Web Application Security

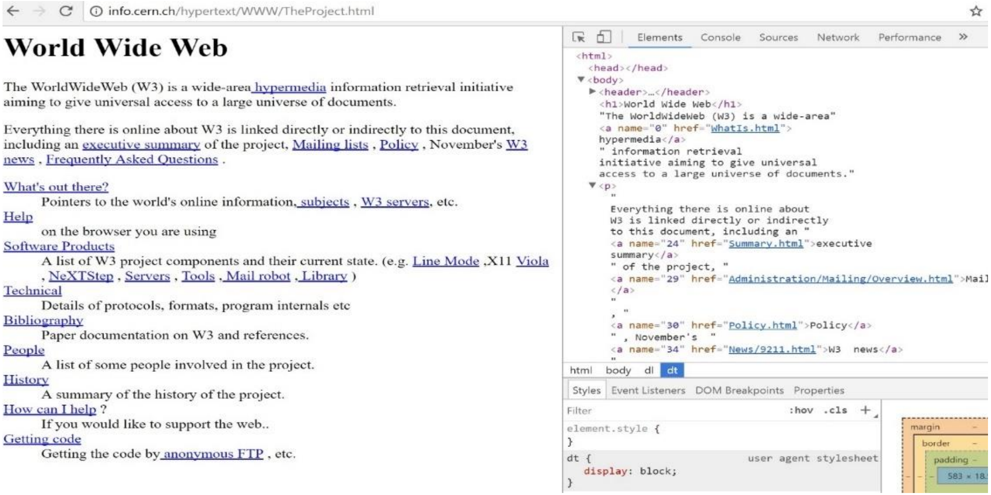
Information Security Inc.

Contents

- Web Application
- Network security threats
- Web Applications security
- Parameter Manipulation
- Cross Site Scripting (XSS)
- SQL Injection
- Google hacking
- References

Web Application

Initially static HTML based websites



World Wide Web

The WorldWideWeb (W3) is a wide-area hypermedia information retrieval initiative aiming to give universal access to a large universe of documents.

Everything there is online about W3 is linked directly or indirectly to this document, including an executive summary of the project, Mailing lists , Policy , November's W3 news , Frequently Asked Questions .

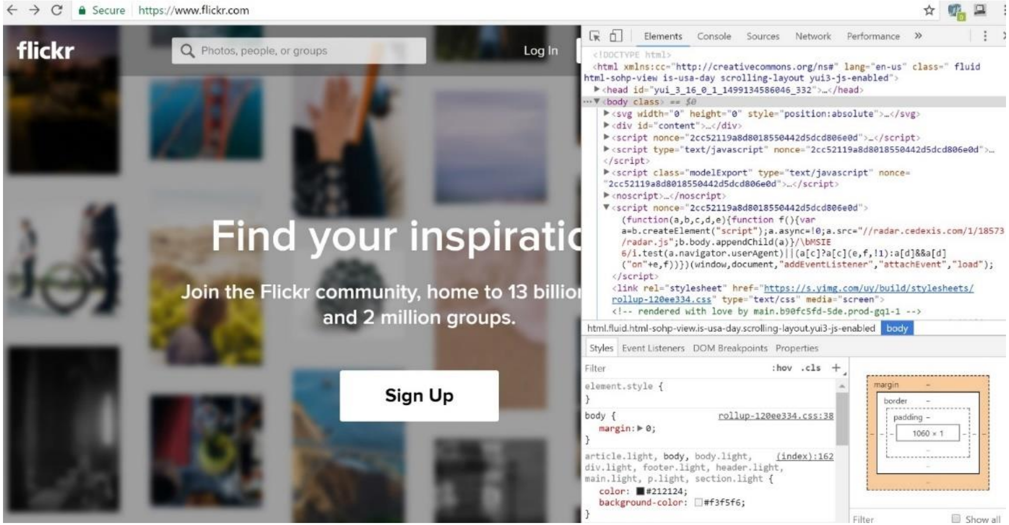
What's out there?
Pointers to the world's online information, subjects , W3 servers, etc.
Help
on the browser you are using
Software Products
A list of W3 project components and their current state. (e.g. Line Mode ,X11 Viola , NeXTStep , Servers , Tools , Mail robot , Library)
Technical
Details of protocols, formats, program internals etc
Bibliography
Paper documentation on W3 and references.
People
A list of some people involved in the project.
History
A summary of the history of the project.
How can I help ?
If you would like to support the web..
Getting code
Getting the code by anonymous FTP , etc.

```
<html>
  <head></head>
 ▼<body>
  ▶<header>…</header>
    <h1>World Wide Web</h1>
    "The WorldWideWeb (W3) is a wide-area"
    <a name="0" href="WhatIs.html">
    hypermedia</a>
    " information retrieval
    initiative aiming to give universal
    access to a large universe of documents."
   ▼<p>
      "
      Everything there is online about
      W3 is linked directly or indirectly
      to this document, including an "
      <a name="24" href="Summary.html">executive
      summary</a>
      " of the project, "
      <a name="29" href="Administration/Mailing/Overview.html">Mail
      </a>
      "
      , "
      <a name="30" href="Policy.html">Policy</a>
      " , November's  "
      <a name="34" href="News/9211.html">W3  news</a>
      "
```

```
element.style {
}
dt {                          user agent stylesheet
   display: block;
}
```

