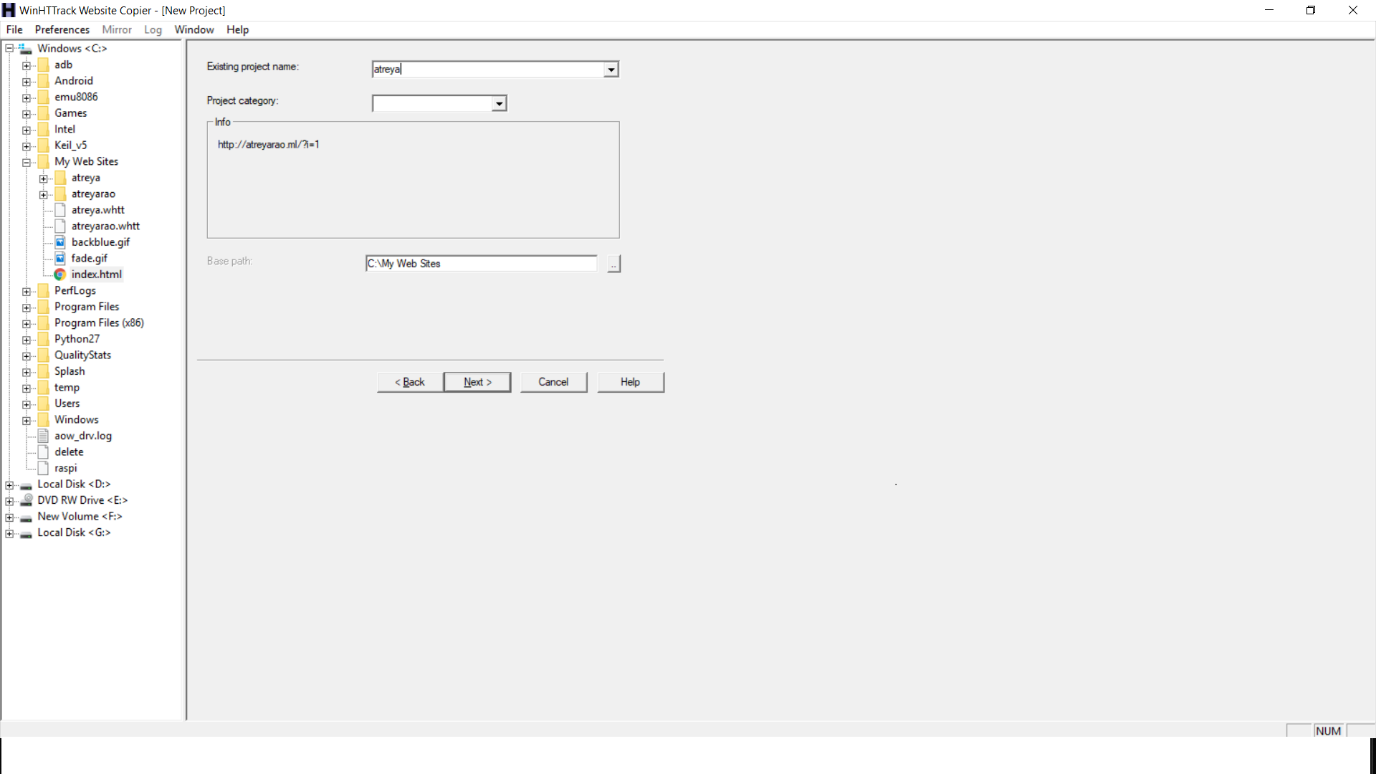
1)Hosting a simple static webpage on a free server and use httrack to download the static webpage and try httrack on a server side.

A) My website URL-http://atreyarao.ml

Httrack:



2) Brief description about SQL injection

A) An SQL injection is an attack where an malicious code is embedded in a software or application and then passed to the database. The malicious data produce sql queries result in compromising the database or which should not be executed.

