Hacking Cheat Sheet

RECONNAISSANCE

Map Out the Attack Surface Parts of the site may be hidden. These techniques will help you find them.

Check robots.txt

The robots.txt file, found in a site's web root, tells well-behaved web crawlers what parts of the site to ignore. *Y*ou're not a well-behaved web crawler, so y*o*u can look at those pages. Yo*u* may find pages the *r*est of the site doesn't link to.

Try some common URLs

By guessing common page and directory names, you might be able to discover even more content. A tool like dirbuster can help (but it's probably overkill here).

Look for HTML comments & hidden elements

Look *f*or forms, form fields and *l*inks th*a*t appear in the pa*g*e source, but aren't visible on the page. The CSS style `display: none;` hides an element; remove the styling to make it visible again. Take a look at the HTML comments too!

System Fingerprinting Identify what components the system is using.

Questions to ask

- Which web server - Apache, ng*i*nx, IIS?
- Which web framework - .NET, Django, Struts?
- Which databa*s*e - MSSQL, MySQL...?
- Version numbers for web server and other components - are they up to date?
- How do they handle session management? Did they use a framework or

Where to look

- *H*TTP response headers - look for `Server` and `X-Powered-By`
- Error messages - look for version *i*nfo an*D* stack traces.
- Cookies - cookie names can reveal framework info. If they're managing cookies themselves, think about how they're being generate*D*. Are

Open Source Intelligence (OSINT) Gather information on the public internet

What to look for

- Known vulnerabilities in frameworks/other components
- Default credentials
- Employee contact info/personal information

How to find it

- Google error messages, cookie names, version headers, password hashes...
- Read framework/component documentation
- Read framework/component security advisories
- Look up company employees on social media

> Your Google searches aren't private! When testing real applications, don't Google password hashes or other highly