكون قديم أو الخاصية مش موجودة أو مش مفعلة، يعني جرب تدخل على صبدومين تابع للدومين الأساسي وبيطلب نفس الـ credentialsعشان تسجل دخول وشوف هيسألك ع 2 FAولا لا.

ء- أحيانا بيعمل تجاهل لل 2 FAلما يكون إصدار التطبيق مختلف عن الموبايل وكده.

-8لما بتلغي الـ 2 FAمش بيطلب معلومات إضافية زي الباسورد أو الـ كود الحالي لل 2 FAوبالتالي بتكون عرضة لل) CSRF لو كان في bypass لل (CSRF Protection ف تقدر تخلي أي يوزر تاني يلغي الـ 2 FAبدون ما يعرف، ف لازم لما يجي يوزر يلغي 2 FAتطلب منه الباسورد أو الكود الحالي.

-9من المستحسن إن بعد تفعيل الـ 2 FAكل السيشن تنتهي زي لما تعمل ,reset password ف لما اليوزر يتم اختراقه ويفعل الـ 2 FAالمفروض تنتهي السيشن عند المهاجم ويطلب منه تسجيل الدخول من الأول.

-10في التطبيقات بيكون الـ 2 FAمُفعل في كذا مكان زي تغيير الاميل والباسورد واسترجاع الباسورد وتسجيل الدخول وبيكون في Rate limit ع كل منهم، ولكن بتختلف ف تلاقي عند تسجيل الدخول في Rate limit صارم ع عكس وأنت جوا الاميل زي تغيير الاميل ف بيكون الـ Rate limit خفيف وتقدر تنفذ عليه.Brute force

-11التلاعب بالـ ,API Version أحيانا بيكون تسجيل الدخول الـ URL بتاعه كده endpoint/api/v4وبعدها بيحولك على صفحة الـ 2 FAبنفس الـ URL ولكن آخره ,fa-check 2ف لو غيرت الـ v4 لـ v3 أحيانا أو في الأغلب بيحولك على ع طول بدون ما يوديك لصفحة الـ 2 fa-check وده لإن الفيرجن القديم لل API مش بينفذ الـ FA.2

-12بعد ما تعدي أول خطوة حاول تروح لل home page أو صفحة داخلية وتشوف هل بيفحص أنت أكملت الخطوتين ولا هيعديك عادي؟

-13أحيانا بعض التطبيقات مش بتتأكد من إن اليوزر الي عمل الـ Step الأولى هو نفس اليوزر الي عمل الـ Step التانية, في الغالب في الخطوة التانية بتستخدم الكوكي عشان تشوف اليوزر عايز ي accessاميل ايه بالظبط ومش بتتأكد إن الاميل الي عايز ت access عليه هو نفس الاميل الي دخلت الـ credentials في الأول, هي بتستخدم الكوكي عشان تشوف أنت عايز تدخل لاميل مين وبتقارنه بالـ codeالي اتبعت للاميل ده ف لو تطابق الـ username مع الـ code بتقدر تدخل على أميل الضحية.

14-أحيانا بعض التطبيقات بتحاول تمنع الـ Brute force لـ 2 FAعن طريق إنها بتسجل خروج المستخدم بعد عدد مرات محدد من المحاولات الفاشلة وترجعه للخطوة الأولى وهنا بنستخدم الـ Featureالي اسمه Macro في البرب سويت وعدد الـ Threads يكون 1.

Other Functionality

1- Keep me logging أو Remember Me

- الخاصية دي منتشرة في معظم التطبيقات عشان تسهل عملية تسجيل الدخول بدون ما تكتب الـ Credentials كل مرة، الخاصية عبارة عن كوكي بيـ createها السيرفر وبيحفظها في المتصفح كل ما تيجي تدخل ع الموقع بيبعت الكوكي دي وبالتالي بيحصلك لوجين ع طول.
- الكوكي أو الـ Token بيكون عبارة عن الـ credentials او اليوزر نيم والـ timestamp وهكذا ف لو المهاجم قدر يحلل التوكين ويوصل لـ هو مركب من ايه ف يقدر بعدين يخمن التوكين بتاع اليوزرز التانيين ويسجل دخول بدون ما يعرف الـ .Credentials

سيناريوهات

- إن الـ auth_token مش بينتهي بعد ما اليوزر بيعمل .logout
- الـ auth_token مش بينتهي بعد عملية تغيير الباسورد أو الـ .reset Password
- التطبيق بينشأ الـ auth_token لوحده بدون ما اليوزر يعمل .Remember me
- الـ auth_token بيكون ثابت والتطبيق مش بيعمل regenerate ليه.

2- Resetting User Password

سيناريوهات

- إرسال كلمة المرور الجديدة عن طريق الأميل, ودي خطيرة جداً لو الموقع بيعتمد على الـ Password لتسجيل الدخول، الأميل مش مكان لحفظ أمور حساسة زي الباسورد وتفاصيل الكريديت كارد وهكذا.
- إرسال URL عن طريق الأميل ولكن في باراميتر (سواء في الـ URL أو Request's body) بيوضح عملية إسترجاع الباسورد هتم لانهو يوزر بالظبط وبالتالي تغيير اليوزر بتاع الباراميتر ده بيمكن المهاجم يسترجع الباسورد لاي يوزر، المفروض والآمن إن التوكين الخاص بعملية إسترجاع الباسورد لازم يكون طويل وعشوائي وميظهرش أي معلومات عن مين الشخص الي هيرجع الباسورد وهنا السيرفر بيقارن بين التوكين الي هو عمله createوبين الي موجود في الـ URL وبيعرف مين اليوزر الي هيرجع الباسورد.