Example:

In a website there is a place where we can search for customer detail by typing the customers social security number. When an user types the number like “123456789” the SQL query which runs on background is

SELECT client\_name, telephone, address, date\_of\_birth WHERE social\_sec\_no=123456789

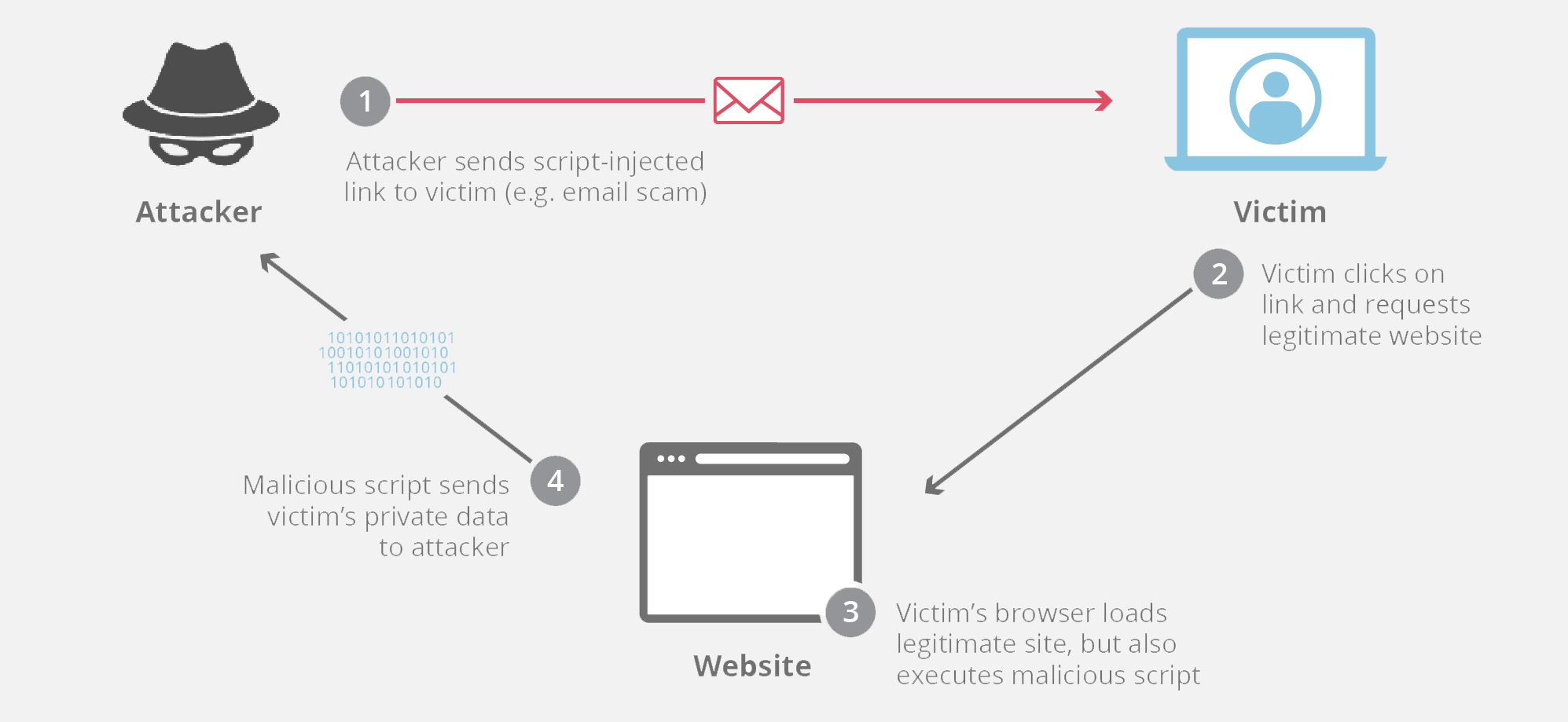
Now a person with SQL knowledge can type “123456789 or 1=1”, which is passed as follows:

SELECT client\_name, telephone, address, date\_of\_birth WHERE social\_sec\_no=123456789 or 1=1

The condition ‘1=1’ is always true hence it will return all the columns in the database.

3) What is XSS? How does it cause information leakage?

