Course Roadmap

- Day 1: Advanced Attacks
- **Day 2: Web Frameworks**
- Day 3: Web Cryptography
- Day 4: Alternative Web Interfaces
- Day 5: WAFs and Filter Bypass
- Day 6: Capture the Flag

Content Management Systems

SharePoint

WordPress

Exercise: WordPress RCE

Web Architectures

Web Design Patterns

Exercise: Mass Assignment in CakePHP

Templates and Injections

Exercise: Template Injections Lab

Languages and Frameworks

Modern PHP

Exercise: Authentication Bypass with Type Juggling

Logic Flaws

Java and Struts

Exercise: Struts 2 RCE

Attacking Object Serialization

Exercise: Jenkins Unsafe Java Deserialization

The MEAN Stack

Exercise: NodeGoat

EXERCISE: WORDPRESS RCE

Target: http://wp.sec642.org

Discovery: A WordPress blog is available on this server. WordPress itself is hardened and no obvious vulnerabilities can be found.

Goals:

- Bruteforce the administrative login to this Wordpress instance (username is admin)
- Look at the theme editor and find the backdoored function
- Gain access to read /etc/passwd, /proc/version, and finally /proc/self/environ

Note1: There is a file on our files server (files.sec642.org) that contains a subset of passwords from the RockYou password leak. (passwords.txt)

Note2: If you use Burp Suite Intruder, use Pro

Note3: You can also use wpscan to perform this task.

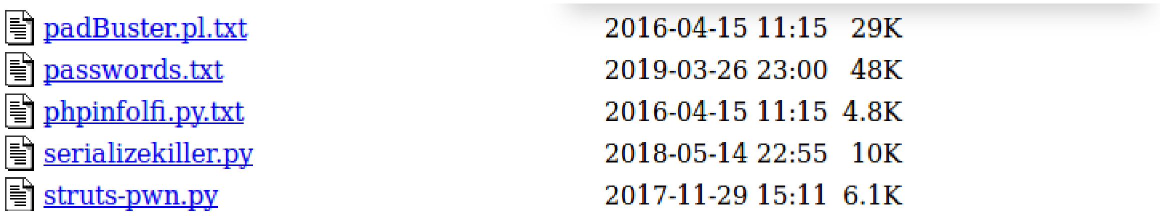
Bonus: Get full system access using a reverse shell to your computer.

EXERCISE WALKTHROUGH

Stop here if you would like to
solve the exercise yourself.

If you are not sure how to accomplish the goals, use the pages ahead to walk you through the exercise, showing you how to achieve each of the goals.

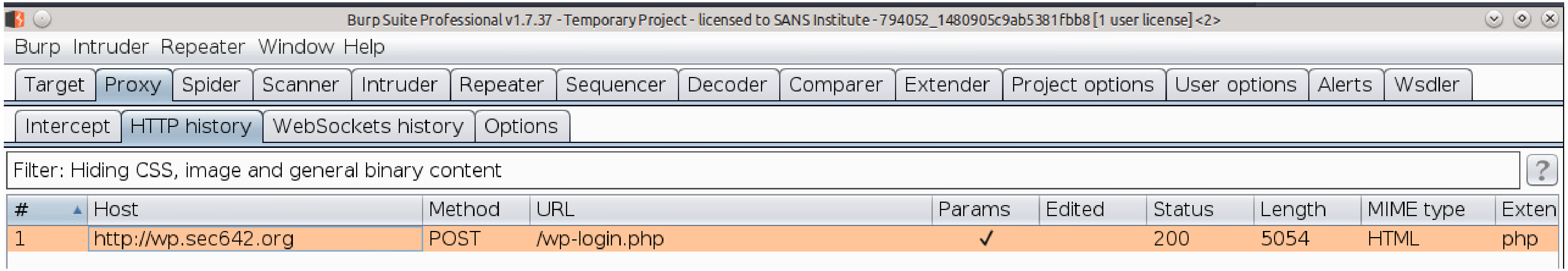
EXERCISE: WORDPRESS RCE
DOWNLOAD PASSWORD.TXT AND USE INTRUDER OR WPSCAN



padBuster.pl.txt	2016-04-15 11:15	29K
passwords.txt	2019-03-26 23:00	48K
phpinfolfi.py.txt	2016-04-15 11:15	4.8K
serializekiller.py	2018-05-14 22:55	10K
struts-pwn.py	2017-11-29 15:11	6.1K

Find the passwords.txt file in the files.sec642.org server

Make sure to chose a POST login event which contains the admin user login.