- المفروض بعد ما اليوزر يرجع الباسورد الـ URL ينتهي وميبقاش صالح للإستخدام مرة تاني ولو مستخدمهوش لازم ينتهي بعد مدة.

- ممكن التوكين يظهر في الـ Response لما تعمل reset password وبالتالي لو كتبت أي اميل وعملتله reset passwordهتقدر تشوف التوكين في الـ response وتغير الباسورد لاي يوزر.
- الـ HOST Header Injection في الـ.Reset Password
- أحيانا لما اليوزر بيعمل reset password وبعدين يعمل Log in) أو هو (login التطبيق مش بيعمل validateعلى الـ Reset password URL وإن التوكين لازم يكون ,valid يعني الـ URLالمفروض يكون

https://example.com/endpoint/reset_password/<token

ولكن بيبقى https://example.com/enpoint/reset_password/

وبالتالي هو مش بيتأكد إن في توكين طالما,token ده بيخليك تغيير الباسورد الحالي، ف لو التطبيق مفعل الـ current passwordداخل التطبيق ف تقدر تعملها.bypass

- لو التطبيق بيرجع الباسورد وبيبعت الـ URL للاميل عن طريق json data حاول تضيف أميل تاني وتشوف لو التطبيق هيبعت اللينك للاميلين وبالتالي تقدر ترجع باسورد الأميل الأول.
- إمكانية تغيير الباسورد عن طريق reset password link حتى بعد تغيير الاميل.
- الـ Reset password URL بيشتغل بدون الـ token حتى وأنت مش.Login
- مفيش rate limit في ريكوست تغيير الباسورد
- أعمل disable أو delete للأكونت وبعدين جربت ترجع الباسورد وتشوف هتقدر تـ access الاميل ولا لا.
- لما بتعمل reset password وتيجي تكتب الباسورد الجديد، لو الـ token صحيح بيغير الباسورد، لو مش صحيح بيقولك الـ token not valid ف جربت تعمل brute force على التوكين.
- مفيش نوتوفوكيشن بتوصل لليوزر لما بيحصل تغيير للباسورد.

