

## ওয়েব সার্ভার হ্যাকিং

ওয়েব সার্ভার হ্যাকিং হলো ওয়েব সার্ভার এর কর্তৃপক্ষকে না জানিয়ে কোন ওয়েব সার্ভার থেকে তথ্য সংগ্রহ করা। এই কাজটি হ্যাকাররা সহজেই করতে পারে যদি প্রোগ্রামে কোন বাগ থাকে অথবা ভুল কনফিগারেশন করা থাকে। যেমন- ডিফল্ড ইউজার নেইম এবং পাসওয়ার্ড, বিভিন্ন প্লাগিন টেস্ট না ব্যবহার করা, রিমুট একসেস এনাবল রাখা, অপ্রয়োজনীয় সার্ভিস অন রাখা ইত্যাদি। তাই যখন কোন ওয়েব সার্ভার তৈরি করা হবে অবশ্যই ভাল করে টেস্ট করে নিতে হবে।

আমরা সাধারণত যে ধরনের ভুল কনফিগারেশন গুলো করে থাকি-

ওয়েব সার্ভার হ্যাকিং এর ধাপসমূহ-

ধাপ-০১: ওয়েব সার্ভার এর তথ্য সংগ্রহ

ধাপ-০২: ওয়েব সার্ভার এর দুর্বল দিকগুলো বের করা

ধাপ-০৩: ওয়েব সার্ভার এর মিররিং করা

ধাপ-০৪: সেশন হাইজ্যাকিং

ধাপ-০৫: ওয়েব সার্ভার এর পাসওয়ার্ড সংগ্রহ

ধাপ-০১: ওয়েব সার্ভার এর তথ্য সংগ্রহ

Whois থেকে যেকোন ওয়েব সার্ভার এর তথ্য খুব সহজেই বের করতে পারবেন।

ধাপ-০২: ওয়েব সার্ভার এর দুর্বল দিকগুলো বের করা

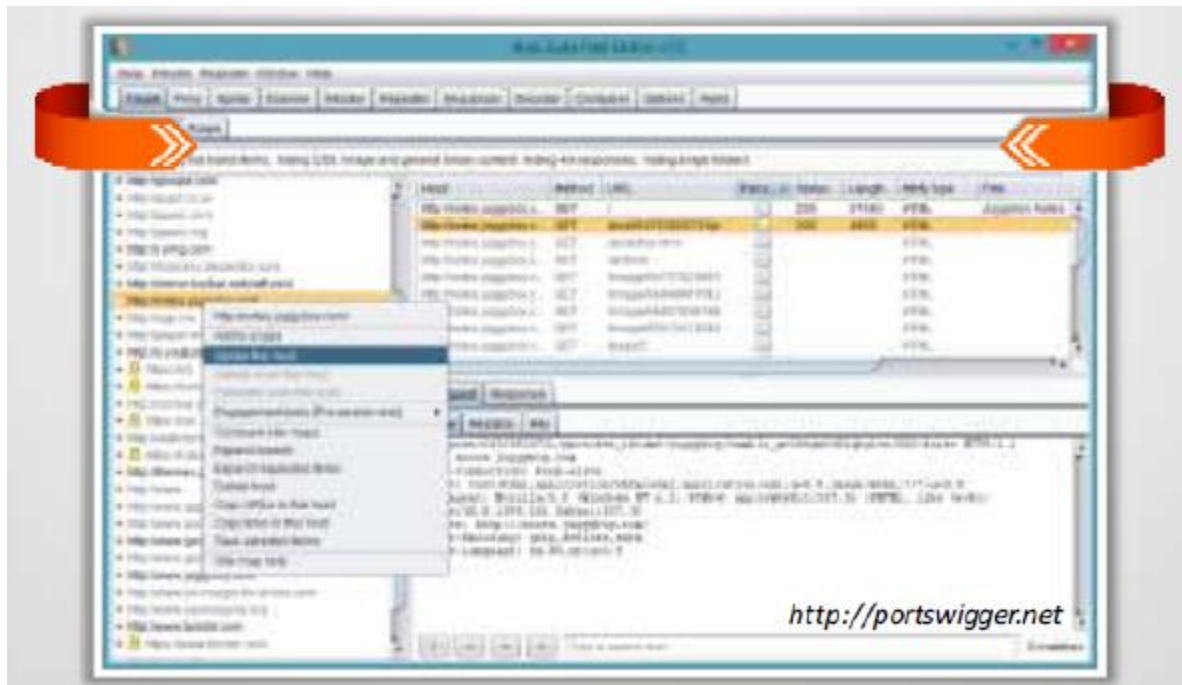
যেমন- ডিফল্ড ইউজার নেইম এবং পাসওয়ার্ড, বিভিন্ন প্লাগিন টেস্ট না ব্যবহার করা, রিমুট একসেস এনাবল রাখা, অপ্রয়োজনীয় সার্ভিস অন রাখা ইত্যাদি