Web Application

Replaced with dynamic multi-technology based websites



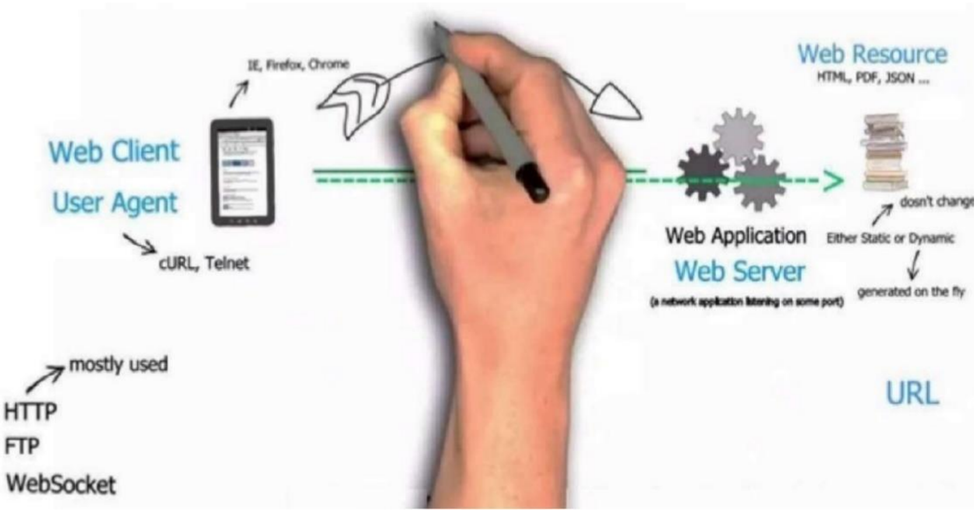
```
<!DOCTYPE html>
<html xmlns:cc="http://creativecommons.org/ns#" lang="en-us" class=" fluid
html-sohp-view is-usa-day scrolling-layout yui3-js-enabled">
 ▶<head id="yui_3_16_0_1_1499134586046_332">…</head>
…▼<body class> == $0
   ▶<svg width="0" height="0" style="position:absolute">…</svg>
   ▶<div id="content">…</div>
   ▶<script nonce="2cc52119a8d8018550442d5dcd806e0d">…</script>
   ▶<script type="text/javascript" nonce="2cc52119a8d8018550442d5dcd806e0d">…
   </script>
   ▶<script class="modelExport" type="text/javascript" nonce=
   "2cc52119a8d8018550442d5dcd806e0d">…</script>
   ▶<noscript>…</noscript>
   ▼<script nonce="2cc52119a8d8018550442d5dcd806e0d">
      (function(a,b,c,d,e){function f(){var
      a=b.createElement("script");a.async=!0;a.src="//radar.cedexis.com/1/18573
      /radar.js";b.body.appendChild(a)}/\bMSIE
      6/i.test(a.navigator.userAgent)||(a[c]?a[c](e,f,!1):a[d]&&a[d]
      ("on"+e,f))})(window,document,"addEventListener","attachEvent","load");
    </script>
    <link rel="stylesheet" href="https://s.yimg.com/uy/build/stylesheets/
    rollup-120ee334.css" type="text/css" media="screen">
    <!-- rendered with love by main.b90fc5fd-5de.prod-gq1-1 -->
```

