Cowbell Shop 8 - SSRF

Security questions

1. Explain the security problem

The server makes a download request to a website by the given URL. The main security problem here is there is no checking where the request is going.

2. Explain the exploit

The server downloads the file from any given source and don't make any check. The picture on Home gives a hint that there is a picture only available from inside the network and the open "Add picture from URL" makes it possible to download any picture from any source from inside the network/from the server.

3. Explain mitigation (how this can be fixed)

- Make input validation and only allow http: and not ftp:, dict:, etc.
- Use standard libraries
- Make unit tests
- Use a WAF
- Validate requested IP
- Least privilige
- Firewall restrictions Local and on physical/virtual FW
- Isolte webserver
- Response handling
- Logging
- Add authentication