ধাপ-০৩: ওয়েব সার্ভার এর মিররিং করা

HTTrack দিয়ে খুব সহজেই সাইট মিররিং করা যায়

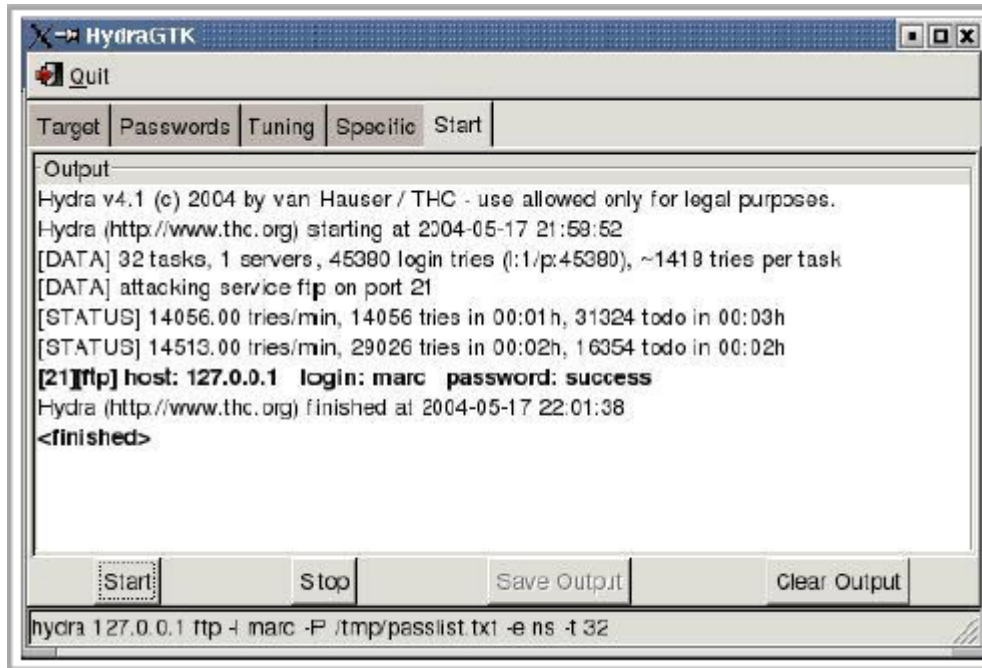
ধাপ-০৪: সেশন হাইজ্যাকিং

Burp, JHijack ইত্যাদি টুল ব্যবহার করে সেশন হাইজ্যাকিং করা যায়।



খাপ-০৫: ওয়েব সার্ভার এর পাসওয়ার্ড সংগ্রহ

THC-Hydra টুল ব্যবহার করে ওয়েব সার্ভার এর পাসওয়ার্ড সংগ্রহ করা যায়।




কিভাবে ওয়েব সার্ভারকে হ্যাকার এর হাত থেকে রক্ষা করা যায়?

১. ওয়েব সার্ভার এর প্যাচ নিয়মিত আপডেট করতে হবে।
২. ওয়েব সার্ভার এর ব্যাকআপ রাখতে হবে।
৩. ফায়ারওয়াল এর মাধ্যমে অনাকাঙ্খিত ট্রাফিক এবং পোর্টগুলো ব্লক করতে হবে।
৪. ডিফল্ট ইউজার নেইম/পাসওয়ার্ড, ডিফল্ট কনফিগারেশন এগুলো বাদ দিতে হবে।
৫. সঠিক সিকিউরিটি সাটিফিকেট ইন্সটল করতে হবে।

৬. ওয়েব সার্ভার এর মনিটরিং টুল ব্যবহার করতে হবে। যেমন- HackAlert

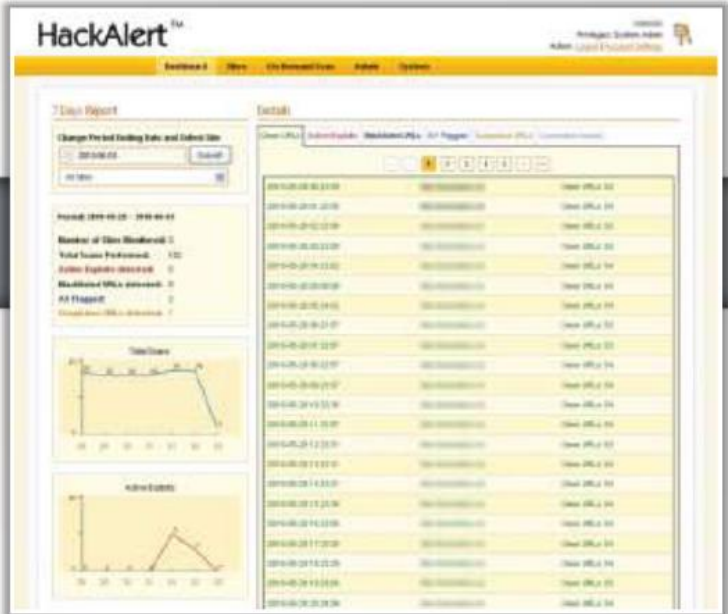
## Web Server Malware Infection Monitoring Tool: HackAlert