html.fluid.html-sohp-view.is-usa-day.scrolling-layout.yui3-js-enabled body

```
element.style {
}
body {                                   rollup-120ee334.css:38
   margin: ▶ 0;
}
article.light, body, body.light,         (index):162
div.light, footer.light, header.light,
main.light, p.light, section.light {
   color: ■#212124;
   background-color: □#f3f5f6;
}
```

Web Application

Web Application structure

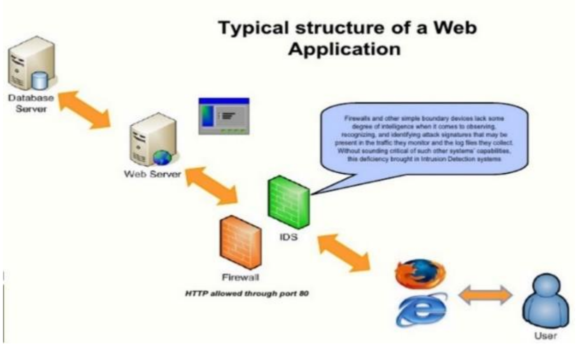


Web Application

◎Web Application structure

Security approach:

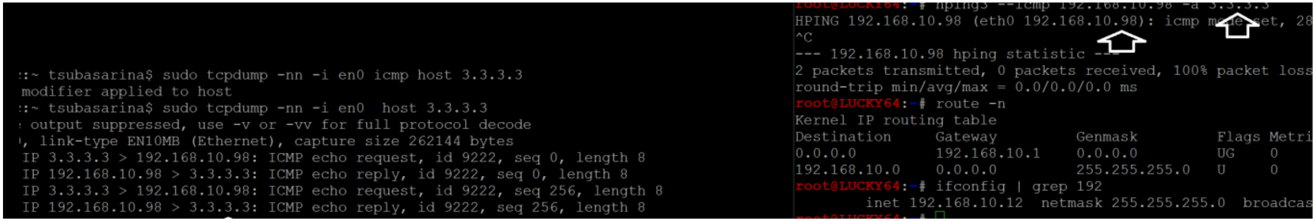
- Firewalls and other perimeter devices are deployed
- Servers are regularly patched
- Network traffic is encrypted but security bugs/vulnerabilities present at the application layer (code level) are not taken into account


Typical structure of a Web Application
Database Server
Web Server
Firewalls and other simple boundary devices lack some degree of intelligence when it comes to observing, recognizing, and identifying attack signatures that may be present in the traffic they monitor and the log files they collect. Without sounding critical of such other systems' capabilities, this deficiency brought in Intrusion Detection systems
IDS
Firewall
HTTP allowed through port 80
User