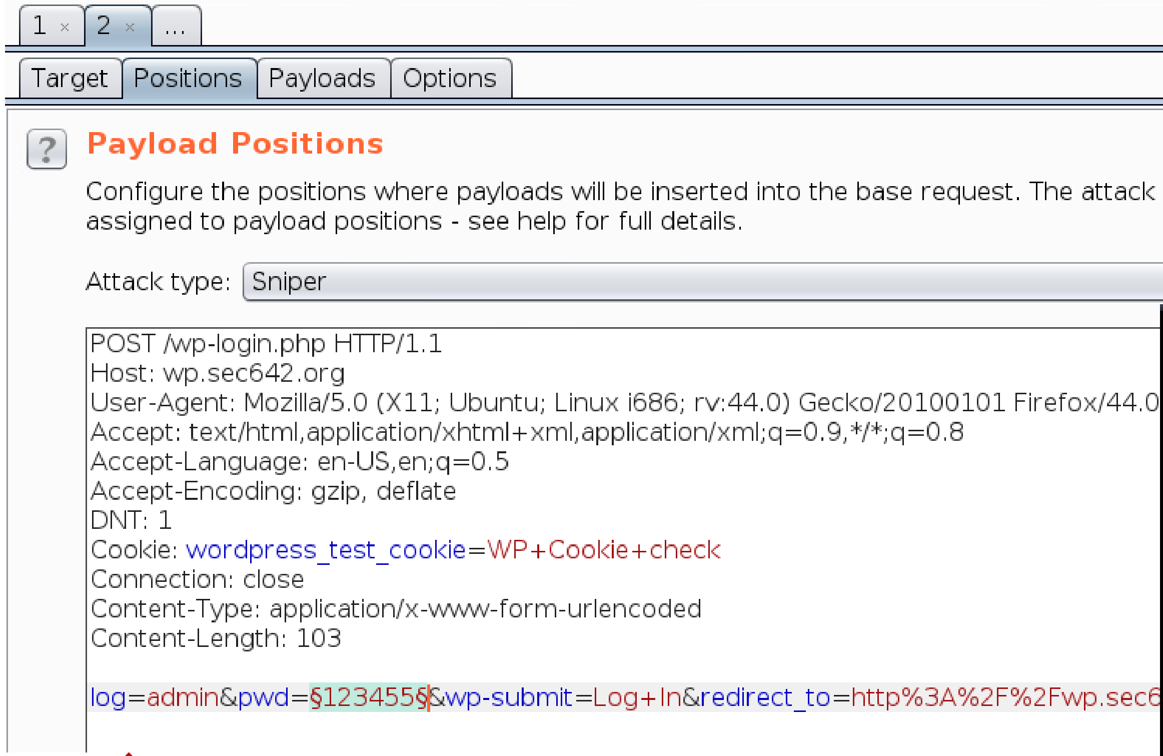
Burp Suite Professional v1.7.37 - Temporary Project - licensed to SANS Institute - 794052_1480905c9ab5381fbb8 [1 user license] <2>

Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Wsdler
Intercept HTTP history WebSockets history Options
?

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Exten
1	http://wp.sec642.org	POST	/wp-login.php	✓		200	5054	HTML	php

