معهد العراب العالي للتدريب

تامين مواقع وتطبيقات الويب

م سمر سعيد

نبذة عن المقرر

تُعَد شبكة الإنترنت مكانًا خطيرًا، إذ نسمع بانتظام عن عدم توفّر مواقع الويب بسبب هجمات حجب الخدمة أو عرض معلومات مُعدَّلة وضارة غالبًا على صفحاتها الرئيسية، وكانت قد سُرِّبت الملايين من كلمات المرور وعناوين البريد الإلكتروني وتفاصيل بطاقة الائتمان إلى النطاق العام في حالات أخرى عالية المستوى، مما عرّض مستخدمي مواقع الويب للإحراج الشخصي والمخاطر المالية، فالغرض من أمان موقع الويب هو منع هذه الهجمات أو أيّ نوع آخر منها. التعريف الرسمي لأمان موقع الويب هو فعل أو ممارسة تهدف إلى حماية مواقع الويب من الوصول، أو الاستخدام، أو التعديل، أو التدمير، أو التعطيل غير المُصرَّح به.

معهد العراب العالي للتدريب

بيل جيتس

يعتمد تقدم التكنولوجيا على جعلها مناسبة بحيث لا تلاحظها حقا ، لذا فهي جزء من الحياة اليومية.

مراحل اختبار الاختراق

أثناء إجراء تقييم الثغرات الأمنية لتحديد نقاط الضعف في النظام والإبلاغ عنها، يتم إجراء اختبار الاختراق لاستغلال/ مهاجمة الثغرات الأمنية المحددة للتحقق مما إذا كان يمكن اختراق الثغرات الأمنية المحددة. هناك خمس مراحل وهي كما يلي:

- **Reconnaissance.**
- **Scanning.**
- **Gaining Access.**
- **Maintaining Access.**
- **Covering Tracks.**

Reconnaissance

خلال هذه المرحلة ، سيقوم فريق اختبار الأمان بجمع أكبر قدر ممكن من المعلومات حول الهدف قبل تنفيذ أي هجمات.
الغرض من هذه المرحلة هو التخطيط بشكل أفضل للهجمات بناء على المعلومات التي تم جمعها. يمكن تصنيف الاستطلاع على النحو التالي:

Passive Reconnaissance

كجزء من هذا ، سيتم جمع المعلومات حول النظام المستهدف دون التفاعل مع النظام. وفيما يلي بعض الأمثلة:

Google Hacking:

البحث عن النظام المستهدف على جوجل

Dumpster Driving

البحث عن المعلومات الموجودة في صناديق المهملات للنظام المستهدف

Active Reconnaissance

وهذا ينطوي على استهداف النظام مباشرة لاسترجاع المعلومات. وفيما يلي بعض الأمثلة: الاتصال بموظف وطلب تفاصيل النظام المستهدف. استخدام تقنيات الشبكة غير التدخلية لمسح النظام المستهدف واسترجاعها المعلومات.

Scanning

يتم إجراء المسح على التطبيق الهدف بهدف تحديد نقاط الضعف التي يمكن استغلالها في مراحل لاحقة للوصول إليها.
سيستخدم فريق اختبار الأمان الأدوات التقنية للمسح. الأدوات التي ستستخدمها فرق اختبار الأمان للمسح:

- **Vulnerability Scanners**
- **Port Scanners**
- **Ping Tools** (Example: ICMP Ping tool can be used to check whether the system is alive on the network)
- **Network Mappers**

على سبيل المثال، بعد معرفة ما إذا كان النظام على قيد الحياة على الشبكة باستخدام أدوات Ping، يمكن استخدام تطبيقات الشبكة مثل Nmap لاكتشاف المنافذ المفتوحة والعثور على الخدمات الموجودة

Gaining Access

يستغل فريق اختبار الأمان النظام للوصول، من خلال المساس بنقاط الضعف التي تم تحديدها في المراحل السابقة.
بمجرد أن يتمكن الفريق من الوصول إلى النظام والتحكم الكامل في النظام، سيتم تنفيذ الهجمات على النظام أو استخدام الوصول المكتسب لشن هجمات على النظام الآخر.
يمكن للفريق استخدام أدوات مثل Hydra للوصول إلى النظام والتحكم الكامل فيه.