Network security threats

◎ IP spoofing

Any station can send packets pretending to be from any IP address



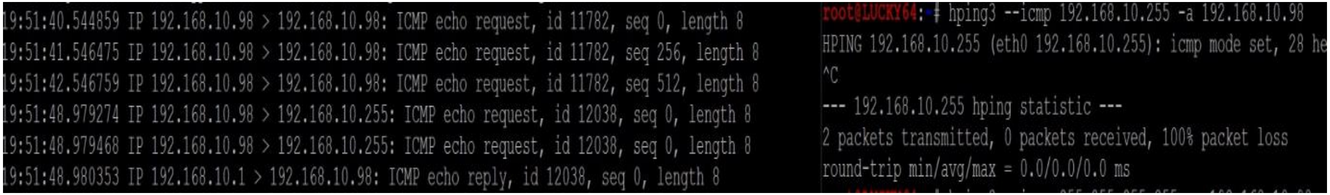
```
:~ tsubasarina$ sudo tcpdump -nn -i en0 icmp host 3.3.3.3
 modifier applied to host
:~ tsubasarina$ sudo tcpdump -nn -i en0  host 3.3.3.3
 output suppressed, use -v or -vv for full protocol decode
, link-type EN10MB (Ethernet), capture size 262144 bytes
 IP 3.3.3.3 > 192.168.10.98: ICMP echo request, id 9222, seq 0, length 8
 IP 192.168.10.98 > 3.3.3.3: ICMP echo reply, id 9222, seq 0, length 8
 IP 3.3.3.3 > 192.168.10.98: ICMP echo request, id 9222, seq 256, length 8
 IP 192.168.10.98 > 3.3.3.3: ICMP echo reply, id 9222, seq 256, length 8
```

```
root@LUCKY64:~# hping3 --icmp 192.168.10.98 -a 3.3.3.3
HPING 192.168.10.98 (eth0 192.168.10.98): icmp mode set, 28
^C
--- 192.168.10.98 hping statistic ---
2 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@LUCKY64:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metri
0.0.0.0         192.168.10.1    0.0.0.0         UG    0
192.168.10.0    0.0.0.0         255.255.255.0   U     0
root@LUCKY64:~# ifconfig | grep 192
        inet 192.168.10.12  netmask 255.255.255.0  broadcas
root@LUCKY64:~#
```

Network security threats

◎ Smurf attack

Ping a broadcast address, with the spoofed IP of a victim



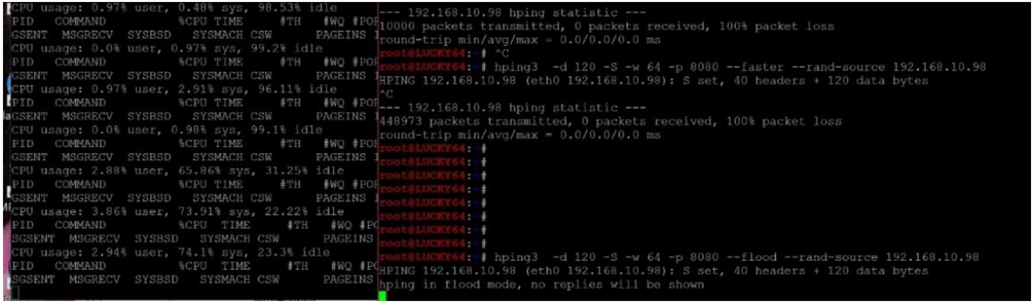
```
19:51:40.544859 IP 192.168.10.98 > 192.168.10.98: ICMP echo request, id 11782, seq 0, length 8
19:51:41.546475 IP 192.168.10.98 > 192.168.10.98: ICMP echo request, id 11782, seq 256, length 8
19:51:42.546759 IP 192.168.10.98 > 192.168.10.98: ICMP echo request, id 11782, seq 512, length 8
19:51:48.979274 IP 192.168.10.98 > 192.168.10.255: ICMP echo request, id 12038, seq 0, length 8
19:51:48.979468 IP 192.168.10.98 > 192.168.10.255: ICMP echo request, id 12038, seq 0, length 8
19:51:48.980353 IP 192.168.10.1 > 192.168.10.98: ICMP echo reply, id 12038, seq 0, length 8
```

```
root@LUCKY64:~# hping3 --icmp 192.168.10.255 -a 192.168.10.98
HPING 192.168.10.255 (eth0 192.168.10.255): icmp mode set, 28 he
^C
--- 192.168.10.255 hping statistic ---
2 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Denial of service (DOS) attack

- Form of attacking computer over a network. A malicious attempt to render a networked system unable but without permanently damaging it.

- If a lot of malicious hosts coordinate to flood the victim with an abundance of attack packets is called Distributed DOS (DDOS) attack.

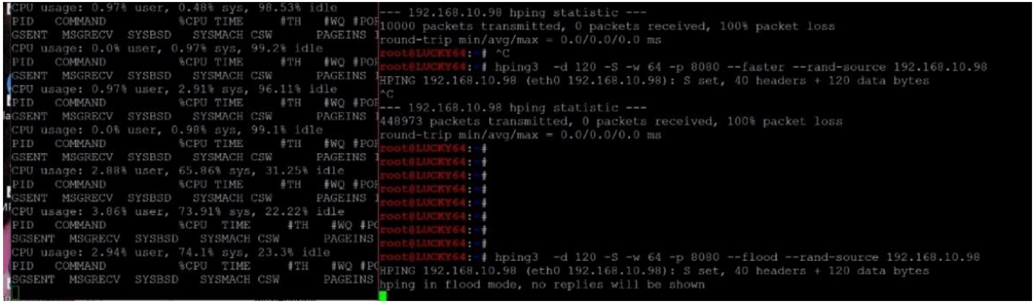


