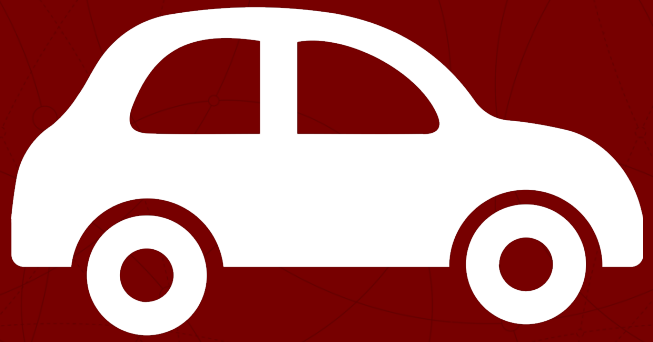
FLORIDA TECH



HACK THIS CAR

Intro to Web Exploitation

Panama Papers

In 2016, hackers breached the law firm of Panamanian offshore law firm and stole 11.5 million documents.

The documents exposed massive international corruption and fraud across several former heads of state, prime ministers, politicians, sports and entertainment figures that were hiding assets in 214 shell companies.

Although, the origin of the hack was never disclosed by the attackers – most assume the hackers breached through a 3-year old vulnerability in the Drupal web software.

FLORIDA TECH

What is the web?

The websites we browse are just a collection of servers on the internet that run applications that provide us data. And sometimes coders make mistakes in developing those applications. Web attacks take advantage of the programmer's mistakes.

FLORIDA TECH

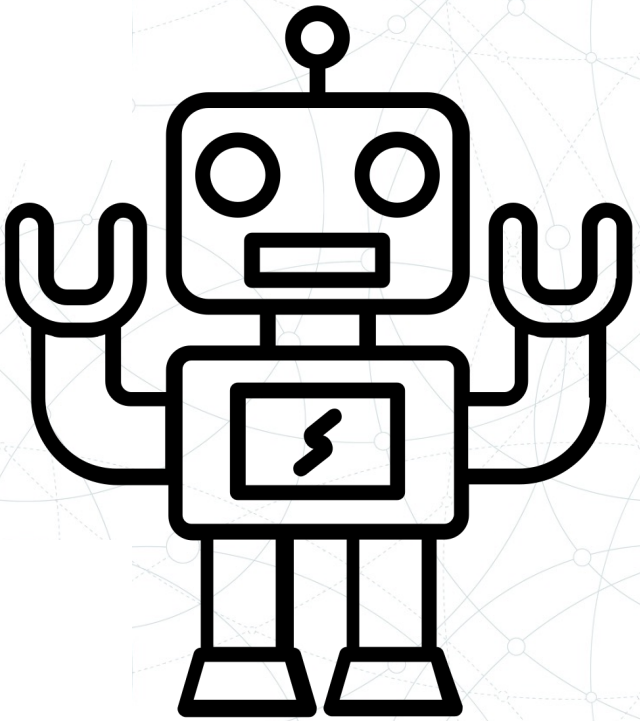
What's hiding behind robots.txt

Servers often have a hidden file named robotos.txt that tells search engines (like Google) to avoid crawling, indexing, and storing these specific pages. This can often be a great place to start attacking.

robots.txt

Which page might you try to visit?

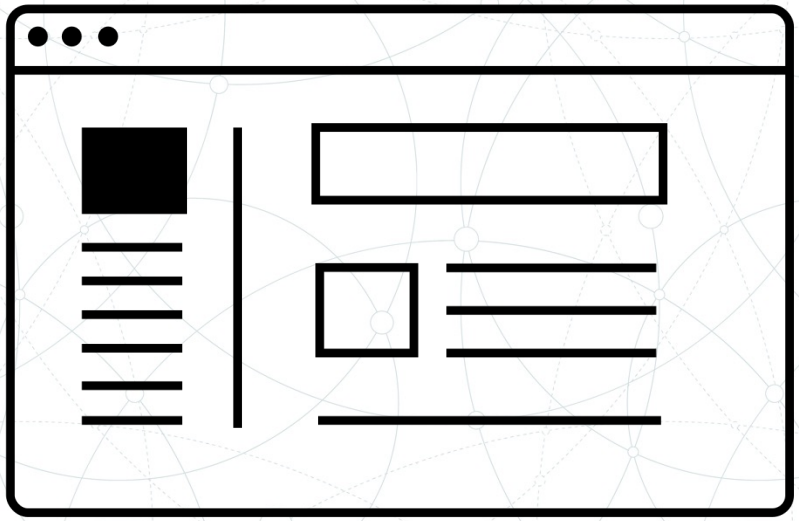
/advertising
/marketing
/admin-backdoor



FLORIDA TECH

Use the Developer Tools

Developer tools (often known as DevTools) are a collection of tools that help web programmers design, debug, and develop web pages. They also have the perfect functionality for hackers like us.



Inspector: View (and modify) the code behind webpages.

Network: Shows all requests and responses, the browser had made and received over the network

Storage: View (and modify) the cookies on webpages

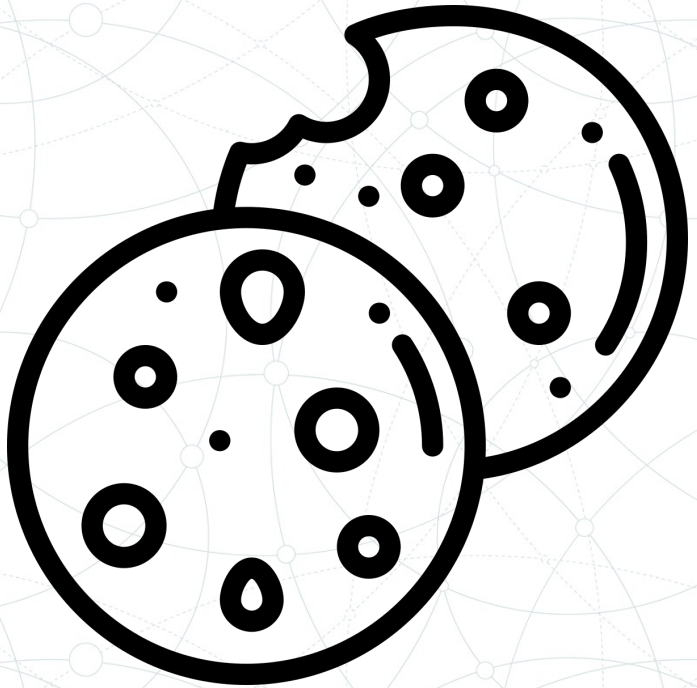
FLORIDA TECH

Who ate the cookies?

Cookies are small bits of data where servers store small bits of data on our computer. Using the **Storage** DevTools tab, we can actually edit them.

What might you change the following cookies to?

Name	Value
LoggedIn	False
User	Guest
AccountBalance	$100



FLORIDA TECH

Command Injection

Sometimes webpages take in user input and pass directly to a shell. Here a webpage takes in a network IP address and concatenates it with the ping command.

```
$target = $_REQUEST[ 'ip' ];
$cmd = shell_exec( 'ping ' . $target );
```

FLORIDA TECH

Command Injection

```
$target = $_REQUEST[ 'ip' ];
$cmd = shell_exec( 'ping ' . $target );
```

Benign Input

```
ip = 127.0.0.1
shell_exec( 'ping 127.0.0.1' );
```

Malicious Input

```
ip = 127.0.0.1 && cat /flag.txt
shell_exec( 'ping = 127.0.0.1 && cat /flag.txt');
```

FLORIDA TECH

Hack This Car Activity

FLORIDA TECH

FLORIDA TECH

Thank you.