Assignment 4: Websec

Computer and Network Security 2019

Brian Johannesmeyer, Elia Geretto

Goals

- Again, to show that you’re more than just a script kiddie
- To train and test your ability to perform the attacks discussed in the websec classes
- To train and test your ability to perform **blind attacks** (without source code)

What to do

- You will receive an email with login info for a webserver you have no direct access to
  - In particular: no source code available
  - Hence: more trial and error than in previous assignments
- You should exploit the websites to obtain hidden secrets
- The secret is a flag
  - Example flag: “flag{clWoLI7oXSkFxwjU}”

Important rule

- Grade Penalties!
  - Do not abuse flaws in Linux, Apache, PHP, …
  - Do not use automated tools and/or vulnerability scanners that can cause heavy network loads e.g. nmap, sqlmap, etc.
  - No DOSing
- Instead attack
  - Vulnerabilities in scripts and binaries we wrote
  - Configuration errors (including but not limited to guessable usernames/passwords)
  - Insecure cryptography

Tools

- Scoreboard (url in email)
  - Updated every minute
- Browser (incl. debug tools)
- Proxy server: Burp, Charles, ngrok, …
- wget (more versatile than you think)
- Packet sniffer: Wireshark, tcpdump, …
- Binary analysis: objdump, IDA Pro, …
- Most important: creative thinking

Submission

- Deadlines and submission will be handled through Canvas.
- Submit a “<hacker-handle>.txt” plain-text ASCII file, listing for each challenge you have beaten:
  - The flag you got
  - Explanation of how you hacked the challenge
  - Preferred format: as brief as possible while still containing all necessary steps

Grading

- The base grade is the number of challenges you've beaten
- Final grade is affected by the number of hints you got from cns@vusec.net
- The "speed" term is computed by sorting students by #levels beaten, then by time (like asg3).
- Documentation must be handed in before the deadline
  - If documentation is submitted late, submission time is counted instead

Questions?