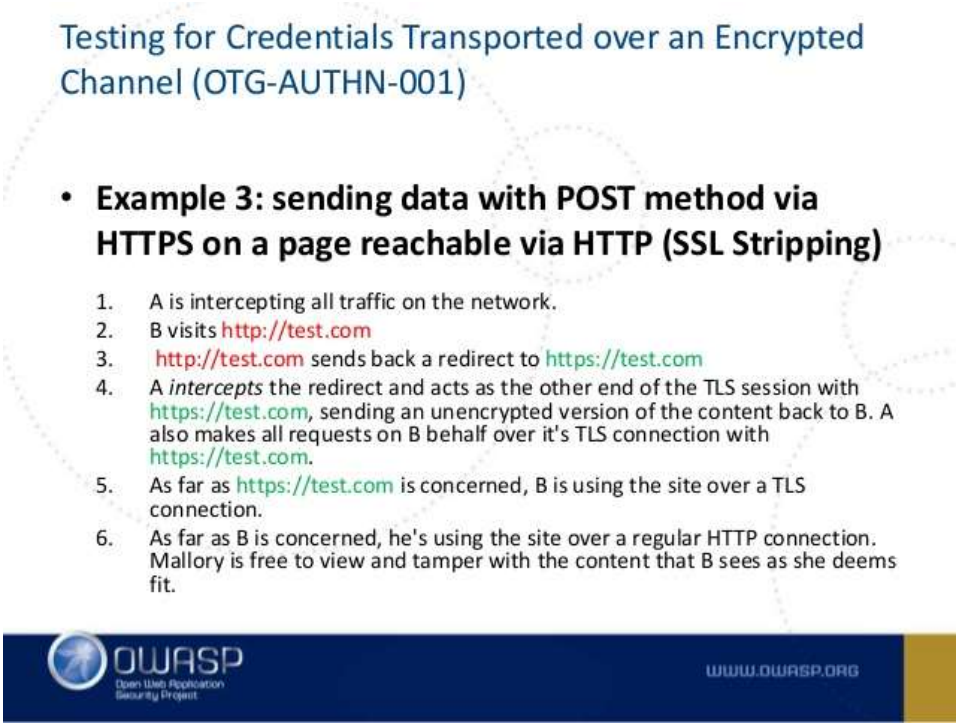
3- Changging User Password

سيناريوهات

- في الغالب لما بتيجي تغير الباسورد بيكون في hidden input فيه اليوزر نيم أو الاميل والي من خلاله بيغير الباسورد لليوزر ده، ف لو تم تغيير اليوزر فـ أنت كده هتغير الباسورد لليوزر ده، ولكن هنا هو بيطلب الـ currentباسورد => وده بنقدر نعرفه من خلال عملية الـ Error message based-Brute force يعني هتعمل بروت فورس وتعرف الباسورد الصح لما يظهرلك إن الباسورد الجديد غير متطابق.
- أحيانا في صفحة تغيير الباسورد لو كتبت باسورد غلط في الباسورد الحالي بيعدي الريكوست, ولو ظهر 401 status code = 400ف خليه 200 وابعت الريكوست.
- مش بيحتاج منك تدخل الConfiramtion new password
- بيمسح إن الباسورد الجديد يكون نفس القديم عادي.
- أحيانا لما بيكون في current password, new password fields وتكتب الـ current غلط والـ 2 new صح بيعملك logout لإنه بيفتكر إنك مش صاحب الأميل، لكن لو كتبت الـ current غلط والـ 2 new مختلفين بيقولك إن الـ current غلط، ف هنا تقدر تعمل brute-force لو مفيش rate-limit.

4-سيناريوهات:

- **1**-بتتأكد من إن الـ credentials بتتبعت من خلال secure channel يعني----:HTTPS
- × يعني ميكونش الريكوست POST والرابط بيبدأ بـ HTTP
- × أو يكون POST وبيبدأ بـ HTTPS بس الـ Referer Header بيبدأ بالـ ,HTTP ده معناه إن الصفحة على الرغم انها بتبعت الداتا مشفرة ولكن نقدر نوصلها بـ.HTTP



- أو تكون الـ credentials أصلا مبعوتة بميثود GET

- **2**-بتتأكد من الـ Default credentials في صفحات:---
  - (login , logout , reset/forgot password , sign-up)
  - يعني وانت بتعمل test على موقع المفروض بتحدد الـ administrative interface وبعدين بتجرب الـ deafult credentialsوهكذا. (لإن موقع الويب لما بيعمل install لـ services / softwares معينة في البداية بيكون في credentials بدائية عشان يقدر يـ access السيرفس دي واحيانا مش بتتغير)
  - ***UserNames***: admin – administrator – root – system – guest – operator – super
  - ***Passwords***: password – pass123 – password123 – admin – guest
  - ممكن كمان تجرب اسم الشركة ف اليوزر نيم والباسورد , او تجرب كل اليوزر نيم بدون باسورد
  - ابحث عن credentials في السورس كود سواء الجافا سكريبت او الكومنتس أو الـbackups
  - لو منفعش الي فوق استخدم payloads واعمل bruteforce لليوزر نيم وبعدين الباسورد.

- **3**-بتتأكد من آلية الـ brute force , إنه بيحظرك بعد عدة مرات معينة ومش بيسيبك تجرب براحتك
- العدد المعروف هو 3-5 مرات وبعدها بيحظرك
- التيست ده بيتعمل مع كل عمليات الـ authentication, بتجرب تسجل الدخول اكتر من 5 مرات بباسورد غلط وتشوف هيوقف الاميل ولا لا, وبعدين 10 مرات وهكذا.

- **4**-بتتأكد من آلية عمل الـ Authentication وإنها مش بتسمحلك غير وانت authenticated
  - الـ bypass ببساطة هو تجاوز صفحة اللوجين وتدخل ع صفحة لازم تكون authenticated عشان تشوفها.
  - تحصل نتيجة لـ (تنادي صفحة داخلية مباشرة - أو تغير البارامتر - أو تخمن الـ(session ID
  - مناداة صفحة داخلية: احيانا بيعمل check لصفحة الـ Login بس ف جرب تدخل صفحة داخلية ع طول.

- تغيير البارامیتر: احيانا بيبقى في بارامیتر بيدل على المصادقة من عدمها زي authenticated=no/0 ف ممكن تغيره وتخليه yes او 1 وتدخل بـ wrong credentials.
- تخمين الـ session ID بإنك تشوف هو بيتعمله generate تبعا لايه, ولو مشفر او decoded فكه.

- **5-**بتتأكد من آلية الـ Remember password /me وتشوف لو بيحفظ الباسورد في الكوكي اتأكد إنه يكون encryptedومش plain text, وتشوف لو الهاش سهل الكسر او الـ ecrypted سهل إنك تفكه, واتأكد إن الـ credentialsالي في الكوكي بتتبعت بس لما تعمل Login مش مع كل ريكوست تعمله

- **6-**بتتأكد من إن الـ browser مش بيخزن معلومات حساسة سواء عن طريق الـ History أو Cache
  - A-زرار الـ Back عبارة عن History, ببساطة بتجرب تدخل على sensitive page/ information)تجرب كلهم) وبعدين تعمل Logout, بعدين بقى تدوس زرار back تشوف هل هتقدر تـ access او حتى تشوف الـ sensitive page دي ولا لا. (أو ممكن تجرب تدوس زرار sign-in بعد ما تعمل تسجيل خروج(
  - لو دوست زرار Back وقدرت تشوف الصفحة الي كنت فيها بدون ما تقدر تـ access صفحات جديدة, ده مش معناه إن الثغرة أو العيب في الـ authentication ولكن ده عيب أو مشكلة تخزين المتصفح وأن التطبيق لم يمنع المتصفح من تخزين بيانات حساسة (الـ default إن التطبيق يمنع المتصفح.(
  - B-تاني حاجة وهي الـ Cache وإن الـ Browser cache مش بيخزن معلومات حساسة, وهنا بتجرب مع كل الصفحات الحساسة وبتشوف الـ response لكل صفحة منهم.
  - وهنا بتتأكد من 3 Response Header وهما
  - Cache-control: no cahce-no store || Expires:0 || Pragma: no-cache

- **7-**هنا بتتأكد من آلية الباسورد وهل ينفع استخدم واحد قديم, وكام مرة اقدر اغير الباسورد ورا بعض.