```
CPU usage: 0.97% user, 0.48% sys, 98.53% idle
PID   COMMAND          %CPU TIME     #TH   #WQ #PO
GSENT  MSGRECV  SYSBSD   SYSMACH CSW      PAGEINS I
CPU usage: 0.0% user, 0.97% sys, 99.2% idle
PID   COMMAND          %CPU TIME     #TH   #WQ #PO
GSENT  MSGRECV  SYSBSD   SYSMACH CSW      PAGEINS I
CPU usage: 0.97% user, 2.91% sys, 96.11% idle
PID   COMMAND          %CPU TIME     #TH   #WQ #PO
GSENT  MSGRECV  SYSBSD   SYSMACH CSW      PAGEINS I
CPU usage: 0.0% user, 0.98% sys, 99.1% idle
PID   COMMAND          %CPU TIME     #TH   #WQ #PO
GSENT  MSGRECV  SYSBSD   SYSMACH CSW      PAGEINS I
CPU usage: 2.88% user, 65.86% sys, 31.25% idle
PID   COMMAND          %CPU TIME     #TH   #WQ #PO
GSENT  MSGRECV  SYSBSD   SYSMACH CSW      PAGEINS I
CPU usage: 3.86% user, 73.91% sys, 22.22% idle
PID   COMMAND          %CPU  TIME     #TH   #WQ #P
SGSENT  MSGRECV  SYSBSD   SYSMACH CSW      PAGEINS
CPU usage: 2.94% user, 74.1% sys, 23.3% idle
PID   COMMAND          %CPU  TIME     #TH   #WQ #P
SGSENT  MSGRECV  SYSBSD   SYSMACH CSW      PAGEINS
```

```
--- 192.168.10.98 hping statistic ---
10000 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@LUCKY64:~# ^C
root@LUCKY64:~# hping3  -d 120 -S -w 64 -p 8080 --faster --rand-source 192.168.10.98
HPING 192.168.10.98 (eth0 192.168.10.98): S set, 40 headers + 120 data bytes
^C
--- 192.168.10.98 hping statistic ---
448973 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@LUCKY64:~#
root@LUCKY64:~#
root@LUCKY64:~#
root@LUCKY64:~#
root@LUCKY64:~#
root@LUCKY64:~#
root@LUCKY64:~#
root@LUCKY64:~#
root@LUCKY64:~# hping3  -d 120 -S -w 64 -p 8080 --flood --rand-source 192.168.10.98
HPING 192.168.10.98 (eth0 192.168.10.98): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

Fragmentation attack

Fragmentation allows oversized packets to be split to fit on a smaller network.Reassembly is difficult. Firewall and IDS may reassemble packets from how the attacked operating systems do it.