EXERCISE: WORDPRESS RCE
SETTING UP INTRUDER



Payload Positions

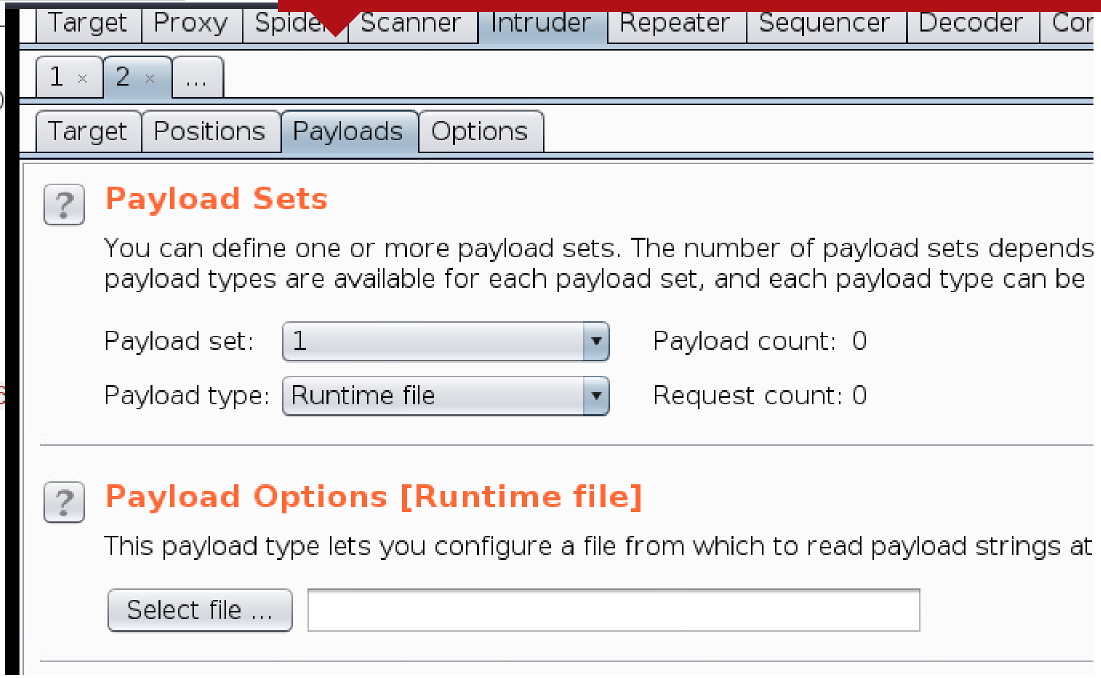
Configure the positions where payloads will be inserted into the base request. The attack type determine assigned to payload positions - see help for full details.

Attack type: Sniper

```
POST /wp-login.php HTTP/1.1
Host: wp.sec642.org
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:44.0) Gecko/20100101 Firefox/44.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: wordpress_test_cookie=WP+Cookie+check
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 103

log=admin&pwd=§123455§&wp-submit=Log+In&redirect_to=http%3A%2F%2Fwp.sec6
```

Ensure the pwd= field is what you are bruteforcing.

Make sure the payload type is runtime file for a file this large.



Payload Sets

You can define one or more payload sets. The number of payload sets depends payload types are available for each payload set, and each payload type can be