- **8-**بتتأكد من آلية الـ reset / change password وتشوف إذا كان اليوزر يقدر يغير او يرجع باسورد يوزر تاني - أو تكون واحدة من العمليتين مصابة بثغرة.CSRF
- A-آلية : reset password هنا بتسأل 4 أسئلة (ايه المطلوب عشان ارجع الباسورد , ازاي الـ reset passwordبتتكلم مع اليوزر , هل استرجاع الباسورد بتتكون عشوائي , هل العملية دي بتتطلب تأكيد قبل ما تغير الباسورد (
- B-آلية : Change password وهنا بتسأل نفس الأسئلة الي فوق + هل بيطلب الباسورد القديم ولا لا لإنه لو مش بيطلبه والـ attacker قدر يوصل لاميل الضحية عن طريق سرقة السيشن ف هيقدر يغير الباسورد بسهولة.

- **9-**هنا لو كل عمليات الـ authentication مفهاش ثغرات بتبدأ تشوف الـ Alternative process يعني تشوف نفس العمليات بس لموبايل تاني او جهاز تاني, وهكذا , وتبدأ تفهم كل العمليات زي (إنشاء أميل, تغيير باسورد , استرجاع اميل وكل ده) وبعدين تبدأ تقارن بين الـ standard website وبين باقي الـ Alternative channels.

- **10-**أحيانا لما تعمل forgot password / reset password بيبعتلك لينك على الميل, حاول تنسخ اللينك ده وتحط في ملف txt وتشوف هل الـ HTTPS هتتغير لـ HTTP ولا هتفضل زي ما هي, لو اتغيرت هتشغل البروكسي وتعمل intercept للريكوست وتشوف بقى لو كان في توكينز او حاجة بتظهر.

-سيناريوهات:

Borken Authorization

-1سيناريوهات:

- **1-**أول شيء بتيست عليه هو الـ Directory traversal/file include وهتمشي على ملف Path traversal.

- **2-**بتتأكد من آلية عمل الـ Authorization schema وهل بيتم تطبيقها صح ولا لا, هل بتحفظ الصلاحيات (يعني محدش يقدر يعمل دور حد تاني أو يـ access مصادر حد غير مصادره.)
  - ❖ هنا بقى المفروض مع كل function التطبيق بينفذها زي (login-logout-reset passwd-change passwd-change e-mailوهكذا) وكل role زي (admin – user – root – Moderator) وبتسأل الأسئلة دي:
  - × هل ممكن اليوزر يـ access الصفحة دي وهو مشauthenticated ؟
  - × هل ممكن يـ access الصفحة بعد ما يعملLogout ؟
  - × هل ممكن تـ access الصفحة أو تعمل action معين وانت مش ليك نفس الـ role بدون تدخل منك (يعني بدون ما تبدل سيشن يوزر بيوزر تاني وكده)

- **3-**دي مرحلة الـ Privilege Escalation وهنا بتتأكد من إن التطبيق مش بيسمح لليوزر إنه يعدل الصلاحيات بتاعته لصلاحيات حد تاني, وإنه يقوم بدور غيره كآدمن مثلا أو يـ access resources مش بتاعته ولكن هنا بتدخل منك عادي (يعني تقدر تغير السيشن بيوزر تاني.)
- إزاي نتيست المرحلة دي؟ :---
  - × بتبدأ إنك تشوف كل حاجة في التطبيق بتندرج تحت إنك تـ create Information زي (تبعت رسالة, تشتري حاجة,تضيف يوزر,تدعي يوزر للعبة,تضيف يوزر كآدمن,....إلخ) أو إنك تـ delete Information زي (تمسح رسالة,تطرد عضو,تشيل عضو من الادمنز,...إلخ) وبعدين تحاول إنك تعمل الحاجات دي كأنك يوزر تاني.

❖ لما توصل للمرحلة دي هتبدأ تعمل تيست لثغرات الـ Access control في ملف الـ Access control

- **4-**هنا بقى هنتيست على ثغرة--: IDOR

تعريفها دي اختصار لـ Insecure Direct Object Refrences, ودي نوع من انواع ثغرات الـ Broken Access Controlوهي شبيهة او مرتبطة أكتر مع الـ Horizontal access control يعني بـ Access resources.

أسباب حدوثها

- بتحصل نتيجة ان التطبيق بيستدعي او بيشاور على اوبجيكت resources – user's file database) for websiteديركت.)
- دي بقى بتحصل لما يكون عندي بارامتر انا مقدرش العب فيه-ده المفروض- ولو انا غيرته بيؤدي لثغرة IDORزي مثلا URL بالشكل ده https://www.example.com/change_email?id=153 هنا البارامتر id بيدل عليا انا كيوزر ولو غيرته احتمال اغير اميل حد تاني.
- بالبلدي لما يكون عندي بارامتر فيه قيمة بتشاور على resource او معلومات خاصة بيا واغير البارامتر لقيمة تاني ف يديني resource خاصة بيوزر تاني او معلومات عنه.

