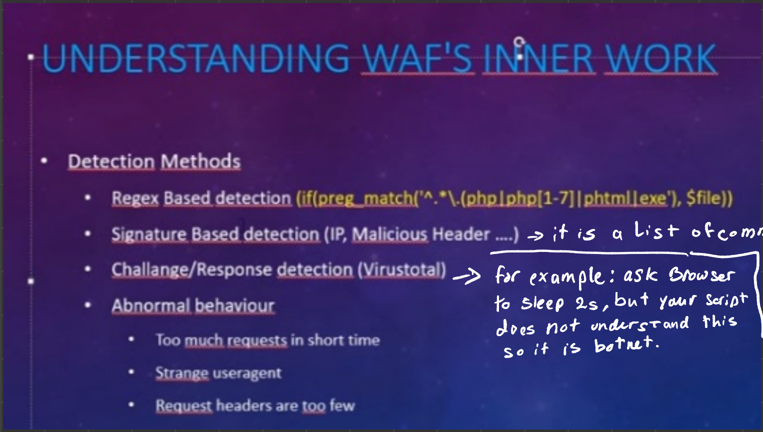
web application firewall

Example of WAF's: Modesecrity, F5, NetScaler, Webknight

- Modesecrity → free
- F5 → most famous powerfull

* WAF operational Modes:

- learning Mode → He works to know what parameters there is and what type of data they accept } WAF now knows that parameter id accept just numbers.
  any.com/lo?id=1
- passive Mode → Monitor user input and detect abnormal behavior (detect, no action) } any.com/lo?id=1<script>...
  this is something new it is maybe malicious so WAF save all data user like IP, User-Agent, time ....
- Active Mode → Same as what passive mode do but with action like (ip block, request block). the admin set this action.

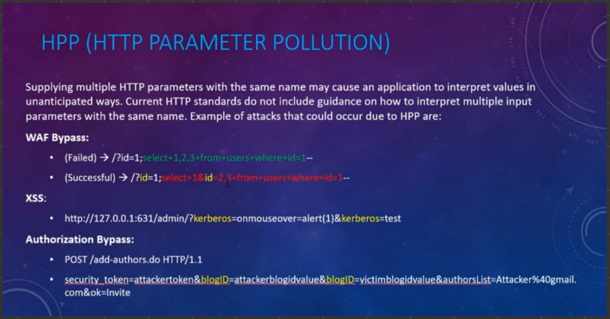


UNDERSTANDING WAF'S INNER WORK

- Detection Methods
  - Regex Based detection (if(preg_match('^.*\.(php|php[1-7]|phtml|exe'), $file))
  - Signature Based detection (IP, Malicious Header ....) → it is a list of commands. if someone inject a code WAF will compare the code, if match, then He will block + He have list of black ip.
  - Challange/Response detection (Virustotal) → for example: ask Browser to sleep 2s, but your Script does not understand this so it is botnet.
  - Abnormal behaviour
    - Too much requests in short time
    - Strange useragent
    - Request headers are too few

Bypassing:

regular expressions: See the video 33



HPP (HTTP PARAMETER POLLUTION)

Supplying multiple HTTP parameters with the same name may cause an application to interpret values in unanticipated ways. Current HTTP standards do not include guidance on how to interpret multiple input parameters with the same name. Example of attacks that could occur due to HPP are:

WAF Bypass:

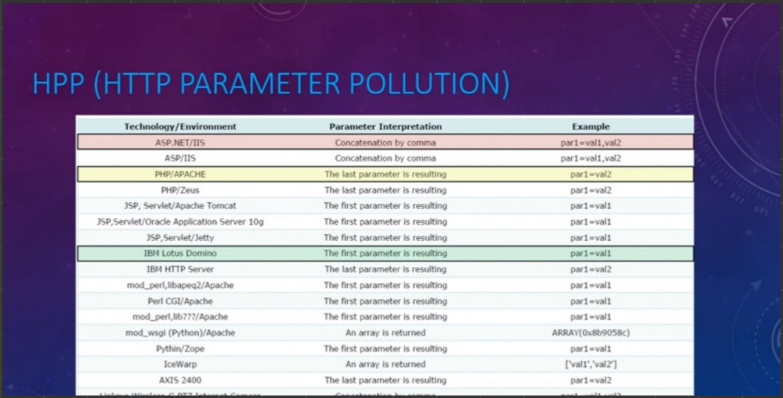
- (Failed) → /?id=1;select+1,2,3+from+users+where+id=1--
- (Successful) → /?id=1;select+1&id=2,3+from+users+where+id=1--

XSS:

- http://127.0.0.1:631/admin/?kerberos=onmouseover=alert(1)&kerberos=test

Authorization Bypass:

- POST /add-authors.do HTTP/1.1
- security_token=attackertoken&blogID=attackerblogidvalue&blogID=victimblogidvalue&authorsList=Attacker%40gmail.com&ok=Invite



HPP (HTTP PARAMETER POLLUTION)

Technology/Environment	Parameter Interpretation	Example
ASP.NET/IIS	Concatenation by comma	par1=val1,val2
ASP/IIS	Concatenation by comma	par1=val1,val2
PHP/APACHE	The last parameter is resulting	par1=val2
PHP/Zeus	The last parameter is resulting	par1=val2
JSP, Servlet/Apache Tomcat	The first parameter is resulting	par1=val1
JSP,Servlet/Oracle Application Server 10g	The first parameter is resulting	par1=val1
JSP,Servlet/Jetty	The first parameter is resulting	par1=val1
IBM Lotus Domino	The first parameter is resulting	par1=val1
IBM HTTP Server	The last parameter is resulting	par1=val2
mod_perl,libapeq2/Apache	The first parameter is resulting	par1=val1
Perl CGI/Apache	The first parameter is resulting	par1=val1
mod_perl,lib???/Apache	The first parameter is resulting	par1=val1
mod_wsgi (Python)/Apache	An array is returned	ARRAY(0x8b9058c)
Pythin/Zope	The first parameter is resulting	par1=val1
IceWarp	An array is returned	['val1','val2']
AXIS 2400	The last parameter is resulting	par1=val2
Linksys Wireless-G PTZ Internet Camera	Concatenation by comma	par1=val1,val2