

- Filename: eccouncil-ceh31250-v12-14-1-1-web-app-basics.md
- Show Name: CEHv12 (312-50)
- Topic Name: Web Application Hacking - Hacking Web Applications
- Episode Name: Web App Basics

=====

Web App Basics

Objectives:

- Is this a concept and vocabulary episode?
 - Absolutely! :)
- So define a Web Application for us.
 - An in-browser software application that allows users to interact with remote resources via web technologies like...
 - HTTP
 - PHP
 - Python
 - JavaScript
- Can you explain the SOAP and REST web services?
 - SOAP (Simple Object Access Protocol)
 - XML-based requests and responses
 - Web Services Description Language (WSDL)
 - Defines how the web service works
 - REST (REpresentational State Transfer)
 - URL-based requests
 - Uses HTTP Methods/Verbs to perform tasks
 - GET
 - POST
 - PUT
 - DELETE
- What are the common security risk types associated with web apps?
 - We're going to take a closer look at the OWASP Top10, but real quick
 - Injections
 - Security Misconfigurations
 - Broken Access
 - Using Components with Known Vulns
- How about security defenses?
 - Security testing
 - SAST
 - DAST
 - Tools for automated and manual security testing
 - Just google it! :)
 - Fuzz testing
 - Checking inputs
 - Size
 - Char type
 - Fuzz strategies
 - **Mutation** = takes normal data and transforms it
 - **Generation** = takes the input model that was provided by the user and breaks

it down into pieces

- Then it fuzzes by generating new random input, while maintaining the original model structure.
 - **Protocol-based** = forges packets based off of protocol specific functionality

- Encoding

- base64
- od
 - `echo -n "this is some text" | od -A n -t x1`
- Programming languages
 - Python3
 - `encoded_text = base64.b64encode(b"This is some text")`
 - <https://gchq.github.io/CyberChef/>

- Whitelisting and Blacklisting

- Content Filtering / Input Sanitization

- WAF

- RASP (Runtime Application Self Protection)

- Intercepts all calls from the app to the system
 - Verifies they don't do anything deemed 'unsafe'
 - <https://www.contrastsecurity.com/knowledge-hub/glossary/rasp-security>

- Bug Bounty programs

- <https://www.bugcrowd.com>
- <https://www.hackerone.com>