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. By leveraging XSS, an attacker does not target a victim directly. Instead, an attacker would exploit a vulnerability within a website or web application that the victim would visit, essentially using the vulnerable website as a vehicle to deliver a malicious script to the victim’s browser.



HOW CROSS-SITE SCRIPTING WORKS?

In order to run the malicious application on the website which the victim visits he must find a way to inject payload on the webpage. He can go for social engineering techniques to convince a user to visit a vulnerable page with an injected JavaScript payload.

In order for an XSS attack to take place the vulnerable website needs to directly include user input in its pages. An attacker can then insert a string that will be used within the web page and treated as code by the victim’s browser.

Example of cross-site scripting:

The following server-side pseudo-code is used to display the most recent comment on a web page.

print "<html>"

print "<h1>Most recent comment</h1>"

print database.latestComment

print "</html>"

The above script is simply printing out the latest comment from a comments database and printing the contents out to an HTML page, assuming that the comment printed out only consists of text.

Attacker’s payload:

<html>

<h1>Most recent comment</h1>

<script>abc();</script>

</html>

Here abc() is some malicious function. The possible thing that can be done by this function is:

a) Cookies are often used to store session tokens, if an attacker can obtain a user’s session cookie, they can impersonate that user.

b) Make arbitrary modifications to the browser’s DOM

c) JavaScript can use XMLHttpRequest to send HTTP requests with arbitrary content to arbitrary destinations.

4)GDPR

GDPR

The General Data Protection Regulation (GDPR) standardizes data protection law across all 28 EU countries and imposes strict new rules on controlling and processing personally identifiable information (PII). It also extends the protection of personal data and data protection rights by giving control back to EU residents. GDPR replaces the 1995 EU Data Protection Directive, and goes into force on May 25, 2018. It also supersedes the 1998 UK Data Protection act.



GDPR replaces the EU Data Protection Directive of 1995. The new directive focuses on keeping businesses more transparent and expanding the privacy rights of data subjects. When a serious data breach has been detected, the company is required by the General Data Protection Regulation to notify all affected people and the supervising authority within 72 hours. Mandates in the General Data Protection Regulation apply to all data produced by EU citizens, whether or not the company collecting the data in question is located within the EU, as well as all people whose data is stored within the EU, whether or not they are actually EU citizens.

Under GDPR, companies may not legally process any person's personally identifiable information without meeting at least one of six conditions.

1)Express consent of the data subject.

2)Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract.

3)Processing is necessary for compliance with a legal obligation.

4)Processing is necessary to protect the vital interests of a data subject or another person.

5)Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

6)Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject

5)What is Windows exploit guard? Where is it used?

A)

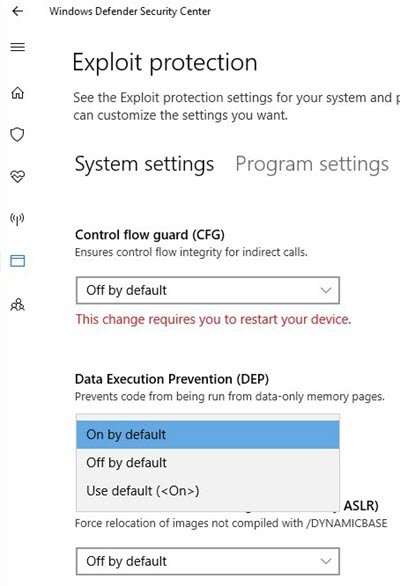
Windows Defender Exploit Guard (Windows Defender EG) is a new set of host intrusion prevention capabilities for Windows 10, allowing you to manage and reduce the attack surface of apps used by your employees.

There are four features in Windows Defender EG:

Exploit protection can apply exploit mitigation techniques to apps your organization uses, both individually and to all apps. Works with third-party antivirus solutions and Windows Defender Antivirus (Windows Defender AV).

Attack surface reduction rules can reduce the attack surface of your applications with intelligent rules that stop the vectors used by Office-, script- and mail-based malware. Requires Windows Defender AV.

