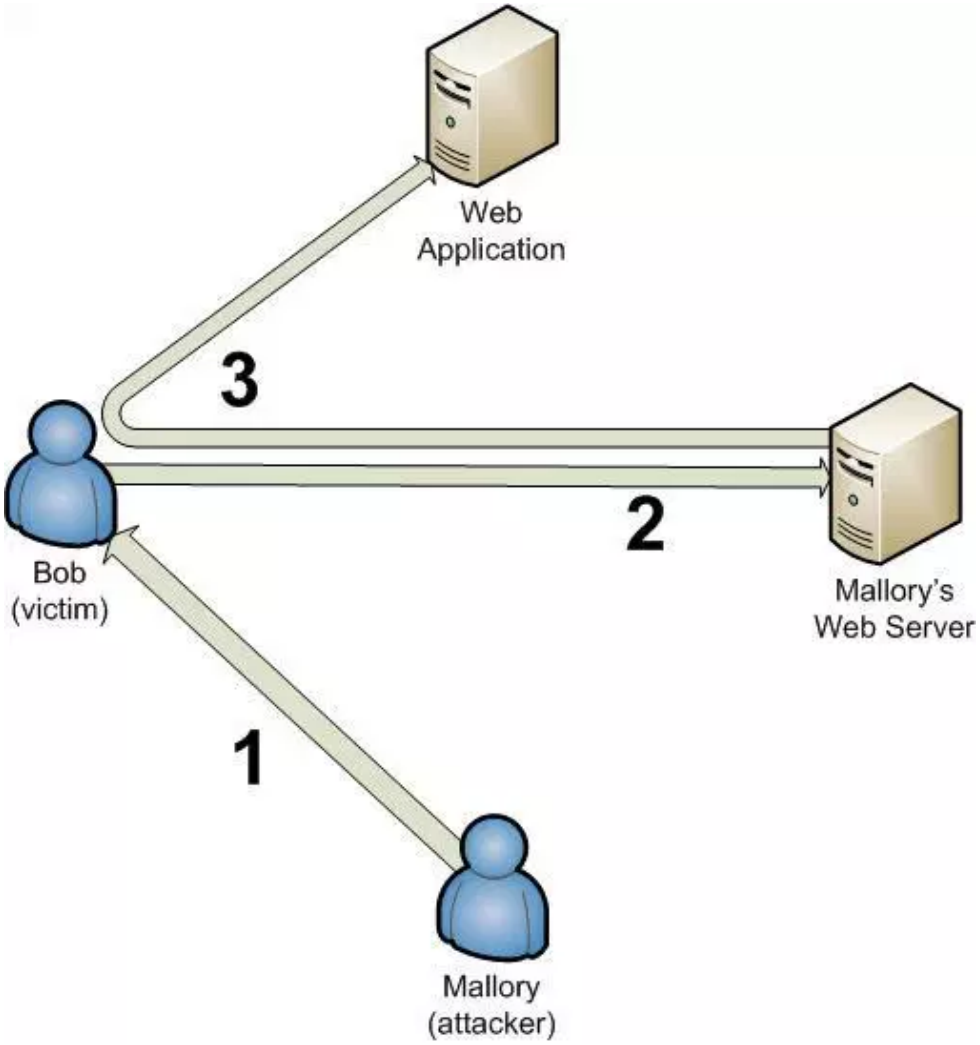
OWASP - Top 10

A8-Cross-Site Request Forgery (CSRF)

By **GURUBARAN S** - December 21, 2016 4



Cross Site Request Forgery is one of the most common form of attack by online spammers and scammers. Exploicity of this attack is bit complex, it's prevalence is common.

Most Popular

Black Hat Asia 2018 – A Biggest Hackers Conference to Meet...

January 26, 2018

New Malware Campaign Trick Victims as an Adobe Flash Player Installers

January 9, 2018

Uber Data Breach Exposed Personal

But CSRF attacks can be predicted easily and their impact is moderate.