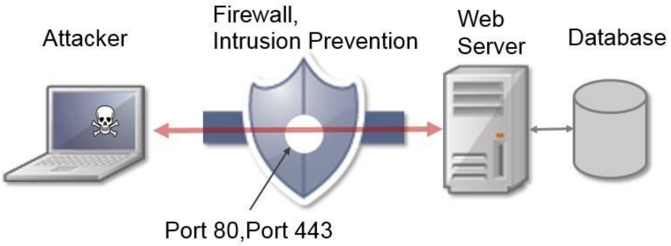


```
CPU usage: 0.97% user, 0.48% sys, 98.53% idle
PID   COMMAND          %CPU TIME     #TH   #WQ #PO
GSENT  MSGRECV  SYSBSD   SYSMACH CSW       PAGEINS
CPU usage: 0.0% user, 0.97% sys, 99.2% idle
PID   COMMAND          %CPU TIME     #TH   #WQ #PO
GSENT  MSGRECV  SYSBSD   SYSMACH CSW       PAGEINS
CPU usage: 0.97% user, 2.91% sys, 96.11% idle
PID   COMMAND          %CPU TIME     #TH   #WQ #PO
GSENT  MSGRECV  SYSBSD   SYSMACH CSW       PAGEINS
CPU usage: 0.0% user, 0.98% sys, 99.1% idle
PID   COMMAND          %CPU TIME     #TH   #WQ #PO
GSENT  MSGRECV  SYSBSD   SYSMACH CSW       PAGEINS
CPU usage: 2.88% user, 65.86% sys, 31.25% idle
PID   COMMAND          %CPU TIME     #TH   #WQ #PO
GSENT  MSGRECV  SYSBSD   SYSMACH CSW       PAGEINS
CPU usage: 3.86% user, 73.91% sys, 22.22% idle
PID   COMMAND          %CPU  TIME     #TH   #WQ #P
SGSENT  MSGRECV  SYSBSD   SYSMACH CSW       PAGEINS
CPU usage: 2.94% user, 74.1% sys, 23.3% idle
PID   COMMAND          %CPU  TIME     #TH   #WQ #P
SGSENT  MSGRECV  SYSBSD   SYSMACH CSW       PAGEINS
```

```
--- 192.168.10.98 hping statistic ---
10000 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@LUCKY64:~# ^C
root@LUCKY64:~# hping3  -d 120 -S -w 64 -p 8080 --faster --rand-source 192.168.10.98
HPING 192.168.10.98 (eth0 192.168.10.98): S set, 40 headers + 120 data bytes
^C
--- 192.168.10.98 hping statistic ---
448973 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@LUCKY64:~#
root@LUCKY64:~#
root@LUCKY64:~#
root@LUCKY64:~#
root@LUCKY64:~#
root@LUCKY64:~#
root@LUCKY64:~#
root@LUCKY64:~#
root@LUCKY64:~# hping3  -d 120 -S -w 64 -p 8080 --flood --rand-source 192.168.10.98
HPING 192.168.10.98 (eth0 192.168.10.98): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

Problems

- Large number of vulnerabilities being reported are web application vulnerabilities.
- The easiest way to compromise hosts
- For web applications to properly work, have to allow traffic (port 80,443) through the firewall



Web Application Security Issues

- Web applications extend an organization's security perimeter
- Easy accessibility for attackers as well
- Over-reliance on SSL
- Most web-applications connect back to databases containing confidential information
- Lack of security awareness amongst developers
- Coding mistakes due to pressure to build and deploy the system
- Applications vary from organization to organization

Web Application Security Issues

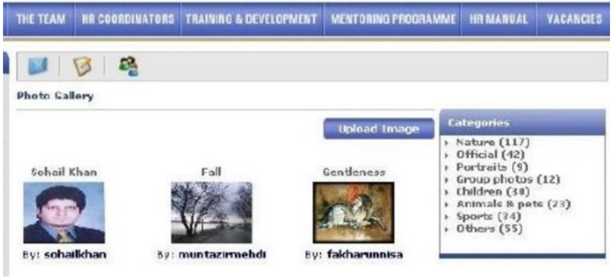
- Misconceptions:

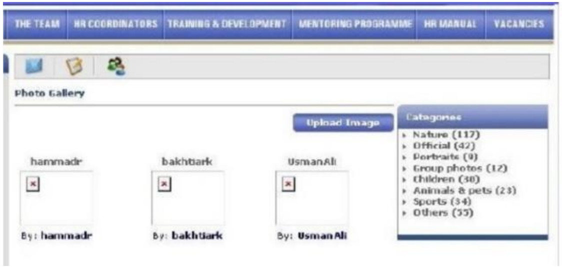
  We are secure, we use SSL
  Great at encrypting traffic
  Does not validate application input

Web Application Security Issues

◎ Basic principle:

Make the web application do something the developer never intended for it to do.





Web Application Security Issues

◎Problem: user input

- All user input is inherently evil
- Malicious input can:
  - Enable attacker to access internal databases
  - Alter flow of web applications

Web Application Security Issues

◎Root cause: Client Input

- Attacks are injected through
  - Text based forms in web pages
  - Manipulating URL addresses
  - Cookie tampering
  - Manipulation of hidden files

Parameter manipulation

◎ Several ways:

- Text based forms in web pages
- Manipulating URL addresses
- Cookie tampering
- Manipulation of hidden files

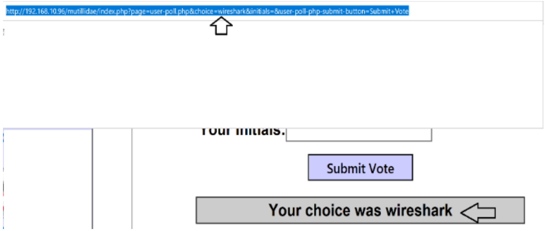
Parameter manipulation

◎Several ways: Basic examples

URLs: Will be looking at choice parameter.

http://192.168.10.96/mutillidae/index.php?page=user-poll.php&choice=wireshark&initials=&user-poll-php-submit-button=Submit+Vote

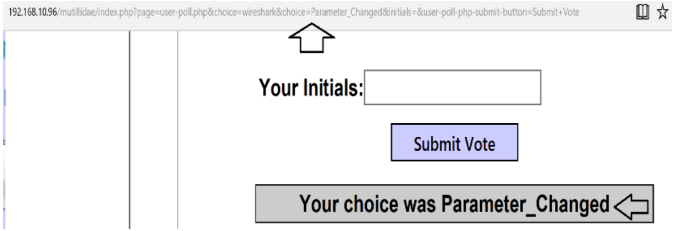
【Normal flow: choice parameter is wireshark】



http://192.168.10.96/mutillidae/index.php?page=user-poll.php&choice=wireshark&initials=&user-poll-php-submit-button=Submit+Vote

Your choice was wireshark

【Duplicate it to influence the Vote】



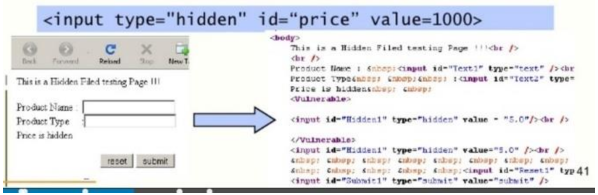
192.168.10.96/mutillidae/index.php?page=user-poll.php&choice=wireshark&choice=Parameter_Changed&initials=&user-poll-php-submit-button=Submit+Vote

Your choice was Parameter_Changed

Parameter manipulation

◎ Several ways:

- Temporary databases
- Cookies
- User sessions
- Hidden Fields in Web pages
- URLs



