URL Redirection

1-تعريفها: هي ثغرة بيستغلها المهاجم في إنه يحول الضحية إلى موقع خارجي وهنا الضحية بيثق في الموقع الخارجي لإنه متحول ليه من موقع موثوق وميعرفش إن دي ثغرة.

- تسمي أيضا الثغرة بـ unvalidated redirects , cross-site redirect, open redirection.

2-أسباب حدوثها:

- السبب الرئيسي هو إن المبرمج بيثق في الـ user input وبيكون واثق في إنه اليوزر مش هيكتب موقع خبيث, وبالتالي الـ Attacker ممكن يستبدل الموقع الموثوق بموقع تاني وهنا مثال:

Ex: https://exmaple.com/authen/?url=https://fourm.example.com

- في لو تلاحظ هنا الموقع exmaple.com بيحول اليوزر من الـ WWW إلى الـ Fourm فـ لو الـ Attacker بدل الـ Fourn.exmaple.com بـ www.evil.com كده هيحول اليوزر لموقع خبيث.
- الكود في الحالة دي بيكون بالشكل ده:

```
$redirect_url = $_GET['url'];
header("Location: " . $redirect_url);
```

- بيكون في variable بيجيب قيمة البارامتر الي اسمه URL أيان كان هو أي بدون ما يعمل عليه أي validationوبعدين بيحول اليوزر ليه.
- إنما الكود الآمن بيكون كده:

```
<?php
/* Redirect browser */
header("Location: http://www.mysite.com");
/* Exit to prevent the rest of the code from executing */
exit;
?>
```

3-أماكن حدوثها:

- الثغرة بتتم عن طريق حاجتين: 1- الـ URL Parameters أو الـ 2-Path Fragments
- الـ Path Fragment الـي هو بعد الـ / الي بعد الدومين https://bing.com/evil.com --
- ممكن تجيب Open Redirection عن طريق الـ XSS أو العكس.

- https://github.com/EdOverflow/bugbounty-cheatsheet/blob/master/cheatsheets/open-redirect.md في اللينك ده في أكتر البارامترز الي بيحصل فيها URL Redirection.
- وبالتالي كل البايلود الي عندنا نقدر نجربها في الـ Path Fragment أو الـ URL Parameters

4-ازاي تلاقيها:

- 1-عن طريق الـ Burp proxy HTTP History وتدور في البارامترز وتشوف مين الي بيعمل ريديركت وتجرب فيه.
- 2-في الـ Functions المرتبطة بعملية الـريديركت زي login, logout , sign-up, forgot password, change language.
- 3-عن طريق دروكات جوجل والاشهر هو :Inurl وبتكتب فيه البارامترز المتوقعة تكون موجودة في الموقع.
- 4-الـ URLs الموجودة في ملفات الجافاسكريبت (في مرحلة تجميع ملفات الـ js هتفيدك هنا.)
- 5-إنك تعمل brute directories وتشوف ممكن يظهرلك URLs مش موجودة.

5-بتستغلها ازاي:

- 1-بنستغلها في الـ Phising Attack وهو إنك بتحول اليوزر لموقع تابع ليك وشبه الموقع الأصلي وبتطلب منه يدخل الـ credentials من جديد وبالتالي بيحصل account take-over.
- 2-لو في SSRF ومش عارف تستغلها بتدمجها مع الـ URL Redirection.
- 3-لو في صفحة في نفس الموقع مش عارف تـ access ها ف بتعمل ريديركت عليها وبتدخل عادي.

http://www.example.com/function.jsp?fwd=admin.jsp

- 4-ممكن تستخدمها في إنك تجيب XSS أو العكس.

6-طرق للـ Bypass:

1-اول حاجة هتجرب الـ payload يكون https://bing.com بس.

2-جرب // بعد الدومين الأساسي exmaple.com//bing.com

أو example.com/@bing.com

3-جرب تكتب البارامتر مرتين, مرة وفيه الموقع الأصلي ومرة فيه الموقع الي عايز تعمل ريديركت عليه.

Url=original-site.com&Url=evil.com

4-لو بيرفض أسم الموقع (evil.com/google.com/bing.com) جرب الـ IPv4 والـ IPv6

5-جرب الـ long IP بإنك تحول الـ IP بتاع الموقع لـ decimal IP.

6-جرب تعمل encode للـ URL الي بتكتبه أو double encode.

7-لو بتجرب XSS جرب prompot أو confirm بدل alert.

-8لو بيتشيك على الـ extension في image url أو file url في جرب تكتب الـ extension في الاخر

File=https://bing.com/.pdf

-9جرب تكتب نفس الدومين بس تضيفه لدولة تاني يعني

https://www.exmaple.com/authen?url=https://example.com.eu

https://www.exmaple.com/authen?url=https://example.com.eg

-10جرب example.com/@evil.com لان في الحالة دي بيكون الـ example.com كيوزر نيم والـ evil.com هو الدومين.

-11ممكن تجرب url=example.com.evil.com عشان لو عامل regex للي مفروض يتكتب.

-12جرب بدون سلاش يعني.http:evil.com

-13جرب الباك سلاش يعني.http:/\/\evil.com

-14لو الموقع بعد الريديركت بيضيف حاجة للدومين الاصلي يعني زي https://www.exmaple.com.mx جرب تغير قيمة الـ .mx وتخليها eu أو eg مثلا.