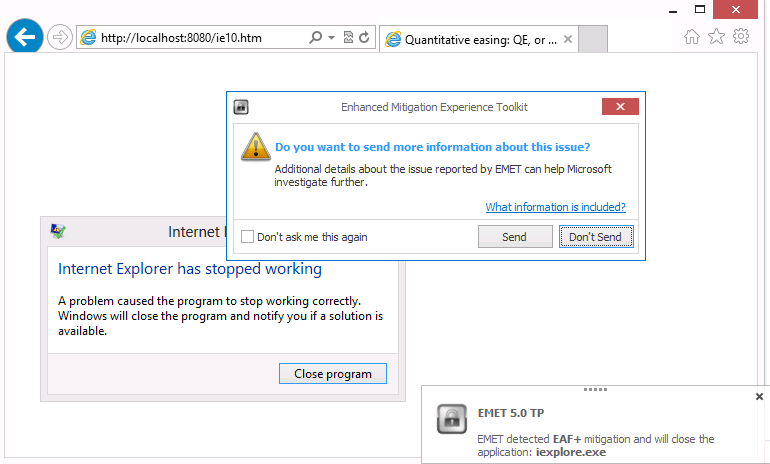
Network protection extends the malware and social engineering protection offered by Windows Defender SmartScreen in Microsoft Edge to cover network traffic and connectivity on your organization's devices. Requires Windows Defender AV.

Controlled folder access helps protect files in key system folders from changes made by malicious and suspicious apps, including file-encrypting omware malware. Requires Windows Defender AV.

6)Why EMET removed in Windows 10?

A)

EMET, a security solution that provides protections against general hacking attack techniques, is getting "deprecated" as a standalone Windows client solution, meaning that it won't get developed and no security updates will arrive for it in the near future. Organizations with older applications typically might use EMET to ward off common exploit techniques. Microsoft more recently announced that EMET's protections are getting moved into the "Windows Defender Exploit Guard" feature of the Windows 10 "fall creators update,"



7)Write briefly how recovery software works

When we delete any item on our pc it doesn’t actually gets deleted but its memory address is marked as delete(this location an be used to allocate memory to different process). The recovery software just reads data from this location (if it is not overwritten) and recovers the file.



8) What is thunking and why Thunking is necessary for Windows

A)

A thunk, in a general computing context, is a piece of low-level machine generated code, which implements the details of a software system. It is one of the following:

A piece of code performing a delayed computation

A feature of a virtual function table implementation

A mapping of machine data from one system specific form to another for compatibility issues

An intermediate code translates memory address between platforms. Microsoft has a thunking layer of itself called Win32s, which permit 32-bit Windows application to run on 16-bit Windows. The 64-bit Windows version also provides a thunking layer, WoW64, which permits using 32-bit Windows applications.

9) Case study: signed overflow, Ariane 5.

A)

In June 1996, the then new Ariane 5 rocket was launched on its maiden flight. It carried a payload of scientific satellites. Ariane 5 was commercially very significant for the European Space Agency as it could carry a much heavier payload than the Ariane 4 series of launchers. Thirty seven seconds into the flight, software in the inertial navigation system, whose software was reused from Ariane 4, shut down causing incorrect signals to be sent to the engines. These swivelled in such a way that uncontrollable stresses were placed on the rocket and it started to break up. Ground controllers initiated self-destruct and the rocket and payload was destroyed.

A subsequent enquiry showed that the cause of the failure was that the software in the inertial reference system shut itself down because of an unhandled numeric exception (integer overflow). There was a backup software system but this was not diverse so it failed in the same way.

This failure occurred when an attempt to convert a 64 bit floating point number representing the horizontal velocity to a signed 16 bit integer caused the number to overflow(become too big).

It could have been prevented if they used an exception handler.

10)Write briefly about Format specifiers and its types.

A)

Format specifiers can be defined as the operators which are used in association with printf() function for printing the data that is referred by any object or any variable. ... Format specifiers start with a percentage % operator and followed by a special character for identifying the type of the data.

%d Integer Format Specifier

%f Float Format Specifier

%c Character Format Specifier

%s String Format Specifier

%u Unsigned Integer Format Specifier

%ld Long Int Format Specifier