🔒 Penetration Test Report for ddark.ru

Test Date: 19.06.2025
Testing was conducted under an agreement with the site owner for external security analysis.

General Information

- Target IP: 185.26.122.21 (serv21-26.hostland.ru)
- Domain: ddark.ru
- Hosting Type: Shared hosting (JustHost)
- Open Ports:
    - FTP (ProFTPD) — 21
    - HTTP (nginx) — 80
    - HTTPS (nginx) — 443
    - SSH (OpenSSH 8.0) — 1024
    - MySQL 5.7.44 — 3306

---

1. Critical Vulnerabilities (OpenSSH 8.0)

CVE-2023-38408 — Remote Code Execution (RCE) via the Forwarded-agent mechanism. An attacker can exploit a compromised server to execute arbitrary code on the client machine.
➡️ Solution: Update OpenSSH to the latest version. Restrict SSH access by IP and disable agent forwarding.

CVE-2020-15778 — Path traversal vulnerability via `scp` commands. Allows attackers to write files to arbitrary directories.

➡️ Solution: Update OpenSSH and use secure flags when executing `scp`.

CVE-2019-16905 — Local privilege escalation in the Linux kernel. Exploiting improper capability handling can lead to root access.
➡️ Solution: Update the Linux kernel and restrict local access.

CVE-2021-41617 — Denial of Service (DoS) vulnerability in OpenSSH due to improper handling of the `AuthorizedKeysCommand` configuration.
➡️ Solution: Update OpenSSH and validate configuration files.

Additional Exploits (GitHub / ExploitDB): Confirmed proof-of-concept exploits are available for OpenSSH 8.0, increasing the likelihood of real-world exploitation.

---

2. Medium Severity Vulnerabilities

CVE-2023-51385 — Session validation bypass in some web authentication systems. Could allow session hijacking without re-authentication.
➡️ Solution: Update backend software and enforce secure session logic.

CVE-2023-48795 — Buffer overflow vulnerability when parsing specific data. May lead to crashes or arbitrary code execution.
➡️ Solution: Update the server or affected parsing libraries.

CVE-2020-14145 — Denial of Service in SMBv3 due to improper packet processing.
➡️ Solution: Apply Microsoft security patches. Limit open ports.

CVE-2016-20012 — Privilege escalation through vulnerable kernel components.
➡️ Solution: Update the kernel and implement user access restrictions.

CVE-2025-26465 — Newly published vulnerability, details currently unavailable. Potential risk.
➡️ Solution: Monitor updates and CVE advisories. Implement IDS/monitoring.

---

3. Configuration Issues

Missing HSTS (Strict-Transport-Security) — Browser does not enforce HTTPS, leaving the site vulnerable to SSL stripping.
➡️ Solution: Add HSTS header and configure 301 redirect from HTTP to HTTPS.

Missing X-Frame-Options — Site can be embedded in an iframe, enabling clickjacking attacks.
➡️ Solution: Set `X-Frame-Options: SAMEORIGIN` or `DENY`.

Missing X-Content-Type-Options — Browsers may guess content type, increasing the risk of XSS.
➡️ Solution: Add header `X-Content-Type-Options: nosniff`.

ETag includes inode and meta-info (CVE-2003-1418) — Metadata leakage may be used for user tracking or cache-related attacks.
➡️ Solution: Remove or reconfigure ETag headers.

Content-Encoding: deflate — Combined with sensitive data, this can lead to BREACH attacks via compression analysis.
➡️ Solution: Disable compression on sensitive pages (e.g., login forms).

Exposed system files and directories (.git, .svn, .htaccess) — Even if returning 403, presence indicates misconfiguration and possible exploitation.
➡️ Solution: Remove or restrict access to these paths at the server level.

---

4. Recommendations and Conclusions

Server Security

- Update OpenSSH and the Linux kernel.
- Restrict SSH access by IP.
- Hide software version information.
- Remove unused directories like /phpmyadmin and /webmail if not in use.

Web Server Configuration (LiteSpeed/nginx)

Add to `.htaccess` or server config:

```
Header always set Strict-Transport-Security "max-age=63072000;
includeSubDomains; preload"

Header set X-Frame-Options "SAMEORIGIN"

Header set X-Content-Type-Options "nosniff"

Header unset ETag

FileETag None
```

General Measures

- Deploy WAF and restrict access to admin panels via IP or VPN.
- Set up IDS/IPS systems.
- Perform regular audits and updates.

This report was prepared to improve site security and protect user data.