Command Injection

Saturday, November 4, 2017 11:53 AM

- Command injection attacks represent a serious threat to any parameter-driven site
- The methods behind the attack are easy to learn and the damage caused can range from considerable to complete system compromise
  - Despite these risks an incredible number of systems on the internet are susceptible to this form of attack
- It is always good practice to sanitize all input data, especially data that will be used in OS commands, scripts, and database queries

Solution

- Use Webscarab
- Click View on the website
- Intercept the request
- Append "& <your os command>
  - To the Value column of HelpFile
- E.g. "& netstat -an & ipconfig

- Can also encode this in Unicode