أنواعها

- Blind = دي الي بتقدر تغير فيها داتا يوزر تاني بدون ما تشوف الريسبونس بتاعة السيرفر.
- Genetic = ودي الي بتشوف فيها الريسبونس بتاع السيرفر عادي, زي إنك بـ access data لشخص تاني وتشوفها أو بـ access ملف.
- IDOR with Reference to Objects = ودي الي بتقدر تعدل أو بـ access داتا يوزر تاني عن طريق الـ reference (ID)
-

تيتست ازاي

- محتاج تلاقي كل البارامترز والأماكن الي بتشير او بتستدعي.Objects directrly
- بعض الأماكن(البارامتر الي بيستدعي صف من الداتا بيس - أو صفحات - أو ملفات(
- ****وانت بتيست وبتغير قيمة بارامتر لقيمة تاني عشان تشوف هل بتقدر بـ access resources تاني او لا ركز ف انها متكونش دي عملية Business logic وإن ده الطبيعي بتاع التطبيق****

-

مناطق حدوثها

- في تغيير الاميل والباسورد واي داتا مهمة
- في حذف صورة معينة أو جروب أو صفحة أو كومنت في حذف أي حاجة لو لقيتها بتتحذف تبعا لـ ID أو UUID (حتى لو (base64 في جرب تحط ID لصورة تاني (يُفضل لو معاك اميلين كل اميل فيه صورة.)
- لو ممنوع تكومنت أو تنزل صورة وهكذا, جرب تكتب كومنت في كومنت بوست تاني وبعدين تغير الـ ID للبوست الي ممنوع تكومنت عليه وتشوف هيظهر الكومنت ولا ولا وهكذا الصور.
- المعظم بيكون إن أنت ممنوع تعمل action في مكان معين (A) في بتروح تعمل الـ action في مكان تاني (B)وتغير بعدين الـ ID بتاع الـ action الي في (B) تخليه يروح لـ.(A)
- أي action بتعمله بيعرضلك حاجات خاصة بيك جرب معاه الـ.IDOR
- لما يحصل وقف للاميل جرب ترجع الباسورد ووقتها هيقولك إن أميلك موقوف, ف جرب تعمل ريكوست بأميل مش موقوف وتبدل الي في الريكوست من A -> B زي password reset token أو غيره وتشوف هتقدر ترجع الأكونت ولا لا.
-

طرق التخطي

1-تغيير الـ GET إلى.POST

2-عن طريق الـ Parameter pollutoin بإنك تكتب البارامتر مرتين مرة فيه الـ ID العادي ومرة فيه الـ ID الـ victim.

3-عن طريق wrapping in Array مثال

* Wrap ID with an array {“id”:111} --> {“id”:[111]} *

* JSON wrap {“id”:111} --> {“id”:{“id”:111}} *

Send wildcard {"user_id":"*"}

4-عن طريق الـ path traversal مثال www.example.com/edit?id=11../12

5-

Session management

- الـ session وُجدت بسبب إن بروتوكول HTPP عنده عيب وهو إنه مش بيعرف إن الكام ريكوست دول من نفس اليوزر لا هو بيتعامل مع كل ريكوست لوحده ولذلك بقى في session عشان تحفظ إن كل ده جاي من نفس اليوزر.
- السيرفر هو الي بيـ create سيشن عنده ويبعت الـ SEssion ID لمتصفح اليوزر ويتأكد إنه في كل ريكوست هيبعت الـ Session IDده عشان يعرفه إنه تبع السيشن الفلانية.
- الـ Session ID مش بس عشان تحفظ الريكوستس لا وكمان بيستخدم كـ باسورد مؤقت عشان تـ access السيشن يعني لو فتحت التطبيق من متصفح تاني هيطلب منك تسجل الدخول ولكن لو دخلت الـ Session ID هيدخلك ع طول.

- ونظراً لأهمية الـ Session والي بتعمل ف بقت هدف للـ attackers لإن الحصول عليها بيوصلك لأميل الضحية ع طول وبالتالي بقى في secuirty للسيشن والتركيز كله على إن الـ attacker ميقدرش يحصل على سيشن يوزر تاني.
- إنه يحصل على سيشن يوزر تاني ممكن تحصل عن طريق الـ Brute force – predection – interception ونقدر نمنعم عن طريق الاتصال الأمن (HTTPS) ونمنع التخمين عن طريق الـ Random value ونمنع البروت فورس عن طريق long value.

1-تعريفها: هي عملية بيقوم بيها السيرفر عشان يبقى فاكر هو بيتعامل مع مين, يعني زي لما تدخل جامع الحسين (رضي الله عنه) ويروح يديك تكيت لمكان الكوتشي, هنا الراجل بيعرف انك صاحب الكوتشي الفلاني من التيكت بتاعك طيب ولو وقع؟ هيعرف منين إنك صاحب الكوتشي ده, وبالتالي هيفتكرك حرامي ويطلعك برا خالص, نفس الكلام السيرفر لو فقدت السيشن الي بيعرفك بيها هيقولك السيشن انتهت ويطلعك برا.

