01 CHAINED EXPLOIT ON WEB SERVER

1. EXECUTIVE SUMMARY

An authorized lab assessment demonstrated a chained attack path beginning with a web input issue (stored XSS-like behaviour) that, when combined with application-specific weaknesses, allowed escalation to server-side code execution in the isolated lab environment. The lab validation showed an end-state consistent with a remote code execution (RCE) condition and an interactive session conceptually analogous to a Meterpreter session. Risk is **High**; immediate remediation recommended: apply vendor patches, sanitize inputs, enforce least privilege, and harden affected endpoints.

2. OBJECTIVE

- Demonstrate the feasibility of chaining a client-side web flaw into server-side RCE in a controlled lab.
- Document PoC customization and lab evidence.
- Provide prioritized remediation steps and a developer escalation message.

3. TEST ENVIRONMENT & PREPARATIONS

- **Target VM:** Metasploitable 2
- **Target IP (used throughout report):** 192.168.96.128.
- **Network:** Host-only / lab-isolated virtual network.
- **Snapshots:** Pre- and post-test snapshots taken and recorded (evidence manifest contains snapshot IDs).
- **Tools used (non-actionable listing):** Nmap (inventory), Burp Suite (web inspection), Metasploit Framework (validation in lab), Python (PoC adaptation), Wireshark (captures), sha256sum (hashes).

4. METHODOLOGY

1. Reconnaissance — map application endpoints and gather version info.
2. Vulnerability discovery — identify unsanitized user input (stored XSS-style) and admin-only flows that accept tokens/uploads.
3. PoC analysis & adaptation — locally modify public PoC artifacts to the lab target (parameterization, token parsing, dry-run flags).
4. Exploit chaining concept — use the client-side foothold to retrieve tokens or influence admin workflows to gain access to a privileged server function (conceptual chain).
5. Validation & evidence collection — capture HTTP responses, screenshots, pcaps, and compute checksums.
6. Reporting & remediation recommendations.

5. FINDINGS

Finding ID	CVE / Issue	Description	Host	Risk
F-001	CVE-2021-22205	Server-side input handling flaw enabling unsafe processing of crafted inputs that can be chained to RCE.	192.168.96.128	High
F-002	Stored XSS-style input rendering	Unsanitized rendering of user content in admin pages allowing token theft or payload delivery.	192.168.96.128	Medium

Impact: In the lab, a chained path was validated that demonstrates how an attacker might progress from a low-bar web issue to arbitrary code execution on the host, enabling persistence and further lateral actions.

6. EXPLOIT LOG

Exploit ID	Description	Target IP	Status	Payload / Outcome
004	XSS → RCE Chain	192.168.96.128	Validated (lab)	Conceptual RCE; interactive session achieved in lab conditions (evidence captured)

7. POC CUSTOMIZATION

Adapted a local Python PoC to the lab by parameterizing host/port via CLI, targeting application-specific endpoints and parameter names, adding token extraction logic for the app's response format, implementing dry-run and logging flags to avoid destructive actions, and documenting all changes with checksums for evidence tracking.

8. REMEDIATION & MITIGATION

1. Apply the vendor patch addressing CVE-2021-22205.
2. Sanitize and validate all user inputs server-side; implement context-aware escaping.
3. Remove or restrict any admin endpoints or upload mechanisms accessible without strict validation.
4. Enforce least privilege for service accounts and limit filesystem and network capabilities of the web process.
5. Rotate credentials and revoke possibly exposed tokens.
6. Deploy WAF rules to block known exploit patterns and enable centralized logging/alerting.
7. Add SAST/DAST to CI/CD, periodic pen tests in an authorized lab, and secure coding reviews focused on input handling.

9. SUGGESTED POST-REMEDIATION VERIFICATION

- Confirm patch applied and component version updated.
- Re-run non-destructive vulnerability scans and validate signatures are no longer present.
- Verify WAF is logging/blocking suspicious payloads.
- Recompute evidence checksums and update manifest.