-15جرب الريديركت في الـ.OAuth

-16أحيانا بيكون الموقع الي هيتعمل عليه ريديركت والبارامتر بتاعه معمولهم encode فـ لو حسيت إنك في صفحة بيتعمل ريديركت ومفيش بارامتر شوف الـ URL ممكن تلاقي حاجة encoded وجرب تعملها.decode

-17احيانا وهو بيعمل ريديركت من مكان معين زي (login,log-out) وغيرهم, بياخد قيمة الـ location من الـ Refererوالي منها بيحولك, ف جرب تغير الـ.Referer Header

-18لو حاولت تعمل ريديركت ولقيت البارامتر اختفى وعملك ريديركت للصفحة الرئيسية ده معناه في ,filter فـ جرب الـ payload ده.http://:@bing.com\@maindomain.com/../d

-19جرب تعمل open redirection في الـ OAuth ولو منفعش شوف طرق للـ, Bypass منها:

- جرب تعمل ريديركت لصبدومين مش موجود تابع للدومين الاصلي كأنه.whitelisted
- لو التطبيق بيدعم إنشاء تطبيقات خلي الموقع يعمل ريديركت للتطبيق بتاعك والـ OAuth يعمل ريديركت للموقع الي هيعمل ريديركت للتطبيق
-

-20جرب الـ google.com//<> وممكن تحولها لـ XSS عن طريق تغيير الـ google.com بالـ.Payload

-21لو بتجرب الثغرة في Path Fragment جرب الاول تضيف كلمة وتشوف هتضاف فين وحاول تجيب XSS ومنها تجيب) Open Redirect عن طريق.(<script> </script>

-22ممكن تحول الـ payload لـ short url أو.double short url

-23لو مفيش بارامتر للريديكت في صفحة اللوجين جرب تضيف واحد وتديله value وتشوف هيعمل ريديركت بعد اللوجين ولا لا.

-24لو في صبدومين بيحولك على الدومين الرئيسي جرب تخليه يحولك ع موقع خارجي عن طريق

https://sub-domian.com//evil.com/%2f/%2e%2eوباقي الـ.bypass

-25ركز في الـ URL كله احيانا بيكون في Parameters بتمنع الـريديركت زي &redirect=flase ف ممكن تلعب بيها وتخليها true وبكده هيسمح بالريديركت.

-26لو بتجرب open redirect في ال path fragment وعايز تجيب xss جرب البايلود ده

/x:1/:///%01javascript:alert(document.cookie)/

-27لو في فلتر بيمنع الريديركت لموقع خارجي ولكن بيسمح لاي صبدومين تابع للموقع, جرب ترفع ملف svg بيعمل ريديركت لموقع خارجي وتخلي الثغرة تروح للملف.

-28لو بتجرب IP موقع معين وفيه أصفار في النص ممكن تتجاهلها وتكتب الـ IP عادي وهيتقبل زي 192.168.1

-29جرب تغير البروتوكول من HTTP لـــ FTP.

-30من خلال الـ Burp HTTP History سيرش على =https أو =aHR0 أو اي URL parameter وتقدر تجيب منها SSRFأو LFI بردو.

-31ممكن الـ Open Redirect نعملها escalation لـ

Open Redirect + Miconfigured OAuth App => OAuth Token Stealing

Open Redirect + Filtered SSRF => SSRF

Open Redirect + CRLFi => XSS

Open Redirect + javascript URI => XSS

-32في الـ path fragment ممكن تجرب http://victim//%0d%0ahttp://google.com/

-33ممكن تستخدم الـ % وتكتب الاول الدومين الي هيتعمل عليه ريديركت وبعدين الدومين الاساسي وممكن تعملها encode وتبقى كدهhxxp://evil.com%EF%BC%http://maindomain.com

-34ممكن تجرب ? في آخر الـ Payload مثلا ?url=evil.com

-35لو في input بياخد subdomian جرب تكتب الدومين كامل وفي الاخر ضيف#

-36

-1قسم الـ open redirect في اللينك ده- https://github.com/EdOverflow/bugbounty) cheatsheet/blob/master/cheatsheets/open-redirect.md)

-1قسم الـ filter bypass في اللينك ده) https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Open%20Redirect)

-7امنعها ازاي؟:

-1أول حاجة وأهم حاجة هي إنك تبعد خالص عن الـريديركت وكده وتتجنب ده.

-2الخطوة التانية موجودة في حالة إنك أستخدمت الريديركت, فـ متدخليش اليوزر يتدخل في عملية الـ Redirection يعني مفيش uner input أصلا (زي الـ safe code الي فوق.)

-3لو مضطر يكون في user input ف انت محتاج تعمل validation كويس وتتأكد إن الـ URL مناسب للموقع وتابع ليه, والـ User authenticated للـ URL ده, وكمان مسموح ليه بالـ Functions الي موجودة في الـ URL ده, ومثال للنقطة دي هي صفحة الادمن الي بيتحكم منها باليوزرز, ف لو يوزر حب يعمل ريديركت عليها لازم الموقع يتأكد إنه الادمن وإن الـ Functions الي جوا الصفحة ينفع اليوزر ده يعملها وهكذا.

-4أعمل Whitelisted بالمواقع الي ينفع تعملها.redirect

-5آخر حاجة وهو إنك بتحط صفحة وسيط آثناء عملية الريديركت بتظهر وتقول لليوزر إنه هيتم نقله من الموقع الأصلي إلى موقع خارجي وده من خلال تأكيده للعملية لما يدوس على input بيظهرله في الصفحة دي.

-8مراجع:

1- https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html

2- https://pentester.land/cheatsheets/2018/11/02/open-redirect-cheatsheet.html

3- https://github.com/EdOverflow/bugbounty-cheatsheet/blob/master/cheatsheets/open-redirect.md

4- https://s0cket7.com/open-redirect-vulnerability/

5- https://medium.com/@__rishabh__/open-redirect-to-account-takeover-e939006a9f24

6- https://0xnanda.github.io/Open-Redirects-Everything-That-You-Should-Know/ وانت بتيست open ارجعلهاredirect