- السيشن هي ملف بتكون فيه مجموعة من الريكوست والريسبونس مرتبطة بنفس اليوزر يعني هو الي عمل الريكوستس دي والسيرفر رد عليه بالريسبونس.
- والسيشن اتعملت تجنبا لمصادقة كل صفحة عايز تزورها, يعني بعد ما تسجل دخول -لو مفيش سيشن- وعايز تزور الصفحة الشخصية بتاعتك هتضطر تعمل Login تاني وهكذا في كل صفحة.
- السيشن اتعملت كمان عشان تحقق الـ Access Control الصحيح.

-السيشن السيكور بتكون ازاي:

-1يفضل الأسم بتاع السيشن ميوضحش أي تفاصيل خاصة بالموقع زي PHPSESSION بتوضح إن الموقع بيسخدم الـPHP.

-2يفضل تكون طويلة لإنها لو قصيرة هيحصل عليها.Brute Forec Attack

-3تكون قيمتها عشوائية عشان ميحصلش عليها تخمين.

-4تكون قيمتها ملهاش معنى عشان متوضحش أي حاجة خاصة بالموقع.

-مراحل الـSession Management:

-1الإنشاء والتحقق من السيشن: الـ Session Management Mechanise يا أما بتكون persmissive أو.strict

-2التحقق من السيشن كأي input في التطبيق لإنها ممكن تسبب.XSS, SQLI

-3إعادة إنشاء وتوليد السيشن بعد أي عملية privilege escalation زي تسجيل الدخول أو تغيير الباسورد والأميل وهكذا.

4-

-أسباب حدوثها:

- إن سياسية السيشن نفسها غير كافية
- إنه يبعت الـ session cookie في Insecure channel يعني HTTP
- ثغرة الsession Fixation
- مفيش حماية على الsession Fixation

-تيتست ازاي؟:

1-بتيست:Session management schema

- في التيست ده بتحتاج إنك تتأكد إن الكوكي والسيشنز أُنشأت في بيئة آمنة وغير متوقعة.
- في كل التفاعلات بين العميل والتطبيق لازم تسأل الأسئلة دي:
  - هل كل توجيهات الـ Set-Cookie فيها تاج الـ secure ؟
  - هل بتحصل أي عملية للكوكي عن طريق الـ HTTP مش الـ HTTPS يعني نقلها او ارسالها او إنشائها؟
  - ممكن ننقل الكوكي عن طريق HTTP بالاجبار؟
  - ايه المدة المحددة للكوكي عشان تنتهي؟
  - ايه هي إعدادات الـ cache-control عشان تحافظ ع الكوكي؟
- في التيست ده لازم تمر بـ3 مراحل:
  - 1- Cookie Collection:أول خطوة تفهم التطبيق بـ create /modify الكوكيز إزاي وهنا بتسأل شوية الأسئلة دي (الكوكيز بتتـ create فين وايه الصفحات بتاعتها وصالحة لانهي دومين وايه خصائصه, ايه الأجزاء الي بتعمل cookies وايه الي بتعدلها, ايه الأجزاء الي بتتطلب الكوكي ده تبقى(authorizwd
  - 2- Cookie Analysis:هنا بتتأكد من عشوائيتهم, ومدى اختلافهم, ومدى مقاومتهم ضد الهجمات

2-بتيست الـ :Cookie attributes

- أحيانا بيكون في اكتر من كوكي, في واحد للمصادقة مثلا, وواحد تاني للبيانات مثلا, وواحد تالت بيخص الحاجات الي هتشتريها -لو في متجر الكتروني- وهكذا.
- بتشوف الـ Secure, Path, Expires, HttpOnly, Domain attributes وتفحصها.

3-بتيست الـ :Session Fixation لما التطبيق ميغيرش قيمة الكوكي بعد ما اليوزر يعمل authenticated دي تبقى ثغرة session fixation ودي بتحصل لما :--

- 1-من اول ما بتطلب الموقع بيبقى في قيمة cookie موجودة, ف المفروض لما تعمل authenticated يشيل قيمة الكوكي دي ويحط قيمة جديدة, ف لو فضلت ثابتة هتبقى ثغرة.
- 2-أو إن المهاجم يفرض session id على الضحية وبالتالي لما يسجل الضحية الدخول المهاجم هيكون ليه صلاحية للدخول بردو, وده بيحصل لما الموقع ينشأ سيشن عبر HTTP وبعدين يعمل redirect لليوزر لصفحة.HTTPS
- لما تيجي تيست الثغرة دي اول حاجة هتطلب الموقع وتشوف الـ response هتلاقي, set-cookie فيها قيمة خدها كوبي واحفظها ف اي حتة وبعدين سجل دخول وشوف الـ response لو نفس القيمة فالـ set-cookieتبقى ثغرة او لو ملقتش الـ set-cookie اصلا.