CSRF scenario

Information of 57 Million Uber Users…

November 22, 2017

Man Hacked into Jail Computer Network to Change his Friend Release…

December 5, 2017

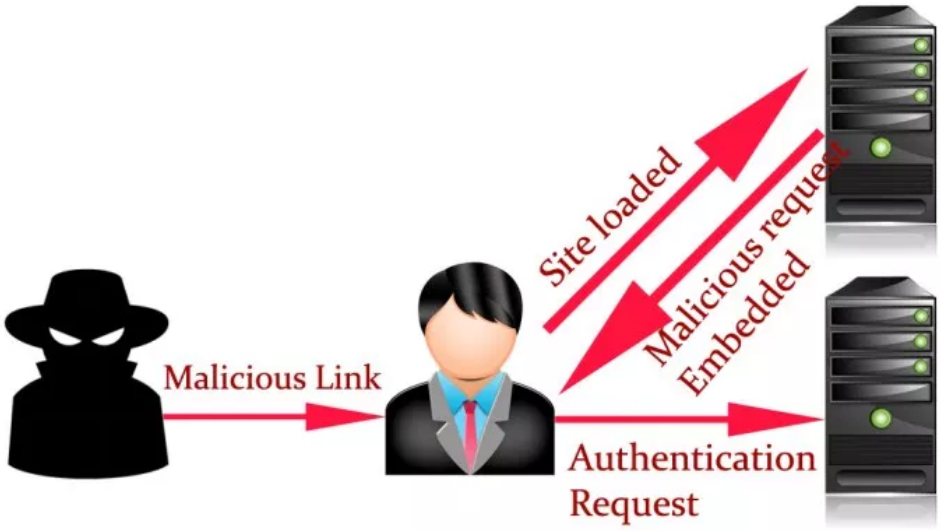
Thousands of Servers Running etcd Leaking Credentials Online – Mitigation's

March 26, 2018

Recommended

4 Cybersecurity Risks We willl Face With New WhatsApp Status…

5 Methods to Secure Your Company's Data from Cybercriminals



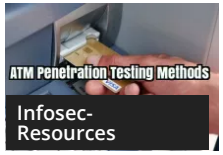
In this scenario we are having an Attacker, User, Attacker's and Target server. Attacker can share the malicious link to user's through Multiple ways.

Link sharing can be done through Social Media, Email and with many of different ways. Once the User click's on the link, then the link goes to the attackers webserver.

Now the request from attackers server also carries the **Embedded Malicious request**, which causes the user browser to issue a request to the target website.

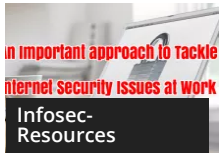
A perfect way to Start and Strengthen your Cyber Security Career

Adobe & Microsoft released New Critical Security updates for software...

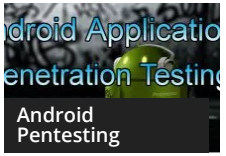


Advanced ATM Penetration Testing Methods

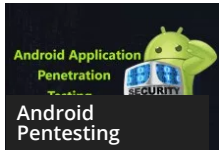
All that You Should Know About Bitcoins and How Does Bitcoin...



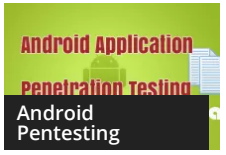
An Important Protection Approach to Tackle Internet Security Issues at Work