Maintaining Access

بمجرد الحصول على الوصول في المرحلة السابقة، يتعين على الفريق اتخاذ خطوات لمواصلة الوصول إلى النظام.
وأحصنة طروادة Rootkitsمن أجل الحفاظ على الوصول إلى النظام، يمكن للفريق تثبيت أدوات مثل وإنشاء حساب المسؤول وأدوات الباب الخلفي الأخرى.
سيتمكن الفريق من الحفاظ على الوصول إلى النظام عن بعد بينما تستمر الأدوات المثبتة في العمل في وضع الاختباء / التخفي.
يمكن للفريق أيضا إضافة النظام المستغل إلى الروبوتات، من أجل الحصول على مزيد من التحكم في النظام أو تنفيذ هجمات على الأهداف الأخرى.

Covering Tracks

أخيرا ، سيتخذ الفريق خطوات لحذف آثار الهجوم بقصد عدم اكتشافها.
كجزء من هذا ، قد يتبع الفريق الأنشطة التالية:
تعديل / حذف سجلات التطبيق والنظام لتجنب الكشف والمقاضاة. يمكن للفريق القيام بذلك يدويا أو باستخدام الأدوات.
إخفاء البيانات باستخدام تقنيات الاختزال لتجنب الكشف بواسطة أي برنامج لمكافحة الفيروسات
تأكد من أن الأدوات المثبتة مثل الجذور الخفية وأحصنة طروادة وأدوات الباب الخلفي الأخرى تظل مخفية.
استخدام تقنيات التهرب لانتحال عنوان IP لانحراف فريق الكشف في الاتجاه الخاطئ.

Penetration Testing Techniques

يتضمن اختبار الاختراق ، المعروف أيضا باسم القرصنة الأخلاقية ، تقييم أمان تطبيق الويب من خلال محاكاة هجمات العالم الحقيقي.

تتضمن بعض التقنيات الشائعة المستخدمة في اختبار الاختراق ما يلي:

Network Scanning and Enumeration:

تحديد المنافذ المفتوحة والخدمات ونقاط الضعف في النظام المستهدف.

تقييم نقاط الضعف **Vulnerability Assessment:**

تحديد نقاط الضعف والضعف في تطبيق الويب أو بنيته التحتية.

استغلال **Exploitation**

محاولة استغلال الثغرات الأمنية المكتشفة للوصول أو التحكم غير المصرح به.:

Password Cracking

اختبار قوة كلمات المرور لتحديد كلمات المرور الضعيفة أو التي يمكن تخمينها بسهولة.

Social Engineering

التلاعب بالأفراد للوصول إلى المعلومات أو الأنظمة الحساسة.

Web Application Testing

تقييم أمان تطبيقات الويب ، بما في ذلك التحقق من صحة الإدخال والمصادقة والتخويل وإدارة الجلسة.

Web Application Penetration Testing

Penetration Testing Process.

Information Gathering & Vulnerability Assessment:

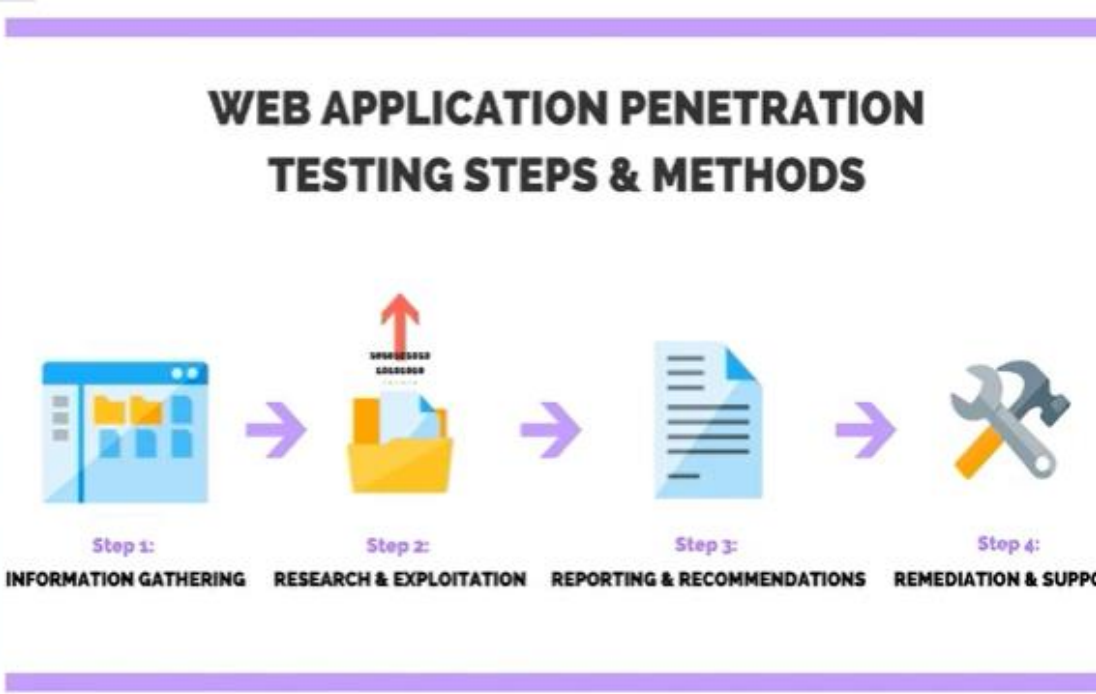
Using NMAP. - Using ZAP. - Dirb.
Using Nikto. - Using Nessus. - Dir Buster.

Different Cyber-Attacks

Password Cracking
Brute-Force
File Inclusion Attacks (LFI/RFI)
SQLi
CSRF
XSS
Command Execution.

Web Penetration Testing Tools:

John the Ripper.
Hashcat.
SQLMAP.
Burp-Suite.
Metasploit.
Wireshark.



معهد العراب العالي للتدريب

2024

النهاية

مراجعة سريعة

سؤال و إجابة

سؤال عن المحاضرة ؟

محاولة استغلال الثغرات الأمنية المكتشفة للوصول أو التحكم غير المصرح به

- Exploitation
- Password crack

معهد العراب العالي للتدريب

تامين مواقع الويب

م سمر الهوارى

محتويات المحاضرة

- Overview of Burp-Suite, Key Features and Techniques.
- Burp-Suite Advanced Proxy Configuration.
- Burp-Suite Intruder Module Usage.
- Understanding of Metasploit Framework, Modules, and Commands.

نظرة عامه Burp-suit

Burp Suiteهي أداة قوية لاختبار أمان تطبيقات الويب تحتوي على تصبح عنصرا أساسيا في ترسانة اختبار الاختراق الحديثة. تم تطويره وصيانته من قبل Portswigger، وهي منظمة رائدة في مجال البحث والتدريب في مجال الأمن السيبراني. يقدم Burp Suiteمجموعة واسعة من الأدوات والميزات التي يمكن استخدامها لتحديد واستغلال نقاط الضعف في تطبيقات الويب. من خلال إتقان تقنيات Burp-suite، يمكنك تحسين قدرتك بشكل كبير على تحديد واستغلال نقاط الضعف في تطبيقات الويب ، مما يؤدي في النهاية إلى تحسين أمان الأنظمة التي تختبرها.

Professional	Community Edition
➢ Web vulnerability scanner	➢ Essential manual tools
➢ Advanced manual tools	
➢ Essential manual tools	

Burp-Suite Key Features

Proxy:

تعمل وحدة الوكيل كوكيل اعتراض ، مما يسمح لك بفحص وتعديل حركة مرور الويب في الوقت الفعلي.