4-في كل مرة بتتبعت فيه الـ session ID المفروض نفحص الـ HTTP Header/method/body وهنا بنتيست على 4 حاجات بالظبط:--

- بتختبر تشفير وإعادة استخدام ثغرات الـ :session tokens يعني المفروض في كل مرة يكون الطلب عبر HTTPSوكمان الـ session id بتتغير.
- بتتأكد إن الـ Expires :0 وكمان الـ Cache-control: max-age=0 عشان تتأكد عن الـ cache مش هيظهر الداتا.

-

Session Fixation

- الثغرة دي بتحصل نتيجة إن السيرفر بيعتمد الـ session الي كانت موجودة قبل ما اليوزر يعمل Login وبالتالي الـ Attacker لو قدر بطريقة من الطرق إن يثبت session معينة في متصفح الضحية فـ هو هيكون ليه access على أميل الضحية لما يعمل login.
- طيب إيه الطرق الي الـ Attacker يقدر بيها يثبت السيشن في متصفح الضحية؟

- دي بتعتمد على الطريقة الي التطبيق بيتعامل بيها مع السيشن سواء URL, Hidden form, Cookie.

1- لو بيعتمد على الـ URL Argument في الـ Attacker هيبعت لينك الموقع وفيه السيشن الي هو عايزها للضحية ولما الضحية يعمل login يقدر المهاجم يـ access أميل الضحية

2- لو بتعتمد على الـ Hidden Form في يقدر يعمل فورم شبه الموقع الأصلي ويستغل الضحية وهنا هيكون سيناريو أقوى من الـ session fixation أصلا.

3- لو بيعتمد على الـ Cookie في نقل السيشن فـ في كذا طريقة يثبت بيها الـ session في متصفح الضحية:

أ- عن طريق الـ Client-side scripting وبإختصار عن طريق الـ XSS, بيستغل وجود XSS ويثبت الجلسة بيها وممكن يوسع نطاق الهجوم عن طريق إضافة الـ domain,Expires attributes

ب- عن طريق الـ META Tag

ج- عن طريق التلاعب بالـ Set-cookie الي في الريسبونس, ممكن يكون التطبيق بيعتمد أي سيشن تتحط في الـ URLويبعتها للمتصفح وبالتالي تكتب أي سيشن وتبعتها لليوزر وتستنى يعمل login, أو عن طريق تلاقي ثغرة XSSفي صبدومين تابع للدومين الرئيسي وتثبت سيشن أنت عايزها بس بشرط تضيف domain attribute وتخليه للنطاق ككل, وآخر حاجة عن طريق الـ DNS وسيرفر خاص بالـ Attacker.

- طيب هنمنعها ازاي؟

1- عن طريق إن السيرفر يـ create سيشن جديدة طالما اليوزر عمل successful login وبقى authenticatedويلغي أي سيشن قبل عملية الـ login.

-سيناريوهات:

- 1-بتفتح صفحة تغيير الباسورد او تغيير الاميل (أو حتى الصفحة الرئيسية)وبتاخد الكوكي بتاعة الاميل كوبي (او ممكن تبعت الريكوست لل (repeaterوبعدين تحاول من متصفح مخفي (أو تعمل تسجيل خروج) إنك تدخل على نفس اللينك , طبعا هو هيطلب منك تسجل دخول, اعمل ريفريش للصفحة وحط الكوكيز القديمة وشوف هيدخل ع الاميل ولا لا. (وجرب مرة تاني إنك تسجل بالسيشن القديمة بس بعد ساعتين او تلاتة.)
- 2-أحيانا بعد ما تسجل دخول بتقدر تزور اكتر من صفحة(صبدومين زي (www , account , fourm جرب تفتحهم كلهم في المتصفح وكل صفحة في new tab وبعدين تعمل تسجيل خروج من واحدة فيهم وتشوف هيعمل Logout من الباقي ولا لا.