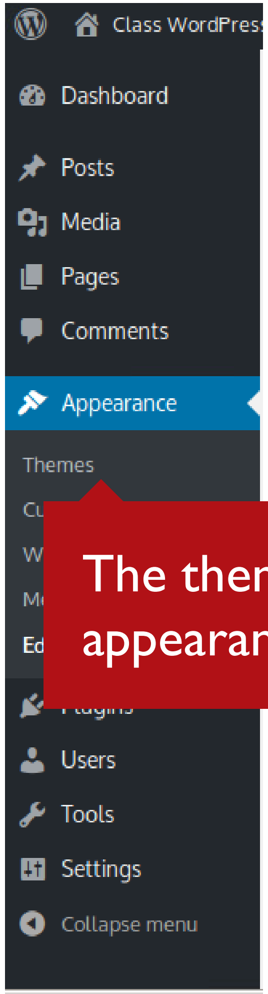
Payload set: 1 Payload count: 0

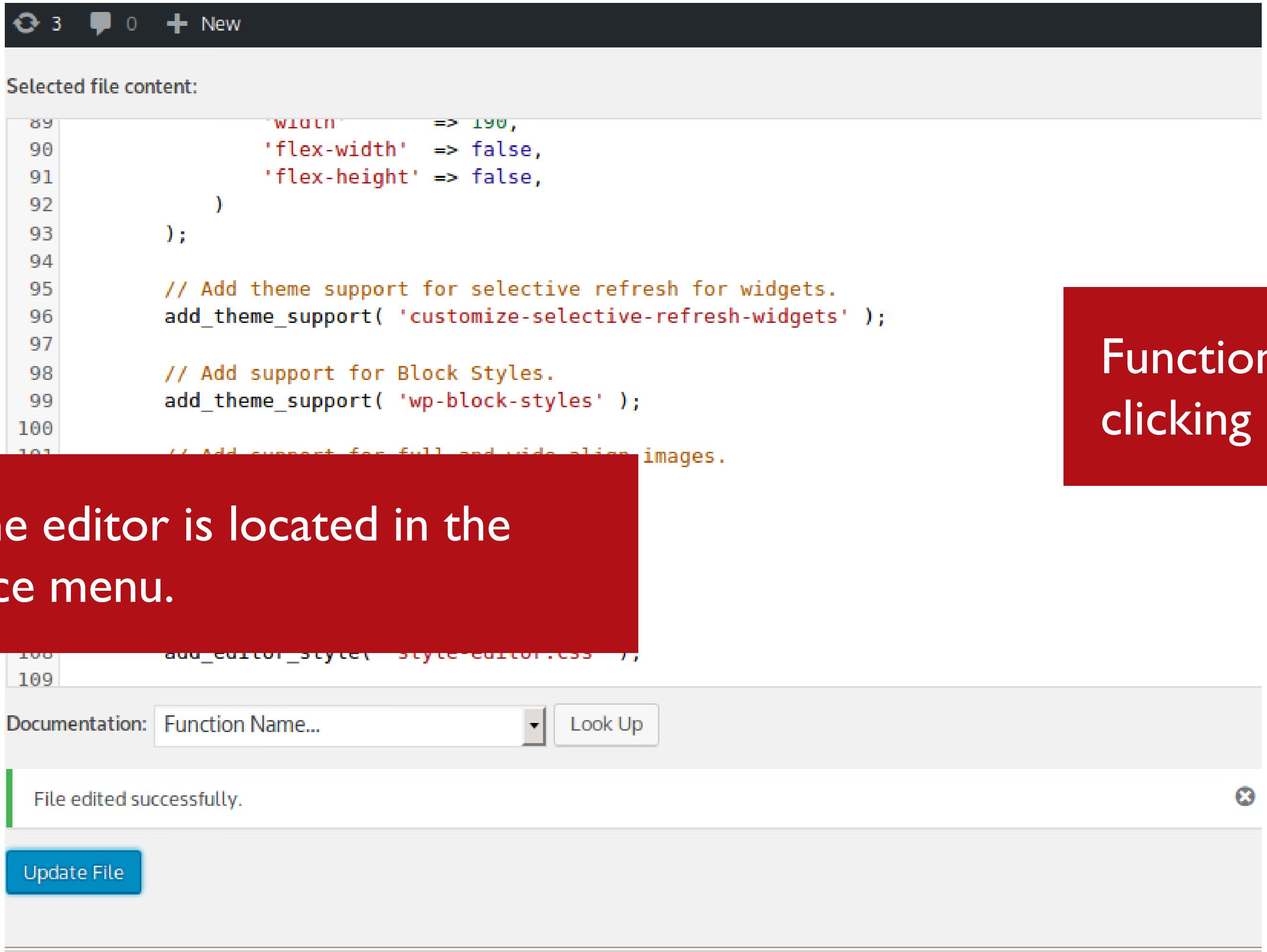
Payload type: Runtime file Request count: 0

Payload Options [Runtime file]

This payload type lets you configure a file from which to read payload strings at

EXERCISE: WORDPRESS RCE
LOCATING THE THEME EDITOR





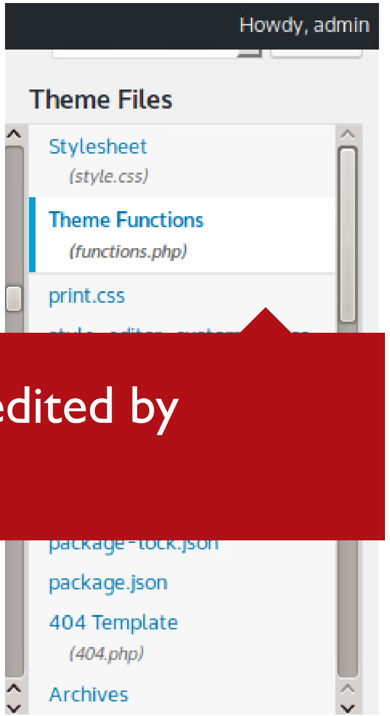
Selected file content:

```
                'width'         => 190,
                'flex-width'  => false,
                'flex-height' => false,
            )
        );

        // Add theme support for selective refresh for widgets.
        add_theme_support( 'customize-selective-refresh-widgets' );

        // Add support for Block Styles.
        add_theme_support( 'wp-block-styles' );

        // Add support for full and wide align images.
        add_editor_style( 'style-editor.css' );
```

Documentation: Function Name...

File edited successfully.

The theme editor is located in the appearance menu.



Functions.php can be edited by clicking it here

EXERCISE: WORDPRESS RCE
CONCLUSION WORDPRESS RCE

WordPress being one of the most popular CMS's on the internet has many ways to be abused.

A simple login on a default installation of WordPress, or one that has not been heavily modified can lead to RCE.

This exercise shows one of many dozen ways that an attacker can very simply and subtly backdoor WordPress