. Spider

تزحف وحدة Spiderإلى تطبيق الويب المستهدف ، وتعيين سطح الهجوم واكتشاف المحتوى المخفي.

Scanner:

إجراء فحص تلقائي للثغرات الأمنية ، وتحديد العيوب الأمنية المختلفة.

Intruder

د وحدة Intruderأداة قوية لأتمتة الهجمات ، مثل تخمين كلمة المرور
شويش المعلمات والمزيد.

Burp-Suite Key Features

Repeater:

تتيح لك وحدة Repeater إعادة تشغيل الطلبات الفردية وتعديلها بسهولة ، مما يساعدك على فهم نقاط الضعف واستغلالها.

Sequencer:

تحلل وحدة Sequencer عشوائية الرموز المميزة للجلسة وملفات تعريف الارتباط والقيم الأخرى ذات الأهمية الأمنية الحرجة.

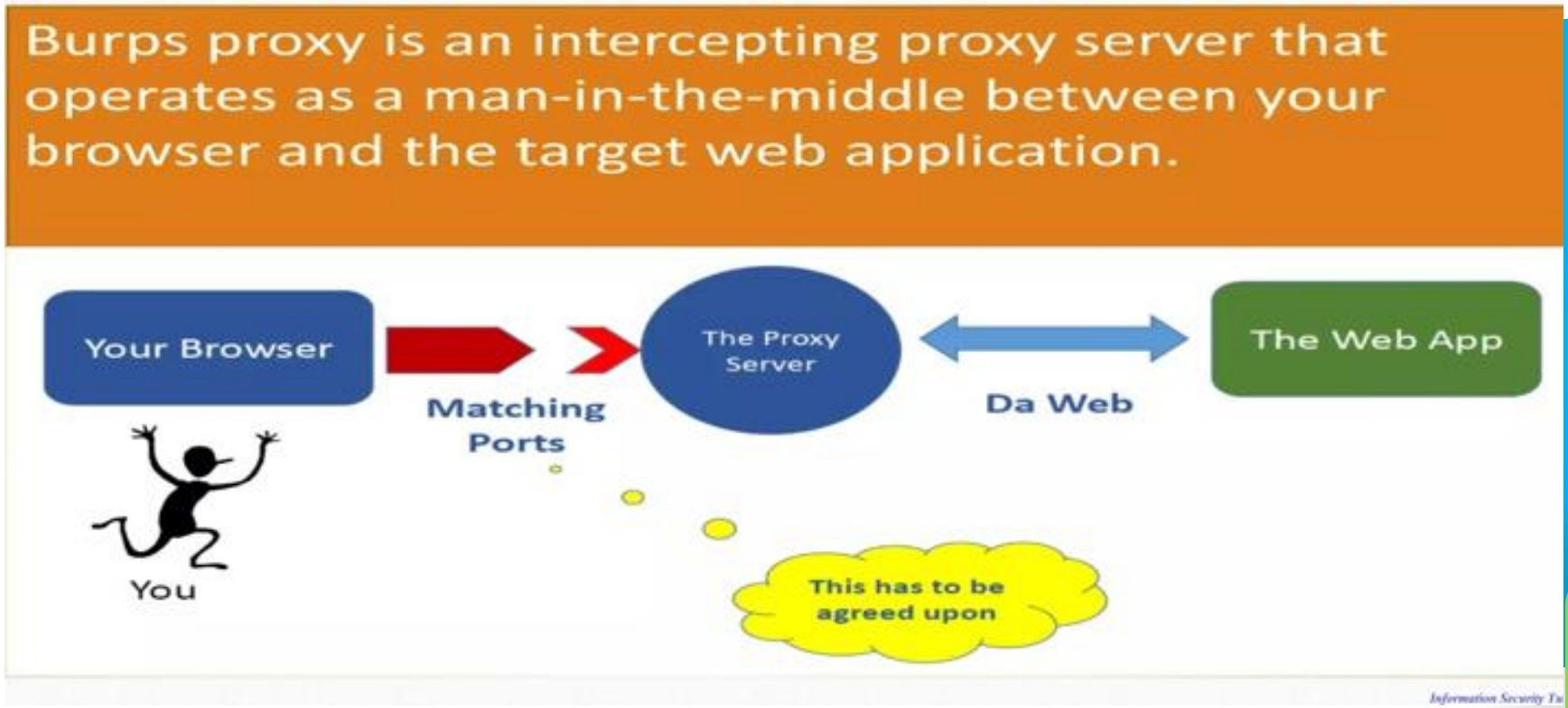
Decoder:

توفر وحدة فك التشفير مجموعة متنوعة من أدوات التشفير وفك التشفير ، مما يسهل العمل مع بيانات تطبيق الويب.

Extender:

تتيح لك وحدة الموسع إضافة وظائف مخصصة إلى Burp Suite عن طريق تثبيت ملحقات الجهات الخارجية.

Burp-Suite Key Features



- **Burp-Suite Techniques**

Advanced Proxy Configurations
Effective Target Scoping
Customized Scanning

Metasploit

Metasploitهو إطار عمل مفتوح المصدر يوفر منصة شاملة لتطوير واختبار وتنفيذ كود الاستغلال ضد الأنظمة المستهدفة. تتم صيانتها بواسطة Rapid7، وهي شركة رائدة في مجال الأمن السيبراني ، ولديها مجتمع واسع من المساهمين والمستخدمين.

Metasploit Techniques

الاستغلال المتقدم: استكشف تقنيات لتجاوز التدابير الأمنية الحديثة ، مثل عمليات تخفيف الاستغلال وحلول مكافحة الفيروسات ، لنشر عمليات استغلال Metasploitبنجاح. التهرب ومكافحة الطب الشرعي: تعرف على كيفية استخدام تقنيات التهرب من Metasploit، بما في ذلك أجهزة التشفير والتشويش وآليات مكافحة الكشف ، لتجاوز الضوابط الأمنية وتقليل مخاطر الكشف. تخصيص الحمولات الصافية: فهم كيفية إنشاء ونشر حمولات مخصصة يمكنها تجاوز الاكتشاف المستند إلى التوقيع وتوفير وظائف محسنة، مثل المثابرة أو تدوين لوحة المفاتيح أو الوصول عن بعد. تكامل قاعدة بيانات :Metasploitاستكشف استخدام قاعدة بيانات Metasploitلتخزين بيانات الاختبار الخاصة بك وإدارتها ، مما يتيح تنظيما وتحليلا وإبلاغا أكثر فعالية لنتائجك. وحدات وملحقات :Metasploitاكتشف كيفية الاستفادة من وحدات وملحقات Metasploitالتابعة لجهات خارجية ، والتي يمكن أن توفر وظائف متخصصة أو عمليات استغلال خاصة بالهدف ، مما يزيد من توسيع قدرات إطار العمل.

ما تمت مناقشته سابقا ، يمكن استخدام Metasploitفي معظم خطوات اختبار الاختراق.
يمكن تلخيص الوظائف الأساسية التي يوفرها Metasploitمن خلال بعض الوحدات:

- 1. Exploits
- 2. Payloads
- 3. scanners
- 4. Encoders

Expliots

الاستغلال هو البرنامج المستخدم لمهاجمة نقاط الضعف في الهدف. هناك قاعدة بيانات كبيرة لعمليات الاستغلال على إطار عمل Metasploit.يمكنك البحث في قاعدة البيانات عن عمليات الاستغلال والاطلاع على المعلومات حول كيفية عملها ووقت اكتشافها ومدى فعاليتها وما إلى ذلك.