- -3افتح الاميل في 2 tabsمختلفة وتسجل الخروج من واحد وتشوف التاني هيسجل الخروج ولا لا.(نفس سيناريو زرار الـ(back
- ★ -4تحاول تعمل login في متصفحين مختلفين وتغير الباسورد في المتصفح الأول وتشوف هل هيعملك تسجيل خروج في المتصفح التاني ولا لا.
- ★ -5اعمل forget password وبعد ما يبعت اللينك على الاميل اعمل تسجيل دخول عادي وخد اللينك الي وصل على الميل وحطه في متصفح تاني وغير الباسورد وشوف هيسجل خروج في المتصفح الأول ولا هتقدر تستخدم المتصفحين عادي.
- -6جرب وانت authenticated للموقع إنك تزور صفحة تسجيل الدخول وتشوف هل هيعملك redirectلـ Home page ولا هيخليك تدخل credentials من جديد؟ , لو معملش ريرديركت وخلاك تدخل ال credentialsمن جديد سجل الدخول باميل تاني وشوف السيشن بتاعة الاميل الأول قاعدة ولا لا.
- ★ -7وانت مثلا اميلك taha@gmail.com اعمل reset password وسيب اللينك وبعدين روح سجل دخول وغير الاميل خليه taha1@gmail.com وبعدين روح للينك الي اتبعت واعمل تغيير الباسورد لان المفروض كل الروابط تبقى expired اول ما تغير الاميل.(أو ممكن تضيف اميل تاني للاك وبعد ما تعمل reset passwdللاميل التاني تحذفه وتسجل خروج وبعدين تروح للينك(
- -8لو التطبيق بيدعم 2 FAافتح الاميل على جهازين, الأول فعل فيه الـ 2 FAوروح للجهاز التاني اعمل ريفريش وشوف هيعمل Logout ولا هيبقى شغال, لان المفروض بعد الـ 2 FAيسجل الخروج من كل الأجهزة.
- -9لو تطبيق فيه خاصية الرسايل, فعل الاشعارات للرسايل وبعدين اعمل logout وشوف الاشعارات هتوصلك ولا لا.
- -10لو بتتعامل مع تطبيق وليه تطبيق على الاندرويد, اربط الاتنين ببعض وبعدين روح على الاندرويد وادخل صفحة من الصفحات الحساسة (تغيير الاميل, الباص,وهكذا) وسيبه فيها وبعدين روح ع الكمبيوتر وافتح الاك واحذف الاندرويد من إنه يكون مرتبط بالاك ده وبعدين روح للاندرويد وحاول تغير الاميل او الباسورد وشوف هينجح ولا السيشن هتنتهي.
- -11جرب تعمل forgot password وتسيب اللينك وبعدين تسجل دخول وتغيير الباسورد من جوا الاك , المفروض كل اللينك تبقى , Invalid ف بعدين ادخل ع اللينك وجرب تغيير الباسورد وتشوف هينفع ولا لا.
- -12جرب تسجل الدخول بكذا اميل وشوف هل الكوكي بتتغير ولا في.session fixation
- -13لو التطبيق بيدعم الـ delete account جرب تدخل على اتنين صبدومينز لنفس الموقع بس بيحتاجوا credentialsيعين زي www.example.com و fourm.exmaple.com وتحذف الاميل من الصبدومين الأول وتشوف هل تقدر تعمل أي action في الصبدومين التاني ولا السيشن هتنتهي,وممكن تفتح كل صبدومين في متصفح.
- -14لو الموقع بيدعم الاندرويد, جرب تدخل على تغيير الباسورد مثلا من الاندرويد وبعدين من اللاب تشيل الفون من الأجهزة المرتبطة بالاك ده شوف هل هتنتهي السيشن ولا لا, ولو انتهت وظهرت مسدج جرب تفصل الواي فاي وتقفل التطبيق وتفتحه تاني وتدخل ع تغيير الباسورد وبعد ما تكتب وتخلص تشغل الواي فاي وتدوس ok وتشوف هيتغير ولالا
- -15دايما لو الموقع بيتعامل مع الاندرويد تفتح الاميل في الجهازين (الكمبيوتر , الفون) وتبدأ تلعب معاهم مرة تحذف الاميل ف جهاز أو تغير الباسورد أو إنك تحذف الفون من الأجهزة المرتبطة وبعدها تعمل sesnsitive actionوهكذا.
- -16جرب تغير اليوزر نيم / ترفع او تغير صورة او تعمل أي action زي تكتتب كومنت او تبعت رسالة أي حاجة من دول وتعمل Intercept للريكوست وبعدين تبعتها للـ repeater وتعمل logout وبعدين تعمل go للريكوست وتسجل الدخول تشوف ال actionحصل ولا لا.
- -17جرب تستخدم رابط forgot password من متصفحين وتشوف الباسورد هيتغير ف التاني ولا لا.
- -18جرب تاخد السيشن من التصفح A وتروح تدخل ع نفس اللينك على متصفح B وتحط نفس السيشن لو منفعش , امسح الكوكي في متصفح B وجرب تضيف كوكي جديدة بنفس الاسم وتحط السيشن وتجرب.

- 19-لو التطبيق بيدعم إضافة رقم للاميل, جرب تضيف الفون لاميلين ف نفس الوقت وتستلم الكود وتفعل الاتنين وبعدين جرب ترجع الاميلين بنفس الرقم وشوف هل هيرجعوا ولا لا.
- 20-لو التطبيق بيفعل الـ FA 2عن طريق الرقم وبيعتلك كود, جرب تضيف الرقم لاميلين مختلفين وتشوف هل هيفعل الاتنين ولا لا, لو فعل الاتنين اعمل تسجيل خروج وحاول تسجل الدخول لو رفض الاتنين تبقى security misconfigration.
- 21-لو التطبيق فيه خاصية أو ميزة إنك تلغي السيشن الحالية جرب تعمل sensitive action وتبعته للـ repeaterوبعدين تبطل السيشن وتشوف تقدر تعمل action ولا لا.
- 22-

==========

2-لينكات مهمة:

1- https://www.slideshare.net/NoppadolSongsakaew/a2-broken-authentication-and-session-managementowasp-thailand-chapter-april-2016

2- https://www.slideshare.net/nikolamilosevic86/owasp-serbia-a3-broken-authentication-and-session-management?qid=29ef4f61-4437-4bf0-a0d6-0b76bcba1a77&v=&b=&from_search=3

3- https://www.slideshare.net/SarwarJahanM/broken-authentication-authorization-88089848?qid=29ef4f61-4437-4bf0-a0d6-0b76bcba1a77&v=&b=&from_search=7

4- https://medium.com/@nick_92077/complete-user-authentication-sessions-vs-jwt-37df744c1a40

5-