**UNIVERSIDADE DE BRASÍLIA – FACULDADE UnB GAMA**

**Disciplina:** Técnicas de Programação **Professor:** Maurício Serrano

**Componentes do grupo**: - Jessica Suzuki 11/0014065

- Priscilla Gonçalves 11/0039106

- Tainara Santos Reis 10/0131280

- Yeltsin Soares

FERRAMENTA DE ANÁLISE ESTÁTICA RIPS –

TUTORIAL DE INSTALAÇÃO

RIPS é uma ferramenta escrita em PHP para encontrar vulnerabilidades em aplicações PHP usando análise estática de código. Por tokenização e parsing de todos os arquivos de código fonte RIPS é capaz de transformar o código-fonte PHP em um modelo de programa para detectar funções potencialmente vulneráveis​ que podem ser contaminados por userinput (influenciado por um usuário mal-intencionado), durante o fluxo do programa. Além da saída estruturada de vulnerabilidades encontradas, RIPS também oferece uma estrutura de framework de código integrado, para posterior análise manual.

Entre algumas das features apresentas pelo RIPS temos:

RIPS consegue identificar por padrão diversas vulnerabilidades em sua aplicação, em sua grande maioria as listadas no OWASP Top 10 são identificadas. Segue abaixo uma pequena lista das principais vulnerabilidades identificadas pela aplicação:

* Code Execution
* Command Execution
* Cross-Site Scripting
* Header Injection
* File Disclosure
* File Inclusion
* File Manipulation
* LDAP Injection
* SQL Injection
* XPath Injection

A interface de auditoria de código do RIPS consiste de algumas funcionalidades muito interessantes, entre elas podemos citar:

* Estatísticas referentes ao Scans e as vulnerabilidades da aplicação
* Linhas de código vulneraveis são agrupadas
* Descrição das Vulnerabilidades com exemplo de código, PoC e patch
* Engine que permite a criação do Exploit para explorer a vulnerabilidade encontrada
* Exibição gráfica de arquivos (conectada pelos includes)
* Exibição gráfica de funções (conectadas pelas calls)
* Userinput list (parámetros da aplicação)
* Visualização do código fonte com destaque em funções e parâmetros

Entre muitas outras que permitem que você faça o debug da aplicação utilizando inclusive expressões regulares. Efetuando a análise estática do código com RIPs, você consegue rapidez ao executar a análise (executar uma análise estática manualmente pode ser dolorosamente demorado). Você consegue identificar blind/non-blind SQL exploitation, detectar backdoors em seu código entre outras vantagens.