Writing reports

Setting up Burp Proxy

HTTP basics

Cookie security

HTML parsing for hackers

MIME sniffing

Encoding sniffing

Same-origin policy

Cross-site request forgery

Cross-site scripting

- Reflected
- Stored
- DOM
- Detection, exploitation, and mitigation

Authorization bypasses and forced browsing

Directory traversal

Command injection

SQL injection

- Detection, exploitation, and mitigation
- Exploiting blind SQLi

Session fixation

Clickjacking

File inclusion vulnerabilities

File upload vulnerabilities

Null termination

vulnerabilities

Unchecked redirects

Secure password storage

Crypto crash course

- XOR
- Symmetric ciphers
  - *Stream*
  - *Block*
- Asymmetric ciphers
- Hashes
- MACs

Crypto attacks

- Stream cipher reuse
- ECB block reordering
- ECB partial decryption
- Padding oracles
- Hash length extension

Crypto tricks

- Detecting ECB
- Determining block sizes
- Determining controllable data offsets

NEW CONTENT

Planned Content Launches - 2018

May: *Lightweight Threat Modeling*

June: *Writing Good Reports*

July: *Introduction to Burp Suite*

August: *Intermediate Burp Suite Techniques*

August: *Advanced Burp Hacks for Bounty Hunters*

September: *Secure Architecture Review*

October: *SSRF*

November: *Source Review Techniques*

December: *Cookie Tampering Techniques & XML External Entity Attack*

Version: 1.1 | Last Updated: 2018-05-25