DOMONIC THEMONICS

INTRODUCTION

DOMONIC THEMONICS IS OUR WEB EXPLOIT CHALLENGE.

WEB EXPLOITATIONS ARE ALLABOUT BREAKING A WEBSITE. YOU HAVE TO KNOW HOW TO LOOK INTO WEBSITE CODE (HTML AND JAVASCRIPT) TO FIND VULNERABILITIES TO EXPLOIT.

THESE ARE SOME OF THE MOST COMMON AND MOST DAMAGING ATTACKS.

JUST LAST WEEK WE HAD AN ATTACK THAT TOOK DOWN LARGE AMOUNTS

OF WEBSITES THAT MILLIONS VISIT ON A DAILY BASIS.

THESE ARE SO IMPORTANT TO THE INTERNET THAT SOME PEOPLE ARE PAID JUST TO FIND EXPLOITS AND BREAK WEBSITES SO THEY CAN BE MADE STRONGER.

TIPS

THERE ARE MANY TYPES OF ATTACKS SOMEONE CAN DO TO A WEBSITE

SQLINTECTION - BREAK THE WEBSITE BY INSERTING A BLOCK OF SQL CODE INTO AN INPUT BOX XSS (CROSS SOURCE SCRIPTING) - IS WHEN YOU INPUT JAVASCRIPT CODE INTO A BROWSER'S INSPECTION TAB THAT RESULTS IN HIJACKING YOUR BROWSER.

INSPECTING WEBSITE CODE IS ALSO AN EXTREMELY USEFUL AS YOU CAN USE THE JAVASCRIPT PORTION OF YOUR BROWSER'S INSPECTION TAB TO ENTER JAVASCRIPT YOURSELF

DOM - DOCUMENT OBJECT MODEL (STORES ALL ELEMENTS OF THE PAGE)

USEFUL COMMANDS:

QUERYSELECTER - ALLOWS YOU TO PULL ELEMENTS FROM THE WEBSITE'S DOM GETELEMENTBYID - QUERYSELECTOR BUT MORE SPECIFIC SETATTRIBUTE - SETS THE ATTRIBUTE OF THE SPECIFIED ELEMENT

HINTS

- I. I WONDER IF THERE'S A WAY TO SEE WHAT ELEMENTS MAKE
 UP THE PAGE?
- 2. IS THERE A WAY YOU CAN SEARCH FOR CERTAIN ELEMENTS IN THE DOM?
- 3. HMM...I WONDER IF THEY USED AN ID OR CLASS NAME WHEN MAKING THIS WERSITE