```
<input type="hidden" id="price" value=1000>
```

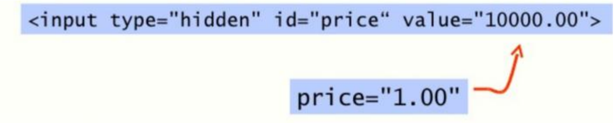
This is a Hidden Filed testing Page !!!

Product Name :

Product Type :

Price is hidden

```
<body>
    This is a Hidden Filed testing Page !!!<br />
    <br />
    Product Name : &nbsp;<input id="Text1" type="text" /><br
    Product Type&nbsp; &nbsp;&nbsp; :<input id="Text2" type=
    Price is hidden&nbsp; &nbsp;
    <Vulnerable>

    <input id="Hidden1" type="hidden" value = "5.0"/><br />

    </Vulnerable>
    <input id="Hidden1" type="hidden" value="5.0" /><br />
    &nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp;
    &nbsp; &nbsp; &nbsp; &nbsp; &nbsp;<input id="Reset1" typ
    <input id="Submit1" type="submit" value="submit" />
```



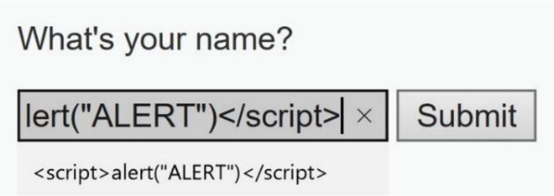
```
<input type="hidden" id="price" value="10000.00">
```