HackAlert is a **cloud-based service** that identifies hidden zero-day malware and drive-by downloads in websites and online advertisements

### Features

- Protects clients and customers from malware injected websites
- Identifies malware
- Displays injected code snippets
- Deploys as cloud-based SaaS
- Integrates with WAF or web server modules for instant mitigation



The screenshot displays the HackAlert dashboard. On the left, there's a sidebar with navigation options like Dashboard, Alerts, Site Remediation, Malware, and Settings. The main area shows a 'Status Report' with a 'Change First and Lasting Date and Column Size' filter. Below this, there are two line graphs: 'Total Counts' and 'Active Counts'. The central part of the dashboard is a table listing detected malware infections. The table has columns for 'IP Address', 'URL', 'Detection Time', and 'Status'. The table contains multiple rows of data, showing various IP addresses and URLs that have been flagged for malware infection.

| IP Address   | URL                    | Detection Time      | Status |
|--------------|------------------------|---------------------|--------|
| 192.168.1.1  | http://www.example.com | 2019-01-01 10:00:00 | Clean  |
| 192.168.1.2  | http://www.example.com | 2019-01-01 10:00:00 | Clean  |
| 192.168.1.3  | http://www.example.com | 2019-01-01 10:00:00 | Clean  |
| 192.168.1.4  | http://www.example.com | 2019-01-01 10:00:00 | Clean  |
| 192.168.1.5  | http://www.example.com | 2019-01-01 10:00:00 | Clean  |
| 192.168.1.6  | http://www.example.com | 2019-01-01 10:00:00 | Clean  |
| 192.168.1.7  | http://www.example.com | 2019-01-01 10:00:00 | Clean  |
| 192.168.1.8  | http://www.example.com | 2019-01-01 10:00:00 | Clean  |
| 192.168.1.9  | http://www.example.com | 2019-01-01 10:00:00 | Clean  |
| 192.168.1.10 | http://www.example.com | 2019-01-01 10:00:00 | Clean  |
| 192.168.1.11 | http://www.example.com | 2019-01-01 10:00:00 | Clean  |
| 192.168.1.12 | http://www.example.com | 2019-01-01 10:00:00 | Clean  |
| 192.168.1.13 | http://www.example.com | 2019-01-01 10:00:00 | Clean  |
| 192.168.1.14 | http://www.example.com | 2019-01-01 10:00:00 | Clean  |
| 192.168.1.15 | http://www.example.com | 2019-01-01 10:00:00 | Clean  |
| 192.168.1.16 | http://www.example.com | 2019-01-01 10:00:00 | Clean  |
| 192.168.1.17 | http://www.example.com | 2019-01-01 10:00:00 | Clean  |
| 192.168.1.18 | http://www.example.com | 2019-01-01 10:00:00 | Clean  |
| 192.168.1.19 | http://www.example.com | 2019-01-01 10:00:00 | Clean  |
| 192.168.1.20 | http://www.example.com | 2019-01-01 10:00:00 | Clean  |
| 192.168.1.21 | http://www.example.com | 2019-01-01 10:00:00 | Clean  |
| 192.168.1.22 | http://www.example.com | 2019-01-01 10:00:00 | Clean  |
| 192.168.1.23 | http://www.example.com | 2019-01-01 10:00:00 | Clean  |
| 192.168.1.24 | http://www.example.com | 2019-01-01 10:00:00 | Clean  |
| 192.168.1.25 | http://www.example.com | 2019-01-01 10:00:00 | Clean  |
| 192.168.1.26 | http://www.example.com | 2019-01-01 10:00:00 | Clean  |
| 192.168.1.27 | http://www.example.com | 2019-01-01 10:00:00 | Clean  |
| 192.168.1.28 | http://www.example.com | 2019-01-01 10:00:00 | Clean  |
| 192.168.1.29 | http://www.example.com | 2019-01-01 10:00:00 | Clean  |
| 192.168.1.30 | http://www.example.com | 2019-01-01 10:00:00 | Clean  |