Encoder

يوفر لك Metasploitأيضا خيار استخدام برامج التشفير التي ستقوم بتشفير الرموز بطريقة تصبح غامضة بالنسبة لبرامج الكشف عن التهديدات لتفسيرها. سيتم فك تشفيرها ذاتيا وتصبح رموزا أصلية عند تنفيذها. ومع ذلك ، فإن برامج التشفير محدودة ويحتوي برنامج مكافحة الفيروسات على العديد من التوقيعات الموجودة بالفعل في قواعد البيانات الخاصة بهم. لذا ، فإن مجرد استخدام برنامج تشفير لن يضمن التهرب من مكافحة الفيروسات. قد تتجاوز بعض برامج مكافحة الفيروسات ببساطة باستخدام برامج التشفير.

Components of Metasploit Framework

Metasploitمفتوح المصدر وهو مكتوب بلغة روبي. إنه إطار عمل قابل للتوسيع ، ويمكنك إنشاء ميزات مخصصة حسب رغبتك باستخدام .Rubyيمكنك أيضا إضافة مكونات إضافية مختلفة. في صميم إطار عمل Metasploit، هناك بعض المكونات الرئيسية:

- . msfconsole
- 2. msfdb
- 3. msfvenom
- 4. meterpreter

msfconsole

ذه هي واجهة سطر الأوامر التي يستخدمها إطار عمل .Metasploitيمكنك من التنقل عبر جميع قواعد بيانات Metasploitبسهولة واستخدام الوحدات المطلوبة. هذا هو الأمر الذي أدخلته من قبل للحصول على وحدة تحكم .Metasploit

msfdb

يمكن أن تصبح إدارة جميع البيانات عقبة حقيقية سريعة ، وهذا هو السبب في أن Metasploit Frameworkيمنحك خيار استخدام قاعدة بيانات PostgreSQLلتخزين بياناتك والوصول إليها بسرعة وكفاءة. على سبيل المثال، يمكنك تخزين نتائج الفحص وتنظيمها في قاعدة البيانات للوصول إليها لاحقا.

معهد العراب العالي للتدريب

2023

النهاية

مراجعة سريعة

يتم كتابة فقرة صغيرة لمراجعة محتوى المحاضرة

سؤال و إجابة

واجهة سطر الأوامر التي يستخدمها إطار عمل Metasploit.

- 2. msfdb
- msfconsole
- 3. msfvenom

XSS

XSS

هي ثغرة تسمح للمخترق بزرع أو حقن سكريبت بأي لغة يدعمها المتصفح الذي يستعمله زائر موقعك، وغالبًا ما يكون هذا السكريبت بلغةجافاسكريبت، وعند تصفح الموقع يتم تنفيذ هذا السكربت

كيف تعمل XSS؟

أولًا في هجوم XSS هناك ثلاثة فاعلين وهم كالتالي:

- الضحية وهو زائر موقعك

- الوسيلة أو الجسر وهو موقعك نفسه

- ثم المخترق وهو الذي يستغل موقعك للإيقاع بالزوار

وفي هجوم XSS يقوم المخترق بإستغلال إحدى طرق إدخال البيانات إلى الموقع، وليكن مثلًا عبر حقول إدخال النص Input Text Fields، فيرسل بيانات على شكل سكريبت، بعد ذلك يتم تنفيذ هذا السكريبت على متصفح الزائر، وتختلف هجمات XSS بإختلاف طريقة التعامل مع السكريبت المحقون، إما أن يُخزن في قاعدة بيانات ثم ينفذ عند إستدعائه، وإما أن يُنفذ مباشرة دون أن يُحفظ عبر دمجه في رابط معين.

ماهي أنواع XSS؟

توجد ثلاثة أنواع من هجمات XSS جميعها قائمة على نفس المبدأ المتمثل في إستغلال موقع عبر إرسال سكريبت يتم تنفيذه على مستوى متصفح الزائر.

و هذه الأنواع الثلاثة من أنواع XSS كما يلي:

• Stored XSS وتسمى كذلك Persistent XSS: وتحدث هذه الثغرة حينما يقوم المخترق بإستغلال أحد مدخلات الموقع فيقوم بإرسال سكريبت يتم تخزينه على مستوى سيرفر الموقع و غالبًا في قاعدة البيانات Database، كأن يرسل السكريبت من مربع كتابة التعليقات في الموقع، أو على شكل رسالة، أو من أي مكان في الموقع يسمح بتخزين القيم في قاعدة البيانات، وحينما يأتي زائر ليستعرض الصفحة التي تحتوي على القيم القادمة من قاعدة البيانات يتم تنفيذ هذا السكريبت.

