University of North Texas

CSCE 5560 Research and Hacking Project Proposal

Catherine Dockendorf

Matthew Wilson

Divya Abburi

Santoshini Girkati

Sushan Sainju

10/02/2022

CSCE 5560 Security Commerce Fall 2022

Hacking Project Proposal

Malicious Hyperlinks

Catherine Dockendorf Matthew Wilson Divya Abburi

Santoshini Girkati Sushan Sainju

I. PROBLEM

The advent of short URL (Uniform Resource Locator) links poses a threat of being redirected to a malicious website. Unlike in traditional links where it is clear which website it redirects to; short URLs takes trust in the sender that the link received leads to a legitimate website.

A problem that has arised in recent times, for example, is the existence of the software program Linode and BeEf as seen in a NetworkChuck video.

Linode is a high-performance Linux server that is hosted on a cloud platform where the user gets to choose the parameters of storage according to business or purpose needs. This in combination with BeEF leads to a serious website security exploit. BeEF (short for Browser Exploitation Framework) is a penetration testing API tool that provides client-side web browser exploitation.

How the exploit works is that if a user clicks on the link that has a BeEf hook attached to it, there will be theft of important customer device information. It may be hard to detect once a javascript payload is delivered.

Knowing this, we are looking at discovering the inner workings of this tool and to recreate some of the concepts utilized.

II. METHOD

This programming project should give us greater understanding and experience with Client-Server architectures. This also exposes us to the use of Virtual Machines and Linux application tools.

III. GOAL

The goal of this hacking project is to dive into the security programming concepts that are being utilized in malicious hyperlink hijacking and lead us to gain an understanding of how to better fortify against cyberattacks.

Hacking Project Proposal

SQL Injection Attacks

Catherine Dockendorf   Matthew Wilson   Divya Abburi

Santoshini Girkati   Sushan Sainju

I. PROBLEM

SQL Injection is the method of sending SQL (short for Structured Query Language) commands to a database without proper authorization. This method can be used on websites that don’t check a user’s typed inputs to make sure the inputs are legitimate. From this concept, we propose a hacking project that employs the process of SQL injection.

II. METHOD

The project starts with a website. On the website page is a login form which will prompt the user for a username and password.

In this scenario, there are different accounts with different levels of access. The site by design will not properly check the username and password text fields. This will allow us, acting as bad actors, to use SQL injection to send commands to the database and gain access to data we shouldn’t have access to. This will lead to a data breach.

To prevent this data breach, the web developer needs to program all the text inputs to be checked for against SQL injection commands and make sure that every possible exception input is covered.

III. RESULT

We will use SQL injection on an insecure database to gain unauthorized access to data and create a data breach.

Knowing that SQL injection attacks are a serious issue in website security, developers must consider this when designing websites.

This hacking project will drill into security programming concepts and further strengthen the user requirement of making sure to as much as possible, cover every exception case known to cause exploitation.

CSCE 5560 Security Commerce Fall 2022

Research Project Proposal

Spyware Pegasus

Catherine Dockendorf Matthew Wilson Divya Abburi

Santoshini Girkati Sushan Sainju

I. PROBLEM

The emergency of a controversial spyware being weaponized against human rights activists is causing a stir in today's political climate. The spyware dubbed Pegasus was developed by Israeli cyber intelligence firm, NSO group.

How it works on a macro level is that it takes a target and discreetly gathers data from their phones such as:

- SMS
- Email
- Social Networks
- Contact Details
- Network Details
- Device Info
- Phone Calls
- Microphone
- Camera
- Photos & Videos
- Location
- File
- Passwords

Pegasus' price tag comes at a high cost, so it has high profile clientele and there has to be a solid and justifiable reason to invest the amount on a specific target.

II. METHOD

How the program works is that it takes and sends a payload to a device with no link clicks needed, just a destination. An example scenario is a missed WhatsApp call. It first accesses the device memory and hacks into the contents, then it has the ability to turn the phone into a recording device for example.

Currently, the spyware is known to self-destruct on command which implies it uses self-destructing code in its program which is normally frowned upon in today's software standards. The only resolution known to mitigate the damage once targeted is to resort to a factory reset.

III. OUTCOME EXPECTATION

Every design has the ability to contribute to the greater good of mankind but at the same time, anything is prone to be weaponized. There is a great responsibility among developers to protect the community from misuse and overstep of intelligence authority.

The goal of our group research is to find out what we know about this spyware and discuss a solution or suggestion to mitigate the damages.

Hacking Project Proposal

Unsecure Printer Data Scraping

Catherine Dockendorf Matthew Wilson Divya Abburi

Santoshini Girkati Sushan Sainju

I. PROBLEM

There are many printers for sale in the market these days that have port forwarding enabled by default. With that feature enabled, this means that anyone can gain access and control of the printer through the internet.

In the past, port forwarding enabled by default in printers have been used to gain control of distant printers from a remote location. This has led to the theft of user's printer information such as their print history.

II. METHOD AND SOLUTION

To begin, we will use a printer with port forwarding enabled and connect the device to the internet. Then, we will print a few test pages to add to the printer history. Next, we will then scan the network for the printer, connect to the printer without a username or password, and print a couple more test pages to demonstrate our control.

Lastly, we will download the complete print history to demonstrate that we have successfully stolen control of the printer privileges.

III. CONCLUSION

Checking the printer ports and closing any ports that are open should prevent this attack from occurring. Disconnecting the printer from the network is one way to mitigate this attack from happening.

Printers with open ports leave the user's data vulnerable to bad actors. This setup exposes all the documents they have ever scanned, faxed, or printed. Closing the ports or disconnecting from the network should prevent the theft of customer print data and address the unauthorized control of the printer.