Android Application Penetration Testing – Part 1

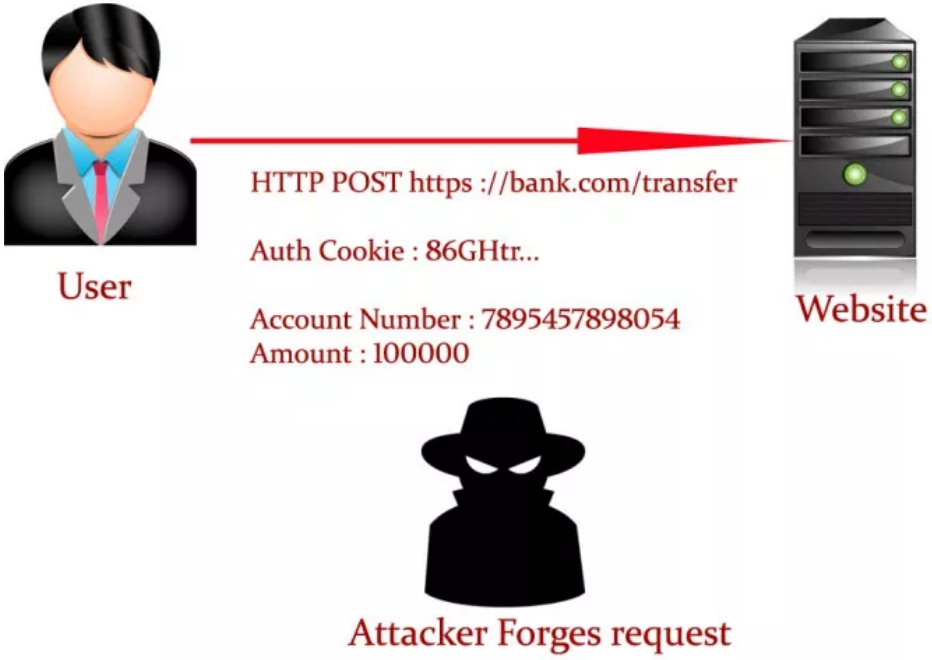


Android Application



Android Application

> *Entire process of CSRF is to get the authenticated user, who is already authenticated to the target website. So that's one of the condition normally need to meet for successful CSRF.*



Cross Site Request Forgery

Penetration Testing – Part 8

Penetration Testing – Part 9

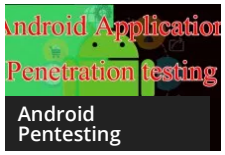
Android Application Penetration Testing – Part 10

Android Application Penetration Testing – Part 11 – Android Checklist

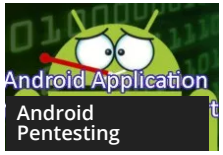
Android Application Penetration Testing – Part 12

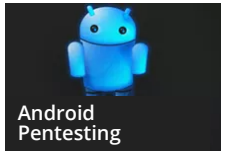
Android Application Penetration Testing – Part 5

Android Application Penetration Testing Part – 4



Android Application Penetration Testing Part 2





In this scenario we are having an user transferring money on a banking website, now the user login to bank and to make Authenticate money transfer request.

The request should be like this HTTP POST http://bank.com/transfer, once the request processed then in-order to persist the user state server will sent an Authcookie : 86GHTR.

Android Application Penetration testing Part 3

Android Application Penetration Testing Part 6

Android Application Penetration Testing- Part 7

APT Group Cyber Attack to Hack Various Companies Web Servers Using...

Being the post request there is a request body which consist of **Target Account number : 7895457898054** and where the money **Amount : 100000** is to transfer.

Now the attacker can forge this request and he is the rub with CSRF, if the attacker can trick the user’s browser in

making this request when I may be able to successfully execute a CSRF request.

So now does an attacker execute that:
Attacker already aware of the HTTP post path, they look at the bank and tell what's the URL that you need to post to transfer money.

They already aware of the fields, so they only require the URL and request body, because if they get the user to make a request to that part with the request body.

Then the Auth Cookie will be sent automatically with the request which browsers normally do, send any cookie with the request valid for a target domain.

Cross Site Request Forgery Defenses

- CSRF is exploited if we use predictable patterns.
- Employ Anti-forgery tokens, add randomness to the request.
- Valid request should not originate externally.
- The referrer should be in each header requests.
- Native browser defenses.
- Fraud detection patterns.

Share and Support Us :

SOURCE OWSAP

TAGS Anti-forgers Authcookie CSRF OWSAP randomness

GURUBARAN S

http://gbhackers.com

Gurubaran is a PKI Security Engineer. Certified Ethical Hacker, Penetration Tester, Security blogger, Co-Founder & Author of GBHackers On Security.

RELATED ARTICLES MORE FROM AUTHOR

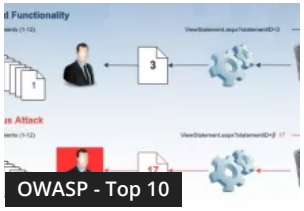
OWASP A10-Unvalidated Redirects and Forwards

A-9 Using Components with known Vulnerabilities – Every Developers Should aware

A7 Missing Function Level Access Control

A6-Sensitive Data Exposure

OWASP A5- Security Misconfiguration



A4-Insecure Direct Object References

ABOUT US

GBHackers on Security is Advanced Persistent Cyber Security Online platform which including Cyber Security Research,Web Application and Network Penetration Testing, Hacking Tutorials,Live Security Updates, Technology updates, Security investigations With dedicated Cyber security Expert Team and help to community more secure.

Contact us: admin@gbhackers.com

FOLLOW US