bug bounty

مبدأيا بدات تظهر فكره ال bug bounty لما ظهر في المواقع ثغرات كتير والشركات غير قادره هي والتيم بتاعها انها تقدر تكتشفها كلها ممكن يكون مثلا نتيجه ان التيم قليل او فعلا عدد الثغرات كبيره عليه وده كان بيكلف الشركات مبالغ ضخمه غير خساره ثقه العملاء كمان وتسريب معلوماتهم في اغلب الاحيان فهنا بدات تظهر فكره مواقع ال bug bounty ومن اهم المواقع دي :

1. Hacker one
2. Bug crowd
3. SynACK وغيرها بس دول الاشهر

وهنا الي بيحصل بشكل مبسط كالتالي ان الشركه بترفع ال source code بتاعها وبيبدأ ال hunters يجيبوا الثغرات ويبلغوا الشركه بيها عن طريق report وهما علي حسب خطوره الثغره بيحددوا المبلغ المدفوع .:

\*\*ازاي ابدأ في ال bug hunting :

* لازم يكون عندي معرفه كافيه الثغرات.
* ابدا يكون عندي أكونت علي موقع من التلاته الي تم ذكرهم فوق وممكن يكون عندي علي التلاته وبيزيد فرصتي اتي في platform SYNACK مثلا لأن العدد فيه ااقل وبالتالي فرصتي ازيد .
* وهنا انت مستعد انك تختار الموقع الي هتدور فيه وتعمل عنه report.

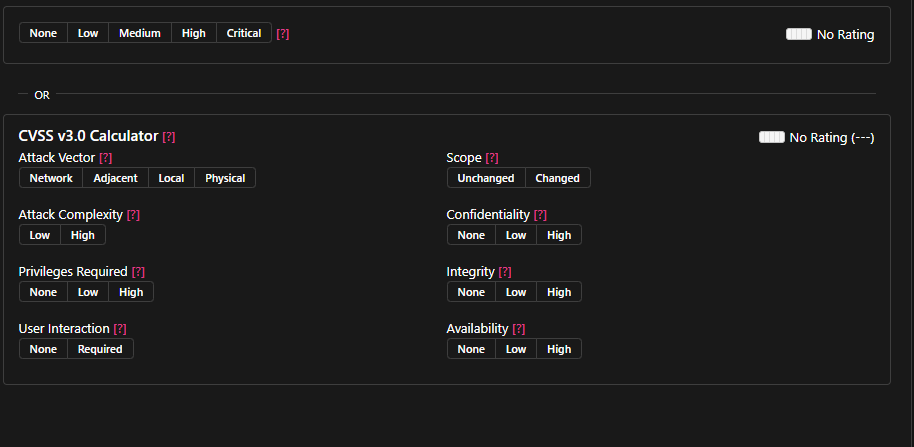
Note:كل ما كانت الثغرات المكتشفه في الموقع الي بتختاره ااقل كل ماكانت الفرصه اكبر.

وهنا ببدأ اقرا كل حاجه التيم الي يخص الموقع ده منزلها وبيكون فيها الشروط والثغرات والمقبوله لانها خطيره والثغرات الاقل في الخطوره الغير مفيده بالنسبه لهم حتي ممكن تكون ثغره critical بس في موقع مش موجود عليه داتا مهمه فبالتالي بتكون غير مهمه بالنسبه لهما .

--وهنا تبدا اهميه ال :report

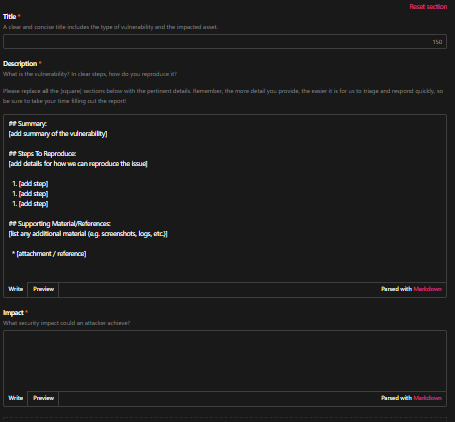
الreport من الحاجات المهم انك تكون علي درايه كافيه بطريقه كتابتها بشكل سليم لان ده بيسهل علي التيم انه يعرف مكان الثغره ونعها وخطورتها بسهوله وبالتالي في معظم الاحيان في bouns.

ده الشكل الي بيظهر عند كتابه ال report: الجزء الي فوق لو انا مش عارفه اكتب ريبورت او تفاصيل والجزء التاني لو انا فاهم وعارف اكترعن خطوره الثغره وهكذا.



وهنا تكمله ال report :وهنا في ال title:ببدا اكتب اسم الثغره الي انا اكتشفتها

Description :ببدأ اكتب وصف الثغره ولقيتها في اي جز وبتعمل ايه وهكذا ولن بكتب جواها حاجه مهمه جدا وهيreproduce steps to: وهي ببساطه الطرق الي بتبعها للوصول للثغره بشكل مبسط ومفهوم.



Impact:معناه لو حد استغل الثغره دي هيحصل ايه.

وبعدها بتبعت ال report . ممكن توصل ان الثغره الي اكتشفتها دي duplicated وده معناه ان حد بلغ عنها قبلك وللاسف مش هيدفعولك عليها.

Note :tax form هو عباره عن اني بسجل بيانتي عشان مياخدش من ضرايب علي الثغره لاني مش عايش في الدوله الي هتاخد الضرايب ةبالتالي مش هستفاد من خدمتها هي ك ورقه اعفاء من الضرايب.

Information disclosure )

* Backup files:وهي معناها ان المدير او الادمن اخد نسخه وسمها .tar او . zip وهذا وسبها علي الموقع فبالتالي انا لو كتبت مثلا wepsite url /backeup.tar هلاقيه نزلي نسخه من البيانات.
* Hidden files:وهو اي ملف بيبدأ ب (. )لان اللينكس بيعتبره ملف مخفي .
* Source code reprositre : .git ده بيبقي ملف في نسخه من الموقع المعدل بحيث لو حبيت ارجعله اة في اكتر من حد شغال علي نفس الملف فهو بيجمعها سوا وكذلك مع .svn
* Source code file :بيبقي في ملفات مثلا .old او .bak او عد علي ملف فبقي في .php~
* Javascript files:في معظم الاحيان بيبقي جواها معلومات مهمه جدا ممكن باسوردات ملفات خاصه بالادمن وهكذا.
* Githup reprositre: استخدام githup مفيد عموما ومن المهم تكون بتعرف تتعامل معاه وتكون قادر علي السيرش فيه لان ممكن مثلا تلاقي فيه باسورد لموقع مهم وهكذا.

تم بحمد الله تعالي