

Ethical Hacking/Penetration Testing & Bug Bounty Hunting v2



❖ Introduction:-

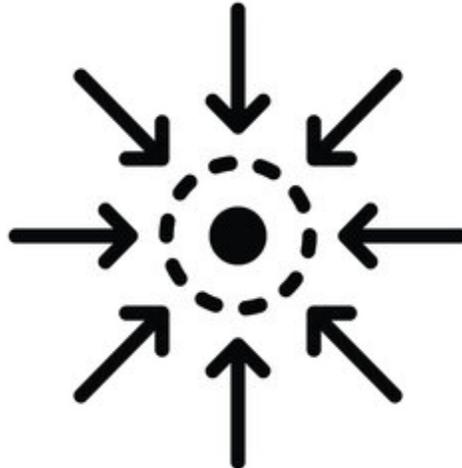
In a digital landscape teeming with complexities and vulnerabilities, the role of ethical hackers and penetration testers has never been more crucial. The relentless surge of cyber threats demands a new breed of cybersecurity professionals who are not only equipped with technical prowess but also possess an unyielding commitment to safeguarding digital assets. Welcome to the transformative Udemy course "Ethical Hacking / Penetration Testing & Bug Bounty Hunting v2." This article serves as your guide to understanding the rich tapestry of topics covered in this course, enabling you to embark on a journey that combines technical mastery with ethical responsibility.

❖ Introduction to Broken Link Hijacking:-



Broken link hijacking occurs when a website link is broken or inactive, and attackers exploit it by redirecting the link to a malicious website. Instead of reaching the intended content, users are redirected to harmful sites, leading to potential security risks. This technique is a form of cyber threat that takes advantage of the trust users have in legitimate links,

❖ **Impact of Broken Link Hijacking:-**



Misleading Users: Visitors expecting one thing may end up on an unintended site, leading to confusion.

Trust Issues: It damages the trust users have in the website, as they may question the reliability and security of the content.

Security Risks: Redirected links may lead to harmful websites, exposing users to potential cybersecurity threats.

SEO Consequences: Search engines may penalize the website's ranking due to broken links and redirections, affecting online visibility.

Brand Damage: Broken link hijacking harms a website's reputation, impacting the perception of its brand.

Loss of Traffic: Users may leave the site if they encounter broken links, resulting in a loss of valuable traffic.

Legal Concerns: If the redirected content is inappropriate or illegal, the website owner may face legal consequences for unwittingly hosting such material.

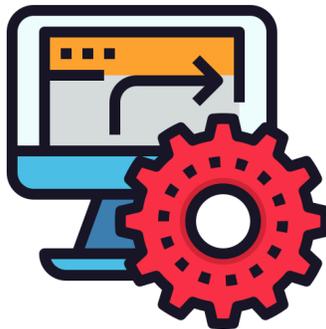
❖ Strategies and technique to Prevent broken link hijacking

Broken link hijacking is a type of web attack that exploits external links that are no longer valid. Attackers can take advantage of resources or third-party services that are no longer available or valid, such as due to expired domains, to carry out various harmful activities, including defacement through acquiring expired domains, impersonation, or even cross-site scripting.

1. Regularly check for broken links: Proactively identify stale or dead links on your website and remove them. Intelligent vulnerability scanning tools like AppTrana can identify thousands of vulnerabilities, including potential broken links and defacements



2. Use automated tools: Automated tools can handle the detection and fixing of broken links on websites of any size, ensuring comprehensive coverage. With automated methods, you can fix broken links in bulk rather than addressing them one by one. This can be especially useful for large websites with a high volume of broken link



3. Monitor and inspect broken links: Regularly scrape your own website, tweets, and other online content to inspect broken links and audit all outbound links



4. **Implement security measures:** Implement security mechanisms to protect your website from broken link hijacking, such as rate limiting, allowing only a certain number of attempts or a time limit for accessing external links



5. **Use tools to check for broken links:** There are several tools available to check for broken links, including Dead Link Checker, a free broken link checker on GitHub, and an expired domain checker for tweets.



6. **Stay updated on best practices:** Keep up-to-date with the latest best practices for securing your website, such as implementing proper security measures, regularly checking for broken links, and using intelligent vulnerability scanning tools



Introduction to Broken link Checker

Broken Link Checker is a web tool that scans websites for broken or dead hyperlinks. It helps users identify and fix URLs that no longer work, improving the overall user experience. The tool crawls through a website, detecting broken links and providing a report with details on each broken URL.