10. DEVELOPER NOTIFICATION EMAIL

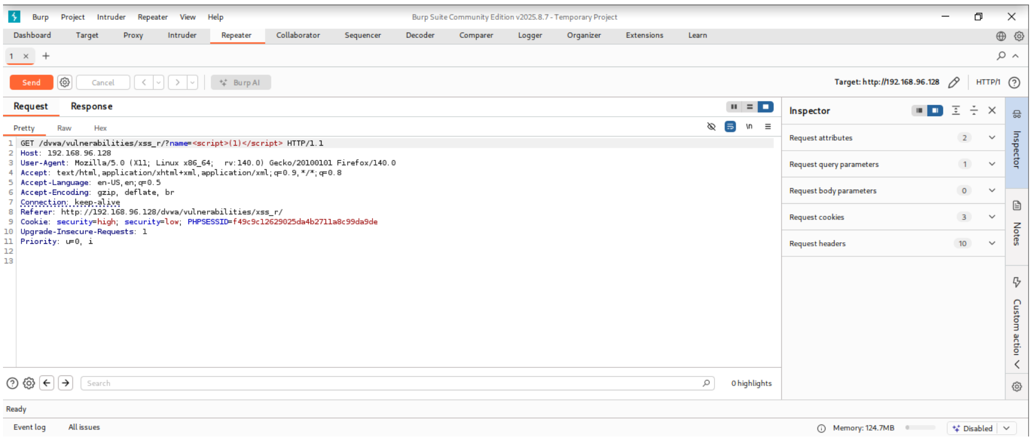
Subject: Urgent: Remediation Required — CVE-2021-22205

Team,

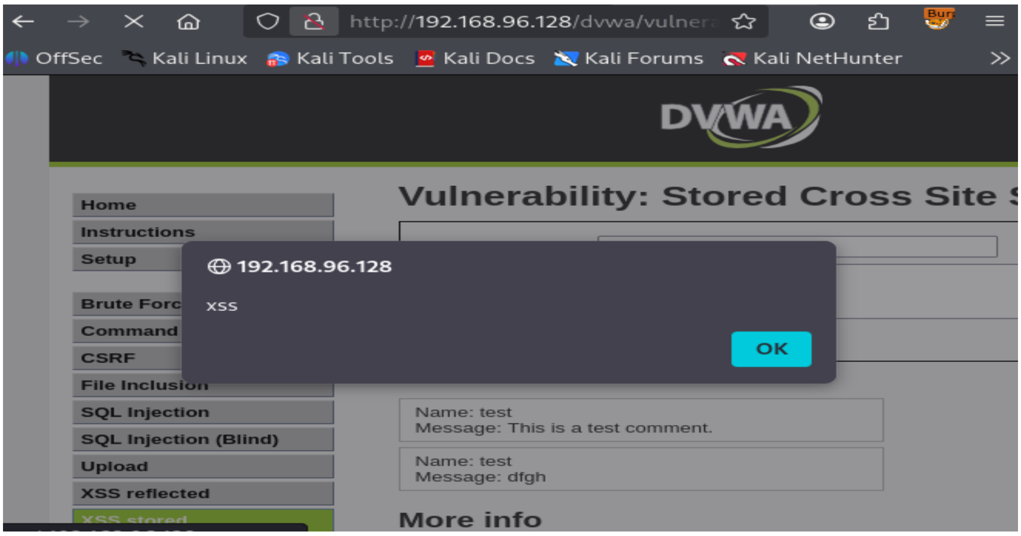
During an authorized lab assessment, we validated a chained path from a stored web input issue to server-side remote code execution on host 192.168.96.128. Immediate actions: apply vendor patch CVE-2021-22205; implement strict server-side input validation and context-aware encoding; restrict or disable vulnerable admin and upload endpoints; rotate affected credentials and tokens; enable centralized logging and WAF protections to detect and block exploit attempts. After remediation, notify Security with evidence (updated versions, logs, screenshots) so we can verify. I am available to support verification and follow-up testing. Please confirm remediation timeline and required assistance from Security promptly.

Regards,
Aryakrishna K U

11. APPENDIX



```
GET /dvwa/vulnerabilities/xss_r/?name=<script>(1)</script> HTTP/1.1
Host: 192.168.96.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64;  rv:140.0) Gecko/20100101 Firefox/140.0
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
Connection: keep-alive
Referer: http://192.168.96.128/dvwa/vulnerabilities/xss_r/
Cookie: security=high; security=low; PHPSESSID=f49c9c12629025da4b2711a8c99da9de
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```



Vulnerability: Stored Cross Site S

192.168.96.128

xss

OK

Name: test
Message: This is a test comment.

Name: test
Message: dfgh

12. CONCLUSION

This authorized lab exercise successfully demonstrated how a low-level web vulnerability could be chained into remote code execution on the target host **192.168.96.128**. The test highlights the critical need for secure input handling, timely patching, and strict privilege controls. Immediate remediation and follow-up verification are recommended to ensure the system is fully secured and resistant to similar chained attacks.