على سبيل المثال قمت ببرمجة مدونة Blog من أجل نشر المقالات عليها، في إحدى مقالاتك دخل المخترق

وبدل أن يكتب لك تعليقًا قام بكتابةسكريبت، هذا السكريبت سيتم تخزينه في قاعدة البيانات، وبالتالي حينما سيأتي زائر ما ليستعرض مقالتك سيتم تحميل التعليقات من قاعدةالبيانات ومعها التعليق الملغوم.

• Reflected XSS وتسمى كذلك Non-persistent XSS، وتحدث حينما يستغل المخترق إحدى مدخلات الموقع دون الحاجة إلى تخزين السكريبت في قاعدة البيانات، فيقوم بإرسال رابط الموقع مدموجًا بسكريبت ملغوم إلى الضحية عبر إيميل مثلًا، أو من خلال نشر هذا الرابط على موقع ما أو على مواقع التواصل الإجتماعي، وحينما يضغط الضحية على الرابط سيذهب به إلى الموقع وسيتم تنفيذ السكريبت المدمج معه وبالتالي سيحصل المخترق على ما يشاء، إما عبر سرقة Cookies أو من خلال KeyLogging أو القيام بعمليات أخرى.

• Dom-based XSS: وهو شبيه جدًا بالنوع Reflected XSS، غير أنه يتركز بالأساس على التحكم في Dom الخاص بالصفحة عبر تنفيذ سكريبت مكان إرسال قيمة معينة.

العملى

SQLI

SQLI

SQLما المقصود بـ

تخزّن قاعدة البيانات .هي لغة برمجة لتخزين المعلومات ومعالجتها في قاعدة بيانات علائقية (SQL)لغة الاستعلام الهيكلية العلائقية المعلومات في شكل جدول، به صفوف وأعمدة تمثل سمات بيانات مختلفة والعلاقات المختلفة بين قيم البيانات

SQLما سبب أهمية

يتعلم محللو البيانات .هي لغة استعلام شائعة تُستخدم بشكل متكرر في جميع أنواع التطبيقات (SQL)لغة الاستعلام الهيكلية على سبيل .ويستخدمونها لأنها تتكامل بشكل جيد مع لغات البرمجة المختلفة (SQL)والمطورون لغة الاستعلام الهيكلية لإنشاء تطبيقات معالجة البيانات Javaفي لغة البرمجة (SQL)المثال، يمكنهم تضمين استعلامات لغة الاستعلام الهيكلية هي (SQL)لغة الاستعلام الهيكلية .MS SQL Serverأو Oracleالرئيسية مثل SQLعالية الأداء مع أنظمة قواعد بيانات .لغة سهلة التعلم إلى حد ما لأنها تستخدم في جملها كلمات أساسية إنجليزية شائعة

- **ما هي الـ SQL Injection؟**
- هي من الثغرات الأمنية التي قد يجلب استغلالها نتائج كارثية، من تسريب لكافة البيانات الخاصة بتطبيق الويب وبيانات المستخدمين من كلمات مرور ومعلومات شخصية أو تفاصيل بطاقات الائتمان المخزنة في قواعد البيانات، حيث تستخدم تطبيقات الويب
- في عمليات المصادقة للتأكد من بيانات المستخدم ولجلب المعلومات من قاعدة البيانات لإظهار بعض SQL Queries
- قد تؤدي لكشف جميع ما تحتويه قاعدة البيانات أو تعديلها أو حتى Queries بـ SQLولكن قد يتم استغلال ذلك يهدد أمان تطبيقات الويب ويشكل تهديداً لسمعتها وثقة عملائها SQLi حذفها.

العملى