```
price="1.00"
```

Cross Site Scripting (XSS)

Attackers inject their own malicious scripts onto web pages and have it executed by the user’s browser

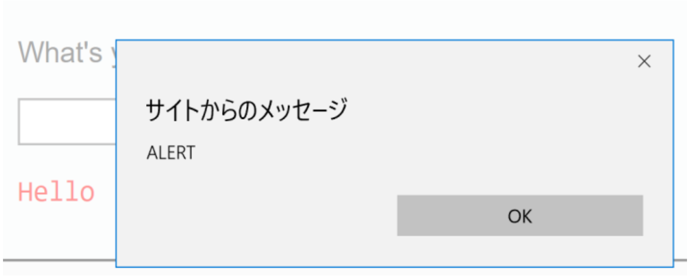
◎Basic example:



What's your name?

lert("ALERT")</script>

<script>alert("ALERT")</script>



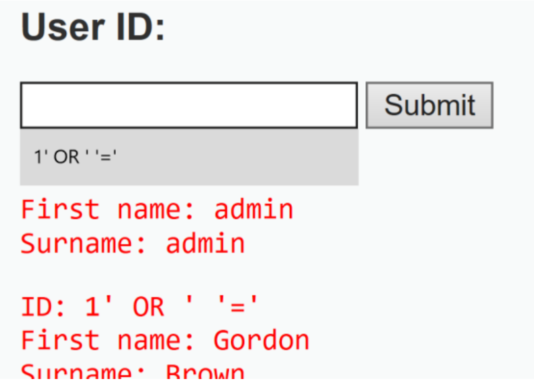
サイトからのメッセージ

ALERT

SQL Injection

Attacker adding his own SQL Statements in user input

◎ Very Basic example: 1' OR ' '='



1' OR ' '='

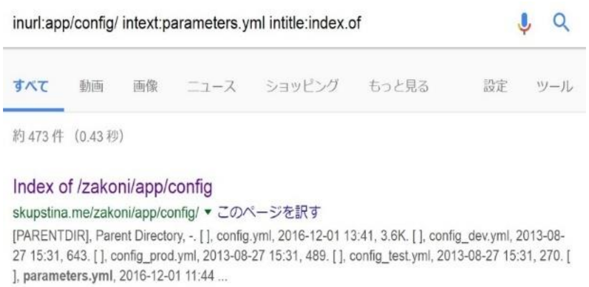
```
First name: admin
Surname: admin

ID: 1' OR ' '='
First name: Gordon
Surname: Brown
```

Google hacking

Using properly Google can be utilized as a security scanner

◎Exploit db

https://www.exploit-db.com/google-hacking-database/

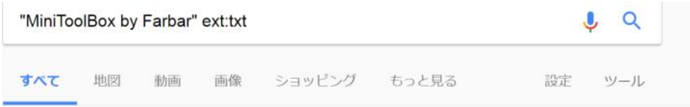

inurl:app/config/ intext:parameters.yml intitle:index.of

約 473 件 （0.43 秒）

Index of /zakoni/app/config

skupstina.me/zakoni/app/config/ ▾ このページを訳す

[PARENTDIR], Parent Directory, -. [ ], config.yml, 2016-12-01 13:41, 3.6K. [ ], config_dev.yml, 2013-08-27 15:31, 643. [ ], config_prod.yml, 2013-08-27 15:31, 489. [ ], config_test.yml, 2013-08-27 15:31, 270. [ ], **parameters.yml**, 2016-12-01 11:44 ...


"MiniToolBox by Farbar" ext:txt

References

- OWASP

  https://www.owasp.org/index.php/OWASP_Vulnerable_Web_Applications_Directory_Project/Pages/VMs
  https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
  https://www.owasp.org/images/a/a8/OWASPTop10ProactiveControls2016-Japanese.pdf
  https://www.owasp.org/index.php/Top_10_2017-Top_10

- Rapid7

  https://community.rapid7.com/docs/DOC-1875