This helps webmasters maintain the integrity of their sites and ensures a smoother navigation experience for visitors."

Steps to use:-

1. Visit this link <https://ahrefs.com/broken-link-checker> and enter the target name.

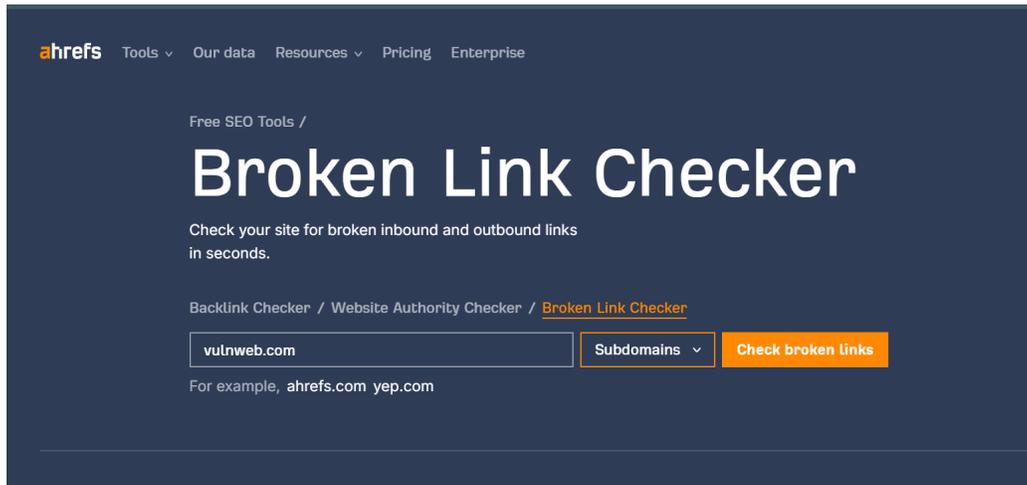


Figure:- The above figure shows the interface of broken link checker

2. Then it will show the broken link.

Broken links for vulnweb.com ×
Domain including subdomains

Broken links on your site [ⓘ] Broken links to your site [ⓘ]
6.9K **54K**
15% dofollow

[Broken outbound links](#) / [Broken inbound links](#)

Referring page [ⓘ]	Int. [ⓘ]	Ext. [ⓘ]	Anchor and backlink [ⓘ]
http://testphp.vulnweb.com/redirect.php?r=https://www.reddit.com/r/StudentPortal/comments/vyuffo/best_essay_writing_service_reddit_users/	0	1	https://www.reddit.com/r/StudentPortal/comments/vyuffo/best_essay_writing_service_reddit_users/ 404
http://testphp.vulnweb.com/redirect.php?r=https://www.reddit.com/r/StudentPortal/comments/wdg7to/where_to_hire_essay_writing_service_reddit_users/	0	1	https://www.reddit.com/r/StudentPortal/comments/wdg7to/where_to_hire_essay_writing_service_reddit_users/

http://testphp.vulnweb.com/udir.php? r=https://www.reddit.com/r/StudentPortal/c omments/wdhm0j/what_is_the_best_pay_for _essay_reddit_company_to/	0	1	https://www.reddit.com/r/StudentPortal/co mments/wdhm0j/what_is_the_best_pay_for_ essay_reddit_company_to/ 404
http://testphp.vulnweb.com/udir.php? r=http://sixs6spkr.com	0	1	http://sixs6spkr.com/ Can't resolve host
http://testphp.vulnweb.com/udir.php? r=https://backlink.ombackilnk.eu.org/ /	0	1	https://backlink.ombackilnk.eu.org/ / 404
http://testphp.vulnweb.com/udir.php? r=https://www.backlink.ombackilnk.eu.org	0	1	https://www.backlink.ombackilnk.eu.org/ Can't resolve host
http://testphp.vulnweb.com/udir.php? r=https://www.techbeats.org/modern- setup-host	0	1	https://www.techbeats.org/modern-setup- host 404

Figure:- The above figure shows the list of URLs which are vulnerable to broken link hijacking.

Reference:-

1. <https://ahrefs.com/broken-link-checker>